УКРАЇНА

(19) **UA** (11) **125677** (13) **C2**

(51) МПК (2022.01)
H04L 12/00
H04L 45/24 (2022.01)
H04L 45/60 (2022.01)
H04L 65/1046 (2022.01)
H04W 12/03 (2021.01)

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНЕ ПІДПРИЄМСТВО "УКРАЇНСЬКИЙ ІНСТИТУТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ"

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2020 06658**

(22) Дата подання заявки: **02.04.2018**

(24) Дата, з якої є чинними права інтелектуальної власності: **12.05.2022**

(31) Номер попередньої заявки відповідно до Паризької конвенції: **62/480,696**

(32) Дата подання попередньої заявки відповідно до Паризької конвенції: **03.04.2017**

(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку: **US**

(41) Публікація відомостей про заявку: **27.01.2021, Бюл.№ 4**

(46) Публікація відомостей про державну реєстрацію: **11.05.2022, Бюл.№ 19**

(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору PCT: **PCT/US2018/025695, 02.04.2018**

(72) Винахідник(и):
Вільямс Річард К. (US),
Верзун Євген (UA),
Голуб Олександр (UA)

(73) Володілець (володільці):
ЛІСТАТ ЛТД.,
Suite 5, Garden City Plaza, Mountainview Boulevard, Belmopan, Belize (BZ)

(74) Представник:
Кістерський Тимофій Арсенійович, реєстр. №457

(56) Перелік документів, взятих до уваги експертизою:
US 2016/219024 A1, 28.07.2016
US 2011/194692 A1, 11.08.2011
WO2016/003525 A2, 07.01.2016

(54) МЕТОДИ ТА ПРИСТРІЙ ГІПЕРЗАХИЩЕНОГО ЗВ'ЯЗКУ "ОСТАННЬОЇ МИЛІ"

(57) Реферат:

Даним винаходом описано способи приховування вмісту зв'язку між клієнтським пристроєм, наприклад, мобільним телефоном або ноутбуком, а також мережею або хмарою медіавузлів. Серед цих способів - маршрутизація пакетів даних у комунікації до різних вузлів шлюзу в "хмарі", відправка пакетів по різних фізичних носіях, таких як Ethernet-кабель або Wi-Fi-канал, і маскування пакетів шляхом надання їм різних адресатів-джерел. Також описано методику відключення звуку деяких учасників конференц-дзвінка і гіперзахищений метод зберігання файлів даних.

UA 125677 C2

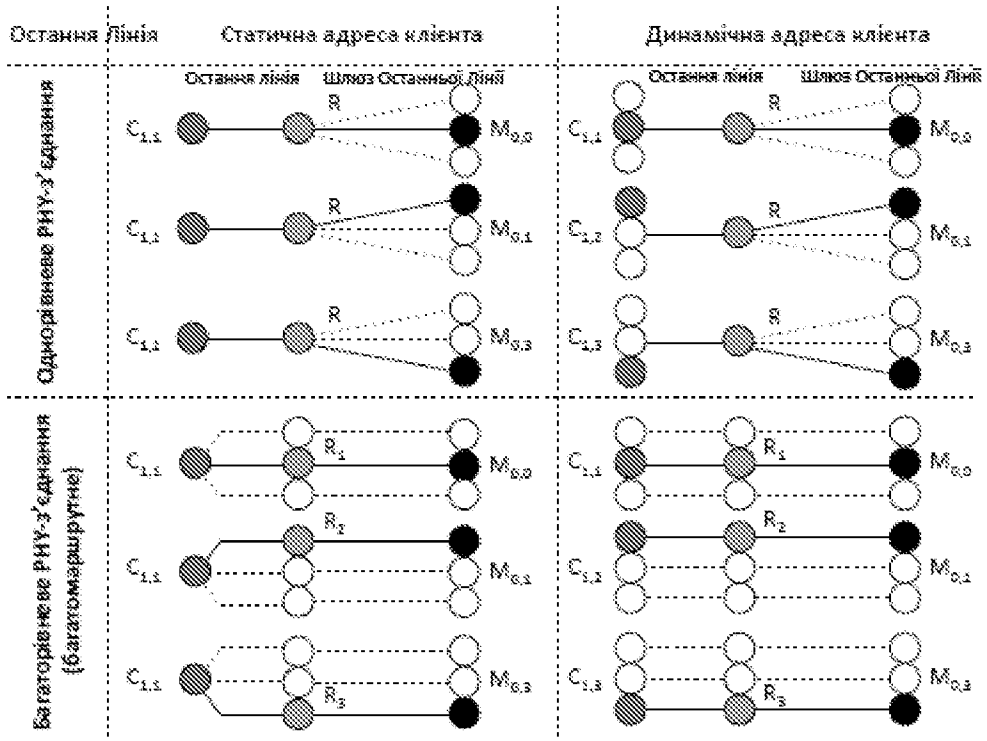

Остання Лінія
Статична адреса клієнта
Динамічна адреса клієнта
Остання лінія
Шлюз Останньої Лінії
Одноразове РНУ-з'єднання
Багаторазове РНУ-з'єднання (багатомаршрутне)

Рис. 52C

Зв'язок із спорідненим заявками

Дана заявка стверджує пріоритетність попереднього патентування в США 62/480,696, поданої 3 квітня 2017 року, і є частковим продовженням заявки 14/803,869, названої "Динамічна Захищена Комунікаційна Мережа та Протокол, " поданої для попереднього патентування 20 липня 2015 року, що, свою чергу, стверджує пріоритетність попередньої заявки на патентування в США 62/107,650, поданої 26 січня 2015 року.

Кожна з перерахованих вище заявок включена в даний документ в якості довідкового матеріалу в повному обсязі.

Область техніки, до якої належить винахід

Даний винахід відноситься до методів і пристроїв, що забезпечують гіперзахищений зв'язок "Останньої Милі" між пристроєм і шлюзом мережі або хмари.

Огляд відомих технічних рішень

Удосконалення систем зв'язку сприяло прогресу цивілізації з найбільш ранніх стадій розвитку людства. Від кур'єрів та посланців, піших або на коні; доставки поштових відправлень на поїзді, автомобілі та літаку; до появи телеграми та телеграфу, телефону, радіо, телебачення, комп'ютерів, стільникового телефону; Інтернету, електронної пошти та Всесвітнього павутиння; а останнім часом через соціальні мережі, голосовий зв'язок через Інтернет, M2M-підключення, Інтернет речей (IoT) і Інтернет всього (IoE), зв'язок завжди прокладав шлях до використання новітніх технологій. З впровадженням кожного нового покоління телефонного технологічного обладнання число людей, між якими встановлювався зв'язок, і швидкість передачі інформації між ними також збільшувалася.

Ефект цієї тенденції полягає в тому, що людство взаємопов'язане більш ніж коли-небудь в історії, при цьому люди довіряють комунікаційним технологіям та покладаються на них як на засіб безпечної та надійної доставки своєї конфіденційної, особистої, сімейної та фінансової інформації тільки тим, з ким вони мають намір зв'язатися. Знання та інформація зараз можуть в лічені секунди поширюватися серед мільйонів людей, а для друзів та членів сім'ї спілкуватися один з одним, попутно займаючись іншими справами, так само просто, як натиснути кнопку. Часто кажуть: "світ тісний".

Незважаючи на те, що такий прогрес надзвичайно корисний для всіх, у нашій великій залежності від технологій є також і негативні наслідки. Не дивно, що, коли система зв'язку не виконує свої функції, наприклад, під час землетрусу або при складних погодних умовах, люди стають дезорієнтованими або навіть впадають в паніку від того, що їх "відключили", навіть якщо це тимчасово. Якість обслуговування, або QoS (англ. Quality of Service – якість обслуговування), системи зв'язку при цьому є критично важливим показником ефективності мережі зв'язку. Душевний спокій, фінансове благополуччя, самосвідомість і навіть саме життя людей залежать від надійності та захищеності з'єднання.

Іншим ключовим аспектом мережі зв'язку є її здатність забезпечити конфіденційність, безпеку та захищеність для клієнта, що її використовує. У міру розвитку комунікаційних технологій також розвивалася і витонченість злочинців та "хакерів", які мають намір наносити шкоду, руйнувати системи, красти гроші та випадково або зловмисно шкодити іншим. Шахрайство з кредитними картами, викрадення паролів, крадіжка особистих даних і несанкціонована публікація конфіденційної інформації, особистих фотографій, файлів, електронних листів, текстових повідомлень та приватних твітів (вкрадених, щоб скомпрометувати або шантажувати жертву) є лише кількома прикладами сучасної кіберзлочинності.

Щоб виділити епідемічну частку проблеми захищеності в сучасних відкритих мережах зв'язку, нижче перераховані відомі приклади порушень конфіденційності та кіберзлочинності на момент оформлення даної заявки на видачу патенту (наведені в хронологічному порядку):

- "Мета: викрадення інформації не менше ніж у 70 млн. чоловік", - CNBC, 10 січня 2014 р.
- "Хакери відправляють шкідливі електронні листи на розумний холодильник та телевізор", - BGR (www.bgr.com), 20 січня 2014 р.
- "Nest відновлює роботу з Google після проблем з конфіденційністю та злому термостата", - Slash Gear (www.slashgear.com) 24 червня 2014 р.
- "Захищеність даних утриманні під питанням через піратське захоплення облікових записів. Лінія, керована додатком безкоштовного виклику та обміну повідомленнями, була вражена недавньою низкою порушень безпеки даних. Додаток виявив, що до сотень облікових записів користувачів отримано несанкціонований доступ сторонами, які не є користувачами цих облікових записів", - Nikkei Asian Review, 2 липня 2014 р.
- "Звичайні американці, залучені до перевірки даних Агентством національної безпеки, заявляють про претензії", - AP, 6 липня 2014 р.

- "Витік паролів Wi-Fi через розумні світлодіодні лампи", - BBC News, 8 липня 2014 р.

- "Шестеро людей звинувачені в шахрайстві під час продажу квитків на престижні заходи через StubHub." StubHub був мішенню хакерів, які використовували вкрадені паролі та номери кредитних карт для покупки та продажу тисячі квитків на концерти поп-музики і гри "Нью-Йорк Янкіз", - зробила заяву влада Нью-Йорка", - Bloomberg 24 липня 2014 р.

- "Дослідження показують, що Інтернет речей" дуже легко піддається злому", - International Business Times (www.ibtimes.com), 4 серпня 2014 р.

- "Російські хакери вкрали понад мільярд інтернет-паролів", - New York Times, 5 серпня 2014 р.

- "Новий витік інформації, яка розкриває секрети США, - підсумовує уряд", - CNN, 6 серпня 2014 р.

- "Хакери отримують доступ до кореневого каталогу термостата Google Nest за 15 секунд", - Enquirer (www.theinquirer.net), 11 серпня 2014 р.

- "Dairy Queen зламано тим же шкідливим ПЗ, яке вразило Target", - Christian Science Monitor, 29 серпня 2014 р.

- "Жертви серед знаменитостей в результаті несанкціонованого доступу до фотографій в оголеному вигляді - вразливість захисту облікових записів iCloud", - CBS News 1 вересня 2014 р.

- "Home Depot може стати новою метою несанкціонованого доступу до кредитних карток … Злом Home Depot може мати набагато серйозніші наслідки, ніж Target (40 млн. карток вкрадено протягом трьох тижнів)", - Fortune 2 вересня 2014 р.

- "Таємничі фейкові вежі стільникового телефонного зв'язку перехоплюють дзвінки на всій території США", - Business Insider 3 вересня 2014 р.

- "Хакерська атака: від банків до роздрібної торгівлі, ознаки кібервійни?" - Yahoo Finance 3 вересня 2014 р.

- "Home Depot підтверджує злом платіжної системи в магазинах США та Канади", - Fox News 9 вересня 2014 р.

- "Yahoo веде судову війну з урядом США через стеження", - CBS/AP 11 вересня 2014 р.

- "Ваша медична карта для хакерів варта більше, ніж ваша кредитна карта", - Reuters, 24 вересня 2014 р.

- "Червоний рівень тривоги: HTTPS зламаний. Використання браузера для атаки на SSL/TLS (BEAST) буде вважатися одним з найгірших зломів (worst hacks [орфографія та пунктуація оригіналу]), тому що ставить під загрозу з'єднання з браузером, на безпеку якого щодня покладаються сотні мільйонів людей", - InfoWorld, 26 вересня 2014 р.

- "Кібератака Sony, що почалася з дрібної неприємності, стрімко переросла у великий скандал", - New York Times, 30 грудня 2014 р.

Дивлячись, як відбувається ескалація темпів кіберзлочинності, порушень безпеки, крадіжки особистих даних та вторгнення до приватного життя, виникає питання: "Чому всі ці кібератаки можливі та що можна зробити, щоб зупинити їх?" У той час як суспільство прагне до підвищення конфіденційності та захищеності, споживачі також потребують більшої комунікабельності, більш дешевого зв'язку підвищеної якості, а також в підвищенні зручності проведення фінансових транзакцій.

Щоб зрозуміти, в чому полягають обмеження якісних характеристик та вразливість сучасних мереж зв'язку, засобів зберігання даних і мережевих пристроїв, спочатку потрібно зрозуміти, як сучасний електронний, оптичний та радіозв'язок працює, транспортує та зберігає дані, в тому числі файли, електронну пошту, текст, аудіо інформацію та відеозображення.

Робота телефонної мережі з комутацією каналів

Електронний зв'язок включає в себе велику кількість апаратних компонентів або мережевих пристроїв, підключених за допомогою дротів, радіоліній, радіорелейних або волоконно-оптичних ліній зв'язку. Інформація передається з одного пристрою до іншого шляхом відправки електричної або електромагнітної енергії через цю мережу з використанням різних методів вбудовування або кодування інформаційного "контенту" в потік даних. Теоретично закони фізики встановлюють максимальну швидкість передачі даних для таких мереж що дорівнює швидкості світла, але в більшості випадків практичні обмеження в кодуванні даних, маршрутизації і управлінні трафіком, відношення сигнал-шум, а також подолання електричного, магнітного та оптичного шуму і небажаних паразитних сигналів спотворюють потік інформації або створюють перешкоди його проходженню, обмежуючи можливості мережі зв'язку до якоїсь частини від її ідеальної продуктивності.

Історично, електронна передача даних була вперше здійснена з використанням виділених "дротяних" електричних з'єднань, що утворюють "мережу" зв'язку між двома або кількома електрично мережевими пристроями. При роботі телеграфу за допомогою механічного ключа

вручну замикають і розмикають електричну мережу постійного струму, намагнічуючи соленоїд, який в свою чергу переміщує металевий важіль, викликаючи в слухаючому пристрої або "реле" клацання з такими ж інтервалами часу, з якими відправник натискає ключ. При цьому відправник використовував узгоджену мову, наприклад, азбуку Морзе, для кодування інформації та перетворення її в імпульсний потік. Аналогічно, слухач також повинен був розуміти азбуку Морзе - послідовність довгих і коротких імпульсів, які називаються точками та тире, щоб розшифрувати повідомлення.

Пізніше Александер Грем Белл розробив перший телефон, користуючись поняттям "хвилеподібного струму", нині званого змінним струмом, щоб переносити звук за допомогою електричного з'єднання. Телефонна мережа складалася з двох магнітних перетворювачів, з'єднаних електричною мережею, в якій кожен магнітний перетворювач складався з рухомої діафрагми та котушки, або "звукової котушки", оточеній нерухомою оболонкою з постійних магнітів. Під час розмови біля цього перетворювача, зміна тиску повітря, що була викликана звуком, змушує звукову котушку виконувати зворотно-поступальне переміщення в навколишньому магнітному полі, створюючи змінний струм в котушці. На стороні слухача струм, що змінюється в часі, протікаючи в звуковій котушці, створює ідентичне коливання та магнітне поле, що змінюється в часі, протилежне навколишньому магнітному полю, змушуючи звукову котушку виконувати зворотно-поступальне переміщення у такий же спосіб, що і пристрій, який записує звук. Результуюче переміщення забезпечує відтворення звуку у такий же спосіб, що і пристрій, який записує звук. Говорячи сучасною простою мовою, коли перетворювач перетворює звук в електричний струм, він працює як мікрофон, а коли перетворювач перетворює електричний струм у звук, він працює як гучномовець. Крім того, оскільки електричний сигнал, що передається, є аналогом звукового сигналу, який переноситься як звичайна хвиля тиску в повітрі, тобто звук, на даний час такі електричні сигнали називають аналоговими сигналами або аналоговими коливаннями.

Оскільки перетворювач, як було описано вище, використовується і для розмови, і для прослуховування, під час бесіди обидві сторони повинні знати, коли говорити і коли слухати. Як в струні зі з'єднаних жерстяних банок, в такій системі абонент не може одночасно говорити та слухати. Незважаючи на те, що така одностороння робота, яка називається "напівдуплексним" режимом, може здатися архаїчною, насправді вона як і раніше широко використовується в радіозв'язку в даний час в портативних радіостанціях, а в сучасній телефонії вона називається "push-to-talk" (натисни та говори) або PTT.

Згодом широкого поширення набули повнодуплексні (тобто, двосторонні або приймально-передавальні) телефони з окремими мікрофонами та гучномовцями, де сторони могли говорити та слухати одночасно. Але навіть сьогодні при роботі з повнодуплексним телефонним зв'язком потрібно приділяти належну увагу запобіганню зворотного зв'язку – стані, при якому звук, що надходить у мікрофон, повертається до того, хто телефонує, створюючи відлуння, а іноді і неприємний свист - проблеми, які особливо характерні для телефонного зв'язку на великій відстані.

Ранні телеграфні та телефонні системи мали ще один недолік - відсутність конфіденційності. У цих ранніх реалізаціях мереж зв'язку кожен, підключений до цієї мережі, чує все, що передається по даній мережі, навіть якщо він цього не хоче. У сільських телефонних мережах ці загальні мережі називалися "лініями колективного користування". Потім система телефонного зв'язку швидко перетворилася в багатоканальні мережі, в яких місцевий телефонний вузол підключав виділені канали безпосередньо до телефонів індивідуальних клієнтів. У місцевому пункті зв'язку системний оператор вручну з'єднував абонентів один з одним через комутатор за допомогою перемичок, а також мав можливість підключатися до іншого пункту зв'язку, та вперше надавати послуги телефонних переговорів "на великій відстані". Великі комплекси, що містять велику кількість реле, що утворюють телефонні "комутаційні" мережі, поступово замінювали людину-оператора, а згодом та вони були замінені електронними перемикачами на вакуумних лампах.

Після того, як в кінці 1950-х років в компанії Bell Laboratories розробили транзистор, автоматичні та місцеві телефонні станції з їх крихкими і швидконагріваючими лампами замінили спочатку твердотільними пристроями - що охолоджуються під час роботи - на транзисторах, а потім і пристроями на інтегральних схемах. З розвитком мережі, число цифр телефонного номера збільшувалось від семизначного префікса та особистого номера до додавання кодів регіонів і, у підсумку, кодів країн, для обробки міжнародних викликів. Мідні кабелі, що передають голосові виклики, швидко покривали весь світ та перетинали океани. Незалежно від величини мережі, принцип дії залишався незмінним - виклики представляли собою пряме електричне з'єднання або "мережу" між абонентами з передачею голосу аналоговими сигналами та з

маршрутизацією виклику, яка визначається автоматичною телефонною станцією. Таку телефонну систему зрештою стали називати "телефонною мережею з комутацією каналів" або в розмовній мові - традиційною телефонною мережею (POTS – Plain Old Telephone System). Пік розвитку телефонії з комутацією каналів припав на 1980-і роки, а згодом відбувалася її планомірна заміна "телефонією з комутацією пакетів", що розглядається в наступному розділі.

Майже паралельно з телефонною мережею відбувався розвиток регулярного радіозв'язку, який починався з радіомовлення в 1920-х роках. Це мовлення було односпрямованим, здійснювалося радіомовними станціями на спеціальних частотах, що надавались за ліцензією уряду, а прийом здійснювався будь-якою кількістю радіоприймачів, налаштованих на цю частоту мовлення або радіостанцію. Радіомовний сигнал був аналоговим або з амплітудною модуляцією (АМ), або пізніше з частотною модуляцією (ЧМ) у виділеній ділянці ліцензійного радіоспектра. У США для управління наданням і регулюванням таких ліцензійних діапазонів була створена Федеральна комісія зі зв'язку (FCC). Концепція мовлення була поширена на ефірні телевізійні програми, які використовують радіопередачу, яка спочатку складалась з чорно-білого, а потім і кольорового контенту. Згодом також з'явилися можливості доставляти телевізійні сигнали до будинків людей або за допомогою радіорелейної супутникової антени, або через коаксіальні кабелі. Оскільки будь-який слухач, налаштований на конкретну частоту мовлення, може приймати мовленнєвий сигнал, термін "мультимовлення" тепер використовується для односпрямованого багатокористувацького зв'язку.

Одночасно з появою радіомовлення почалося створення перших систем двостороннього зв'язку для торгових та військових океанських суден, та до початку Другої світової війни радіостанції перетворилися в дуплексні переносні приймачі, які об'єднують передавачі та приймачі в єдиному пристрої. Як і телефонні системи, перші системи повнодуплексного радіозв'язку працювали в "симплексному" режимі, що дозволяє здійснювати передачу тільки однієї радіомовної станції по одному радіоканалу, в той час як інші слухали. Після об'єднання передавачів та приймачів, що працюють на різних частотах, стали можливими одночасна передача та прийом на кожному кінці радіолінії, забезпечуючи можливість повнодуплексного режиму зв'язку між двома сторонами.

Однак для запобігання перекриття передачі від декількох сторін для управління каналом зазвичай використовується протокол, званий напівдуплексним або push-to-talk (натисни і говори), що дозволяє здійснювати передачу виключно за певним каналу за принципом "першим прийшов - першим обслужений". Стандартні промислові типи радіостанцій, що використовують аналогову модуляцію, включають аматорські (хем-радіо та безліцензійні) радіостанції, морські УКХ-радіостанції, радіостанції універсальної об'єднаної системи зв'язку UNICOM (Universal Integrated Communication) для управління повітряним рухом і радіостанції FRS для особистого спілкування. У цих мережах двостороннього радіозв'язку радіостанції відправляють свої дані по конкретних частотних "каналах" на центральну вежу радіозв'язку, а базова станція підсилює та ретранслює сигнал, передаючи його по всій мережі радіозв'язку. Кількість доступних частот, що передають інформацію в широкомовній області, визначає загальну смугу пропускання системи та кількість користувачів, які можуть одночасно незалежно обмінюватися даними в цій мережі радіозв'язку.

Щоб розширити загальну пропускну здатність мережі радіозв'язку для роботи більшого числа абонентів, в 1970-х роках була продемонстрована та протягом десятиліття набула широкого поширення концепція мережі, в якій велика площа розбита на більш дрібні частини або "стільники" радіозв'язку. Стільникова концепція полягала в тому, щоб обмежити широкомовний діапазон вишки радіозв'язку меншим простором, тобто меншою дальністю зв'язку, і, отже, отримати можливість використовувати одні й ті ж смуги частот для одночасної роботи різних абонентів, що знаходяться в різних стільниках. Для цього було створено програмне забезпечення для управління перемиканням виклику при переході з одного стільника в сусідній без "зникнення сигналу" і раптового відключення виклику. Так само, як і традиційна телефонна мережа (POTS), повнодуплексний радіозв'язок, а також радіо- та телемовлення, спочатку мережі стільникового зв'язку були аналоговими за своєю природою. Для управління маршрутизацією викликів була прийнята система телефонних номерів для визначення належного бездротового електричного з'єднання. Цей вибір також був корисний тим, що він дозволив легко підключити нову бездротову стільникову мережу до традиційної телефонної "провідної" системи, забезпечивши міжмережеві з'єднання та спільну роботу в рамках цих двох систем.

Починаючи з 1980-х років, телефонний і радіозв'язок, поряд з радіо та телевізійним мовленням, почали невблаганний перехід з методів і форматів аналогового зв'язку на цифрові, що було обумовлено необхідністю знизити енергоспоживання та збільшити термін служби

акумуляторів, поліпшити якість за рахунок підвищення продуктивності співвідношення сигнал-шум, а також почати приділяти увагу необхідності передачі даних та тексту голосом. З'явилися такі формати радіозв'язку, як EDACS і TETRA, здатні одночасно забезпечувати режими зв'язку "один-до-одного", "один-до-багатьох" та "багато-до-багатьох". Стільниковий зв'язок також швидко перейшов на цифрові формати, такі як GPRS, і телевізійне мовлення.

До 2010 року більшість країн припинило або знаходилося в процесі припинення всього аналогового телевізійного мовлення. На відміну від ефірного телебачення, у провайдерів кабельного телебачення не було необхідності переходити на цифровий формат, і вони підтримували гібридний склад аналогових та цифрових сигналів аж до 2013 року. Їх остаточний перехід на цифрові методи був мотивований не державними стандартами, а комерційними причинами - необхідністю розширення кількості доступних каналів мережі, щоб мати можливість доставляти контент високої (HD) та надвисокої (UHD) чіткості, пропонувати більше послуг платного телебачення (PPV, також відомих як "одностороння передача даних"), а також надавати послуги цифрового зв'язку з високою пропускною спроможністю для своїх клієнтів.

Незважаючи на те, що прийнято зіставляти перехід глобальних мереж зв'язку з аналогового формату на цифровий з появою Інтернету і, більш конкретно, з прийняттям і широким поширенням інтернет-протоколу (IP), перехід на цифровий формат передував комерційному визнанню IP в телефонії, забезпечуючи, якщо не прискорений, то універсальний перехід зв'язку на IP і "мережі з комутацією пакетів" (що розглядаються в наступному розділі).

Результатом еволюція телефонного зв'язку з комутацією каналів стала "абонентська мережа зв'язку" (PSTN), що включає об'єднання радіозв'язку, стільникового зв'язку, міні-АТС, а також POTS-з'єднань та підмереж, кожна з яких включає різнорідні технології. Ця мережа включає в себе шлюзи абонентської мережі зв'язку, з'єднані магістральними лініями з високою пропускною здатністю, а також, наприклад, підключення через дротяні з'єднання шлюз POTS, мережа стільникового зв'язку, міні-АТС та мережа двостороннього радіозв'язку. Кожна підмережа працює незалежно, керуючи пристроями відповідного типу.

Абонентська мережа зв'язку також підключається до стільникових мереж з комутацією каналів, використовуючи аналогові і цифрові протоколи AMPS, CDMA і GSM. Через вежу стільникового зв'язку мережі стільникового зв'язку з комутацією каналів з'єднуються з використанням стандартизованих частот стільникового радіозв'язку з такими мобільними пристроями, як мобільні телефони. У разі мереж GPRS, надбудови над технологією GSM, мережі стільникового зв'язку з комутацією каналів можуть також з'єднуватися з планшетами, одночасно забезпечуючи низькошвидкісну передачу даних і голосу. Мережі повнодуплексного радіозв'язку, такі як TETRA і EDACS, з'єднують абонентські мережі зв'язку з портативними радіостанціями і більшими вбудованими та настільними радіостанціями через вишки радіозв'язку високої потужності та радіо з'єднання. Такі мережі повнодуплексного радіозв'язку, які зазвичай використовуються працівниками поліції, швидкої допомоги, парамедиками, пожежними і навіть працівниками портових установ, також вважаються службовими мережами та службами зв'язку, та призначені для урядових, муніципальних служб та ліквідаторів надзвичайних ситуацій, а не для звичайних споживачів. (Примітка. Використовувані тут терміни "стаціонарний комп'ютер", "планшет" і "ноутбук" використовуються в якості скороченого посилання на комп'ютери відповідного типу).

На відміну від шлюзу POTS, мережі стільникового зв'язку та міні-АТС, які використовують традиційні телефонні номери для виконання маршрутизації викликів, мережа повнодуплексного радіозв'язку використовує виділені радіоканали (а не номери телефонів) для організації радіоліній між вишкою і мобільними пристроями, які вона обслуговує. Таким чином, системи службового радіозв'язку зберігають явно виражені та унікальні відмінності від мереж стільникових телефонів для звичайних споживачів.

Таким чином, мережі зв'язку PSTN дозволяють гнучко поєднувати між собою підмережі, заснованих на різних технологіях. Саме ця різноманітність визначає внутрішню слабкість сучасних мереж з комутацією каналів - можливість спільної роботи підмереж. Оскільки різні підмережі не здійснюють зв'язок відповідно до будь-яких загальних протоколів управління або мовою, і оскільки кожна технологія обробляє передачу даних і голосу по-різному, ці різні системи по суті несумісні, за винятком їх обмеженої можливості направити телефонний виклик через основну магістраль абонентської мережі зв'язку або міжміські магістральні лінії. Наприклад, під час терористичної атаки 11 вересня в Центрі міжнародної торгівлі в Нью-Йорку багато рятувальників з різних районів США юрмилися в Мангеттені, намагаючись допомогти в боротьбі з катастрофою, тільки щоб дізнатися систему радіозв'язку, їх радіостанції були несумісні з обладнанням добровольців з інших країн і міст, що унеможливлювало управління централізованим командуванням та контролем зусиль з надання допомоги. Через відсутність

стандартизації протоколів зв'язку, їх радіостанції просто не могли встановити зв'язок одна з одною.

Крім того, при безпосередньому електричному та радіо з'єднанні телефонних мереж з комутацією каналів, особливо з використанням аналогових або незахищених цифрових протоколів, для хакера не складає труднощів за допомогою радіо сканеру знаходити активні канали зв'язку і аналізувати, відбирати, прослуховувати або перехоплювати розмови, що відбуваються в даний момент часу. Оскільки абонентська мережа зв'язку утворює "постійно включений" канал або мережу зв'язку між сторонами, що спілкуються, у хакера достатньо часу, щоб ідентифікувати з'єднання і "використати його": у законний спосіб урядовими організаціями, замовивши прослуховування за рішенням федерального суду; або злочинним шляхом: кіберзлочинцями або урядовими організаціями, що здійснюють незаконне, заборонене або несанкціоноване спостереження. Визначення законного і незаконного шпигунства та спостереження та зобов'язання оператора мережі зі співробітництва в цій діяльності в різних країнах суттєво різняться і є предметом гарячих суперечок серед таких глобальних компаній, як Google, Yahoo і Apple, що працюють на багатьох міжнародних напрямках. Мережі зв'язку та Інтернет є глобальними та не знають кордонів, але закони, що регулюють таку електронну інформацію, є місцевими, та підкоряються юрисдикційному органу уряду, який в даний час контролює внутрішній та міжнародний зв'язки і торгівлю.

Незалежно від його законності або етики, електронне відстеження та спостереження сьогодні є звичайним явищем, починаючи від моніторингу за допомогою камер відеоспостереження, розташованих на кожному розі вулиці і над усіма автошляхами та лініями метрополітену, до складного злому і розшифровки кодів, що виконується різними підрозділами та агентствами національної безпеки держав. Незважаючи на те, що вразливі місця мають всі мережі, архаїчні та недостатні засоби захисту абонентських мереж зв'язку роблять їх особливо легкими для злому. Таким чином, абонентська мережа зв'язку, навіть підключена до захищеної сучасної мережі, є слабкою ланкою в загальній системі та створює вразливе місце, що дозволяє долати захист та здійснювати кіберзлочин. Проте, ще потрібно багато років, якщо не десятиліть, для виходу з глобальної абонентської мережі зв'язку та її повної заміни на мережу зв'язку з комутацією пакетів на основі IP. Такі мережі з комутацією пакетів (розглядаються нижче), хоча вони і більш сучасні, ніж абонентська мережа зв'язку, як і раніше не захищені від подолання засобів захисту, злому, атак, що викликають відмову в обслуговуванні (DoS-атак), та розкритті конфіденційної інформації.

Робота мережі зв'язку з комутацією пакетів

Якщо роботу сучасної телефонної мережі з комутацією каналів можна образно уявити, як дві бляшані банки, з'єднані струною, то аналогічним образним поданням роботи мереж зв'язку з комутацією пакетів може служити робота поштового відділення. У такому підході текст, дані, голос та відео перетворюються в файли та потоки цифрових даних, та потім ці дані об'єднуються в квантовані "пакети" даних, які передаються по мережі. Механізм передачі заснований на електронних адресах, які однозначно визначають, куди вирушає пакет даних та звідки він надходить. Формат та протокол зв'язку також передбачають включення інформації про характер даних, що містяться в пакеті, в тому числі про контент, призначений для програми або програм, в яких він буде використовуватися; а також для обладнання, що забезпечує фізичні канали зв'язку та електричні або радіо з'єднання для передачі пакетів.

Запропонована в 1960-х роках концепція мереж з комутацією пакетів була створена в самий розпал холодної війни після запуску радянського супутника. У той час Міністерство оборони США (МО) висловило занепокоєння у зв'язку з тим, що нанесення ракетно-ядерних ударів з об'єктів космічного базування може знищити всю комунікаційну інфраструктуру США, придушивши її здатність реагувати на попереджуючий удар СРСР, і що вразливість до такої атаки може дійсно спровокувати її. Тому МО профінансувало створення надлишкової системи зв'язку або решітчастої "мережі", в якій здатність мережі передавати інформацію між військовими об'єктами не могла бути порушена внаслідок знищення будь-якого конкретного каналу передачі даних або навіть великої кількості каналів передачі даних в мережі. Ця система, названа ARPANET, стала прабатьком Інтернету та горезвісною Євою сучасних цифрових комунікацій.

Незважаючи на створення мережі з комутацією пакетів, масового поширення Інтернету не відбувалося до 1990-х років, поки в результаті спільного впливу першого простого у використанні веб-браузера Mosaic, появи веб-сторінок на основі гіпертексту, швидкого впровадження Всесвітнього павутиння, а також широкого використання електронної пошти не відбулося глобальне прийняття інтернет-платформи. Один з основоположних принципів - відсутність централізованого контролю або необхідності в центральному комп'ютері - спонукали

до повсюдного використання Інтернету певною мірою тому, що ніяка країна і жодний уряд не могли його зупинити (або навіть повністю усвідомити глобальні наслідки цього), а також тому, що його призначену для користувача базу становили споживачі, які працюють на своїх нещодавно придбаних персональних комп'ютерах.

Ще одним наслідком зростання Інтернету стала стандартизація інтернет-протоколу (IP), що використовується для маршрутизації пакетів даних в мережі. До середини 1990-х років користувачі Інтернету усвідомили, що для тої самої мережі з комутацією пакетів, яка передає дані, також може використовуватися для передачі голосу, і незабаром після цього з'явилася технологія VoIP. Незважаючи на те, що концепція теоретично дозволяла будь-кому, хто має доступ до Інтернету, здійснювати голосовий зв'язок через Інтернет безкоштовно, затримки поширення в мережі знижували якість передачі мови та часто робили її нерозбірливою. Незважаючи на те, що, завдяки впровадженню високошвидкісних ліній Ethernet, високошвидкісного підключення Wi-Fi, покращенню якості зв'язку 4G на ділянці "останньої милі", час затримки зменшився, сам по собі Інтернет створювався для забезпечення точної доставки пакетів даних, а не для того, щоб гарантувати доставку цих пакетів в заданий час, тобто Інтернет не створювався для роботи в мережі реального часу.

Таким чином, мрія про використання Інтернету замість дорогих послуг провайдера телекомунікації залишилася практично невиконаною, незважаючи на наявність таких OTT-провайдерів (абр. від англ. Over the Top), як Skype, Line, KakaoTalk, Viber та інших. OTT-телефонія страждає від якості зв'язку QoS внаслідок неконтрольованої затримки в мережі, низької якості звуку, скидання виклику, луни, реверберації, зворотного поширення, переривчастого звуку та часто навіть від нездатності зробити виклик. Низька якість OTT-зв'язку за своєю суттю є вадою не технології VoIP, а самої мережі, в якій OTT-провайдери не мають можливості контролювати шлях проходження даних, або затримки, з якими здійснюється зв'язок. По суті, OTT-провайдери не можуть надати якість зв'язку, тому що OTT-зв'язок працює як автостоп в Інтернеті. За іронією долі, найкращим чином використовувати зв'язок на основі технології VoIP сьогодні можуть компанії, які є провайдерами міжнародного телефонного зв'язку з виділеними апаратними мережами з малим часом затримки - саме ті телефонні компанії, які мають найменшу мотивацію для цього.

Крім внутрішньо властивій їй мережевій надмірності, однією з найсильніших сторін зв'язку з комутацією пакетів є її здатність передавати інформацію від будь-якого джерела в будь-який пункт призначення, якщо дані впорядковані в пакетах, відповідних Інтернет-протоколу, та за умови, що пристрої зв'язку підключені до мережі та пов'язані з Інтернетом. Інтернет-протокол управляє здатністю мережі доставляти корисне навантаження в пункт призначення, не піклуючись і не турбуючись про те, яка інформація передається, або про те, яка програма буде її використовувати, виключаючи при цьому необхідність в настроюванні програмних інтерфейсів і дорогому пропрієтарному обладнанні. У багатьох випадках навіть додатки, пов'язані з корисним навантаженням, налаштовують на задані формати, наприклад, для читання електронної пошти, для відкриття веб-сторінки в браузері, для перегляду зображення або відео, перегляду файлу прошивки або читання PDF-документа і т.д.

Оскільки він використовує універсальний формат файлів, що дозволяють уникнути залежності від пропрієтарного або фірмового програмного забезпечення, Інтернет можна розглядати як комунікаційну платформу з "відкритим вихідним кодом", здатну встановлювати зв'язок з найширшим діапазоном мережевих пристроїв: від комп'ютерів до стільникових телефонів, від автомобілів до побутової техніки. Сучасний вислів, що описує цю універсальну зв'язність - це "Інтернет всього" (IoE).

Велика кількість комп'ютерів, в тому числі швидкодіючих хмарних серверів, і хмарне сховище даних, з'єднані лініями зв'язку з високою пропускною здатністю, зазвичай оптоволоконними, поряд з безліччю інших серверів (не показані), що формує хмару Інтернету. Образне уявлення у вигляді хмари в даному випадку доречно, тому що немає чітко визначеної межі, що визначає, які сервери вважаються частиною хмари, а які ні. Щодня і навіть щохвилини, одні сервери можуть виходити в Інтернет, а інші можуть бути відключені для обслуговування, що не робить ніякого впливу на функціональні можливості та продуктивність Інтернету. Ця перевага дійсно надлишкової розподіленої системи - немає єдиної точки управління і, отже, немає єдиної точки відмови.

Хмара може бути підключена до призначеного для користувача або інших мережних пристроїв за допомогою будь-якого з'єднання дротової, Wi-Fi або бездротової лінії зв'язку. Бездротовий телефонний зв'язок з комутацією пакетів використовує стільникові протоколи 3G, включаючи HSUPA і HSDPA, а також 4G/LTE. Стандарт LTE або "довготривалий розвиток" відноситься до мережевих стандартів, що забезпечують сумісність з різними стільниковими

протоколами, в тому числі, можливість безшовного перемикання телефонних дзвінків з одного стільника в інший, навіть якщо ці стільники працюють з різними протоколами. Примітка. В контексті цього документа терміном "остання миля" називається канал передачі даних між будь-яким типом клієнтського пристрою, наприклад, планшетом, стаціонарним комп'ютером або мобільним телефоном, і хмарним сервером. Залежно від напрямку передачі даних також іноді використовується термін "перша миля" для вказівки каналу передачі даних між абонентським пристроєм, який ініціює передачу даних і хмарним сервером. У таких випадках канал "остання миля" також є і каналом "перша миля".

При меншій дальності зв'язку точка доступу Wi-Fi з'єднується Wi-Fi радіо модулем зі смартфоном, планшетом, ноутбуком, стаціонарним комп'ютером або мережевим пристроєм побутової техніки і може використовуватися в локальних бездротових пристроях в будинках, кафе, ресторанах і офісах. Wi-Fi поширюється на зв'язок, що працює відповідно до стандартів IEEE для специфікацій 802.11a, 802.11b, 802.11g, 802.11n з однією частотою, а останнім часом для формату 802.11ac з двочастотним діапазоном. Засоби захисту Wi-Fi на основі простого статичного ключа входу в основному використовуються для запобігання несанкціонованому доступу до з'єднання, але не призначені для захисту даних протягом необмеженого часу від прослуховування або злому.

Розподілений блок дротових ліній може підключатися волоконно-оптичним кабелем, коаксіальним кабелем або по каналу Ethernet до ноутбука, стаціонарного комп'ютера, телефону, телевізійного приймача або мідною крученою парою дротів до телефонних ліній, що йдуть до касового терміналу торгової точки, що обслуговує стаціонарні або підключені дротовою лінією зв'язку центри торгівлі, в тому числі готелі, заводи, офіси, центри обслуговування, банки та будинки. Дротове підключення може включати розділення волоконно-оптичним або коаксіальним кабелем до дому, офісу, заводу або комерційної організації, підключені локально за допомогою модему для перетворення ліній передачі високошвидкісних даних (HSD) в лінії на основі Wi-Fi, Ethernet або мідною крученою пари дротів. У віддалених областях, де немає волоконно-оптичного або коаксіального кабелю, все ще використовується з'єднання по цифровій абонентській лінії (DSL), але з істотним зниженням швидкості передачі даних та надійності з'єднання. В цілому, враховуючи доступ по бездротових, Wi-Fi та провідних ліній зв'язку прогнозують, що до 2020 року кількість об'єктів, підключених до Інтернету в глобальному масштабі, досягне 20 мільярдів.

На відміну від мереж з комутацією каналів, які встановлюють та підтримують безпосереднє з'єднання між приладами, зв'язок з комутацією пакетів використовує адресу для "маршрутизації" пакета через Інтернет до пункту призначення. Таким чином, в мережах зв'язку з комутацією пакетів немає окремої виділеної мережі, яка підтримує з'єднання між пристроями зв'язку, і дані, проходячи через Інтернет, не йдуть по одному та тому ж конкретному шляху. Кожен пакет повинен знайти свій шлях через лабіринт взаємопов'язаних комп'ютерів, щоб потрапити в пункт призначення.

Наприклад, при маршрутизації IP-пакета від ноутбука до стаціонарного комп'ютера при використанні мережевого зв'язку з комутацією пакетів в процесі роботи перший пакет даних, відправлений з ноутбука в маршрутизатор Wi-Fi за допомогою бездротової технології, направляється до ряду DNS-серверів, де DNS (Domain Name Server) - сервер доменних імен. Завданням ряду DNS-серверів є перетворення текстового імені або номера телефону пристрою-адресата, в даному випадку стаціонарного комп'ютера, в IP-адресу. В результаті, IP-адреса передається з ряду DNS-серверів назад на адресу відправника, тобто ноутбуку.

Після цього ноутбук збирає свої пакети IP-даних та послідовно починає їх відправку адресату, спочатку через Wi-Fi радіомодуль до маршрутизатора Wi-Fi, а потім через мережу маршрутизаторів та серверів, які виступають в якості проміжних маршрутизаторів до адресата. Разом маршрутизатори і ряд комп'ютерних серверів працюють як вузли в Інтернеті, або як точки присутності, або POP (англ. Point Of Presence), тобто шлюзи з обмеженою зв'язністю, здатні здійснювати доступ до Інтернету. У той час як деякі маршрутизатори або сервери, що діють як точки присутності, підключаються до Інтернету за допомогою лише невеликої кількості сусідніх пристроїв, сервер, з'єднаний з великою кількістю пристроїв іноді називається "суперточкою присутності". Для більшої ясності слід зауважити, що термін POP (точка присутності) не слід плутати з ім'ям програми POP (англ. Plain Old Postoffice) або звичайним поштовим відділенням, використовуваним в поштових додатках.

Кожен маршрутизатор або сервер, який виступає в ролі маршрутизатора, містить в своїх файлах пам'яті таблицю маршрутизації, що ідентифікує IP-адреси, які він може адресувати, і, можливо, також адреси, які можуть адресувати маршрутизатори над ним. Ці таблиці маршрутизації автоматично завантажуються та встановлюються на кожному маршрутизаторі

при першому Інтернет-підключенні та зазвичай не завантажуються в процесі маршрутизації пакета через мережу. Коли IP-пакет входить в маршрутизатор, точку присутності або суперточку присутності, маршрутизатор зчитує достатню частину IP-адреси, як правило, цифри старших розрядів адреси, щоб знати, куди далі направляти пакет на його шляху до адресата. Наприклад, пакет, відправлений в Токіо з Нью-Йорка, може проходити спочатку через Чикаго, потім через сервери в Сан-Франциско, Лос-Анджелесі або Сіетлі, а потім вирушати в Токіо. І оскільки кількість маршрутизаторів, через які проходить пакет, і доступна швидкість передачі даних для кожного із з'єднань між маршрутизаторами розрізняються по інфраструктурі, а також з мережевого трафіку та завантаження, апріорі немає способу визначити, який шлях є найшвидшим або кращим.

На відміну від телефонного зв'язку з комутацією каналів, яка встановлює та підтримує безпосереднє з'єднання між клієнтами, для комутації пакетів даних немає універсального інтелекту, що переглядає Інтернет, щоб вирішити, який шлях є найкращим, оптимальним або найшвидшим для маршрутизації пакета, і немає ніякої гарантії, що два пакета, відправлених послідовно, підуть за одним та тим самим маршрутом. Таким чином, пакет "визначає" свій шлях через Інтернет на основі пріоритетів компаній, що експлуатують маршрутизатори та сервери, через які проходить цей пакет. Кожен маршрутизатор, по суті, містить певні таблиці маршрутизації і алгоритми маршрутизації, які визначають його кращі маршрути на основі стану мережі. Наприклад, переваги маршрутизатора можуть встановити високий пріоритет для відправки пакетів іншим маршрутизаторам, що належать тій же компанії, врівноважуючи трафік серед підключень до сусідніх маршрутизаторів, знаходячи найкоротшу затримку для наступного маршрутизатора, укладаючи прямі угоди зі стратегічними партнерами по бізнесу або створюючи лінію термінової відправки для VIP-клієнтів за рахунок пропуску якомога більшої кількості проміжних маршрутизаторів. Коли пакет надходить в маршрутизатор, немає способу дізнатися, чи були варіанти маршрутизації обрані конкретною точкою присутності з максимальним урахуванням інтересів відправника або оператора мережевого сервера.

Таким чином, в якомусь сенсі маршрут, по якому проходить пакет, залежить від часу і удачі. У попередньому прикладі маршрутизації від Нью-Йорка до Токіо сам маршрут і результуюча якість обслуговування можуть істотно змінюватися в залежності навіть від невеликих відхилень в дорозі, тобто в нелінійних рівняннях так званого "ефекту метелика". Розглянемо випадок, коли пакет з Нью-Йорка проходить через "маршрутизатор А" в Чикаго, і, через тимчасово високий трафік у Каліфорнії, він буде відправлений швидше в Мехіко, ніж у Каліфорнію. Потім маршрутизатор Мехіко відправляє IP-пакет в Сінгапур, звідки він, нарешті, відправляється в Токіо. Наступний пакет відправляється через "маршрутизатор В" в Чикаго, який при низькому трафіку в цей момент часу направляє пакет в Сан-Франциско, а потім прямо в Токіо всього за два "хмарних стрибка". В такому випадку другий пакет може прибути в Токіо раніше першого, спрямованого по більш довгому шляху. Цей приклад наочно ілюструє проблемне питання використання Інтернету для зв'язку в реальному часі, наприклад, для передачі онлайн-відео або технології VoIP в реальному часі, а саме те, що Інтернет не призначений для забезпечення гарантованого часу передачі або для контролю за затримками при передачі. Затримка може змінюватися від 50 мс до 1 с і більше тільки в залежності від того, через два сервера проходить пакет або через п'ятнадцять.

Відсутність контролю за маршрутизацією в Інтернеті є проблемою для додатків реального часу і, зокрема, є причиною низької якості обслуговування для OTT-провайдерів, які намагаються організувати надання VoIP (Voice over Internet Protocol)-телефонії, використовуючи Інтернет як безкоштовну інфраструктуру для своїх сервісів. Оскільки OTT-провайдери не контролюють маршрутизацію, вони не можуть контролювати затримку в мережі. Ще одна проблема зв'язку з комутацією пакетів полягає в тому, що можна легко заволодіти даними, не будучи виявленим. Якщо пірат перехоплює пакет та визначає IP-адресу його відправника або одержувача, він може різними методами перехоплювати дані від зламаних маршрутизаторів і або прослуховувати їх, або перенаправляти трафік через свою власну піратську мережу для здійснення шпигунського прослуховування розмови та навіть розшифровки зашифрованих файлів.

Вихідні та цільові IP-адреси відправника і одержувача та інша важлива інформація, яка використовується для маршрутизації пакета (а також використовувана кіберзлочинцями для злому пакета), представлені у вигляді рядка цифрових даних. IP-пакет містить цифрову інформацію, що визначає фізичне з'єднання між пристроями, спосіб організації даних для зв'язку пристроїв, мережеву маршрутизацію пакета, засоби забезпечення точності передачі корисних даних (корисного навантаження) та тип даних корисного навантаження, а потім самі дані корисного навантаження, призначені для використання різними прикладними програмами.

IP-пакет відправляється та приймається послідовно у вигляді ланцюжка послідовних цифрових бітів, організованих певним чином, який називається Інтернет-протоколом, та встановлений різними комітетами по стандартизації, в тому числі IETF (Internet Engineering Task Force - інженерним радою Інтернету) і іншими. Стандарт гарантує, що будь-який IP-пакет, що відповідає встановленому протоколу, може бути переданий та зрозумілий будь-яким мережним пристроєм, відповідним цьому ж IP-стандарту. Забезпечення зв'язку та спільної роботи мережевих пристроїв і додатків, підключених до Інтернету, є характерною особливістю Інтернету і керівним принципом організації Open Source Initiative (OSI), що не дозволяє будь-якій компанії, уряду або окремій особі взяти під контроль Інтернет або обмежити його доступність або функціональні можливості.

Модель OSI — це абстрактна конструкція, що складається з семи рівнів функціональних можливостей, яка точно визначає формат IP-пакета і кожного сегмента цього пакета. Кожна частина або "сегмент" IP-пакета відповідає даним, що застосовуються до функції конкретного рівня моделі OSI. Ці сім рівнів моделі OSI виконують такі ролі:

- Рівень 1 - фізичний рівень - містить конкретну інформацію про обладнання, що визначає фізичну природу зв'язку як електричні, радіо і оптичні сигнали, а також спосіб перетворення цих сигналів в біти для використання в системі зв'язку. Завданням рівня PHY (абревіатура від англ. Physical layer - фізичний рівень) є перетворення в потік бітів певних носіїв інформації, таких як Wi-Fi-радіо, Ethernet, послідовні порти, оптичне волокно, стільниковий радіозв'язок 3G або 4G, DSL на мідній кручений парі, USB, Bluetooth, кабельне або супутникове телебачення, цифрове аудіо мовлення, відео або мультимедіа контент. В IP-пакеті преамбула представляє дані рівня 1 та використовується для синхронізації всього пакета даних або "кадру" з передавачем та приймаючим обладнанням.

- Рівень 2 - канальний рівень, що містить біти, розташовані у вигляді кадрів, який визначає правила та засоби, за допомогою яких потоки бітів, передані з фізичного рівня 1, перетворюються в інтерпретовані дані. Наприклад, потоки бітів, засновані на даних Wi-Fi радіо модуля, можуть відповідати будь-якому заданому стандарту IEEE, в тому числі 802.11a, b, g, n і ac; сигнали радіозв'язку 3G можуть бути модульовані з використанням високошвидкісних методів пакетного доступу HSDPA або HSUPA; модульований світловий сигнал у волоконно-оптичній лінії або електричні сигнали в коаксіальному кабелі можуть бути декодовані в дані відповідно до стандарту DOCSIS 3 і т.д. В IP-пакеті дані рівня 2 охоплюють решту пакету з попереднім "заголовком каналу передачі даних" та завершувачем каналу передачі даних, які спільно визначають, коли починається та закінчується охоплюване корисне навантаження, а також забезпечують контроль за відсутністю втрат в процесі передачі. Одним з ключових елементів даних рівня 2 є MAC-адреса або адреса доступу до середовища, що використовується для направлення трафіку даних на конкретні адреси Ethernet, радіолінії або конкретні апаратні приймально-передавальні лінії.

- Рівень 3 - мережевий рівень або рівень Інтернету - містить пакети, "датаграми", що містять інформацію інтернет-протоколу (IP), яка використовується для маршрутизації IP-пакета, в тому числі, чи містить пакет дані IPv4 або IPv6 та відповідні IP-адреси відправника та одержувача, а також інформацію про характер корисних даних, що містяться в пакеті, наприклад, використовує даний тип протоколу управління передачею TCP (англ. Transmission Control Protocol – протокол управління передачею), протокол датаграм користувача UDP (англ. User Datagram Protocol) та ін. Рівень 3 також включає функцію запобігання утворенню "безсмертних" пакетів - IP-пакетів, які ніколи не доставляються, а й ніколи не вмирають. Спеціальний тип пакета рівня 3-ICMP (протокол міжмережевих керуючих повідомлень) - використовується для діагностики стану мережі, включаючи добре відому функцію "ping". В IP-пакеті рівень 3 містить "IP-заголовок" та включає дані про корисне навантаження, що міститься в сегментах транспортного та верхнього рівня.

- Рівень 4 - транспортний рівень - містить сегменти даних, що визначають характер з'єднання між комунікаційними пристроями, де протокол UDP визначає мінімальний опис корисного навантаження без встановлення з'єднання, а саме, наскільки великий обсяг корисного навантаження, чи є втрачені біти і яка служба додатків (порт) буде використовувати доставлені дані. Протокол UDP розглядається без встановлення з'єднання, оскільки він не підтверджує доставку корисного навантаження, натомість покладаючись на додаток для перевірки наявності помилок або втрати даних. Зазвичай UDP використовується для чутливого до часу зв'язку, наприклад, для широкомовної, багатомовної та онлайн-передачі, де повторне відправлення пакета не використовується. Навпаки, TCP забезпечує віртуальне з'єднання, підтверджуючи, що пакет і корисне навантаження достовірно доставлені до відправки наступного пакета та повторно відправляє недоставлені пакети. TCP також перевіряє цілісність

даних доставлених пакетів по контрольній сумі та включає засоби повторного складання несвоєчасно доставлених пакетів в їх первинному порядку. Як TCP, так і UDP визначають порти відправлення і отримання, опис служби або програми верхнього рівня, наприклад, веб-сервер або поштовий сервер, пов'язаний з інформацією, що міститься в корисних даних рівня 4. У IP-пакеті рівень 4 містить заголовок TCP/UDP і містить відомості про даних/корисного навантаження, включаючи контент, призначений для використання верхніми рівнями 5, 6 і 7 моделі OSI.

- Рівні 5, 6 і 7 - верхні або прикладні рівні - описують контент, що доставляється через Інтернет як дані/корисне навантаження. Рівень 7 - прикладний рівень - є найвищий рівень в моделі OSI та спирається на шість базових рівнів моделі OSI для підтримки як ПО з відкритим кодом, так та пропрієтарного прикладного програмного забезпечення. До часто використовуваних додатків рівня 7 відносяться електронна пошта з використанням SMTP, POP або IMAP; перегляд веб-сторінок з використанням HTTP (Chrome, Safari, Explorer, Firefox); передача файлів з використанням FTP і емуляція терміналу з використанням Telnet. Пропрієтарні програми включають набір продуктів Microsoft Office (Word, Excel, PowerPoint), Adobe Illustrator і Photoshop; додатки для роботи з базами даних Oracle і SAP; фінансове програмне забезпечення Quicken, Microsoft Money і QuickBooks; плюс аудіо- та відеоплеєри (наприклад, iTunes, QuickTime, Real Media Player, Window Media Player, Flash), а також такі програми для читання документів, як Adobe Acrobat Reader і Apple Preview. Додатки рівня 7 також зазвичай використовують вбудовані об'єкти, синтаксично визначаються рівнем 6 - представницьким рівнем - включає текст, графіку та зображення, звук та відео, такі презентації документів, як XML або PDF, а також такі функції захисту, як шифрування. Рівень 5 - сеансовий рівень - встановлює можливість підключення декількох додатків, наприклад, імпорт одного об'єкта в файл іншої програми і управління ініціюванням та завершенням сеансу.

Як описано вище, семирівнева модель OSI визначає функції кожного рівня, а відповідний IP-пакет включає дані, що відносяться до кожного рівня, один всередині іншого за принципом матрьошки ... Зовнішній пакет або фізичний рівень 1 визначає весь IP-кадр і містить інформацію, що відноситься до всіх більш високих рівнів. В рамках цих фізичних даних кадр даних рівня 2 описує канал передачі даних і містить мережеву датаграму рівня 3. Ця датаграма, в свою чергу, визначає рівень Інтернету як корисне навантаження, а сегмент даних рівня 4 описують транспортний рівень. Транспортний рівень передає дані верхнього рівня як корисне навантаження, в тому числі контент рівнів 5, 6 і 7. Це семирівневе вкладення іноді також мнемонічно співвідносять з фразою англійською мовою "all people seem to need data processing" (схоже, що всі люди мають потребу в обробці даних), в якій перші літери слів відповідають першими літерами назв семи рівнів, починаючи з самого верхнього: application (прикладний), presentation (представницький), session (сеансовий), transport (транспортний), network (мережевий), data-link (канальний) і physical (фізичний).

У той час як нижні рівні - фізичний і канальний - пов'язані з обладнанням, середні рівні моделі OSI, що включаються в IP-пакет для опису мережевої та транспортної інформації, абсолютно незалежні від апаратної платформи, що використовується для здійснення зв'язку та доставки IP-пакета. Більш того, верхні рівні, що включаються як корисне навантаження транспортного рівня, специфічні тільки для додатків, для яких вони призначені, та працюють абсолютно незалежно від маршрутизації пакета і його доставки через Інтернет. Таке розділення дозволяє незалежно контролювати кожен рівень, підтримуючи величезну кількість можливих комбінацій технологій і користувачів, які не потребують організаційного схвалення формату пакета або перевірки життєздатності корисного навантаження пакета. Неповні або неправильні IP-пакети просто відкидаються. Таким чином, мережі з комутацією пакетів здатні маршрутизувати, транспортувати та передавати різноманітну інформацію, пов'язану з додатками, в різнорідних комунікаційних середовищах узгодженим чином між будь-якими мережевими пристроями або об'єктами, підключеними до Інтернету.

Підводячи підсумок, слід зазначити, що мережі з комутацією каналів вимагають одного безпосереднього з'єднання між двома або кількома сторонами, що зв'язуються (подібно традиційній телефонній мережі), в той час як в мережах з комутацією пакетів здійснюється поділ документів, звуку, відео та тексту з кількох пакетів, що передаються декількома мережевими шляхами (аналогічно поштовому відділенню, котрі використовують оптимальний варіант для забезпечення точної та своєчасної доставки), а потім виконується складання вихідного контенту з підтвердженням того, що на цьому шляху нічого не втрачено. Порівняння абонентської мережі зв'язку з комутацією каналів та технології VoIP з комутацією пакетів представлено в наступній таблиці:

Мережа	Абонентська мережа зв'язку (PSTN)	Інтернет
Технологія	З комутацією каналів	З комутацією пакетів
Підключення	Виділена електрична лінія зв'язку	Кожен пакет маршрутизується через Інтернет
Передача даних	У режимі реального часу (мережа)	Оптимальний варіант (пакет)
Сигнал	Аналоговий або цифровий	Цифровий, IP, технологія VoIP
Контент	Голос	Голос, текст, дані, відео
Швидкість передачі даних	Низька	Висока
Контроль помилок	Відсутня або мінімальний	Глибокий
Вплив пошкодження лінії зв'язку	Не здійснений або перерваний виклик	Зміна маршруту виклику
Вплив відмови електроживлення	Електроживлення забезпечує мережу	Потрібна резервна акумуляторна батарея

Тут слід зазначити, що, незважаючи на те, що абонентська мережа зв'язку (PSTN) працює в режимі реального часу, з'єднання електричної лінії зв'язку використовують методи "оптимального варіанту" доставки пакета і корисного навантаження, на відміну від поштового відділення, що використовує будь-які автомобілі та листонош, щоб в кінцевому підсумку доставити пошту, навіть якщо і доставлена із запізненням. Детальніше робота мережі і зв'язку описана в довідковому розділі спорідненої патентної заявки під назвою "Динамічна Захищена Комунікаційна Мережа та Протокол".

Розглядаючи якість роботи мережі, оцінюють кілька факторів, а саме:

- швидкість передачі даних, тобто пропускну здатність;
- якість обслуговування;
- захищеність мережі і даних;
- конфіденційність користувачів.

На підставі наведених вище міркувань швидкість передачі даних оцінюється мільйонами біт в секунду (Мбіт/с). Крім того, QoS враховує ще кілька чинників, в тому числі затримку, якість звуку, стабільність мережі, уривчастість роботи або часті переривання для обслуговування, порушення синхронізації або підключення, низьку потужність сигналу, зниження швидкості роботи додатків і функціональну мережеву надмірність в умовах надзвичайної ситуації. Кібербезпека спрямована на запобігання атак на мережу і запобігання несанкціонованого доступу до трафіку і контенту даних, включаючи кіберзлочинність, стеження, перехоплення IP-пакетів, опитування портів і атаки на відмову в обслуговуванні, профілювання, шахрайство, кіберінфікування, спостереження, і т.д.

Якість обслуговування

Якість обслуговування описує продуктивність мережі по ємності, пропускної спроможності, затримок, швидкості передачі даних, масштабованості, цілісності даних, якості звуку, швидкості передачі бітових помилок і інші параметри продуктивності. Для програм, файлів та перевірок, пов'язаних з безпекою, визначальним фактором є точність даних. Важливість факторів залежить від характеру корисного навантаження, що передається по мережі з комутацією пакетів. Навпаки, для голосу та відео, що включають додатки реального часу, ключовими є фактори, що впливають на час доставки пакета. Показники якості та їх вплив на різні додатки, такі як відео, голос, дані та текст відрізняються в залежності від додатку. Хороший стан мережі, що характеризується прийнятною формою сигналу IP-пакета з високою швидкістю передачі даних - це стан, що відрізняється мінімальними тимчасовими затримками, чистим сильним сигналом, відсутністю спотворень сигналу, стабільною роботою та відсутністю втрат передачі пакетів.

Переривчасті мережі, що характеризуються формою сигналу пакета зі зниженою швидкістю передачі даних з випадковими перериваннями, найбільш суттєво впливають на функції відео, викликаючи повільне завантаження звичайного відео і неприйнятну якість онлайн-відео. Перевантажені мережі, що працюють зі зниженою ефективною швидкістю передачі даних з регулярними короткочасними перериваннями, на прикладі форми сигналу IP-пакета, не тільки серйозно погіршують якість відео через рвані переривчасті рухи, розмите зображення і неправильну передачу кольору і яскравості, але й починають також погіршувати якість звукового або голосового зв'язку через перекручування, відлуння і навіть випадання речень з бесіди або саундтрека. Однак в перевантажених мережах дані все-таки можуть бути доставлені при використанні протоколу TCP за допомогою повторних запитів на ретрансляцію. Нестабільні мережі демонструють низьку пропускну здатність з численними зупинками і непередбачуваною

тривалістю передачі даних. Нестабільні мережі також містять пошкоджені IP-пакети, які при передачі на основі протоколу TCP повинні бути відправлені повторно, а при передачі на основі протоколу UDP просто відкидаються як пошкоджені або неправильні дані. При зниженні якості мережі до певного рівня навіть електронні листи стають переривчастими, та порушується синхронізація IMAP (англ. Internet Message Access Protocol - протокол доступу до електронної пошти Інтернету). Завдяки полегшеному формату даних, більшість SMS та текстових повідомлень будуть доставлені, хоча і з деякою затримкою, навіть при серйозному перевантаженні мережі, але вкладення завантажуватися не будуть. У нестабільних мережах може статися порушення роботи усіх програм і навіть припинення нормальної роботи комп'ютера або мобільного телефону в очікуванні доставки файлу. У таких випадках відео зависає, звук настільки змінюється, що стає нерозбірливим, VoIP-з'єднання багаторазово відкидаються, іноді навіть більше десятка разів протягом декількох хвилин виклику, а в деяких випадках не вдається підключитися взагалі. Аналогічно, передача електронних листів зупиняється або зависає, а круглі значки на екрані комп'ютера обертаються нескінченно. Індикатори виконання завдання зупиняються взагалі. Навіть текстові повідомлення відкидаються і приймають статус "не доставлених".

Незважаючи на те, що нестабільність мережі може виникати під впливом великої кількості факторів, в тому числі несправностей електроживлення серверів управління ключами і "суперточок присутності", перевантаження по числу викликів, передачі величезних файлів даних або UHD-фільмів, та під час активних DoS-атак (англ. Denial of Service -"відмова в обслуговуванні") на вибрані сервери або мережі, ключовими факторами, що використовуються для відстеження QoS мережі, є частота відкидання пакетів та затримка пакетів. Відкидання пакетів відбувається тоді, коли IP-пакет не може бути доставлений та по перевищенню ліміту часу визначається як "безсмертний", або, коли маршрутизатор або сервер виявляє помилку контрольної суми в заголовку IP-пакета. Якщо при передачі пакета використовується протокол UDP, цей пакет втрачається, при цьому прикладний рівень 7 повинен бути досить інтелектуальним, щоб дізнатися, що щось було втрачено. Якщо при передачі пакета на транспортному рівні 4 використовується протокол TCP, буде сформований запит для повторної передачі пакета, що збільшить навантаження на вже потенційно перевантажену мережу.

Інший фактор, що визначає QoS - затримку поширення - можна кількісно виміряти кількома способами: або як затримку передачі IP-пакета від вузла до вузла або, при односпрямованій передачі, від відправника до одержувача, або, в альтернативному варіанті, як час прийому-передачі від відправника до одержувача і назад до відправника. Ефект затримки поширення на доставку пакетів при використанні протоколів передачі даних UDP і TCP є різним. У міру збільшення міжмодової затримки поширення в мережі збільшується необхідний час прийому-передачі, наприклад, під час розмови з використанням технології VoIP. У разі UDP-передачі час прийому-передачі збільшується лінійно з затримкою поширення. Оскільки великі затримки поширення пов'язані з більш високою частотою помилок по бітам, кількість втрачених UDP-пакетів збільшується, але оскільки UDP запитує повторну передачу відкинутих пакетів, лінійна залежність часу прийому-передачі від затримки зберігається при збільшенні затримки. TCP-передача показує значно більш тривалий час прийому-передачі для кожного відправленого пакету, ніж UDP, через необхідність підтвердження встановлення зв'язку для підтвердження доставки пакета. Якщо частота помилок по бітам залишається низькою, і більшість пакетів не вимагають повторної відправки, то затримка поширення TCP збільшується лінійно з міжмодовою затримкою поширення. Якщо, проте, мережа зв'язку стає нестабільною, в міру збільшення затримки поширення, то час прийому-передачі, пов'язаний з передачею по протоколу TCP, експоненціально зростає через передбачену протоколом необхідність повторної передачі відкинутих пакетів. Таким чином, застосування TCP протипоказано для додатків, чутливих до часу передачі, таких як технологія VoIP і онлайн-відео.

Оскільки весь пакетний зв'язок має статистичний характер, та в ньому немає двох пакетів з однаковим часом поширення, найкращим способом оцінки мережевої затримки для односпрямованої передачі є вимірювання часу прийому-передачі великої кількості IP-пакетів однакового розміру з подальшим розділенням навпіл для оцінки затримки односпрямованої передачі. Затримка до 100 мс вважається відмінною, до 200 мс - дуже хорошою і до 300 мс - ще допустимою. Затримки поширення величиною 500 мс, що є характерною для OTT додатків в Інтернеті, створюють некомфортні умови для користувачів та заважають нормальній розмові. Зокрема, в процесі голосового зв'язку такі тривалі затримки поширення створюють "погане" звучання і можуть призводити до виникнення реверберації, створюючи "дзвінкий" або металевий звук, перериваючи розмову, коли інша сторона чекає відповіді на свій останній коментар, та в результаті мова стає спотвореною або нерозбірливою.

Для більшої ясності, затримка при односпрямованій передачі даних відрізняється від результату ping-тесту, що виконується за допомогою утиліти ICMP рівня 3 (наприклад, програми безкоштовного тестування мережі на сайті http://www.speedtest.net), частково через те, що ICMP - пакети зазвичай менш об'ємні, в порівнянні з реальними IP-пакетами, оскільки в ping-тесті не використовується функція TCP "запит на повторну відправку", а також тому, що немає ніякої гарантії, що при передачі по загальнодоступній мережі Інтернету маршрут ping-тесту буде відповідати фактичному маршруту пакета. По суті, виходить, що якщо сигнал ping-тесту приходить з великою затримкою, то це означає, що щось не так з мережею або з будь-яким зв'язком між пристроєм і мережею, наприклад, в маршрутизаторі Wi-Fi або на ділянці останньої милі, але хороший результат ping-тесту сам по собі не може гарантувати малу величину затримки поширення реального пакета.

З метою підвищення захищеності мережі часто використовуються методи шифрування та верифікації для запобігання злому, перехоплення або шпигунства. Але складне шифрування та протоколи шифрування з декількома ключами постійно підтверджують ідентичність співрозмовників, створюють додаткові затримки та тим самим збільшують ефективну затримку мережі, знижуючи якість обслуговування за рахунок підвищення захищеності.

Інформаційна безпека та конфіденційність інформації

До основних понять в галузі зв'язку відносяться інформаційна безпека і конфіденційність інформації. Ці два поняття, хоча вони і пов'язані, дещо відрізняються один від одного. "Інформаційна безпека, що включає мережеву безпеку, комп'ютерну безпеку та захищений зв'язок, охоплює методи, використовувані для контролю, перехоплення та запобігання несанкціонованого доступу, неправильного використання, модифікації або відмови від обслуговування комп'ютера або мережі зв'язку, доступних для мережі ресурсів або даних, що містяться в мережевих пристроях. Такі дані можуть включати в себе особисту інформацію, біометричні дані, фінансові записи, записи про здоров'я, особисті повідомлення та записи, а також приватні фотографії та відеозаписи. До мережевих пристроїв відносяться стільникові телефони, планшети, ноутбуки, стаціонарні комп'ютери, файлові сервери, сервери електронної пошти, веб-сервери, бази даних, сховища персональних даних, хмарні сховища, підключені до Інтернету побутові прилади, автомобілі з мережевими можливостями, а також загальнодоступні пристрої, що використовуються окремими особами, такі як касові апарати або POS-термінали, бензоколонки, банкомати і т.д.

Очевидно, що кіберзлочинці і комп'ютерні хакери, які намагаються отримати несанкціонований доступ до захищеної інформації, скоюють злочин. Якщо незаконно отримані дані містять особисту інформацію, атака також є порушенням недоторканності особистого життя жертви. Однак, з іншого боку, порушення конфіденційності можуть відбуватися без порушення закону і, фактично, не можуть бути попереджені. У сьогоднішньому мережевому світі несанкціоноване використання особистої інформації людини може здійснюватися без порушення вимог до інформаційної безпеки. У ряді випадків компанії, що збирають дані для будь-якої однієї мети, можуть продати свою базу даних іншим клієнтам, зацікавленим у використанні цих даних для іншої мети. Навіть коли Microsoft купила Hotmail, було добре відомо, що список розсилки був проданий рекламодавцям, зацікавленим в розсилці інформації потенційним клієнтам. Чи вважаються такі дії порушенням конфіденційності інформації, залишається спірним питанням.

"Конфіденційність інформації", що включає конфіденційність в Інтернеті, конфіденційність комп'ютера та приватне спілкування, має на увазі персональне право особистості або повноваження розпоряджатися своєю особистою і конфіденційною інформацією і її використанням, в тому числі на збір, зберігання, спільне використання або обмін інформацією з іншими. Конфіденційна інформація може включати інформацію, що ідентифікує особу, в тому числі зріст, вагу, вік, відбитки пальців, групу крові, номер посвідчення водія, номер паспорту, номер карти соціального страхування або будь-яку особисту інформацію, корисну для ідентифікації людини без знання його імені. В майбутньому навіть карта ДНК людини може стати предметом юридичної реєстрації. Крім особистої ідентифікаційної інформації, існує неособиста конфіденційна інформація, яка може включати бренди одягу, які ми купуємо; веб-сайти, які ми часто відвідуємо; чи куримо ми; вживаємо алкоголь; чи володіємо пістолетом; на якому автомобілі їздимо; якими захворюваннями перехворіли протягом життя; чи є в нашій родині спадкові захворювання або недуги, і навіть яким людям ми подобаємося.

Ця конфіденційна інформація в поєднанні з публічними звітами, що стосуються особистого доходу, податків, майнових документів, судимості, порушень правил дорожнього руху, а також будь-яка інформація, розміщена на сайтах соціальних мереж, утворюють потужний набір даних для зацікавлених сторін. Технологія навмисного збору великих наборів даних, які фіксують

демографічну, особисту, фінансову, біомедичну та поведінкову інформацію, а також аналіз цих даних за шаблонами, тенденціями та статистичній кореляції, сьогодні відома як "великі дані". Система охорони здоров'я, в тому числі страхові компанії, медичні працівники, фармацевтичні компанії та навіть адвокати підозрюваних у злочинній недбалості лікарів, виявляють дуже великий інтерес до особистої інформації, що зберігається у вигляді великих даних. Автомобільні компанії та виробники товарів широкого споживання також хочуть отримати доступ до таких баз даних, щоб направляти свою ринкову стратегію і рекламний бюджет. Навіть політики у ході недавніх виборів почали шукати великі дані, щоб краще зрозуміти думки виборців та предмети політичних суперечок, яких слід уникати.

Проблема конфіденційності інформації полягає не в тому, що сьогодні великі дані фіксують особисту інформацію (це вже стандартна процедура), а в тому, чи зберігає цей набір даних ваше ім'я або достатню особисту ідентифікаційну інформацію, щоб ідентифікувати вас, навіть не знаючи вашого імені. Наприклад, спочатку уряд США заявив, що особиста інформація, зібрана веб-сайтом healthcare.gov, використовувана для підписання Закону про доступне медичне обслуговування, буде знищена після створення приватних медичних рахунків. Потім недавно він відверто визнав, що стороння корпорація, яка допомагала уряду США виконувати збір даних, раніше підписала урядовий контракт, що дає їй право зберегти та використовувати зібрані дані, а це означає, що конфіденційні особисті дані, що стали відомими уряду США, в дійсності не є конфіденційними.

І нарешті, слід зазначити, що спостереження практикується як урядами, так і злочинними синдикатами, що використовують аналогічні технологічні методи. Звичайно, злочинці явно не мають законного права на збір таких даних, але випадки несанкціонованого спостереження з боку держави є більш сумнівною практикою, що істотно відрізняється в різних країнах. Наприклад, Агентство національної безпеки США неодноразово чинило тиск на Apple, Google, Microsoft та інші компанії, вимагаючи забезпечити доступ до їх хмар і баз даних. Прослуховувалися та перехоплювалися навіть розмови та заяви урядових офіційних осіб. На питання, чи відслідковує Skype, який є підрозділом Microsoft, вміст передач своїх абонентів, IT-директор Skype несподівано відповів: "Без коментарів".

Методи кіберзлочинності і кіберспостереження - Зосередившись на темі кібербезпеки, слід зазначити, що існує безліч засобів для отримання несанкціонованого доступу до даних пристрою, мережі і комп'ютера, в тому числі велику кількість шкідливих і хакерських технологій, що використовуються для здійснення кіберзлочинів і несанкціонованого проникнення в нібито захищені мережі.

Наприклад, людина з планшетом, підключеним до Інтернету, може захотіти зателефонувати на телефон бізнес-офісу, відправити повідомлення на телевізор, подзвонити другу на телефон, або завантажити файли з веб-сховища, або відправити електронну пошту через поштовий сервер. Незважаючи на те, що всі ці програми - це звичайні додатки Інтернету і глобальних систем зв'язку, на різних ділянках мережі існує велика кількість можливостей для спостереження, кіберзлочинності, шахрайства та крадіжки особистих даних.

Наприклад, для планшета, підключеного до мережі через антену стільникової радіостанції та базову станцію LTE або через антену радіосистеми ближньої дії та загальнодоступну базову станцію мережі Wi-Fi, зловмисник може контролювати радіолінію. Аналогічно, виклики LTE можна контролювати або аналізувати радіоприймачем-перехоплювачем або сніффером. Той же перехоплювач може бути налаштований для контролю передачі даних по каналу Wi-Fi і на приймаючій стороні по кабелю між кабелем термінальної системи кабельних модемів (CMTS) і кабельним модемом.

У деяких випадках виклик LTE також може бути перехоплений шахрайською піратською вишкою шляхом перенаправлення каналу зв'язку між планшетом та вишкою стільникового зв'язку. Передача даних по мережі з комутацією пакетів в маршрутизатор, сервер та сервер, а також хмарне сховище, - також вразливості для атаки "людина посередині". Підключення до дротової лінії можуть перехоплювати виклики на лінії традиційної телефонної мережі (POTS) від шлюзу абонентської мережі зв'язку (PSTN) до телефону, а також на лінії корпоративної АТС від сервера АТС до офісного телефону.

Завдяки ряду вразливостей в захисті, шпигунське ПЗ може автоматично встановитись на планшет, на маршрутизатор, на PSTN-міст, на хмарне сховище, на термінальну систему кабельних модемів (CMTS) або на стаціонарний комп'ютер. Троянська програма може встановитися на планшет або стаціонарний комп'ютер для фішингу паролів. Шкідлива програма також може використовуватися для атаки на стаціонарний комп'ютер, особливо якщо на комп'ютері встановлена операційна система Microsoft з ActiveX керуючими елементами.

Нарешті, для запуску атак типу "відмова в обслуговуванні" вірус може атакувати будь-яку кількість мережевих пристроїв, включаючи сервери, стаціонарний комп'ютер та планшет.

Шкідливе програмне забезпечення може діяти на різних частинах комунікаційної мережі та інфраструктури, де кібер-напад може включати віруси, урядове спостереження за атаками людини в середині та атаки на відмову в обслуговуванні. "Остання миля" мережі зв'язку надає ще більш великі можливості для шкідливих програм і кібератак і ділиться на три секції: місцева телефонна компанія/мережа, "остання миля" та пристрій. Місцева телефонна компанія/мережа містить високошвидкісний волоконно-оптичний кабель, маршрутизатор, термінальну систему кабельних модемів (CMTS), коаксіальний/волоконно-оптичний кабель, кабельний модем, антену Wi-Fi та вишку радіозв'язку LTE. У цій частині мережі може застосовуватися перехоплення радіоканалу, шпигунське ПЗ, вірус і атака "людина посередині".

В останній ланці - місцевому підключенні до пристрою - підключення до мережі включає дротову лінію, з'єднання Wi-Fi та з'єднання LTE/радіо, що піддається впливу шпигунського ПЗ, перехоплення радіоканалу, прослуховування та піратської вишки. Сам пристрій, що включає, наприклад, планшет, ноутбук, стаціонарний комп'ютер, а можливо також смартфони, смарт-телевізори, POS-термінали і т.д., піддається безлічі атак, включаючи шпигунське ПЗ, троянській, вірусній або шкідливій програм. Такі методи спостереження і шпигунські пристрої легкодоступні на комерційному та онлайн-ринку, включаючи пристрої, що використовується для контролю трафіку в локальних мережах Ethernet, контролю даних Wi-Fi та стільникового зв'язку. Незважаючи на те, що аналіз пакетів хмарних з'єднань волоконно-оптичним кабелем не ідентифікований як загроза, під час досліджень стало очевидним, що неінвазійне перехоплення даних для оптичної лінії зв'язку, тобто таке, де волоконно-оптичний кабель не потрібно обрізати або хоча б тимчасово порушувати його нормальну роботу, вже існує.

Крім використання методів злому та спостереження, існує велика кількість комерційних легкодоступних шпигунських програм для контролю розмов по стільниковому телефону та передачі даних через Інтернет. Сьогодні легко можна знайти шпигунські програм, які рекламують здатність успішно стежити за своїми співробітниками, дітьми та чоловіком (дружиною). На подив широкий вибір функцій, що включає відстеження дзвінків, фотографій та відео, текстових повідомлень SMS/MMS, сторонніх миттєвих повідомлень, електронних листів, відстеження координат GPS, використання Інтернету, адресної книги, подій календаря, прослуховування, управління додатками і навіть функції віддаленого управління, в сукупності містить переконливу кількість способів порушення конфіденційності інформації. Насправді кібератаки стали настільки частими, що їх відстежують щодня.

Для запуску кібератаки зазвичай задіються кілька етапів або поєднань методів, у тому числі:

- Аналіз IP-пакетів;
- Опитування портів;
- Профілювання;
- Імперсонація;
- Перехоплення пакетів;
- Кіберінфекування;
- Спостереження;
- Піратське адміністрування.

Аналіз IP-пакетів - Використовуючи пристрої радіоконтролю, кіберзлочинець може отримати значний обсяг інформації про користувача, його транзакціях і його облікових записах. Вміст IP-пакета можна отримати або проаналізувати в будь-якій точці шляху між двома користувачами. Наприклад, коли користувач відправляє файл, наприклад, фотографію або текст в IP-пакеті зі свого ноутбука на мобільний телефон свого друга, кіберзлочинець може виявити IP-пакет в одному з декількох місць, перехопивши останнє посилання відправника, перехопивши локальну мережу відправника, контролюючи хмару, перехопивши дзвінок одержувача по місцевому телефонному дзвінку або перехопивши остання повідомлення одержувача. У перехопленому IP-пакеті доступні для спостереження наступні дані: MAC-адреси рівня 2 задіяні в інформаційному обміні пристроїв, адреси рівня 3 відправника приймаючої сторони, тобто одержувача пакета, включаючи використовуваний протокол передачі, наприклад, UDP, TCP і т.д. IP-пакет також містить номери портів рівня 4 відправляючих та приймаючих пристроїв, що потенційно дозволяють визначити тип запитуваної послуги, а також сам файл даних. Якщо файл не зашифрований, дані, що містяться в файлі, також можуть бути легко прочитані кіберзлочинцем.

Якщо корисне навантаження не зашифроване, текстова інформація, наприклад, номери облікових записів, логіни та паролі, можуть бути прочитані і, якщо вони представляють цінність, вкрадені та змінені в злочинних цілях. Якщо корисне навантаження містить відео або

піктографічну інформацію, потрібно виконати деяку додаткову роботу, щоб визначити, який формат прикладного рівня 6 використовується для передачі вмісту, але як тільки він буде ідентифікований, вміст можна буде переглянути, опублікувати або навіть використовувати для шантажу однієї або обох сторін інформаційного обміну. Така кібератака називається атакою "людина посередині", тому що кіберзлочинець особисто не знайомий ні з однією з сторін інформаційного обміну.

Як було зазначено раніше, маршрутизація IP-пакетів в хмарі непередбачувана, тому контроль хмари є більш складним, тому що кіберзлочинець повинен захопити важливу інформацію IP-пакета при першій зустрічі з ним, оскільки наступні пакети можуть не слідувати по тому ж маршруту, та проаналізувати пакет. Перехоплення даних на "останній милі" підвищує ймовірність спостереження послідовності пов'язаних пакетів з однієї і тієї ж розмови, оскільки місцеві маршрутизатори зазвичай слідують продиктованій таблиці маршрутизації, у крайньому випадку, до тих пір, поки пакети не досягнуть точки присутності (POP) за межами області обслуговування власного оператора клієнта. Наприклад, клієнт Comcast, швидше за все, буде передавати IP-пакети в ланцюжок маршрутизації доти, повністю використовуючи Comcast мережу, поки пакет не буде географічно переміщений за межі доступу і області обслуговування клієнтів Comcast.

Якщо послідовність пакетів, що передаються між одними та тими ж двома IP-адресами, спостерігається протягом досить тривалого часу, всю розмову можна відтворити по частинах. Наприклад, якщо текстові SMS-повідомлення передаються по одній і тій же мережі на ділянці "останньої милі", кіберзлочинець може ідентифікувати через IP-адреси і номери портів, що кілька IP-пакетів, що передають текст, являють собою розмову між одними та тими ж двома пристроями, тобто між стільниковим телефоном і ноутбуком. Тому навіть якщо номер облікового запису та пароль були в тексті різних повідомлень або були відправлені в повному обсязі та поширилися по багатьом пакетам, збіг ідентифікаторів пакетів як і раніше дозволяє кіберзлочинцю відтворити розмову та вкрасти інформацію про обліковий запис. Після того, як дані облікового запису будуть вкрадені, зловмисники можуть або перевести гроші в офшорний банк, або навіть узурпувати повноваження облікового запису, змінивши пароль облікового запису та параметри безпеки, тобто використовуючи крадіжку особистих даних на тимчасовій основі.

Навіть якщо корисне навантаження зашифроване, інша частина IP-пакета, включаючи IP-адреси і номери портів, не шифрується. Після багаторазового аналізу великої кількості IP-пакетів кіберзлочинець, що володіє достатньою обчислювальною потужністю, може методом "грубої сили" систематично перевіряти кожну комбінацію, поки не зламає пароль шифрування. Як тільки ключ буде зламаний, цей пакет та всі наступні пакети можуть бути розшифровані та використані кіберзлочинецем. Імовірність злому пароля входу в систему шляхом "вгадування пароля" значно підвищується, якщо аналіз пакетів поєднується з описаним нижче "профілюванням" користувача і облікового запису. Слід звернути увагу на те, що атаки "людина посередині" на пристрої зв'язку зазвичай не виконуються, тому що кіберзлочинець не має до них прямого доступу.

Опитування портів - Ще один спосіб злому пристрою полягає в тому, що за його IP-адресою проводиться опитування великої кількості портів рівня 4 та перевірка наявності відповіді на направлені запити. Коли кіберзлочинець визначає за результатами аналізу пакету або іншими засобами, що мобільний телефон з IP-адресою "CP" є цільовим пристроєм, кіберзлочинець запускає послідовність опитувань портам на стільниковому телефоні в пошуках незахищеного або відкритого порту, порту сервісного та технічного обслуговування або шляхів обходу захисту. Поки хакерська програма опитування систематично перевіряє кожен номер порту, атаки зазвичай зосереджені на таких сумнозвісних портах, як порт №7 для ping-тесту, порт №21 для FTP, порт №23 для емуляції терміналу telnet, порт №25 для простої електронної пошти і т.д… Кожен раз, коли відправляється відповідь, пірат дізнається більше про операційну систему цільового пристрою.

В процесі опитування портів кіберзлочинець не хоче розкривати свою реальну ідентифікацію, тому він використовує приховану псевдо-адресу для прийому повідомлень, що не простежується до його персонального пристрою. В якості альтернативи, кіберзлочинці можуть використовувати крадений комп'ютер і обліковий запис, при цьому ситуація виглядає так, ніби хтось намагається зламати цільовий пристрій, але, якщо його відстежити, це приведе слідство до невинної людини, а не до зловмисника.

Профілювання - Профілювання користувачів і облікових записів - це процес, в ході якого кіберзлочинець проводить дослідження з використанням загальнодоступної інформації, щоб більше дізнатися про цільовий об'єкт, його облікових записах і його особистої історії, щоб

зламати його паролі, ідентифікувати облікові записи та визначити активи. Як тільки хакер отримує IP-адресу цілі за результатами аналізу трафіку або іншими засобами, він може скористатися утилітою traceroute для пошуку DNS-сервера облікового запису пристрою. Потім, використовуючи функцію "Who is" (Хто це) в Інтернеті, можна дізнатися ім'я власника облікового запису. Потім в процесі профілювання кіберзлочинець здійснює пошук в Інтернеті для збору всієї наявної інформації про власника облікового запису. В якості джерел інформації використовуються такі загальнодоступні записи, як документи про власність, дані про реєстрацію автомобілів, шлюби і розлучення, заставних правах на майно для забезпечення сплати податку, паркувальних квитках, порушеннях правил дорожнього руху, судимості і т.д… У багатьох випадках веб-сайти університетів та професійних товариств також містять домашню адресу, адреси електронної пошти, номери телефонів і дату народження людини. Вивчаючи сайти соціальних мереж, такі як Facebook, LinkedIn, Twitter і інші, кіберзлочинець може зібрати значну докладну інформацію, в тому числі про родину і друзів, імена домашніх тварин, адреси колишнього місця проживання, відомості про однокласників, головні події в житті, а також фотографії та відеофайли, в тому числі що містять делікатні подробиці, сімейні таємниці і дані про особистих ворогів.

Наступним кроком кіберзлочинця є використання даних цього профілю для "вгадування" паролів користувача на основі його профілю для злому цільового пристрою та інших облікових записів цієї людини. Після того, як кіберзлочинець підбере пароль одного пристрою, велика ймовірність того, що він зможе підійти і до інших облікових записів, тому що люди схильні використовувати одні й ті ж самі паролі для зручності їх запам'ятовування. У цей момент може з'явитися можливість вкрасти ідентифікаційні дані людини, перевести гроші, зробити його мішенню поліцейських розслідувань та по суті зруйнувати чиєсь життя, викравши все його майно. Наприклад, як описано у вступній частині цього документа, зібравши довгий список паролів з вкрадених облікових записів, кіберзлочинці використовували ці паролі для незаконної покупки преміум квитків на концерти та спортивні події на кілька мільйонів доларів з використанням тих же паролів та логінів.

Імперсонація - Коли кіберзлочинець видає себе за когось іншого, він не використовує або використовує незаконно отримані захищені облікові дані, щоб отримати доступ до повідомлень або файлів під хибним приводом того, що він є уповноваженим агентом або пристроєм, кіберзлочинець діє як "самозванець". Кібератака типу "самозванець" може виникати, коли у кіберзлочинця є достатня інформація або доступ до облікового запису користувача, щоб скомпрометувати обліковий запис жертви, відправляти від її імені повідомлення і навмисно спотворювати їх зміст від імені власника зламаного облікового запису. Нещодавно, наприклад, у близької знайомої одного з винахідників було зламано особистий обліковий запис месенджера "Line". Отримавши контроль над обліковим записом, кіберзлочинець відправив повідомлення її друзям з неправдивою інформацією про те, що "вона потрапила в автомобільну аварію, і їй терміново потрібні гроші в борг", вказавши платіжні реквізити для відправки грошей. Не знаючи, що обліковий запис був зламаний, її друзі подумали, що запит реальний, погодилися заплатити викуп. Щоб уникнути підозр, у кожному відправленому запиті були вказані суми менше 1000 доларів США. На щастя, перш ніж відправляти гроші, один з друзів подзвонив їй, щоб перевірити ще раз платіжні реквізити, і, таким чином, виявив шахрайство. Якби не цей дзвінок, ніхто ніколи не дізнався б, що запити були від самозванця, а власник облікового запису Line ніколи не дізнався б про те, що гроші були відправлені або навіть запитані.

Інша форма введення в оману виникає, коли пристрою надані привілеї безпеки та воно має можливість обмінюватися інформацією з сервером або іншим мережевим пристроєм, та при цьому якимось чином пристрою кіберзлочинця вдається видавати себе за авторизований сервер, в результаті чого пристрій жертви охоче передає файли і інформацію на піратський сервер, не усвідомлюючи, що цей сервер є самозванцем. За наявними даними, цей метод використовувався, щоб схилити знаменитостей до резервного копіювання особистих файлів зображень за допомогою iCloud, промовчавши, що ця резервна хмара була самозванцем.

Інша форма самозванця виникає, коли хтось, маючи фізичний доступ до особистого телефону або відкритого браузеру людини, виконує такі шахрайські операції, як відправка електронної пошти, відповідь на телефонний дзвінок, текстове повідомлення, надіслане з облікового запису або пристрою іншої особи. Одержувач вважає, що він підключений до відомого пристрою або облікового запису, і що особа, яка керує цим пристроєм або обліковим записом, є його власником. Самозванець може виявитися жартівником, який, наприклад, виставляє делікатні коментарі в Facebook, або його дії можуть носити більш особистий характер, коли чийсь чоловік відповідає на особисті виклики або перехоплює конфіденційні текстові повідомлення особистого характеру. Результатом цього несанкціонованого доступу

можуть бути ревнощі, розлучення та судове переслідування. Залишаючи пристрій тимчасово неконтрольованим в офісі або кафе, наприклад, виходячи в туалет, ви піддаєтеся додатковому ризику, надаючи самозванцю можливість швидкого доступу до особистої або корпоративної інформації, відправки несанкціонованих повідомлень електронної пошти, передачі файлів або завантаження будь-якої шкідливої програми в пристрій, як описано в наступному розділі, що називається "Кіберінфекції".

Кібератака з боку самозванця також має велике значення при крадіжці пристрою. У таких випадках, навіть незважаючи на те, що пристрій вийшов з системи, у злодія достатньо часу, щоб підібрати логін. Функція "find my computer" (знайти мій комп'ютер), яка повинна знайти вкрадений пристрій в мережі та стерти файли комп'ютера при першому вході кіберзлочинця в систему на цьому пристрої, більше не працює, тому що високотехнологічні злочинці сьогодні знають, як активувати тільки саме пристрій без стільникового або Wi-Fi-з'єднання. Цей ризик особливо великий для стільникових телефонів, де безпеку входу забезпечує простий чотиризначний ідентифікаційний номер або PIN-код. Підбір PIN-коду - це всього лише питання часу, оскільки є тільки 9999 можливих комбінацій.

Ключовою проблемою для захисту будь-якого пристрою є запобігання доступу для самозванців. Запобігання втручання самозванців вимагає надійних засобів автентифікації особистості користувача через певні проміжки часу та підтвердження того, що тільки вони мають право на доступ до інформації та привілеїв, яких вони потребують. Захист пристрою часто є найслабшою ланкою в цьому ланцюжку. Після подолання захисту пристрою необхідність в надійній мережевій безпеці є спірною.

Перехоплення пакетів - Перехоплення пакетів - це кібератака, в ході якої нормальний потік пакетів через мережу перенаправляється через шкідливий пристрій

Наприклад, якщо маршрутизатор був атакований, IP-пакети, що проходять через маршрутизатор, можуть бути перезаписані в переглянуті IP-пакети, які ділі будуть перенаправленні на іншу адресу призначення та номер порту кіберпіратського пристрою. Після цього кіберпіратський пристрій отримує будь-яку необхідну йому інформацію з корисного навантаження IP-пакета і, можливо, змінює вміст корисного навантаження IP-пакета. Шахрайське корисне навантаження може використовуватися для здійснення ряду шахрайських злочинів, для збору інформації або для завантаження шкідливого ПЗ в стільниковий телефон, як описано нижче в розділі "Кіберінфекції".

Потім зламаний пакет IP-пакет перевизначається так, щоб він виглядав як вихідний IP-пакет з IP-адресою відправника, за винятком того, що пакет передається по провідному з'єднанню замість провідного з'єднання. В якості альтернативи, перехоплений IP-пакет може бути повернутий на скомпрометований маршрутизатор, а потім відправлений у хмару через дротове з'єднання. Щоб максимізувати злочинну вигоду від перехоплення пакету, кіберзлочинцю необхідно приховати свої ідентифікаційні дані при перехопленні пакетів, та з цієї причини вони маскують справжню маршрутизацію IP-пакета, при цьому навіть функція "traceroute" ICMP рівня 3 буде зазнавати труднощів при ідентифікації істинного шляху передачі даних. Якщо, проте, це перехоплення помітно збільшує затримку при маршрутизації пакетів, ця незвичайна затримка може бути приводом для дослідження з боку оператора мережі.

Кіберінфекції - Однією з найпідступніших категорій кібератак є "кіберінфекції" - установка на цільові пристрої або в мережу шкідливого ПЗ, за допомогою якого можна збирати інформацію, здійснювати шахрайські дії, перенаправляти трафік, інфікувати інші пристрої, порушувати роботу або вимикати систему або викликати відмову в обслуговуванні. Кіберінфекція може поширюватися через електронні листи, файли, веб-сайти, системні розширення, прикладні програми або по мережах. Один з основних класів шкідливих програм - "шпигунське ПЗ" - збирає всі види інформації про транзакції і направляє кіберзлочинцю. У разі "фішингу" веб-сторінка або оболонка додатку, яка відображається як знайома сторінка входу в систему, запитує логін облікового запису або особисту інформацію, а потім передає цю інформацію кіберзлочинцю. Інші шкідливі інфекції можуть управляти обладнанням, наприклад, управляти маршрутизатором для виконання вищезазначеного перехоплення пакетів. У цих випадках кіберзлочинець намагається отримати інформацію або отримати вигоду для досягнення своїх цілей.

Інший клас кіберінфекцій, що містить віруси, шкідливі та троянські програми, призначений для перезапису критичних файлів або для повторного виконання беззмістовних функцій, щоб позбавити пристрій можливості виконання своїх звичайних завдань. В основному, щоб заборонити обслуговування, погіршити якість роботи або повністю знищити пристрій. Ці зловмисні інфекції за своєю суттю руйнівні та використовуються з метою помсти, щоб порушити

нормальну роботу бізнесу конкурента або просто заради забави хакером, охочим побачити, чи можливо це.

Спостереження - Підслуховування та стеження виходять за рамки кіберзлочинності. У таких випадках приватного детектива або знайомого наймають або примушують встановити пристрій або програму в особисті пристрої суб'єкта, що представляє інтерес, для здійснення контролю над його розмовами, обміном даними та місцем розташування. Ризик бути спійманим збільшується, тому що детектив повинен отримати тимчасовий доступ до цільового пристрою так, щоб суб'єкт про це не дізнався. Наприклад, у продажу є SIM-карти, які можуть копіювати права доступу до мережі телефону, але одночасно передається інформація кіберзлочинця, який контролює виклики та трафік даних жертви.

До інших форм спостереження відноситься використання підпільних відеокамер для спостереження за кожною дією та телефонним дзвінком людини, багато в чому аналогічно казино. За допомогою відео контролю, пароль або PIN-код пристрою можна дізнатися, просто спостерігаючи за натисканнями клавіш користувачем під час процесу входу в систему. При досить великій кількості камер на місці спостереження, в кінцевому рахунку, рано чи пізно процес входу в систему буде записаний. Щоб отримати доступ до мережі камер, не викликаючи підозр, кіберзлочинець може зламати існуючу систему відеоспостереження на будівлях, в магазинах або на вулицях, а також, через доступ до чужої мережі, стежити за поведінкою нічого непідозрюючих жертв. Об'єднання відеоспостереження з аналізом пакетів надає ще більш повний набір даних для подальшого запуску кібератак.

Піратське адміністрування (несанкціоноване проникнення) - Ще один засіб, завдяки якому кіберзлочинці можуть отримати інформацію - це злом і отримання доступу до прав системного адміністратора пристрою, сервера або мережі. Таким чином, замість отримання несанкціонованого доступу до облікового запису одного користувача, зламавши логін адміністратора системи, кіберзлочинеці отримує набагато ширший доступ та привілеї без відома тих, хто використовує систему. Оскільки системний адміністратор виступає системі в якості поліцейського, ніхто не може припинити його злочинну діяльність - по суті, в системі або мережі з корумпованою адміністрацією ніхто не може контролювати поліцію.

Висновок - Повсюдне поширення та сумісність, які Інтернет, мережі з комутацією пакетів і майже загальне визнання семирівневої моделі OSI (Open Source Initiative), за останні двадцять років дозволили розширити глобальний зв'язок в небувалому масштабі, з'єднавши широкий діапазон пристроїв від смартфона до планшетів, комп'ютерів, інтелектуальних телевізорів, автомобілів і навіть побутової техніки та лампочок. Глобальне визнання інтернет-протоколу (IP) в якості основи для підключення до Ethernet, стільникового зв'язку, Wi-Fi і кабельного телебачення не тільки уніфікував зв'язок, але й значно спростили проблему для хакерів і кіберзлочинців, які намагаються проникнути в максимально можливу кількість пристроїв та систем. З огляду на безліч програмних і апаратних методів, доступних зараз для атаки сучасних мереж зв'язку, очевидно, що одного методу захисту недостатньо для повної безпеки. Замість цього необхідний системний підхід до захисту кожного пристрою, останньої ланки, місцевої телефонної компанії/мережі та хмарної мережі, щоб забезпечити їх захист від складних кібератак. Використовувані методи повинні забезпечувати внутрішню інформаційну безпеку і конфіденційність інформації без шкоди для якості обслуговування, затримки мережі, якості відео або звуку. Незважаючи на те, що шифрування має залишатися важливим елементом розробки наступного покоління безпечної передачі та зберігання даних, безпека мережі не повинна спиратися виключно на методи шифрування.

Короткий виклад суті винаходу

Відповідно до цього винаходу дані (які в широкому сенсі включають в себе текстові, аудіо-, відео-, графічні та всі інші види цифрової інформації або файлів) передаються через динамічну захищену комунікаційну мережу та протокол (SDNP) або "хмару". Хмара SDNP включає в себе безліч "вузлів", іноді званих "медіа-вузлами", які індивідуально розміщуються на серверах або інших типах комп'ютерів або цифрового обладнання (в сукупності іменованих тут як "сервери"), розташованих в будь-якій точці світу. Можливе розміщення двох і більше вузлів на одному сервері. Як правило, дані передаються між медіа-вузлами світлом по волоконно-оптичним кабелям, радіохвилями в високочастотному або надвисокочастотному діапазоні, електричними сигналами по мідних дротах або коаксіальному кабелю або по каналах супутникового зв'язку, але в широкому сенсі винахід включає в себе будь-які засоби, за допомогою яких цифрові дані можуть передаватися з однієї точки в іншу. Мережа SDNP включає хмару SDNP, а також канали "останньої милі" між хмарою SDNP і клієнтськими пристроями, такими як мобільні телефони, планшети, ноутбуки та стаціонарні комп'ютери, мобільні споживчі електронні пристрої, а також пристрої та побутові прилади Інтернету речей, автомобілі та інші транспортні засоби. Системи

зв'язку останньої милі також включають вежі стільникового телефонного зв'язку, кабель або оптоволокно, прокладені в будинку, та загальнодоступні маршрутизатори Wi-Fi.

При передачі між медіа-вузлами в хмарі SDNP дані представлені в вигляді "пакетів", дискретних ланцюжків цифрових бітів, які можуть мати фіксовану або змінну довжину, при цьому дані замасковані з використанням таких методів: скремблювання, шифрування або розділення - або відповідних зворотних процесів: дескремблювання, дешифрування та змішування. (Примітка. У даному документі, якщо із контексту не слідує іншого, слово "або" використовується в його кон'юнктивному (та/або) сенсі.)

Скремблювання має на увазі зміну порядку проходження даних в пакеті. Наприклад, для сегментів даних A, B і C, які в початковому пакеті слідують в порядку ABC, порядок проходження зміниться на CAB. Зворотна по відношенню до скремблювання операція називається "дескремблювання" і має на увазі зміну порядку проходження даних в пакеті на той, в якому він спочатку з'явився - ABC в наведеному вище прикладі. Об'єднана операція дескремблювання, а потім скремблювання пакета даних називається "повторним скремблюванням". При повторному скремблюванні пакета, який раніше був скрембльований, цей пакет може бути скрембльований тим же самим або іншим способом по відношенню до попередньої операції скремблювання.

Друга операція - "шифрування" - це кодування даних в пакеті і їх подання у формі, званої зашифрованим текстом, яка може бути зрозуміла тільки відправнику та всім іншим авторизованим сторонам, а також того, хто повинен виконувати зворотну операцію - "дешифрування". Об'єднана операція дешифрування пакета даних із зашифрованим текстом і його подальшого шифрування, як правило, але не обов'язково з використанням методу, який відрізняється від методу, який використовується при його попередньому шифруванні, в даному документі називається "повторним шифруванням".

Третя операція - "розділення", згідно з назвою, означає поділ пакета на два або більше пакети меншого розміру. Зворотна операція - "змішування" - визначається як об'єднання двох або більше розділених пакетів назад в один пакет. Розділення пакета, який раніше був розділений, а потім змішаний, може бути виконано таким же чином або може відрізнятися від попередньої операції розділення. Порядок виконання операцій є оборотним, при цьому розділення може бути скасовано шляхом змішування, і, навпаки, змішування декількох вхідних елементів в один вихідний може бути скасовано шляхом розділення для відновлення складових компонентів. (Примітка. Оскільки скремблювання і дескремблювання, шифрування і дешифрування, а також розділення та змішування є зворотними процесами, для виконання зворотної операції необхідно тільки знання алгоритму або методу, який використовувався для прямої операції. Отже, коли мова йде про конкретний алгоритм скремблювання, шифрування або розділення, має бути зрозуміло, що знання цього алгоритму дозволяє виконати зворотний процес).

У відповідності до даного винаходу пакет даних, який проходить через хмару SDNP, скремблюється або шифрується, або ж над ним виконується одна або обидві ці операції в поєднанні з розділенням. Крім того, в пакет можуть додаватися "сміттєві" (тобто беззмістовні) дані, щоб зробити пакет більш складним для дешифрування, або привести довжину пакета у відповідність до встановлених вимог. Крім того, пакет може бути підданий статистичному аналізу, тобто розділений на окремі частини. Професійною мовою комп'ютерних фахівців проводити синтаксичний аналіз - це значить розділити оператор комп'ютерної мови, комп'ютерну команду або файл даних на частини, які можуть бути корисні для комп'ютера. Синтаксичний аналіз може також використовуватися для ускладнення розуміння мети команди або пакета даних, або для упаковки даних в пакети, що мають певну довжину.

Незважаючи на те, що формат пакетів даних відповідає інтернет-протоколу, в хмарі SDNP адреси медіа-вузлів не є стандартними інтернет-адресами, тобто вони не можуть бути ідентифіковані будь-яким сервером доменних імен Інтернету. Отже, незважаючи на те, що медіа-вузли можуть технічно отримувати пакети даних через Інтернет, ці медіа-вузли не будуть розпізнавати адреси або відповідати на запити. Більш того, навіть якщо б користувачам Інтернету потрібно було зв'язатися з медіа-вузлом, вони не змогли б отримати доступ або переглянути дані всередині медіа-вузла, тому що медіа-вузол може розпізнати їх як самозванців, які не мають необхідних ідентифікаційних облікових даних як медіа- вузла SDNP. Зокрема, якщо медіа-вузол не зареєстрований як діючий вузол SDNP, що працює на сервері, що відповідає вимогам сервера імен SDNP або його еквівалентної функції, пакети даних, що відправляються з цього вузла на інші медіа-вузли SDNP, будуть ігноруватися та відкидатися. Аналогічним чином, тільки клієнти, зареєстровані на сервері імен SDNP, можуть звертатися до

медіа-вузлу SDNP. Подібно незареєстрованим серверам, пакети даних, отримані з джерел, які не є зареєстрованими клієнтами SDNP, будуть ігноруватися і негайно відкидатися.

В порівняно простому варіанті здійснення, званому "одномаршрутний", пакет даних проходить по єдиному шляху через ряд медіа-вузлів у хмарі SDNP, при цьому він скремблюється в медіа-вузлі, в якому він входить в хмару і дескремблюється в медіа-вузлі, в якому він виходить з хмари (ці два вузли називаються "шлюзовими вузлами" або "шлюзовими медіа-вузлами"). У кілька більш складному варіанті здійснення пакет повторно скремблюється на кожному медіа-вузлі з використанням методу скремблювання, відмінного від того, який використовувався на попередньому медіа-вузлі. В інших варіантах здійснення пакет також шифрується в шлюзовому вузлі, в якому він входить в хмару і дешифрується в шлюзовому вузлі, в якому він виходить з хмари, і, крім того, пакет може бути повторно зашифрований в кожному медіа-вузлі, через який він проходить в хмарі. Оскільки даний вузол при скремблюванні або шифруванні пакету кожен раз використовує один та той же алгоритм, цей варіант здійснення називається "статичним" скремблюванням і шифруванням.

У разі, коли виконується дві і більше операції перетворення пакета, наприклад, він скремблюється і шифрується, зворотні операції рекомендується виконувати в протилежному порядку, тобто в зворотній послідовності. Наприклад, якщо пакет скремблюється, а потім шифрується до виходу з медіа-вузла, то при надходженні на наступний медіа-вузол, він спочатку дешифрується, а потім дескремблюється. Пакет відтворюється в своїй вихідній формі тільки в тому випадку, якщо він знаходиться в медіа-вузлі. Поки пакет передається між медіа-вузлами, він знаходиться в скрембльованому, розділеному або змішаному або зашифрованому вигляді.

В іншому варіанті здійснення, званому "мультимаршрутною" передачею даних, в шлюзовому вузлі проводиться розділення пакета, після чого декілька пакетів, що утворилися, перетинають хмара по ряду "паралельних" маршрутів, причому жоден із шляхів не має загальних медіа-вузлів з іншими, за винятком шлюзових вузлів. Потім ці кілька пакетів змішуються для відтворення вихідного пакета, як правило, в вихідному шлюзовому вузлі. Таким чином, навіть якщо хакеру вдалося зрозуміти сенс одного пакета, у нього буде тільки частина всього повідомлення. Пакет також може бути скрембльований та зашифрований в шлюзовому вузлі до або після його розділення, а декілька пакетів, що утворилися, можуть бути повторно скрембльовані або повторно зашифровані в кожному медіа-вузлі, через який вони проходять.

У наступному варіанті здійснення винаходу пакети передаються не тільки по одному шляху або ряду паралельних шляхів в хмарі SDNP, а можуть передаватися різними шляхами, багато з яких перетинаються один з одним. Оскільки в цьому варіанті здійснення винаходу зображення можливих шляхів нагадує решітку, цей процес називається "решітчастою передачею". Як і в описаних вище варіантах здійснення винаходу, пакети можуть бути скрембльовані, зашифровані і розділені або змішані при проходженні через окремі медіа-вузли в хмарі SDNP.

Маршрути пакетів через мережу SDNP визначаються сигнальною функцією, яка може виконуватися або сегментами самих медіа-вузлів, або переважно в "двоканальному" або "триканальному" варіантах окремими сигнальними функціями, які працюють на виділених сигнальних серверах. Сигнальна функція визначає маршрут кожного пакету, коли він залишає клієнтський пристрій (наприклад, стільниковий телефон), на основі стану (наприклад, затримки поширення) мережі, пріоритету та терміновості виклику, і інформує кожен з медіа-вузлів на маршруті про те, що він повинен отримати пакет, та вказує вузол, якому його потрібно відправити. Кожен пакет ідентифікується міткою, а сигнальна функція вказує кожному медіа-вузлу, яку мітку застосувати для кожного з пакетів, які він відправляє. В одному варіанті здійснення винаходу мітка даних включається в заголовок або підзаголовок SDNP, поле даних, прикріплене до кожного субпакету даних, використовується для ідентифікації субпакета. Кожен субпакет може містити сегменти даних з одного або декількох джерел, що зберігаються в спеціальних "слотах" даних в пакеті. Кілька субпакетів можуть бути присутніми в одному більшому пакеті даних при передачі даних між будь-якими двома медіа-вузлами.

Функція маршрутизації узгоджується з функціями розділення та змішування, так як після розділення пакета необхідно визначити відповідні маршрути кожного з субпакетів, на які він розділений, а вузлу, в якому ці субпакети повинні бути відновлені (змішані), має бути дано вказівку провести їх змішування. Пакет може бути розділений, а потім змішаний один раз, як в мультимаршрутному варіанті, або він може бути розділений та змішаний кілька разів у міру проходження по мережі SDNP до вихідного шлюзового вузла. Визначення вузла, в якому буде проводитися розділення пакета, на скільки субпакетів він буде розділений, відповідні маршрути субпакетів та вузли, в яких ці субпакети будуть змішані, щоб відтворити початковий пакет - всі ці питання знаходяться під контролем сигнальної функції, незалежно від того, виконується вона

окремими сигнальними серверами чи ні. Алгоритм розділення може визначати, які сегменти даних при передачі повинні бути включені в кожен з субпакетів, а також порядок та положення сегментів даних в цих субпакетах. Алгоритм змішування визначає зворотний процес в вузлі, де субпакети змішуються, щоб відтворити початковий пакет. Зрозуміло, що при наявності відповідної команди від сигнальної функції, в цьому вузлі пакет може бути знову розділений відповідно до іншого алгоритму розділення, який відповідав би часові або стану у момент виникнення розділеного процесу.

Коли медіа-вузол отримує команду від сигнальної функції відправити кілька пакетів в конкретний цільовий медіа-вузол при "наступному переході" по мережі, навіть якщо ці пакети є розділеними пакетами (субпакетами) або відносяться до різних повідомлень, цей медіа-вузол може об'єднувати пакети в один більший пакет, особливо коли кілька субпакетів повинні бути відправлені в один та той же медіа-вузол для наступного переходу (аналогічно поштовому відділенню, в якому поміщають пачку листів з однією і тією же адресою одержувача в ящик та відправляють цей ящик за адресою).

В "динамічних" варіантах здійснення винаходу окремі медіа-вузли в хмарі SDNP не користуються одними та тими ж методами і алгоритмами скремблювання, шифрування або розділення для пакетів, що по проходять по них по черзі. Наприклад, даний медіа-вузол може скремблювати, шифрувати або розділяти будь-який пакет з використанням одного конкретного алгоритму скремблювання, шифрування або розділення, а потім скремблювати, шифрувати або розділяти наступний пакет з використанням іншого алгоритму скремблювання, шифрування або розділення. Робота в "динамічному" режимі значно збільшує труднощі, з якими стикаються потенційні хакери, тому що у них залишається короткий проміжок часу (наприклад, 100 мсек), щоб зрозуміти смисловий зміст пакета, і навіть якщо їм це вдасться, користь від цих знань буде короткочасною.

У динамічних варіантах здійснення винаходу кожен медіа-вузол пов'язаний з так званим "сервером DMZ (англ. DeMilitarized Zone - демілітаризована зона)", який можна розглядати як частину вузла, яка ізольована від частини передачі даних, та в якій є база даних, яка містить списки або таблиці ("селектори") можливих алгоритмів скремблювання, шифрування та розділення, які цей медіа-вузол може застосовувати до вихідних пакетів. Селектор є частиною обсягу інформації, яка називається "спільними секретами", оскільки ця інформація невідома навіть медіа-вузлам і оскільки всі сервери DMZ мають однакові селектори в даний момент часу.

Коли медіа-вузол приймає пакет, який був скрембльований, в динамічних варіантах здійснення винаходу, він також отримує "початковий стан", який використовується для вказівки приймаючому вузлу, який алгоритм повинен використовуватися при дескремблюванні пакета. Початковий стан являє собою приховане числове значення, яке саме по собі не має сенсу, але засноване на стані, який постійно змінюється, наприклад, на моменті часу, в який пакет був скрембльований попереднім медіа-вузлом. Коли попередній вузол виконав скремблювання пакета, пов'язаний з ним DMZ-сервер сформував початковий стан на основі стану. Відповідно, цей стан також використовувався відповідним сервером DMZ при виборі алгоритму, який повинен застосовуватися при скремблюванні пакета, який був переданий на відправляючий медіа-вузол у вигляді вказівки про те, як скремблювати пакет. Таким чином, вузол, що відправив, отримав вказівки про скрембльований пакет та початковий стан, які повинні бути передані на наступний медіа-вузол. Генератор початкових станів, що працює на сервері DMZ, генерує початковий стан відповідно до алгоритму, заснованому на стані під час виконання процесу. Незважаючи на те, що генератор початкових станів і його алгоритми є частиною спільних секретів медіа-вузла, згенерований початковий стан не є секретним, оскільки без доступу до алгоритмів числове початкове значення не має сенсу.

Таким чином, наступний медіа-вузол на маршруті пакету отримує скрембльований пакет та початковий стан, заснований на стані, який пов'язаний з пакетом (наприклад, моменту часу, в який було виконано скремблювання). Початковий стан може бути включено в сам пакет або може бути відправлено на приймаючий вузол до відправки пакета, або за тим же маршрутом, що і пакет, або по якомусь іншому маршруту, наприклад, через сигнальний сервер.

Незалежно від того, як він отримує початковий стан, приймаючий вузол відправляє цей початковий стан на свій сервер DMZ. Оскільки на цьому сервері DMZ є селектор або таблиця алгоритмів скремблювання, які є частиною спільних секретів та тому є такими ж, як і селектор на сервері DMZ відправляючого вузла, він може використати початковий стан для ідентифікації алгоритму, який використовувався при скремблюванні пакета і може вказати приймаючому вузлу, як дескремблювати пакет. Таким чином, приймаючий вузол відтворює пакет в дескрембльованому вигляді, тим самим відновлюючи вихідні дані. Як правило, до передачі на наступний вузол пакет знову скремблюється відповідно до іншого алгоритму скремблювання. В

цьому випадку приймаючий вузол підключається до свого сервера DMZ, щоб отримати алгоритм скремблювання та початковий стан, і процес повторюється.

Таким чином, коли пакет проходить свій шлях по мережі SDNP, він скремблюється кожним вузлом відповідно до різних алгоритмів скремблювання, і на кожному вузлі створюється новий початковий стан, який дозволяє наступному вузлу дескремблювати пакет.

В альтернативному варіанті здійснення даного винаходу фактичний стан (наприклад, час) може передаватися між вузлами (тобто, відправляючому вузлу не потрібно посилати початковий стан приймаючому вузлу). Сервери DMZ, зв'язані як з відправляючим, так і з приймаючим медіа-вузлами, містять генератори прихованих чисел (знову ж таки, що є частиною спільних секретів), які містять однакові алгоритми в будь-який момент часу. Сервер DMZ, зв'язаний з відправляючим вузлом, використовує стан для генерації прихованого числа, а приховане число - для визначення алгоритму скремблювання з селектора або таблиці можливих алгоритмів скремблювання. Відправляючий вузол передає стан приймаючому вузлу. На відміну від початкових станів, приховані номера ніколи не передаються по мережі, а передаються виключно по конфіденційній лінії зв'язку між медіа-вузлом і сервером DMZ. Коли приймаючий медіа-вузол приймає стан для вхідного пакета даних, генератор прихованих чисел у зв'язаному з ним сервері DMZ, використовує стан для створення ідентичного прихованого номера, який згодом використовується селектором або таблицею для ідентифікації алгоритму, відповідно до якого буде дескремблюватися пакет. Цей стан може бути включено в пакет або може бути передано з відправляючого вузла в приймаючий вузол до передачі пакета або будь-яким іншим маршрутом.

Методи, які використовуються для динамічного шифрування та розділення, аналогічні методам, використовуваним при динамічному скремблюванні, але замість "початкового стану" для динамічного шифрування використовуються "ключі". Спільні секрети, що зберігаються на серверах DMZ, включають в себе селектори або таблиці алгоритмів шифрування та розділення, а також генератори ключів. У разі шифрування с симетричним ключем, відправляючий вузол передає ключ приймаючому медіа-вузлу, який може використовуватися сервером DMZ приймаючого вузла для ідентифікації алгоритму, який використовується при шифруванні пакета, та тим самим дешифрувати файл. У разі шифрування з асиметричним ключем медіа-вузол запитує інформацію, тобто приймаючий вузол спочатку відправляє ключ шифрування вузлу, який містить пакет даних для передачі. Потім відправляючий медіа-вузол зашифровує дані відповідним ключем шифрування. Тільки приймаючий медіа-вузол, який генерує ключ шифрування, має відповідний ключ дешифрування і можливість дешифрувати зашифрований текст, створений з використанням цього ключа шифрування. Важливо відзначити, що при асиметричному шифруванні доступ до ключа шифрування, що використовується для шифрування, не надає ніякої інформації про те, як розшифрувати пакет даних.

При операції розділення медіа-вузол, в якому пакет був розділений, передає початковий стан медіа-вузлу, в якому результуючі субпакети будуть змішуватися, а сервер DMZ, зв'язаний з вузлом змішування, використовує цей початковий стан для ідентифікації алгоритму розділення і, отже, алгоритму, який буде використовуватися при змішуванні субпакетів.

Як зазначено вище, в дво- або триканальних варіантах здійснення винаходу сигнальна функція виконується сигнальним вузлом, який працює в окремій групі серверів, які називаються сигнальними серверами. У таких варіантах здійснення винаходу початкові стани і ключі можуть передаватися через сигнальні сервери, а не з відправляючого медіа-вузла безпосередньо до приймачого медіа-вузлу. Таким чином, відправляючий медіа-вузол може відправляти початковий стан або ключ на сигнальний сервер, а сигнальний сервер може перенаправляти початковий стан або ключ на приймаючий медіа-вузол. Як було зазначено вище, сигнальні сервери відповідають за розробку маршрутів пакета, тому сигнальний сервер знає наступний медіа-вузол, якому направляється кожен пакет.

Щоб ускладнити завдання для потенційних хакерів, список або таблиця можливих методів скремблювання, розділення або шифрування в селекторі може періодично (наприклад, щогодини або щодня) "перетасовуватися" таким чином, щоб методи, що відповідають конкретним початковим станам або ключам, були змінені. Таким чином, алгоритм шифрування, застосовуваний даними медіа-вузлом до пакету, створеного в момент часу t_1 в день 1, може відрізнятися від алгоритму шифрування, який він застосовує до пакету, що був створений в той же час t_1 в день 2.

Кожен з серверів DMZ зазвичай фізично пов'язаний з одним або декількома медіа-вузлами в одній і тій же "групі серверів". Як було зазначено вище, медіа-вузол може запитувати вказівки про те, що робити з отриманим пакетом, надаючи пов'язаному з ним серверу DMZ початковий стан або ключ (наприклад, на основі часу або стану при створенні пакета), але цей медіа-вузол

не може отримати доступ до спільних секретів або будь-яким іншим даним або коду на сервері DMZ. Сервер DMZ відповідає на такі запити, визначаючи початковий стан або ключ і метод, який повинен використовувати медіа-вузол для дескремблювання, дешифрування або змішування пакета. Наприклад, якщо пакет скрембльований, і медіа-вузол хоче знати, як його дескремблювати, сервер DMZ може перевірити список (або селектор) алгоритмів скремблювання, щоб знайти конкретний алгоритм, який відповідає цьому початкового стану. Потім сервер DMZ дає команду медіа-вузлу дескремблювати пакет відповідно до цього алгоритму. Іншими словами, медіа-вузол передає запити, що містяться в початкових станах або ключах, серверу DMZ, а сервер DMZ відповідає на ці запити видачею команд.

Незважаючи на те, що медіа-вузли доступні через Інтернет (хоча у них немає IP-адрес, які розпізнаються DNS), сервери DMZ повністю ізольовані від Інтернету, та з'єднуються тільки в локальній мережі дротами або волоконно-оптичним кабелем з підключеними до цієї мережі медіа-серверами.

В "одноканальних" варіантах здійснення винаходу початкові стани і ключі передаються між відправляючим та приймаючим медіа-вузлами в складі пакету даних або можуть передаватися в окремому пакеті до передачі пакета даних по тому ж маршруту, що і пакет даних. Наприклад, при шифруванні пакета медіа-вузол №1 може включити в пакет ключ шифрування на основі моменту часу, в який було виконано шифрування. Коли цей пакет надходить на медіа-вузол №2, медіа-вузол №2 передає ключ на відповідний сервер DMZ, а сервер DMZ може за допомогою цього ключа вибрати метод дешифрування в своєму селекторі та виконати дешифрування. Потім медіа-вузол №2 може направити запит свого облікового запису DMZ, і знову зашифрувати пакет, перш ніж передати його в медіа-вузол №3. Сервер DMZ знову звертається до селектору, повідомляє медіа-вузлу №2, який метод він повинен використовувати при шифруванні пакета, та передає медіа-вузлу №2 ключ, який відображає стан, що відповідає методу шифрування. Медіа-вузол №2 виконує шифрування та передає зашифрований пакет і ключ (окремо або в складі пакету) медіа-вузлу №3. Потім цей ключ може бути аналогічним чином використаний медіа-вузлом №3 для дешифрування пакета і т.д. В результаті немає одного статичного методу дешифрування, який хакер міг би використовувати при дешифруванні пакетів.

Використання часу або умови динамічного "стану" в наведеному вище прикладі для визначення методу скремблювання, шифрування або розділення, який необхідно включити в початковий стан або ключ, є тільки ілюстративними. Будь-який змінний параметр, наприклад, кількість вузлів, через які пройшов пакет, також може бути використаний як "початковий стан" або ключ, який буде використаний для вибору конкретного методу скремблювання, шифрування або розділення.

В "двоканальних" варіантах початкові стани і ключі можуть передаватися між медіа-вузлами через другий канал "команд і управління", який складається із сигнальних серверів, а не передаватися безпосередньо між медіа-вузлами. Сигнальні вузли можуть також надавати медіа-вузлам інформацію маршрутизації та повідомляти медіа-вузлам на маршруті пакету, як саме цей пакет повинен бути розділений або змішаний з іншими пакетами, при цьому вони вимагають, щоб кожен медіа-вузол застосовував ідентифікаційну "мітку" для кожного переданого пакета, щоб наступний медіа-вузол (вузли) був здатний розпізнавати пакет (и). Сигнальні сервера, по можливості, надають даному медіа-вузлу інформацію тільки про попередній і наступний медіа-вузол для пакета, що проходить через мережу. Жоден окремий медіа-вузол не знає весь маршрут пакета через хмару SDNP. У деяких варіантах здійснення винаходу функція маршрутизації може бути розділена між двома або більше сигнальними серверами, при цьому один сигнальний сервер визначає маршрут до конкретного медіа-вузлу, другий сигнальний сервер визначає маршрут від цього медіа-вузла до іншого медіа-вузлу і так далі до вихідного шлюзового вузла. При цьому жоден сигнальний сервер теж не має повної інформації про маршрут пакета даних.

В "триканальних" варіантах третя група серверів, звана "серверами імен", використовується для ідентифікації елементів в хмарі SDNP і для зберігання інформації, що стосується ідентифікації пристроїв, підключених до хмари SDNP, і їх відповідних IP-адрес або SDNP-адрес. Крім того, сервери імен постійно контролюють медіа-вузли в хмарі SDNP, підтримуючи, наприклад, поточний список активних медіа-вузлів та таблицю затримок поширення для кожної комбінації медіа-вузлів у хмарі. На першому етапі розміщення виклику клієнтський пристрій, наприклад, планшет, може відправити IP-пакет на сервер імен із запитом адреси та іншу інформацію одержувача або абонента. Крім того, окремий виділений сервер імен використовується для роботи при першому контакті щоразу, коли пристрій вперше підключається, тобто реєструється, в хмарі.

В якості додаткового переваги, з точки зору безпеки, в одиночній хмарі SDNP можуть бути передбачені окремі "зони" безпеки, що мають різні селектори, початкові стани і генератори ключів та інші спільні секрети. Суміжні зони з'єднуються мостовими медіа-вузлами, які містять спільні секрети обох зон і мають можливість перетворювати дані, відформатовані відповідно до правил для однієї зони, в дані, відформатовані відповідно до правил для іншої зони, і навпаки.

Аналогічним чином, для зв'язку між різними хмарами SDNP, що обслуговуються, наприклад, різними провайдерами послуг, між інтерфейсами мостових серверів в кожній хмарі формується двобічний канал зв'язку. Кожен інтерфейс мостового серверу має доступ до відповідних спільних секретів і інших елементів безпеки для кожної хмари.

Важливою перевагою даного винаходу є те, що в мережі SDNP немає єдиного пункту управління і що жоден вузол і жоден сервер в цій мережі не має повного уявлення про те, як відбувається передача даних або як вона може динамічно змінюватися.

Наприклад, сигнальні вузли, що працюють на сигнальних серверах, знають маршрут (або, в деяких випадках, тільки частину маршруту), за яким відбувається передача даних, але вони не мають доступу до вмісту переданих даних і не знають, хто є істинним абонентом або клієнтом. Крім того, сигнальні вузли не мають доступу до спільних секретів на серверах DMZ медіа-вузла, тому вони не знають, як шифруються, скремблюються, розділяються або змішуються пакети даних під час передачі.

Сервери імен SDNP знають справжні номери телефонів або IP-адреси абонента, але не мають доступу до переданих даних або маршрутизації різних пакетів та субпакетів. Як і вузли сигналізації, сервери імен не мають доступу до спільних секретів на серверах DMZ медіа-вузла, тому вони не знають, як шифруються, скремблюються, розділяються або змішуються пакети даних під час передачі.

Медіа-вузли SDNP, фактично передають медіа-контент, не маючи уявлення про те, хто є відправником інформації, і не знають маршрут, по якому проходять різні фрагментовані субпакети через хмару SDNP. Насправді, кожен медіа-вузол знає тільки, які пакети даних очікувати (ідентифікуються своїми мітками або заголовками) і куди їх відправляти далі, тобто "наступний перехід", але медіа-вузли не знають, як дані шифруються, скремблюються, змішуються або розділяються, а також не знають, як вибрати алгоритм або дешифрувати файл, використовуючи стан, числове значення початкового стану або ключ. Знання, необхідні для правильної обробки сегментів даних вхідних пакетів, відомі тільки серверу DMZ, який використовує свої спільні секрети, алгоритми, недоступні через мережу або самому медіа-вузлу.

Іншим оригінальним аспектом цього винаходу є його здатність зменшувати мережеву затримку і мінімізувати затримку поширення для забезпечення QoS, а також виключати ехо-сигнали або відкидати виклики шляхом управління розміром пакетів даних, тобто одночасно відправляючи невеликі пакети даних через хмару, а не покладаючись на одне високошвидкісне з'єднання. Динамічна маршрутизація мережі SDNP використовує свої знання про затримки поширення між вузлами мережі для динамічного вибору найкращого маршруту для передачі даних в цей момент часу. В іншому варіанті здійснення винаходу для високопріоритетних клієнтів мережа може полегшувати маршрутизацію передачі, відправляючи дубльовані повідомлення у фрагментованому вигляді через хмару SDNP, вибираючи тільки найшвидші дані для відновлення вихідного звуку або вмісту даних.

Серед багатьох переваг системи SDNP відповідно до цього винаходу в варіантах з паралельною і "решітчастою передачею" пакети можуть бути фрагментовані при їх переході в хмару SDNP, таким чином попередивши можливість потенційним хакерам зрозуміти вміст повідомлення навіть у тому випадку, якщо вони здатні розшифрувати окремий субпакет або групу субпакетів; також в "динамічних" варіантах методи скремблювання, шифрування і розділення, що застосовуються до пакетів, постійно змінюються, що не дає потенційному хакеру будь-якої переваги від успішного дешифрування пакета в даний момент часу. Численні додаткові переваги варіантів здійснення даного винаходу стануть очевидні фахівцям в даній області після ознайомлення з наведеними нижче описом.

Аналогічні методи забезпечення безпеки зазвичай застосовуються на "останній милі" між SDNP хмарою і клієнтським пристроєм, таким як мобільний телефон або планшет. Клієнтський пристрій зазвичай розміщується в окремій від хмари зоні безпеки, і він може спочатку стати авторизованим SDNP клієнтом, що передбачає установку на клієнтський пристрій пакету програмного забезпечення, специфічні для зони безпеки пристрою, зазвичай шляхом завантаження з адміністративного сервера SDNP. Клієнтський пристрій підключається до SDNP хмари через медіа-вузол шлюзу (іноді званий просто "шлюзом") в хмарі. Медіа-вузол шлюзу має доступ до загальних секретів, які належать як до хмари, так і до зони безпеки клієнтського

пристрою, але клієнтський пристрій не має доступу до загальних секретів, які належать до хмари SDNP.

В якості додаткового рівня безпеки клієнтські пристрої можуть обмінюватися матеріалами і ключами безпосередньо один з одним через сигнальні сервери. Таким чином, передавальний клієнтський пристрій може посилати матеріал і/або ключ безпосередньо на приймаючий клієнтський пристрій. У таких варіантах пакет, отриманий приймаючим клієнтським пристроєм, буде в тому ж зашифрованому вигляді, що і пакет, що відправляє клієнтський пристрій. Тому що приймаючий клієнтський пристрій може використовувати ключ або матеріал, який він отримує від передавального клієнтського пристрою, щоб розпакувати або розшифрувати пакет. Обмін матеріалами та ключами безпосередньо між клієнтськими пристроями є доповненням до власного динамічного скремблінгу і шифрування мережі SDNP і, таким чином, являє собою додатковий рівень безпеки, званий вкладеної безпекою.

Крім того, клієнтський пристрій або вузол шлюзу, з яким він взаємодіє, може змішувати пакети, що представляють один і той же вид даних, наприклад, голосові пакети, файли текстових повідомлень, документи, частини програмного забезпечення або різноманітну інформацію, наприклад, один голосовий пакет і один текстовий файл, один текстовий пакет і один відео або фотофайл, перш ніж пакети досягнуть точки призначення SDNP, або вихідний шлюз може розділити пакет клієнта на кілька пакетів. Це на додаток до скремблінгу, шифрування або розділення, яке відбувається в мережі SDNP. У таких випадках клієнтський пристрій відправника може відправити приймаючому клієнтському пристрою ключ, що вказує йому, як розділити пакет таким чином, щоб відтворити оригінальні пакети, які були змішані в медіа-пристрої відправника клієнта або вузлі шлюзу. Послідовне змішування і розділення може представляти собою лінійну послідовність операцій або ж використовувати вкладену архітектуру, в якій клієнти і SDNP хмара виконують свої власні заходи безпеки.

Щоб ще більше заплутати потенційних хакерів, клієнтський пристрій може передавати послідовні пакети (або субпакети) в одному з'єднанні на різні вузли шлюзу і/або може передавати їх по різним фізичним каналам зв'язку (стільникового, Wi-Fi, Ethernet кабель і т.д.) - процес, іноді іменований тут "Multi-PHY" передача. Щоб додати плутанини, він може також включати різні адреси джерел в послідовні пакети, тим самим запобігаючи хакерську ідентифікацію пакетів як виходять з одного і того ж клієнтського пристрою.

Винахід також включає унікальні досягнення в обробці телефонних конференц-дзвінків. Звичайними пакетами конференц-зв'язку всім учасникам розмови відправляються пакети конференц-зв'язку. Відповідно до цього винаходом, деякі обрані учасники можуть бути "відключені", тобто виключені з розмови, перешкоджаючи передачі клієнтському пристрою або іншому вузлу пакетів учаснику або учасникам, які повинні бути відключені. В альтернативному варіанті пакети даних відправляються в широкомовному режимі всім учасникам групового виклику, але з впровадженням різних методів шифрування. Що стосується звичайних конференц-дзвінків пакети даних надсилаються всім користувачам з використанням шифрування, де у всіх учасників є копія ключа дешифрування. У приватному режимі або в режимі відключення звуку пакети даних, що передаються користувачем, використовують інше шифрування, при якому ключ дешифрування передається тільки обраним користувачам.

Короткий опис зображень

На наведених нижче зображеннях компонентам, які мають загальну схожість, присвоєні подібні числові позначення. Однак слід зазначити, що не кожен компонент, якому присвоєно певне числове позначення, обов'язково ідентичний іншому компоненту з тим же числовим позначенням. Наприклад, операція шифрування, що має конкретне числове позначення, необов'язково ідентична іншій операції шифрування з тим же числовим позначенням. Більш того, групи компонентів, наприклад, сервери в мережі, які мають одне спільне ідентифікаційне числове позначення, необов'язково ідентичні один одному.

На Рис. 1 схематично показано процес стандартної передачі пакетів по мережі.

На Рис. 2A схематично показано процес скремблювання пакета.

На Рис. 2B схематично показано процес дескремблювання пакетів.

На Рис. 2C схематично показано різні алгоритми скремблювання пакетів.

На Рис. 2D схематично показано статичне параметричне скремблювання пакетів.

На Рис. 2E схематично показано динамічне скремблювання з прихованим числом.

На Рис. 3 схематично показано процес повторного скремблювання пакетів.

На Рис. 4A схематично показано процес шифрування пакетів.

На Рис. 4B схематично показано процес дешифрування пакетів.

На Рис. 5 схематично показаний процес скремблювання з шифруванням і його зворотна функція.

На Рис. 6 схематично показано процес повторного пакетування даних DUSE, що включає повторне скремблювання і повторне шифрування.

На Рис. 7A схематично показано процес розділення пакетів фіксованої довжини.

На Рис. 7B схематично показано процес змішування пакетів фіксованої довжини.

На Рис. 8 схематично показано різні способи змішування пакетів.

На Рис. 9A наведено таблицю, яка узагальнює функції та анти-функції безпеки SDNP.

На Рис. 9B представлена блок-схема, що ілюструє операції безпеки SDNP, виконувані на вхідних і вихідних пакетах даних одномаршрутного зв'язку "Останньої Милі".

На Рис. 9C представлена блок-схема, що ілюструє операції безпеки SDNP, виконувані на вхідних і вихідних пакетах даних для багатомаршрутного зв'язку "Останньої Милі".

На Рис. 9D представлена блок-схема, що ілюструє створення аудіо, відео, текстового і файлового контенту, підготовку пакетів даних, розпізнавання пакетів даних і відтворення контенту на клієнтському пристрої SDNP.

На Рис. 9E представлено зображення пакета даних SDNP з використанням 7-рівневої моделі OSI для ілюстрації ієрархічної інкапсуляції даних.

На Рис. 9F представлена графіка і таблиця із зображенням корисного навантаження SDNP.

На Рис. 9G представлена блок-схема, що ілюструє процес обробки вхідних пакетів даних "Останньої Милі" в шлюзі SDNP з використанням триканального зв'язку.

На Рис. 9H представлена блок-схема, що ілюструє процес обробки вхідних пакетів даних "Останньої Милі" в шлюзі SDNP з використанням одноканального зв'язку.

На Рис. 9I представлена блок-схема, що ілюструє процес обробки вихідних пакетів даних "Останньої Милі" в шлюзі SDNP з використанням триканального зв'язку.

На Рис. 10 наведено схематичне зображення SDNP хмари.

На Рис. 11 схематично показані приклади небезпечного зв'язку "Останньої Милі" без перевірки автентичності.

На Рис. 12 показано небезпечний зв'язок "Останньої Милі" за старою телефонною системою (POTS) без перевірки особи абонентів.

На Рис. 13 схематично показані приклади небезпечного зв'язку "Останньої Милі" з перевіркою автентичності.

На Рис. 14 показано небезпечний зв'язок "Останньої Милі" за аналоговою телефонною мережею загального користування (PSTN) з перевіркою особи оператора.

На Рис. 15 показано небезпечний зв'язок "Останньої Милі" по цифровій дротовій мережі з перевіркою автентичності на основі логіна або токена.

На Рис. 16 показано небезпечний зв'язок "Останньої Милі" по аналоговій дротовій мережі з перевіркою особи на основі PIN-коду або кредитної картки.

На Рис. 17 показано приклади комунікації гіперзахищеного зв'язку "Останньої Милі", що підтримує перевірку автентичності.

На Рис. 18 показано гіперзахищений зв'язок "Останньої Милі" по бездротовій мережі Wi-Fi, яка може бути перевірена на предмет ідентифікації.

На Рис. 19 показано гіперзахищений зв'язок "Останньої Милі" по стільниковій бездротовій мережі, яка може бути перевірена на предмет ідентифікації.

На Рис. 20 показано гіперзахищений зв'язок "Останньої Милі" по дротовій мережі Ethernet, яка може бути перевірена на предмет ідентифікації.

На Рис. 21 показано гіперзахищений зв'язок "Останньої Милі" по кабельній дротовій мережі, який може бути перевірено.

На Рис. 22 показано ідентифікований гіперзахищений зв'язок "Останньої Милі" по комбінованих кабельних лініях і домашніх бездротових мережах Wi-Fi.

На Рис. 23 схематично представлено приклад з'єднання по "Останній Милі", що включає ідентифікатор ділянки гіперзахищеного зв'язку, підключеного до захищеного LAN останнього з 'єднання з ідентифікатором.

На Рис. 24 проілюстровано зв'язок "Останньої Милі", що складається з ідентифікатора ділянки дротової лінії гіперзахищеного зв'язку (який піддається перевірці), підключеного по дротовій лінії до захищених пристроїв з порушенням ідентифікації і до невпізнаних незахищених пристроїв.

На Рис. 25 проілюстровано зв'язок "Останньої Милі", що складається з ідентифікатора ділянки дротової лінії гіперзахищеного зв'язку (який піддається перевірці), підключеного через Wi-Fi LAN до захищених ідентифікатором WPA обчислювальних і комунікаційних пристроїв на роботі і вдома.

На Рис. 26 проілюстровано зв'язок "Останньої Милі", що складається з ідентифікатора ділянки дротової лінії гіперзахищеного зв'язку (який піддається перевірці), підключеної через Wi-Fi LAN до захищених WPA-пристроїв Інтернету речей, що забезпечують ідентифікацію.

На Рис. 27 проілюстровано зв'язок "Останньої Милі", що складається з ділянки дротової лінії гіперзахищеного зв'язку (який піддається ідентифікації), підключена по Ethernet або Wi-Fi LAN до пристроїв, захищених WPA-ідентифікацією для бізнесу.

На Рис. 28 схематично проілюстровано приклад зв'язку "Останньої Милі", що складається з етапів гіперзахищеного зв'язку (які піддаються ідентифікації), з'єднаних захищеними дротовими або захищеними бездротовими LAN каналами.

На Рис. 29A схематично проілюстровані дротові і бездротові мости гіперзахищеного зв'язку, що включають Ethernet і Wi-Fi, що застосовуються в мережах зв'язку "Останньої Милі".

На Рис. 29B схематично проілюстровані дротові та бездротові гіперзахищені мости з використанням супутникових та автомобільних мереж зв'язку "Останньої Милі".

На Рис. 29C схематично проілюстровані дротові і бездротові гіперзахищені мости з використанням кабельних і стільникових мереж, що застосовуються в мережах зв'язку "Останньої Милі".

На Рис. 30 проілюстровано зв'язок "Останньої Милі", що складається з бездротового гіперзахищеного зв'язку (який піддається ідентифікації) через супутник до різних пристроїв, включаючи телефони, літаки, потяги, судна і домашні супутникові приймачі (телевізійні приставки).

На Рис. 31A показано приклад останнього каналу гіперзахищеного зв'язку між пристроями бортового зв'язку літака із супутником.

На Рис. 31B наведено приклад супутникового зв'язку і антенного модуля літака.

На Рис. 32 наведено приклад останнього каналу гіперзахищеного зв'язку між пристроями в мережі зв'язку на борту круїзного судна з кількома каналами супутникового зв'язку.

На Рис. 33 наведено приклад гіперзахищеного зв'язку "Останньої Милі" між пристроями бортової мережі залізничного зв'язку з радіозв'язком і супутником.

На Рис. 34 показано гіперзахищений зв'язок "Останньої Милі" з автомобільним телематичним модулем, включаючи підключення до останнього стільникового каналу.

На Рис. 35 наведено приклад останньої ланки зв'язку між телематичними модулями в мережі автомобільного зв'язку зі стільниковим зв'язком і пристроями, підключеними до мережі Wi-Fi в кабіні.

На Рис. 36 наведено приклад міжтранспортного гіперзахищеного зв'язку зі стільниковим зв'язком.

На Рис. 37 зображена гіперзахищена технологія для магістрального зв'язку по мікрохвильовій, супутниковій та оптоволоконній мережам.

На Рис. 38 показано порівняння функцій безпеки, перевірки особи та анонімності того, хто дзвонить для гіперзахищених, захищених і незахищених мереж зв'язку.

На Рис. 39 представлена схема одномагістрального гіперзахищеного з'єднання останньої милі зі статичними IP-адресами.

На Рис. 40A представлено схематичне зображення IP стека одномагістрального гіперзахищеного з'єднання "Останньої Милі" з використанням статичних IP-адрес.

На Рис. 40B представлено спрощене подання одномаршрутного гіперзахищеного зв'язку "Останньою Милі" з використанням статичних IP-адрес.

На Рис. 41 представлена схема одномаршрутного гіперзахищеного зв'язку з динамічними клієнтськими IP-адресами в режимі "Останньої Милі".

На Рис. 42A представлено зображення IP стека одномагістрального гіперзахищеного зв'язку "Останньої Милі" з використанням динамічних клієнтських IP-адрес.

На Рис. 42B представлено альтернативне зображення IP стека одномагістрального з'єднання гіперзахищеного зв'язку "Останньою Милі" з використанням динамічних клієнтських IP-адрес.

На Рис. 43 наведено схему багатомаршрутного гіперзахищеного зв'язку зі статичними IP-адресами "Останньої Милі".

На Рис. 44A наведено зображення IP стека багатоканального гіперзахищеного зв'язку "Останньою Милі" зі статичними IP-адресами з використанням останнього PHY з' єднання.

На Рис. 44B наведено зображення IP стека багатоканального гіперзахищеного зв'язку "Останньою Милі" зі статичними IP-адресами з використанням декількох останніх PHY-з' єднань.

На Рис. 45 наведена схема багатомаршрутного гіперзахищеного зв'язку з динамічними клієнтськими IP-адресами, побудована за принципом "Останньої Милі".

На Рис. 46A представлено зображення IP стека багатоканального гіперзахищеного зв'язку "Останньою Милі" з динамічними клієнтськими IP-адресами за допомогою одного PHY останнього з' єднання.

На Рис. 46B представлено зображення IP стека багатоканального гіперзахищеного зв'язку "Останньої Милі" з динамічними клієнтськими IP-адресами з використанням декількох останніх PHY-з' єднань.

На Рис. 47 представлена схема альтернативної версії багатомаршрутного гіперзахищеного зв'язку "Останньої Милі" з динамічними клієнтськими IP-адресами.

На Рис. 48 показано IP стек альтернативної версії багатомаршрутного гіперзахищеного зв'язку "Останньої Милі" з динамічними клієнтськими IP-адресами.

На Рис. 49 представлені датаграми IPv4 і IPv6 для Ethernet-комунікацій з корисним навантаженням SDNP.

На Рис. 50A представлені пакети IPv4 і IPv6 "Останньої Лінії" Ethernet, що використовуються у зв'язках Клієнт – SDNP Хмара.

На Рис. 50B представлені пакети Ethernet-з'єднання IPv4 і IPv6 шлюзу, що використовуються в хмарному зв'язку між клієнтом і SDNP.

На Рис. 50C представлені пакети Ethernet-з'єднання IPv4 і IPv6 шлюзу, що використовуються в SDNP хмарі для зв'язку з Клієнтом.

На Рис. 50D представлені пакети IPv4 і IPv6 "Останньої Лінії" Ethernet, що використовуються в SDNP-хмарі для зв'язку з Клієнтом.

На Рис. 51A показано послідовні пакети даних Ethernet (скорочені), які використовуються в одномаршрутному зв'язку "Останньою Милі" зі статичною адресацією клієнта.

На Рис. 51B показано послідовні пакети даних Ethernet (скорочені), які використовуються в одномаршрутному зв'язку "Останньою Милі" з динамічною адресацією клієнта.

На Рис. 51C показано послідовні пакети даних Ethernet (скорочені), які використовуються у багатомаршрутному зв'язку "Останньою Милі" зі статичною адресацією клієнта.

На Рис. 51D показано послідовні пакети даних Ethernet (скорочені), які використовуються в багатомаршрутному зв'язку "Останньою Милі" з динамічною адресацією клієнта.

На Рис. 52A наведена таблиця, що узагальнює маршрутизацію SDNP-зв'язку "Останньої Милі" по мережі Ethernet.

На Рис. 52B наведені топологічні описи одномагістрального зв'язку "Останньої Милі" по мережі Ethernet.

На Рис. 52C наведені топологічні описи багатомаршрутного зв'язку "Останньої Милі" по мережі Ethernet.

На Рис. 52D наведені додаткові топологічні описи багатомаршрутного зв'язку "Останньої Милі" по мережі Ethernet.

На Рис. 53 графічно представлені IPv4 і IPv6 для Wi-Fi зв'язку з корисним навантаженням SDNP.

На Рис. 54A являє собою графічне представлення пакетів IPv4 і IPv6 "Останньої Лінії" по мережі Wi-Fi, що використовуються у зв'язках між клієнтом і SDNP хмарою.

На Рис. 54B графічно представлені Wi-Fi пакети IPv4 і IPv6 Gateway Link, що використовуються в Wi-Fi зв'язках при комунікації клієнта і SDNP хмари.

На Рис. 54C графічно представлені Wi-Fi пакети IPv4 і IPv6 Gateway Link, що використовуються при комунікації клієнта і SDNP хмари.

На Рис. 54D графічно представлені датаграми пакетів IPv4 і IPv6 "Останньої Лінії" за Wi-Fi, що використовуються при комунікації клієнта і SDNP хмари.

На Рис. 55 графічно представлені датаграми пакетів IPv4 і IPv6 для стільникового зв'язку 4G з корисним навантаженням SDNP.

На Рис. 56A графічно представлені пакети даних стільникового зв'язку IPv4 і IPv6 "Останньої Лінії" 4G, що використовуються при комунікації клієнта і SDNP хмари.

На Рис. 56B графічно представлені стільникові пакети IPv4 і IPv6 "Останньої Лінії" по мережі 4G, що використовуються при комунікації SDNP хмари і клієнта.

На Рис. 57A графічно представлено одномедійне PHY (фізичного)-з'єднання "Останньої Лінії".

На Рис. 57B графічно представлено взаємодію змішаних мультимедійних PHY-каналів "Останньої Лінії".

На Рис. 57C графічно представлені альтернативні реалізації зв'язку багаторівневого PHY-з' єднання "Останньої Лінії".

На Рис. 58 графічно представлені послідовні з 'єднання клієнта з SDNP хмарою "Останньої Лінії" з використанням датаграм IPv6, що передаються за протоколом Multi-PHY Ethernet.

На Рис. 59 графічно представлені послідовні з 'єднання клієнта з SDNP хмарою "Останньої Лінії" з використанням датаграм IPv6, що передаються за протоколом Multi-PHY Wi-Fi.

На Рис. 60 графічно представлено послідовний зв'язок клієнта з SDNP хмарою "Останньої Лінії" з використанням датаграм IPv6, що передаються по стільникових мережах Multi-PHY 4G.

На Рис. 61 графічно представлені послідовні з 'єднання клієнта з SDNP хмарою "Останньої Лінії" з використанням датаграм IPv6 з використанням Multi-PHY доставки по Ethernet і Wi-Fi.

На Рис. 62 графічно представлено послідовний зв'язок клієнта з SDNP хмарою "Останньої Лінії" з використанням датаграм IPv6 з використанням мульти-PHY доставки і Wi-Fi і 4G стільникових мереж.

На Рис. 63 представлена схема стека рівнів OSI кабельної модемної мережі зв'язку DOCSIS, що ілюструє функціональність від першого до сьомого рівнів.

На Рис. 64 графічно представлені базові комунікаційні пакети DOCSIS3, призначені для кабельних систем з корисним навантаженням SDNP.

На Рис. 65A графічно представлені методи розподілу спектра і модуляції несучої для різних протоколів DOCSIS3.

На Рис. 65B графічно представлено послідовність комунікацій DOCSIS3.1 між CTMS і CM.

На Рис. 65C графічно зображено висхідний зв'язок DOCSIS3.1.

На Рис. 65D графічно зображено низхідний зв'язок DOCSIS3.1.

На Рис. 66 наведена схема тримаршрутної SDNP-мережі для зв'язку "Останньої Милі".

На Рис. 67 схематично представлена операція "запит виклику" в триканальному зв'язку "Останньої Милі" SDNP.

На Рис. 68 наведено схему операції "запит адреси" в триканальному каналі зв'язку "Останньої Милі" SDNP.

На Рис. 69 схематично представлена операція "доставки адреси" в триканальному каналі зв'язку "Останньої Милі" SDNP.

На Рис. 70 наведено схему, що ілюструє синтез команд SDNP і пакетів керування.

На Рис. 71 наведено схему виконання операції "Інструкції з маршрутизації" в одномаршрутному триканальному зв'язку "Останньої Милі" SDNP.

На Рис. 72 схематично представлена операція " SDNP виклик" в одномаршрутный триканальній передачі даних "Останньої Милі" SDNP від клієнта SDNP до SDNP хмари.

На Рис. 73A показана схема з 'єднання SDNP хмари і маршруту "Останньої Милі" з клієнтом SDNP у вигляді триканального з' єднання при SDNP виклику.

На Рис. 73B представлена схема з 'єднання SDNP хмари і триканального каналу зв'язку "Останньої Милі", реалізованої у вигляді "виклику" по не-SDNP-клієнту.

На Рис. 74 наведено схему виконання операції "інструкції з маршрутизації" в багатоканальному триканальному SDNP-зв'язку "Останньої Милі".

На Рис. 75A схематично зображена операція "SDNP call" в триканальному SDNP-зв'язку "Останньої Милі" в напрямку від клієнта SDNP до хмари SDNP.

На Рис. 75B представлена схема операції "SDNP дзвінок" у багатоканальному триканальному SDNP-зв'язку "Останньої Милі" в напрямку від SDNP хмари до клієнта SDNP.

На Рис. 76 наведено схему роботи функції групового виклику "інструкції з маршрутизації" при одномаршрутному триканальному SDNP-зв'язку "Останньої Милі".

На Рис. 77A схематично зображений "груповий виклик SDNP" з використанням багатомаршрутного хмарного транспорту SDNP і SDNP-зв'язку "Останньої Милі" в напрямку від клієнта зони U1 до клієнтів в інших зонах.

На Рис. 77B представлена схема "групового виклику SDNP" з використанням багатомаршрутного хмарного транспорту SDNP і протоколу SDNP-зв'язку "Останньої Милі" в напрямку від клієнта зони U7 до клієнтів в інших зонах.

На Рис. 77C представлена схема "груповий виклик SDNP" з використанням багатомаршрутного хмарного транспорту SDNP і SDNP-зв'язку "Останньої Милі" в напрямку від клієнта зони U9 до інших клієнтів в тій же зоні і в інших зонах.

На Рис. 78 представлена схема "групового виклику SDNP" з використанням багатомаршрутного хмарного транспорту SDNP і зв'язку "Останньої Милі" як для клієнтів SDNP, так і для незахищених пристроїв PSTN.

На Рис. 79A в табличній формі представлені операції звичайних і приватних викликів у групі SDNP.

На Рис. 79B в табличній формі показано звичайні та гіперприватні виклики в групі SDNP-викликів.

На Рис. 80A в табличній формі показано звичайні та приватні групові дзвінки в SDNP PTT.

На Рис. 80B в табличній формі представлені звичайні та гіперприватні групові виклики SDNP PTT.

На Рис. 81 наведено схему передачі даних для операції запису фрагментованих даних у гіперзахищене файлове сховище.

На Рис. 82A наведено схему потоку даних для запису фрагментованих даних у гіперзахищене файлове сховище.

На Рис. 82B наведено схему потоку даних для читання в гіперзахищеному файловому сховищі.

На Рис. 83 наведено схему передачі даних для читання фрагментованих даних у гіперзахищеному файловому сховищі.

На Рис. 84A показано різні приклади з'єднаних до хмар файлових сховищ SDNP.

На Рис. 84B представлена схема гіперзахищеної розподіленої мережі зберігання файлів, що складається з локальних і хмарних серверів зберігання даних.

На Рис. 85A показано відображення файлів резервного (RRF=0) гіперзахищеного файлового сховища.

На Рис. 85B показано відображення файлів RRF=1 зчитування надлишкового гіперзахищеного файлового сховища.

На Рис. 85C наведено співставлення файлів RRF=2 зчитування надлишкового гіперзахищеного файлового сховища.

На Рис. 86 представлена схема мережі розподіленої гіперзахищеної файлової системи зберігання з використанням триканального мережевого зв'язку.

На Рис. 87A показано запит на запис файла у розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 87B буде показано дію запиту на назву файлового сервера у розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 87C показана операція планування сигнального сервера в розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 87D показано інструкцію маршрутизації на стороні сигнального сервера клієнта "Останньої Милі" і хмари SDNP для запису в розподілену гіперзахищену систему зберігання файлів.

На Рис. 87E показано інструкцію з маршрутизації на стороні сигнального сервера "Останньої Милі" і хмари SDNP для запису в розподілену гіперзахищену систему зберігання файлів.

На Рис. 88 показано передачу файлів у розподілену гіперзахищену систему зберігання файлів.

На Рис. 89A показано відповідь посилання, що підтверджує роботу сховища файлів і запис до розподіленої гіперзахищеної системи зберігання файлів.

На Рис. 89B показано передачу каналу зв'язку з сервером зберігання файлів у розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 89C показано сервер зберігання файлів для запису пакету даних підтвердження, що містить посилання FS.

На Рис. 89D показано синтез посилання на читання файлового сховища в клієнтському SDNP-месенджері.

На Рис. 90A показано файлову карту нерезервного RRF=0 гіперзахищеного файлового сховища з посиланнями LRF=0 нерезервних FS.

На Рис. 90B показана карта гіперзахищеного файлового сховища RRF=0 з резервуванням каналів LRF=1.

На Рис. 90C показана карта гіперзахищеного файлового сховища RRF=1 з резервуванням каналів LRF=1.

На Рис. 91 представлено графік стійкості сховища залежно від кількості серверів зберігання файлів і клієнтських FS-з'єднань.

На Рис. 92 наведено схему функцій SDNP-шифрування і SDNP-дешифрування.

На Рис. 93A представлено схему розподіленого файлового сховища SDNP із захистом клієнтських файлів і гіперзахищеною передачею файлів.

На Рис. 93B представлено схему розподіленого файлового сховища SDNP з вкладеною системою захисту та гіперзахищеної передачею файлів.

На. 94 зображено спрощену схему гіперзахищеного кодування у розподіленому файловому сховищі SDNP.

На Рис. 95 наведено спрощену схему гіперзахищеного декодування в розподіленому файловому сховищі SDNP для читання.

На Рис. 96A представлено схему, яка описує дії AAA під час читання гіперзахищених файлів.

На Рис. 96B представлено схему, що описує доступ до файлів і транспорт SDNP у процесі читання гіперзахищених файлів.

На Рис. 97A показано роботу з запитами на читання файлів у розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 97B показано запит на назву сервера зберігання файлів у розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 97C показано планування доставки імені сервера зберігання файлів і сигнального сервера в розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 97D показана інструкція з читання в розподіленій гіперзахищеній системі зберігання файлів на стороні сигнального сервера "Останньої Милі" і в хмарі SDNP.

На Рис. 97E показано інструкцію з маршрутизації на стороні сигнального сервера клієнта "Останньої Милі" і хмари SDNP для читання в розподіленій гіперзахищеній системі зберігання файлів.

На Рис. 98 показано декодування файлів на стороні сховища під час читання у розподіленій гіперзахищеній файловій системі зберігання.

На Рис. 99 показано передачу файлових даних у розподіленій гіперзахищеній файловій системі зберігання під час читання.

На Рис. 100 показано передачу даних у розподіленій гіперзахищеній системі зберігання файлів під час оновлення посилання.

На Рис. 101 показано передачу даних у розподіленій гіперзахищеній системі зберігання файлів, яка використовується для перерозподілу файлів.

На Рис. 102 показано позначки часу в текстових повідомленнях SDNP.

На Рис. 103 наведено схему зареєстрованого зв'язку SDNP.

На Рис. 104A показано наскрізне шифрування в OTT-комунікації Internet OTT.

На Рис. 104B показано наскрізне шифрування в гіперзахищеній комунікації.

На Рис. 105A представлена схема операції "SDNP виклик" з агентом безпеки SDNP, що здійснює невидимий моніторинг вихідного виклику.

На Рис. 105B показана схема операції "SDNP виклик" з агентом безпеки SDNP, що здійснює невидимий моніторинг вхідного виклику.

На Рис. 106 показано передачу даних між сервером зберігання файлів у розподіленій гіперзахищеній системі зберігання з агентом безпеки SDNP, що виконує невидимий моніторинг маршрутизації каналів FS.

На Рис. 107 наведено схему операції "SDNP виклик" з агентом безпеки SDNP, що виконує невидимий моніторинг вихідного виклику з використанням багатоканального зв'язку "Останньої Милі".

На Рис. 108 наведено схему дій з призначення та авторизації агента служби безпеки SDNP.

На Рис. 109 показано зв'язок між мобільним телефоном і станцією, схильною до вразливості SS7.

На Рис. 110 показано зв'язок SDNP з використанням маскування телефонних номерів для відбиття атак SS7.

На Рис. 111 показано хостинг хмарних мереж SDNP SoftSwitch на виділених серверах.

На Рис. 112 показано хостинг хмарних мереж SDNP SoftSwitch на публічних серверах.

На Рис. 113 показано хостинг хмарних мереж SDNP SoftSwitch на мережах, що перетинаються.

На Рис. 114 підключення хмарних мереж SDNP SoftSwitch до глобальної хмарної телекомунікаційної мережі SDNP.

На Рис. 115 наведено приклад підмережі SDNP.

Опис винаходу

Після майже півтора століття використання телефонних мереж з комутованими каналами сучасні системи і мережі зв'язку за період часу тривалістю всього лише в якесь десятиліття перейшли до використання методу пакетної комутації даних з використанням протоколу мережі Інтернет, з передачею даних через мережі стандартів Ethernet, Wi-Fi, 4G/LTE і DOCSIS3 по звичайним і оптоволоконним кабелями. Можна назвати багато переваг технології спільної передачі голосових, текстових даних і комп'ютерних даних, а також статичних та відеозображень; серед них - використання резервних шляхів передачі даних для гарантування надійної доставки IP-пакетів (що є причиною, по якій Інтернет спочатку і створювався), а також безпрецедентний рівень взаємодії та можливостей по об'єднанню мереж в масштабах всього світу. Однак, як і у випадку з будь-якими інноваціями, ступінь складності завдань, які доводиться

вирішувати в зв'язку з введенням в дію нових технологій, можна порівняти з кількістю наданих ними переваг.

Недоліки існуючих провайдерів послуг зв'язку

Як було описано у вступній частині цієї розповіді, сучасні системи зв'язку характеризуються багатьма недоліками. Найпродуктивніші системи зв'язку сьогодні, що складаються з створеного на замовлення цифрового обладнання, яке знаходиться у власності найбільших світових провайдерів послуг телекомунікації, таких як AT & T, Verizon, NTT, Vodaphone і т.д., як правило, забезпечують чудову якість передачі голосу, але за високою вартістю, яка включає в себе високі тарифи щомісячної абонплати, тарифи на підключення послуг, тарифи на використання телекомунікації, складні плани обліку різних швидкостей передачі даних, оплату роумінгових послуг при використанні телекомунікації, а також різні тарифи на використання послуг з технічного обслуговування обладнання. Так як форма власності зазначених мереж є приватною, інформація про фактичну безпеку передачі даних не знаходиться в громадському доступі; і факти порушення безпеки даних, здійснення хакерських атак і несанкціонованого втручання в роботу систем не оприлюднюють публічно. З урахуванням кількості фактів підслуховування телефонних розмов та порушення права на недоторканність приватного життя, про які засоби масової інформації повідомляють щодня, існують серйозні сумніви в безпеці процесу зв'язку, що забезпечується приватними провайдерами відповідних послуг - під загрозою може перебувати безпека передачі даних, що знаходяться якщо не в приватній хмарі зазначених провайдерів, то, у крайньому разі, в процесі їх передачі з використанням з'єднань "останньої милі".

"Інтернет-провайдери" є ще однією ланкою в глобальній мережі комунікацій. Як описано в передмові до даного винаходу, процес передачі голосових повідомлень по мережі Інтернет з використанням технології VoIP характеризується безліччю проблем, пов'язаних з QoS, включаючи наступні:

- Інтернет, будучи мережею з пакетною комутацією даних, не призначений для регулярної в часі передачі IP-пакетів, або ж для підтримки додатків в режимі реального часу з низькими значеннями тимчасових затримок та високою якістю обслуговування.

- Характер маршрутизації IP-пакета є непередбачуваним, що призводить до виникнення затримок мінливою величини, раптовим "викидам" великої кількості помилок передачі даних, а також несподіваним "провалам" в передачі голосових даних.

- Маршрут передачі IP-пакета вибирається на розсуд Інтернет-провайдера, який визначає конкретну мережу, через яку буде здійснюватися передача пакетних даних, і може регулювати процес маршрутизації з урахуванням балансування завантаження своєї власної мережі або ж кращого обслуговування своїх VIP-клієнтів за рахунок погіршення якості з'єднання основної маси своїх клієнтів - загального трафіку в своїй мережі.

- Провайдери послуг "низької якості" ("OTT providers"), такі як, наприклад, Line, KakaoTalk, Viber і т.д., використовують вільні канали передачі даних в мережі Інтернет, подорожуючи по ньому "автостопом" і, таким чином, не маючи можливості контролювати чинники, що забезпечують якість передачі даних в мережі.

- Використання "великовагових" аудіокодеків, які не здатні забезпечити розбірливість переданих голосових даних навіть при помірних швидкостях передачі даних.

- Використання технології передачі голосових даних, що базується на застосуванні протоколу передачі даних TCP, призводить до високих тимчасових затримок та зниження якості аудіопотока, що пов'язано з наявністю затримок, викликаних використанням протоколів "рукостискання" та процесами повторної передачі IP-пакетів. При використанні в процесі передачі даних тільки протоколу UDP без допоміжних засобів, відсутні гарантії збереження цілісності корисного навантаження.

Окрім проблем низької якості обслуговування, рівень безпеки сьогоднішніх пристроїв і мереж є абсолютно неприйнятним і не відповідає потребам майбутніх глобальних комунікацій. Як було раніше описано у вступі, рівень безпеки мереж перед обличчям великої кількості здійснюваних кібернетичних атак з використанням комунікаційних пристроїв, включаючи ті, на яких встановлено шпигунське програмне забезпечення, троянські програми, програми-віруси та програми для фішингу, є неадекватним; серед небезпек, що чекають користувача на рівні "останньої ланки" - шпигунське програмне забезпечення, перехоплення пакетів, підслуховування телефонних розмов та перехоплення розмов з використанням шахрайських піратських базових станцій; на рівні місцевої мережі або частини мережі, що обслуговується місцевими телефонними компаніями (з'єднання "останньої милі") - шпигунське програмне забезпечення, перехоплення пакетів, вірусні програми та піратські "атаки посередників". До самої хмари може здійснюватися несанкціонований доступ, що супроводжується зломом

засобів забезпечення безпеки на будь-якому з шлюзів - тут вступають в дію такі фактори, як використання вірусного програмного забезпечення, атаки кіберзлочинців ("атаки посередників"), DoS-атаки, а також несанкціоноване урядове стеження. Підсумувавши, можна сказати, що безпека сьогоднішнього процесу зв'язку знаходиться під загрозою з урахуванням численних вразливостей, з легкістю використовуваних кіберзлочинцями, що забезпечують можливість здійснення кіберзлочинів або порушення приватності користувачів в кібернетичному просторі; серед зазначених видів уразливості можна назвати наступні:

- Наявність відкритої інформації про одержувача IP-пакета, включаючи IP-адресу одержувача, номер порту одержувача і MAC-адресу одержувача.
- Наявність відкритої інформації про джерело IP-пакета, включаючи IP-адресу джерела, номер порту джерела і MAC-адресу джерела.
- Наявність відкритої інформації про тип використовуваного транспортного рівня 4, а також (на основі інформації про номер порту) - про тип запитуваної послуги і даних програми, вкладених усередині корисного навантаження IP-пакета
- При використанні незашифрованих файлів - наявність доступу до всіх даних програми та файловим даним, закритим усередині корисного навантаження IP-пакета, - включаючи приватну та конфіденційну інформацію, дані входу в систему, паролі додатків, фінансові дані, а також відео- та фотодані.
- Наявність діалогу зв'язку, що дає можливість кіберзлочинцю здійснювати повторні спроби злому зашифрованих файлів
- Наявність численних можливостей по установці шкідливого ПО (включаючи шпигунське ПЗ, програми для фішингу та троянські програми) на пристрої зв'язку і маршрутизатори з використанням шляхів проникнення вірусів через протокол FTP, повідомлення електронної пошти та веб-сторінки.

Повторюючи ключове положення, можна заявити, що основним недоліком, характерним для мереж з пакетною комутацією, що використовують Інтернет-протокол є те, що будь-яка вороже налаштована сторона або кіберзлочинець, перехопивши IP-пакет, можуть бачити, які пристрої брали участь в процесі створення даних, що входять до складу IP-пакета, звідки прийшов цей IP-пакет, куди він пересилається зараз, як відбувається процес передачі даних (тобто, чи використовується протокол UDP або ж використовується протокол TCP), а також запит на надання якої послуги був відправлений (тобто, дані програми якого типу містяться всередині корисного навантаження). В даному відношенні, кіберзлочинець здатний визначити "контекст" розмови, що полегшує йому процес злому використовуваного коду шифрування, компрометації безпеки використовуваного пароля і діставання несанкціонованого доступу до файлів, даних та змістом корисного навантаження.

Шифрування - Для захисту від різного роду описаних кібератак, сучасні мережеві адміністратори, фахівці з інформаційних технологій та самі програмні додатки можуть використовувати, в основному, лише один засіб захисту - шифрування. Шифрування є засобом перетворення звичайного, простого тексту (тексту, призначеного для читання, тексту виконуваних програм, призначених до перегляду відеофайлів, файлів зображень або ж призначених до прослуховування аудіофайлів) в альтернативні типи файлів, відомі під назвою "зашифрований текст", які представляються у вигляді потоків беззмістовних текстових символів.

Процес шифрування, перетворення незахищеного файлу в зашифрований файл, включає в себе використання логічних або математичних алгоритмів, які називаються "кодом", що дозволяє перетворити дані в еквівалентні текстові елементи без демонстрації будь-якої очевидної моделі процесу перетворення, що протікає під час шифрування. Після цього зашифрований файл пересилається по мережі зв'язку або ж з використанням будь-якого комп'ютерного носія на пристрій-одержувач. Після отримання файлу отримуючий пристрій декодує зашифроване повідомлення з використанням процесу, відомого під назвою "дешифрування", для відображення оригінального вмісту файлу. Дисципліна, що вивчає процеси шифрування і дешифрування та відома під загальним найменуванням "криптографія", поєднує в собі елементи математики (включаючи теорію чисел, теорію множин та теорію розробки алгоритмів), комп'ютерної науки і електротехніки.

При використанні простих технологій шифрування, із застосуванням "одного ключа" або "симетричного ключа", для розблокування процесу шифрування і дешифрування файлу може використовуватися одне ключове слово або одна ключова фраза, заздалегідь відома обом сторонам, що обмінюються інформацією. Наприклад, під час Другої світової війни підводні човни і морські судна обмінювалися повідомленнями по відкритих каналах радіозв'язку з використанням технології шифрування повідомлень. На самому початку, в процесі шифрування використовувався лише один ключ. Шляхом аналізу моделей коду, криптологи Альянсу іноді

могли вирахувати ключове слово або модель, що використовувалися в процесі шифрування, і, таким чином, таємно прочитати зашифровані повідомлення. В міру ускладнення методів шифрування процес злому коду вручну все більше складнішав.

Код шифрування еволюціонував в шифр, заснованому на механіко-машинному обчисленні, яке було ранньою формою комп'ютерних обчислень. У той час єдиним способом злому коду була крадіжка шифрувального апарату та використання для дешифрування повідомлень тих же самих інструментів, які використовувалися і для їх шифрування. Найважчим завданням було викрасти шифрувальний апарат і не бути спійманим при виконанні цього завдання. Якщо ворогові ставало відомим, що таємниця шифрувальної машини була порушена, він просто змінював використовуваний код (шифр) і оновлював з урахуванням цієї зміни вже функціонуючі шифрувальні апарати. Даний принцип все ще практикується й сьогодні - найефективнішою кібератакою є та, яка не була виявлена.

З появою комп'ютерних технологій і настанням часів Холодної війни процес шифрування став більш складним, проте швидкість роботи комп'ютерів, що використовуються в процесі злому кодів шифрування, також збільшилася. На кожній стадії розвитку процесу безпечного зв'язку, технології та практичні навички шифрування інформації і можливості по злому коду шифрування розвивалися практично паралельно один одному, з однією та тією ж швидкістю. Важливий наступний крок у розвитку технологій шифрування був зроблений в 70-х роках, коли була представлена інноваційна технологія шифрування подвійним ключем; цей принцип використовується і по сьогодні. Одним з найбільш відомих методів шифрування подвійним ключем є використання криптосистеми відкритого ключа RSA-кодування - методу, названого за першими літерами імен його розробників: Rivest, Shamir і Adleman. Незважаючи на те, що в розвитку зазначеного методу офіційно визнані заслуги лише зазначених розробників, багато хто з їхніх сучасників незалежно від них також прийшли до використання подібного методу. Метод RSA використовує два криптографічних ключі, в основі яких лежать два великих простих числа, які не розголошуються публічно. Один з алгоритмів використовується для перетворення зазначених двох простих чисел в ключ шифрування, який в цьому документі позначається як E-key; інший математичний алгоритм використовується для перетворення тих же двох таємних простих чисел в таємний ключ дешифрування, який в даному документі позначається також як D-key. Користувач системи RSA, який вибрав таємні прості числа (в даному документі позначається як "власник ключа"), поширює, або "публікує" даний ключ E-key, згенерований з використанням відповідного алгоритму і має розмір, який, як правило, варіюється від 1024 біт до 4096 біт, всім, хто бажає зашифрувати свій файл. У зв'язку з тим, що цей ключ відправляється багатьом користувачам в незашифрованому вигляді, ключ E-key відомий під назвою "відкритого ключа".

Сторони, які бажають підтримувати зв'язок з власником ключа, потім використовують вказаний відкритий ключ E-key в поєднанні з доступним алгоритмом, що знаходяться у відкритому доступі, який, як правило, пропонується в формі комерційного програмного забезпечення, в процесі здійснення шифрування будь-якого файлу, який передбачається переслати конкретному власнику ключа. При отриманні зашифрованого файлу власник ключа використовує таємний ключ D-key для дешифрування зазначеного файлу; в процесі даної дії файл перетворюється в звичайний незашифрований текст. Унікальністю методу подвійного ключа, в загальному випадку, і, конкретно, алгоритму RSA є той факт, що відкритий ключ E-key, який використовується для шифрування файлу, не може використовуватися для дешифрування. Для дешифрування може бути використаний тільки таємний ключ D-key, яким володіє власник ключа.

Концепція використання подвійного ключа, роздільного ключа або "множинного" ключа для шифрування і дешифрування файлів не обмежується методом RSA або будь-яким іншим алгоритмічним методом, але, з методологічної точки зору, описує метод здійснення зв'язку в якості певної послідовності кроків. Наприклад, при обміну двома ключами під час процедури обміну інформацією засобами мережі з комутованими пакетами даних пристрій, наприклад, ноутбук, який "хоче" отримати захищений файл з стільникового телефону, спочатку генерує два ключі - ключ E-key для шифрування і ключ D-key для дешифрування, з використанням конкретного алгоритму. Ноутбук потім пересилає ключ E-key на стільниковий телефон з використанням громадської мережі, через яку передається IP-пакет. Процес пересилання IP-пакета, очевидно, ілюструє використання незашифрованої форми, MAC-адреси, IP-адреси джерела (NB) і адреси порту ноутбука, а також IP-адреси одержувача (CP), порту стільникового телефону та протоколу передачі даних TCP, а також зашифрованої копії ключа E-key в якості свого корисного навантаження.

Використовуючи заздалегідь узгоджений алгоритм шифрування або програмний пакет, стільниковий телефон потім обробляє незашифрований текстовий файл з використанням алгоритму шифрування і ключа шифрування E-key, що дає на виході зашифрований файл, а саме, зашифрований текст, який передається в якості корисного навантаження IP-пакета в процесі захищеної передачі даних з мобільного телефону на ноутбук. При отриманні IP-пакета, для дешифрування файлу з використанням секретного ключа дешифрування (наприклад, ключа D-key) використано алгоритм. Так як забезпечується узгодження ключа D-key з ключем E-key, то, по суті, при роботі алгоритму для дешифрування зашифрованого тексту використовується інформація про обидва ключі; в процесі забезпечується створення незашифрованого звичайного тексту. У той час як корисне навантаження IP-пакета захищене в формі зашифрованого файлу (тобто, зашифрованого тексту), інша частина IP-пакета і раніше пересилається в незашифрованій формі (що відкриває можливість її перехоплення), відкритої до прочитання будь-яким кіберзлочинцем, включаючи інформацію про IP-адресу джерела (CP) та номер порту, а також про IP-адресу одержувача (NB) та пов'язаному номера порту. Отже, навіть якщо корисне завантаження саме по собі і не може бути відкрито, інші складові процесу обміну інформацією як і раніше можуть відслідковуватися.

Віртуальні приватні мережі - Іншим методом забезпечення безпеки, також заснованим на використанні процедури шифрування, є використання так званої віртуальної приватної мережі, або VPN (Virtual Private Network). При використанні VPN в мережі, де відбувається передача зашифрованих IP-пакетів, формується" тунель "або" безпечний канал". При використанні VPN шифрується не тільки корисне навантаження, але також і вміст всього IP-пакета, який потім "вбудовується" в інший незашифрований IP-пакет, виконуючи функцію "переносника" даних, за допомогою якого інкапсульований пакет передається від одного шлюзу VPN до іншого. Спочатку, віртуальні приватні мережі використовувалися для об'єднання нерівноправних локальних мереж в одне ціле на великій відстані - наприклад, коли компанії-власники приватних мереж в Нью-Йорку, Лос-Анджелесі і Токіо хотіли об'єднати свої різні локальні мережі в одну з використанням такої ж функціональності, як нібито це була одна глобальна приватна мережа.

Основний принцип роботи віртуальних приватних мереж можна представити як зашифрований зв'язок між двома пристроями, де, наприклад один сервер, будучи частиною однієї локальної мережі, яка підтримує певну кількість пристроїв в бездротовому режимі з використанням радіо з'єднань та в дротовому режимі з використанням з'єднань, з'єднується за допомогою "віртуальної приватної мережі" (VPN), що складається з контенту і VPN-тунелю, та другий сервер, який має провідні з'єднання зі стаціонарними комп'ютерами, ноутбуком, а також з базовою станцією Wi-Fi. На додаток до вказаного з'єднання, що характеризується відносно низькою пропускною здатністю, сервер з'єднаний також з суперкомп'ютером за допомогою високошвидкісного з'єднання. В результаті обмін даними складається з послідовності пакетів даних, що містять внутрішній пакет VPN, вбудований в зовнішній IP-пакет. У процесі функціонування даної системи, зовнішній IP-пакет з сервера (із зазначенням IP-адреси джерела і номера порту) відсилається на сервер з IP-адресою одержувача і номером порту. Зазначений зовнішній IP-пакет описує процес формування серверами і зашифрованого "тунелю" передачі даних між ними в прямому та зворотному напрямку. Корисне навантаження VPN зовнішнього пакета містить в своєму складі IP-пакет "останньої милі", що забезпечує безпосередній обмін інформацією між настільним комп'ютером з IP-адресою джерела DT та відповідним спеціально створеним для цієї мети портом, а також ноутбуком з IP-адресою джерела NB та відповідним спеціально створеним для цієї мети портом; зазначений пакет несе в собі запит на передачу файлів.

Для того щоб здійснити зазначену передачу даних в безпечному режимі з використанням віртуальної приватної мережі, створюється тунель VPN, та ініціюється сесія ще до того, як сталася фактична передача даних. При використанні в корпоративному середовищі, тунель не надсилається через Інтернет з використанням спеціально створених для цього портів, але, в загальному випадку, пересилається з використанням спеціально виділеного провайдера Інтернет-послуг або провайдера пов'язаних послуг, що має в своєму розпорядженні власний волоконно-оптичний кабель і мережу апаратних засобів. Провайдер послуг часто укладає з компанією щорічні або довгострокові контакти, за умовами яких гарантується певна пропускна здатність VPN-серверів за певну плату. В ідеальному випадку вказаний виділений високошвидкісний канал зв'язку використовується для прямого з'єднання серверів без проміжних з'єднань (або "з'єднань останньої милі"), застосування яких могло б негативно відбитися на швидкості передачі даних через віртуальну приватну мережу, якість надаваних послуг або безпеки переданих даних.

На практиці, використання традиційних віртуальних приватних мереж вимагає наявності двоступеневого процесу – на першій стадії створюється віртуальна приватна мережа або здійснюється "вхід" до неї, а на другому – відбувається передача даних всередині безпечного каналу, або "тунелю". Концепція тунелювання, де зовнішні IP-пакети переносяться 7-рівневими стеками (використовуваними для здійснення VPN-з 'єднання), що складаються з рівнів 1-4, де рівень 5 використовується для створення віртуальної VP сесії, а рівень 6, презентаційний рівень, використовується для шифрування, необхідного для формування каналу V. Тоді як VPN-з'єднання використовує Інтернет протокол для надсилання IP-пакетів, фізичний рівень1 і канальний рівень VPN часто підтримується окремим оператором для мінімізації непередбачуваності маршрутизації. Наприклад, дані прикладного рівня 7, що передаються від "пристрою до пристрою" між взаємодіючими стаціонарними комп'ютерами, передаються у вигляді тунельних даних, включаючи всі сім рівнів OSI, необхідних для встановлення зв'язку, так ніби б VPN і не було. Таким чином, VPN можна уявити собі як протокол зв'язку, що працює на сьомому рівні, що використовується для передачі внутрішніх пакетів VPN.

У процесі функціонування зовнішній IP-пакет зі стека передачі даних передається з одного комунікаційного стека в інший, для виявлення інкапсульованих даних – істинного вмісту пакета. Таким чином, наскрізне з'єднання відбувається без знання деталей, що використовуються для створення VPN тунелю, за винятком того, що VPN тунель повинен бути сформований заздалегідь до будь-якої спроби з'єднання і повинен бути закритий після завершення розмови. Неможливість відкрити VPN тунель насамперед призведе до незашифрованої передачі IP пакета, чутливого до прослуховування, захоплення, зараження тощо. Незакриття VPN після завершення розмови може надати кіберзлочинцеві можливість приховати свою незаконну діяльність у чужому VPN тунелі і, в разі перехоплення, може призвести до пред'явлення можливих кримінальних звинувачень невинній особі.

У той час як використання віртуальних приватних мереж є звичайним способом забезпечення з'єднання множинних приватних локальних мереж одну з одною з використанням приватних з'єднань з виділеною пропускною здатністю і шириною пропускання, використання віртуальних приватних мереж у складі громадських мереж та Інтернету є проблематичним при спілкуванні між двома зацікавленими сторонами. Однією з проблем використання віртуальних приватних мереж є те, що VPN-з'єднання має бути встановлено заздалегідь, ще до того, як воно може бути використано, а не на основі взаємного обміну пакетами даних. Наприклад, при виклику за протоколом VoIP, реалізованим засобами мережі з пакетною комутацією даних, перед тим, як стільниковий телефон зможе зв'язатися з передбачуваним одержувачем виклику на другому стільниковому телефоні, він повинен спочатку встановити сеанс VPN. Для цього на мобільний телефон викликаючого абонента спочатку має бути завантажено додаток VPN з'єднання. Потім абонент повинен відправити IP-пакети на вузол VPN, зазвичай це постачальник послуг. Ці пакети передаються по будь-якій доступній маршрутизації "Останньої Милі", наприклад, радіозв'язку з мобільного телефону на найближчу базову станцію Wi-Fi, за нею слідує дротовий зв'язок з локальним маршрутизатором, а потім дротовий зв'язок з вузлом VPN. Як тільки сеанс між мобільним телефоном викликаючого абонента і вузлом VPN встановлено, стільниковий телефон абонента повинен потім проінструктувати вузол VPN про створення VPN тунелю від стільникового телефону викликаючого абонента до вузла VPN. Ця частина VPN тунелю спрощується як сеанс 5-го рівня з тунелем, зашифрованим за допомогою 6-го рівня.

Після встановлення VPN з'єднання мобільний телефон абонента може здійснити виклик через будь-який додаток для VoIP-телефонії на будь який інший телефон. Якщо телефон, що викликається, не підключений до однієї і тієї ж VPN, при виконанні даної інструкції додаток повинен встановити з'єднання "виклику" з використанням систем "останньої милі" між VPN-хостом і стільниковим телефоном. Якщо VoIP-додаток не може цього зробити або не має відповідних прав на проведення подібних дій, дзвінок не відбудеться – він буде негайно перерваний. В іншому випадку внутрішній IP-пакет встановить сеанс зв'язку Рівня 5 додатка між стільниковим телефоном і стільниковим телефоном-адресатом, а також підтвердить той факт, що тестові IP-пакети належним чином дешифровані і розбірливі.

Для того щоб здійснити дзвінок, дзвінок обов'язково повинен бути ініційований Рівнем 7 додатка, що працює на телефоні абонента, а не звичайними телефонними функціями набору номера, оскільки SIM-карта провайдера послуг телефонії, встановлена в телефоні, не сумісна з функціями VPN-тунелю. Як тільки виклик буде здійснено, стільниковий телефон передаватиме послідовність IP-пакетів, що являє собою малі фрагменти (або "уривки") голосової інформації, відібрані відповідно до встановленого на телефоні додатка зв'язку. Ці пакети відправляються з додатка в мобільному телефоні абонента, що викликає абонента через мережу, наприклад, по

Wi-Fi каналу до найближчої базової станції Wi-Fi, потім через дротове з'єднання до маршрутизатора і, нарешті, через дротове з'єднання до вузла VPN. Потім дані безпечно передаються на вузол VPN через VPN тунель на кінцевий пристрій VPN мережі, цільовий VPN шлюз. У цьому прикладі VPN тунель не простягається до стільникового телефону одержувача, а замість цього перестає викликатися пристрій. За шлюзом призначення VPN дані більше не шифруються, оскільки оператор VPN більше не використовується. Для пакетів даних, що виходять з VPN тунелю, хост VPN вводить дані, що передаються за останньою милею з'єднання пристрою призначення, наприклад, дротове з'єднання з найближчим маршрутизатором, потім дротове з'єднання з місцевою системою стільникового зв'язку і станцією, передаючи виклик як звичайний стільниковий виклик за допомогою 2G, 3G або 4G. Процес виклику з програми для мобільного телефону на телефон, на якому не запущено той же додаток, називається функцією "call out".

Вищенаведений приклад підкреслює ще одну проблему з підключенням до VPN по публічній мережі – з 'єднання останньої милі від вузла VPN до викликаного абонента не є частиною VPN, і тому не гарантує безпеку, продуктивність або QoS. Зокрема, остання миля викликаючого абонента, що містить з 'єднання, відкрита для прослуховування і схильна до кібератак. Як тільки виклик завершено, VPN з'єднання має бути перервано, при цьому Рівень 5 VPN подає команду на закриття VPN сеансу і стільниковий телефон абонента відключається від вузла VPN.

Адаптація віртуальної приватної мережі -технології початково створеної для передачі даних між комп'ютерами, - стикається з низкою серйозних проблем.

- Остання миля зв'язку між VPN-шлюзом і мобільним телефоном призначення не захищена і перебуває під загрозою прослуховування і спостереження.

- Остання миля зв'язку між мобільним телефоном викликаючого абонента і шлюзом VPN безпечна тільки в тому випадку, якщо викликаючий абонент використовує додаток, заснований на передачі даних. Якщо абонент підключається до шлюзу VPN по телефонній лінії, тобто підключається до функції, то зв'язок з мобільного телефону викликаючого абонента до найближчого шлюзу VPN не безпечний і схильний до ризику прослуховування і спостереження.

- Безпека виклику може бути забезпечена тільки в тому випадку, якщо обидва абоненти використовують передачу даних, а не телефонний зв'язок по лінії останньої милі і знають, що перед початком виклику обидві сторони повинні підключитися до однієї і тієї ж VPN.

Останній параграф підкреслює парадокс безпечного VPN зв'язку – викликаний абонент повинен знати, що йому дзвонять, перш ніж він буде викликаний, щоб приєднатися до мережі. Для того, щоб повідомити людині про те, що їй необхідно зателефонувати, необхідно спочатку зв'язатися з ним і проінструктувати його увійти в VPN, перш ніж він зможе почати дзвінок. По суті, він повинен отримати незахищений телефонний дзвінок для підключення до захищеного телефонного дзвінка. Незахищений телефонний дзвінок легко скомпрометувати і прослухати. Крім того, метадані незахищеного виклику показують, хто і кому дзвонить і в який час. Метадані виклику надзвичайно корисні для відстеження активності людини або для її профілювання в якості мети злочинців.

Навіть якщо всі зазначені інструкції були виконані, все одно немає гарантії того, що спроба здійснення телефонного дзвінка або пересилання документів через віртуальну приватну мережу не опиниться безуспішною з кількох причин, включаючи наступні:

- Затримка передачі даних у віртуальній приватній мережі може виявитися занадто великою, що унеможливить роботу додатків в режимі реального часу, передачу голосу по IP-протоколу або передачу потокового відео;

- Затримка передачі даних в з'єднанні "останньої милі" віртуальної приватної мережі абонента, який телефонує абонентом і шлюзом VPN або між шлюзом VPN і адресатом телефонного дзвінка може виявитися занадто великою, що унеможливить роботу додатків в режимі реального часу, передачу голосу по IP-протоколу або передачу потокового відео;

- Найближчий до викликаючого абонента або до абонента-адресата шлюз VPN (тобто, з'єднання "останньої милі") може виявитися розташованим на занадто великій відстані – можливо, навіть більше за відстань до абонента-адресата, без використання VPN, що призведе до значної затримки передачі даних всередині з'єднання, нестабільної роботи мережі, неконтрольованої маршрутизації з використанням невідомих мереж, варіюванню якості обслуговування та численним можливостям для здійснення атаки "людина посередині" з використанням незахищених сегментів з'єднання;

- З'єднання "останньої милі" віртуальної приватної мережі між шлюзом VPN і абонентом-адресатом виклику може не підтримувати функцію "зовнішнього" виклику та передачі пакетів, або ж не підтримувати з'єднання з місцевими телефонними компаніями;

- Місцеві провайдери послуг або урядові цензори можуть блокувати виклики, які надходять від невідомих шлюзів VPN, або ж процес встановлення з'єднання з такими шлюзами з причин, пов'язаних з необхідністю забезпечення національної безпеки або відповідності нормам законодавства;

- При використанні корпоративних віртуальних приватних мереж можливість здійснення викликів з використанням функціональності технології VoIP може надаватися тільки співробітникам компанії або чітко визначеним уповноваженим категоріям користувачів; процеси проведення фінансових транзакцій або перегляду онлайн-відео можуть бути заблоковані; можуть бути заблоковані сервери передачі приватних поштових повідомлень в публічну мережу, такі як, наприклад, Yahoo, Google і т.д.; а також може бути заблокований доступ до численних веб-сайтів, таким як YouTube, програмам онлайн-чатів, або ж, наприклад, сервісу Twitter - відповідно до політики компанії;

- У разі нестабільної роботи мереж, віртуальна приватна мережа по завершенні дзвінка може залишитися у відкритому стані, що виразиться в підтримці поточної розмови в безперервному режимі з виходом на пристрій абонента до тих пір, поки не буде здійснено скид з'єднання VPN-провайдером в ручному режимі. Це може привести до втрати частини пропускної здатності при здійсненні подальших дзвінків або ж до необхідності виплати великих сум за тарифами за незакрите з'єднання.

Порівняння мереж - порівняння комунікацій, пропонованих "over-the top" або OTT-провайдерами, з системами зв'язку, що використовують загальнодоступні мережі для підключення до спеціального VPN, швидко виявляє, що крім самого VPN-зв'язку, більшість обох систем зв'язку мають майже ідентичні компоненти та з'єднання. Зокрема, "остання миля" абонента, що має стільниковий телефон, радіозв'язок Wi-Fi, базову станцію Wi-Fi, дротяні з'єднання і маршрутизатор, являють собою той самий зв'язок "останньої милі" в обох реалізаціях. Аналогічно, на "останній милі" іншого боку, стільниковий телефон, з'єднання стільникового телефону, базова станція стільникового зв'язку та вишка, дротяні з'єднання і маршрутизатор ідентичні для версій Інтернету і VPN. Основна відмінність полягає в тому, що в загальнодоступній мережі VPN-тунель з захищеним зв'язком між VPN-вузлами і замінюється серверами/маршрутизаторами, що забезпечують небезпечне комунікаційне з'єднання. Інша відмінність полягає в зв'язку OTT, виклик доступний миттєво, як описано в інструкції, де для використання VPN необхідні додаткові інструкції і для настройки VPN та завершення сеансу VPN перед наступним викликом.

В обох прикладах з'єднання "останньої милі" пропонують непередбачувану якість послуг зв'язку, можливість перехоплення пакетів і ризик кібератак. Оскільки сервери/маршрутизатори, ймовірно, управляються різними провайдерами в різних локальних мережах, можна інтерпретувати сервери як існуючі різні хмари, тобто хмари. Наприклад, публічно відкриті мережі, що належать і керовані Google, Yahoo, Amazon і Microsoft, можуть розглядатися як різні хмари, наприклад, "хмара Amazon", хоча всі вони пов'язані Інтернетом.

Конкуруюча мережева топологія, однорангова мережа або PPN включає мережу, що складається з великого числа тимчасових вузлів з маршрутизацією пакетів, керованих PPN, а не маршрутизатором або провайдером. У той час як однорангові мережі існували на апаратних засобах протягом десятиліть, саме Napster популяризував цю концепцію як засіб уникнути контролю, витрат і регулювання Інтернет-провайдерів. Зазнаючи переслідувань в судовому порядку з боку урядових органів США за порушення авторських прав на музику, засновники Napster були змушені оголосити про банкрутство компанії; в цей же час, OTT-оператор Skype тільки починав розвиватися. Пізніше, мережа Skype відійшла від традиційної OTT моделі мережі до пірингової, запропонованої компанією Napster.

У PPN-комутації кожен пристрій, який підключається для входу в PPN, стає ще одним вузлом в PPN. Наприклад, якщо в мережі з топологією стільниковий телефон з встановленим ПЗ PPN реєструється в тимчасовій мережі, він, як і всі інші підключені пристрої в регіоні, стає частиною мережі. Виклики, що видаються будь-якими пристроями, переходять з одного пристрою на інший, щоб дістатися до пункту призначення, іншого пристрою, підключеного до PPN. Наприклад, якщо в мережі з топологією стільниковий телефон використовує своє з'єднання PPN для виклику іншого пристрою з підключеним PPN, наприклад, стільникового телефону, виклик слідує обхідним шляхом через будь-який пристрій (пристрої), фізично розташований в PPN між цими двома пристроями. Виклик, що виходить від стільникового телефону з'єднується Wi-Fi через базову станцію Wi-Fi з настільним комп'ютером, потім з ноутбуком, зі стаціонарним комп'ютером, потім зі стаціонарним комп'ютером і, нарешті, з стільниковим телефоном через базову станцію стільникового телефону та вишку. Таким чином, вся маршрутизація контролюється PPN, а Інтернет не бере участі в управлінні маршрутизацією.

Оскільки задіяні обидві сторони, ПЗ PPN, що використовується для підключення до мережі, також виступає в якості додатку для голосового зв'язку на основі технології VoIP.

У разі, коли стільниковий телефон намагається викликати стільниковий телефон з пристроєм не на основі PPN на протилежному кінці землі, маршрутизація повинна обов'язково включати передачу даних через Інтернет, використовуючи точки доступу, особливо при передачі пакетів через океани або гірські хребти. Перша частина маршрутизації в мережі з топологією протікає аналогічно до попереднього прикладу, починаючи з стільникового телефону та проводить маршрут через базову станцію Wi-Fi, настільний комп'ютер, ноутбук, настільні комп'ютери. На цей момент, якщо ноутбук підключений до мережі, виклик буде прокладений через нього, в іншому випадку виклик повинен бути направлений через базову станцію стільникового телефону та вишку на стільниковий телефон, а потім повернутий назад до базової станції стільникового телефону та вишки перед подальшою відправкою.

Якщо виклик перетинає Тихий океан, тоді комп'ютери та стільникові телефони не можуть переносити трафік через океан, тому дзвінок потім обов'язково маршрутизується в Інтернет на сторонній сервер/маршрутизатор в хмарі і далі за допомогою бездротової технології на сторонній сервер/маршрутизатор в хмарі. Потім виклик виходить з Інтернету та входить в PPN в мережі з топологією спочатку через стаціонарний комп'ютер, який, в свою чергу, підключається до Wi-Fi, до ноутбука і до базової станції. Оскільки Wi-Fi не працює з програмним забезпеченням PPN додатка, фактичний пакет, що входить в Wi-Fi, повинен відправитися на планшет або стільниковий телефон і назад на Wi-Fi, перш ніж вирушати на базову станцію стільникового телефону та вишку через дротове з'єднання. Нарешті, виклик стільникового телефону підключається до стільникового телефону, який не є пристроєм з підтримкою PPN. Таким чином, з'єднання є "викликом" для PPN, оскільки воно виходить з мережі з топологією PPN. Використовуючи цей підхід PPN, VPN спочатку реєструє зухвалий пристрій в мережі PPN згідно з інструкцією, виконавши авторизацію PPN. Після цього виклик може бути виконаний через додаток PPN згідно з інструкцією. Перевага такої пірингової мережі в тому, що для передачі виклику на великі відстані необхідності в додатковому обладнанні немає, і, так як кожен пристрій, підключений до PPN, регулярно оновлює свій статус, завантаження та затримку, провайдер PPN може керувати маршрутизацією пакета для мінімізації затримки.

Недоліки такого підходу в тому, що пакети перетинають мережу, що містить безліч невідомих вузлів, що представляють потенційну загрозу безпеці і мають непередбачуваний вплив на затримку і якість обслуговування викликів. Таким чином, за винятком Skype, однорангові мережі, що працюють на Рівні 3 та вище, як правило, не використовуються в мережах зв'язку з комутацією пакетів.

Загальне порівняння провайдерів спеціальних VPN, Інтернет-провайдерів OTT та тимчасових мереж PPN наведене нижче.

Мережа	Віртуальна приватна мережа VPN	OTT Мережа	Однорангова мережа PPN
Вузли	Публічні/ Хост-сервера	Публічні маршрутизатори/сервери	Користувачі PPN
Пропускна спроможність вузла	Відома інфраструктура	Відома інфраструктура	Змішана, невідома
Хмарна пропускна здатність	Гарантована	Непередбачувана	Непередбачувана
Пропускна здатність "останньої милі"	Залежить від провайдера	Залежить від провайдера	Залежить від PPN
Затримка	Некерована	Некерована	Оптимальний варіант
Стабільність мережі	Некерована	Некерована, надлишкова	Оптимальний варіант
Налаштування виклику	Комплексний вхід	Не вимагається	Авторизація
Ідентифікація користувача	Ім'я користувача	Номер телефону	Ім'я користувача
Якість обслуговування технології VoIP	Від змінного до хорошого	Змінна	Змінна
Хмарна безпека	Шифрується тільки корисне	Незашифрована	Незашифрована

Мережа	Віртуальна приватна мережа VPN	OTT Мережа	Однорангова мережа PPN
	навантаження		
Захист "останньої милі"	Незашифрована	Незашифрована	Незашифрована
Схильність до перехоплення	Заголовок пакета (Хмара) Весь пакет (Остання миля)	Весь пакет	Весь пакет

В той час як VPN та Інтернет мають фіксовану інфраструктуру, вузли тимчасової мережі розрізняються залежно від того, хто зареєстрований і які пристрої підключені до PPN. Хмарна пропускна здатність, представлена в контексті цієї таблиці як високошвидкісні міжміські з'єднання мереж, наприклад, мережі, які перетинають океани і гірські ланцюги, гарантується за контрактом тільки в разі VPN, в іншому разі – вона непередбачувана. Пропускна здатність "останньої милі" - це локальний провайдер, що залежить як від Інтернет-провайдерів, так і від VPN, але для PPN повністю залежить від того, хто увійшов в систему.

Затримка поширення послідовних IP-пакетів некерована для OTT і VPN, оскільки провайдер не контролює маршрутизацію в "останньої милі", але замість цього залежить від місцевих телефонних операторів або інтернет-провайдерів, тоді як PPN мають обмежені можливості, використовуючи оптимальні варіанти для прямого трафіку між вузлами, які в даний момент знаходяться в мережі в певній географії. Аналогічно, для стійкості мережі, PPN мають можливість перенаправляти трафік, щоб підтримувати мережу, але повністю залежать від того, хто входить в систему. Інтернет, з іншого боку, є внутрішньо надлишковим і майже впевнено гарантує доставку, але не обов'язково своєчасну. Стійкість мережі для спеціального VPN залежить від кількості вузлів, дозволених для підключення до хосту VPN. Якщо ці вузли відключені, VPN буде непридатний.

З точки зору налаштування виклику Інтернет завжди доступний, PPN вимагають додаткової інструкції для входу в PPN до здійснення дзвінка, а VPN можуть включати складну процедуру входу в систему. Більш того, більшість користувачів вважають використання OTT телефонних номерів, а не окремих ідентифікаторів входу, використовуваними VPN і PPN, в якості важливого переваги для простоти користування. Всі перераховані три мережі страждають від нестійкої якості технології VoIP, в цілому відстаючи від комерційних операторів зв'язку. З точки зору безпеки всі три варіанти не можуть виступати в якості з'єднань "останній милі", так як схильні до перехоплення пакетів з відкритими адресами і корисними навантаженнями. VPN забезпечують шифрування хмарного з'єднання, але все ж надають IP-адреси хостів VPN. Таким чином, ніяка мережева опція не вважається безпечною. Таким чином, шифрування використовується різними додатками для запобігання злому і кібератакам, або як протокол Рівня 6, або як впроваджена частина Прикладного рівня 7.

Надмірна довіра до шифрування. Незалежно від того, чи використовується вона для шифрування IP-пакетів або створення VPN, сьогоднішня мережева безпека залежить майже виключно від шифрування і являє собою одну слабку сторону в сучасних мережах зв'язку на основі пакетної комутації. Наприклад, було проведено безліч досліджень по методам здійснення атак на шифрування RSA. Хоча обмеження простих чисел на великі розміри значно знижує ризик "злому" коду D-ключа дешифрування з використанням методів "грубої сили", методи поліноміального коефіцієнта успішно продемонстрували злом ключів на основі менших простих чисел. Існують побоювання, що еволюція "квантових обчислень" в кінцевому підсумку призведе до практичних методів "злому" ключів RSA і інших ключів шифрування при кібератаці. Для боротьби з постійно присутнім ризиком "злому" коду з'явилися нові алгоритми і методи шифрування "більшого ключа", такі як "покращений стандарт шифрування" або шифрування AES, затверджений US NIST в 2001 році. Принцип проектування, заснований на шифрі Rijndael, відомому як підстановочно-перестановочна мережа, поєднує в собі як заміну символів, так і перестановку з використанням різних розмірів ключа і блоку. У своєму нинішньому втіленні алгоритм містить фіксовані розміри блоків 128 біт з ключами, що включають в себе різні довжини 128 біт, 192 біта і 256 біт, з відповідною кількістю повторень, використовуваних при перетворенні вхідного файлу, що варіюються в круглих числах в 10, 12, і 14 ступенях відповідно. У практичному плані шифр AES можна ефективно і швидко виконувати як в програмному, так і в апаратному забезпеченні для будь-якого розміру ключа. У криптографічній мові шифрування на основі AES з використанням ключа 256b називається "шифруванням AES256". Також є шифрування AES512 з використанням ключа 512b.

У той час як кожне нове покоління піднімає планку криптографії, щоб зробити кращими методи шифрування, зацікавлені в прибутку кіберзлочинці, щоб швидше "зламати" ці методи, часто концентруються на своїх цілях, замість того, щоб використовувати обчислення для злому зашифрованого файлу. Як описано раніше, використовуючи перехоплення пакетів і опитування портів, кіберпірат може отримати цінну інформацію про розмову, корпоративний сервер або навіть VPN-шлюз. Замість атаки на мережу, кібераналіз дозволяє атакувати персональні комп'ютери, ноутбуки і мобільні телефони Головного або Фінансового директора компанії. Як тільки співробітники компанії переходять по посиланню, що вкладене в електронні листи, автоматично встановлюється шкідливе і шпигунське ПЗ, яке повністю обходить захист брандмауера, оскільки таким чином шкідливі програми отримують доступ "зсередини".

Імовірність злому шифру також збільшується, якщо дані переміщаються по мережі без зміни, тобто статично. Наприклад, в мережі на Рис. 1 базові дані в пакетах 790, 792, 794 і 799 залишаються незмінними в міру того, як пакети переміщаються по мережі. Кожен показаний пакет даних містить послідовність даних або звуку, розташованих послідовно за часом або сторінок, незмінених від вихідного порядку, коли він був створений. Якщо вміст пакета даних є текстовим, читання незашифрованого текстового файлу в послідовності 1A-1B-1C-1D-1E-1F призведе до "розбірливому" тексту для комюніке номер "1". Якщо вміст пакета даних являє собою аудіо, перетворення, тобто "відтворення", незашифрованого текстового файлу в послідовності 1A-1B-1C-1D-1E-1F через відповідний аудіокодек, по суті, заснований на програмному забезпеченні ЦАП, призведе до звуку для номера звукового файлу номер "1".

У будь-якому випадку, в розглядуваному описі, кожен інтервал даних, представлений блоками фіксованого розміру, містить задану кількість біт, наприклад, два байта (2B). Точна кількість біт на кожен інтервал є гнучким тільки в тому випадку, якщо кожен вузол зв'язку в мережі знає, який розмір кожного інформаційного інтервалу. У кожному інтервалі даних містяться аудіо-, відео- або текстові дані, зазначені на кресленнях як число, за яким слідує буква. Наприклад, як показано на рисунку, перший інтервал пакету 790 даних містить контент 1A, де число "1" вказує конкретний зв'язок №1, а буква "A" представляє першу частину даних в повідомленні №1. Аналогічно, другий інтервал пакету 790 даних містить вміст 1B, де число "1" вказує, що воно є частиною одного та того ж повідомлення №1, а буква "B" представляє другу частину даних в повідомленні №1, послідовно дотримуючись за 1A.

Якщо, наприклад, один та той же пакет даних імовірно включає в себе контент "2A", дані представляють перший пакет "A" в іншому повідомленні, зокрема для зв'язку №2, не пов'язаного з повідомленням №1. Пакети даних, що містять однорідні повідомлення, наприклад, де всі дані для зв'язку №1 легше аналізувати та читати, ніж ті, які змішують різні повідомлення. Дані, впорядковані послідовно в правильному порядку, дозволяють кіберзлочинцю інтерпретувати природу даних, будь то аудіо, текст, графіка, фотографії, відео, виконуваний код і т.д.

Більш того, в показаному прикладі, оскільки IP-адреси джерела та призначення пакета залишаються постійними, тобто коли пакети залишаються незміненими під час транспортування по мережі в тій же формі, що і дані, що входять або виходять з шлюзових серверів 21A і 21F, оскільки базові дані не змінюються, у хакера більше шансів перехопити пакети даних і отримати більше шансів проаналізувати та відкрити файли або прослухати розмову. Проста транспортна і одномірна безпека, тобто така, що покладається тільки на шифрування для захисту, збільшує ризик кібератаки, тому що ймовірність успіху вище при такому надмірно простому використанні Інтернету в якості мережі з комутацією пакетів.

Захист мереж реального часу і мережевих пристроїв

Для того, щоб поліпшити якість обслуговування телефонії, відео та передачі даних, одночасно усуваючи безліч уразливих місць в системі безпеки, що створюють проблеми сучасним мережами з комутацією пакетів, необхідний новий та інноваційний системний підхід до управління маршрутизацією IP-пакетів, який управляє глобальною мережею, яка включає розрізнені технології і одночасно сприяє наскрізній безпеці. Завдання такої інноваційної мережі з комутацією пакетів включають такі критерії:

1. Забезпечити безпеку і якість обслуговування глобальної мережі або провайдера послуг телекомунікації, включаючи динамічне управління маршрутизацією трафіку голосу, відео і даних в режимі реального часу в мережі;

2. Застрахувати безпеку і якість обслуговування "локальної мережі або телефонної компанії" в останній милі мережі зв'язку;

3. Забезпечити безпеку і якість обслуговування "останньої ланки" мережі зв'язку, включаючи забезпечення безпечного зв'язку, що проходить по незахищеним лініях;

4. Забезпечити безпеку комунікаційних пристроїв і автентифікувати користувачів для запобігання несанкціонованого або шахрайського доступу або використання;

5. Сприяти безпечному способу зберігання даних на пристрої, в онлайн, в мережі або в хмарному сховищі даних, щоб уникнути несанкціонованого доступу;

6. Забезпечити безпеку і конфіденційність всієї непублічної особистої інформації, включаючи всі фінансові, особисті, медичні і біометричні дані та записи;

7. Забезпечити безпеку і конфіденційність всіх фінансових транзакцій, пов'язаних з онлайн-банкінгом та покупками, кредитними картами і електронною оплатою; а також забезпечити безпеку, конфіденційність і анонімність в проведенні транзакцій і обміні інформацією при міжмашинній (M2M) і міжавтомобільній (V2V) взаємодіях, а також при обміні інформацією між автомобілем та транспортною інфраструктурою (V2X).

З вищевикладених цілей зміст винаходу, що приводиться в даному описі, відноситься до другої теми, описаної в пункті "безпека і якість обслуговування глобальної мережі або провайдера послуг телекомунікації в останній милі комунікаційної мережі". Дане питання можна розглядати як досягнення безпеки мережі або хмари без шкоди для експлуатаційних характеристик зв'язку в реальному часі.

Глосарій

Якщо контекст не вимагає іншого, терміни, використовувані в описі динамічної захищеної комунікаційної мережі та протоколу, мають таке значення:

Анонімні пакети даних: Пакети даних, що не містять інформації про початкового відправника або кінцевого одержувача.

Клієнт або клієнтський пристрій: Пристрій, зазвичай мобільний телефон, планшет, ноутбук, персональний комп'ютер або пристрій IoT, підключений до SDNP хмари по "Останній Милі".

Приховування: Процес кодування, при якому вміст SDNP-пакета або його частин стає недоступним для розпізнавання за допомогою будь якої послідовної комбінації операцій по забезпеченню безпеки, таких як шифрування, розділення, вставка "сміттєвих" даних і шифрування. Відновлення прихованих даних вимагає виконання антифункціональних процесів або декодування в зворотному порядку, наприклад, дешифрування, видалення "сміттєвих" даних, змішування і розпакування.

Дешифрування: Математична операція, яка використовується для перетворення пакетів даних з зашифрованого тексту в незашифрований текст.

Зберігання дезагрегованих даних: Процес фрагментації файлів даних і приховування їх вмісту перед зберіганням різних фрагментованих файлів на різних вузлах зберігання даних.

Сервер DMZ (англ. Demilitarized Zone - демілітаризована зона): Комп'ютерний сервер, недоступний безпосередньо з мережі SDNP (англ. Secure Dynamic Network And Protocol - динамічна захищена комунікаційна мережа та протокол) або Інтернету, який використовується для зберігання селекторів, генераторів початкових станів, генераторів ключів та інших спільних секретів.

Динамічне шифрування/дешифрування: Шифрування і дешифрування, засновані на ключах, які динамічно змінюються в міру проходження пакету даних через мережу SDNP.

Динамічне змішування: Процес змішування, коли алгоритми змішування (зворотні по відношенню до алгоритмів розділення) динамічно змінюються в залежності від початкового стану на основі стану, наприклад, часу, стану та зони, коли створюється змішаний пакет даних.

Динамічне скремблювання/дескремблювання: скремблювання та дескремблювання, засновані на алгоритмах, які динамічно змінюються в залежності від стану, наприклад, коли створюється пакет даних або зона, в якій він створюється.

Динамічне розділення: Процес розділення, коли алгоритми розділення динамічно змінюються в залежності від початкового стану на основі стану, наприклад, часу, стану та зони, коли пакет даних розділяється на кілька субпакетів.

Шифрування: Математична операція, яка використовується для перетворення пакетів даних з незашифрованого тексту в зашифрований текст.

Передача фрагментованих даних: Маршрутизація розділених та змішаних даних по мережі SDNP.

Видалення "сміттєвих" даних (або "видалення інформаційного сміття"): Видалення "сміттєвих" даних з пакетів даних для відновлення вихідних даних або відновлення початкової довжини пакета даних.

Вставка "сміттєвих" даних (або "вставка інформаційного сміття"): Навмисне введення в пакет даних беззмістовної інформації, або для ускладнення розуміння реального вмісту даних, або для управління довжиною пакета даних.

Ключ: Приховане цифрове значення, яке генерується шляхом введення стану, наприклад, часу, в генератор ключів, який генерує ключ по секретному алгоритму. Ключ використовується для вибору алгоритму для шифрування даних в пакеті з селектора. Ключ можна використовувати для безпечної передачі інформації про стан з публічних або незахищених лініях.

Сервер обміну ключами: Комп'ютерний сервер, часто належить сторонній організації і не залежить від оператора мережі SDNP, який розподіляє відкриті ключі для клієнтів і, при необхідності, для серверів, використовуючи симетричне шифрування, особливо при роботі з ключами, керованими клієнтом, тобто, на основі наскрізного шифрування клієнтом, щоб запобігти можливості шпигунства з боку оператора мережі.

Остання ланка: Мережеве з'єднання між пристроєм клієнта та першим пристроєм в мережі, з яким він обмінюється інформацією, як правило, це вишка радіозв'язку, маршрутизатор Wi-Fi, кабельний модем, телевізійна приставка або з'єднання Ethernet.

Остання миля: Мережеве з'єднання між шлюзом SDNP і клієнтом, включаючи останню ланку.

Змішування: Об'єднання даних з різних джерел та типів даних для створення одного довгого пакета даних (або ряду менших субпакетів) з нерозпізнаваним вмістом. У деяких випадках раніше розділені пакети даних змішуються для відновлення справжнього вмісту даних. Операція змішування може також включати в себе вставку та видалення "сміттєвих" даних та синтаксичний аналіз.

Синтаксичний аналіз: Числова операція, при якій пакет даних розбивається на більш короткі субпакети для зберігання або для передачі.

Скремблювання: Операція, в якій порядок або послідовність сегментів даних в пакеті даних змінюється по відношенню до його звичайного порядку і набуває нерозпізнаваної форми.

Розділення: Операція, в якій пакет даних (або кілька послідовних пакетів даних) розбивається на кілька субпакетів, які направляються декільком адресатам. Операція розділення також може включати в себе вставку та видалення "сміттєвих" даних.

Програмний комутатор: Програмне забезпечення, що містить виконуваний код, який виконує функції комутатора і маршрутизатора.

SDNP: Абревіатура (англ. Secure Dynamic Network and Protocol - Динамічна захищена комунікаційна мережа та протокол), що означає гіперзахищену мережу зв'язку, виконану відповідно до даного винаходу.

Сервер адміністрування SDNP: Комп'ютерний сервер, який розподіляє виконуваний код та спільні секрети по серверам SDNP в глобальному просторі або в певних зонах.

Мостовий вузол SDNP: Вузол SDNP, що з'єднує одну хмара SDNP з іншою, що мають різні зони і облікові дані безпеки.

Клієнт або клієнтський пристрій SDNP: Мережевий пристрій, зазвичай - стільниковий телефон, планшет, ноутбук, стаціонарний комп'ютер або пристрій IoT, що працює з додатком SDNP для підключення до хмари SDNP, зазвичай підключається на останній милі цієї мережі.

Хмара SDNP: Мережа взаємозалежних серверів SDNP, що запускають виконуваний код програмного комутатора для виконання операцій вузла зв'язку SDNP.

Шлюзовий вузол SDNP: Вузол SDNP, що з'єднує хмару SDNP з останньою милею SDNP і клієнтом. Шлюзові вузли SDNP вимагають доступу, щонайменше, до двох зон - до хмари SDNP і останньої милі.

Медіа-вузол SDNP: Виконавчий код програмного комутатора, який обробляє вхідні пакети даних з певними ідентифікаційними мітками відповідно до інструкцій сигнального сервера або іншого комп'ютера, що виконує сигнальну функцію, в тому числі шифрування/дешифрування, скремблювання/дескремблювання, змішування/розділення, тегів розмітки і генерування заголовків та підзаголовків SDNP. Медіа-вузол SDNP відповідає за ідентифікацію вхідних пакетів даних, що мають певні мітки, та за пересилку новостворених пакетів даних до наступного адресату.

Медіа-сервер SDNP: Комп'ютерний сервер, на якому розміщується програмний комутатор, який виконує функції медіа-вузла SDNP при двоканальному та триканальному зв'язках, а також виконує завдання вузла сигналізації SDNP та вузла сервера імен SDNP при одноканальному зв'язку.

Сервер імен SDNP: Комп'ютерний сервер, на якому розміщений програмний комутатор, який виконує функції вузла сервера імен SDNP при триканальному зв'язку.

Вузол сервера імен SDNP: Виконавчий код програмного комутатора, який управляє динамічним списком кожного пристрою SDNP, підключеного до хмари SDNP.

Мережа SDNP: Вся гіперзахищена мережа зв'язку, яка поширюється від клієнта до клієнта, в тому числі що охоплює ділянки зв'язку останньої ланки і останньої милі, а також хмара SDNP.

Вузол SDNP: вузол зв'язку SDNP, що містить програмний комутатор, який запускається на комп'ютерному сервері або на апаратному пристрої, підключеному до мережі SDNP, що функціонує як вузол SDNP - медіа-вузол, сигнальний вузол або вузол сервера імен.

Сервер SDNP: Комп'ютерний сервер, який представляє собою або медіа-сервер SDNP, або сигнальний сервер SDNP, або сервер імен SDNP і реалізує відповідні функції програмного комутатора для роботи в якості вузла SDNP.

Сигнальний вузол SDNP: Виконавчий код програмного комутатора, який ініціює виклик або зв'язок між сторонами, визначає всю або частину з декількох маршрутів для передачі фрагментованих даних на основі критеріїв абонента і динамічну таблицю затримок поширення між вузлами, а також формує команди для медіа-вузла SDNP, як управляти вхідними та вихідними пакетами даних.

Сигнальний сервер SDNP: Комп'ютерний сервер, на якому розміщується програмний комутатор, який виконує функції вузла сигналізації SDNP в двоканальній та триканальній системах зв'язку SDNP, та також виконує функції вузла сервера імен SDNP в двоканальних системах зв'язку.

SDNP тег: Вихідна адреса, поштовий індекс SDNP або будь-який інший код, який використовується для ідентифікації вхідного пакета даних або його субпакета.

Операція по забезпеченню безпеки: Процес зміни пакета даних для виконання приховування (або відновлення вмісту прихованого пакета) за допомогою залежних від стану облікових даних, що відносяться до зони і стану, в якому пакет створений.

Параметри безпеки: Цифрові значення, наприклад, початкові стани і ключі, які генеруються генераторами початкових станів або генераторами ключів по секретним алгоритмам в поєднанні з постійно змінюваним вхідним станом, наприклад, мережевим часом, і які тому можна безпечно передавати по загальнодоступних або незахищених лініях зв'язку.

Початковий стан: Приховане цифрове значення, яке генерується шляхом введення стану, наприклад, часу, в генератор початкових станів, який генерує початковий стан за секретним алгоритмом. Початковий стан використовується для вибору алгоритму для скремблювання або розділення даних в пакеті з селектора. Початковий стан можна використовувати для безпечної передачі інформації про стан по загальнодоступним або незахищеним лініям зв'язку.

Селектор: Список або таблиця можливих алгоритмів скремблювання, шифрування або розділення, які є частиною спільних секретів і які використовуються разом з початковим станом або ключем для вибору конкретного алгоритму скремблювання, дескремблювання, шифрування, дешифрування, розділення або змішування пакета або пакетів.

Спільні секрети: Конфіденційна інформація про роботу вузлів SDNP, що включає таблиці або селектори алгоритмів скремблювання/дескремблювання, шифрування/дешифрування та змішування/розділення, а також алгоритми, що використовуються генераторами початкових станів, генераторами ключів, інформація про зони та процеси перетасовки алгоритмів, локально зберігаються на серверах DMZ, недоступних по мережі SDNP або через Інтернет.

Стан: Вхідні дані, наприклад, місце розташування, зона або мережевий час, які використовуються для динамічного генерування параметрів безпеки, наприклад, початкових станів або ключів, або для вибору алгоритмів для конкретних операцій SDNP, наприклад, змішування, розділення, скремблювання і шифрування.

Час: Універсальний мережевий час, що використовується для синхронізації зв'язку в мережі SDNP.

Дескремблювання: Процес, який використовується для відновлення сегментів даних скрембльованого пакету даних до їх первісного порядку або послідовності. Дескремблювання - це функція, зворотна по відношенню до функції скремблювання.

Зона: Мережа певних взаємопов'язаних серверів, які спільно використовують загальні облікові дані безпеки і спільні секрети. З'єднання останньої милі представляють собою окремі зони від тих, які знаходяться в хмарі SDNP.

Розробка Динамічної Захищеної Комунікаційної Мережі та Протоколу (SDNP)

Для запобігання кібератак та злому системи зв'язку з комутацією пакетів при мінімальній затримці пакетів в режимі реального часу, забезпечення можливості встановлення стійкого з'єднання і максимальної безперервності голосового зв'язку та онлайн-відео, розроблена розглянута в цьому документі динамічна захищена комунікаційна мережу та протокол (SDNP), заснована на ряді керівних принципів, а саме:

- Передача даних в режимі реального часу повинна завжди відбуватися по шляху найменшої затримки.

- При несанкціонованому стеженні або аналізі пакета даних має бути недоступним вміст, відносно того, звідки надійшов пакет, куди він прямує і що в ньому знаходиться.

- Корисне навантаження пакета даних має бути динамічно перешифроване, тобто дешифровано, а потім знову зашифровано з використанням іншого алгоритму шифрування, виключаючи ризик злому в будь-який прийнятний момент часу.

- Навіть після дешифрування, все корисне навантаження пакета даних як і раніше містить незрозумілу інформацію, що представляє собою динамічно скрембльоване поєднання кількох розмов і незв'язаних даних, змішаних зі "сміттєвими" заповнювачами пакета.

Впровадження вищезазначених керівних принципів охоплює безліч унікальних та інноваційних методів, функцій, властивостей і реалізацій, включаючи всі або деякі із наступних варіантів втілення винаходу:

- SDNP використовує одну або кілька виділених хмар, що містять телефонну систему, функції програмного комутатора, реалізовані з використанням пропрієтарного програмного забезпечення управління і контролю, недоступного через Інтернет.

- Передача даних всередині хмари повністю відбувається з використанням виділеної системи маршрутизації пакетів SDNP в пропрієтарних хмарах на основі адрес SDNP і динамічних портів (тобто пропрієтарних адрес NAT), а не IP-адрес. Адреси SDNP не можуть використовуватися або маршрутизуватись через Інтернет або за межами хмари SDNP.

- Мережа SDNP постійно ідентифікує та здійснює динамічну маршрутизацію всієї передачі даних в режимі реального часу за наявними шляхами з найменшою затримкою.

- Ніяка захищена або виконувана в режимі реального часу передача даних не маршрутизується поза хмарою SDNP або через Інтернет, крім передачі даних між хмарами і на ділянці останньої милі, і крім того зазвичай використовує маршрутизацію для одного переходу з невидимими адресами.

- Дані маршрутизації, що містяться в пакеті даних, ідентифікують маршрут для одного переходу між двома сусідніми пристроями, визначаючи тільки адреси SDNP або IP-адреси попереднього і наступного сервера

- Номер телефону або IP-адреси абонента і одержувача виклику, тобто відповідні адреси відправника і одержувача клієнта не присутні ні в заголовках IP-пакетів, ні в зашифрованому корисному навантаженні.

- Спільні секрети, пов'язані з управлінням і контролем, існують в системному програмному забезпеченні, встановленому на захищених серверах DMZ, недоступних через Інтернет.

- Передача пакетів SDNP може здійснюватися по трьох незалежних каналах, якими є "сервер імен", який використовується для ідентифікації елементів в хмарі SDNP; "Медіа-сервери", що використовуються для маршрутизації вмісту і даних, і "сигнальні сервери", що використовуються для управління і контролю пакетів та викликів.

- Інформація про маршрут разом з ключами та числовими початковими станами (при необхідності) надається усім учасникам в обміні медіа-серверів по окремому сигнальному каналу до виклику або встановлення зв'язку і без вмісту. Сигнальний сервер передає медіа-серверам тільки дані про попередній і наступний адресатів пакета, що проходить через мережу.

- Медіа-пакети містять фрагментовані дані, що представляють тільки частину виклику, документа, тексту або файлу, динамічно змішані та повторно змішані з іншими пакетами, що містять фрагментовані дані з інших джерел і різного типу.

- Для захисту передачі даних на ділянках першої і останньої милі використовуються спеціальні методи захисту, в тому числі розділення повідомлень, пов'язаних з сигнальним сервером, і медіа-пакетів та пов'язаних з ними пакетів вмісту.

- Передача пакетів залежить від типу вмісту: голосові повідомлення та відео реального часу або онлайн-відео передаються на основі поліпшеного протоколу UDP, в той час як сигнальні пакети, пакети команд і управління, файли даних, файли додатків, системні файли і інші файли, які чутливі до втрати пакетів або затримки, використовують протокол TCP.

- Для підтвердження того, що пристрій є реальним клієнтом, а не клоном, і для перевірки автентичності того, що людина, яка бере участь у комунікації - є справжнім власником пристрою, а не самозванцем, використовуються спеціальні методи захисту та перевірки автентичності.

Щоб забезпечити захищену передачу даних з малою затримкою та високою якістю обслуговування в технології VoIP і додатках реального часу, "динамічна захищена комунікаційна мережа та протокол" (SDNP), що розглядається в цьому документі, використовує мережу "динамічної решітки", що включає:

- динамічну адаптивну багатомаршрутну і решітчасту маршрутизації з мінімальною затримкою;

- динамічне скремблювання пакетів;
- динамічну фрагментацію з використанням розділення, змішування, синтаксичного аналізу пакетів, а також заповнювачі пакетів "сміттєвими" бітами;
- динамічне внутрішньовузлове шифрування корисного навантаження в мережі або хмарі;
- динамічний мережевий протокол з маскуванням адрес і необхідною інформацією маршрутизації;
- багатоканальний зв'язок, що відокремлює носій та вміст від сигнальної, командних і контрольних, та мережевих адрес;
- динамічний адаптивний транспортний протокол реального часу з функціями для конкретних типів даних і контекстною маршрутизацією;
- підтримку шифрування корисних навантажень клієнтом з управлінням ключами під керівництвом користувача;
- полегшений аудіокодек для підвищення якості обслуговування в перевантажених мережах.

Як вже було зазначено, зв'язок в мережі SDNP заснований на мультимаршрутній та решітчастій передачі для динамічної маршрутизації пакетів даних. На відміну від одноканального зв'язку з комутацією пакетів, використовуваних для передачі даних OTT в Інтернет та технології VoIP, в системі SDNP, відповідно до даного винаходу, вміст пакетів даних не передається послідовно цілісними пакетами, що містять інформацію з загального джерела або від абонента, а передається у фрагментованій формі з динамічним змішуванням та повторним змішуванням вмісту, що виходить від кількох джерел і абонентів, при якому зазначені дані об'єднують неповні уривки даних, вмісту, голосу, відео і файлів з даними різного типу, об'єднаних з заповнювачами із "сміттєвих" даних. Перевага розглядуваної реалізації фрагментації та передачі даних полягає в тому, що навіть незашифровані і нескрембльовані пакети даних майже неможливо інтерпретувати, оскільки вони являють собою комбінацію незв'язаних даних та типів даних.

Завдяки поєднанню фрагментованого змішування та розділення пакетів зі скремблюванням і динамічним шифруванням пакетів, ці гібридні пакети динамічно зашифрованих, скрембльованих фрагментованих даних являють собою беззмістовні пакети інформації, абсолютно незрозумілі для будь-якої сторони або спостерігача, що не мають спільних секретів, ключів, числових початкових станів, а також змінних стану та часу, які використовуються для створення, пакетування і динамічного повторного пакування цих даних.

Крім того, фрагментований вміст кожного пакета та секрети, які використовуються для його створення, діють всього лише на частку секунди, перш ніж пакет буде переконструйований новими фрагментами і новими заходами захисту, наприклад, зміненими початковими станами, ключами, алгоритмами та секретами. Обмежена тривалість часу, протягом якого у кіберзлочинця є доступ для злому і розкриття залежного від стану пакета даних SDNP, ще більше підвищує захищеність SDNP, при цьому є тільки одна десята секунди на те, щоб виконати обробку, що вимагає десятків тисяч років обчислень, що на дванадцять порядків величини більше часу, доступного для злому.

Комбінація вищезгаданих методів задіє багатовимірний захист, що значно перевершує захист при статичному шифруванні. З цієї причини розглядувана в цьому документі динамічна захищена комунікаційна мережа та протокол визначаються як "гіперзахищена" мережа.

Скремблювання пакетів даних - Відповідно до цього розглядуваного винаходу, захищений зв'язок в мережі з комутацією пакетів спирається на кілька елементів, що дозволяють запобігти злому та забезпечити безпеку, одним з яких є скремблювання пакетів SDNP. Скремблювання пакетів SDNP передбачає перегрупування сегментів даних з послідовності, що робить інформацію незрозумілою і непотрібною. Згідно Рис. 2A, дескрембльований пакет даних - пакет даних 923 - після виконання операції скремблювання 924, перетворюється в скрембльований пакет даних 925. Операція скремблювання може використовувати будь-який алгоритм, чисельний метод або метод управління послідовністю. Алгоритм може являти собою статичне рівняння або включати динамічні змінні або числові початкові стани на основі таких "станів", як час 920 при скремблюванні, та числовий початковий стан 929, згенерованих генератором початкових станів 921, який може генерувати початковий стан 929, використовуючи алгоритм, який також залежить від такого стану, як час 920 при скремблюванні. Наприклад, якщо кожна дата перетворюється в унікальне монотонно зростаюче число, то кожне початкове значення 929 є унікальним. Час 920 та початковий стан 929 можуть використовуватися для вибору конкретного алгоритму та також можуть використовуватися для вибору або обчислення конкретної операції скремблювання 924, обраної зі списку доступних методів скремблювання, тобто з алгоритмів скремблювання 922. На схемах потоків даних зручно ілюструвати цю

операцію та послідовність скремблювання пакетів з використанням схематичного або символічного уявлення, позначеного тут символом 926.

Операція дескремблювання, показана на Рис. 2B, ілюструє функцію, зворотну операції скремблювання 924, а саме, операцію дескремблювання 927, де стан або час 920 та відповідний початковий стан 929, що використовуються для створення скрембльованого пакета даних 925, знову використовуються для скасування операції скремблювання, щоб отримати дескрембльовані дані, а саме, дескрембльований пакет даних 923. Якщо при первинному скремблювання пакетів використовувалося певний стан або час 920, той же метод скремблювання повинен бути знову використаний та в операції 927 дескремблювання шляхом його вибору зі списку алгоритмів скремблювання 922. Незважаючи на те, що список алгоритмів скремблювання 922 відноситься до терміну "скремблювання", та ж таблиця алгоритмів використовується для ідентифікації та вибору оберненої функції, необхідної для виконання "дескремблювання", тобто список алгоритмів скремблювання 922 містить інформацію, необхідну як для скремблювання пакетів даних, так і для дескремблювання пакетів даних. Оскільки ці дві функції включають в себе одні й ті ж інструкції, що виконуються в зворотному порядку, список 922 також може бути перейменований в список алгоритмів "скремблювання/дескремблювання" 922. Проте для більшої наочності ця таблиця відзначена тільки назвою функції без вказівки її зворотної функції.

Якщо алгоритм скремблювання, обраний для реалізації операції дескремблювання 927, не відповідає вихідному алгоритму, використаному при скремблюванні пакетів, або якщо початковий стан 929 або стан або час 920 не збігаються з часом скремблювання, то операція дескремблювання не зможе відновити вихідний дескрембльований пакет даних 923, і дані пакета будуть втрачені. На схемах потоків даних зручно ілюструвати цей процес дескремблювання пакетів з використанням схематичного або символічного уявлення, позначеного тут символом 928.

Відповідно до розглядуваного винаходу для виконання операції скремблювання можуть використовуватися різні алгоритми за умови, що процес є оборотним, а це означає, що повторення дій в зворотному порядку по відношенню до вихідного процесу повертає кожен сегмент даних в вихідне та правильне положення в заданому пакеті даних. З математичної точки зору допустимими алгоритмами скремблювання є ті алгоритми, які оборотні, тобто коли функція F(A) має зворотну функцію $F^{-1}(A)$ або, як варіант, перетворення має відповідну зворотну функцію, для якої

$F^{-1}[F(A)]=A$

Це означає, що при застосуванні функції F до файлу даних, послідовності, рядку символів, файлу або вектору A та при подальшому застосуванні зворотної функції F^{-1}, будуть отримані вхідні дані A, що не змінилися ні за величиною, ні за порядком проходження елементів.

Приклади таких оборотних функцій ілюструються статичними алгоритмами скремблювання, показаними на Рис. 2C, в тому числі алгоритмами дзеркального відображення і фазового зсуву. В алгоритмах дзеркального відображення сегменти даних замінюються іншими сегментами даних, які є їх дзеркальним відображенням відносно осі симетрії, яка визначається модулем ("mod") процесу дзеркального відображення. При дзеркальному відображенні по модулю 2, згідно рисунку, кожні два сегмента даних вихідного пакета вхідних даних 930 міняються місцями, тобто міняються місцями 1A і 1B, аналогічно 1C і 1D, 1E і 1F, і т.д., при цьому утворюється скрембльований пакет вихідних даних 935 з осями симетрії між першим і другим сегментами даних, між третім та четвертим сегментами даних і т.д. або, на мові математики, в позиціях 1,5; 3,5; 5,5; ...; (1,5+2n).

При дзеркальному відображенні по модулю 3 перший та третій сегменти даних в кожній трійці сегментів даних міняються місцями, а середній пакет кожної трійки залишається в початковому положенні. Відповідно, сегменти даних 1A та 1C міняються місцями, а 1B залишається в центрі трійки; сегменти даних 1D і 1F міняються місцями, а 1E залишається в центрі трійки і т.д., при цьому утворюється скрембльований пакет вихідних даних 936. При дзеркальному відображенні по mod3 осі симетрії знаходяться в позиціях 2, 5, 8,..., (2+3n).

При дзеркальному відображенні по mod4 перший та четвертий, а також другий та третій сегменти даних з кожної четвірки сегментів даних міняються місцями і т.д., при цьому утворюється скрембльований пакет вихідних даних 937 з пакету вхідних даних 931. Відповідно, сегмент даних 1A міняється місцями з 1D; сегмент даних 1B міняється місцями з 1C; і т.д. При дзеркальному відображенні по mod4 вісь симетрії знаходиться між другим та третім сегментами даних кожної четвірки, тобто між 2-м і 3-м сегментами даних, 6-м і 7-м сегментами даних і т.д., або, на мові математики, в позиціях 2,5; 6,5; ...; (2,5+4n). При дзеркальному відображенні по модулю m m-й сегмент даних вхідного пакета даних 932 замінюється першим, тобто 0-м

сегментом даних; 0-й сегмент даних замінюється на m-й елемент; і аналогічним чином n-й елемент замінюється на (mn)-й сегмент даних, при цьому утворюється скрембльований пакет вихідних даних 938.

Інший спосіб скремблювання, також показаний на Рис. 2C, являє собою зсув кадру, де кожен сегмент даних зсувається вліво або вправо на один, два або більше кадрів. Наприклад, при фазовому зсуві на один кадр кожен сегмент даних зсувається на один кадр, при цьому перший сегмент даних зсувається в другу позицію; другий сегмент даних зсувається в позицію третього кадру і т.д., при цьому утворюється скрембльований пакет вихідних даних 940. Останній кадр вхідного пакета даних 930, кадр 1F в наведеному прикладі, зміщується в позицію першого кадру, раніше зайняту сегментом даних 1A.

При фазовому зсуві на 2 кадри перший сегмент даних 1A вхідного пакета даних 930 зсувається на два кадри в позицію, раніше зайняту сегментом даних 1C, четвертий кадр 1D зсувається в останню позицію скрембльованого пакету вихідних даних 941, передостанній сегмент даних 1E зсувається в першу позицію, а останній 1F зсувається в другу позицію. Аналогічним чином, при фазовому зсуві на 4 кадри сегменти даних вхідного пакета даних 930 зсуваються на чотири позиції, при цьому перший кадр 1A, замінює кадр, який раніше займав 1E, 1B замінює 1F, 1C замінює 1A, і т.д., при цьому утворюється скрембльований пакет вихідних даних 942. У разі максимального фазового зсуву перший кадр замінює останній; другий кадр, спочатку зайнятий сегментом 1B, стає першим кадром пакету вихідних даних 943, при цьому другий елемент зсувається в першу позицію, третій - в другу і т.д. Фазовий зсув одного кадру за межі максимального фазового зсуву призводить до того, що вихідні дані не відрізняються від вхідних. У наведених прикладах фазовий зсув даних проводиться вправо. Алгоритм також працює і при фазовому зсуві вліво, але з іншими результатами.

Вищезазначені алгоритми і аналогічні методи в даному описі називаються алгоритмами статичного скремблювання, оскільки операція скремблювання відбувається в один момент часу, та перетворює набір вхідних даних в унікальні вихідні дані. Крім того, описані раніше алгоритми не використовують значення пакета даних для визначення порядку виконання скремблювання. Згідно Рис. 2D, відповідно до розглядуваного винаходу, параметричне скремблювання означає, що метод скремблювання вибирається з таблиці можливих алгоритмів скремблювання, наприклад, sort #A, sort #B і т.д. на основі значення, отриманого з даних, що містяться в самому пакеті даних. Наприклад, припустимо, що кожен сегмент даних може бути перетворений в числове значення, засноване на обчисленні даних, що містяться в цьому сегменті даних. Одним з можливих підходів до визначення чисельного значення сегмента даних є використання десяткового або шістнадцятирічного еквівалента бітових даних в сегменті даних. Якщо сегмент даних містить кілька членів, числовий еквівалент можна знайти, підсумовуючи числа в сегменті даних. Потім сегмент даних об'єднується в одне число або "параметр", за яким потім вибирається метод скремблювання.

У показаному прикладі на етапі 950 проводиться параметричне перетворення нескрембльованого пакета даних 930 в таблицю даних 951, що містить числове значення для кожного сегмента даних. Згідно рисунку, сегмент даних 1A (0-й кадр) має числове значення 23, сегмент даних 1B (1-й кадр) має числове значення 125 і т.д. Потім на етапі 952 для всього пакета даних 930 витягується одне значення пакета даних. У наведеному прикладі сума 953 являє собою результат лінійного змішування всіх значень сегментів даних з таблиці 951 і дорівнює 1002. На етапі 954 це параметричне значення, тобто сума 953, порівнюється з таблицею умов, наприклад, з наявним в програмному забезпеченні набором визначених операторів типу "if-then-else", щоб порівняти суму 953 з рядом неперекриваючих числових діапазонів в таблиці 955, щоб визначити, яку процедуру сортування слід використовувати. У цьому прикладі параметричне значення 1002 знаходиться в діапазоні від 1000 до 1499, а це означає, що слід використовувати процедуру сортування sort #C. Після вибору процедури сортування параметричне значення більше не потрібно. Після цього на етапі 956 вхідні нескрембльовані дані 930 скремблюється обраним методом, при цьому утворюється скрембльований пакет вихідних даних 959. У наведеному прикладі результат сортування Sort #C, наведений в таблиці 957, містить набір відносних переміщень для кожного сегмента даних. Перший сегмент даних скрембльованого пакета даних 959 (0-й кадр) визначається переміщенням сегмента даних 1D на три позиції вліво, тобто його зрушенням три рази. Перший кадр містить сегмент даних 1B, він не змінює своє початкове положення, тобто переміщається на 0 місць. Другий кадр містить сегмент даних 1E, зрушений на дві позиції вліво щодо вихідного положення. Точно так же третій кадр містить сегмент даних 1F, зрушений на дві позиції вліво щодо вихідного положення. Четвертий кадр скрембльованого пакету вихідних даних 959 містить сегмент даних 1C, зрушений вправо, тобто на +2 позиції, щодо свого вихідного положення.

П'ятий кадр містить сегмент даних 1A, зрушений на п'ять позицій вправо, тобто на +5 позицій, щодо свого вихідного положення.

Таким чином, згідно таблиці 957 для процедури сортування sort #C, кожен сегмент даних переміщається в однозначно певну нову позицію, при цьому утворюється параметрично певний скрембльований пакет даних 959. Щоб дескремблювати цей скрембльований пакет даних, процес виконується в зворотному порядку з використанням того ж методу сортування sort #C. Щоб гарантувати вибір того ж алгоритму для виконання операції дескремблювання, параметричне значення 953 пакета даних не може бути змінено в результаті операції скремблювання. Наприклад, лінійне змішування параметричного значення кожного сегмента даних дає одне й те саме числове значення незалежно від порядку чисел.

Динамічне скремблювання використовує стан системи, наприклад, час, щоб мати можливість ідентифікувати умови, при яких був скрембльований пакет даних, що дозволяє вибрати той же метод для виконання операції дескремблювання. В системі, показаної на Рис. 2E, стан використовується для створення замаскованого числового початкового стану, який передається відправнику або одержувачу пакета, який потім використовує цей початковий стан для вибору алгоритму скремблювання з таблиці. В якості альтернативи, відправнику або одержувачу може бути передано саме стан, і цей стан може використовуватися генератором прихованих чисел, розташованим у відправника або одержувача, для генерування прихованого числа, за яким здійснюється вибір алгоритму скремблювання/дескремблювання. Така компоновка показана на Рис. 2E, де стан, наприклад, час 920 використовується для генерування прихованого числа 961 за допомогою генератора прихованих чисел 960 і для вибору методу скремблювання зі списку алгоритмів скремблювання 962. Генератор прихованих чисел 960 також може ввести приховане число HN 961b безпосередньо в операцію. Операція скремблювання 963, де HN може виступати в якості змінної при виконанні операції скремблювання. Як показано на Рис. 2F скрембльованний пакет даних 930 перетворюється в скрембльованний пакет даних 964. Використовуючи прихований номер 961 для вибору алгоритму з таблиці 962 алгоритму скремблювання, операція скремблювання 963 перетворює нескрембльований пакет даних 930 в скрембльований пакет даних 964. Відповідно до Рис. 2E, стан 920 може бути передано генератору прихованих чисел 960 безпосередньо, або стан 920 може бути передано генератору прихованих чисел через генератор початкових станів 921.

Вибір алгоритму скремблювання по таємному номеру, а не просто по числовому початковому стану, має перевагу, яка полягає в тому, що він виключає будь-яку можливість злочинного відтворення таблиці скремблювання шляхом аналізу потоку даних, тобто статистичного зіставлення повторюваних наборів скрембльованих даних з відповідними числовими початковими станами. Початковий стан може бути видимим в потоці даних і, отже, вразливим для шпигунства, в той час як генератор прихованих чисел та приховане число HN, яке він створює, ґрунтуються на спільних секретах. Таким чином, приховане число HN не присутнє в потоці даних, невразливо для шпигунства та синтаксичного аналізу, що означає, що воно не передається по мережі, а генерується локально по числовому початковому стану. Таким чином, ця математична операція - генератор прихованих чисел - забезпечує підвищення рівня захищеності в частині запобігання хакерських атак, тому що призначення числового початкового стану замасковано.

Відразу після вибору алгоритму числовий початковий стан також може використовуватися як вхідна змінна в алгоритмі процесу скремблювання 963. Подвійне призначення числового початкового стану додатково заплутує аналіз, тому що початковий стан не безпосередньо обирає алгоритм, а працює разом з ним при визначенні остаточної послідовності сегментів скрембльованих даних. Аналогічним чином, щоб дескремблювати динамічно скрембльований пакет даних, початковий стан 929 (або, як варіант, стан або час 920) має бути передано з вузла зв'язку, пристрою або програмного забезпечення, що виконує скремблювання, до будь-якого вузла або пристрою, який буде його дескремблювати.

Відповідно до розглядуваного винаходу, алгоритм генерації початкових станів 921, генератор прихованих чисел 960 та список алгоритмів скремблювання 962 представляють собою "спільні секрети" - інформацію, що зберігається на сервері DMZ (як описано нижче) і невідому ні відправнику, ні одержувачу пакета даних. Спільний секрет встановлюється заздалегідь і не пов'язаний з переданими пакетами даних, крім, можливо, часу установки коду, де використовуються різні процедури автентифікації для виключення витоку секрету. Як описано нижче, спільні секрети можуть бути обмежені "зонами", тому знання одного набору вкрадених секретів як і раніше не дозволяє хакеру отримати доступ до всієї мережі зв'язку або перехоплювати повідомлення в реальному часі.

Крім спільних секретів при динамічному скремблюванні, де алгоритм скремблювання змінюється під час передачі пакета даних, для скремблювання або дескремблювання даних потрібен початковий стан на основі "стану". Це стан, на якому засновано початковий стан, може бути будь-яким фізичним параметром, таким як час, номер вузла зв'язку, ідентифікатор мережі або навіть координати GPS, за умови, що не існує невизначеності щодо стану, використовуваного при генеруванні початкового стану, та за умови наявності засобів інформування наступного вузла про те, який стан використовувався при скремблюванні попереднього пакету даних. Алгоритм, який використовується генератором початкових станів для створення початкового стану, є частиною спільних секретів, і, отже, знання початкового стану не дозволяє визначити стан, на якому ґрунтується цей початковий стан. Початковий стан можна передавати від одного вузла зв'язку до іншого, помістивши його в сам пакет даних, відправивши його через інший канал або шлях або застосувавши будь-яку комбінацію цих методів. Наприклад, стан, що використовується при генеруванні початкового стану, може являти собою лічильник, який спочатку містить випадкове число, яке згодом збільшується на постійну величину при кожному проходженні пакета даних через вузол зв'язку, при цьому кожне значення лічильника відповідає конкретному алгоритму скремблювання.

В одному з варіантів здійснення динамічного скремблювання при першому виконанні операції скремблювання генерується випадкове число для вибору використовуваного методу скремблювання. Це випадкове число поміщається в пакет даних в його заголовку або тієї частини пакета даних, яка зарезервована для команд і управління, і не піддається скремблюванню. Коли пакет даних надходить в наступний вузол, це введене число зчитується вузлом зв'язку та використовується програмним забезпеченням для вибору належного алгоритму для дескремблювання вхідного пакета даних. Потім це число, тобто "Значення лічильника", збільшується на одиницю або яке-небудь інше задане ціле число, пакет скремблюється відповідно до алгоритму, пов'язаним з цим новим числом, а це нове число записується в вихідний пакет даних замість попереднього числа. Наступний вузол зв'язку повторює цей процес.

В альтернативному варіанті здійснення даного методу на основі лічильника для вибору алгоритму скремблювання генерується випадкове число для вибору початкового алгоритму скремблювання, і це число надсилається кожному вузлу зв'язку, використовуваному для передачі конкретного пакета даних як "спільний секрет". Значення лічильника, наприклад, починаючи з 0, поміщається в пакет даних в його заголовку або в тій частині пакета даних, яка зарезервована для команд і управління, і не піддається скремблюванню. Потім цей пакет даних пересилається на наступний вузол зв'язку. Коли пакет надходить на наступний вузол зв'язку, сервер зчитує значення лічильника, додає це значення до початкового випадкового числа, ідентифікує алгоритм скремблювання, застосований до попередньої операції скремблювання пакета даних, і дескремблює пакет відповідно до нього. Потім значення лічильника збільшується на одиницю або будь-яке інше задане ціле число, і це значення лічильника знову зберігається в заголовку пакета даних або тієї частини пакета даних, яка зарезервована для команд і управління, і не піддається скремблюванню, перезаписуючи попереднє значення лічильника. Випадкове число, що служить спільним секретом, не передається в пакеті даних зв'язку. Після того як пакет даних надходить в наступний вузол зв'язку, сервер додає випадкове число, яке є спільним секретом, доданим до зміненого значення лічильника, витягнутої з пакета даних. Це нове число однозначно ідентифікує алгоритм скремблювання, використовуваний попереднім вузлом зв'язку для скремблювання вхідних пакетах. У разі застосування цього методу кіберзлочинцем може бути перехоплено тільки неінформативне значення лічильника з дескрембльованої частини пакета даних, які не несуть ніякої важливої інформації.

В іншому альтернативному методі може використовуватися приховане число для передачі стану пакета та того, який алгоритм використовувався для його скремблювання. Приховане число об'єднує змінні в часі стан або початковий стан з спільним секретом, який, як правило, являє собою числовий алгоритм, при цьому вони разом використовуються для створення конфіденційного числа, тобто "прихованого числа", яке ніколи не передається між вузлами зв'язку і, отже, не є предметом розбору або дослідження при проведенні атаки "людина посередині" або з боку кіберзлочинця. Потім приховане число використовується для вибору застосовуваного алгоритму скремблювання. Оскільки стан або початковий стан не має сенсу без знання алгоритму, який використовується для обчислення прихованого числа, і оскільки алгоритм, який є спільним секретом, може зберігатися за міжмереживим екраном, недоступним по мережі або Інтернету, жодний моніторинг мережевого трафіку не зможе виявити схему. Для додаткового ускладнення ситуації місцезнаходження початкових станів також може являти собою спільний секрет. В одному з варіантів здійснення винаходу число, яке передається до

нескрембльованої частини пакета даних та доступне для спостереження та синтаксичного аналізу даних, наприклад, 27482567822552213, є довге число, в якому тільки його частина є початковим станом. Якщо, наприклад, початковий стан визначається цифрами з третьої по восьму, то реальний початковий стан - це не все число 27482567822552213, а тільки його частина, виділена жирним шрифтом, тобто початковий стан - це 48256. Потім цей початковий стан разом з спільним секретом використовується алгоритмом для генерування прихованого числа, а це приховане число, що використовується для вибору алгоритму скремблювання, динамічно змінюється по всій мережі.

Застосування шифрування пакетів даних в мережі SDNP описано в додатку № 803 869 від 20 липня 2015 року, що має назву ""Динамічна Захищена Комунікаційна Мережа та Протокол". Застосування шифрування пакетів даних в мережі зв'язку "Останньої Милі" буде описано більш детально далі в цьому розділі.

Представлені дані, що проходять по мережі, хоча вони і скрембльовані, можна вважати "текстовим файлом", оскільки в пакетах даних присутні фактичні дані, тобто пакети не перетворені в зашифрований текст. Навпаки, в зашифрованому тексті рядок символів, який містить вихідні дані, незалежно від того, скрембльовані вони чи ні, перетворюється в серію беззмістовних символів за допомогою ключа шифрування, і не може бути знову перетворений в вихідну форму текстового файлу без ключа дешифрування. Роль шифрування в даній системі зв'язку на основі SDNP обговорюється нижче в розділі "Шифрування".

Щоб змінити послідовність пакетів даних під час передачі по мережі, потрібно "ре-скремблювати" пакети, згідно Рис. 3. Процес ре-скремблювання пакетів перетворює скрембльований пакет даних в його спочатку не скрембльований стан, а потім знову скремблює його відповідно до нового алгоритму скремблювання. Таким чином, використовуваний тут термін "ре-скремблювання" означає дескремблювання пакета даних і його подальше повторне скремблювання, як правило, за допомогою іншого алгоритму або методу скремблювання. Такий підхід дозволяє виключити ризик пошкодження даних, що виникає при скремблюванні раніше скрембльованого пакета та втрати контролю над стеженням за послідовністю, необхідною для відновлення вихідних даних. Згідно рисунку, скрембльований пакет даних 1008, спочатку скремблюється за допомогою операції скремблювання пакетів 926, "ре-скремблюється", спочатку шляхом його дескремблювання за допомогою операції дескремблювання 928, використовуючи зворотну операцію алгоритму скремблювання, за яким було виконано скремблювання даних, а потім пакет даних скремблюється знову за допомогою операції скремблювання 926, але за іншим алгоритмом скремблювання, а не по тому, який використовувався в попередній операції скремблювання 926. Результуючий ре-скрембльований пакет даних 1009 відрізняється від попереднього скрембльованого пакета даних 1008. Операція ре-скремблювання 1017 являє собою послідовне виконання дескремблювання та подальшого скремблювання, та в цьому документі називається "US ре-скремблювання", де "US" - абревіатура від англ. Unscrambling-Scrambling, що означає "дескремблювання-скремблювання". Щоб відновити вихідний пакет даних 930, при операції дескремблювання остаточного пакета 928 необхідно застосувати зворотну функцію того ж алгоритму, який використовувався для попереднього ре-скремблювання пакета даних.

Відповідно до розглядуваного винаходу статичне і динамічне скремблювання даних позбавляє інтерпретації скрембльованих даних будь-якого сенсу, перетворюючи звук в невпізнанний шум, перетворюючи текст в незв'язний набір символів, перетворюючи відео в "відео-сніг" і код скремблювання в такий, що є невідновлюваним. Само по собі скремблювання забезпечує високу ступінь безпеки. Однак в методі SDNP, розглянутому в цьому документі, скремблювання - це тільки один з елементів, призначених для того, щоб забезпечити і гарантувати захищений зв'язок, що виключає втручання хакерів, проведення кібератак, кіберзлочинів та проведення атак типу "людина посередині".

Шифрування пакетів. Відповідно до розглядуваного винаходу, захищений зв'язок у мережі з комутацією пакетів спирається на кілька елементів, що дозволяють запобігти злому та забезпечити безпеку, одним з яких є шифрування SDNP. Як зазначено вище, слово "шифрування" має грецьке походження, що означає "приховувати, ховати, затемнювати", і являє собою засіб перетворення нормальної інформації або даних, зазвичай званих "текстовим файлом", в "зашифрований текст", який має незрозумілий формат, який робить дані нечитабельними без секретних знань. У сучасному зв'язку ці секретні знання зазвичай пов'язані зі спільним використанням одного або декількох "ключів", які використовуються для шифрування і дешифрування даних. Зазвичай ці ключі містять псевдовипадкові числа, що генеруються за певним алгоритмом. Сьогодні написані численні статті та тексти, які обговорюють переваги і недоліки різних методів шифрування, наприклад: "Криптономікон" Ніла

Стівенсона, © 1999 р.; "Книга шифрів: наука про секретності від Стародавнього Єгипту до квантової криптографії" Саймона Сінгха, © 1999 р.; "Практична криптографія" Нільса Фергюсона, © 2013 року і "Криптоаналіз: дослідження шифрів і їх розшифровка", вперше опублікована в 1939 р

Незважаючи на те, що поняття шифрування або шифрів з'явилося в давні часи і добре відомо фахівцям в даній області, застосування криптографії в розглядуваній динамічній захищеній комунікаційній мережі та протоколі є унікальним, воно полегшує як наскрізне шифрування, так і динамічне шифрування для одного міжвузлового переходу стосовно архітектурі самої мережі незалежно від власного шифрування даних будь-якого клієнта. Базовий принцип архітектурного проектування системи передачі даних SDNP полягає в тому, що при наявності достатнього часу будь-який статично зашифрований файл або повідомлення можна в кінцевому підсумку зламати та викрасти інформацію, незалежно від того, наскільки складний шифр. Незважаючи на те, що це припущення може не відповідати дійсності, немає необхідності доводити або спростовувати його, тому що протилежний підхід, тобто очікування збою конкретного методу шифрування, може привести до неприйнятних і незворотних наслідків.

Замість цього система передачі даних SDNP базується на передумові, що всі зашифровані файли мають обмежений "термін зберігання", це метафоричне висловлювання означає, що зашифровані дані є надійними (захищеними) тільки протягом обмеженого періоду часу, і що конфіденційні дані повинні бути заново динамічно перешифровані через регулярні інтервали часу, в ідеалі набагато менші, ніж найоптимістичніші оцінки часу, необхідного для злому шифру з використанням сучасних комп'ютерів. Наприклад, якщо, за оцінкою криптологів, велика серверна ферма криптодвигунів може зламати цей шифр за один рік, то в системі передачі даних SDNP пакет даних буде перешифровуватися через кожну секунду або навіть через кожні 100 мс - інтервал, величина якого на багато порядків менша інтервалу, протягом якого найкраща технологія здатна зламати його. Тому шифрування в SDNP обов'язково є динамічним, тобто залежить від часу, а також може бути залежним від простору, тобто залежати від місця розташування вузла зв'язку в мережі з комутацією пакетів або географічного положення. Таким чином, використовуваний тут термін "перешифрування" відноситься до розшифрування пакету даних і його подальшого повторного шифрування, як правило, за допомогою іншого алгоритму або методу шифрування.

Отже, шифрування в SDNP передбачає багаторазове та часте перетворення даних з незашифрованого текстового файлу в зашифрований текст, що робить інформацію незрозумілою і непотрібною. Навіть якщо шифрування даних конкретного пакета неймовірним чином вдалося зламати, то при використанні методів динамічного шифрування SDNP у наступного пакета даних буде зовсім інший ключ шифрування або шифр, що потребують починати з самого початку новий процес злому його шифрування. Обмеження загального вмісту кожного унікально зашифрованого пакета даних пом'якшує потенційний збиток від несанкціонованого доступу, оскільки відкритий пакет даних сам по собі містить занадто маленький файл даних і не представляє особливої цінності або користі для кіберзлочинця. Більш того, комбінуючи динамічне шифрування з вищезгаданими методами скремблювання SDNP, можна значно підвищити захищеність зв'язку. Навіть в незашифрованому вигляді перехоплений файл даних містить лише невеликий фрагмент даних, голосу або відео, який скремблювання перетворює в беззмістовну і незрозумілу послідовність сегментів даних.

У відповідності до даного винаходу шифрування SDNP є динамічним та залежним від стану. Згідно Рис. 4А, незашифрований пакет даних являє собою текстовий файл 930, оброблений за допомогою операції шифрування 1020 при цьому утворюється зашифрований пакет даних, що містить шифротекст 1024 або 1025. У разі шифротекста 1024 весь пакет даних текстового файлу 930 шифрується повністю, при цьому сегменти даних від 1А до 1F обробляються як один файл даних. У разі шифротекста 1025 кожен сегмент даних текстового файлу 930 від 1А до 1F шифрується окремо і незалежно, і не об'єднується з іншими сегментами даних. Перший сегмент даних 1А шифрується та поміщається у відповідний перший сегмент даних шифротекста, показаного для наочності рядком символів, що починається з 7$ та представляє собою довгий рядок символів або цифр, які не показані. Аналогічно, другий сегмент даних 1В текстового файлу шифрується та поміщається в другий сегмент даних шифротекста, що представляє собою довгий рядок символів, показаний для наочності, починаючи з *^. Символи 7$ і *^ показані, щоб продемонструвати початкові елементи беззмістовних рядків символів, цифр, і літер, що не обмежують і не містять ніяких конкретних даних про джерело текстового файлу або довжину рядків символів, які були зашифровані.

Операція шифрування 1020 може використовувати будь-який доступний алгоритм, криптографічний метод або метод шифрування. Незважаючи на те, що алгоритм може являти

собою статичне рівняння, в одному з варіантів здійснення винаходу операція шифрування використовує динамічні змінні або "стан", наприклад, час шифрування 920, а також генератор шифрування 1021 для створення "E-key"1022, який також може залежати від стану, наприклад, часу шифрування 920. Наприклад, дата та час шифрування можуть використовуватися як числове значення для генерації ключа шифрування, який не можна відтворити, навіть якщо був виявлений алгоритм шифрування. Час 920 або інші "стани" також можуть використовуватися для вибору конкретного алгоритму зі списку алгоритмів шифрування 1023, який є списком доступних алгоритмів шифрування. На діаграмах потоків даних зручно ілюструвати цю операцію та послідовність шифрування пакету з використанням схематичного або символічного уявлення, позначеного тут символом, показаним для операції шифрування 1026. У всіх матеріалах опису винаходу символом, що представляє захищені та зашифровані дані, може також служити замок. Замок з розташованим над ним циферблатом вказує на захищений механізм доставки, наприклад, на зашифровані файли, які, якщо вони не будуть прийняті протягом певного інтервалу часу або до певного моменту часу, саморуйнуються і губляться назавжди.

Операція дешифрування, показана на Рис. 4B, ілюструє обернену функцію операції шифрування 1020, а саме, операцію дешифрування 1031, де стан або час 920 і інші стани, які використовуються для створення шифротекста 1024, разом з ключем дешифрування ("D-key") 1030, генеруються генератором ключів D-key 1029, повторно використовуються для скасування шифрування, тобто розшифрування файлу, для отримання незашифрованих даних, що містять вихідний пакет даних 990 текстового файлу. Якщо при первинному шифруванні пакетів використовувався певний стан або час 920, та ж операція шифрування повинна бути знову використана та в операції дешифрування 1031 шляхом її вибору зі списку алгоритмів шифрування 1023. Незважаючи на те, що список алгоритмів шифрування 1023 відноситься до терміну "шифрування", ця ж таблиця алгоритмів використовується для ідентифікації та вибору оберненої функції, необхідної для виконання "дешифрування", тобто список алгоритмів шифрування 1023 містить інформацію, необхідну як для шифрування, так і для дешифрування пакетів даних. Оскільки ці дві функції включають в себе одні й ті ж інструкції, що виконуються в зворотному порядку, таблиця 1023 також може бути перейменована в таблицю алгоритмів "шифрування/дешифрування" 1023. Однак для більшої наочності ця таблиця відзначена тільки назвою функції без вказівки її зворотної функції.

Якщо алгоритм шифрування, обраний для реалізації операції дешифрування 1031, не відповідає зворотному алгоритму по відношенню до вихідного алгоритму, використаному в операції шифрування пакетів, або якщо стан або час 920 не збігаються з часом шифрування, або якщо D-key 1030 не пов'язаний відомим числовим співвідношенням з E-key 1022, використовуваним під час шифрування, то операція дешифрування 1031 не зможе відновити вихідні незашифровані дані 990, і дані пакета будуть втрачені. На схемах потоків даних цей процес дешифрування пакетів зручно ілюструвати за використанням схематичного або символічного уявлення, позначеного тут символом операції дешифрування 1032.

Як вже було зазначено в цьому описі, використання ключів шифрування і дешифрування в криптографії та загальні алгоритми шифрування, такі як симетричне шифрування, з відкритим ключем, шифрування за методом RSA (абревіатура від прізвищ Rivest, Shamir і Adleman) і шифрування за методом AES256 (англ. Advanced Encryption Standard - покращений стандарт шифрування) і ін., є питаннями, добре відомими фахівцям в даній області. Однак застосування таких відомих криптографічних методів в даній системі передачі даних SDNP не так вразливе до злому або дешифрування через приховану інформацію, спільні секрети, залежних від часу динамічних змінних та станів, які є унікальними для даної системи передачі даних SDNP.

Тому навіть в малоймовірному випадку, коли кіберзлочинець володіє достатньою обчислювальною потужністю, щоб в кінцевому підсумку зламати надійну систему шифрування, йому не вистачає певної інформації, включеної в мережу SDNP як непублічна або як спільні секрети, які необхідні для виконання операції дешифрування; крім того він повинен зламати систему шифрування за частку секунди, поки не зміниться шифр. Крім того, кожен пакет даних, що проходить по даній мережі SDNP, використовує власний метод шифрування з унікальними ключами і динамічними станами. Необхідність одночасного отримання недостатньої інформації, динамічних станів і обмеженого інформаційного вмісту в будь-якому конкретному пакеті робить викрадення скільки-небудь важливих даних з будь-якого конкретного пакета даних як надто складною, так і невдячним завданням для кіберзлочинця.

Застосування динамічного шифрування і дешифрування пакетів даних в мережі SDNP описано в додатку 14/803,869 "Динамічна Захищена Комунікаційна Мережа та Протокол", на яке

зроблено посилання вище. Застосування криптографії пакетів даних в мережі зв'язку "Останньої Милі" буде описано більш детально далі в цьому розділі.

Щоб перехопити весь документ, онлайн-відео або голосову бесіду для відновлення зв'язаної послідовності даних, кібератака повинна послідовно зламувати і розшифровувати не один, а тисячі послідовних пакетів SDNP. Вкрай серйозне завдання безперервного злому послідовності пакетів SDNP ще більш ускладнюється поєднанням динамічного шифрування з раніше описаними методами скремблювання пакетів даних. Згідно Рис. 5, створення зашифрованого скрембльованого пакета даних 1024 включає в себе послідовну комбінацію операції скремблювання 926 і операції шифрування 1026 для перетворення нескрембльованого пакета даних 990 текстового файлу спочатку в скрембльований пакет даних 1008 текстового файлу, а потім в шифротекст 1024 скрембльованого пакета даних. Щоб відновити зашифрований скрембльований пакет, зворотні функції повинні бути застосовані в зворотній послідовності - спочатку операція дешифрування 1032 для відновлення скрембльованого пакета даних 1035 текстового файлу, а потім операція дескремблювання 928 для відновлення нескрембльованого пакета даних 990 текстового файлу.

Згідно рисунку, скремблювання і шифрування - це додаткові технології для забезпечення захищеного зв'язку. Незашифровані скрембльовані дані, що проходять по мережі, можна вважати "текстовим файлом", оскільки в пакетах даних присутні фактичні дані, тобто пакети не перетворені в шифротекст. Зашифровані пакети даних, або шифротекст, містять скрембльовані або нескрембльовані рядки символів, перетворені в беззмістовну серію безглуздих символів за допомогою ключа шифрування, і не можуть бути відновлені в вихідну форму текстового файлу без відповідного ключа дешифрування. Залежно від використовуваного алгоритму, ключі шифрування і дешифрування можуть являти собою один та той же ключ або різні ключі, пов'язані відомою математичною залежністю. Таким чином, скремблювання і шифрування представляють додаткові засоби для забезпечення захищеного зв'язку відповідно до розглядуваного винаходу для системи передачі даних SDNP.

Ці два методи, скремблювання і шифрування, можуть розглядатися незалежно, навіть коли вони використовуються в поєднанні один з одним, за винятком того, що послідовність, яка використовується для відновлення вихідного пакета даних з зашифрованого скрембльованого пакета даних, повинна бути зворотною по відношенню до послідовності, що використовується для його створення. Наприклад, якщо пакет даних 990 спочатку був скрембльований з використанням операції скремблювання 926, а потім зашифрований з використанням операції шифрування 1026, то для відновлення вихідного пакета даних зашифрований скрембльований пакет даних 1024 спочатку повинен бути дешифрований з використанням операції дешифрування 1032, а потім дескрембльований з використанням операції дескремблювання 928. З точки зору математики, якщо операція скремблювання F перетворює рядок бітів або символів в еквівалентну скрембльовану версію, а операція дескремблювання F-1 скасовує це скремблювання, внаслідок чого

$F^{-1}[F(A)]=A$,

і, аналогічно, якщо операція шифрування G перетворює рядок текстового файлу в еквівалентний шифротекст, а операція дешифрування G-1 скасовує це шифрування, внаслідок чого

$G^{-1}[G(A)]=A$,

то в комбінованому варіанті при послідовному виконанні операцій скремблювання і шифрування з подальшим дешифруванням і дескремблюванням виходить вихідний аргумент A - нескрембльований пакет даних текстового файлу. Відповідно,

$F^{-1}\{G^{-1}[G(F(A))]\}=A$

тому що дії виконуються у зворотній послідовності, зокрема, дешифрування [G-1] зашифрованого скрембльованого пакета [G (F (A))] відновлює скрембльований пакет даних текстового файлу F (A). Подальша операція дескремблювання F-1 скрембльованого пакета текстового файлу F (A) відновлює вихідний пакет даних A.

При використанні лінійних методів ця послідовність оборотна. Наприклад, якщо пакет даних спочатку зашифрований, а потім скрембльований, то для відновлення вихідного пакета даних скрембльований шифротекст повинен бути спочатку дескрембльований, а потім дешифрований. Відповідно,

$G^{-1}\{F^{-1}[F(G(A))]\}=A$

Зміна послідовності не допускається. Дешифрування пакета даних, який раніше був зашифрований, а потім скрембльований, без попереднього дескремблювання не відновить вихідний пакет даних, тобто

$F^{-1}\{G^{-1}[F(G(A))]\}\neq A$

Аналогічно, дескремблювання пакета, який був скрембльований, а потім зашифрований, також не зможе відновити вихідний пакет даних, тому що

$G^{-1}\{F^{-1}[G(F(A))]\}\neq A$

У підсумку, якщо пакет текстового файлу скремблюється перед шифруванням, він повинен бути дешифрований до дескремблювання; якщо пакет текстового файлу зашифрований перед скремблюванням, він повинен бути дескрембльований до його дешифрування.

Хоча й зрозуміло, що скремблювання і шифрування можуть виконуватися в будь-якій послідовності, в одному з варіантів здійснення методів SDNP, у відповідності до даного винаходу, шифрування і дешифрування під час передачі по мережі відбуваються частіше, ніж скремблювання, і тому шифрування має відбуватися після скремблювання, а дешифрування - до дескремблювання, згідно з рисунком 5, а не навпаки. Для зручності комбінація операції скремблювання пакета 926 з подальшою операцією шифрування 1026 визначається як операція шифрування скрембльованого пакета 1041, а її зворотна операція - комбінація операції дешифрування 1032 з подальшою операцією дескремблювання пакета 928 - як операція дескремблювання дешифрованого пакета 1042. Ці гібридні операції можуть використовуватися в статичній та динамічній системі передачі даних SDNP відповідно до даного винаходу.

Один із засобів підвищення безпеки в будь-який реалізації з використанням статичного скремблювання шифрування полягає в тому, що для кожного пакета даних, що відправляється, застосовуються різні методи скремблювання та/або шифрування, що включають зміну стану, початкових станів та/або ключів в момент часу t_1, коли кожен пакет даних входить в мережу зв'язку.

Однак більш надійним є альтернативне рішення з динамічною зміною методу шифрування та/або скремблювання пакета даних у міру проходження пакету по мережі в часі. Щоб полегшити необхідну обробку даних для реалізації чисто динамічної версії системи зв'язку SDNP, необхідно об'єднати раніше певні процеси, щоб "ре-скремблювати" (тобто дескремблювати, а потім скремблювати) і "перешифрувати" (тобто дешифрувати, а потім зашифрувати) кожен пакет у міру його проходження через кожен вузол зв'язку в мережі зв'язку з комутацією пакетів. У цьому документі іноді використовується термін "перепакетувати" або "перепакетування" для комбінації "ре-скремблювання" і "перешифрування", незалежно від того, чи дешифрується пакет спочатку перед дескремблюванням або дескремблюється перед дешифруванням. У будь-якому випадку, операції дескремблювання і дешифрування в даному вузлі повинні виконуватися в порядку, зворотному виконанню операцій скремблювання і шифрування при виході пакета з попереднього вузла, тобто, якщо пакет був скрембльований, а потім зашифрований в попередньому вузлі, то в поточному вузлі він повинен бути спочатку дешифрований, а потім дескрембльований. Як правило, пакет після цього скремблюється, а потім зашифровується, коли залишає поточний вузол.

Операція "перепакетування" в вузлі зв'язку показана на Рис. 6, де пакет даних вхідного шифротекста 1040 спочатку дешифрується з допомогою операції дешифрування 1032, а потім дескремблюється за допомогою операції дескремблювання 928 для відновлення пакета нескрембльованого текстового файлу 990, що є вмістом вихідного пакету. Якщо будь-яку інформацію в пакеті необхідно перевірити, зробити розбивку, розділити або перенаправити, незашифрований файл текстового файлу є найкращим форматом для виконання таких операцій. Потім пакет даних текстового файлу 990 знову скремблюється за допомогою операції скремблювання 926, після чого виконується нове шифрування за допомогою операції шифрування 1026 для створення нового скрембльованого пакета даних шифротекста 1043. Оскільки операція перепакетування вхідного скрембльованого пакета даних шифротекста 1040 здійснюється шляхом послідовного виконання дешифрування, дескремблювання, скремблювання і шифрування, для позначення цієї методики використовується абревіатура DUSE (англ. Decryption - дешифрування, Unscrambling - дескремблювання, Scrambling - скремблювання, Encryption - шифрування). У динамічній захищеній комунікаційній мережі та протоколі бажано, щоб стан або час, ключ дешифрування і будь-які початкові стани, використовувані для виконання операції дешифрування 1032 і операції дескремблювання 928, відрізнялися від стану або часу, початкових станів або ключів шифрування, які використовуються для виконання операції скремблювання 926 і операції шифрування 1026.

Застосування перепакетування пакетів даних в мережі SDNP описано в заявці 14/803,869 "Динамічна Захищена Комунікаційна Мережа та Протокол", на яке зроблено посилання вище. Застосування перепакетування пакетів даних в мережі зв'язку "Останньої Милі" буде описано більш детально далі в цьому розділі.

Змішування та розділення пакетів - Ще одним ключовим елементом динамічної захищеної комунікаційної мережі та протоколу, що розглядаються в цьому документі, є її здатність

розділяти пакети даних на кілька субпакетів, направляти ці субпакети по декількох маршрутах, змішувати та возз'єднувати субпакети для відновлення повних пакетів даних. Процес розділення пакетів показаний на Рис. 7А, де пакет даних 1054 розділяється за допомогою операції розділення 1051 в поєднанні з операцією алгоритмічної розбивки 1052 та з операцією додавання "сміттєвих" даних 1053, яка має можливість вставляти або видаляти сегменти, що не є даними "сміттєвих" даних. Аналогічно надлишковій ДНК, яка присутня в геномі людини, "сміттєві" сегменти даних вставляються за допомогою операції додавання "сміттєвих" даних 1053, для розширення або управління довжиною пакета даних або, при необхідності, для їх видалення. Операція додавання "сміттєвих" даних 1053 особливо важлива, коли для заповнення пакета є недостатня кількість даних. Наявність сегментів "сміттєвих" даних, вставлених в пакет даних, також ускладнює для кіберзлочинців можливість відділення реальних даних від шуму. У цьому документі "сміттєвий" сегмент даних - це пакет або сегмент даних, який цілком складається з неінформативних даних (бітів). Ці "сміттєві" біти можуть бути введені в потік пакетів даних, оточуючи реальні дані морем неінформативних бітів.

Мета операції розбивки 1052 полягає в тому, щоб розбити пакет даних 1054 на більш дрібні пакети даних, наприклад, субпакети даних 1055 і 1056 для обробки кожного зі складових компонентів. Розбиття пакета даних 1054 на більш дрібні частини дає такі унікальні переваги, як підтримка багатомаршрутної передачі, тобто передачі пакетів даних декількома різними шляхами, та полегшення унікального шифрування складових частин субпакетів з використанням різних методів шифрування.

Операція розділення може використовувати будь-який алгоритм, чисельний метод або метод розбивки. Алгоритм може являти собою статичне рівняння або включати динамічні змінні або числові початкові стани або такі "стани", як час 920 при першому формуванні вхідного пакета даних 1054 поруч субпакетів та числовий початковий стан 929, згенерований генератором початкових станів 921, який також може залежати від такого стану, як час 920 в момент створення пакета даних. Наприклад, якщо кожна дата перетворюється в унікальне монотонно зростаюче число, то кожний початковий стан 929 є унікальним. Час 920 та початковий стан 929 можуть використовуватися для ідентифікації конкретного алгоритму, обраного зі списку доступних методів, тобто з алгоритму 1050. Розділення (не змішування) пакета є зворотна операція по відношенню до змішування з використанням того ж алгоритму, що виконується в прямо протилежній послідовності по відношенню до раніше використовуваної, яка була застосована для створення конкретного пакета. В кінцевому рахунку, все, що було зроблено, скасовується, але не обов'язково за один крок. Наприклад, скрембльований зашифрований пакет даних може бути розшифрований, але залишається скрембльованим. Оброблений за допомогою операції розділення 1051 нерозділений вхідний пакет даних 1054 перетвориться в кілька пакетів даних, наприклад, розділиться на пакети 1055 та 1056 постійної довжини за допомогою операції розбивки 1052, щоб алгоритмічно виконати операцію. На діаграмі потоків даних операцію розділення пакета 1051, що включає в себе розбивку 1052 і операцію додавання "сміттєвих" даних 1053, зручно ілюструвати за використанням схематичного або символічного уявлення, позначеного тут символом операції розділення 1057.

Термін "розділення", що використовується в цьому документі, може включати в себе розбивку, яка полягає в розділенні пакета на два або більше пакета або субпакета, і крім того він може включати в себе вставку "сміттєвих" пакетів або субпакетів, в пакети або субпакети, що утворилися при "розбивці", або видалення "сміттєвих" пакетів або субпакетів з утворених при "розбивці" пакетів або субпакетів.

Зворотна функція - операція змішування пакетів 1060, показана на Рис. 7В, об'єднує кілька пакетів 1055 та 1056 в один і формує змішаний пакет 1054. Подібно розділенню пакетів, операція змішування пакетів може використовувати будь-який алгоритм, чисельний метод або метод змішування. Алгоритм може являти собою статичне рівняння або включати динамічні змінні або числові початкові стани або такі "стани", як час 920, які використовуються для задання умов, при яких змішуються пакети вхідних даних 1055 і 1056. Операція змішування, яка використовується для створення пакета даних, може використовувати числові початкові стани 929, які генеруються генератором початкових станів 921, які також можуть залежати від стану, наприклад, часу 920. Час 920 та початковий стан 929 можуть використовуватися для ідентифікації конкретного алгоритму змішування, обраного зі списку доступних методів змішування, тобто з алгоритмів змішування 1050. На схемах потоків даних цей процес змішування пакетів зручно ілюструвати за використанням схематичного або символічного уявлення, позначеного тут символом операції змішування 1061.

У відповідності до даного винаходу, змішування та розділення пакетів можуть використовувати будь-який з можливих алгоритмів. На Рис. 8 показані три з можливих способів

змішування, а саме: конкатенація, чергування і алгоритмічні методи. В процесі конкатенації послідовність сегментів пакета даних 1056 додається в кінець пакета даних 1055, при цьому утворюється змішаний пакет 1054. У процесі чергування сегменти пакетів даних 1055 і 1056 по черзі перемішуються, наприклад, як 1A, 2A, 1B, 2B і т.д., при цьому утворюється змішаний пакет даних 1065. Ще одним з методів, використовуваних для змішування пакетів, є алгоритм. У показаному прикладі алгоритм, який представляє собою віддзеркалену симетрію з чергуванням, змінює порядок проходження сегментів даних на 1A, 2A, 1B, 2B, 1C, 2C в першій половині змішаного пакета 1066 і на протилежний порядок в другій половині, тобто 2D, 1D, 2E, 1E, 2F, 1F.

Застосування змішування та розділення пакетів даних у мережі SDNP описано у вищезгаданій Заявці на патентування в США № 14/803,869, озаглавленій "Динамічна захищена комунікаційна мережа і протокол". На Рис. 9A узагальнені функціональні елементи SDNP, включаючи функції та їх зворотну дію, тобто антифункції, а також динамічні компоненти відповідних функцій, тобто стан або час виконання кожної функції в пакеті даних. Функція SDNP, що включає в себе скремблювання пакетів 926 і її антифункцію дескремблювання пакетів 928; операції фрагментації, що включають скремблювання 1057 і її антифункцію змішування 1061; операції приховування, включаючи вставку "сміттєвих даних" 1053A і видалення 1053B, а також операції шифрування 1026 і дешифрування 1032. Всі ці функції виконуються однозначно відповідно до змінних часу або стану 920.

Застосування змішування та розділення пакетів даних, а також скремблювання, дескремблювання, шифрування, дешифрування та приховування під час передачі даних у "Останній Милі" в сукупності складають операцію безпеки "Останньої Милі" SDNP. Ця операція з забезпечення безпеки "Останньою Милі" SDNP є "спрямованою", тобто операція, виконувана для і на всіх вихідних пакетах даних, відрізняється від операції, виконуваної на вхідних пакетах даних.

Операція безпеки "Останньої Милі" SDNP також є симетричною і оберненою по відношенню до "Останньою Милі", що означає, що при використанні локальних облікових даних безпеки, таких як ключі, початкові значення, загальні секрети, характерні для конкретної "Останньої Милі", операції, що виконуються з вихідним пакетом даних на пристрої клієнта, скасовуються в шлюзі SDNP, зазвичай виконуючи антифункцію, тобто математичну зворотну або будь-яку іншу операцію, що спочатку виконується клієнтом, але в зворотному порядку. Таким чином, шлюз SDNP дозволяє відновлювати вихідний вміст при підготовці до маршрутизації через хмару SDNP. Аналогічним чином, для вхідних пакетів даних на пристрій клієнта, що використовують облікові дані безпеки зони для останньої милі, операція безпеки "Останньої Милі" SDNP, виконувана на пристрої клієнта, скасовує кожну операцію безпеки, виконувану шлюзом SDNP, виконуючи анти-функцію у зворотній послідовності. Таким чином, клієнтський пристрій може відновити вихідні дані на всіх вхідних пакетах даних.

Операція із забезпечення безпеки SDNP "останньої милі" є динамічною і локалізованою, тобто прив'язаною до конкретної зони, з використанням залежних від стану умов, наприклад, місця розташування, часу і т. д. для визначення, які параметри використовувалися в момент підготовки пакета даних і для якого регіону, географії або локалі для конкретної "останньої милі". Завдяки локалізації підготовка пакетів даних, виконувана в різних регіонах і за різними з'єднаннями "останньої милі", ніколи не має однакового кодування і не використовує однакові облікові дані безпеки. Крім того, ці облікові дані безпеки "останньої милі" завжди відрізняються від облікових даних, що використовуються в "хмарі" SDNP. Більш того, будучи динамічним, стан, що використовується для створення пакетів даних, постійно змінюється, що ще більше ускладнює реальний процес забезпечення безпеки кожного пакету даних і виводить на екран не два однакових пакети даних.

Завдяки унікальному комбінованому застосуванню спрямованих симетричних обернених динамічних локалізованих операцій безпеки, характерних для кожної взаємодії з каналом "Останньої Милі", алгоритмічного застосування динамічного шифрування, динамічної фрагментації, динамічного приховування і динамічного шифрування, які використовуються згідно даного винаходу, забезпечується гіперзахищений зв'язок, який неможливо досягнути без використанні звичайних статичних методів шифрування. Повсюдне застосування динамічних методів, що діють протягом всього лише десятків мілісекунд, не тільки робить дешифрування практично неможливим, але і не дає хакеру часу для дешифрування або інтерпретації пакету даних до прибуття наступного. На практиці операції із забезпечення безпеки "Останньої Милі" SDNP можуть виконуватися з використанням програмного забезпечення, програмно-апаратних засобів, апаратної частини, спеціалізованих IC або будь-якої комбінації перерахованих вище засобів.

Хоча можливо безліч комбінацій послідовностей, один приклад операції по забезпеченню безпеки "Останньої Милі" SDNP показаний на Рис. 9B конкретно для послідовних корисних навантажень SDNP, що використовуються в одномаршрутному зв'язку "Остання Милі", тобто коли пристрій клієнта взаємодіє з одним шлюзом SDNP. Процес включає дві робочі послідовності, одну для вихідних пакетів даних, іншу для вхідних пакетів даних. У разі вихідних пакетів даних, показаних у верхній половині рисунка, дані, що "надсилаються", спочатку шифруються за допомогою операції пакетного шифрування 926, потім здійснюється приховування шляхом вставлення "сміттєвих" даних 1053A. У деяких випадках весь пакет може складатися виключно з "сміттєвих" даних, що ще більше вводить в оману спроби хакерів зібрати дані.

Потім ці пакети розбиваються на кілька частин шляхом розділення 1057, за допомогою операції парсингу 1052, і відправляються окремо на операцію шифрування 1026. Потім кожна частина шифрується за допомогою загальних або окремих ключів шифрування, а отриманий шифрований текст впорядковується в послідовне корисне навантаження SDNP, що відображається як пакет даних 1199A. Потім пакет форматується в IP-пакети даних, тобто відбувається "підготовка IP-пакета" до передачі на "Останню Лінію" і "Останню Милю". Всі операції, що виконуються, є динамічними, що відбуваються в певний час або з певним станом 920A під час виконання процесу забезпечення безпеки.

У разі вхідних пакетів даних, показаних у нижній половині рисунка, дані з "Останньої Лінії", що містять послідовне корисне навантаження SDNP 1199B, тобто "розпізнавання IP-пакета", спочатку дешифруються по частинах, або в повному обсязі, за допомогою операції дешифрування 1032 і операції змішування 1061 для відновлення реального потоку даних. Потім з пакетів вилучаються "сміттєві" дані, тобто непотрібні дані видаляються з пакетів за допомогою операції видалення "сміттєвих" даних 1053B, за якою слідує операція вилучення пакетів 928 для відновлення "отриманих даних". Всі дії, що виконуються з вхідними пакетами даних, повинні використовувати стан 920B, який використовується шлюзом SDNP при створенні пакета даних, тобто містити інформацію певного часу або з певним станом 920B при створенні пакета. Ця інформація про стан може передаватися сигнальним сервером по іншому каналу зв'язку або передаватися в пакеті вхідних даних у вигляді простого тексту або статичного зашифрованого тексту, тобто тексту, ключ дешифрування якого вже відомий операцією безпеки "Останньої Милі" SDNP. Однак відомості про стан 920B не можуть бути зашифровані за допомогою ключа, що вимагає інформацію про стан, що міститься в стані 920B, інакше код не зможе відкрити і використовувати свої власні реквізити безпеки.

Ще один приклад операції із забезпечення безпеки "Останньої Милі" SDNP показано на Рис. 9C конкретно для паралельних корисних навантажень SDNP, що використовуються в багатомаршрутній комунікації "Останньої Милі", тобто коли пристрій клієнта взаємодіє з кількома шлюзами SDNP. Як і в описаній вище одномаршрутному зв'язку, процес включає дві робочі послідовності, одну для вихідних пакетів даних, іншу для вхідних пакетів даних. У разі вихідних пакетів даних, показаних у верхній половині рисунка, дані, що "надсилаються", спочатку шифруються за допомогою операції пакетного шифрування 926, потім здійснюється приховування шляхом вставлення "сміттєвих" даних 1053C. У деяких випадках весь пакет може складатися виключно з "сміттєвих" даних, що ще більше вводить в оману спроби хакерів зібрати дані.

Потім ці пакети розділяються на кілька субпакетів шляхом операції розділення 1057, використовуючи операцію парсингу 1052, і відправляються окремо на операцію шифрування 1026. Потім кожна частина шифрується за допомогою загальних або окремих ключів шифрування, а отриманий шифрований текст впорядковуватиметься в кілька корисних навантажень SDNP, які відображаються як пакети даних 1199C, 1199D і 1199E. Потім пакети форматуються в розділені окремі IP-пакети даних, тобто відбувається "підготовка IP-пакетів" до передачі на "Останню Лінію" і "Останню Милю". Всі операції, що виконуються, є динамічними, що відбуваються в певний час або з певним станом 920C під час виконання процесу забезпечення безпеки.

У разі вхідних пакетів даних, показаних у нижній половині рисунка, дані з "Останньої Милі", що містять паралельні корисні навантаження SDNP 1199F, 1199G і 1199H, тобто "Розпізнавання IP-пакетів", спочатку дешифруються по частинах, потім використовується операція дешифрування 1032, потім операція змішування 1061 для відновлення реального пакету даних. Потім з пакетів витягуються "сміттєві" дані, тобто непотрібні дані видаляються з пакетів даних за допомогою операції видалення "сміттєвих" даних 1053D, за якою слідує операція вилучення пакетів 928 для відновлення "отриманих даних". Всі дії, що виконуються з вхідними пакетами даних, повинні використовувати стан 920D, який використовується шлюзом SDNP при створенні

пакета даних, тобто містить інформацію певного часу або з певним станом 920D при створенні пакета. Ця інформація про стан може передаватися сигнальним сервером по іншому каналу зв'язку або передаватися в пакеті вхідних даних у вигляді простого тексту або статичного зашифрованого тексту, тобто тексту, ключ дешифрування якого вже відомий операцією безпеки "Останньої Милі" SDNP.

Операція із забезпечення безпеки "Останньої Милі" SDNP не обов'язково повинна використовувати одні і ті ж алгоритми або методи як для вхідних, так і для вихідних пакетів даних. Як показано на Рис. 9D, вихідні пакети даних використовують операцію із забезпечення безпеки "Останньої Милі" SDNP 1190A, а вхідні пакети даних — операцію із забезпечення безпеки "Останньої Милі" SDNP 1190B. Посилаючись на верхню половину рисунка, вихідні пакети даних можуть містити дані, що є будь-якою комбінацією джерел даних у режимі реального часу від перетворювачів або датчиків, або можуть містити файли, створені до передачі даних.

Наприклад, звук 1198A, перетворений на електричні сигнали за допомогою мікрофона 1180, і відеосигнали з камери 1181 перетворюються на еквівалентний цифровий формат за допомогою аудіо-відео кодека 1182A. Створені формати зазвичай включають стандарти png, pic, mpeg, mov тощо, інтерпретовані та сумісні зі стандартними пристроями відповідно до Рівня 6 OSI. Використання стандартних аудіо-відео форматів дозволяє уникнути необхідності передачі пропрієтарного коду для відкриття файлу між вихідними та кінцевими адресами.

Потім похідні цифрові дані аудіо/відео кодека 1182A змішуються з текстовими даними з віртуальної клавіатури 1183 (клавіатури, реалізованої на сенсорному екрані) і з файлами даних 1179A за допомогою програми змішування контенту 1184. Ця програма змішування, у свою чергу, відправляє дані для операції із забезпечення безпеки "Останньої Милі" SDNP 1190A і надає інформацію SDNP-заголовка для операції підготовки IP-пакета 1191A з метою ідентифікації та маркування пакетів даних у режимі реального часу зі статичних файлів.

Потім операція із забезпечення безпеки "Останньої Милі" SDNP 1190A передає захищені пакети даних в операцію підготовки IP-пакетів 1191A, яка потім вбудовує корисне навантаження SDNP в IP-пакети даних відповідно до інструкцій з маршрутизації, отриманих сигнальним сервером SDNP 1603. Пакети даних можуть бути розділені в декілька IP-пакетів для багатомаршрутного зв'язку "Останньої Милі" або можуть бути об'єднані в послідовний рядок даних і вбудовані, і поміщені в один або кілька послідовних пакетів даних для єдиної лінії зв'язку "Останній Милі". Ці пакети потім передаються клієнтові PHY 1192A для додавання даних рівнів 1 і 2 для завершення IP-пакету даних.

У зворотній операції, показаній у нижній половині рисунка, дані з "Останньої лінії", отримані клієнтом PHY 1192B, передаються в операцію розпізнавання IP-пакетів 1191B, яка ідентифікує вхідні дані як дійсне повідомлення або як невідомий і потенційно шкідливий пакет даних. Дійсні повідомлення ідентифікуються за допомогою SDNP -тегів, -початкових даних, -ключів та інших ідентифікаторів, попередньо переданих клієнтському пристрою та операції розпізнавання IP-пакетів 1191B через сигнальний сервер 1603. Антропоморфічно, операція розпізнавання IP-пакетів 1191B очікує і навіть передбачає прийом дійсних вхідних пакетів даних. Несподівані пакети даних, які не мають належної ідентифікації, відкидаються і більше ніколи не відкриваються і не обробляються. Таким чином, хакер не може замаскуватися і відправити достовірні дані на будь-який вузол SDNP без попередньої реєстрації своєї особи в хмарі SDNP.

Операція розпізнавання IP-пакетів 1191B передає дійсні пакети даних до операції із забезпечення безпеки "Останньої Милі" SDNP 1190B, яка, в свою чергу, виконує всі необхідні операції з відновлення справжнього змісту пакета даних — даних, що складаються з послідовно впорядкованої комбінації відео, аудіо, текстів і файлів даних. Демультиплексор вмісту 1193, який дозволяє відновити дані після операції змішування, використовуваної при створенні пакетів даних, наприклад, відновлює послідовний файл даних, створений при операції змішування 1184 в телефоні іншого абонента, який потім використовується для відокремлення різних типів файлів. Дані, відновлені демультиплексором 1193 включають текст, що відображається у вікні месенджера 1196, файли даних 1179A і дані, надіслані в режимі реального часу аудіо-відео кодеку 1182B. Аудіо-відео кодек 1182B перетворює дані цифрового рівня презентації на живі відеозображення 1195 або через динамік 1194 на звук 1198B.

Для передачі даних "Останньої Милі" дані повинні бути введені або упаковані в багаторівневу систему організації, показану на Рис. 9E, подібну до вищезгаданої вкладеної моделі за принципом "матрьошки". Відповідно, корисне навантаження SDNP 438 являє собою транспортне корисне навантаження 437, яке разом з транспортним заголовком 436 становить корисне навантаження IP 435. Комбінація корисного навантаження IP 435 з IP-заголовком 434 являє собою IP-датаграму, еквівалентну корисному навантаженню MAC 432. Обгортання

корисного навантаження MAC 432 в MAC-заголовок 431 і нижній колонтитул MAC 433 призводить до створення "кадру" MAC, кадру, який є еквівалентом фізичного рівня 490, також відомому як вміст Рівня PHY 1, що складається з такого фізичного середовища як електричні сигнали.

У SDNP-маршрутизації MAC-заголовок 431 на Рівні 2 описує MAC-з'єднання Останньої Лінії, тобто з'єднання між клієнтським пристроєм і першим пристроєм у з'єднанні "Останньої Милі". Використовуючи вихідні та кінцеві адреси клієнтського пристрою та шлюзу SDNP, заголовок 434 на Рівні 3 визначає кінцеві точки маршрутизації через "Останню Милю". Однак, оскільки "Остання Міля" не є частиною хмари SDNP, точний маршрут, по якому проходять пакети даних в Останній Милі, не може бути чітко визначений або контролюватися. У з'єднанні "Останньої Милі" SDNP транспортний заголовок 436 на Рівні 4 визначає UDP, який використовується для корисного навантаження SDNP в режимі реального часу, а також визначає спеціально призначену адресу SDNP-порту в кожному пакеті — адресу, що змінюється динамічно для запобігання атаки опитування портів.

Корисне навантаження SDNP 438, корисне навантаження IP-пакету "Останньої Милі", містить SDNP-преамбулу 1198, що містить інформацію про зони, ключі, початкові значення, і поле даних SDNP 1199A, послідовний рядок з декількох сегментів незалежно зашифрованого шифротексту. Дешифрована форма шифрованого тексту складається з текстових файлів 1197A, 1997B і 1197C, кожен з яких містить свій унікальний SDNP-заголовок, а також відповідні дані про файли даних 91, 92 і 93. Окремі підзаголовки містять інформацію, що стосується тегів, архівів, адрес, терміновості та QoS-даних, при необхідності.

Функції преамбули і заголовків SDNP відрізняються залежно від використовуваних методів контролю і управління. У тристоронній комунікації Останньої Милі сигнальний сервер інструктує клієнтський пристрій і шлюз(и) SDNP, як взаємодіяти один з одним для здійснення дзвінка, надсилання файлу або відкриття сесії. Таким чином, інструкції передаються на обидва пристрої за допомогою пакету контролю та керування даними за допомогою TCP протоколу перш ніж відбувається передача будь-яких пакетів мультимедійних даних. Таким чином, для зв'язку "Останньої Милі" між клієнтом і шлюзом SDNP мінімально необхідними даними є теги або адреси, які використовуються для ідентифікації вхідного пакета. У деяких випадках, наприклад, якщо неможливо досягти сигнального сервера, то в альтернативному варіанті пакет даних SDNP може містити додаткові дані в заголовках і преамбулі пакета.

Пакет даних і таблиця 1177, показана на Рис. 9F, ілюструють один приклад формату, використовуваного для передачі інформації SDNP в межах корисного навантаження SDNP 438. Пакет даних включає преамбулу SDNP 1198 і від одного до восьми заголовків полів даних 1178X з відповідними полями даних "Поле Даних X". Кожному полю даних, такому як "поле даних 1", "поле даних 2" тощо, передує відповідний заголовок Hdr 1, Hdr 2 тощо і містить контент комюніке, включаючи голосові повідомлення, текст, відео, зображення, фільми, файли тощо. Кількість полів даних може варіюватися від одного до восьми відповідно до 4b довжини поля #, тобто від бінарного 0001 до бінарного 1111. Довжина преамбули SDNP 1198 і корисного навантаження SDNP 438 залежить від специфікації Поля #. Якщо вибрано лише одне поле, тобто якщо поле # = 0001 бінарне, преамбула SDNP 1198 буде містити тільки L Fld 1 (L Fld 2 за L Fld 8 буде усунуто) і корисне навантаження SDNP 438 буде включати тільки Hdr 1 і поле data 1. Якщо вибрано максимальну кількість восьми полів, тобто якщо поле # = 1111 бінарне, то преамбула SDNP 1198 буде містити вісім специфікацій довжини полів від L Field 1 до L Field 8 і корисне навантаження SDNP 438 буде включати вісім полів даних і заголовків послідовників Hdr 8, поле Data 8. Як показано в преамбулі SDNP 1198 містяться специфікації довжини поля L Fld 1, L Fld 2 і L Fld 8. Невеликий розрив між L Fld 2 і L Fld 8 призначений для того, щоб показати, що послідовність продовжується, і не являє собою розриву в даних.

Довжина кожного поля даних, визначеного в L Fld X, може варіюватися від нуля або 0B (нульове поле даних) до максимальної шістнадцяткової довжини FFFF або 65,535B. З практичних міркувань сумісності з Ethernet, максимальна довжина пакета даних для будь-якого поля переважно обмежена 1500B або шістнадцятковим 05DC, а загальна довжина всіх полів даних не повинна перевищувати розмір пакета в 9000B або шістнадцятковий 2328. Вказана довжина кожного поля даних може змінюватися незалежно один від одного. Довжина нульового поля, наприклад, де L Fld 8=0000 шістнадцяткове, призводить до вилучення відповідного поля даних 8, але не до вилучення відповідного заголовка Hdr 8. Заголовки вилучаються лише за специфікацією Поля #.

Згідно з цим протоколом SDNP розділення контенту по різних полях даних є надзвичайно гнучким. Дані, що направляються в один пункт призначення, можуть міститися в межах одного поля даних або в цілях приховування можуть бути розділені на кілька полів даних і об'єднані з

непотрібними даними. Розмір полів даних може змінюватися незалежно один від одного. Поля даних також можуть містити лише "сміттєві" дані або можуть бути створені цілі пакети даних, що містять лише "сміттєві" дані. Однак для ефективної пакетної маршрутизації дані, призначені для різних місць призначення, повинні бути розділені на окремі поля даних, кожне з яких має свої унікальні заголовки.

Формат пакета SDNP можна застосувати для наскрізної передачі даних по всій мережі SDNP, включаючи кілька хмар та зон, таких як хмара SDNP або канал комунікації Остання Миля. Хоча вміст пакетів даних SDNP змінюється в міру їх переміщення по мережі, формат пакетів SDNP залишається незмінним. Оскільки цей формат включає мінімальні накладні витрати на передачу даних, формат пакетів даних SDNP однаково підходить для великих робочих навантажень або для важливої комунікації в режимі реального часу. Формат пакета підходить для двонаправленого потоку даних, тобто для потоку даних з Останньої Милі в шлюз SDNP і через хмару SDNP, або навпаки, для доставки пакетів даних, що виходять з хмари SDNP для транспортування через Останню Милю на клієнтський пристрій.

У процесі роботи напрямок маршрутизації даних SDNP визначається Мережевим джерелом Рівня 3 та адресами призначення, описаними в IP-заголовку 434 на Рис. 9E. Кожен пакет завантажується зі своїми адресами джерела і призначення, тоді як медіа-вузол готує пакет до передачі на наступний медіа-вузол за його маршрутом. У триканальному зв'язку SDNP або IP-адреса призначення пакета доставляється від сигнального сервера до медіа-вузлів у вигляді пакету контролю і управління (C & C) перед підготовкою вихідних пакетів. Загалом, сигнальний сервер здатний відправляти інструкції контролю і управління на кожен вузол комунікаційного шляху, включаючи як передавальні (викликаючі), так і приймаючі (отримуючі) пристрої. Якщо доступний тільки одноканальний зв'язок, наприклад, у з'єднанні з тривалими затримками поширення, сигнальний сервер не може заздалегідь попередити медіа-вузол вхідного пакета що з ним робити. У цьому випадку адреси маршрутизації передаються в пакеті вхідних даних у корисному навантаженні SDNP 438. У таких випадках медіа-сервер слідує встановленими за замовчуванням інструкціями про те, як обробляти вхідний пакет, використовуючи поля даних, що містяться у вхідному пакеті SDNP, включаючи маршрутизацію та інформацію про стан, а також облікові дані безпеки.

Корисне навантаження 438 складається з двох частин: частини, що призначена для читання, що включає преамбулу 1198, і частини, що не підлягає читанню 1199a, що містить дані в "прихованій формі". Вміст цього пакета може використовувати будь-яку кількість методів приховування для маскування його вмісту, таких як шифрування, скремблювання, і, можливо, використання "сміттєвих" даних. Використовуваний метод приховування повинен бути обернений у вихідне положення, щоб витягти корисний вміст 1197a, 1997b і 1197c. Ці пакети містять адреси призначення майбутніх вихідних пакетів. Адреси існують тільки в нескритій або розшифрованій формі протягом короткого проміжку часу, перш ніж можна буде підготувати і зашифрувати наступні пакети.

Як описано, преамбула SDNP 1198 містить інформацію, що відноситься до всього пакету. Крім специфікацій полів даних, Рис. 9F ілюструє преамбулу SDNP 1198 і включає зону SDNP, в якій був створений SDNP-пакет, наприклад, зону U1, два цифрових початкових значення і дві ключі. Ці ключі та початкові значення можуть використовуватися як спеціальні облікові дані безпеки для зон у процесі скремблювання/дескремблювання, додавання/видалення "сміттєвих" даних, процесів змішування/розділення та шифрування/дешифрування. Початкові значення та ключі можуть використовуватися в якості унікального засобу доставки облікових даних, необхідних для відкриття і читання полів даних, або в поєднанні з пакетами контролю і управління, що відправляються на пристрій клієнта і на шлюз SDNP з сигнального сервера, мережі контролюючих і керуючих комп'ютерів, які не беруть участь у передачі вмісту повідомлень в пакетах даних.

Початкові значення і ключі можуть бути безпечно доставлені у відкритій формі, тобто в незашифрованому вигляді, оскільки дані не містять необхідної для їх використання інформації — вони становлять лише частину облікових даних безпеки. Інші частини облікових даних безпеки, які відсутні, можуть бути відправлені раніше в іншому пакеті даних або можуть містити загальні секрети алгоритмів, таблиці пошуку і коди, не доставлені по мережі і що не є частиною повідомлення. Ключі шифрування можуть бути симетричними, коли і відправник, і одержувач мають ключ, або відкритими ключами, коли декілька сторін, включаючи відправника, мають доступ до ключа шифрування, але тільки одержувач, тобто сторона, що генерує ключ шифрування, має ключ дешифрування. Більш того, всі облікові дані безпеки обмежені певною зоною безпеки, наприклад, U1, і є динамічними, обмеженими певним часом або станом, термін дії яких закінчується, якщо вони не використовуються протягом певного часу. Якщо поля даних

ключів і початкові значення не використовуються в якості облікових даних безпеки, наприклад, оскільки сигнальний сервер самостійно інструктує пристрої SDNP щодо операцій безпеки, то ці поля можуть бути заповнені цифровими значеннями, які видаються за ключі шифрування, помилково направляючи зловмисника на аналіз помилкового ключа безпеки, змушуючи витрачати час даремно.

У комунікації "Останньої Милі" проміжні маршрутизатори між пристроєм клієнта і шлюзом SDNP не обробляють, не розшифровують і не відкривають пакети даних, що передаються, оскільки вони не є частиною мережі SDNP і не можуть виконувати запити або інтерпретувати дані всередині пакета SDNP. Замість цього всі операції з забезпечення безпеки виконуються виключно в двох кінцевих точках — клієнті SDNP і шлюзі SDNP, оскільки тільки ці пристрої працюють як вузли зв'язку SDNP. Оскільки кожна кінцева точка динамічно виконує протоколи SDNP, комунікація "Останньої Милі" є гіперзахищеною протягом всієї Останньої Милі. Якщо інший абонент також використовує програмне забезпечення SDNP, то "Остання Миля" другого абонента також захищена вищезгаданими методами SDNP, і гарантується наскрізний гіперзахищений зв'язок — від одного абонента до іншого.

Однак якщо кінцевий пристрій не є клієнтом SDNP, то найближчий до викликаючого пристрою маршрутизатор, тобто маршрутизатор Останньої Лінії, може бути оснащений SDNP, і Остання Лінія може бути досить захищена від спеціальних функцій виконуваних SDNP-маршрутизатора, навіть якщо вона і не оснащена SDNP. Цей альтернативний метод захисту Останньої лінії більш детально описаний у наступних розділах документа і не буде розглядатися в даному розділі. Описаний метод, хоча і застосовний для забезпечення безпеки комунікації Останньої Лінії, але не достатній для захисту інших частин Останньої Милі.

Повертаючись до Рис. 9F, можна помітити, що кожне поле даних SDNP супроводжується заголовком поля даних SDNP 1178X, що містить інформацію, унікально застосовну до відповідного поля даних, але не корисну для інших полів даних. Зокрема, в даному винаході кожен заголовок містить поле типу даних, що описує, які дані містяться у відповідному полі даних, поле адреси призначення, що використовується для ідентифікації конкретного поля даних і його призначення, поле зони, що використовується для перенесення інформації про зону з однієї зони в іншу, а також інформацію про терміновість і доставку. Як показано на рисунку, кожне корисне навантаження SDNP 438 містить одну преамбулу SDNP 1198 і один або кілька заголовків полів даних SDNP 1178X і відповідні поля даних X, де X описує кількість окремих корисних навантажень, яка може коливатися від 5 до 50 залежно від розміру і терміновості цих корисних навантажень.

Хоча сигнальний сервер може надати більшу частину описаної інформації клієнту SDNP і шлюзу SDNP, одним з фундаментальних компонентів обов'язково переданих пакетом даних Останньої Милі є "поле адреси" або тег, необхідний для ідентифікації цього пакета даних. Поле, яке називається адресою призначення корисного навантаження SDNP (на рисунку "Адреса Призначення"), може містити будь-який унікальний ідентифікатор, достатній для розпізнавання ідентифікатора одного поля даних від іншого. Його призначення аналогічне функції штрих-кодів, використовуваних для маркування і відстеження багажу в аеропорту або пакунках, що відправляються кур'єром. Типи адрес можуть включати, наприклад, цифрові теги, SDNP zip-архіви, IPv4 або IPv6 адреси, NAT адреси або навіть POTS номер телефону, якщо ідентифікатор є унікальним для запобігання конфліктів при ідентифікації пакета даних. Розмір поля адреси залежить від типу вибраного типу адреси.

Для збереження анонімності пакетів під час маршрутизації краще використовувати конфіденційні коди, такі як поштовий індекс SDNP як адреси призначення SDNP, а не використовувати справжні номери телефонів або IP адреси. При роботі, щоразу, коли пакет даних від клієнта SDNP надходить на шлюз SDNP, корисне навантаження SDNP дешифрується, а потім кожен заголовок поля даних перевіряється на предмет визначення адреси призначення. Перед тим, як перевірити заголовок пакета даних, пакет даних повинен бути дешифрований або оброблений, щоб скасувати методи приховування, використані при створенні цього пакета. У випадку двоканального або триканального з'єднання, як показано на Рис. 9G, сигнальний сервер 1603 попередньо проінформував шлюз SDNP про плановане прибуття пакета даних і його відповідне ідентифікаційне маркування та облікові дані безпеки. Таким чином, коли шлюз SDNP отримує пакет даних 438A, що включає в себе передачу даних "Останньої Милі" від клієнта SDNP, шлюз виконує операцію безпеки "Останньої Милі" SDNP 1190D для перетворення корисного навантаження SDNP з шифрованого тексту в простий текстовий пакет даних 438B. Операція безпеки описує обробку вихідного пакета даних для приховування його вмісту і процес модифікації вхідного пакета даних для розкриття його вмісту. Зокрема, операція безпеки, що виконується над вхідним пакетом даних, використовується для відновлення його

вмісту шляхом скасування операцій приховування, що виконуються над ним перед транспортуванням, включаючи використання дешифрування для скасування шифрування, дескремблювання для скасування скремблювання, скасування операції вставки "сміттєвих" даних для видалення "сміттєвих" даних і змішування для скасування розділення. Ці процеси виконуються відповідно до стану та зони пакету даних на момент його створення. Для вихідних пакетів даних операція безпеки полягає в приховуванні вмісту пакету даних перед транспортуванням шляхом виконання шифрування, скремблювання, вставки "сміттєвих" даних і розділення пакета відповідно до стану і зони пакета даних на момент його створення. Незашифрованими початковими значеннями і ключовими полями даних у пакеті даних 438A можна знехтувати або, за бажанням, використовувати у поєднанні з інформацією сигнального сервера для дешифрування зашифрованого тексту. У результаті операції відкривається поле даних 1 і пов'язаний з ним заголовок поля даних 117D з позначкою Hdr 1, що містить адресу призначення поля даних, тип даних, терміновість та інформацію про доставку. У таких випадках адреса призначення — це не адреса маршрутизації, а тільки код маршрутизації SDNP, тобто тег, який використовується для ідентифікації пакета, який є частиною конкретної комунікації.

Після того, як певне поле даних виявило ідентифіковану адресу призначення, наприклад, код маршрутизації SDNP, що відповідає інструкціям сигнального сервера 1603, поле даних витягується, опціонально змішується з іншим пов'язаним вмістом мікшером 1184Z і перепакетується в нову IP- або SDNP-датаграму за допомогою операції підготовки 1191Z для доставки до наступного місця призначення. Новий пакет даних, що спрямовується в хмару, включає заголовок SDNP 434Z, що містить призначення нового пакета і зміст даних, корисне навантаження SDNP 435Z. Одержувач, що постачається сигнальним сервером 1603 на шлюзовий мультимедійний вузол у вигляді IP-адреси або SDNP-адреси, може складатися з іншого сервера SDNP, що працює в якості хмарного вузла SDNP, або може включати в себе передачу даних "Останньої Милі" іншому SDNP клієнту. У таких випадках триканального з'єднання адреса призначення насправді є не адресою, а засобом ідентифікації пакета, де його наступне призначення вже відоме шлюзу SDNP. У разі, коли призначення пакета призначене для хмарної маршрутизації SDNP, пакет даних обробляється хмарною операцією безпеки SDNP 1190Z відповідно до облікових записів Z1 для хмари, а не обліковими записами U1, що використовуються в "Останній Милі".

При одноканальному зв'язку, як показано на Рис. 9H, сигнальний сервер не може повідомити шлюзу SDNP заздалегідь про майбутнє прибуття пакета даних і його полів даних, або тому, що (i) в локальній мережі немає сигнального сервера, (ii) сигнальні сервери тимчасово відключені, або (iii) сигнальний сервер занадто зайнятий і не в змозі заздалегідь маршрутизувати пакети в часі. У таких випадках пакет даних від клієнта SDNP повинен містити необхідні повноваження безпеки Зони U1, Початкового значення 1, Початкового значення 2, Ключа 1 і Ключа 2 для дешифрування пакета даних за допомогою операції безпеки "Остання Миля" SDNP, що перетворює зашифрований пакет даних 438A в простий текстовий пакет даних 438B. Стандартний формат пакета даних SDNP резервує ці поля даних, навіть якщо вміст поля не потрібен конкретним медіа-вузлам. Наприклад, якщо конкретний процес маскування, який використовується для створення пакета даних, не використовує поле Ключ 2, дані в цьому полі безглузді і не використовуються вузлом призначення. Тим не менш, пакет даних резервує однакову кількість байт для використовуваного або не використовуваного поля, так що всі пакети даних SDNP мають однорідний формат. Після дешифрування шифрованого тексту в пакеті даних 438A, шлюз SDNP витягує вміст поля пакета даних 1 і пов'язаного з ним заголовка поля Hdr 1 1178D з пакета простих текстових даних 438B. З цього пакета даних процес розпізнавання IP-пакетів 1191D об'єднує поля даних типу A і адресу призначення з заголовка поля Hdr 1 1178D з двох причин — по-перше, в триканальному зв'язку для підтвердження очікуваного вхідного пакета, і, по-друге, для створення нової адреси SDNP. Ця нова адреса SDNP об'єднується з полями Тип D, Терміновість і Доставка і обробляється операцією підготовки пакета SDNP 1191Z для створення заголовка SDNP 434Z в пакеті вихідних даних. Вміст поля даних 1 також витягується з вхідного текстового пакета даних 438B, і його вміст опціонально змішується 1184Z з іншим вихідним вмістом для створення вихідного корисного навантаження SDNP 435Z. Потім пакет обробляється хмарною системою безпеки SDNP 1190Z при підготовці до пересилання. Таким чином, адресне поле виконує декілька функцій, як для ідентифікації вхідного пакета даних, так і для надання адреси пересилання при необхідності.

Якщо медіа-вузол отримує пакет даних без попередніх інструкцій від сигнального сервера, то медіа-вузол повернеться до інструкцій за замовчуванням про те, як обробляти вхідний пакет даних і як готувати вихідні пакети даних. Якщо медіа-вузол не містить інструкцій з обробки неоголошених вхідних пакетів, то пакет даних буде відкинуто. Якщо медіа-вузол володіє

інструкціями про те, як обробляти невпізнані пакети, то медіа-вузол спочатку підтвердить відповідно до облікових даних безпеки, що пакет є дійсним SDNP пакетом, і обробить його відповідним чином. Однак, якщо відправник не може бути ідентифікований, наприклад, якщо код шифрування, початкові значення або вихідна адреса недійсні, то пакет буде відкинуто як шкідливий.

Повертаючись до Рис. 9F, пакетне поле з позначкою "Зона Поля" описує зону, в якій було створено певне поле, тобто чи здійснювалося минуле шифрування або скремблінг, наприклад, з налаштуваннями зони U1 або U2. У разі вкладених протоколів безпеки або інших методів приховування вкладених даних, для дескремблювання, дешифрування або скасування приховування пакета даних потрібна додаткова інформація, наприклад, ключ, початкові значення, час або стан, то в цьому випадку поле пакета з позначкою "Інше Поле" може бути використано для передачі інформації про конкретне поле. Зазвичай ці поля не використовуються, за винятком вкладених протоколів безпеки, наприклад, коли зашифроване поле даних потім шифрується або зашифровується вдруге. Необхідно дотримуватися обережності при використанні вкладених методів безпеки для відновлення даних в точному зворотному порядку підготовки пакету даних, інакше вміст буде втрачено назавжди.

Пакетне поле з позначкою "Тип даних", якщо воно використовується, полегшує маршрутизацію в залежності від контексту, розрізняє дані, відео, текстові та комп'ютерні файли, що не потребують зв'язку в реальному часі з пакетами даних, що містять конфіденційну інформацію, таку як голос і відео в реальному часі, тобто розрізняє маршрутизацію в реальному часі від даних, які не належать до реального часу. Типи даних включають голос, текст, відео в реальному часі, дані, програмне забезпечення тощо.

Пакетні поля з позначками "Терміновість" та "Доставка" використовуються разом для визначення оптимальної маршрутизації даних у певному полі даних. Терміновість включає в себе категорії "Повільна", "Нормальна", "Пріоритетна" і "Термінова". Доставка включає в себе різні QoS-маркери для нормальної, надлишкової, особливої та VIP-категорій. В одному із втілень цього винаходу двійковий розмір різних полів даних, як показано в таблиці 1177, вибирається для мінімізації необхідної смуги пропускання. Наприклад, поля даних, як показано, можуть мати діапазон від 0 до 200B, при цьому вісім полів даних по 200B на одне поле даних означають, що пакет SDNP може містити 1600B даних.

І Рисунок 9G, і Рисунок 9H ілюструють випадок, коли клієнтський пристрій посилає пакети даних в зоні U1 через "Останню Милю" до вузла шлюзу. Потім вузол шлюзу обробляє вхідні пакети даних, щоб скасувати використовувані методи захисту і приховування "Останньої Милі", використовуючи облікові дані безпеки зони U1. Вузол шлюзу може потім змішувати вміст пакета з вмістом інших пакетів у процесі змішування 1184Z для створення нового пакета (або пакетів), пов'язаного для передачі через SDNP хмару, використовуючи облікові дані безпеки Зони Z1.

Подібний процес використовується, коли шлюз SDNP отримує пакет даних з хмари (включаючи інший шлюз) і відправляє пакет даних на клієнтський пристрій, наприклад, з хмари SDNP на телефон клієнта (викликаного). Як показано на Рис. 9I, при двоканальній або триканальній комунікації сигнальний сервер 2603 раніше повідомляв шлюзу SDNP про плановане прибуття пакета даних і його відповідне ідентифікаційне маркування та облікових даних безпеки, що надходять з хмари. Таким чином, коли шлюз SDNP отримує пакет даних 2438A з хмари SDNP, шлюз виконує операцію безпеки хмари 2190D SDNP з метою перетворення корисного навантаження SDNP з шифрованого тексту в простий текстовий пакет даних 2438B. Незашифрованими початковими значеннями і ключовими даними в пакеті даних 2438A можна знехтувати або, за бажанням, використовувати в поєднанні з інформацією сигнального сервера для дешифрування зашифрованого тексту. Використання полів даних залежить від алгоритмів, що використовуються для приховування корисного навантаження пакета. Наприклад, якщо шифрування не використовується, поля, що містять ключі шифрування, ігноруються.

У результаті операції вилучається ряд полів даних. Подальша операція розбиває ці поля даних в операції розділення вмісту 2184Z для вилучення специфічного вмісту, що складається з поля даних 1 і пов'язаного з ним заголовка поля даних 2117D з позначенням Hdr 1 за допомогою операції розпізнавання 2191D. Заголовок Hdr 1 містить адресу призначення поля даних, тип даних, терміновість та інформацію про доставку. Потім вилучене поле даних перегортається в нову IP- або SDNP-датаграму за допомогою операції підготовки SDNP-пакета 1191Z для доставки до наступного місця призначення. Новий пакет даних, що направляється в хмару, включає в себе заголовок SDNP 2434Z, що містить пункт призначення нового пакета (IP-адреса, що відповідає номеру телефону людини) і вміст даних, корисне навантаження SDNP 2435Z. Вихідний пакет потім обробляється операцією безпеки SDNP "Останньої Милі" 2190Z

відповідно до облікових даних безпеки зони U1 для "Останньої Милі", а не обліковими даними зони Z1, використовуваними в "хмарі".

Якщо сигнальний сервер недоступний, тобто при одноканальному зв'язку, то медіа-вузол повинен обробляти вхідний пакет даних, використовуючи інструкції, раніше доставлені в якості інструкції за замовчуванням. У таких випадках вхідний пакет даних перевіряється за критеріями, необхідними для підтвердження того, що відправник є дійсним клієнтом SDNP (таким як код маршрутизації SDNP або код автентифікації, доставлений раніше у вигляді заздалегідь визначеного загального секрету). Якщо пакет визначається як дійсний, пакет обробляється згідно з інструкціями за замовчуванням. Якщо ні, то пакет відкидається.

Вищевказані методи приведені в якості прикладу та не призначені для обмеження обробки та маршрутизації пакетів даних до певного формату пакету даних.

Безпека і конфіденційність при комунікації

Важливим міркуванням у зв'язку "Останньої Милі" є здатність мережі підтримувати як безпечне, так і приватне спілкування. Хоча конфіденційність і безпека часто асоціюються, вони не є однаковими. Безпека, як термін використовуваний в області комунікацій, розглядається як "дисципліна для запобігання несанкціонованого доступу до комунікаційних даних у впізнаваній формі". Безпека, однак, не поширюється на випадки, коли окрема особа або установа має право доступу до повідомлення або контролю за ним. Конфіденційність визначається як "стан або умова свободи від спостереження або посягань з боку інших людей і свободи від суспільної уваги". З юридичної точки зору конфіденційність визначається як право людини контролювати доступ до своєї особистої інформації.

При спілкуванні, права людини на недоторканність приватного життя щодо голосових дзвінків, відео, текстових повідомлень, електронної пошти, особистих повідомлень і т. д. сильно розрізняються в різних країнах. Роль у дотриманні відповідних урядових постанов для забезпечення юридично дійсного доступу до зв'язку розглядається в одному з наступних розділів. Крім цього, ідеальна мережа і комунікаційна система повинні бути здатні запобігати злому зв'язку, тобто вона повинна бути абсолютно безпечною, і всі комунікації повинні бути захищені тільки для тих, хто має право знати, тобто повинні бути конфіденційними.

При оцінці можливостей забезпечення конфіденційності та безпеки мережі необхідно ретельно враховувати параметри мережі "Останньої Милі" та підключених до неї пристроїв. Залежно від облікових даних безпеки, що використовуються для встановлення прав доступу до інформації, "Остання Миля" і підключені до неї пристрої часто визначають безпеку і конфіденційність мережі, тобто "Остання Миля" являє собою найслабшу ланку. Необхідно розглянути чотири можливі комбінації комунікаційних мереж:

- Безпечні та приватні мережі. З індивідуальної точки зору, цей випадок являє собою ідеальну продуктивність мережі, яка забезпечує як безпеку інформації, так і конфіденційність для користувача. У своєму крайньому прояві, дійсно безпечна приватна мережа означає, що будь-яка людина, уряд, агентство або корпорація не може ні перехопити критично-важливу комунікацію, ні отримати особисті дані про поведінку, дії, контакти і партнерів, особисті уподобання і діяльність людини тощо. Хоча захисники прав на недоторканність приватного життя вважають ідеалізовану захищену приватну мережу золотим стандартом у конфіденційній комунікації, уряди, організації з безпеки і корпорації розглядають абсолютну автономію в спілкуванні як проблему, що дозволяє людям займатися злочинною діяльністю і тероризмом з абсолютною секретністю і безкарністю.

- Незахищені мережі, в яких відсутня конфіденційність. Мережа, яка не захищена і не має положень про конфіденційність (наприклад, сьогодні це OTT інтернет-провайдери), являє собою серйозний ризик для будь-якої особи, групи, клубу, компанії або уряду, що використовує канал зв'язку. Оскільки кіберзлочинець може легко отримати доступ до викликів і даних, будь-яке злочинне угруповання може використати цю інформацію для будь-яких цілей за своїм вибором. Для зловмисників і спамерів небезпечні канали зв'язку можуть послужити закликом до активних дій, наповнення мереж спамом, ініціювання атак типу "відмова в обслуговуванні" і створення руйнівної шкоди. Для ідеологів, політичних активістів і релігійних культів небезпечна комунікація може бути використана для витоку конфіденційної інформації, щоб прискорити політичні зміни, дискредитувати державних чиновників, стимулювати заворушення або навіть повалити уряди (див. історичний художній фільм "П'ята влада" (DreamWorks © 2013) як, наприклад, хроніки витоку великої кількості конфіденційної дипломатичної інформації з WikiLeaks, за яким відбулась серія міжнародних скандалів). Для фінансово мотивованих кіберзлочинців, таких як ті, хто пов'язаний з організованою злочинністю і мафією, напади зосереджені на грошових злочинах, таких як крадіжка, помилковий переказ коштів, шахрайство, розкрадання особистих даних, відмивання грошей, вимагання, шантаж та інші злочини. Для тих, хто причетний до

страху і залякування, таких як наркокартелі, банди і терористи, небезпечний зв'язок може відслідковуватися для відстеження місцезнаходження, пересування і дій їхніх конкурентів, ворогів і жертв з метою планування і здійснення насильницьких злочинів, таких як напади, викрадення, вбивства, вибухи або акти тероризму. Нарешті, у разі особистих кібератак незахищені комунікації можуть бути використані для незаконного злому баз даних, що містять особисту інформацію фізичних осіб, включаючи номери соціального страхування, паспорти, банківську інформацію, інформацію кредитних карт, медичні картки та іншу конфіденційну особисту інформацію.

- Безпечні мережі, в яких відсутня конфіденційність. Приклади безпечних мереж, в яких відсутня конфіденційність, зазвичай включають корпоративні облікові записи, в яких менеджер з IT (Інформаційних Технологій) або відділ безпеки мають право і повноваження контролювати всі корпоративні комунікації, щоб гарантувати, що в мережі компанії не відбувається неналежного або незаконного спілкування. Незважаючи на те, що мережа захищена від хакерів і кіберзлочинців, комунікації в такій мережі не є приватними і можуть відстежуватися уповноваженими агентами для виявлення порушень, включаючи несанкціоноване особисте використання комунікаційної інфраструктури компанії, корпоративне шпигунство, порушення угод про конфіденційність, несанкціоноване розкриття інтелектуальних прав (ІП витік), сексуальне насильство, порушення положень про прозоре розкриття інформації (Regulation Fair Disclosure), інсайдерську торгівлю, підкуп, порушення FCPA (корупційних дій за кордоном). У корпоративних комунікаціях при вступі в компанію фізична особа інформується про те, що її корпоративні комунікації не є приватними і можуть контролюватися, включаючи телефонні дзвінки, електронну пошту, текстові повідомлення, особисті повідомлення та SMS, а також інші комюніке. У разі судових розглядів, будь то цивільних або кримінальних, ці комюніке також можуть бути викликані до суду і представлені як докази, навіть якщо особиста інформація змішується з корпоративною інформацією. По суті, якщо співробітник компанії використовує комунікації, пристрої та мережі компанії для особистого користування, то (за винятком випадків адвокатської таємниці) вся інформація є законною і не повинна розглядатися як приватна. З цієї та інших причин змішане використання особистих месенджерів, таких як Line і KakaoTalk, в ділових і особистих цілях особливо проблематично, оскільки співробітник не може посилатися на право на конфіденційність для запобігання перегляду своїх текстових чатів, зображень і файлів.

- Квазі-приватні, незахищені мережі. Квазі-приватна небезпечна мережа — це мережа, в якій можна зламати дані, наприклад, прослуховуючи розмови, але приватні операції можуть здійснюватися конфіденційно, незважаючи на відсутність безпеки при дотриманні певних умов. Таким чином, конфіденційність встановлюється шляхом підтвердження особи (або осіб), хто телефонує різними способами з використанням загальних секретів, що не виявляються навіть хакером, який перехопив виклик. Поширеним прикладом незахищеного приватного спілкування є голосова банківська операція. Той, хто дзвонить, підтверджує свою особу, відповідаючи на ряд постійно змінних запитань, на які самозванець навряд чи дізнається відповіді, наприклад, "Ми бачимо, як ви вечеряли минулої ночі і платили кредитною карткою". Чи не могли б ви сказати, в якому місті ви вечеряли? " Або: "Ви отримуєте регулярні рахунки від виноробні. Що це за виноробня?" Інший приклад питання: "Чи не могли б ви назвати мені прізвище вашого улюбленого вчителя початкової школи?" Для того щоб ці методи перевірки особи працювали, банк повинен або мати доступ до закритої інформації (такої як виписки з кредитних карток), або банк і його клієнти повинні встановити сукупність загальних секретів при відкритті рахунку, як правило, особисто, а не в електронній формі. Після встановлення особи клієнт може дати вказівку установі вчинити певні дії, які не принесуть користі кіберзлочинцю. Наприклад, "будь ласка, переведіть 10 000 доларів з моїх заощаджень на мій розрахунковий рахунок". Однак, якщо переказ грошових коштів здійснюється в інший банк, необхідно провести ще більш сувору перевірку, щоб забезпечити конфіденційність клієнта. У будь-якому випадку, недоторканність приватного життя залежить від виконання умови, що повідомлення не може розкривати загальні секрети ні в електронному, ні в усній формі, в іншому випадку вся конфіденційність буде втрачена і облікові записи можуть опинитися під загрозою. Як таке, автентифіковане повідомлення на незахищеній лінії називається квазі-приватне повідомлення, що означає умовну конфіденційність. Інший приклад або квазі-приватна комунікація по незахищеній мережі може бути здійснена з використанням токена безпеки — пристрою, випущеного банком, який належить тільки клієнту. Квазі-випадковий номер, що генерується пристроєм, повідомляється оператору банку, який підтверджує, що номер збігається з авторизованими номерами банку. Оскільки число становить 8 і більше цифр, шанс вгадати правильний код в перший раз малоймовірний. Якщо надходить повідомлення про неправильний номер токена, дзвінок

переривається, рахунок блокується, а відділ боротьби з шахрайством повідомляється про необхідність проведення розслідування. У будь-якому випадку, важливість забезпечення конфіденційності в незахищеній мережі залежить від можливості спілкуватися без розголошення будь-яких конфіденційних даних, таких як номери рахунків, PIN-коди, дані кредитних карт і т. д…

Перевірка особи і протокол AAA (Аутентифікація, Авторизація, Адміністрування) - Концепція безпеки і конфіденційності заснована на точній і надійній перевірці особи, тобто на тому, що той, хто телефонує, є тим, за кого себе видає. Перевірка справжності, також відома як "автентифікація", важлива для забезпечення правильного використання даних і зв'язку, а також для запобігання незаконного або несанкціонованого доступу. Надійна перевірка особи має важливе значення для національної безпеки, правозастосування, права власності ІП, підприємств та індивідуальних прав. Приклад важливості перевірки особи включає наступне:

- Для національної безпеки країни, перевірка особи, яка телефонує, важлива для відстеження особи злочинців, шпигунів, терористів, наркоторговців і всіх, хто розголошує національну таємницю або загрожує національній безпеці. Не менш важливо вміти ідентифікувати осіб, які мають право доступу, читання або відправки конфіденційних, секретних або цілком секретних комюніке, даних і файлів.

- Для правоохоронних органів перевірка особи, яка телефонує, важлива для виявлення осіб або організацій, причетних до злочинної діяльності, такої як грабежі, підпали, незаконний обіг наркотиків, контрабанда, проституція і торгівля людьми, вимагання, шантаж та інші злочини. Не менш важливо вміти ідентифікувати осіб, які є уповноваженими співробітниками правоохоронних органів, включаючи поліцію, пожежників, парамедиків, рейнджерів, маршалів авіації, адміністрації транспортної безпеки і безпеки аеропортів, портові влади, митницю і служби берегової охорони.

- Для власників ІП, таких як кіностудії, ідентифікація особистості важлива для ідентифікації осіб, організацій і установ, що займаються піратством і несанкціонованим розповсюдженням матеріалів, захищених авторським правом, таких як музика, фільми, книги, відео тощо. Це також важливо для підтвердження законного і дійсного розповсюдження матеріалів ІП і матеріалів, захищених авторським правом.

- Для комерційних підприємств перевірка особи їх співробітників важлива для відстеження навмисного або випадкового розголошення критичної внутрішньої інформації, виявлення осіб, які займаються комерційним шпигунством, виявлення осіб, причетних до незаконного розголошення інтелектуальної власності, та осіб, які вчиняють інші злочини, такі як шахрайство або використання корпоративного зв'язку в особистих цілях. Не менш важливо підтвердити особу тих, кому доступна конфіденційна інформація компанії, щоб індивідуально налаштувати права доступу з уточненням до яких саме типів даних вони мають. Наприклад, інженерний відділ компанії не повинен мати доступу до кадрового обліку відділу маркетингу, щоб порівняти, скільки платять маркетинговим співробітникам.

- Для приватних осіб перевірка особи важлива для забезпечення "конфіденційності" того, хто дзвонить, підтверджуючи, що особа або особи, з якими ви спілкуєтеся, не є самозванцями.

Таким чином, роль перевірки особи полягає в підтвердженні особи людини, тобто в посвідченні того, ким вона себе видає, а також в ідентифікації, блокуванні і, в кінцевому рахунку, затриманні осіб, які вводять в оману щодо своєї особи. Автентифікація — це перша буква "A" в моделі безпеки потрійне-A, або AAA, що означає "Автентифікація, авторизація і адміністрування". Для перевірки особи людини і автентифікації її облікового запису в системі можуть використовуватися численні методи, такі як PIN-код, паролі, відбитки пальців, токени і методи відповіді на запити.

Після автентифікації дійсна особа користувача потім використовується для визначення прав і привілеїв доступу до комюніке, даних, файлів, роботи системи тощо. Ці привілеї і права доступу в сукупності називаються "авторизацією" користувача, що надається системою, тобто авторизований користувач може отримати доступ тільки до тих комунікацій, даних, файлів і системних функцій, для яких він авторизований. Тому авторизація є синонімом "привілеїв" або "доступу".

Третя літера "A" в AAA означає "адміністрування". Адміністрування — це ведення обліку авторизованого доступу до мережі і файлів, наприклад, для цілей виставлення рахунків за користування, а також для відстеження і повідомлення про спроби несанкціонованого доступу до мережі, файлів і роботи системи. Адміністрування також відіграє важливу роль у відстеженні змін в облікових даних безпеки, PIN-кодах, паролях і т. д., необхідних для операції автентифікації.

Здатність мережі виконувати операції протоколу AAA має першорядне значення для забезпечення конфіденційності та запобігання компрометації мережі з боку несанкціонованих користувачів або операторів мережі. Будь-яка мережа, нездатна забезпечити ідентифікацію особи своїх користувачів, може бути пошкоджена в незаконних цілях. Пошкодження мережі несанкціонованими користувачами неминуче створює проблеми при спілкуванні за допомогою OTT, оскільки не існує ніяких засобів для підтвердження особи викликаючого абонента. Несанкціонований доступ і мережева комунікація з боку невпізнаних користувачів, тобто анонімність, являють собою значний ризик у сучасній комунікації.

Анонімність – Принцип анонімності в спілкуванні — це практика навмисного приховування особи, що телефонує з метою спілкування без відстеження. Майже символічним прикладом анонімного спілкування є таксофон. При таксофонному дзвінку оплата проводиться готівкою, номер таксофона є загальнодоступним, і будь-хто може користуватися телефоном, тобто особа того, хто телефонує невідома, і немає ніяких засобів визначити, чи справді той, хто телефонує, є тим, за кого він/вона себе видає. Оскільки номер телефону не внесено до списку, ніхто не володіє цим номером і (за винятком складного програмного забезпечення для розпізнавання голосу) не може ідентифікувати особу абонента, який робить виклик. У разі зареєстрованого пристрою, такого як мобільний телефон, особу власника пристрою можна відстежити за номером телефону, але особа абонента, яка викликає, може залишатися невідомою. Наприклад, телефон може бути вкрадений або SIM-карта з оплатою за фактом використання може бути використана для приховування справжньої особи викликаючого абонента. Крім того, ноутбук, планшет або мобільний телефон можна підключити через Wi-Fi в громадському кафе, забезпечуючи анонімність, схожу з анонімністю будь-якого таксофона або телефонної будки.

Деякі оператори OTT вибрали використання VoIP-телефонії як таксофона без перевірки особи своїх абонентів. Наприклад, у недавньому онлайн-звіті CNN Money (http://money.cnn.com/2015/11/17/technology/isis-telegram/) йдеться: "Додаток під назвою Telegram — це" гаряча новина серед джихадистів ". Дослідження підтверджують, що застосування Telegram зіграло важливу роль у таємному плануванні атаки терористів ІДІЛ на Париж. У статті "Засновник Telegram знав, що ІДІЛ використовує додаток для планування атаки на Париж" (http://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-knew-isis-communicate-paris-pavel-durov-a6742126.html), засновник Telegram Павло Дуров сказав: "Право на приватне життя важливіше, ніж страх перед такими жахливими подіями, як тероризм".

Іншим прикладом використання конфіденційності та анонімності при скоєнні злочинів, про які повідомляється в пресі, є BitTorrent — додаток і мережа даних, яка часто використовується для незаконного завантаження матеріалів, що охороняються авторським правом, або обміну ними. У новинній статті CNN Money Tech (http://money.cnn.com/2011/06/10/technology/bittorrent_lawsuits/) під назвою "50 000 користувачів BitTorrent стали відповідачами у справі про незаконні завантаження" повідомлялося, що користувачі були притягнуті до відповідальності за новими законами про боротьбу з піратством за нелегальне завантаження фільму "The Hurt Locker" та інших захищених авторським правом матеріалів. Мережевий оператор BitTorrent зайняв позицію таксофона, який не несе відповідальності за те, що люди роблять, використовуючи свою мережу для своєї приватної діяльності. Прихильники свободи слова підтримують цю позицію, в той час як представники правоохоронних органів і урядів, органів національної безпеки і захисту прав ІВ зневажають таке ставлення як безрозсудне і безвідповідальне. Незалежно від політики в цьому питанні, до тих пір, поки системи зв'язку не зможуть здійснювати перевірку особи, обговорення питання про припинення анонімних дзвінків носить суто академічний характер.

Перевірка особистості викликаючого абонента особливо важлива для корпорацій і комерційних підприємств для контролю доступу до конфіденційних даних компанії, включаючи інтелектуальну власність, технічні розробки, оцінку продукції, виробничі ноу-хау, конфіденційні фінансові звіти і прогнози, бізнес статус, прогнози продажів, інвентаризацію і WIP, аудит якості, ділові контракти, списки клієнтів і співробітників, і інші комерційні таємниці. При доступі до корпоративних комунікацій привілеї доступу, що надаються будь-якому співробітнику, підряднику або керівнику, залежать від підтвердження його особи. При конференц-дзвінках, включаючи виклики інвесторів, перевірка особи важлива для підтвердження того, хто присутній на дзвінку, і для гарантії того, що без підтвердження факту особистості, розмова не відбудеться.

Як не парадоксально, але хоча перевірка особи викликаючого абонента може бути використана для запобігання планам злочинців і корпоративного шпигунства, така ж перевірка особи корисна для забезпечення конфіденційності викликаного абонента. Якщо обидві сторони дзвінка або текстового чату підтверджують свою особу за допомогою певної процедури

автентифікації, самозванці не мають доступу до дзвінка або його даних, захищаючи дзвінок від злочинних атак.

Нарешті, необхідно проводити відмінність між анонімними абонентами і анонімними дзвінками. Анонімна особа — це особа, яка приховує свою справжню особистість від мережі, в якій він спілкується. Анонімний дзвінок, однак, не вимагає умови від абонента бути анонімним в мережі, а тільки те, що його справжня особистість під час спілкування має бути замовчена в пакетах даних виклику. Зареєстрований власник облікового запису в мережі SDNP може здійснити дзвінок або відправити дані, використовуючи анонімну передачу даних, навіть якщо мережа знає його особу і номер телефону. Таким чином, законослухняні громадяни можуть спілкуватися анонімно, без необхідності приховувати свою особу від оператора мережі SDNP. Якщо абонент здійснює звичайні приватні дзвінки, бере участь у розважальних або ділових заходах, його виклик SDNP залишається конфіденційним і безпечним, навіть якщо в мережі відомо, що його ім'я зберігається в базі даних сервера імен SDNP.

Приклади необхідності легального анонімного спілкування включають в себе глобальні ігри, в яких важливо захистити особистість гравця, особливо дітей. Ще одна перевага анонімності пов'язана зі спілкуванням між транспортними засобами (vehicle-to-vehicle, V2V) для запобігання злочинних дій з боку водіїв, шляхом ідентифікації особистих даних водіїв, що перешкоджають водінню. На відміну від цього, якщо той, хто телефонує, вчиняє злочинні чи інші недобросовісні дії при спілкуванні, співробітники правоохоронних органів можуть (відповідно до законодавства) отримати доступ до їхніх дзвінків і передачі даних. Таким чином, оператор мережі може задовольнити вимоги судових наказів і повісток до суду, не розкриваючи особистості і не розголошуючи розмови дзвінків законослухняних громадян.

Таким чином, використовуючи розглянуті раніше способи комунікації в мережі SDNP, тільки абоненти SDNP, що підлягають ідентифікації, можуть здійснювати анонімні дзвінки. Невпізнані абоненти не мають доступу до мережі SDNP або можливості здійснювати анонімні дзвінки.

Національна безпека і конфіденційність – характер захищених і приватних повідомлень ще більш ускладнюється, коли враховані ролі і закони уряду. Кожна країна відстоює своє суверенне право контролювати комунікації в межах своїх кордонів. Однак з появою Інтернету і динамічної маршрутизації мереж передачі даних з пакетною комутацією виникає безліч технічних і юридичних проблем, пов'язаних з мережевим наглядом і моніторингом. Однією з проблем є моніторинг наскрізного трафіку мережі "сервер-сервер" — пакетів даних, що проходять через країну без зупинки. Оскільки інтернет-трафік динамічно маршрутизується, оператор не має уявлення про те, які пакети даних несе його мережа серверів. Будь-яка країна може, звичайно, спробувати перехопити і дешифрувати ці великі обсяги даних, але через шифрування доступ без знання ключів шифрування є складним завданням, особливо для моніторингу в режимі реального часу. А оскільки абоненти можуть не проживати в країні, у конкретної країни немає юрисдикції для виклику до суду або запиту ключів шифрування, що використовуються для здійснення виклику. Така мережа наскрізних даних аналогічна радіохвильовому трафіку, що проходить через земну атмосферу. Незважаючи на те, що радіохвилі можуть проходити непоміченими, зупинити їх практично неможливо. Аналогічним чином, за винятком повної ізоляції інфраструктури країни від Інтернету, не існує ніякого реального способу зупинити мережевий трафік через передачу даних.

Більш прагматичним рішенням для управління комунікаціями є зосередження моніторингу на каналах зв'язку "Останньої Милі", тобто перехоплення і моніторинг викликів і даних про них в тих місцях, де джерело і/або пункт призначення виклику знаходяться на території країни. Цей підхід має ряд переваг порівняно з перехопленням великого обсягу трафіку через дані, включаючи (i) менший обсяг даних, а саме більш керований для аналізу, (ii) оператор останньої милі зв'язку або оператор мережі підпорядковується законодавству країни, в якій він знаходиться (iii) оператор останньої милі або оператор мережі може бути викликаний до суду для передачі будь-яких доступних ключів шифрування, (iv) пристрій викликаючого абонента має "зареєструватися" в електронній формі для підключення до мережі останньої милі і при цьому передати інформацію про такого абонента, а також (v) адреса мережі GPS може бути визначена за допомогою тріангуляції сигналу.

На відміну від правових і технічних проблем, пов'язаних із забезпеченням дотримання правил передачі даних по мережі, закони, що регулюють передачу даних по "останній милі" і припинення викликів, повністю належать державі, в якій проживає оператор мережі "Остання Миля". Залежно від національних законів про недоторканність приватного життя уряд країни може наполягати на необхідному рівні доступу до каналів зв'язку "Останньої Милі", включаючи наступні комбінації:

- Відсутність права контролювати будь-які дані або дзвінки без повістки до суду з поважної причини. За рішенням суду, право таємно спостерігати за будь-яким дзвінком або обміном даними.

- Право на моніторинг метаданих будь-якого виклику без судового рішення.

- Право контролювати всі дзвінки і передачу даних без санкції суду.

- Право на перехоплення, моніторинг і, при необхідності, блокування будь-яких повідомлень.

Наприклад, різні уряди, такі як Сполучені Штати, дотримуються позиції, згідно з якою вони залишають за собою право здійснювати моніторинг "метаданих" викликів без судового рішення. Метадані включають інформацію про пакет даних про те, хто кому дзвонить, як довго тривав виклик, де перебували абоненти на момент виклику і т. д., фактично не маючи доступу до самих даних виклику. По суті, метадані включають в себе заголовок IP-пакету, але не його корисне навантаження. Моніторинг викликів і передачі даних, навпаки, передбачає доступ не тільки до даних заголовків, але і до корисного навантаження. У таких випадках, коли корисне навантаження може бути зашифроване, уряд може наполягти на тому, щоб мережевий оператор надав йому майстер-ключі шифрування, якщо такі є. Одне з питань, порушених захисниками недоторканності приватного життя, стосується зловживання владою з боку уряду. Зокрема, якщо мережа покладається на один набір майстер-ключів шифрування, то відмова від цих ключів у відповідь на постанову суду, що дозволяє вести спостереження за конкретною особою, фактично дозволяє уряду контролювати дзвінки кожного, навіть якщо судова постанова стосувалася тільки однієї особи або групи осіб. Іноді цю проблему називають ускладненням: "Хто виступає поліцією для поліції?"

Ще одне міркування стосується права на недоторканність приватного життя осіб, які здійснюють міжнародні дзвінки. У таких випадках ті, хто дзвонить, повинні знати, що відповідні закони про державний доступ залежать від місцезнаходження обох абонентів, тобто від того, де знаходяться дві останні милі мереж. Виклик зі Сполучених Штатів до Китаю буде регулюватися законодавством США для того, хто телефонує в Сполучених Штатах і законодавством Китаю для іншого, що телефонує в Китаї. У таких ситуаціях доступ до телефону одного уряду може бути більшим, ніж в іншого. Таким чином, той, хто телефонує в країні з ширшими правами на недоторканність приватного життя, може вважати своє право на приватне життя порушеним урядом іншої країни, але оскільки він подзвонив у цю країну, у нього немає жодних законних підстав для скарги.

У разі зв'язку з використанням раніше розглянутої захищеної динамічної мережі і протоколу перехоплення наскрізних даних у гіперзахищеній хмарній комунікації фрагментованих зашифрованих пакетів даних, що передаються анонімно по мережі SDNP, практично неможливий. Таким чином, конфіденційність і безпека гіперзахищених викликів визначаються самим пристроєм і каналом зв'язку "Остання Миля". Завдяки адаптації розглянутих раніше SDNP-методів для каналу зв'язку "Останньої Милі" можна реалізувати гіперзахищену функцію взаємодії, розкриту в цьому документі, і досягти високого рівня конфіденційності.

Крім того, розглядаються механізми налаштування параметрів безпеки та конфіденційності мережі SDNP відповідно до місцевого законодавства, що регулює передачу даних "Останньої Милі" в кожній країні. Ці методи включають запобіжні заходи, що дозволяють уповноваженому органу безпеки контролювати зв'язок відповідно до закону і судових рішень, не піддаючи дані про виклики небезпеці для хакерів і кіберзлочинців. Таким чином, у розглянутому тут гіперзахищеному каналі зв'язку "Останньої Милі" не використовується "бекдор", вразливий для кібератак.

Методи та Устрій Гіперзахищеного Зв'язку "Останньої Милі"

Щоб гарантувати наскрізну гіперзахищеність, застосування методів, описаних раніше для маршрутизації зашифрованих анонімних фрагментованих пакетів даних у хмарі SDNP, також має бути адаптовано для зв'язку в межах "Останньої Милі". Безпека зв'язку "Останньої Милі" особливо проблематична, оскільки дані можуть передаватися в мережах, не підтримуваних оператором SDNP, пакетна маршрутизація може включати звичайну IP-пакетну маршрутизацію, а внутрішня безпека мережі "Останньої Милі" може бути несвідомо скомпрометована кіберзлочинцем, можливо, причетним до змови з оператором останньої милі.

Відповідно до цього винаходу, передача даних по "Останній Милі" обов'язково передбачає передачу IP-датаграм за межі хмарної мережі з використанням пакетного формату, відмінного від формату пакетів даних всередині хмари SDNP. Як показано на Рис. 10, SDNP хмара, що складається з серверів 1201 (схематично представлених вузлами SDNP з підтримкою програмних комутаторів від $M_{0,0}$ до $M_{0,F}$.), транспортує VoIP, відео, текст і дані за допомогою датаграм SDNP, представлених у зразках пакетів даних 1222B, 1222C, та 1222F. Датаграма SDNP містить адреси джерела та призначення SDNP рівня 3, а не IP-адреси Інтернету. SDNP-

адреси відрізняються від IP-адрес тим, що вони розпізнаються тільки серверами імен SDNP або іншими серверами, що виконують функції серверів імен SDNP, а не DNS-серверів імен Інтернету.

Як описано вище в патенті 14/803,869, SDNP-пакети змінюються динамічно в міру переміщення по мережі, з оновленими адресами маршрутизації і постійно змінюється корисним навантаженням, що виконується відповідно до загальних секретів і динамічних станів (таких як час). Наприклад, пакет даних 1222B, що надсилається вузлом $M_{0,0}$, включає датаграму рівня 3 SDNP з унікальними SDNP адресами і унікально зашифрованим корисним навантаженням. Вихідний пакет даних 1222C з вузла $M_{0,1}$ складається з датаграми рівня 3 SDNP C з різними адресами SDNP і зашифрованим корисним навантаженням. Через кілька десятків мілісекунд те ж корисне навантаження досягає вузла $M_{0,f}$, який обробляє дані і пересилає пакет даних 1223G, що включає IP-датаграму G через "Останню Милю".

Оскільки зміни виконуються відповідно до заданих станів, вихідні пакетні дані можуть бути відновлені шляхом виконання низки операцій анти-функцій, що виконуються в зворотному порядку, порівняно з тим, в якому вони були виконані. Наприклад, функціональна послідовність SDNP, що складається з кроків скремблювання, вставки "сміттєвих даних" (приховування) і шифрування, може бути скасована шляхом дешифрування, видалення "сміттєвих даних" і дескремблювання, якщо для виконання відповідної анти-функції викликається один і той же стан, який використовується для виконання даної функції. Дані стану пакета можуть передаватися у вигляді часу, початкових значень або ключа, або вбудованого в корисне навантаження пакета, або надісланого заздалегідь. Транспортування та обробка даних у межах хмари SDNP здійснюється з використанням спеціальних загальних секретів та облікових даних безпеки SDNP. Медіа-вузли, що мають загальний набір загальних секретів та облікових даних безпеки, можна назвати "зоною безпеки". Зона, яка використовується для доступу до облікових даних, що працюють у хмарі SDNP, не може бути доступна жодному користувачеві за межами хмари SDNP. Таким чином, всі з'єднання "останньої милі" повинні являти собою зону безпеки, відмінну від зони SDNP "хмари".

У наведеному прикладі сервер 1201A і сервер 1201F, на якому розташовані відповідні вузли $M_{0,0}$ і $M_{0,f}$, працюють як шлюзи SDNP, тобто взаємодіють з пристроями поза SDNP хмари, а також з іншими внутрішньо-хмарними вузлами SDNP. Зв'язок між цими шлюзами і комунікаційними пристроями за межами хмари являє собою "останню милю" зв'язку. Відповідно, вузли шлюзу повинні розуміти облікові дані безпеки зон як в хмарі SDNP, так і в мережі "останньої милі", до якої вони підключаються, виступаючи в якості транслятора під час пакетної маршрутизації. З семантичної точки зору термін "остання миля" — це абстракція, що означає зв'язок за межами SDNP хмари і не відноситься конкретно до відстані в одну милю. Замість цього термін "остання миля" охоплює будь-який зв'язок між клієнтським пристроєм і SDNP хмарою на будь-якій відстані, незалежно від того, чи працює клієнтський пристрій як клієнт SDNP, тобто чи працює SDNP-додаток або мікропрограма, чи ні.

Термін "остання миля" також застосовується як до клієнтського пристрою, що ініціює виклик, так і до клієнтського пристрою, що викликається. Буквально кажучи, дані абонента являють собою "першу милю" виклику, а не останню – відмінність між першою і останньою милями довільна. Зокрема, при будь-якому дуплексному перетворенні або в будь-який "сеанс" IP-зв'язку, пристрій, що приймає виклик, обов'язково відповідає на виклик або запит сеансу, відправляючи відповідь викликаючому абоненту. Таким чином, в будь-якому двосторонньому зв'язку перша миля завжди працює як остання миля в шляху передачі даних відповіді. По суті, перша миля для того, хто дзвонить, є одночасно і останньою милею для відповіді. Таким чином, термін "остання миля" використовується у всьому цьому додатку для позначення як першої, так і останньої милі, незалежно від того, який пристрій ініціював сеанс зв'язку або виклику.

Зв'язок за межами SDNP хмари з будь-яким пристроєм, відмінним від клієнта SDNP, обов'язково здійснюється з використанням IP-датаграм, а не SDNP-датаграм. Наприклад, повертаючись до Рис. 10, пакет даних 1223A включає в себе "IP-датаграму A", побудовану з використанням корисного навантаження SDNP з IP-адресою, а не SDNP-адресою. Аналогічним чином, IP-датаграма G включає пакет даних 1223G, що містить корисне навантаження SDNP, маршрутизоване з використанням IP-адреси. IP-адреси джерела і призначення являють собою будь-які IPv4 або IPv6-адреси, розпізнавані мережею, за якою здійснюється маршрутизація. IP-адреси можуть включати в себе Інтернет-адреси, що розпізнаються DNS-серверами Інтернету, або ж можуть включати NAT-адреси, що використовуються для маршрутизації по локальних мережах, визначених постачальником послуг локальної мережі.

Оскільки апаратне і мікропрограмне забезпечення, що використовується в комунікації "Останньої Милі", може істотно відрізнятися і може включати телефонні лінії, оптоволоконні

лінії, мережі кабельного телебачення, 3G і 4G радіо, вишки мікрохвильового зв'язку і супутники, аналіз зв'язку "Останньої Милі" повинен розглядатися для різних фізичних мереж рівня 1 і їх відповідних використовуваних форматів даних зв'язку рівня 2. Наприклад, формати можуть включати аналогові (POTS), Ethernet, Wi-Fi, 3G, 4G/LTE і DOCSIS3. Відповідні можливості забезпечення безпеки та конфіденційності кожної реалізації програми "Останньої Милі" розглядаються в кожному окремому випадку окремо в наступному розділі, присвяченому зв'язку за протоколом SDNP "call out".

SDNP Call Out через незахищені лінії зв'язку – будь-який виклик, що виходить за межі певної мережі для транспортування через окрему (і зазвичай різну) мережу, зазвичай називається "call out", термін означає що дані або голос, що залишають одну мережу для транспортування по іншій. Наприклад, спілкування між клієнтами, які використовують програми Skype, зазвичай називається дзвінком Skype, а виклик з клієнта Skype на звичайний номер або номер стільникового телефону називається викликом Skype call out, або викликом Skype Out. Як правило, дзвінки на звичайні телефони вимагають певної додаткової плати, як у вигляді передплати, так і у вигляді плати за користування.

У контексті цього розділу, обмін даними з SDNP хмари через незахищене з'єднання "Останньої Милі" з будь-яким пристроєм, відмінним від клієнта SDNP, далі називається терміном "SDNP Call Out". На Рис. 11 схематично представлені два приклади маршрутизації виходу SDNP на незахищену "Останню Милю". У прикладі вище зв'язок здійснюється за допомогою аналогових сигналів з аналоговим пристроєм, таким як телефон або таксофон 6A. У таких випадках шлюз SDNP повинен бути оснащений цифро-аналоговим перетворювачем. В іншому випадку на шлюзі можуть бути додані модеми або пристрої перетворення. Інформація передається за аналоговим сигналом 1221, а не через пакет даних. Аналогові телефонні сигнали, що є ефективними для передачі голосу, проте вони не дуже добре пристосовані для високошвидкісної передачі даних.

У прикладі нижче SDNP Call Out відбувається через цифрову мережу на будь-який цифровий пристрій (наприклад, стільниковий телефон 32), який не активовано як клієнт SDNP, або не має SDNP мікропрограми. У таких випадках пакет даних 1223 передає виклик або дані, використовуючи звичайний Інтернет-протокол, тобто формат IP-пакетів, що відповідає 7-рівневій моделі OSI. IP-датаграма включає IP або NAT-адреси в полях адреси джерела та призначення, а також IP або VoIP-дані як корисне навантаження. Цифровий шлях може включати різні форми цифрових даних, такі як Ethernet, Wi-Fi або 4G/LTE, які різняться залежно від типу з'єднання "Останньої Милі".

На наведених прикладах, дані зв'язки "Останньої Милі" переносяться за межі SDNP мережі по незахищеному каналу зв'язку або мережі, і оскільки виклик не захищений, він піддається злому, шпигунству, прослуховуванню та іншим кібератакам. Як описано в довідковому розділі цієї заявки, небезпечні лінії зв'язку і підключення "Останньої Милі", чи то мідні дроти витої пари, коаксіальний кабель, оптичне волокно, Ethernet, Wi-Fi, стільниковий або супутниковий зв'язок, не захищені по своїй суті, якщо в маршрут наскрізної передачі даних не додані спеціальні методи безпеки, таке як наскрізне шифрування. Тому безпека навіть найбезпечнішої "хмари" даних або VPN піддається ризику через його найслабшу ланку — в даному прикладі, канал "Останньої Милі". Навіть шифрування не гарантує безпеки, особливо на одному чітко визначеному електричному, мікрохвильовому або радіохвильовому з'єднанні. Крім відсутності безпеки, приклади не включають в себе ніяких механізмів перевірки автентичності. Не маючи можливості автентифікації, канал "Останньої Милі" не має гарантії конфіденційності. Тому наведені приклади являють собою небезпечні мережі "Останньої Милі", в яких відсутня конфіденційність даних абонентів, що викликають.

Рис. 12 ілюструє шлюз SDNP, що виконує виклик SDNP call out на незахищений канал "Останньої Милі" без забезпечення конфіденційності, підключаючись до телефонної мережі загального користування або шлюзу PSTN 1A по дротовому або оптичному каналу постачальника послуг цифрової мережі 24. Шлюз PSTN 1A маршрутизується на мережевий комутатор POTS 3 через аналоговий зв'язок 4. Мережевий комутатор POTS 3 дозволяє виконувати звичайні телефонні дзвінки по витій мідній парі 7 на домашній телефон 6, на бездротову телефонну систему 5 або на таксофон 6A. Вся "остання миля" є ні приватною, ні безпечною. Хоча при передачі пакета даних 1222A, що містить датаграму SDNP-A, використовується адресація SDNP і корисне навантаження SDNP в мережі SDNP, переваги гіперзахищеності втрачаються після введення даних в "останню милю". Наприклад, пакет даних 1223B, що містить IP-датаграму B, що передається по дротовій або оптоволоконній лінії 24 мережі NSP, використовує звичайну IP-адресу, що розпізнається DNS-серверами Інтернету, і містить звичайну IP-адресу, яка може бути виявлена будь-яким кіберзлочинцем. Аналогові лінії

4 і 7 однаково вразливі, оскільки вони передають прості аналогові аудіо сигнали, як і аналогові дані виклику 1221. Хоча шлюз SDNP може підтримувати незахищені небезпечні виклики, не доцільно підключати безпечні виклики SDNP до небезпечних мереж "Останньої Милі" без забезпечення конфіденційності.

Невелике поліпшення у вищезгаданій небезпечній реалізації Останньої милі може бути досягнуто за допомогою перевірки автентичності. Рисунок 13 схематично ілюструє приклади маршрутизації викликів SDNP на незахищену "останню милю", але з двома різними типами автентифікації. У верхньому прикладі показано вихід SDNP зі шлюзу SDNP 1220A за аналоговою або POTS-лінією на офісний стаціонарний телефон 9. Як показано на рисунку, оператор 1225 виконує автентифікацію вручну для підтвердження особи власника облікового запису та посвідчення його ідентифікатора. Незважаючи на автентифікацію, аналоговий звуковий сигнал 1221 є небезпечним і залишається конфіденційним, тільки якщо в розмові не розкриваються секрети або інформація про обліковий запис, тобто якщо не розкриваються секрети, то інформація є конфіденційною, а якщо розкривається інформація, то повідомлення перестає бути конфіденційним. Таким чином, термін напів-приватності використовується в цьому документі для позначення автентифікованих повідомлень по незахищених лініях, тобто умовно приватних повідомлень.

На нижній схемі показано виклик SDNP з шлюзу SDNP 1220A на незахищену цифрову "Останню Милю". Дані, що переносяться IP-датаграмою 1223 на електронний пристрій, наприклад настільний ПК 36, хоча і незахищені, можуть бути перевірені за допомогою електронного методу перевірки особи, такого як токен 1226, до якого зломщик не має доступу. Оскільки зв'язок небезпечний і може прослуховуватися, в цифровому діалозі слід проявляти обережність, щоб не розголошувати номери рахунків або конфіденційні дані.

Конкретні приклади напів-приватних незахищених дзвінків наведені в декількох наступних прикладах. На Рис. 14 зображено незахищений зв'язок "Останньої Милі" з посвідченням особи між мережею SDNP і офісним настільним телефоном 9, наприклад, телефоном приватного банкіра. Дзвінок власника облікового запису, якщо він зроблений на міжнародному рівні, наприклад, буде спрямований по всьому світу за допомогою гіперзахищеного зв'язку в мережі SDNP і, нарешті, підключений до "Останньої Милі" як виклик SDNP через SDNP шлюз 1201A. Міжміська частина виклику виконується за допомогою динамічно змінюваних датаграм SDNP, таких як пакет даних 1222A, що містить SDNP датаграму A з корисним навантаженням SDNP. Пакет даних 1222A конвертується шлюзом SDNP 1201A з датаграми A SDNP в IP-датаграму B, показану пакетом даних 1223B. На відміну від SDNP датаграми A, IP-датаграма B містить відслідковуване IP корисне навантаження. Пакет даних 1223B передається провайдером послуг стільникового зв'язку (NSP) по дротовому або оптоволоконному зв'язку 24 в телефонну мережу загального користування або шлюз PSTN 1A. Цей шлюз, у свою чергу, підключається до розподіленого комутатора компанії 8A по POTS лінії 4 з аналоговим викликом 1221. Комутатор компанії 8A підключається до настільного телефону 9 за аналоговою АТС або телефонної лінії 7A до настільного телефону 9, а також до персонального оператора автентифікації 1225. Під час розмови власник облікового запису зв'язується з приватним банкіром за настільним телефоном 9, але перш ніж приступити до здійснення будь-яких операцій, оператор особистої автентифікації 1225 приєднується до виклику для підтвердження особи, що телефонує, а потім залишає виклик для збереження конфіденційності викликаючого абонента. Однак, оскільки дзвінок небезпечний, як приватний банкір, так і власник рахунку повинні проявляти обережність, щоб не розголошувати конфіденційну інформацію, таку як номери рахунків, паролі або PIN-коди. Як такий, дзвінок є напів-приватним, тобто умовно приватним.

На Рис. 15 показано незахищений зв'язок між мережею SDNP і настільним комп'ютером 36, що засвідчує особу. У сеансі цифрового зв'язку настільний комп'ютер 36 зв'язується зі шлюзом SDNP 1201A, використовуючи IP-датаграму B, перенесену з декількох цифрових носіїв. У першому сегменті Ethernet 106A передає пакет даних 1223D, що складається з IP-датаграми B, з настільного комп'ютера 36 на локальний маршрутизатор 27B на базі Ethernet. Локальний Ethernet-маршрутизатор, у свою чергу, з'єднується з мережевим маршрутизатором 27 через провайдера Інтернет-послуг (ISP), дротовий або оптоволоконний канал 24A, використовуючи пакет даних 1223C, що містить IP-датаграму B. Дротовий або оптоволоконний канал 24 оператора мережі NSP несе пакет даних 1223B, що містить IP-датаграму B на кінцевій частині останньої милі між мережевим маршрутизатором 27 і SDNP-шлюзом 1201A. Оскільки використовуються IP-датаграми, Остання Миля небезпечна. Цифрові методи перевірки ідентифікаційних даних, такі як вікно входу 1227 і токен безпеки 1228, можуть використовуватися для автентифікації, щоб гарантувати, що комунікації залишаються напів-приватними. Ці методи автентифікації повинні бути обмежені одиничним використанням для

запобігання їх використання сторонніми особами. Наприклад, як тільки токен генерує число і воно використовується для отримання доступу, комбінація більше не підходить для використання, тому що, якщо хакер перехопить токен, він буде мати значення, оскільки термін його дії закінчився і він більш недійсний.

Інші приклади незахищеного зв'язку "Останньої Милі" з ідентифікацією описані на Рис. 16, де шлюз SDNP 1201A взаємодіє як SDNP call out з терміналом точки продажів 38 (POS) і POS-терміналом заправної станції 38A. Зв'язок Останньої Милі являє собою об'єднання цифрових і аналогових з'єднань, включаючи дротовий або оптоволоконний канали 24 NSP, що містить пакет даних 1223B, включає IP-датаграму B в маршрутизатор 27, потім дротовий або оптоволоконний канал 24A з IP-датаграмою B в пакеті даних 1223C на PSTN міст 3A, і POTS або аналогові лінії 30B з цифровою PCM (імпульсний код доданої) даних 1221, підключений до аналогової мережі. Автентифікація у фінансових операціях здійснюється на підставі даних банківської картки 1229, які можуть включати в себе електронну валідацію на основі інтегральної схеми смарт-картки і за динамічним PIN 1228. Автентифікація включає підтвердження у фінансовій установі 1230, підключеній до мережі SDNP або через шлюз SDNP 1201A, або через інший зв'язок "Останньої Милі".

Гіперзахищений Зв'язок "Останньої Милі" – Завдяки адаптації методів динамічної захищеної мережі зв'язку і протоколу, гіперзахищений зв'язок може бути досягнуто на "Останній Милі". Для забезпечення гіперзахищеності, підключений пристрій повинен виконувати код SDNP як "клієнт SDNP". Клієнт SDNP містить інструкції з експлуатації, загальні секрети та інформацію про підключення SDNP, розміщену на підключеному комунікаційному пристрої. Клієнт SDNP може включати програмне забезпечення, що працює на операційній системі, мікропрограмне забезпечення, що працює на мікроконтролері або програмується на мікросхемі, або на спеціалізованому апаратному забезпеченні або інтегральній схемі. Рис. 17 — це приклад гіперзахищеної взаємодії на "Останній Милі" за допомогою "SDNP з'єднання". Як показано на Рис. , шлюз SDNP 1201A підключається до пристрою під управлінням клієнта SDNP, в даному прикладі SDNP програми 1335 працює на настільному комп'ютері 36. Клієнт SDNP є специфічним для апаратного забезпечення та операційної системи. Для мобільних пристроїв потрібні окремі програми для різних платформ мобільних пристроїв з операційними системами Android, iOS і Windows Mobile. Подібним чином, для ноутбуків, настільних ПК і серверів, включаючи Windows 10, MacOS, Unix, Linux і т. д., потрібні різні специфічні програми для ОС. Апаратний хостинг SDNP-клієнтів у пристроях без операційних систем більш високого рівня, таких як POS-термінали, точки доступу, IoT і т. д., повинні бути адаптовані до програмованого пристрою, що виконує код. Програмовані інтегральні мікросхеми часто вимагають програмування в специфічному для мікросхем середовищі розробки, характерного тільки для виробників мікросхем наприклад, Qualcomm, Broadcom, Intel, AMD, NVidia, Microchip тощо.

Оскільки шлюз SDNP 1201A і SDNP 1335 взаємодіють за допомогою корисного навантаження SDNP 1222, ідентичність викликаючих абонентів і корисне навантаження викликів не піддаються прослуховуванню пакетів, особливо корисне навантаження SDNP 1222 містить псевдо адресу джерела і призначення, що не розпізнаються DNS-серверами, а також містить SDNP дані, що можуть бути срембльованими, фрагентованими, перемішеними зі вставками "сміттєвих" даних, а також динамічно зашифрованими. Корисне навантаження SDNP 1222 вбудоване в IP-датаграму 1223, яка направляє маршрутизацію по "Останній Милі", використовуючи IP-адреси або NAT-адреси стільникової, кабельної або ISP мережі, що використовуються для підключення "останньої милі", а не за SDNP адресою.

Ще одним аспектом гіперзахищеного зв'язку "Останньої Милі" на базі SDNP є те, що будь-який клієнт SDNP здатний до автентифікації і перевірки автентичності. Функції конфіденційності, таким чином, але не засновані на здатності мережі забезпечити конфіденційність для підтримки AAA, чи призначені клієнтські програмні забезпечення або мікропрограми для полегшення процесу верифікації чи ні. Оскільки будь-який гіперзахищений зв'язок "Останньої Милі" може бути перевірено, слід розуміти, що наступні приклади гіперзахищеного зв'язку "Останньої Милі" застосовні як до приватного, так і до незахищеного зв'язку. Таким чином, на відміну від незахищених мереж "Останньої Милі" з напів-приватними функціями, захищений гіперзахищений зв'язок "Останньої Милі" визначається клієнтом SDNP, а не мережею, і здатен підтримувати будь-який ступінь однофакторної або багатофакторної автентифікації.

Конкретні приклади гіперзахищених дзвінків показано в наступних прикладах: На Рис. 18 показано гіперзахищений зв'язок "Останньої Милі" між мережею SDNP і різними стільниковими мобільними пристроями з останнім Wi-Fi з'єднанням. Як показано на Рис. , пакет даних 1222A, що містить SDNP датаграму A і корисне навантаження SDNP, перетворюється шлюзом SDNP 1201A для зв'язку Останньої Милі в пакет даних 1223B з IP-датаграмою B, що також містить

корисне навантаження SDNP. Оскільки гіперзахищений зв'язок "Останньої Милі" використовує різні загальні секрети, числові параметри, ключі шифрування та інші облікові дані безпеки, характерні для конкретної зони, відмінні від тих, що використовуються в SDNP хмарі, робоче навантаження SDNP в IP-датаграмі B відрізняється від корисного навантаження SDNP в SDNP-датаграмі A. Іншими словами, шлюз SDNP 1201A перетворює датаграми SDNP в IP-датаграми шляхом перемикання робочого навантаження з однієї зони безпеки в іншу, а також шляхом вставки маршрутизації SDNP як джерела та адреси SDNP-адреси, що не розпізнаються DNS серверами.

Потім це корисне навантаження SDNP, специфічне для конкретної зони, упаковується в пакет IP-датаграми з IP-заголовком, що містить IP-адреси, специфічні для Останньої Милі мережі, або NAT, або адреси Інтернету, для полегшення маршрутизації пакетів між шлюзом. Оскільки проміжні пристрої маршрутизації "Останньої Милі" не є клієнтами SDNP, структура корисного навантаження SDNP в рамках IP-датаграми B залишається незмінною при проходженні через "Останню Милю". Іншими словами, пакети даних 1223B, 1223C і 1223D являють собою ідентичні датаграми, що складаються з SDNP-датаграми B з ідентичними корисними навантаженнями SDNP — корисні навантаження, які не змінюються в міру переміщення пакетів від пристрою до пристрою в "Останній Милі". Простіше кажучи, тільки вузол мережі SDNP або клієнт SDNP може реконструювати корисне навантаження SDNP, вбудоване в датаграму третього рівня, чи то IP-датаграма або SDNP-датаграма.

Як показано на Рис. , пакет даних 1223B, що складається з IP-датаграми B, передається по дротовому або оптоволоконному каналу зв'язку 24 на маршрутизатор 27, а потім пакет даних 1223C також включає IP-датаграму B, що передається по дротовому або оптоволоконному каналу 24A на Wi-Fi маршрутизатор 26. Потім Wi-Fi роутер 26 забезпечує зв'язок останньої лінії за допомогою пакета даних 1223D, що містить IP-датаграму B через Wi-Fi з'єднання 29 з мобільними пристроями, такими як стільниковий телефон 32 і планшет 33, на яких працює додаток SDNP 1335A. Таким чином, ці пристрої функціонують як SDNP клієнт, здатний інтерпретувати дані, що містяться в пакеті даних 1223D, що містить IP-датаграму B, включаючи дешифрування, видалення "сміттєвих" даних, витяг і змішування вмісту корисного навантаження з фрагментами даних з інших пакетів даних для відтворення вихідного повідомлення або звуку.

На Рис. 19 показано гіперзахищений зв'язок "Останньої Милі" між мережею SDNP і різними стільниковими мобільними пристроями за допомогою стільникового радіозв'язку "Останньої Лінії". Як показано на Рис. , пакет даних 1223B, що складається з IP-датаграми B, передається по дротовій або оптоволоконної лінії зв'язку 24, керованої NSP, на мережевий маршрутизатор 27, за яким слідує пакет даних 1223C, що також включає IP-датаграму B, що передається оператором мобільного зв'язку через дротовий або оптоволоконний канал зв'язку до стільникової базової станції 17 для утворення стільникової мережі 25. Базова станція 17 забезпечує зв'язок "Останньої Лінії" за допомогою пакета даних 1223D, що включає IP-датаграму B по 3G, 4G/LTE по стільниковому зв'язку 28 з мобільними пристроями, такими як стільниковий телефон 32 і планшет 33, на яких встановлено додаток 1335A SDNP.

Як і в попередньому прикладі, оскільки проміжні пристрої маршрутизації "Останньої Милі" не є клієнтами SDNP, структура корисного навантаження SDNP в межах IP-датаграми B залишається незмінною при проходженні через "Останню Милю". Іншими словами, пакети даних 1223B, 1223C і 1223D є ідентичними датаграмами, що складаються з SDNP-датаграми B з ідентичними корисними навантаженнями SDNP — корисні навантаження, які не змінюються в міру переміщення пакетів від пристрою до пристрою під час проходження "Останньої Милі".

На Рис. 20 показано гіперзахищений зв'язок "Останньої Милі" між мережею SDNP і різними немобільними (пов'язаними) пристроями з "Останньої Лінії" по мережі Ethernet. Як показано на Рис. , пакет даних, що складається з IP-датаграми B, передається по дротовому або оптоволоконному каналу зв'язку 24, керованому NSP, на мережевий маршрутизатор 27, за яким слідує пакет даних 1223C, що також включає IP-датаграму B, що передається провайдером Інтернет послуг по дротовому або оптоволоконному каналу зв'язку 24A до Ethernet маршрутизатора 103A. Ethernet маршрутизатор 103A забезпечує зв'язок "Останньої Лінії" за допомогою пакету даних 1223D, що включає IP-датаграму B по Ethernet 106A з такими пов'язаними пристроями, як настільний комп'ютер 36 з SDNP додатком 1335C і настільний телефон 37 з мікропрограмою SDNP 1335B. За відсутності вузлів мережі SDNP або клієнтів SDNP в "Останній Милі" пакети даних 1223B, 1223C і 1223D є ідентично побудованими датаграмами, всі вони містять SDNP-датаграму B з ідентичними корисними навантаженнями SDNP - корисні навантаження, які не змінюються по мірі [хмарного] переходу від одного пристрою до іншого по зв'язку Останньої Милі.

На Рис. 21 показано гіперзахищений зв'язок "Останньої Милі" між мережею SDNP і клієнтами кабельної служби. Як показано на Рис. , пакет даних 1223A, що складається з IP-датаграми B, передається по дротовій або оптоволоконної лінії NSP 24 на кабельний CMTS (термінальну систему кабельних модемів) 101, що є центром управління, зв'язку і розподілення контенту кабельного оператора. Такі кабельні оператори надають широкий спектр послуг, такий як кабельне телебачення, платне телебачення, послуги телефонного зв'язку, послуги Інтернет, бізнес-послуги та багато іншого. Потім центральний пристрій CMTS 101 підключається до клієнтів по кабелю 106 за допомогою волоконно-оптичного або коаксіального модуля відповідно до DOCSIS3 і trellis-модуляції (описаної в довідковому розділі даного документа) для оптимізації пропускної здатності і послуг реального часу. Відкритий перед клієнтами, кабельний оператор може підтримувати формат датаграм або упаковувати IP-датаграми у власний формат датаграм. Ці пакети даних, далі іменовані CMTS-датаграмою C, використовують специфічну для кабелю NAT адресацію і інкапсулюють корисне навантаження SDNP як вкладене корисне навантаження в пакет даних 1224C для передачі по кабелю 106.

Як показано на Рис. , кабель CMTS 101 направляє CMTS -датаграму 101 C на кабельний модем 103, який у свою чергу витягує пакет даних корисного навантаження 1223B, що містить IP-датаграму B з незміненим корисним навантаженням SDNP для доставки по "Останній лінії". Пристрої, що підтримують останній зв'язок з клієнтом SDNP, можуть працювати в декількох форматах, включаючи Ethernet 106A на комп'ютері 36 під управлінням клієнтської програми 1335C SDNP або по витій парі 7 на телефон 5A з мікропрограмою 1335B для клієнта SDNP. Кабель CMTS 101 також направляє CMTS-датаграму C на кабельний модем 103, який у свою чергу витягує вихідну IP-датаграму, наприклад, IP-датаграму B, і відправляє її та інший відеоконтент на приставку кабельного телебачення через кабель 106. Потім приставка кабелю переадресує IP-датаграму B і контент через HDMI-2 107 на інтерактивне телебачення в ультра високій роздільній здатності 39, запустивши SDNP додаток 1335D. В якості альтернативи мікропрограма SDNP може бути розміщена на приставці 102 для кабельного телебачення.

На Рис. 22 показано гіперзахищений зв'язок "Останньої Милі" між мережею SDNP і домашньою мережею Wi-Fi, підключеною через постачальника кабельних послуг. Як показано на Рис. , пакет даних 1223B, що складається з IP-датаграми B, передається по дротовій або оптоволоконній лінії 24A NSP до кабелю CMTS 101, який є центром управління, зв'язку і розподілення контенту кабельного оператора. Потім головний пристрій CMTS 101 підключається за допомогою дротового або оптоволоконного з'єднання 24A за коаксіальним або оптоволоконним кабелем до певного клієнтського модемного маршрутизатора (Wi-Fi) 100B для створення точки доступу Wi-Fi 26. Маршрутизація пакета даних 1224C може включати IP-датаграму з Інтернет-адресами або містити пропрієтарну CMTS-датаграму C з NAT-адресою. Маршрутизація між шлюзом SDNP 1201A і кабельним (Wi-Fi) модемом маршрутизатором 26 являє собою дротовий сегмент гіперзахищеного зв'язку "Останньої Милі".

Останній ступінь у домашній мережі включає в себе Wi-Fi з'єднання 29 сполучного кабелю (Wi-Fi) модема маршрутизатора 26 з різними домашніми пристроями за пакетом даних 1223D, що містить IP-датаграму B. Для забезпечення гіперзахищеності такі пристрої повинні працювати як клієнт SDNP або за допомогою програмного забезпечення, або мікропрограмного забезпечення, завантаженого на пристрій. Наприклад, ноутбук 35 і настільний комп'ютер 36 працюють як SDNP клієнти за допомогою комп'ютерного додатку 1335C, мобільний телефон 32 і планшет 33 працюють як SDNP клієнти за допомогою мобільного додатку 1335A. IoT пристрої, в даному випадку холодильник 34K, можуть працювати в якості SDNP клієнта, якщо їх система управління завантажена прошивкою SDNP 1335E. Однак якщо такі пристрої не інтегрують або не можуть інтегрувати програмне забезпечення SDNP клієнта, то безпека повинна бути забезпечена іншими способами.

Безпека "Останньої лінії" з ідентифікацією – У випадках, коли підключений пристрій не може виступати як клієнт SDNP, гіперзахищеність не може бути гарантована від початку до кінця. У цьому випадку використання віддаленого шлюзу SDNP може розширити гіперзахищене з'єднання, щоб охопити "Останню Милю" з'єднання, за винятком "Останньої лінії" зв'язку. Якщо параметр "Остання лінія", частина "Останньої Милі", що з'єднується безпосередньо з комунікаційним пристроєм, не включена в якості вузла SDNP, то безпека "Останньої Лінії" повинна бути забезпечена через локальну мережу (LAN), що використовується для забезпечення зв'язку "Останньої Лінії". Рис. 23 схематично представляє використання віддаленого шлюзу SDNP 1350 в з'єднанні "Останньої Милі". Віддалений шлюз SDNP 1350 включає в себе будь-який комунікаційний пристрій, що працює на мікропрограмі SDNP 1335H в якості віддаленого шлюзу. Таким чином, з'єднання SDNP між шлюзом SDNP 1201A і віддаленим шлюзом SDNP 1350 включає IP-датаграму 1223A, IP або NAT адресу джерела і призначення та

корисне навантаження 1222 SDNP. Корисне навантаження SDNP 1222 включає в себе адресу SDNP, що не розпізнається DNS серверами, і вкладене корисне навантаження SDNP з використанням спеціальних реквізитів безпеки зони "Останньої Милі". Дане гіперзахищене SDNP-з'єднання підтримує перевірку особистості і конфіденційність абонента, який дзвонить.

Між віддаленим шлюзом SDNP 1350 і будь-яким підключеним пристроєм, відмінним від клієнта SDNP (наприклад, стаціонарним комп'ютером 36), зв'язок здійснюється через локальну мережу або LAN з'єднання, таке як Ethernet, Wi-Fi або інші протоколи. Безпека забезпечується протоколами безпеки локальної мережі і сполученням пристроїв між комунікаційним пристроєм і віддаленим шлюзом SDNP. Сполучення пристроїв — це процес, за допомогою якого послідовність автентифікації між двома сполученими пристроями встановлює особу цих двох пристроїв, запобігаючи несанкціонованому доступу.

На Рис. 24 маршрутизатор з підтримкою SDNP 1351, тобто маршрутизатор з мікропрограмою SDNP 1335H, виконує функцію віддаленого шлюзу SDNP. Цей шлюз перетворює пакет даних 1223A, що містить IP-датаграму A, в пакет даних 1223B, що містить IP-датаграму B. Хоча мікропрограма SDNP 1335H може інтерпретувати корисне навантаження SDNP, що міститься в IP-датаграмі A, підключені пристрої не є SDNP клієнтами. Замість цього SDNP-маршрутизатор 1351 перетворює корисне навантаження SDNP на звичайне корисне навантаження IP. Якщо тільки в пристроях не використовуються додаткові методи безпеки, Остання лінія є небезпечною. Для домашнього використання це небезпечне підключення пристрою часто не є проблемою, оскільки останнє підключення відбувається всередині будинку. Якщо хакер фізично не вторгається в будинок, щоб підключити прослуховування, такі дротові з'єднання неможливо прослуховувати. До останніх дротових домашніх ліній на пристрої, що не є SDNP, належать Ethernet 106A, показані на прикладі підключення до настільного комп'ютера 36 і модема 103C або HDMI-2, підключеного до телевізора 39.

Оскільки SDNP-з'єднання і гіперзахищений зв'язок поширюються тільки на маршрутизатор 1351 SDNP, для забезпечення безпеки дротових з'єднань Остання Лінія повинна покладатися на автентифікацію і шифрування. Для Ethernet така безпека може використовувати будь-яку кількість методів безпеки (http://www.computerweekly.com/feature/iSCSI-security-Networking-and-security-options-available), включаючи iSCSI, що працюють на рівнях від 1 до 3, таких як робота віртуальних локальних мереж або віртуальних мереж VLAN із використанням шифрування серед аутентифікованих пристроїв. Альтернативно, безпека може бути досягнута за допомогою методів рівнів від 4 до 6 за допомогою "IP Security" або IPSec інфраструктури. Початково розроблена для зберігання даних і представлена компанією Cisco в якості галузевого стандарту, IPSec пропонує два режиму безпеки. У режимі "Заголовок автентифікації" пристрій може розпізнавати відправника даних. У цьому режимі поле даних шифрується, але заголовок використовує розпізнавану IP-адресу. При інкапсуляції корисного навантаження системи безпеки (ESP), також відомої як тунельний режим, весь IP пакет, включаючи заголовок IP, зашифрований і вкладений в новий незашифрований IP пакет, щоб маршрутизація могла працювати правильно і пакет міг досягти свого призначення в мережі.

У будь-якому випадку, безпека залежить від пристроїв автентифікації, що дозволяють їм підключатися до мережі. У домашніх мережах, наприклад, у персональних мережах, підключених до комп'ютерів, загальних накопичувачів, IoT та інших пристроях, апаратне забезпечення, підключене до мережі, змінюється не часто. У таких випадках автентифікація, по суті, включає в себе процес реєстрації пристрою, що отримує доступ до мережі або маршрутизатора. Замість ідентифікації особи конкретного користувача, цей тип автентифікації застосовується між пристроями, зазвичай з використанням тега пристрою, імені або ідентифікаційного номера для ідентифікації та розпізнавання пристроїв, допущених до підключення. Встановлення мережевого з'єднання включає в себе етап налаштування, коли пристрої вперше представлені один одному і схвалені користувачем для підключення, за яким слідує автоматична послідовність автентифікації кожен раз, коли дротовий пристрій фізично підключається до іншого або по Wi-Fi, коли два пристрої знаходяться в межах досяжності один одного. Етап встановлення, що називається ідентифікаційним сполученням, також може називатися реєстрацією пристрою, з'єднанням пристрою, сполученням пристрою, сполученням або парним сполученням. Аналогічний процес використовується з пристроями для підключення навушників Bluetooth до мобільного телефону або для сполучення мобільного телефону Bluetooth з аудіосистемою автомобіля з функцією гучного зв'язку. До протоколів належать: протокол перевірки автентичності за запитом (CHAP), протокол взаємної аутентифікації двох співрозмовників перед встановленням зв'язку між ними в умовах незахищеного каналу (Kerberos V5), прикладний програмний інтерфейс загальних служб безпеки (GSS-API), протокол парольної аутентифікації (SRP), протокол передачі даних для автентифікації, авторизації та

адміністрування сервісів (RADIUS). Деякі методи, такі як RADIUS, засновані на методах шифрування, були вразливими до криптоаналізу, але все ще використовуються в поєднанні з іншими методами.

Так як Ethernet-комунікація захищає пристрої ідентифікації, такі як модем Ethernet 103C, вихід модема, що складається з аналогових телефонних сигналів, що передаються по мідній витій парі 7 до бездротового телефону 5A і домашнього телефону 37, тому Остання Лінія не є безпечною. Крім того, формат зв'язку бездротового телефону 5A небезпечний і підлягає прослуховуванню та спостереженню. З цієї причини, використання домашніх телефонів у захищеному зв'язку не рекомендується.

Поширення відеоматеріалів також є предметом інтересу в безпеці. Наприклад, під час передачі даних між маршрутизатором SDNP 1351 і HDTV 39 формат відео зв'язку, такий як мультимедійний інтерфейс високої чіткості (HDMI), цифровий інтерфейс дисплея DisplayPort (DP), стандарт для передачі відеозображення на цифрові пристрої відображення Digital Visual Interface (DE), менш популярний цифровий відео інтерфейс для високоякісної нестиснутої передачі відео з цифрового відеоапаратури Gigabit Video Interface (GVIF) або Уніфікований цифровий інтерфейс (UDI) зазвичай включає фізичне підключення до HDTV або монітора дисплея. Початково безпека цього зв'язку і її даних була предметом для обговорення кіностудій і контент-провайдерів, з упором на запобігання незаконного копіювання і розповсюдження матеріалів, захищених авторським правом. Одним із протоколів безпеки, розроблених Intel Corp. для забезпечення безпеки відео зв'язку, є високошвидкісний захист цифрового контенту (High-bandwidth Digital Content Protection або HDCP) (https://en.wikipedia.org/wiki/High-bandwidth_Digital_Content_Protection). Спочатку ця система призначалася для запобігання відтворення зашифрованого HDCP контенту на несанкціонованих пристроях. Перед відправкою контенту система перевіряє авторизацію ТВ-приймача або дисплея. Тому DHCP використовує автентифікацію для запобігання отримання даних без ліцензії, шифрує дані для запобігання прослуховування інформації та відкликання ключів у зламаних пристроїв.

За допомогою HDCP потік контенту від модема до телевізора може бути захищений автентифікацією, тобто за допомогою зв'язку ідентифікаційних даних. Однак з появою smart телевізорів потік даних стає двонаправленим. Як засіб, що полегшує передачу потокових даних, тобто від телевізора до модема або приставки, починаючи з версії 1.4, HDMI інтегрує високошвидкісний двонаправлений канал даних, відомий як HEC або HDMI Ethernet Channel. Цей канал даних означає, що HDMI-підключені пристрої можуть відправляти і приймати дані через Ethernet зі швидкістю 100MC/сек, що робить їх готовими до роботи в додатках на базі IP, таких як IP-TV. Канал HDMI Ethernet дозволяє пристроям HDMI з підтримкою Інтернету спільно використовувати підключення до Інтернету по каналу HDMI, без необхідності використання окремого кабелю Ethernet. Таким чином, безпечний зв'язок може бути підтриманий через HDMI з використанням тих же протоколів безпеки та ідентифікації, що і в Ethernet.

На Рис. 25 використання Wi-Fi роутера 1352 з підтримкою SDNP, тобто Wi-Fi роутера з прошивкою SDNP 1335J, виконує функцію віддаленого шлюзу SDNP. Цей шлюз перетворює пакет даних 1223A, що містить IP-датаграму A, в пакет даних 1223B, що містить IP-датаграму B. Хоча мікропрограма 1335J SDNP може інтерпретувати корисне навантаження SDNP, що міститься в IP-датаграмі A, підключення Замість цього SDNP Wi-Fi роутер 1352 перетворює корисне навантаження SDNP на звичайне корисне навантаження IP і здійснює бездротовий зв'язок з підключеними пристроями через точку доступу Wi-Fi 26 для забезпечення зв'язку по Wi-Fi 29. Якщо тільки в пристроях не використовуються додаткові методи безпеки, Остання лінія є небезпечною. У разі Wi-Fi зв'язку в будинку або офісі, безпека є проблемою, оскільки пакети даних можуть бути прослухані з відстані. Приклади домашніх і офісних пристроїв, підключених до Wi-Fi, включають настільний комп'ютер 36, ноутбук 35, планшет 33, мобільний телефон 32, динаміки 34B, принтер/сканер 34A і загальний накопичувач даних 34C.

Безпека між шлюзом SDNP, тобто SDNP Wi-Fi роутером 1352, і підключеним пристроєм забезпечується використанням будь-якої кількості стандартних протоколів, таких як Wi-Fi Protected Access WPA-II або WPA2 (IEEE 802.11i-2004). Зв'язок WPA2 захищено за допомогою CCMP, протокол блочного шифрування з кодом автентифікації повідомлень Counter Mode Cipher Block Cipher Message Authentication Code Protocol, заснованого на обробці AES 128-бітним ключем і 128-бітним розміром блоку. CCMP забезпечує конфіденційність даних, вимагає автентифікації і встановлює контроль доступу. Автентифікація включає прив'язку ідентифікаційних даних при налаштуванні. Повторна прив'язка повинна виконуватися вручну. Безпека CCMP, хоча і надійна, не є гіперзахищеною, оскільки в ній відсутні анонімні пакети даних і динамічний характер SDNP-з'єднання, що надається клієнтом SDNP.

У прикладі на Рис. 26, для пристроїв, підключених до Інтернету Речей (IoT) в домашній мережі, Wi-Fi роутер 1352 з підтримкою SDNP, тобто Wi-Fi роутер з мікропрограмою SDNP 1335J, виконує функцію віддаленого шлюзу SDNP. Цей шлюз перетворює пакет даних 1223A, що містить IP-датаграму A, в пакет даних 1223B, що містить IP-датаграму B. Хоча мікропрограма SDNP 1335J може інтерпретувати корисне навантаження SDNP, що міститься в IP-датаграмі A, підключені IoT-пристрої не є SDNP клієнтами. Замість цього SDNP Wi-Fi роутер 1352 перетворює корисне навантаження SDNP на звичайне IP навантаження і здійснює бездротовий зв'язок з підключеними пристроями по Wi-Fi каналу 29 з точки доступу Wi-Fi 26. Якщо не будуть реалізовані додаткові методи безпеки, Остання Лінія буде небезпечною, особливо тому, що пакети даних Wi-Fi можуть бути прослухані з відстані. Приклади підключених до Wi-Fi пристроїв Інтернету Речей у будинку включають центральне опалення та кондиціонування повітря 34D, освітлення 34G, жалюзі 34F, великі прилади 34K, портативні та кімнатні системи опалення HVAC 34E, гаражні двері 34L, домашні камери спостереження 34J, і домашню центральну систему безпеки 34H.

Безпека між шлюзом SDNP, тобто маршрутизатором 1352 SDNP Wi-Fi, і підключеним пристроєм забезпечується за допомогою будь-якої кількості стандартних протоколів, таких як вищезазначений протокол Wi-Fi Protected Access Protocol WPA2 з використанням CCMP сприяє конфіденційності даних, потребує автентифікації, і дозволяє налаштувати контроль за доступом. WPA2 досягає безпеки за допомогою прив'язки ідентифікаційних даних, перевірка пристроїв реалізована як протокол другого рівня. Цей метод є громіздким і передбачає використання методів ручної автентифікації.

Альтернативний протокол, який використовується для локальних обчислювальних мереж, нещодавно впроваджений для IoT комунікацій - проксимальна мережа під назвою AllJoyn фреймворк. Фреймворк виявляє пристрої, створює сеанси і забезпечує безпечний зв'язок. Фреймворк розроблений для підтримки підключення пристроїв Інтернету речей з використанням численних транспортних рівнів другого рівня, включаючи Wi-Fi, Ethernet, послідовну шину і лінії електропередач. Програми можуть бути засновані на C, C++, Obj. C і Java, що працюють на різних платформах, включаючи Linux, Windows, MacOS, Android, iOS, RTOS (операційну систему реального часу) і відкрите вихідне середовище розробки Arduino.

Всі сумісні з AllJoyn програми автентифікують один одного і обмінюються зашифрованими даними для забезпечення безпеки на наскрізному рівні. Автентифікація і шифрування даних виконуються на рівні програми 7. Транспортний рівень 2, також званий маршрутизатором, передає повідомлення, пов'язані з безпекою, між кінцевими точками додатків, але не реалізує жодної логіки безпеки. Функція зворотного виклику, відома як "Auth Listener", також реалізована на рівні програми 7, забезпечує автентифікацію з використанням PIN-кодів, паролів або сертифікатів автентифікації. Безпека досягається за допомогою однорангового шифрування AES128. Як і WPA, AllJoyn використовує прив'язку ідентифікаційних даних у процесі автентифікації перед виконанням командних і керуючих послідовностей. Підтримуються такі методи автентифікації: загальний ключ або PSK, протокол парольної аутентифікації (SRP) або вхід з вказанням ім'я користувача і пароля. Протокол також підтримує обмін ключами (еліптична крива Діффі-Хеллмана): (i) без автентифікації, (ii) автентифікації з попередньо обміняним ключем і (iii) автентифікацією за допомогою сертифіката X.509 ECDSA.

Така ж технологія може бути застосована і до комерційних підприємств. У прикладі на Рис. 27 для пристроїв, підключених до IoT в домашній мережі, Wi-Fi і Ethernet роутер 1352Z з підтримкою SDNP, тобто Ethernet і Wi-Fi роутера з встановленою мікропрограмою SDNP 1335J, виконує функцію віддаленого шлюзу SDNP. Цей шлюз перетворює пакет даних 1223A, що містить IP-датаграму A, в пакет даних 1223B, що містить IP-датаграму B. Хоча мікропрограма 1335J SDNP може інтерпретувати корисне навантаження SDNP, що міститься в IP-датаграмі A, підключені IoT-пристрої не є SDNP клієнтами. Замість цього SDNP і Ethernet Wi-Fi роутер 1352Z перетворює корисне навантаження SDNP на звичайне IP корисне навантаження, взаємодіє з підключеними пристроями по Wi-Fi каналу 29 і Ethernet 106A.

Якщо не реалізовані додаткові методи безпеки, Остання Лінія буде небезпечною, особливо для Wi-Fi пакетів даних, які можуть бути прослухані з відстані. Приклади пристроїв Інтернету речей, підключених до Wi-Fi, включають центральне опалення і кондиціонування повітря 34D, освітлення 34G, системи спостереження 34J, системи безпеки 34H, POS-термінали 38 і пристрої, підключені до точки доступу Wi-Fi, такі як планшет 33. Пристрої, що підключаються до дротової мережі підприємства, залежать від характеру бізнесу. У банківській сфері пристрої включають банкомат 38D, підключений до мережі Ethernet. На АЗС пристрої включають, наприклад, газові насоси 38A, підключені до мережі Ethernet.

Таким чином, Остання Лінія може бути захищена не-SDNP клієнтами, які взаємодіють з віддаленим шлюзом SDNP. Таким чином, більша частина "Останньої Милі" є гіперзахищеною, в той час як "Остання Лінія" використовує зашифрований захист з використанням ідентифікаційних даних.

Мости SDNP комунікації – Як описано вище, передача даних у зв'язку "Останній Милі" за межі SDNP хмари обов'язково використовує IP-датаграми, тобто пакети даних з використанням інтернет адрес-джерел і адрес-призначення, або, в якості альтернативи, NAT-адреси оператора мережі. У разі приватних мереж, наприклад, працюючих в межах офісних будівель, або у співпраці з місцевими постачальниками мережевих послуг, які бажають розмістити програмні комутатори SDNP на своїх серверах, можна також використовувати датаграми SDNP для досягнення гіперзахищеності з'єднань на ділянках "Останньої Милі".

Як описано вище, гіперзахищений зв'язок ґрунтується на тому, що сервери використовують програмне забезпечення або мікропрограму SDNP і обмінюються даними з використанням датаграм SDNP і анонімних адрес, а не з IP-датаграмами. В межах SDNP хмари ці сервери SDNP називаються вузлами SDNP, як вказано у позначеннях вузлів $M_{0,0}$, $M_{0,1}$, $M_{1,0}$, $M_{1,1}$, тощо. Вищевказане положення № 14/803, 869 США також розкриває зв'язок між кількома незалежними хмарами SDNP, з'єднаними мостами SDNP – шлюзами SDNP, що маршрутизують IP-датаграми до інших хмар SDNP.

Концепція мосту SDNP може бути аналогічно адаптована для використання на ділянках зв'язку "Останньої Милі". Для створення підмереж SDNP або міні-хмар в межах "Останньої Милі" необхідно включити два або більше сервери за допомогою програмного забезпечення або мікропрограми мосту SDNP. На відміну від клієнтського ПЗ SDNP або мікропрограми, що працює на кінцевому пристрої, тобто в пристрої, що викликає, для маршрутизації даних використовується операція моста SDNP, а не для зв'язку в якості кінцевого з'єднання. Таким чином, два або більше суміжних мости SDNP можуть працювати як окрема мережа мостів SDNP, міні-хмари SDNP або як мережа SDNP спеціального призначення. Функція мосту SDNP, як описано вище, являє собою конструкцію третього рівня, аналогічну опису роботи режиму моста другого рівня Wi-Fi маршрутизатора. В межах моста SDNP або мережі мостів SDNP зв'язок здійснюється за допомогою датаграм SDNP. Для зв'язку з мостом SDNP поза межами мосту SDNP або з мережею мостів SDNP використовуються IP-датаграми з корисним навантаженням SDNP.

Робота мосту SDNP в рамках комунікації "Останньої Милі" показана на Рис. 28, що складається з мережі SDNP зі шлюзом SDNP 1201A, моста SDNP з маршрутизаторами SDNP 1350 і 1352Z з мікропрограмою SDNP 1335H і 1335J відповідно і підключеного клієнтського пристрою, що не є клієнтом SDNP, схематично представленого у вигляді ноутбуку 35. Як показано на Рис. , зв'язок між шлюзом SDNP 1201A і мостом SDNP 1350 являє собою захищене з'єднання з використанням IP-датаграми 1223A з IP-адресою і корисним навантаженням SDNP. Корисне навантаження SDNP 1222A, у свою чергу, містить інформацію про маршрутизацію SDNP і безпечне корисне навантаження SDNP, закодоване за допомогою спеціальних облікових даних безпеки зони. Таким чином, гіперзахищеність досягається за допомогою корисного навантаження SDNP, навіть якщо використовується маршрутизація по IP-адресу.

В межах мосту SDNP, тобто між маршрутизатором 1350 і Wi-Fi маршрутизатором 1352Z, гіперзахищене з'єднання здійснюється за допомогою датаграми SDNP 1222B. Інформація про маршрутизацію SDNP витягується з адресації SDNP, що міститься в корисному навантаженні SDNP 1222A. У сукупності SDNP-міст і SDNP-з'єднання являють собою дротовий канал гіперзахищеного зв'язку "Останньої Милі", здатний підтримувати ідентифікацію і перевірку облікового запису, а також конфіденційність.

При підключенні від SDNP-мосту маршрутизатора 1352Z до клієнтського пристрою, відмінного від SDNP, тобто ноутбука 35, використовується IP-датаграма 1223B з IP-адресою і корисним навантаженням по локальній мережі, Wi-Fi або Ethernet. Безпека цієї Останньої Лінії, хоча і не є гіперзахищеною, забезпечується будь-яким з вищезгаданих протоколів безпеки Ethernet і Wi-Fi, таких як iSCSI, IPSec, WPA, AllJoyn та інші.

Реалізація мосту SDNP може відбуватися між будь-якими двома пристроями з підтримкою SDNP, що підтримують будь-яку кількість фізичних носіїв, що означає, що міст SDNP є протоколом третього рівня, що працює незалежно від реалізацій першого фізичного PHY 1 і другого транспортного 2 рівнів. Наприклад, на верхній схемі, показаній на Рис. 29A, два мостових маршрутизатора SDNP 1351A з Ethernet-мостом SDNP і вбудованим ПЗ 1335H підтримують зв'язок по Ethernet- (дротовому) мосту за допомогою датаграми 1222 SDNP. У центральній схемі з'єднань два маршрутизатори 1352Z з мостом SDNP, кожен з яких підтримує Ethernet і Wi-Fi зв'язок і підтримує мікропрограму SDNP 1335J, взаємодіють по Wi-Fi

(бездротовому) мосту за допомогою датаграми 1222 SDNP. На найнижчій схемі на мосту SDNP маршрутизатор Ethernet з мікропрограмою SDNP зв'язується по Ethernet (дротовому) мосту за допомогою датаграми 1222 SDNP з маршрутизатором, що підтримує Ethernet і Wi-Fi зв'язок і підтримує мікропрограму SDNP 1335J. Таким чином, міст SDNP, що складається з двох або більше маршрутизаторів з підтримкою SDNP, може маршрутизувати або розділяти датаграми SDNP по будівлі або приватній мережі, навіть якщо вони працюють поза хмарами SDNP в "Останній Милі".

SDNP-міст може бути розширений на системи, що використовують власне обладнання, наприклад, системи кабельного телебачення. Наприклад, на верхній схемі, показаній на Рис. 29B, два "головні" кабельні сервери CMTS модифіковані для роботи з мікропрограмою SDNP або програмним забезпеченням 1335L для роботи в якості кабельних CMTS SDNP мостів 101 і зв'язуватись по кабельному або оптоволоконному (дротовому) мосту за допомогою датаграми 1222 SD. SDNP-міст може простягатися від "голови" CMTS в будинок абонента. Як показано на схемі в центрі, кабельний CMTS SDNP міст 101 з мікропрограмою SDNP або програмним забезпеченням 1335L здійснює зв'язок за допомогою SDNP датаграми 1222 через кабельний (коаксіальний) міст до приставки кабельного телебачення або кабельного модему 102 з підтримкою мікропрограми SDNP 1335M. Таким чином, міст SDNP розширює гіперзахищену взаємодію на будинок або офіс.

Розглянуті методи SDNP-мосту можуть також використовуватися для передачі даних по радіо мережам. На нижній схемі Рис. 29B дві базові станції стільникового зв'язку і радіовишки з мікропрограмою SDNP або програмним забезпеченням 1335N функціонують як SDNP мости базових станцій стільникового зв'язку17X і 17Y, щоб забезпечувати бездротовий зв'язок по стільниковій мережі, що складається з мостів 25X і 25Y з використанням датаграм SDNP 1222. На верхній схемі Рис. 29C наземна мікрохвильова базова станція з мікропрограмою SDNP або програмним забезпеченням 1335O функціонує як SDNP-міст "земля-супутник" 92C для зв'язку в режимі мікрохвильового супутникового мосту з використанням датаграм SDNP 1222 з орбітальним супутником, що підтримує мікропрограму або програмне забезпечення SDNP 1335P, тобто до моста SDNP супутника. Потім супутник, у свою чергу, зв'язується з абонентами або з іншими супутниками.

Мостовий зв'язок SDNP може бути адаптований до автомобільних додатків, що використовують автомобілі в якості спеціальної однорангової мережі зв'язку. На нижній схемі Рис. 29C телематичний модуль в автомобілі 1390A з мікропрограмою SDNP 1335F взаємодіє по автомобільному радіо мосту за допомогою SDNP датаграми 1222 з найближчим автомобілем 1390B, в якому також встановлена мікропрограма SDNP 1335F. Кожен автомобіль з увімкненою мікропрограмою SDNP утворює ще один вузол зв'язку в динамічній телематичній мережі SDNP мосту. Цей зв'язок не є передачею інформації конкретному автомобілю або водієві, а формує комунікаційну мережу, здатну передавати інформацію по шосе навіть за відсутності вежі стільникового зв'язку на місці.

Концепція мостових мереж SDNP особливо корисна для зв'язку у великих географічних регіонах, а також при пасажиро- і вантажоперевезеннях легковими автомобілями, вантажними машинами, машинами швидкої допомоги, поїздами, літаками, катерами і морськими суднами. Зокрема, для забезпечення широкого покриття всієї території дії мережі зв'язку необхідні супутникові мережі. Зазвичай ця система передбачає підключення до мережі супутникового оператора, іменованого супутниковим мостом або транзитною мережею, і супутниковий зв'язок зі своїми клієнтами і абонентами, також відомий як супутникове розподілення. Рис. 30 схематично представляє різні супутникові з'єднання, адаптовані для гіперзахищеного SDNP зв'язку. Як показано на Рис. , шлюз SDNP 1201A, взаємодіючи з наземною супутниковою антеною 92C, працює під управлінням мікропрограми або програмного забезпечення SDNP 1335O, використовуючи дротове з'єднання 94A, несучий пакет даних 1222A, що складається з датаграми A SDNP і корисного навантаження SDNP, які в свою чергу передають таку ж SDNP датаграму A, як пакет даних 1222B через супутниковий міст 95A на супутник 93, що містить прошивку або програмне забезпечення 1335P SDNP.

Розподілення пакетів даних гіперзахищеного зв'язку зі супутника SDNP 93 між різними клієнтами включає пакет даних 1222C і пакет даних SDNP-A з корисним навантаженням SDNP. Супутниковий зв'язок є двонаправленим, з низхідною лінією від супутника 93 до наземних клієнтів, здатною забезпечити більш високий рівень сигналу і більш високу швидкість передачі даних, ніж висхідна лінія зв'язку. Іншими словами, супутник може передавати земному клієнту більш високі швидкості передачі даних і з більшою інтенсивністю сигналу, ніж відповідь клієнта. Приклади супутникових 93 каналів зв'язку з абонентами включають супутниковий зв'язок 95B для антени 92G абонента Інтернету 92G, для якого працює мікропрограма SDNP 1335T,

супутниковий телефон 92F з мікропрограмою SDNP 1335S, встановлену супутникову антенну мережу 92H на високошвидкісному поїзді 1360C з мікропрограмою SDNP 1335G, встановлену супутникову антенну мережу 92E на океанському судні 1360B з мікропрограмою SDNP 1335R, а також встановлену супутникову антенну мережу 92D на повітряному судні 1360A з мікропрограмою SDNP 1335Q.

У разі великих транспортних засобів, таких як кораблі, літаки і поїзди, кожна система підключає цей канал супутникового гіперзахищеного зв'язку до власної внутрішньої системи зв'язку або локальної мережі. Рис. 31A, наприклад, ілюструє комерційний літак, де супутниковий антенний модуль 92D з мікропрограмою SDNP 1335X, встановлений на фюзеляжі літака 1360A, підключається до центрального сервера зв'язку 1361 з програмним забезпеченням SDNP 1335Z. Центральний комунікаційний сервер 1361 підключається до різних систем, включаючи прилади 1367, реєстратор даних і "чорну скриньку" 1368, модуль зберігання даних 1363 і модуль 1362, опціонально з мікропрограмою SDNP 1335L. Модуль Wi-Fi маршрутизатора 1362 підключається до мережі антен 1361, розташованих по всьому літаку, для забезпечення зв'язку в точці доступу Wi-Fi. Весь зв'язок, за винятком радіоуправління польотом, здійснюється за загальною супутниковою лінією зв'язку з використанням антенного модуля 92D, як показано на прикладі Рис. 31B. Антенний модуль включає в себе передавальну супутникову антену 1360A, приймальну супутникову антену 1368A, блок курування 1369 і регулятор напруги 40W 1370. Супутникова приймальня антена 1368A менше, ніж антена супутникової передачі 1360A, тому що потужність і рівень сигналу супутникового мовлення більше, ніж широкомовна потужність антени і можливості висхідного зв'язку.

Супутниковий зв'язок корабля використовує кілька діапазонів супутникового зв'язку, включаючи супутники на великій висоті і навколоземній орбіті. Наприклад, Рис. 32 ілюструє використання декількох діапазонів зв'язку, включаючи супутникову антену Ku-діапазону 1383A і низькоорбітальні супутникові антени 1383B і 1383C. Висотні супутники не мають можливості або обмежені в можливостях висхідного зв'язку, але здатні покривати великі площі з великих висот, включаючи геосинхронні орбіти. Завдяки великій висоті над рівнем моря, площа покриття кожного супутника є значною, як показано на карті 1384. Як показано на карті 1385, супутники на низькій навколоземній орбіті охоплюють менші площі, що вимагає більшої кількості супутників і, отже, більш високих витрат на покриття області мовлення. Залежно від курсу судна доступ до низькоорбітальних супутників може бути переривчастим залежно від орбітального положення супутників.

Оскільки супутникова антена діапазону Ku 1383A в основному використовується для поширення телевізійного і відео контенту, безпека SDNP, як правило, не потрібна. Відстеження і позиціонування здійснюється за допомогою антени управління 1383. Багатоканальні дані із супутникової антени 1383A надходять у багатоканальний L-діапазон 1381, розділяючи сигнали на фіксовані відеосигнали, що передаються на телевізійні приймачі і тюнери 1382 і цифрове мовлення DVB даних. Відео контент подається на центральні комунікаційні сервери 1380. Однак, якщо потрібен безпечний зв'язок, супутникова антена Ku-діапазону 1383A може бути адаптована для роботи з програмним забезпеченням SDNP.

Дані з низькоорбітальних супутникових антен 1383B і 1383C, що працюють на мікропрограмі SDNP 1335U і 1335V, передають інформацію із супутникових антен на центральні комунікаційні сервери 1380, що працюють за SDNP 1335Z. У радіусі дії суші система зв'язку також здатна здійснювати зв'язок з використанням стільникової мережі 4G/LTE 25, розміщеної на базовій станції 17 стільникового зв'язку з мікропрограмою SDNP 1335N. Зв'язок через сервери 1380 розділено по судну за допомогою SDNP Wi-Fi маршрутизатора 1362 з мікропрограмою SDNP 1335L. Точка доступу Wi-Fi точка 26 розділена по судну за допомогою антен Wi-Fi 1361. Зв'язок з клієнтами SDNP, такими як стільниковий телефон 32 з додатком SDNP 1335, полегшує наскрізне гіперзахищене з'єднання. Пристрої, не включені як клієнти SDNP, повинні покладатися на сполучення ідентифікаційних даних за допомогою WAP, AllJoyn або інших протоколів безпеки.

Рис. 33 ілюструє застосування багатосмугового зв'язку у високошвидкісних поїздах. Як показано на Рис. , сервер залізничного дата-центру 1380 з програмним забезпеченням SDNP 1335Z, підключеним до шлюзу SDNP 1201A, з'єднується з високошвидкісним поїздом 1360C через кілька фізичних PHY з'єднань, включаючи супутниковий мікрохвильовий зв'язок 95B, 400MHz радіо 1372 і 60Ghz НВЧ 1373. Під час обміну даними SDNP центр обробки даних SDNP 1380 передає дані через супутникову антену 92C з мікропрограмою SDNP 1335D на супутник 93 з мікропрограмою SDNP 1335P. Супутник зв'язується із залізничною антеною 1383V, підключеною до сервера 1361, на якому встановлено програмне забезпечення SDNP 1335Y. Альтернативний зв'язок можливий від SDNP центру обробки даних 1380 до 400 МГц антени

1381 або 60 ГГц антени 1382, розташованої через регулярні проміжки часу вздовж залізничних колій. Ці супутники також підтримують зв'язок з антеною 1383B, підключеною до SDNP сервера поїзду 1361, на якому встановлено програмне забезпечення SDNP 1335Y. Зв'язок, отриманий SDNP-сервером 1361, потім розподіляється по поїзду по Wi-Fi мостах 1335Z, а клієнтам – у вигляді точок доступу Wi-Fi.

Функція комунікацій в автомобілебудуванні та професійних вантажоперевезеннях багатогранна і включає в себе наступне:

- Голосовий зв'язок
- Навігація, карти, інформація про дороги, оповіщення
- Розваги, hotspot-послуги, інформаційно-розважальні послуги
- Бездротові платежі, плата за проїзд
- Служби екстреної допомоги, придорожня допомога
- Служби запобігання зіткненням
- Розклад роботи диспетчерських центрів

Додаткові функції необхідні також для автономних транспортних засобів, тобто для автомобілів з автоматичним керуванням. Засновані в основному на старих стільникових мережах, таких як керований центральний блок CDMA (2.5G), званий "телематичним" модулем, існуючі автомобільні системи надзвичайно вразливі до хакерських атак, кібератак і атак на конфіденційність. Для усунення цієї вразливості вся мережа повинна бути захищена без значних витрат, тобто установка нової мережі не повинна бути фінансово проблемним варіантом. Замість цього, інфраструктура безпеки повинна бути накладена "поверх" апаратної мережі в якості методів безпеки, розгорнутих на Рівнях від 3 до 7. Ця стратегія сумісна з реалізаціями "Останньої Милі" SDNP, описаними тут.

Рис. 34 ілюструє приклад гіперзахищеного з'єднання "Останньої Милі" між автомобілем і хмарою SDNP. Як і в попередніх з'єднаннях "Останньої Милі", конкретні носії даних, що беруть участь у транспортуванні пакетів через "Останню Милю", можуть істотно відрізнятися залежно від місця розташування. Таким чином, показано приклад, що представляє гіперзахищений зв'язок незалежно від використовуваних носіїв даних. Як показано на Рис. , шлюз SDNP 1201A підключається до мережевого маршрутизатора 67A через дротове або оптоволоконне з'єднання 24, кероване постачальником мережевих послуг (NSP), перетворюючи пакет даних 1222A, що містить SDNP датаграму A в пакет даних 1223A, що містить IP датаграму B з корисним навантаження SDNP. Мережевий маршрутизатор 67A потім направляє IP-датаграму B у вигляді пакету даних 1223B на базову станцію стільникового зв'язку 17 по дротовій або оптоволоконній лінії 24A, що належить оператору мобільного зв'язку (MNO) або керованої ним. Потім пакет даних IP B передається по бездротовому зв'язку по стільниковій мережі 25 у вигляді пакета даних1223C, що містить SDNP датаграму B з корисним навантаженням SDNP в телематичний модуль автомобіля 1390A з використанням стільникового зв'язку 28, використовуючи 2.5G, 3G, 3.5G, або 4G/LTE в залежності від оператора стільникової мережі, діючого в регіоні. Мікропрограма SDNP 1335F, що працює в модулі телематики, інтерпретує корисне навантаження SDNP, вбудоване у вхідний пакет даних 1223C для завершення гіперзахищеного з'єднання. Таким чином, автомобільне стільникове з'єднання "Останньої Лінії" функціонує як частина гіперзахищеного зв'язку "Останньої Милі".

Як показано на Рис. 35, телематичний модуль автомобіля 1390A потім використовує захищену інформацію для різних функцій, керованих інформаційно-розважальним інтерфейсом 1377. Внутрішня точка доступу Wi-Fi 1362D також розподіляє пакети даних 1223B і 1223C, що містять IP-датаграму B і IP-датаграму C, відповідно. IP-датаграма B містить корисне навантаження SDNP, яке полегшує наскрізне гіперзахищене з'єднання з будь-яким клієнтом SDNP, таким як стільниковий телефон 32B з SDNP додатком 1335. IP-датаграма C, що використовує тільки звичайне IP корисне навантаження, менш безпечна, але працює з пристроями, що не працюють в якості SDNP клієнтів, такими як мобільний телефон 32A і планшет 33A. Зв'язок ідентифікаційних даних може бути використано для поліпшення безпеки "Останньої Лінії" для пристроїв без протоколу SDNP за допомогою WPA, AllJoyn або інших протоколів.

Іншою важливою функцією автомобільного зв'язку є зв'язок між транспортними засобами, також званий Vehicle-to-Vehicle, або V2V-зв'язком. V2V-зв'язок призначений в першу чергу для запобігання зіткнень. Але відповідно до описаних тут методів SDNP, комунікації V2V можуть також функціонувати як спеціальні пірингові гіперзахищені мережі. Такий міжтранспортний SDNP зв'язок проілюстровано на Рис. 36, де автомобілі 1390A, 1390B і 1390C з мікропрограмою SDNP 1335F утворюють пірингову мережу один з одним і з базовою станцією 17, підключеною

до шлюзу SDNP 1201A. Зв'язок між транспортними засобами може здійснюватися з використанням або IP-датаграм, або SDNP-датаграм.

Якщо клієнт SDNP або шлюз взаємодіє з пристроєм, який не є SDNP, зв'язок здійснюється за допомогою IP-датаграм. Наприклад, шлюз SDNP 1201A перетворює датаграму A SDNP з корисним навантаженням SDNP на пакет даних 1223A, що містить IP-датаграму B з вбудованим корисним навантаженням SDNP. Як показано на Рис. , базова станція 17 здійснює зв'язок з автомобілем 1390A по стільниковому зв'язку 2.5G або 3G 28A, або використовуючи пакет даних 1223B, що містить IP-датаграму B з вбудованим корисним навантаженням SDNP, але здатний взаємодіяти з автомобілем 1390C по стільниковому зв'язку 3.5G або 4G/LTE 28B, або, використовуючи пакет даних 1223C, що також містить IP-датаграму B з вбудованим корисним навантаженням SDNP. Таким чином, корисне навантаження SDNP розподіляється незалежно від мережі, яка використовується для передачі пакетів даних.

Автомобілі, що підтримують мікропрограму SDNP 1335F, можуть також утворювати спеціальні однорангові SDNP мости або мостові мережі. Наприклад, автомобіль 1390A зв'язується з автомобілем 1390B по V2V-радіоканалу 1391A, використовуючи пакет даних 1222B, що містить SDNP датаграму C, а не IP-датаграму. Аналогічним чином, автомобіль 1390B зв'язується з автомобілем 1390C по V2V-радіоканалу 1391B, використовуючи пакет даних 1222C, що містить SDNP датаграму D, і не покладається на IP-датаграми. Незалежно від типу датаграми, вбудований контент залишається гіперзахищеним з корисним навантаженням SDNP.

Іншою особливістю V2V SDNP мережі спеціального призначення є її здатність виконувати функції тунелювання, тобто передавати дані з одного транспортного засобу на інший без можливості моніторингу та інтерпретації даних. У разі збою стільникового зв'язку 28B через те, що автомобіль 1390C знаходиться поза зоною покриття, в якості альтернативного шляху стільникова базова станція 17 може використовувати мостову мережу SDNP для досягнення того ж абонента, як показано на прикладі стільникового зв'язку 28A, V2V 1391A і, нарешті, V2V радіозв'язку 1391B. Під час передачі пакети даних 1223B, 1222B і 1222C змінюються з IP-датаграми B на SDNP датаграму C і, нарешті, на SDNP датаграму D. Оскільки корисне навантаження SDNP для автомобіля 1390C створено спеціально для цільового автомобіля, автомобіль 1390B і його пасажири не можуть зламати або контролювати вміст SDNP датаграми C, навіть якщо вони передають пакет даних 1222B через мережу спеціального призначення.

Крім традиційного зв'язку "Останньої Милі", та ж технологія SDNP-мосту може бути використана для передачі великих обсягів даних за допомогою гіперзахисту на великі відстані, тобто цифрового магістрального зв'язку. Три таких приклади наведено на Рис. 37, а саме: мікрохвильовий 98, волоконно-оптичний 90 і супутниковий 95A канали передачі даних 95B. Хоча цю функцію можна розглядати як частину хмари SDNP, єдиний маршрут передачі даних аналогічний маршруту зв'язку "Останньої Милі", і тому використовує схожі методи для забезпечення гіперзахищеності. Наприклад, сервери 21A і 21B, що працюють з програмним забезпеченням SDNP 1335Z, можуть обмінюватися даними по каналу мікрохвильового зв'язку 98 через станції 96A і 96B, що працюють з мікропрограмою SDNP 1335W, використовуючи пакет даних 1222, що містить датаграми SDNP, або сервери 21A і 21B можуть аналогічно можуть здійснювати прямий зв'язок через волоконну магістраль 98, також використовуючи пакет 1222 даних, що містить датаграми SDNP. У глобальному комунікації, наприклад, у транстихоокеанському каналі зв'язку, сервери 21A і 21B можуть взаємодіяти із супутником 93, що працює з мікропрограмою SDNP 1335B, за допомогою мікрохвильових супутникових магістралей 95A і 95B, використовуючи наземні супутникові антени 92A і 92B, які обидві працюють з мікропрограмою SDNP 1335U. Як і в прикладах волоконно-оптичних і мікрохвильових вишок, у магістральному супутниковому зв'язку використовується пакет даних 1222, що містить датаграми SDNP.

У заключенні, функції безпеки та конфіденційності, пропоновані в комунікації "Останньої Милі", залежать від двох взаємодіючих пристроїв. Рис. 38 контрастує з чотирма різними комбінаціями, що представляють собою, за порядком знизу вгору, підвищення безпеки і конфіденційності. У кожному випадку враховуються три фактори: i) безпека, можливість запобігання несанкціонованого доступу до комунікації, ii) перевірка посвідчення особи, можливість автентифікації користувача та коригування доступу і привілеїв на основі його особи та iii) анонімність, можливість приховати особу викликаючих абонентів від спостереження.

У нижньому прикладі шлюз SDNP 1395 відкрито спілкується з не-SDNP клієнтом, який не має жодних гарантій безпеки, використовуючи пакет даних 1223C, що складається з IP-датаграми з уразливою до прослуховування IP-адресою і корисним навантаженням. Таким чином, з'єднання "Останньої Милі" не є безпечним і конфіденційним. У прикладі, другому знизу,

шлюз SDNP 1395 взаємодіє з клієнтом, який не є SDNP, пропонуючи функції авторизації та сполучення пристроїв. Зв'язок здійснюється за допомогою пакета даних 1223B, що містить IP-датаграму з уразливою до прослуховування IP-адресою, але з використанням зашифрованого корисного навантаження, що містить шифрований текст, де дешифрування може виконувати тільки пристрій з обмеженою ідентифікацією. Хоча зв'язок не є приватним або анонімним, він забезпечує підвищену безпеку, принаймні протягом обмеженого періоду часу.

Приклад зверху ілюструє, що шлюз SDNP 1395 може маршрутизувати комунікації через будь-який міст або маршрутизатор 1397 і при цьому досягти гіперзахищеності, за умови, що пакет даних 1223A містить корисне навантаження SDNP в IP-датаграмі. Досягнутий рівень безпеки залежить тільки від кінцевого пристрою, а не від маршрутизатора. У прикладі вище, обмін даними між шлюзом SDNP 1395 і клієнтом SDNP 1396 з використанням пакетів даних 1222, що містять датаграми SDNP з адресою SDNP, тобто з використанням адрес джерела і призначення, не розпізнаваних серверами DNS і з використанням безпечного корисного навантаження SDNP, є гіперзахищеним, що забезпечує чудову безпеку, повне дотримання конфіденційності та анонімну маршрутизацію пакетів.

Маршрутизація пакетів всередині гіперзахищеної "Останньої Милі" – Незалежно від алгоритму, який використовується, і методів фізичного обладнання і каналу передачі даних першого і другого рівнів, маршрутизація пакетів між клієнтом SDNP або мостом SDNP і шлюзом SDNP залежить від IP-датаграм для передачі і маршрутизації пакетів даних через "Останню Милю". На відміну від маршрутизації даних всередині SDNP хмари, що направляється сигнальними серверами SDNP, SDNP хмара або її сигнальні сервери не контролюють IP-датаграми, що проходять через "Останню Милю". У зв'язку з цим слід очікувати деякої змінності в затримках поширення "Останньої Милі". На щастя, через обмеженість відстаней зв'язку "Останньої Милі" і кількості можливих маршрутів ця невизначеність невелика порівняно із загальною наскрізною затримкою поширення глобального зв'язку. Зміна загальних затримок поширення через змінність "Останньої Милі" оцінюється менш ніж на 10 % від сукупної затримки.

Рис. 39 ілюструє єдиний маршрут з'єднання "Останньою Милі" між клієнтом SDNP 1400 і шлюзом SDNP 1401 з використанням фіксованих IP-адрес. IP-датаграма 1405 включає IP-адресу призначення $M_{0,0}$ (шлюз SDNP) і IP-адресу джерела пакета даних $C_{1,1}$ — клієнта SDNP. Останнє з'єднання відбувається за одним маршрутом 1404 до маршрутизатора 1402A. Дані направляються через будь-яку кількість маршрутизаторів R, наприклад, маршрутизатор 1402B, на шлюз SDNP $M_{0,0}$.

Альтернативне представлення мережевого підключення "Останньої Милі" описує кожен комунікаційний пристрій як IP-стек, що представляє PHY, канал передачі даних і мережеві з'єднання як рівні OSI 1, 2 і 3. Наприклад, на Рис. 40A показаний IP-стек, що являє собою одномаршрутне гіперзахищене з'єднання "Останньої Милі" з використанням статичних IP-адрес. Таким чином, клієнтський пристрій, що складається з клієнта SDNP $C_{1,1}$ встановлює єдиний маршрут з'єднання "Останньої Милі" 1409 зі шлюзом SDNP 1401, що включає шлюз SDNP $M_{0,0}$ через маршрутизатори 1402A і 1402B, де маршрутизатор 1402A включає Wi-Fi, а маршрутизатор 1402B-Ethernet-роутер. Клієнтський пристрій 1400 підключається до маршрутизатора 1402A через "Останню Лінію" 1404, де фізичне з'єднання PHY рівня 1 і відповідний канальний рівень 2 клієнтського IP стека 1411 з'єднуються з відповідними рівнями 1 і 2 в IP-стеці 1412A маршрутизатора.

У свою чергу, роутер 1402A підключається до роутера 1402B через Ethernet, де фізичне з'єднання PHY рівня 1 і відповідний канал передачі даних рівня 2 IP-стека 1412A Wi-Fi роутера з'єднуються з відповідними рівнем 1 і рівнем 2 в IP стеку 1412B Ethernet роутера. Нарешті, маршрутизатор 1402B підключається до сервера шлюзу SDNP 1401 через Ethernet, де фізичне з'єднання PHY рівня 1 і відповідний канал передачі даних рівня 2 IP-стека 1412B маршрутизатора Ethernet підключаються до відповідних рівня 1 і рівня 2 в IP-стеці шлюзу 1422. У процесі роботи маршрутизатори передають дані без перешкод, так що мережеві датаграми третього рівня непомітно передаються з одного IP-стека в інший, зокрема з третього рівня в IP-стеці 1411-1412A, 1412B і, нарешті, в 1422. Таким чином, мережа передає IP-датаграми у вигляді одного маршруту через віртуальне з'єднання "Останньої Милі" 1409, навіть якщо дані фізично передаються через кілька пристроїв.

Іншими словами, мережеві потоки даних Рівня 3 проходять через "Останню Милю" незалежно від фізичних з'єднань, що використовуються для передачі IP-даних, тобто зв'язок рівня 3 "Останньої Милі" працює агностично на нижчі рівні 1 і 2, що використовуються для передачі даних. Цей принцип може бути представлений у спрощеному вигляді шляхом видалення проміжних вузлів зі схеми з'єднань, як показано на Рис. 40B, де клієнтські пристрої

1400 і сервер шлюзу SDNP 1401, включаючи IP-стеки зв'язку 1411 і 1422, що передають дані на відповідні обчислення і функції зберігання даних 1410 і 1421 і назад. IP-датаграма 1405 проходить через з'єднання "Останньої Милі" 1409 незалежно від носія або кількості маршрутизаторів, що використовуються в процесі доставки пакетів даних. Таким чином, "Останню Милю" можна розглядати як "конструкцію даних", тобто абстракцію, що означає будь-які і всі фізичні засоби, якими IP-датаграма передається між пристроями і між ними. Останнє з'єднання, однак, має більше фізичне значення, оскільки підключений пристрій абонента не може бути встановлений на маршрутизаторі вхідного каналу зв'язку. Наприклад, якщо викликаючий абонент має планшетний комп'ютер тільки з Wi-Fi підключенням і знаходиться в кафе з Wi-Fi, але у нього немає пароля WPA до мережі Wi-Fi, то функція "Останньої Лінії" не може бути встановлена, а викликаючий абонент не може підключитися до "Останньої Милі", до хмари SDNP або здійснити виклик.

Ще одним варіантом комунікації "Останньої Милі" є те, що корисне навантаження IP-датаграми 1405 містить всю інформацію для верхніх рівнів OSI, включаючи дані Транспортного рівня 4, дані Сесійного рівня 5, дані рівня Подання 6 і дані рівня Додатка 7. Крім даних рівня 4, необхідних для вибору транспортних протоколів UDP або TCP, інші дані в корисному навантаженні IP-датаграми специфічні для розглянутої SDNP комунікації і не можуть бути інтерпретовані маршрутизаторами, що працюють уздовж Останньої Милі, якщо вони самі не використовують ПЗ або прошивання SDNP. Відповідно, тільки кінцеві пристрої, тобто викликаючий абонент або клієнт SDNP і шлюз SDNP, можуть інтерпретувати з'єднання "Останньої Милі", навіть якщо сама мережа "Останньої Милі" може являти собою злиття різних пристроїв, операторів зв'язку та інтернет провайдерів.

Хоча корисне навантаження SDNP захищене численними секретами, включаючи шифрування, фрагментацію, вставку "сміттєвих даних" і видалення, статичним форматуванням і динамічним шифруванням, IP-адреси IP-датаграм, що проходять через мережу "Останньої Милі", обов'язково показують адреси джерела і призначення клієнтського пристрою 1400 і шлюзу сервера SDNP 1401. Щоб забезпечити певний ступінь анонімності "Останньої Милі", корисно маскувати адреси, тобто неправильно направляти кіберзлочинців, динамічно змінюючи адреси джерела і призначення в IP-датаграмі. Маскування IP-адрес може бути здійснено шляхом динамічної зміни IP-адреси підключеного пристрою викликаючого абонента, іменованого тут "динамічною адресацією клієнта", або шляхом зв'язку з кількома шлюзами SDNP, тобто багатомаршрутним зв'язком "Останньої Милі".

Перший з описаних способів маскування IP-адресу полягає в динамічній зміні адреси джерела послідовних пакетів даних. Як показано на Рис. 41, IP-датаграми A, B і C, що надсилаються послідовно, складаються з трьох різних адрес джерела. Зокрема, IP-датаграма 1405A включає в себе адресу джерела IP $C_{1,1}$, IP-датаграма B 1405B включає адресу джерела IP $C_{1,2}$, а IP-датаграма C 1405C включає адресу джерела IP $C_{1,3}$. Так що хоча всі пакети, що входять в маршрутизатор 1402A, виходять від клієнта SDNP 1400, вихідна адреса клієнта $C_{1,n}$ змінюється динамічно, створюючи плутанину між істинною IP-адресою і виступаючи більш ніж одним передавальним пристроєм. Щоб завершити шараду, MAC-адреса передавального пристрою також повинна змінюватися відповідно до динамічної адреси джерела.

Цей метод ілюструється на прикладі IP-стеків на Рис. 42A, де пристрої 1400, 1402A, 1402B, 1401 взаємодіють через відповідні IP-стеки 1411N, 1412A, 1412B і 1422, використовуючи Wi-Fi і Ethernet, але де мережева ідентифікація клієнта SDNP третього рівня включає кілька IP-адрес $C_{1,1}$, $C_{1,2}$ и $C_{1,3}$. У результаті виходить, що послідовні пакети даних, що надходять до маршрутизатора 1402A, відправляються з трьох різних клієнтських пристроїв, а не з одного, як показано на схематичному зображенні "Останньої Лінії", показаному на Рис. 42B. Загальний рівень PHY включає стандартні частоти Wi-Fi, а канальний рівень, що з'єднує пристрої, відповідає встановленим стандартам, таким як 802.11ac або 802.11n.

IP-датаграми 1405N, що відправляються на маршрутизатор 1402A по мережевому з'єднанню 1408, містять фіксовану IP-адресу призначення IP $M_{0,0}$ та адреси послідовних джерел IP $C_{1,1}$, IP $C_{1,2}$, IP $C_{1,3}$ та ін., представлені в математичній нотації як IP $C_{1,n}$ де n=1, 2, 3,... унікальна ідентифікація кожного послідовного пакета. Кожен наступний IP пакет також включає відповідний корисний пакет SDNP 1, SDNP 2, SDNP 3 тощо. Зверніть увагу, що хоча цей опис стосується кожної IP-адреси з використанням скороченого математичного позначення IP $C_{1,n}$, існує розуміння, що IP-адреси є реальними IP-адресами, створеними відповідно до міжнародних стандартів IPv4 або IPv6, і виключають будь-які резервні IP-адреси.

Ще одним варіантом підвищення безпеки є використання багатомаршрутного пакетного транспорту в "Останній Милі". Подібно передачі даних всередині SDNP хмари, аудіо і послідовні дані аналізуються і фрагментуються, потім поділяються на окремі пакети і адресуються різним

шлюзам SDNP в багатомаршрутному режимі. Приклад багатомаршрутної передачі даних з використанням статичних IP-адрес наведено на Рис. 43, де клієнт SDNP 1400 взаємодіє з кількома шлюзами 1401A, 1401B і 1401C. Як показано на Рис. , перший пакет даних 1405A включає в себе корисне навантаження SDNP 1 з IP-адресою джерела $C_{1,1}$ і адресу призначення $M_{0,0}$. Потім пакет даних 1405A направляється через "Останню Лінію" 1404A через маршрутизатори 1402A і 1402B на шлюз SDNP 1401A. Аналогічним чином другий пакет даних 1405B включає в себе корисне навантаження SDNP 2 з IP-адресою джерела $C_{1,1}$ і адресою призначення $M_{0,1}$. Потім пакет даних 1405B направляється через "Останню Лінію" 1404B через маршрутизатор 1402C на шлюз SDNP 1401B. Третій пакет даних 1405C включає в себе корисне навантаження SDNP 3 з IP-адресою джерела $C_{1,1}$ і адресою призначення $M_{0,3}$. Потім пакет даних 1405C направляється по останньому каналу зв'язку 1404C через маршрутизатор 1402D і 1402E на шлюз SDNP 1401C.

На шляху між клієнтським пристроєм 1400 і одним з трьох шлюзів 1401A, 1401B або 1401C показані IP-датаграми, які прямують через кілька "Останніх Ліній" 1404A, 1404B і 1404C на кілька маршрутизаторів 1402A, 1402B і 1402C. Ці маршрутизатори можуть включати (i) повністю незалежні маршрутизатори, що використовують однакові фізичні середовища, такі як Wi-Fi або Ethernet, (ii) кілька каналів маршрутизації в одному апаратному пристрої, наприклад, кілька решіткових каналів в кабельному модемі або (iii) різні фізичні середовища для зв'язку, наприклад, один проходить через Wi-Fi, другий через 3G і т.д.

Наприклад, Рис. 44A ілюструє IP-стек, що зображає вищезгадане багатомаршрутне гіперзахищене з'єднання "Останньої Милі" через фізичний рівень "Останньої Лінії" 1404 з використанням статичних IP-адрес. Під час роботи клієнт SDNP $C_{1,1}$ взаємодіє з маршрутизаторами 1401A, 1402B і 1402C як один пристрій, використовуючи загальні фізичний рівень PHY, канал даних і мережу. Маскування адрес здійснюється з використанням послідовних IP-датаграм, що містять статичну адресу клієнта IP $C_{1,1}$, але зі зміною адрес шлюзу SDNP IP $M_{0,0}$, IP $M_{0,1}$ та IP $M_{0,3}$. Переадресація пакетів може відбуватися алгоритмічно або випадково. Наприклад, якщо кожна 10-та датаграма, що відправляється з клієнтського пристрою 1400, направляється на сервер SDNP 1401C, то 10-та вихідна датаграма з клієнтського пристрою 1400 буде містити адресу призначення IP $M_{0,3}$ і IP-адреса джерела IP $C_{1,1}$. Відповіді з сервера шлюзу SDNP 1401C повертаються на клієнтський пристрій 1400 по зворотньому шляху, тобто з IP-адресою джерела IP $M_{0,3}$ і адресою призначення IP $C_{1,1}$.

Як показано на Рис. , фізичний рівень PHY і канал передачі даних між клієнтським пристроєм 1400 і маршрутизаторами 1402A, 1402D і 1402C являє собою єдиний носій, наприклад, Wi-Fi. Хоча з'єднання "Останньої лінії" представлені у вигляді окремих ліній, розділених на три частини, слід розуміти, що всі фізичні з'єднання виконані за принципом "точка-точка", а не за електричними Y-роз'ємами, використовуваними для створення паралельних проводів. Замість цього зображення означає, що з'єднання повинні показувати ефект з'єднання, тобто фізичний рівень PHY клієнтського IP-стека 1411 розширює одне PHY-з'єднання на три, тобто з'єднання на фізичному рівні PHY IP-стека 1412A, 1412C і 1412D. Функціонально ця "Остання Лінія" працює як один вихід на три вхідні модулі розширення, де один клієнт підключається до трьох функцій маршрутизатора, незалежно від того, чи містяться функції маршрутизатора в одному загальному електронному пристрої або рознесені на окремі маршрутизатори. Зверніть увагу, що, як показано на Рис. , "Остання Лінія" 1404 являє собою один тип носіїв інформації - кабель, волокно, Wi-Fi, Ethernet або стільниковий.

Однак решта "Останньої Милі" може складатися з будь-яких носіїв, які не обов'язково збігаються з "Останньою Милею". Альтернатива "Останній Лінії" включає кілька різних фізичних рівнів PHY, що з'єднуються з незалежними маршрутизаторами. При такій реалізації, IP-стек, що виконує багатомаршрутне гіперзахищене з'єднання "Останньої Милі" з використанням статичних IP-адрес по декількох фізичних PHY останніх каналах, показана на Рис. 44B. Зокрема, клієнтський пристрій 1400 працює із загальним мережевим інтерфейсом рівня 3 зі статичною клієнтською IP-адресою $C_{1,1}$, але використовує окремі та відмінні інтерфейси рівня 1 і рівня 2, представлені IP-стеками 1411A, 1411B і 1411C. У процесі роботи IP-стек 1411A підключається до маршрутизатора 1402A через "Останню Лінію" 1404A, що направляє IP-датаграму, що складається з IP-адреси джерела $C_{1,1}$ та IP-адреси призначення $M_{0,0}$, що проходить через маршрутизатор 1402B. Аналогічно, IP-стек 1411B з'єднується з маршрутизатором 1402C через "Останню Лінію" 1404B, направляючи IP-датаграми, що складаються з IP-адреси джерела $C_{1,1}$ та IP-адреси призначення $M_{0,1}$. IP-стек 1411C підключається до маршрутизатора 1402D через "Останню Лінію" 1404C, направляючи IP-датаграми, що складаються з IP-адреси джерела $C_{1,1}$ та IP-адреси призначення $M_{0,3}$, що проходить через маршрутизатор 1402E.

Поєднання динамічної адресації джерела і багатомаршрутної передачі даних показано на Рис. 45, де клієнт SDNP 1400 взаємодіє з кількома шлюзами 1401A, 1401B і 1401C, використовуючи динамічні адреси джерела. У цьому методі перший пакет даних 1405A включає в себе корисне навантаження SDNP 1 з динамічною IP-адресою джерела $C_{1,1}$ і IP-адресою призначення $M_{0,0}$. Потім пакет даних 1405A направляється через "Останню Лінію" 1404A через маршрутизатори 1402A і 1402B на шлюз SDNP 1401A. Аналогічним чином другий пакет даних 1405B включає в себе корисне навантаження SDNP 2 з динамічною IP-адресою джерела $C_{1,2}$ і IP-адреса призначення $M_{0,1}$. Потім пакет даних 1405B направляється через "Останню Лінію" 1404B через маршрутизатор 1402C на шлюз SDNP 1401B. Третій пакет даних 1405C включає в себе корисне навантаження SDNP 3 з динамічною IP-адресою джерела $C_{1,3}$ і IP-адресою призначення $M_{0,3}$. Потім пакет даних 1405C направляється по останньому каналу зв'язку 1404C через маршрутизатори 1402D і 1402E на шлюз SDNP 1401C.

Таким чином, кожен наступний пакет даних містить корисне навантаження SDNP, що змінюється, використовує динамічно змінювані адреси джерел, що направляються за різними останніми посиланнями на унікальні шлюзи SDNP. Для передачі даних по декількох "Останніх Лініях", а саме "Останніх Лініях" 1404A, 1404B і 1404C, використовується або один маршрутизатор з кількома IP входами, такими як кабельний модем DOCSIS3 з треліс-модуляцією (або решітчастим кодуванням), або через кілька медіа, наприклад, кілька діапазонів Wi-Fi, комбінації радіо і Wi-Fi, або інші комбінації дротового і бездротового зв'язку. В одному з прикладів на Рис. 46A показано IP-стек гіперзахищеного мультимаршрутного з'єднання "Останньої Милі" з використанням динамічних клієнтських IP-адрес за однорівневим фізичним PHY з'єднанням "Останньої Лінії" 1404. Клієнтський пристрій 1400, ілюструє загальний фізичний інтерфейс, що складається з комунікацій рівнів 1 і 2, показаних в IP-стеці 1411A. На мережевому рівні IP-стек 1411A генерує клієнтську адресу $C_{1,1}$, спрямовану на шлюз SDMP $M_{0,0}$, IP-стек 1411B генерує клієнтську адресу $C_{1,2}$, спрямовану на шлюз SDMP $M_{0,1}$, а IP-стек 1411C генерує клієнтську адресу $C_{1,3}$, спрямовану на шлюз SDMP $M_{0,3}$.

Такий же багатомаршрутний підхід може поєднуватися з динамічною адресацією клієнтів і кількома останніми рівнями PHY, як показано на схемі IP-стека на Рис. 46B. Як показано на Рис. , клієнтський пристрій 1400 містить три IP-стеки 1411A, 1411B і 1411C, що передають IP-датаграми з відповідними IP-адресами $C_{1,1}$, $C_{1,2}$ та $C_{1,3}$ за "Останньою Лінією" 1404A, 1404B і 1404C на шлюз SDNP з IP-адресами $M_{0,0}$, IP $M_{0,1}$ та IP $M_{0,3}$.

У багатьох випадках "Остання Лінія" являє собою єдиний маршрут, де за межами першого маршрутизатора використовується багатомаршрутна передача даних. На Рис. 47 клієнт SDNP 1400 взаємодіє з одним маршрутизатором 1402A через "Останню Лінію" 1404. Крім маршрутизатора 1402A, пакети даних направляються на кілька шлюзів 1401A, 1401B і 1401C з використанням динамічних адрес джерела. У цій реалізації перший пакет даних 1405A включає в себе корисне навантаження SDNP 1 з динамічною IP-адресою джерела $C_{1,1}$ і IP-адресою призначення $M_{0,0}$. Пакет даних 1405A маршрутизується через "Останню Лінію" 1404 і через маршрутизатори 1402A і 1402B на шлюз SDNP 1401A.

Аналогічним чином, другий пакет даних 1405B включає в себе корисне навантаження SDNP 2 з динамічною IP-адресою джерела $C_{1,2}$ і IP-адресою призначення $M_{0,1}$. Пакет даних 1405B маршрутизується через "Останню Лінію" 1404 і через маршрутизатори 1402A і 1402C на шлюз SDNP 1401B. Третій пакет даних 1405C включає в себе корисне навантаження SDNP 3 з динамічною IP-адресою джерела $C_{1,3}$ і IP-адресою призначення $M_{0,3}$. Пакет даних 1405C послідовно маршрутизується через "Останню Лінію" 1401 і через маршрутизатори 1402A, 1402D і 1402E на шлюз SDNP 1401C. Таким чином, кожен наступний пакет даних містить корисне навантаження SDNP, що змінюється, використовує динамічно змінювані адреси джерел, що направляються за загальними останніми посиланнями на унікальні шлюзи SDNP.

Таке підключення "Останньої Милі" показано на прикладі IP-стеків на Рис. 48, де IP-стек 1411 на клієнтському пристрої SDNP 1400 з функцією "Останньої Лінії" 1404 виключно з маршрутизатором 1402A відправляє пакети даних на мережевому рівні 3 в стек 1412A з трьома різними мережевими адресами, а саме IP IP $C_{1,1}$, IP $C_{1,2}$ і IP $C_{1,3}$. Таким чином, клієнтський пристрій 1400 виглядає маршрутизатором 1402A як три окремих клієнта, хоча насправді він складається з одного клієнта. Як тільки IP-датаграми досягають маршрутизатора 1402A, вони розділяються і проходять різні маршрути до різних шлюзів призначення. Пакети з адресою джерела IP $C_{1,1}$, наприклад, можуть бути направлені через маршрутизатор 1402B на IP $M_{0,0}$, пакети з IP-адресою джерела $C_{1,2}$, можуть бути направлені через маршрутизатор 1402C на IP $M_{0,1}$, і пакети з IP-адресою джерела $C_{1,3}$, можуть бути направлені через маршрутизатори призначення 1402D і 1402E на IP $M_{0,3}$. Таблиця маршрутизації для напрямку пакета даних з вказаною динамічною клієнтською адресою $C_{1,n}$ на певний шлюз SDNP не має попередньої

установки і може динамічно змінюватися. IP-адреси можуть призначатися за пакетами, що ще більше ускладнює той факт, що очевидно незв'язані пакети даних є частиною одного фрагментарного з'єднання між двома викликаючими абонентами.

Фізична реалізація маршрутизації "Останньої Милі" – Фізична реалізація "Останньої Милі" може включати зв'язок різними каналами зв'язку, включаючи Ethernet, Wi-Fi, стільникову або DOCSIS3-сумісні кабельні та оптоволоконні лінії. Незалежно від використовуваного середовища передачі, маршрутизація пакетів даних по "Останній Милі" в основному контролюється трьома змінними, а саме:

- Номер мережевої карти (MAC-адреса) пристроїв зв'язку,
- IP-адреса джерела IP-датаграми,
- IP-адреса призначення IP-датаграми.

Таким чином, MAC-адреси контролюють фізичні носії, що використовуються для виконання кожного переходу в з'єднанні "Останньої Милі", тобто інформацію рівнів 1 і 2, а IP-адреси ідентифікують клієнтський пристрій і шлюз SDNP, тобто пристрої на обох кінцях "Останньої Милі". Хоча корисне навантаження, що використовується в гіперзахищеному з'єднанні, відповідає протоколам, визначеним відповідно до Захищеної Динамічної Мережі і Протоколу, проміжні пристрої в "Останній Милі", тобто маршрутизатори та інші пристрої на маршруті пакета між клієнтським пристроєм і шлюзом, зазвичай не можуть виконувати функції SDNP через відсутність виконуваного коду SDNP в таких пристроях. Тому корисне навантаження SDNP не впливає на маршрутизацію пакетів даних гіперзахищеної "Останньої Милі".

Одним з прикладів є використання Ethernet для зв'язку "Останньої Милі". Адаптуючи пакет даних Ethernet, описаний вище на Рис. 9E для передачі даних SDNP "Останньої Милі", Рис. 49 - це графічне представлення датаграм IPv4 і IPv6 для передачі даних Ethernet з корисним навантаженням SDNP. Як показано на Рис. , пакет Ethernet 188 рівня 1 містить заголовок кадру даних, тобто преамбулу 180, роздільник початкового кадру SFD 181 і пакет Ethernet рівня 2 189. Пакет Ethernet 189 включає MAC-адреси 182 та одержувача і джерела 183, додатковий тег 802.1Q 184 для реалізації VLAN, поле Ethertype 185 для зазначення типу використовуваного каналу передачі даних (Ethernet II або специфікація довжини згідно з IEEE802.3) і перевірку кадрів 186, що включає 32-бітну контрольну суму CRC для всього пакета каналу передачі даних. Ethernet-пакет 189 також містить корисне навантаження 187 MAC-адреси змінної довжини, що використовується для інкапсуляції вмісту SDNP 1430 в IP-датаграму. Зокрема, корисне навантаження MAC 187 містить IP заголовок 434 і IP заголовок 435, включаючи транспортний заголовок 436 і SDNP 1430.

IP-заголовок 434 змінюється залежно від того, чи слідує IP-датаграма протоколу IPv4 або IPv6, як визначено за полем протоколу 447, що містить двійковий запис 4, або полю протоколу 448, що містить двійковий запис 6. Преамбули 440 і 444 містять транспортний заголовок 470, що використовується для визначення використовуваного методу транспортування рівня 4, наприклад, TCP, UDP або функції обслуговування ICMP і IGMP. Зокрема, відповідно до захищеної динамічної мережі зв'язку та протоколу, TCP транспорт використовується для передачі програмного забезпечення і файлів даних, а UDP використовується для передачі даних в режимі реального часу, таких як VoIP і відео. Довжина і формат транспортного заголовка 436 варіюється залежно від транспортного заголовка 470. Заголовок 434 містить IPv4-адреси джерела та призначення 441 і 442 або IPv6-адреси джерела та призначення 445 і 446.

Маршрутизація "Останньої Милі" Ethernet пакетів залежить як від IP-адрес, так і від MAC-адрес, представлених зразками імен пристроїв, до яких належать IP або MAC-адреси, наприклад, MAC $C_{1,1}$ або IP $M_{0,0}$. Для більшої ясності замість цифрової адреси використовуються символічні імена, що представляють собою числову адресу, виконану відповідно до Інтернет-протоколу у форматі Ethernet. Зауважте, що IP-адреса IP $C_{1,1}$ має різні формати і використовує різну кількість байт для IPv4 і IPv6 імен. Крім того, формат MAC-адреси залежить від використовуваного протоколу каналу передачі даних другого рівня. Таким чином, MAC-адреса MAC $C_{1,1}$ для стільникового радіозв'язку не збігається з MAC-адресою для одного і того ж пристрою, що взаємодіє за Wi-Fi або Ethernet. MAC-адреси не мають відношення до IP-адрес, тобто IP-адреса і MAC-адреса одного і того ж клієнта не відносяться один до одного.

Послідовна маршрутизація "Останньої Милі" Ethernet пакетів показана в прикладах з Рис. 50A по Рис. 50D. Кожен рисунок містить два Ethernet-пакети - верхній, що містить датаграму IPv4, і нижній, що містить датаграму IPv6. Оскільки IPv4 і IPv6 використовують різні формати з різною довжиною поля, показані два Ethernet-пакети, як правило, мають різну довжину навіть при однаковому корисному навантаженні. На першому етапі передачі даних корисне навантаження SDNP-A переміщується від клієнта SDNP 1400 до маршрутизатора 1402A через "Останню Лінію" 1404, а потім через канал шлюзу 1414 до шлюзу SDNP 1401. Відповідь від

шлюзу SDNP клієнту включає корисне навантаження G SDNP від шлюзу 1401 через канал шлюзу 1414 до маршрутизатора 1402A, потім через "Останню Лінію" 1404 до клієнта 1400. Клієнт SDNP 1400 має числові MAC та IP-адреси MAC $C_{1,1}$ та IP $C_{1,1}$, маршрутизатор 1402A має числову MAC адресу MAC R, а шлюз SDNP має числові MAC та IP-адреси MAC $M_{0,0}$ та IP $M_{0,0}$. IP-адреса маршрутизатора 1402A в пакетах даних не використовується.

На відміну від хмари SDNP, де пакетна маршрутизація датаграм SDNP повністю контролюється мережею SDNP, в мережах зв'язку "Останньої Милі" з використанням IP-датаграм корисне навантаження SDNP не може бути інтерпретовано або впливати на маршрутизацію, тобто кожне з'єднання, що передається через "Останню Милю", містить фіксовані IP-адреси джерела і призначення. Фізичні носії або канали, що використовуються для направлення пакетів Ethernet, управляються MAC-адресами, що з'єднують кожен вузол зв'язку в "Останній Милі". Наприклад, на Рис. 50A показані пакети IPv4 і IPv6 з'єднання "Останньої Лінії" по мережі Ethernet, що використовуються для маршрутизації маршрутизатором 1402A по одному каналу, включаючи MAC адресу джерела MAC $C_{1,1}$, MAC адресу призначення MAC R, IP-адресу джерела IP $C_{1,1}$, адресу призначення IP $M_{0,0}$ і корисне навантаження SDNP. Рис. 50B ілюструє відповідні пакети Ethernet, що передають корисне навантаження SDNP по каналу шлюзу 1414. Як описано вище, IP-адреси джерела та призначення залишаються незмінними при IP $C_{1,1}$ та IP $M_{0,0}$, а адреси джерела та призначення MAC змінюються з вихідних значень на MAC R і MAC $M_{0,0}$.

У відповідному зв'язку між шлюзом SDNP 1401 і клієнтом 1400, корисне навантаження G SDNP проходить через ту ж саму мережу в зворотній послідовності, тобто там, де відбувається обмін адресами джерела і призначення. Як показано на Рис. 50C, IP-адреси джерела і призначення складаються відповідно з IP $M_{0,0}$ та IP $C_{1,1}$, а MAC-адреси включають MAC-адресу джерела $M_{0,0}$ і MAC-адресу призначення R. У з'єднанні "Останньої Лінії", показаному на Рис. 50D, MAC-адреса джерела і призначення MAC R і MAC $C_{1,1}$, а IP-адреса джерела і призначення залишається незмінною, як IP $M_{0,0}$ і IP $C_{1,1}$.

Одним із зручних способів представлення комунікації "Останній Милі" з клієнтом SDNP є використання "скорочених" пакетів даних, що містять поля даних, що містять MAC адреси джерела і призначення, IP-адреси джерела і призначення, а також корисне навантаження SDNP. Скорочена форма зручна для ілюстрації потоку даних у будь-якій комунікаційній "сесії", тобто побудови послідовних пакетів даних, що передаються через "Останню Милю" на шлюз SDNP, і відповідей на них. Наприклад, послідовні пакети Ethernet (показані в скороченому вигляді), що відправляються від клієнта SDNP на шлюз SDNP, показані у верхній частині Рис. 51A. Кожен рядок - це послідовні пакети даних, що містять корисне навантаження SDNP, A, B і C. У лівому стовпчику показані пакети даних у "Останній Лінії", а в правій - пакети даних, що містять те ж саме навантаження по шлюзу. Як показано на Рис. , всі пакети вказують IP $C_{1,1}$ як IP-адреси джерела та IP $M_{0,0}$ як IP-адреси призначення. Оскільки використовується лише одна пара IP-адрес, "Остання Миля" тут називається з'єднанням за одним маршрутом SDNP "Останньої Милі". Крім того, оскільки IP-адреса джерела, що використовується клієнтом SDNP 1400 для передачі послідовних пакетів даних, є незмінною, в "Останній Лінії" використовується "статична адресація клієнта".

Щоб полегшити з'єднання другого рівня між кожним вузлом зв'язку та сусідами, MAC-адреси в різних сегментах "Останньої Милі" обов'язково змінюються. Як показано на Рис. , всі наступні пакети, що проходять по останньому каналу зв'язку від клієнта до маршрутизатора, використовують MAC-адреси джерела та MAC-адреси призначення $C_{1,1}$ і MAC R. Оскільки для клієнта використовується одна MAC-адреса в наступних пакетах даних, "Остання Лінія" включає в себе один фізичний носій, тобто один фізичний рівень PHY "Останньої Лінії". Транспортування по каналу шлюзу використовує MAC-адреси джерела і призначення MAC R і MAC $M_{0,0}$, відповідно.

Так що хоча показаний пакет даних містить корисне навантаження SDNP, маршрутизація через "Останню Милю" обов'язково використовує перехоплювані MAC і IP-адреси - адреси, які можуть бути інтерпретовані неавторизованими слухачами. Відстежуючи пакети з ідентичними IP-адресами джерела і призначення, неавторизований слухач може зробити висновок, що пакети даних, ймовірно, є частиною однієї і тієї ж розмови або сесії, і навіть якщо вони не можуть відкрити корисне навантаження SDNP, вони можуть збирати метадані, такі як час виклику, розмір файлів, швидкість передачі даних і т.д. для відтворення профілю викликаючого. Більш того, слідуючи MAC і IP-адресам, що метафорично нагадують слід з хлібних крихт, хакер може відстежити походження виклику до кінцевого пристрою, тобто клієнтського пристрою, а потім особисто ідентифікувати викликаючого абонента.

У документі, що розглядається, найкращий спосіб запобігти відстеженню клієнтських пристроїв, замаскувати пов'язані з ними пакети викликів і блокувати збір метаданих - це динамічна зміна MAC і IP-адрес у з'єднаннях "Останньої Милі" і "Останньої Лінії". Ці винахідницькі методи маскування включають в себе:

- Надсилання пакетів даних за змінними засобами зв'язку шляхом динамічної зміни MAC-адрес "Останньої Лінії", що називаються в даному документі "багаторівневим фізичним з'єднанням" Останньої Лінії ",

- Маскування викликаючого абонента, шляхом динамічної зміни ідентифікаційних даних IP-адреси клієнтського пристрою, званого "динамічною адресацією клієнта",

- Зміна шляху передачі послідовних пакетів даних через "Останню Милю" шляхом динамічної зміни IP-адреси зв'язку на різні IP-адреси шлюзу SDNP і назад, звані тут "багатомаршрутним з'єднанням" Останньої Милі".

Поєднання багатофункціональної високошвидкісної, динамічної адресації клієнтів і багатомаршрутного зв'язку "Останньої Милі" робить моніторинг і відстеження з'єднань "Останньої Милі" і "Останньої Лінії" надзвичайно складним, оскільки тільки викликаючий абонент SDNP і шлюз SDNP знають, які пакети є частиною одного виклику або сесії. Ці методи можуть використовуватися окремо або в комбінації.

Наприклад, нижня половина Рис. 51A ілюструє використання "багаторівневого фізичного з'єднання" Останньої Лінії "зв'язку в одномаршрутному з'єднанні" Останньою Милі "зі статичною адресацією клієнта. Як показано на Рис. , кожен рядок містить пару пакетів даних, що використовуються в комунікації між клієнтом SDNP і шлюзом SDNP - ліва сторона, що представляє пакет даних "Останньої Лінії", права сторона, що описує пакет даних каналу шлюзу. Три рядки представляють собою три послідовні повідомлення, де верхній рядок містить перший набір даних "корисне навантаження SDNP A", середній рядок містить корисне навантаження SDNP B, а нижній рядок описує третій пакет даних, що містить корисне навантаження SDNP C. Для одного маршруту комунікації "Останньої Милі" зі статичним клієнтом, адресованим всі наступні пакети даних, використовується статична IP-адреса клієнта $C_{1,1}$ і IP-адреса постійного призначення IP $M_{0,0}$.

Для того, щоб виконати багаторівневе фізичне з'єднання "Останньої Лінії", тобто направити дані в "Останню Лінію" через кілька фізичних носіїв, MAC-адрес клієнта SDNP повинен бути динамічно змінений в послідовних пакетах даних. Кожна MAC-адреса відповідає певному фізичному рівню PHY, наприклад, Ethernet 100BASE-T і 1000BASE-T з'єднанням. У разі трьох фізичних носіїв MAC-адреса клієнта динамічно змінюється послідовно з MAC $C_{1,1}$ на MAC $C_{1,2}$, а потім на MAC $C_{1,3}$. Якщо доступні лише два носії, MAC-адреси можуть змінюватися довільно, щоб уникнути розпізнавання образів, таких як MAC $C_{1,1}$, MAC $C_{1,2}$, MAC $C_{1,2}$, MAC $C_{1,1}$, MAC $C_{1,2}$, MAC $C_{1,1}$, MAC $C_{1,2}$, MAC $C_{1,2}$, MAC $C_{1,1}$, MAC $C_{1,1}$... Хоча початкова MAC-адреса відрізняється, L може залишатися постійним, тобто місцем призначення останнього з них - MAC R. Оскільки всі маршрути "багаторівневого фізичного з'єднання Останньої Лінії" закінчуються в одному маршрутизаторі, шлях даних через решту "Останньої Милі" залишається фіксованим як один маршрут зв'язку. Іншими словами, незважаючи на те, що "Остання Лінія" використовує багаторівневе фізичне з'єднання, "Остання Миля" входить в SDNP хмару через один шлюз, а "Остання Миля" містить одномаршрутне з'єднання.

Хоча підхід багаторівневого фізичного з'єднання забезпечує деяку ступінь маскування, пакетне прослуховування пакетів даних з певного виклику все ще може бути ідентифіковано, оскільки вони мають спільну IP-адресу клієнта. Цей метод виявлення блокується за допомогою динамічної адресації клієнта - операції, при якій клієнт змінює IP-адресу з кожним пакетом, який він надсилає. Як приклад, Рис. 51B ілюструє використання динамічної IP-адресації клієнта в одному маршруті зв'язку "Останньої Милі". Верхній набір пакетів даних ілюструє одне фізичне з'єднання "Останньої Лінії", в той час як нижній набір пакетів даних описує реалізацію декількох фізичних з'єднань PHY. При переданні даних SDNP "Останньою Милею", IP-адреса призначення шлюзу залишається постійною з числовим значенням IP $M_{0,0}$ у всіх пакетах даних незалежно від того, чи використовуються методи одно- або багатомаршрутного з'єднання PHY.

Як показано на Рис. , в пакетах даних динамічної адресації клієнтів з корисним навантаженням SDNP A використовується динамічно обрана IP-адреса джерела 441, що включає IP $C_{1,1}$, а в пакетах даних з корисним навантаженням SDNP B використовується динамічно обрана IP-адреса джерела $C_{1,2}$, в даних з корисним навантаженням SDNP C використовується динамічно обрана IP-адреса джерела $C_{1,3}$, і т.д. Кількість динамічно вибраних адрес практично необмежена, особливо в IPv6. Крім того, IP-адреси можуть використовуватися так довго, що через деякий час, наприклад, через 1 секунду, вони можуть бути використані повторно. У разі динамічних клієнтських адрес з одноріневим фізичним з'єднанням "Останньої

Лінії" значення вихідної MAC-адреси 183 залишається постійним, в даному прикладі на MAC $C_{1,1}$, навіть якщо IP-адреса джерела змінюється. У разі динамічних клієнтських адрес з декількома фізичними з'єднаннями "Останньої лінії" значення вихідної MAC-адреси 183 змінюється послідовно, змінюючись з MAC $C_{1,1}$ на MAC $C_{1,2}$, а потім на MAC $C_{1,3}$. Між змінною MAC-адресою клієнта і його динамічною IP-адресою немає особливого математичного зв'язку.

Хоча динамічна адресація клієнтів включає повідомлення, відправлені від різних користувачів, пакети даних все ще проходять більшу частину "Останньої Милі" (за винятком реалізацій багаторівневих фізичних з'єднань "Останньої Лінії") по одному маршруту. Більш просунутим способом вирішити проблему прослуховування пакетів при з'єднанні в "Останній Милі" є використання "багатомаршрутного" зв'язку. У багатомаршрутному зв'язку для підключення клієнта до SDNP хмари використовується більше однієї IP-адреси шлюзу SDNP. Оскільки мережева маршрутизація SDNP наказується сигнальними серверами і використовує ідентифікаційні теги SDNP на кожному пакеті, хмара SDNP може направляти пакети в пункт призначення незалежно від того, чи надходять дані в хмару SDNP через один шлюз або через кілька шлюзів. Рис. 51C ілюструє використання багатомаршрутного зв'язку "Останньої Милі" зі статичною адресацією клієнта. У кожному пакеті даних, показаному в останньому посиланні, IP-адреса джерела клієнта 441 залишається статичним з числовим значенням IP $C_{1,1}$, а послідовні пакети даних, що містять корисні навантаження SDNP A, B і C, динамічно змінюють IP-адресу призначення 442 від IP $M_{0,0}$ до IP $M_{0,1}$ і IP $M_{0,3}$. IP-адреси шлюзів SDNP обираються не випадковим чином, а "обираються" сигнальними серверами SDNP для представлення шлюзів, що знаходяться в тимчасовій близькості від викликаючого абонента, тобто шлюзів з мінімальною затримкою статистичного поширення між клієнтом SDNP і конкретним шлюзом SDNP. У цьому прикладі динамічні адреси призначення змінюються незалежно від фізичних з'єднань рівня PHY. Наприклад, верхній набір пакетів даних ілюструє однорівневе з'єднання "Останньої Лінії" з MAC-адресою джерела клієнта 183 для "Останньої Лінії", що має числове значення MAC $C_{1,1}$, а нижній набір пакетів даних описує реалізацію багаторівневого з'єднання "Останньої Лінії", змінюючи MAC-адресу джерела на різних носіях, наприклад, MAC $C_{1,1}$, MAC $C_{1,2}$ и MAC $C_{1,3}$. Між змінюваними MAC-адресами клієнта та IP-адресами призначення шлюзів SDNP не існує відповідної закономірності або математичного зв'язку.

Найбільш ефективним способом маскування є поєднання динамічної адресації клієнта з багатомаршрутним зв'язком "Останньої Милі". Ця нова комбінація функцій безпеки показана на Рис. 51D як для реалізації функції однорівневого фізичного з'єднання "Остання Лінія" (показана у верхній частині Рис.), так і для версії багаторівневого фізичного з'єднання "Останньої Лінії" (показана в нижній частині Рис.). У цій повністю динамічній версії, показаній в нижній половині, IP-адреса джерела 441 динамічно і випадково змінюється з IP $C_{1,1}$, на IP $C_{1,2}$ і на IP $C_{1,3}$, при цьому IP-адреса призначення 442 шлюзу SDNP незалежно змінюється з IP $M_{0,0}$, на IP $M_{0,1}$ і на IP $M_{0,3}$. Адреса шлюзу SDNP вибирається сигнальними серверами SDNP для мінімізації затримок поширення при зміні динамічної адреси клієнта іншим способом. Як і в попередніх прикладах, верхній набір пакетів даних ілюструє однорівневого фізичного з'єднання "Останньою Лінією" з MAC-адресою джерела клієнта 183 для Last Link, що має числове значення MAC $C_{1,1}$, а нижній набір пакетів даних описує реалізацію декількох рівнів PHY, що варіює MAC-адресу джерела на різних носіях, наприклад MAC $C_{1,1}$, MAC $C_{1,2}$ і MAC $C_{1,3}$. Не існує відповідної закономірності або математичного зв'язку між зміною MAC-адрес клієнта і зміною IP-адрес клієнта або шлюзу SDNP. Однак при багатомаршрутному зв'язку "Останньої Милі" багаторівневе фізичне з'єднання "Останньої Лінії" може бути вигідніше при підключенні до трьох окремих маршрутизаторів R1, R2 і R3, ніж направляти всі дані в один маршрутизатор R.

Маскування "Останньої Милі", як описано вище, являє собою десять різних випадків, наведених у таблиці Рис. 52A, починаючи від найменш безпечної реалізації (показаної внизу таблиці в рядку 10), що включає один маршрут "Останньої Милі" зі статичною адресою клієнта і один фізичний рівень PHY "Останньої Лінії" для більш просунутого маскування, запропонованого багаторівневим фізичним з'єднанням PHY "Останньої Лінії" з динамічною адресацією джерела і багатомаршрутним з'єднанням "Останній Милі" у верхньому рядку 1. Проміжні комбінації ранжуються в порядку безпеки. Символи $C_{1,n}$, $M_{0,n}$ і R_n належать до динамічно змінюваних адрес для клієнтів SDNP, шлюзів SDNP і маршрутизатора "Останньої Лінії". Динамічні адреси некорельовані. Рядки з 7 по 10 описують один маршрут зв'язку "Останньої Милі", тобто використовують один шлюз $M_{0,0}$, тоді як рядки з 1 по 6 описують багатомаршрутний зв'язок "Останньої Милі" з кількома шлюзами. За винятком затінених рядків 1 і 4, зв'язок "Останньої Лінії" з'єднується з одним маршрутизатором з MAC-адресою R. На відміну від зв'язку за кількома маршрутами, затінені рядки 1 і 4 описують багаторівневе фізичне

з'єднання PHY "Останньої Лінії" з кількома маршрутизаторами з динамічними MAC-адресами R_n.

Топологічно робота одномаршрутного з'єднання "Останньої Милі" показана на Рис. 52B в чотирьох комбінаціях - статична адресація клієнта з однорівневим фізичним з'єднанням "Останньої Лінії" і статична адресація клієнта з багаторівневим фізичним з'єднанням "Останньої Лінії", динамічна адресація клієнта з однорівневим фізичним з'єднанням "Останньої Лінії" і динамічна адресація клієнта з багаторівневим фізичним з'єднанням "Останньої Лінії". Кожна рамка ілюструє три послідовні канали пакетної передачі даних, що показують шлях передачі даних. Суцільні лінії - це потік пакетів даних, тоді як пунктирні лінії ілюструють можливі невикористані шляхи. Затінені кола ілюструють вузли зв'язку, які використовуються в комунікації "Останньої Милі", порожні кола ілюструють невикористовувані вузли зв'язку. Як показано на Рис. , всі приклади завершують маршрутизацію даних "Останньої Милі" через одне з'єднання між маршрутизатором R і шлюзом SDNP $M_{0,0}$.

У разі статичної адресації клієнта з однорівневим фізичним з'єднанням "Останньої Лінії", показаної у верхньому лівому куті, кожен наступний пакет проходить один і той самий шлях по всій "Останній Милі", використовуючи незмінні IP-адреси. У разі статичної адресації клієнта з багаторівневим фізичним з'єднанням "Останньої лінії", показаної в нижньому лівому куті, кожен наступний пакет проходить по різному шляху через "Останню Лінію", як наказано MAC-адресами, що динамічно змінюються. Решта "Останньої Милі" складається з одного маршруту, зазначеного незмінними IP-адресами. Незважаючи на одномаршрутну передачу, зміна фізичних носіїв "Останньої Лінії" ускладнює відстеження викликаючого абонента. У разі динамічної адресації клієнта з однорівневим фізичним з'єднанням "Останньої лінії", показаної в правому верхньому куті, кожен наступний пакет проходить один і той самий шлях по всій "Останній Милі", використовуючи незмінну IP-адресу призначення і постійну MAC адресу клієнта для "Останньої Лінії". Замість цього маскування досягається зміною ідентичності клієнта шляхом зміни динамічної IP-адреси джерела. У разі одномаршрутного зв'язку як з динамічною адресацією клієнта, так і багаторівневим фізичним з'єднанням "Останньої Лінії", показаною в правому нижньому куті, MAC-адреса клієнта та IP-адреса джерела змінюються динамічно і випадково, навіть якщо всі пакети направляються на один шлюз SDNP.

Динамічна адресація клієнта - це процес, під час якого клієнтський пристрій використовує одну або декілька тимчасових IP-адрес. Процес складається з двох етапів. На першому етапі, коли пристрій вперше входить в мережу, він реєструє свою присутність в локальній підмережі, зв'язуючись з найближчим маршрутизатором. Потім маршрутизатор перенаправляє з'єднання на найближчий сервер DHCP в тій же підмережі. DHCP — скорочена назва протоколу динамічної конфігурації вузла (DHCP) — це протокол управління мережею, який використовується для динамічного призначення IP-адрес. Під час реєстрації клієнтський пристрій завантажує одну або декілька IP-адрес і зберігає їх у регістрі даних зв'язку. Допоки призначені IP-адреси не оновлюються локальним DHCP сервером, або шляхом запуску нової сесії, або шляхом запиту нових адрес, щоразу, коли клієнтський пристрій взаємодіє, він використовує ці IP-адреси. Оскільки адреси динамічно видаються в межах певної підмережі, IP-адреси клієнтських пристроїв не є Інтернет-адресами.

На другому етапі, коли клієнтський пристрій виконує виклик або входить до мережі SDNP, пристрій автоматично зв'язується з сигнальним сервером SDNP на основі статичної IP-адреси сервера SDNP. Після отримання вхідного повідомлення сервер SDNP завантажує спеціальну IP-адресу або адреси на сервер імен SDNP. Потім сервер імен SDNP присвоює SDNP-адреси як псевдокод для кожної тимчасової IP-адреси. У процесі роботи перед маршрутизацією вихідна адреса SDNP пакета замінюється локальною IP-адресою. У разі динамічної адресації SDNP ідентичність клієнтського пристрою маскується шляхом багаторазової відправки пакетів із змінними вихідними адресами. Таким чином, динамічне маскування приховує справжню ідентичність клієнтського пристрою.

При досягненні шлюзу SDNP адреси джерела для вихідних пакетів відкидають IP-адреси клієнтів і замінюють їх адресою SDNP сервера шлюзу. Кожен вихідний пакет SDNP змінює локальну IP-адресу пристрою на спеціальну перед транспортуванням. На відміну від передачі пакетів Інтернет, де IP-адреси джерела і одержувача залишаються постійними і необхідні для відповідей, при передачі SDNP кожен перехід використовує нові IP-адреси. Тому, коли SDNP-повідомлення нарешті досягає пункту призначення, вихідна адреса клієнтського пристрою не включається в пакет даних. Замість цього сигнальний сервер інформує пристрій про шлях повернення відповідей.

Топологічно робота "багатомаршрутного" з'єднання "Остання Миля" показана на Рис. 52C в чотирьох комбінаціях статичної та динамічної адресації клієнтів, а також при одно- і

багаторівневих фізичних з'єднаннях "Останньої Лінії". У кожному багатомаршрутному з'єднанні IP-адреса призначення, тобто шлюз SDNP, постійно змінюється, що означає, що маршрут "Останньої Милі" з'єднується з різними входами в SDNP хмару. У лівому стовпчику відображаються статичні адреси клієнтів, тобто ідентичність абонента залишається незмінною. У прикладі в лівому верхньому куті використовується однорівневе фізичне з'єднання "Останньої Лінії", що означає, що MAC-адреса клієнта також залишається статичною. Навіть незважаючи на те, що зв'язок відбувається з різними шлюзами призначення, незмінне фізичне середовище "Останньої Лінії" і незмінна IP-адреса клієнта робить "Останню Милю" вразливою для відстеження викликів. Цю проблему можна усунути або шляхом зміни носія "Останньої Лінії", що використовується для передачі пакетів даних, або шляхом маскування справжньої IP-адреси викликаючого абонента.

Приклад у лівому нижньому куті використовує багаторівневе фізичне з'єднання "Останньої Лінії", що означає динамічну зміну MAC-адреси клієнта. Такий підхід компенсує той факт, що статичну IP-адреса підтримує особистість клієнта. У рамках наскрізного багатомаршрутного зв'язку "Останньої Милі" кожна унікальна "Остання Лінія" з'єднується з окремими маршрутизаторами в послідовних передачах пакетів до окремих шлюзів SDNP. Таким чином, перший пакет маршрутизується від клієнта зі статичною адресою IP $C_{1,1}$ до маршрутизатора з MAC адресою MAC R_1 через унікальний носій PHY, а потім направляється на шлюз SDNP з IP-адресою $M_{0,0}$. Другий пакет ідентичної клієнтської адреси IP $C_{1,1}$ направляється на інший маршрутизатор з медіа-адресою MAC R_2 через унікальний носій PHY перед остаточною маршрутизацією на шлюз SDNP з IP-адресою $M_{0,1}$. Аналогічно третій пакет зі статичною клієнтською IP-адресою $C_{1,1}$ також направляється на маршрутизатор з медіа-адресою MAC R_3 через унікальний носій PHY, де він потім направляється на шлюз SDNP $M_{0,3}$. Використання декількох маршрутизаторів дозволяє використовувати багаторівневе фізичне з'єднання "Останньої Лінії" для доставки пакета "Останньої Милі" абсолютно різними шляхами, незважаючи на використання клієнта з єдиною IP-адресою джерела.

В іншому варіанті, показаному в правому верхньому куті, особистість клієнта динамічно змінюється, навіть якщо використовуються тільки одна MAC-адреса і одне PHY-з'єднання. Показана IP-адреса клієнта динамічно змінюється з $C_{1,1}$ на IP $C_{1,2}$ на IP $C_{1,3}$, а фізичне середовище залишається постійним з вихідною адресою MAC $C_{1,1}$ і адресою призначення MAC R. Потім дані направляються до шлюзів $M_{0,0}$, $M_{0,1}$ і $M_{0,3}$ у випадковому порядку, визначеному сигнальними серверами SDNP.

Просунута безпека досягається шляхом об'єднання всіх трьох методів маскування "Останньої Милі", а саме багатомаршрутного зв'язку з багаторівневим фізичним з'єднанням "Останньої Лінії" і динамічною адресацією клієнтів. Цей приклад ілюструється на прикладі нижнього правого кута Рис. 52C, де пакети даних, що відправляються за допомогою багаторівневого фізичного з'єднання "Останньої Лінії" і декількох маршрутизаторів, доставляються від клієнта з динамічними IP-адресами на кілька шлюзів SDNP за кількома маршрутами. Як показано на Рис. , перший пакет від клієнта з динамічною мережевою адресою джерела IP $C_{1,1}$ відправляється за кількома маршрутами до IP $M_{0,0}$ з використанням багаторівневого фізичного з'єднання "Останньої Лінії", визначеного медіа-адресами джерела і призначення MAC $C_{1,1}$ і MAC R_1. Другий пакет даних від клієнта, що має динамічно вибрану мережеву адресу джерела IP $C_{1,2}$, відправляється за кількома маршрутами до IP $M_{0,1}$ призначення з використанням багаторівневого фізичного з'єднання "Останньої Лінії", визначеного медіа-адресами джерела і призначення MAC $C_{1,2}$ і MAC R_2. Нарешті, третій пакет даних від клієнта, що має динамічно обрану мережеву адресу джерела IP C1,3, відправляється за кількома маршрутами до IP M0,3 з використанням багаторівневого фізичного з'єднання "Останньої лінії", визначеного медіа-адресами джерела і призначення MAC $C_{1,3}$ і MAC R_3. Таким чином, комбінація IP-адреси клієнта, IP-адреси шлюзу SDNP, MAC-адреси клієнта та MAC-адреси маршрутизатора змінюються динамічно, що робить відстеження викликів і збір метаданих практично неможливим.

Маскування IP-адреси клієнтського пристрою і затемнення маршрутизації "Останньої Милі" динамічною IP-адресацією, багаторівневим фізичним з'єднанням і багатомаршрутною передачею до кількох шлюзів може бути визначено або клієнтським пристроєм, або сигнальним сервером. Процес переспрямування може бути досягнутий за допомогою генерації випадкових чисел або інших псевдопромінювальних алгоритмів. Ключовим принципом є те, що зміни маршрутизації та транспорту є непередбачуваними.

Дві дещо менш надійні версії передачі даних пакетів "Останньої Милі" по мережі Ethernet за кількома маршрутами показані на Рис. 52D, де ліва сторона ілюстрації використовує статичну адресацію клієнта і з'єднання з багаторівневим фізичним з'єднанням "Останньої Лінії", а права -

динамічну адресацію клієнта, також з підключенням з багаторівневим фізичним з'єднанням "Останньої Лінії". Різниця між цими версіями і версіями багаторівневого фізичного з'єднання, які показані на Рис. 52C, полягає в тому, що раніше ці версії використовували один маршрутизатор R, а не розподіляли передачу даних кільком маршрутизаторам. При багатомаршрутній передачі з використанням одного маршрутизатора для підключення "Останньої Лінії" послідовні дані від клієнта розподіляються на кілька фізичних носіїв, тобто відбувається багаторівневе фізичне з'єднання "Останньої Лінії", потім повторно збираються одним маршрутизатором R і відправляються по решті частини "Останньої Милі", включаючи кілька шлюзів і будь-які інші паралельні частини "Останньої Милі" R. (не показано) з цього загального маршрутизатора на кілька окремих шлюзів призначення SDNP.

Як додаток до мережі Ethernet бездротовий зв'язок Wi-Fi може також використовуватися для зв'язку "Останньої Милі" між клієнтом SDNP і шлюзом SDNP. Для Wi-Fi зв'язку потрібен пакет даних з трьома або чотирма MAC-адресами, двома для радіозв'язку, одним або двома для дротового мережевого з'єднання, особливо з використанням пакетів даних Ethernet. Рис. 53 ілюструє той самий формат пакета Wi-Fi, адаптований для обміну даними за протоколами SDNP "Остання Миля" і "Остання Лінія". Як точку доступу для зв'язку "Остання Лінія" потрібно тільки три MAC-адреси довжиною 6B, а саме MAC-адреса 1 поле 235 для базової станції або "приймача", MAC-адреса 2 поле 236 для базової станції або "передавача" і MAC-адреса 3 поле 237 для дротового мережевого підключення до Wi-Fi маршрутизатору, тобто Ethernet або "інтернет". У процесі роботи цифрові значення MAC-адрес, завантажених у поля даних приймача і передавача, залежать від установки напрямку К або ОТ розподільної системи (i) чи передається пакет даних по радіо або Ethernet (ii) і чи конвертуються вхідні дані по Ethernet, в радіозв'язок. Поле даних MAC-адреса 4 239 необов'язкове, використовується тільки в тому випадку, якщо Wi-Fi-пристрій використовується як радіоміст в "бездротовому режимі розподілу". Хоча такий режим може використовуватися в мережах зв'язку "Останньої Милі" на великих відстанях в якості альтернативи стільниковим або мікрохвильовим мережам, наприклад, в пустелі, в цілому, використання Wi-Fi зв'язку в мережах "Останньої Милі" SDNP зазвичай орієнтовано на підключення "Останньої Милі" до клієнта SDNP. У зв'язку з цим, наступне обговорення буде зосереджено на режимі точки доступу для Wi-Fi роутерів з розумінням того, що методи SDNP однаково застосовні при маршрутизації в режимі бездротового розподілу.

Як і пакети даних Ethernet, преамбула 230 і роздільник стартових кадрів SFD 232 містять дані першого рівня для синхронізації даних і пристрою. Процедура конвергенції фізичного рівня PLCP 232 включає в себе поєднання інформації рівнів 1 і 2 (відповідна довжина пакета, швидкість передачі даних, перевірка помилок у заголовку тощо). Згідно зі стандартами IEEE 802.11 поля даних, що залишилися, містять інформацію про канал передачі даних другого рівня, включаючи Frame Control 233, в якому вказується тип пакета версії Wi-Fi в якості типу управління, контролю, резервування або "даних", що використовується для доставки корисних навантажень SDNP.

Тривалість та ідентифікатор 234 містить тривалість NAV (Вектор Розподілу Мережі), якщо тільки Wi-Fi-пристрій не знаходиться в режимі енергозбереження, у цьому випадку поле містить ідентифікатор радіостанції. NAV - це механізм віртуального виявлення оператора зв'язку, що використовується для економії електроенергії в бездротових системах зв'язку. Тривалість NAV можна розглядати як лічильник, зворотний відлік до нуля з однаковою швидкістю, після чого він визначає, чи знаходиться радіостанція в режимі очікування або продовжує спілкуватися. У режимі очікування лічильник багаторазово підраховує тривалість NAV, перевіряючи, чи не виявлена активність радіозв'язку, що вимагає уваги. Поле 238 "Керування послідовністю" або "Послідовність" описує послідовність пакетів та номер фрагмента, який визначає кадр пакета другого рівня. Перевірка кадрів 240 містить 32-бітову контрольну суму CRC всього пакету даних, тобто для перевірки з'єднання даних на наявність помилок.

Корисне навантаження Wi-Fi 241 — це поле даних довжиною від 0B до 2312B, що використовується для передачі корисного навантаження Wi-Fi. У повідомленні "Останньої Милі" SDNP це поле містить IP-датаграму, яку використовують у з'єднанні "Останньої Милі", включаючи IP-заголовок 434, транспортний заголовок 436 і корисне навантаження 435 SDNP.

IP-заголовок 434 змінюється залежно від того, чи слідує IP-датаграма протоколу IPv4 або IPv6, як визначено за полем протоколу 447, що містить двійковість 4, або поле протоколу 448, що містить двійковість 6. Преамбули 440 і 444 містять транспортний заголовок 470, що використовується для визначення використовуваного методу транспортування рівня 4, наприклад, TCP, UDP або функції обслуговування ICMP і IGMP. Зокрема, відповідно до захищеної динамічної мережі зв'язку та протоколу, TCP транспорт використовується для передачі програмного забезпечення і файлів даних, а UDP використовується для передачі

даних в режимі реального часу, таких як VoIP і відео. Довжина і формат транспортного заголовка 436 варіюється залежно від транспортного флагу 470. Заголовок 434 містить IPv4-адреси джерела та призначення 441 і 442 або IPv6-адреси джерела та призначення 445 і 446.

Як і пакети даних Ethernet, маршрутизація пакетів Wi-Fi "Останньої Милі" залежить як від IP-адрес, так і від MAC-адрес, символічно представлених іменами пристроїв, до яких належать IP або MAC-адреси. Послідовна маршрутизація пакетів Wi-Fi "Останньої Милі" показана в прикладах з Рис. 54A по Рис. 54D. Кожен рисунок містить два пакети Wi-Fi — верхній, що містить датаграму IPv4, і нижній, що містить датаграму IPv4. Оскільки IPv4 і IPv6 використовують різні формати з різною довжиною поля, показані два Wi-Fi пакети, як правило, мають різну довжину навіть при однаковому корисному навантаженні.

На першому етапі передачі даних корисне навантаження SDNP-A переміщується від клієнта SDNP 1400 до базової станції/маршрутизатора 1402W через "Останню Лінію" 1404 в якості носія радіосигналу Wi-Fi і по дротовій лінії до маршрутизатора 1402X по каналу BS 1415. Потім маршрутизатор 1402X передає пакет даних по каналу шлюзу 1414 на шлюз SDNP 1401. Відповідь від шлюзу SDNP клієнту включає корисне навантаження G SDNP від шлюзу 1401 по дротовій лінії зв'язку 1414 до маршрутизатора 1402X, по BL каналу 1415 до Wi-Fi маршрутизатора 1402W і через "Останню Лінію" 1404 до клієнта 1400, використовуючи Wi-Fi роутер як засіб зв'язку. Клієнт SDNP має числові MAC та IP-адреси MAC $C_{1,1}$ та IP $C_{1,1}$, Wi-Fi роутер 1402Ц має числову MAC адресу MAC W, роутер 1402A має числові MAC і IP-адреси MAC $M_{0,0}$ і IP $M_{0,0}$. IP-адреси Wi-Fi-роутера 1402W і дротового маршрутизатора 1402X не потрібні у відображенні на цьому Рис. .

На відміну від хмари SDNP, де пакетна маршрутизація датаграм SDNP повністю контролюється мережею SDNP, в мережах зв'язку "Останньої Милі" з використанням IP-датаграм корисне навантаження SDNP не може бути інтерпретовано або вплинути на маршрутизацію, тобто кожне з'єднання, що передається за "Останньою Милі", містить фіксовані IP-адреси джерела і призначення. Фізичні носії або канали, що використовуються для направлення пакетів Wi-Fi в радіозв'язку і для направлення пакетів Ethernet у дротовому зв'язку, управляються MAC-адресами, що з'єднують кожен вузол зв'язку в "Останній Милі".

Наприклад, на Рис. 54A показані пакети IPv4 і IPv6 "Останньої Лінії" Wi-Fi, що використовуються для однорівневої маршрутизації радіосигналу PHY до Wi-Fi маршрутизатора 1402W через "Останню Лінію" 1404, включаючи MAC-адресу MAC $C_{1,1}$ передавача і MAC-адресу одержувача MAC W. Wi-Fi маршрутизатор 1402W також забезпечує BS-канальну дротову лінію 1415 для маршрутизатора 1402X з "чистою" MAC-адресою призначення MAC R. Мережа третього рівня включає тільки кінцеві пристрої, тобто клієнт SDNP 1400 з вихідною IP-адресою IP $C_{1,1}$, а шлюз SDNP 1401 з адресою призначення IP $M_{0,0}$. На відміну від пакету даних Ethernet, пакет Wi-Fi містить три адреси - MAC-адреса передавача або джерела радіосигналу MAC $C_{1,1}$, MAC-адреса приймача або радіо пункту призначення MAC-адреса W і MAC-адреса Ethernet "net". У цьому напрямку передачі даних маршрутизатор 1402X діє як мережеве призначення пристрою Wi-Fi-роутера. Таким чином, пакет даних Wi-Fi визначає два носії, Wi-Fi роутер "Останньої Лінії" 1404 і Ethernet дротовий канал BS 1415. Рис. 54B ілюструє відповідні пакети Ethernet, що передають корисне навантаження SDNP A по каналу шлюзу 1414. Як описано вище, IP-адреси джерела та призначення залишаються незмінними як IP $C_{1,1}$ і IP $M_{0,0}$, тоді як MAC-адреси джерела і призначення змінюються з вихідних значень на MAC R і MAC $M_{0,0}$.

Зв'язок у відповідь включає в себе зміну IP-адрес одержувача і джерела та відповідне налаштування MAC-адрес. Рис. 54C ілюструє Ethernet пакети IPv4 і IPv6 для передачі даних від шлюзу SDNP 1401 до дротового маршрутизатора 1402X по шлюзу 1414. Щоб отримати інформацію про датаграму третього рівня IP-адреса джерела 441 містить мережеву адресу шлюзу SDNP 1401, тобто IP $M_{0,0}$, а IP адреса призначення містить значення IP $C_{1,1}$, адресу клієнта. MAC-адреси для Ethernet-пакету шлюзу - MAC $M_{0,0}$ для вихідної адреси 183 і MAC R для MAC-адреси призначення 182.

Рис. 54D ілюструє пакети IPv4 і IPv6 Wi-Fi для бездротових BS з'єднань 1415 і Wi-Fi радіостанцій "Останньої Лінії" 1404. Маршрутизація на мережевому рівні 3 включає в себе шлюз SDNP 1401 адресу IP $M_{0,0}$ і клієнтську адресу SDNP IP $C_{1,1}$ в якості адрес джерела і призначення 445 і 446. Функція поля MAC-адреси 237 з позначкою "net" змінюється відповідно до режиму радіо. У показаному тут режимі передачі в даному полі вказано Ethernet MAC-адресу джерела вхідних даних радіостанції, тобто числове значення MAC R маршрутизатора 1402X, що відправляє пакети даних в точку доступу Wi-Fi. У режимі приймача, показаному раніше на Рис. 54A, це поле визначає призначення даних за Ethernet, отриманих у вигляді радіо-пакетів і перетворених на Ethernet-пакети. У показаному прикладі в полі "net" 237 вказана одна і та ж

MAC-адреса маршрутизатора 1402X, тобто MAC R, для режиму передачі і прийому, що означає, що точка доступу Wi-Fi використовує один Ethernet-роутер для підключення "Останньої Милі".

При багатомаршрутному зв'язку по "Останній Милі" дротовий маршрутизатор, який використовується для маршрутизації пакетів даних, отриманих точкою доступу Wi-Fi, тобто в режимі прийому, може відрізнятися від того, який використовується для маршрутизації пакетів даних, що передаються точкою доступу Wi-Fi, тобто в режимі передачі даних. Наприклад, мережева MAC-адреса 237 для радіопередач в режимі приймача може мати цифрову MAC-адресу MAC R_1 в режимі передачі, дані можуть бути змінені на інший MAC R_2, тобто канал BS може за вибором містити багатофункціональну систему, залежну від напрямку. У режимі передачі пакети "Останньої Лінії" Wi-Fi, що використовуються для одноканальної радіо маршрутизації 1404 "Останньої Лінії" від Wi-Fi роутера до клієнта SDNP 1400 містять MAC-адресу 236 передавача з числовим значенням MAC W і MAC-адресу приймача 235, який містить числове значення MAC $C_{1,1}$. У цьому напрямку передачі даних дротовий маршрутизатор 1402A виступає як джерело даних, що передаються пристроєм Wi-Fi-маршрутизатора. Таким чином, пакет даних Wi-Fi об'єднує два середовища, Wi-Fi радіостанцію "Останньої Лінії" 1404 і Ethernet дротову BS лінію 1415.

Стільникові мережі являють собою ще одну форму бездротового зв'язку, адаптовану для зв'язку за протоколом SDNP "Останньої Милі". Стільникові мережі перерозподіляють вхідні пакети Ethernet на пакети MAC (Radio-Control Media Access Control). Дані можуть передаватися і прийматися за часом мультиплексування (TDMA), за кодовим розподілом (CDMA) або шляхом розповсюдження контенту на кілька підканальних частот (OFDM). У разі зв'язку 4G/LTE на основі OFDM або ортогонального частотного мультиплексування, пакети даних другого рівня складаються в стопку між трьома різними рівнями вбудованих сервісних блоків даних або SDU всередині другого рівня; найнижчий рівень включає PHY PDU 299, що містить однокадровий MAC SDU 304 разом з MAC-заголовком 303 і відступом 305, розподіленим по 20 слотах часу 300, які включають в себе наступне MAC SDU 304, які, в свою чергу, містить функцію управління радіоканалом або RLC SDU 308.

Функція керування радіоканалом (RLC) - це протокол другого рівня, який використовується в телефонії на базі 3G (UMTS) і 4G/LTE (OFDM). Функція керування радіоканалом полягає в реагуванні на запити верхнього рівня в одному з трьох режимів, тобто режимі підтвердження, режимі невизнання і режимі прозорості, а також у виявленні помилок, виправленні помилок, виявленні дублікатів і пакетуванні даних відповідно до зазначених форматів. Пакетизація даних включає об'єднання, сегментацію та збирання SDU RLC, а також впорядкування та пересегментацію PDU даних RLC. Наприклад, після виділення часу на виконання радіопередач, однокадровий RLC SDU 308 неминуче обмежується тривалістю і розміром файлу даних, доступного для передачі корисного навантаження. Однокадровий RLC SDU 308 повинен бути розділений на сегменти і відображений в іншому форматі другого рівня RLC - багатокадровий RLC SDU 319.

Як показано на Рис. 55, відображення однокадрового RLC SDU 308 в різні сегменти K, K+1, K+2 313, 314, 315 та ін. Багатокадрових RLC SDU 319 не відбувається на принципі один-к-одному. Як показано на прикладі, відображення однокадрового RLC SDU 308 закінчується в середині сегмента K+2 315. Частина залишеного сегмента K + 1, яка не була передана, передається в новому однокадровому RLC SDU 312, але тільки з урахуванням часу відступу 310, необхідного для синхронізації радіочасів і обробки заголовка 311 RLC. У цьому методі передача даних, інкапсульованих в слот K+2, відновлюється саме там, де вона була перервана, як якщо б потік даних не був перерваний. Функція 4G аналогічна призупиненню відтворення фільму в кодуванні DVD в середині розділу DVD, очікуванню моменту для виконання деяких інших функцій, а потім відновленню відтворення саме там, де воно було призупинено. Таким чином, не втрачається вміст даних, а швидкість передачі даних у стільниковій мережі максимізується без втрати пропускної здатності радіостанції, за винятком пропускної здатності пакета (наприклад, заголовків PDU), і мінімальної деградації швидкості передачі даних в результаті додавання часу синхронізації 310.

Багатокадрові RLC SDU 319 інкапсулюють PDCP PDU 320 в листуванні один-на-один з кожним сегментом K. Наприклад, сегмент K^{th} 313 несе PDCP заголовок 321A і корисне навантаження IP 323, сегмент $(K+1)^{th}$ 314 несе PDCP заголовок 321B і корисне навантаження IP 324, сегмент $(K+2)^{th}$ 315 несе PDCP заголовок 321C і корисне навантаження IP 325б і т.д. Термін PDCP - абревіатура від Протоколу конвергенції пакетних даних, як зазначено в протоколі зв'язку 3G і 4G/LTE, що виконує такі функції, як стиснення, шифрування, забезпечення цілісності, а також контроль передачі даних користувача. Заголовки PDCP відрізняються залежно від типу даних, що передаються, наприклад, дані користувача, контрольні дані тощо.

Оскільки передача даних у пакетах даних 4G має безперервно скомбінований потік даних, розмір корисного навантаження не квантується на блоки певної довжини, як у пакетах даних Ethernet і Wi-Fi. Замість цього поля даних 323, 324, 325..., що передаються відповідними сегментами даних другого рівня 313, 314, 315... можуть поступово підтримувати корисне навантаження будь-якого розміру, як показано на Рис. , включаючи IP-заголовок 434 і IP-заголовок 435, що містить транспортне навантаження 436 і SDNP 1430. Більш того, в OFDM-комунікаціях кожен раз, коли слот одночасно передає дані на кілька частотних підносіїв, це означає, що загальна пропускна здатність даних визначається не тільки тривалістю часу по одному каналу, як це відбувається в TDMA. Однак для зручності часто буває зручно підтримувати розмір IP-датаграми відповідно до стандартів Ethernet або Wi-Fi.

Як показано на зображенні, заголовок 434 змінюється залежно від того, чи слідує IP-датаграма за протоколом IPv4 або IPv6, як визначено полем протоколу 447, що включає двійковість 4 або протокол 448, що включає двійковість 6. Преамбули 440 і 444 містять транспортний заголовок 470, що використовується для визначення використовуваного методу транспортування рівня 4, наприклад, TCP, UDP або функції обслуговування ICMP і IGMP. Зокрема, відповідно до Захищеної динамічної мережі та протоколу, TCP транспорт використовується для передачі програмного забезпечення та файлів даних, а UDP використовується для передачі даних в режимі реального часу, таких як VoIP і відео. Довжина і формат транспортного заголовка 436 змінюється залежно від біта 470 транспортного заголовка. Заголовок 434 містить IPv4-адреси джерела та призначення 441 і 442 або IPv6-адреси джерела та призначення 445 і 446.

Як приклад 4G-зв'язку з використанням датаграм IPv6, Рис. 56A ілюструє стільникову радіостанцію 1404 "Останньої Лінії" маршрутизацію до вишки стільникового зв'язку та базової станції 1402Q. Зокрема, в полі джерела MAC-адреси 300A PDU RLC визначає адресу джерела даних стільникового зв'язку як MAC $C_{1,1}$, пристрій клієнта. Аналогічно поле призначення MAC-адреси 300B визначає медіа-адресу приймача стільникового зв'язку як MAC BS, що описує вишку стільникового зв'язку і базову станцію. Мережева маршрутизація третього рівня включає в себе тільки кінцеві пристрої "Останньої Милі", тобто клієнт SDNP 1400 з вихідною IP-адресою IP $C_{1,1}$ і шлюз SDNP 1401 з адресою призначення IP $M_{0,0}$. Як описано вище, поля даних 323, 324 і 325 не обов'язково відповідають певним розділам даних датаграми IPv6, де поле даних 323 включає IP-адресу джерела 445, IP-адресу призначення 446 і частину корисного навантаження SDNP A 435, включаючи транспортний заголовок 436. Поля даних 324 і 325 містять частину корисного навантаження SDNP 435, яка не була передана.

Рис. 56B ілюструє пакети даних для корисного навантаження G відповідного повідомлення SDNP через стільникове з'єднання "Останньої Лінії" 1404 від вишки стільникового зв'язку та базової станції 1402Q до мобільного клієнтського пристрою 1400, де адреса джерела і призначення з попередніх пакетів даних були замінені, а саме адреса джерела стільникового зв'язку 300A йде з медіа адресою MAC BS як навантаження, 300B адресу призначення стільникового зв'язку встановлено в полі MAC $C_{1,1}$, IP-адресу MAC-адреса клієнта в полі $IP_{0,0}$, MAC-адресу джерела даних встановлено в полі M6. Маршрутизація між мережевим маршрутизатором 1402X і вишкою стільникового зв'язку і базовою станцією 1402Q по каналу BS 1415 використовує пакети даних Ethernet, що відповідають попереднім прикладам.

Багаторівневе фізичне з'єднання за "Останньою Лінією" може включати будь-яке з вищезгаданих медіа, що використовуються в різних комбінаціях. Реалізації багаторівневого з'єднання можуть включати кілька дротових з'єднань, що передають дані з однаковою або різною швидкістю передачі і використовують загальні або різні протоколи другого рівня, такі як USB, Ethernet 10BASE-T, 100BASE-T, 1000BASE-T або DOCSIS3. Фізичні носії можуть включати мережеві кабелі Ethernet або USB, що відповідають стандартам, коаксіальні кабелі, оптоволоконні з'єднання або навіть мідні з'єднання вітою пари для DSL, хоча і зі зниженим рівнем продуктивності.

Бездротове багаторівневе фізичне з'єднання може включати в себе поєднання форматів Wi-Fi, стільникового, супутникового або пропрієтарного радіозв'язку, що працюють в радіочастотному і надвисоких частотах. Бездротовий зв'язок "Останньої Лінії" може також включати технології малого радіусу дії, такі як Bluetooth або мікростільникові мережі, такі як PHS в Японії. Бездротові протоколи можуть включати стільникові формати 2G, 2.5G, 3G і 4G/LTE, включаючи, наприклад, аналогові, TDMA, GSM, CDMA, UMTS і OFDM, протоколи Wi-Fi 802.11a, 802.11b, 802.11g, 802.11n и 802.11n, а також власні формати супутникового зв'язку або спеціальні радіоканали. Оскільки протоколи 2-го рівня відрізняються залежно від фізичних носіїв рівня 1, термін "взаємодія декількох рівнів", що використовується в контексті даного опису,

означає комбінацію фізичного та канального рівнів OSI, тобто рівні 1 і 2, і не повинен тлумачитися виключно як такий, що обмежує вимоги до фізичних носіїв рівня 1.

Приклади багатоканального високошвидкісного зв'язку з використанням загального протоколу рівня 2 наведено на Рис. 57A, включаючи Ethernet, Wi-Fi і стільникову реалізацію. У самому верхньому прикладі багаторівневого фізичного з'єднання по Ethernet маршрутизатор 27 зв'язується з персональним комп'ютером 36 за допомогою двох Ethernet-кабелів, що складаються з дротових або оптоволоконних ліній 24A і 24B, що працюють відповідно за 100BASE-T і 1000BASE-T. Для забезпечення взаємодії гіперзахищеної комунікації через "Останню Милю", на Рис. показано ноутбук 36, на якому встановлено програмне забезпечення SDNP 1335C.

У центральній частині рисунка багаторівневе з'єднання по Wi-Fi, Wi-Fi роутер 100 зв'язується з ноутбуком 35 через два Wi-Fi канали, показаних як Wi-Fi з'єднання 29A і 29B, перший працює за протоколом 801.11n на частоті 2.4GHz, а другий використовує 802.11ac для зв'язку по каналу 5GHz. Для роботи в режимі багаторівневого з'єднання ноутбук 35 повинен бути включений для одночасної передачі і прийому сигналів на декількох частотах за допомогою багатодіапазонної антени 26B, вбудованої в ноутбук. Аналогічним чином, Wi-Fi роутер повинен бути здатний передавати і приймати сигнали на декількох частотах одночасно, використовуючи багатодіапазонні антени 26. Для забезпечення взаємодії гіперзахищеної комунікації через "Останню Милю" на Рис. зображено ноутбук 35, на якому встановлено програмне забезпечення SDNP 1335C.

У нижній частині рисунка, що показує багатосмуговий стільниковий зв'язок, базова станція 17 здійснює одночасний зв'язок через багатосмугову стільникову вежу 18A з планшетом 39, використовуючи два різних радіоканали, що складаються зі стільникових ліній 28A і 28B з відповідними частотами 1,8ГГц і 900МГц. У наведеному прикладі стільниковий зв'язок являє собою мережу 4G/LTE. Як показано на Рис. , планшет 39 повинен бути включений для одночасної передачі і прийому сигналів на декількох частотах за допомогою внутрішньої багатодіапазонної антени 18B. Для забезпечення взаємодії гіперзахищеної комунікації через "Останню Милю" на Рис. зображено ноутбук 35, на якому встановлено додаток SDNP 1335A.

Така багаторівнева взаємодія з використанням загального протоколу 2-го рівня збиває з пантелику кіберзлодія, оскільки хакер повинен отримати фізичний доступ до двох різних каналів передачі даних 2-го рівня, кожен з яких може включати власну безпеку. Крім того, якщо клієнт використовує програмне забезпечення SDNP 1335C, SDNP додаток 1335A або мікропрограму SDNP 1335B (не показана), маршрутизація корисного навантаження SDNP через багаторівневе з'єднання використовує унікальні динамічні облікові дані безпеки, що робить перехоплення і інтерпретування пакетів SDNP занадто складною для злому в реальному часі.

Приклади багаторівневої передачі даних з використанням змішаних протоколів рівня 2 і рівня 2 показані на Рис. 57B. У цих прикладах дані "Останньої Лінії" передаються з використанням комбінацій стільникових, Wi-Fi і супутникових систем. У верхньому прикладі змішаного мульти-високочастотного зв'язку Wi-Fi роутер 100 взаємодіє з персональним комп'ютером 36, використовуючи комбінацію дротового або оптоволоконного з'єднання 100BASE-T Ethernet 24B і Wi-Fi каналу 802.11ac 29B, що працюють на частоті 5GHz. Щоб гарантувати гіперзахищену взаємодію через "Останню Милю", на Рис. відображено персональний комп'ютер 36 з встановленим програмним забезпеченням SDNP 1335C. Такий приклад є комбінацією дротового та бездротового зв'язку, коли перехоплення бездротових пакетів не дозволяє перехопити або переглянути дані дротового зв'язку. Цей змішаний метод розподілу Ethernet + мультисмугове з'єднання Wi-Fi через "Останню Лінії" особливо добре підходить для розгортання корпоративних офісних мереж, що складаються з захищених персональних комп'ютерів в будівлі або кампусі, що зв'язуються з закритими серверами в закритих приміщеннях з обмеженим доступом.

У середній схемі змішаного багаторівневого з'єднання, показаного на Рис. 57B, стільниковий телефон 32 з внутрішньою багатодіапазонною антеною 18C спілкується за допомогою двох різних бездротових технологій. Одне Wi-Fi з'єднання 29C з'єднується з Wi-Fi роутером 100 і антеною 26, використовуючи, наприклад, протокол 802.11n на частоті 5GHz. Друге з'єднання, стільниковий зв'язок 28C, використовує 1,8 ГГц оператора, що працює за протоколом 4G/LTE для забезпечення підключення "Останньої Лінії" до вишки стільникового зв'язку 25 і базової станції 17. Оскільки вишки стільникового зв'язку 25 і антени Wi-Fi 26 працюють на незв'язаних системах, такий підхід до багаторівневого з'єднання повністю приховує будь-які зв'язки між пакетами даних, що передаються безліччю фізичних носіїв в "Останній Лінії". Щоб забезпечити гіперзахищену комунікацію через "Останню Милю", на Рис. відображено мобільний телефон 32 з встановленим додатком SDNP 1335A.

Подібний спосіб досягнення багаторівневого з'єднання в "Останній Лінії", що об'єднує стільниковий і супутниковий зв'язок, показаний на нижній ілюстрації Рис. 57B, де супутник/стільниковий телефон 32Z працює під управлінням програми SDNP 1335A і взаємодіє по двох мережах далекого зв'язку - стільниковим зв'язком 28D зі стільниковою вишкою 25 і базовою станцією 17 на 1,8 ГГц і супутниковим зв'язком 95W із супутником 92, наприклад, 1,9 ГГц. Супутник 92, у свою чергу, зв'язується з наземною супутниковою антеною і базовою станцією 92B по широкосмуговому каналу зв'язку 95X, не обов'язково на тій же частоті, що і зв'язок з клієнтом.

Рис. 57C ілюструє ще один різновид багатоканального високочастотного зв'язку - кілька фізичних середовищ, що використовують загальні протоколи, але здатних одночасно використовувати кілька каналів зв'язку з розділенням частот. Така система вимагає високу пропускну здатність середовища, щоб працювати без сильних навантажень, тобто там, де продуктивність знижується в міру того, як все більше користувачів займають смугу пропускання і пропускну здатність середовища. Лише три таких носії легкодоступні з такою великою пропускною здатністю, а саме: i) кабельні системи DOCSIS3 з використанням коаксіального кабелю; ii) кабельні системи DOCSIS 3 з використанням оптичного волокна; і iii) супутникові системи зв'язку з частотою декількох ГГц на низьких навколоземних орбітах. Зокрема, на самій верхній ілюстрації багатосмугової кабельної системи показана приставка або кабельний модем 102B з мікропрограмою SDNP 1335M, що підключається до кабелю CMTS 101 через кілька діапазонів коаксіальним або оптоволоконним кабелем 105 за протоколом DOCSIS3.

На нижній схемі показана супутникова мережа з кількома з'єднаннями, в якій стільниковий телефон 32Z з встановленим додатком SDNP 1335A підтримує зв'язок із супутником зв'язку 92, використовуючи кілька несучих частот 95Z, відформатованих за власним протоколом зв'язку. Зв'язок між супутником 92 і наземною супутниковою антенною і базовою станцією 92B використовує протокол магістральної лінії 95X, що змішує тисячі викликів, що робить ідентифікацію і перехоплення певного виклику проблематичним для хакера, а використання багатоканального зв'язку за кількома діапазонами забезпечує гіперзахищений зв'язок лінії для клієнта 95Z.

Інший приклад пакетів даних, які використовуються у маршрутизації багаторівневого з'єднання "Останньої Лінії", показано на Рис. 58, де клієнт SDNP 1400 взаємодіє з маршрутизатором 1402A через два окремих з'єднання, що включають дротові або оптоволоконні лінії Ethernet 24A і 24B, наприклад, протоколи 100BASE-T і 1000BASE-T, відповідно. Маршрутизатор 1402A, у свою чергу, підключається до шлюзу SDNP 1401 по каналу 1414. Обидва Ethernet-пакети визначають IP-адресу джерела 445, тобто клієнтського пристрою, як IP $C_{1,1}$, а IP-адресу призначення 446 шлюзу SDNP як IP $M_{0,0}$. Пакет A Ethernet, що передається по мережі по дротовій або оптоволоконній лінії 24A, включає MAC-адресу призначення 182, включаючи MAC R і MAC-адресу джерела 183, включаючи MAC $C_{1,1}$. Пакет B Ethernet, що передається за з'єднанням, реалізованим за дротовою або оптоволоконною лінією 24B, включає MAC-адресу призначення 182, що містить MAC R та іншу MAC-адресу джерела 183, що містить MAC $C_{1,2}$, що визначає альтернативне з'єднання.

Зміна медіа-адреси джерела з MAC $C_{1,1}$ на MAC $C_{1,2}$ перенаправляє Ethernet-комунікацію з частоти 2,6 ГГц 100BASE-T на 1000BASE-T-підключення. У процесі роботи пакети даних з клієнтського пристрою SDNP 1400 фрагментуються і потім розподіляються на корисне навантаження SDNP A і SDNP B відповідно до алгоритмів SDNP і загальних секретів. Фрагментована передача даних по "Останній Лінії" багаторівневого з'єднання відбувається з корисним навантаженням SDNP A, що передається по пакету A по Ethernet через дротовий або оптоволоконний канал і корисним навантаженням SDNP B, що передається по пакету B Ethernet по дротовому або оптоволоконному каналу 24B.

Інший приклад пакетів даних, які використовуються у маршрутизації багаторівневого з'єднання "Останньої Лінії", показано на Рис. 59, де клієнт SDNP 1400 взаємодіє з Wi-Fi роутером 1402W через два окремих з'єднання, що містять Wi-Fi з'єднання 29A і 29B, використовуючи, наприклад, протоколи 802.11n на частоті 2.4GHz і 802.11ac на 5GHz відповідно. Маршрутизатор 1402W у свою чергу підключається до маршрутизатора 1402X по каналу BS 1415, а маршрутизатор 1402X - до шлюзу SDNP 1401 по каналу шлюзу 1414. Обидва Wi-Fi пакети визначають IP-адресу джерела 445, тобто клієнтського пристрою, як IP $C_{1,1}$, а IP-адресу призначення 446 шлюзу SDNP як IP $M_{0,0}$. Пакет Wi-Fi A, маршрутизований по мережі Wi-Fi A, включає MAC-адресу джерела радіосигналу 236, включаючи MAC $C_{1,1}$, MAC-адресу одержувача радіосигналу 235 і MAC-адресу одержувача 235, MAC-адресу одержувача мережі 237, MAC-адресу отримувача 237, MAC-адресу мережі Wi-Fi пакет B, маршрутизований по

мережі Wi-Fi 29B включає MAC-адресу одержувача 2,236, MAC-адресу одержувача радіосигналу 2.

Зміна медіа-адреси джерела з MAC $C_{1,1}$ на MAC $C_{1,2}$ перенаправляє передачу з Wi-Fi радіо 2,6 ГГц на 5 ГГц трансівер. У процесі роботи пакети даних з клієнтського пристрою SDNP 1400 фрагментуються і потім розподіляються на корисне навантаження SDNP A і SDNP B відповідно з алгоритмами SDNP і розділюваними секретами. Фрагментована передача даних через багаторівневе з'єднання "Останньої Лінії" відбувається з корисним навантаженням SDNP A, що передається по Wi-Fi каналу 29A пакетом A, і корисним навантаженням SDNP B, що передається по Wi-Fi пакету B по Wi-Fi каналу 29B.

Ще один приклад пакетів даних, що використовуються в маршрутизації багаторівневого PHY-з'єднання "Останньої Лінії", представлений на Рис. 60, де клієнт SDNP 1400 взаємодіє з вишкою стільникового зв'язку 1402Q через два окремих PHY-з'єднання, що включають стільникові лінії 28A і 28B, використовуючи, наприклад, протоколи 4G/LTE на частоті 1,8GHz і 4G/LTE на частоті 900MHz відповідно. Маршрутизатор 1402Q у свою чергу підключається до маршрутизатора 1402X по каналу BS 1415, а маршрутизатор 1402X - до шлюзу SDNP 1401 по каналу шлюзу 1414. Обидва стільникові радіопередавачі визначають IP-адресу джерела 445, тобто клієнтського пристрою, як IP $C_{1,1}$, а IP-адресу призначення 446 шлюзу SDNP як IP $M_{0,0}$. Стільниковий пакет A, який маршрутизовано за PHY-з'єднання, реалізованого по стільниковій лінії 28A, включає MAC-адреси джерела 300A, включаючи MAC $C_{1,1}$, і MAC-адреси одержувача 300B, що містить MAC BS. Стільниковий пакет B, який маршрутизовано за PHY-з'єднання, реалізованого по стільниковій лінії 28B, включає MAC-адресу передавача 300A, що включає MAC $C_{1,2}$, і MAC-адресу одержувача 300B, що включає MAC BS.

Зміна медіа-адреси джерела з MAC $C_{1,1}$ на MAC $C_{1,2}$ перенаправляє передачу зі стільникового радіо 1,8GHz 4G/LTE на 900MHz. У процесі роботи пакети даних з клієнтського пристрою SDNP 1400 фрагментуються, а потім розподіляються на корисне навантаження SDNP A і SDNP B відповідно до алгоритмів SDNP і загальних секретів. Фрагментована передача даних через багаторівневе PHY-з'єднання "Останньої Лінії" відбувається з корисним навантаженням SDNP A, що переноситься стільниковим пакетом A по Wi-Fi каналу 28A, і корисним навантаженням B SDNP, що переноситься стільниковим пакетом B по Wi-Fi каналу 28B.

Як було описано вище, комунікація за методом "багаторівневого PHY-з'єднання" може також включати різні комунікаційні середовища. У таких випадках пакет даних для кожного з'єднання повинен бути відформатований відповідно до протоколів другого рівня для відповідних фізичних носіїв. Наприклад, на Рис. 61 показано гібридний зв'язок "Останньої Лінії", що включає Ethernet і Wi-Fi, при якій клієнт SDNP 1400 взаємодіє з Wi-Fi роутером через два окремих PHY-з'єднання, що включають дротовий або оптоволоконний канал Ethernet 24A і Wi-Fi 29B, використовуючи, наприклад, 100BASE-T і 802.11ac при 5ГГц відповідно. Маршрутизатор 1402W, у свою чергу, підключається до маршрутизатора 1402X по каналу BS 1415, а маршрутизатор 1402X - до шлюзу SDNP 1401 по каналу шлюзу 1414. Обидва Wi-Fi пакети визначають IP-адресу джерела 445, тобто клієнтського пристрою, як IP $C_{1,1}$, а IP-адресу призначення 446 шлюзу SDNP як IP $M_{0,0}$. Ethernet маршрутизація по PHY-з'єднанню, здійснювана за дротовою або оптоволоконною лінією 24A, включає MAC-адресу джерела 183, включаючи MAC-адресу $C_{1,1}$, і MAC-адресу одержувача 182, включаючи MAC-адресу W. Пакет Wi-Fi B, що передається за PHY-з'єднання, що реалізується за Wi-Fi лінії 29B, включає MAC-адресу джерела 236, включаючи MAC-адресу C1,2, MAC-адресу 235, включаючи MAC-адресу W, і MAC-адресу одержувача 237.

Зміна медіа-адреси джерела сигналу з MAC $C_{1,1}$ на MAC $C_{1,2}$ перенаправляє передачу з Ethernet на Wi-Fi. У процесі роботи пакети даних з клієнтського пристрою SDNP 1400 фрагментуються, а потім розподіляються на корисне навантаження SDNP A і SDNP B відповідно до алгоритмів SDNP і загальних секретів. Фрагментована передача даних за допомогою багаторівневого PHY-з'єднання "Останньої Лінії" відбувається з корисним навантаженням SDNP A, що передається за пакетом Ethernet A через дротове або оптоволоконне з'єднання і корисним навантаженням B SDNP, що передається по Wi-Fi пакету B по каналу Wi-Fi 29B.

Рис. 62 ілюструє гібридне з'єднання "Останньої Лінії", що включає Wi-Fi і стільниковий зв'язок, де клієнт SDNP 1400 взаємодіє з більш ніж двома окремими PHY-з'єднаннями з двома різними бездротовими базовими станціями, а саме по Wi-Fi зв'язку 29A з Wi-Fi роутером 1402W працює на частоті 802.11n 2.4GHz і 28B зі стільниковою базовою станцією 1402Q працює на частоті 4G/LTE більш 900MHz. Маршрутизатори 1402W і 1402Q, своєю чергою, підключаються до маршрутизатора 1402X каналом BS 1415A і 1415B відповідно, а маршрутизатор 1402X підключається до шлюзу SDNP 1401 каналом шлюзу 1414. І Wi-Fi, і 4G стільникові пакети визначають IP-адресу джерела 445, тобто клієнтського пристрою, як IP $C_{1,1}$, а IP-адресу

приймача 446 шлюзу SDNP як IP $M_{0,0}$. Пакет Wi-Fi A, який маршрутизовано за PHY-з'єднанням, реалізованим по Wi-Fi лінії 29A, включає MAC-адресу передавача радіосигналу 236, включаючи MAC-адресу $C_{1,1}$, MAC-адресу радіоприймача 235, включаючи MAC W, і MAC-адреса джерела мережі 237, включаючи MAC R. Стільникова станція B, яка маршрутизовано за PHY-з'єднанням, що реалізується по Wi-Fi лінії 29B, включає MAC-адресу джерела 300B, включаючи MAC-адресу $C_{1,2}$ і MAC-адресу приймача 330B, включаючи MAC-адресу BS.

Зміна медіа-адреси джерела з MAC $C_{1,1}$ на MAC $C_{1,2}$ перенаправляє передачу даних з Wi-Fi LAN мережі в стільникову мережу. У процесі роботи пакети даних з клієнтського пристрою SDNP 1400 фрагментуються, а потім розподіляються на корисне навантаження SDNP A і SDNP B відповідно до алгоритмів SDNP і загальних секретів. Фрагментована передача даних через багаторівневе PHY-з'єднання "Останньої Лінії" відбувається з корисним навантаженням SDNP A, що передається по Wi-Fi пакету A через Wi-Fi канал 29A, і корисним навантаженням B, що передається по стільниковому пакету B по стільниковому каналу 28B.

Інша форма багаторівневого PHY-з'єднання включає фізичні комунікаційні середовища, здатні підтримувати безліч каналів на різних частотах і використовувати різні протоколи для різних пакетів даних. Така реалізація може бути спрощена за допомогою системи розподілу кабелів на базі DOCSIS3, що виконує програмне забезпечення SDNP. Стек зв'язку OSI для SDNP-сумісної кабельної розподільної системи DOCSIS3 представлений на Рис. 63, включаючи PHY-з'єднання рівня 1, канал передачі даних рівня 2 і мережу рівня 3 як для кінцевого пристрою кабельних модемів CMTS 101, так і для кабельного модема CM 103 або конвертеру відеосигналу STB 102. Зокрема, кінцевий пристрій кабельного модема CMTS 101 і пов'язаний з ним стек 378 містить мережевий інтерфейс рівня 1 361, підключений до хмарних серверів 22 та Інтернету 20, або, опціонально до головної станції мережі кабельного телебачення, системи IPTV або системи VoIP (не показана). Поєднання мережевого інтерфейсу 361 і канального рівня 366 включено в комунікаційний стек 378 інтерфейсу кінцевого пристрою кабельних модемів CMTS 101. На каналі зв'язку другого рівня дані передаються зі стека зв'язку мережевого інтерфейсу в стек зв'язку кабельного інтерфейсу мережі через функцію переадресації 370, а саме в контролер рівня зв'язку LLC 369. Контроль рівня зв'язку 802.2 LLC 369 являє собою апаратно-незалежний протокол, визначений відповідно до специфікації 802.2 стандарту IEEE. Пакетні дані потім модифікуються за допомогою функції безпеки 368 для забезпечення елементарної безпеки пакетів, в першу чергу для запобігання несанкціонованого перегляду контенту, такого як трансляція за типом "оплата за перегляд".

PHY-кабельний інтерфейс рівня 1 362 потім відправляє кадри даних по розподільчій мережі 102, що містять коаксіальний кабель 104 або оптоволоконний кабель 91, на відповідний PHY-кабельний інтерфейс рівня 1 363 в кабельному модемі CM 103 або конвертер відеосигналу STB 102. Кабельний інтерфейс 363 являє собою фізичний рівень інтерфейсу кабельної мережі, показаний як стек зв'язку OSI 379 кабельного модема CM 103 або конвертер відеосигналу STB 102. Після отримання пакета даних кабельний MAC інтерфейс 371 інтерпретує кабельні MAC-адреси, передаючи своє корисне навантаження для забезпечення безпеки з'єднання 372 для дешифрування і в кінцевому підсумку апаратно незалежному управлінню канальним рівнем 802.2 LLC 373 для інтерпретації. Вхідні дані стека кабельної мережі зв'язку CM або STB потім передаються через прозорий міст (transparent bridging) 374 до стеку зв'язку інтерфейсу CM або STB пристрою, а саме до незалежного управління канальним рівнем 802.2 LLC 375 пристрою відповідно до специфікації IEEE 802.2. Потім пакет передається або в HSD & IPTV MAC блоці 376, або в Wi-Fi 802.11 MAC блоці 377 для оновлення MAC-адрес пакета. У разі Wi-Fi зв'язку пакет даних передається з блоку 377 MAC-адреси 802.11 на Wi-Fi радіо інтерфейс фізичного рівня 1 365 для передачі на Wi-Fi антену 26. У разі дротових з'єднань пакет даних потім передається від MAC-адреси HSD і IPTV блоку 376 до блоку інтерфейсу Ethernet або HDMI 364 для підключення до телевізора 39 або персонального комп'ютера 36.

Фізичний і канальний рівні, як описано вище, встановлюють з'єднання між кінцевою системою кабельних модемів CMTS і будь-якою кількістю кабельних модемів CM. У комунікаційних стеках CMTS 378 і CM 379 пакети даних готуються на третьому рівні OSI 360A і 360B, відповідно, у вигляді IP-датаграм IPv4, IPv6 або ICMPv6 з використанням IP-адрес, що розпізнаються кабельною мережею або DNS-серверами. У комунікації "Останньої Милі" пакети даних SDNP, що використовують пакети даних IPv4 або IPv6 з IP-адресами джерела і призначення SDNP, зазвичай не використовуються, оскільки підключені пристрої, не підтримувані програмним забезпеченням або мікропрограмою SDNP, не мають можливості інтерпретувати адреси маршрутизації даних SDNP.

Робота на транспортному рівні 4 в мережі кабельного модема залежить від конкретного пристрою. У разі CMTS 101, транспортний рівень 4 рівня 1420 комунікаційного стека 378 OSI

використовує виключно UDP, так як його робота вимагає комунікації в режимі реального часу, наприклад, потокової передачі відео даних. З цієї точки зору кабельний зв'язок 102 більше схожий на SDNP мережу реального часу, ніж Інтернет. Оскільки кабельний модем має функціональну сумісність як з Інтернетом, так і з кабельною мережею в якості клієнта, тобто кінцевого комунікаційного пристрою, транспортний рівень 4 рівня 1420B в комунікаційному стеку 379 OSI CM 103 або конвертері відеосигналу STB 102 використовує UDP для операцій в режимі реального часу і використовує TCP для інтернет даних. Таке використання проблематичне для операторів OTT, що використовують VoIP-телефонію, оскільки кабельна мережа буде інтерпретувати IP-датаграми як дані, автоматично використовуючи TCP і транспортний протокол і покращуючи якість обслуговування і затримку поширення в режимі реального часу зв'язку. Ця проблема не виникає в кабельних модемах з підтримкою SDNP - в тих випадках, коли CM або STB працюють з мікропрограмою або програмним забезпеченням SDNP, програмне забезпечення SDNP контекстуально визначає, коли використання TCP є виправданим (для програмного забезпечення і файлів), а коли немає, тобто для даних у режимі реального часу.

Рівні додатків, а саме рівні OSI від 5 до 7, розташовуються на верхньому рівні транспортних операцій 1420A в CMTS 101 і 1420B в CM 103 або STB 102. У CMTS 101 ці програми зазвичай пов'язані з комунікаційними завданнями, такими як SNMP 1431A, стандартний протокол Інтернету для збору та організації інформації про підключені пристрої в IP-мережах. Інші функції включають DHCPv4 1432A і DHCPv6 1433A. DHCP, абревіатура для протоколу динамічної конфігурації хосту - це протокол для клієнтів і серверів, який автоматично надає IP хосту необхідну інформацію про маршрутизацію, включаючи динамічно створену (нестатичну) IP адресу, основний шлюз і маску підмережі. Хоча генерація в Інтернеті залежить від конкретного покоління, тобто для IPv4 або IPv6, функція генерації динамічних IP-адрес, як шлюз NAT або SNMP, є загальною і однаково застосовною в кабельних системах DOCSIS3 для CMTS 101 і CM 103 або STB 102.

Реалізація на прикладному рівні захищеної динамічної мережі зв'язку та протоколу, описаних тут, реалізованої у вигляді мікропрограми SDNP 1430A, що працює поверх операційної системи CMTS 101, може виконувати будь-яку кількість унікальних завдань, у тому числі:

- Робота в режимі наскрізного пропуску без інтерпретації корисного навантаження SDNP 1430, в цьому випадку CM 103 повинен бути дозволений для відкриття і зчитування корисного навантаження SDNP, тобто CM 103 повинен бути клієнтом SDNP.

- Робота в якості віддаленого шлюзу SDNP "Останньої Милі", тобто інтерпретація вмісту корисного навантаження SDNP і перетворення вмісту в спеціальне повідомлення DOCSIS3 (включаючи безпеку посилань) для пересилання в CM 103. У таких випадках CM 103 не вимагає використання клієнтського ПЗ SDNP або мікропрограмного забезпечення.

- Працює як SDNP міст "Останньої Милі", перетворює IP-датаграми в датаграми SDNP і передає дані SDNP в CM 103. У таких випадках CM 103 повинен працювати з клієнтським ПЗ SDNP або мікропрограму для підключення до SDNP-мосту, тобто формувати спеціальну "плаваючу" мережу SDNP.

Як показано на Рис. , комунікаційний стек OSI 379 для CM 103 і STB 102 включає безліч додатків, що класифікуються як OSI з рівня 5 по рівень 7, включаючи вищезазначені програми SNMP 1431B, DHCPv4 1432B і DHCPv6 1433B. Інша функція, утиліта TFTP 1434B або "тривіальний протокол передачі файлів" в основному використовується в DOCSIS3 як засіб для завантаження оновлень програмного забезпечення та програмного забезпечення з CMTS на кабельні модеми і конвертери відеосигналу по всій кабельній мережі. У кабельних мережах протокол HTTP 1435B, або протокол передачі гіпертексту призначений в першу чергу для відмальовки динамічних меню, що використовуються в смарт-телевізорах. Інші програми (позначені скороченою нотацією "Otr" 1436B) включають ігрові програми, діагностику, IPTV програми, функції відеозапису та багато іншого. Мікропрограма SDNP 1430B, що працює на CM 103 або STB 102, може бути розширена, - гіперзахищена "Остання Миля" забезпечує зв'язок з користувачем і з "Останньою Лінією" незалежно від того, чи використовує CMTS 101 програмне забезпечення SDNP чи ні.

Рис. 64 ілюструє побудову пакета даних DOCSIS3, адаптованого для доставки корисного навантаження SDNP 1430. Як показано на Рис. , рівень 1 включає кадр фізичного носія 390 змінної довжини і тривалості, що містить дані MAC-адреси другого рівня, включаючи преамбулу 391, корисне навантаження змінної довжини або кодові слова 392 і тимчасове вікно 393. Залежно від напрямку комунікації преамбула 391 містить або висхідну преамбулу, або спадну преамбулу. У випадку з висхідною преамбулою, преамбула 391 містить фізичний заголовок

PMD пристрою носія 398, MAC заголовок 399A і дані PDU 400A. У разі низхідної преамбули, преамбула 391 містить MPEG-заголовок 401, MAC-заголовок 399B і дані PDU 400B. Як дані PDU 400A у висхідній преамбулі, так і дані PDU 400B в низхідній преамбулі містять адресу призначення MAC (DA) 403B і адресу джерела MAC (SA) 403A. Вміст корисного навантаження змінної довжини 392 може включати коротке кодове слово 394 або довге кодове слово 397.

Коротке кодове слово 394 містить корисне навантаження 395A, що включає дані A і коригування помилок 396A, що містить FEC A. У разі довгого кодового слова 397 корисне навантаження ділиться на кілька блоків 395A, 395B і 395C з даними A, B і C відповідно, при тому кожне корисне навантаження містить власні блоки перевірки помилок 396A, 396B і 396C, включаючи відповідні дані FEC A, FEC B і FEC C, відповідно. Після перевірки помилок дані DOCSIS3 включають в себе блоки даних 395A, 395B і 395C в разі довгого кодового слова і тільки блок даних 395A у разі короткого кодового слова. Поєднання даних A, B і C об'єднуються в суміжну IP-датаграму, в даному прикладі IPv6 датаграма, що містить адресу джерела IP 445, IP адресу призначення 446 і поле даних 435 з корисним навантаженням SDNP 1430 і транспортний заголовок 436 з даними 4 рівня. Таким чином, DOCSIS3 гнучко передає дані по кабельній мережі, використовуючи протокол даних з пакетною комутацією.

Як показано на Рис. 65A, пакети даних передаються кількома каналами по гібридній кабельній волоконно-оптичній мережі, тобто на різних частотах. У DOCSIS 3.0 канали передачі даних коливаються від 5 МГц до 1002 МГц, включаючи аналогові телевізійні сигнали 1440 (трикутники), дані QAM 1441 і "диплексер" каналу управління 1443. На першому етапі DOCSIS3.1 діапазон частот розширюється до 1218 МГц, і додаються DOCSIS3.1 канали даних 1442 для полегшення модуляції OFDM, в основному в смузі частот вище існуючих каналів, призначених для QAM.

OFDM краще методів QAM, оскільки канали можуть бути більш щільно розташовані один над одним. Порівнюючи схеми модуляції, розподіл частот QAM 1445A має більш широкий розкид за спектральним змістом, ніж розподіл частот OFDM 1445B. Зокрема, ширина спектральної бічної смуги від f_0 до f_{-50}, тобто ширина від краю несучої до частоти, де сигнал падає на -50 дБ, становить 4,3 одиниці нормалізованої частоти при розподілі частоти QAM 1445A, а в разі розподілу частоти OFDM 1445B - тільки 0,4 одиниці нормалізованої частоти. Оскільки спектральна ширина менша, в один спектр може бути запаковано більше каналів зв'язку, що збільшує загальну смугу пропускання і максимальну загальну швидкість передачі даних у мережі. На другому етапі розгортання DOCSIS 3.1 діапазон частот розширено до 1794 МГц. Багато діапазонів, спочатку призначених для даних QAM 1441, замінюються новими каналами, призначеними спеціально для даних OFDM 1442.

У кабельній мережі з підтримкою DOCSIS один пристрій CMTS підтримує багато CM, що керують доступними каналами. Хоча CMTS може динамічно розподіляти вхідний зв'язок і вибір каналу, при необхідності, висхідний зв'язок вимагає вирішення конфліктів, щоб полегшити ситуацію, коли кілька CM намагаються відправити дані одночасно. Тому перед надсиланням даних кожен модем повинен запросити у CMTS канал висхідного зв'язку. Цей процес показано на Рис. 65B і включає послідовність операцій зв'язку між CMTS 101, що працює з додатком 1335L SDNP, і CM 103, що працює на прошивці SDNP 1335M. Маршрутизація IP-датаграм у багатофункціональній мережі використовує IP-адреси "IP CMTS" і "IP CM1" і кілька MAC-адрес, наприклад "MAC CM1" для CM 103 і "MAC CMTS1", ""MAC CMTS3" і "MAC CMTS4" для CMTS 101. На самому верхньому Рис. , що показує графік залежності частоти від часу, CM 103 надсилає запит на передачу сигналу RQST 1445A по виділеному каналу.

Після неотримання відповіді відправляється другий RQST 1445B, в результаті чого CMTS 101 надсилає відповідь по іншому каналу у вигляді пакета даних MAP 1446. Вміст пакета даних MAP 1446 вказує CM103, коли передавати дані і які канали зв'язку він може використовувати для свого висхідного зв'язку. Після отримання пакета даних 1446 MAP CM 103 відправляє свої вихідні дані одночасно по двох каналах у висхідних пакетах даних 1447A і 1447B. Розділення даних, що передаються одночасно двома каналами, як показано на малюнку в центрі, називається з'єднанням каналів. З'єднання каналів - це засіб, за допомогою якого можна збільшити пропускну здатність і швидкість передачі даних між CMTS і CM. Це також динамічний метод, який гарантує відсутність невикористаної доступної пропускної здатності. На зображенні внизу показані відповіді CMTS 101 по чотирьох каналах зв'язку, а саме 1448A, 1448B, 1448C і 1448D, з одночасною, але різною тривалістю передачі даних.

Як у висхідному, так і в низхідному зв'язку по гібридній волоконно-оптичній мережі, пропускна здатність динамічно розподіляється між кількома каналами, розділеними на невеликі часові сегменти, звані "мініслотами". Рис. 65C ілюструє зв'язок між CM 103 і CMTS 101 у висхідному потоці. Такі попередні повідомлення, як правило, включають повідомлення або

прохання про передачу. У цьому прикладі дані передаються за частотами f_1 і f_2, що складаються з п'яти тимчасових мініслотів. Як показано на зображенні, мініслоти 1, 2 і 3 передаються на частоті f_1 в інтервалах K, (K+1) і (K+2), а мініслоти 4 і 5 - на частоті f_2 в інтервалах K і (K+1), але не в інтервалі (K+2). Попередній пакет даних 1450A, представлений у скороченому вигляді, вказує IP-адресу джерела "IP CM1" і IP-адресу призначення з'єднання "Останньої Милі", тобто "IP $M_{0,0}$", вузол шлюзу мережі SDNP, розташований на сервері 1201A.

Для зв'язку "Останньої Лінії" пакет даних 1450A визначає "MAC CM1" в якості MAC-адреси джерела кабельного модема і PHY-середовище, в даному випадку канал на частоті f_1 в якості MAC-адреси призначення "MAC CMTS1". Пакет даних 1450A, що містить корисне навантаження SDNP A, займає в цілому три мініслоти, а саме 1, 2 і 3, хоча разом вони несуть один пакет даних і корисне навантаження. З іншого боку, мініслот-4 і мініслот-5 містять тільки по одному пакету даних, тобто 1450B і 1450C з відповідним корисним навантаженням даних SDNP B і корисним навантаженням даних SDNP C. Як і пакет даних1450A, обидва пакети 1450B та 1450C вказують IP адресу призначення хмари SDNP $M_{0,0}$.

Однак для MAC-адреси призначення, замість того щоб вказувати одну і ту ж MAC-адресу і фізичний носій, що і для першого пакета, обидва пакети 1450B і 1450C містять MAC-адресу призначення "MAC CMTS2". Цю адресу можна використовувати для зазначення, що пакети даних 1450B і 1450C повинні передаватися на частоті, відмінній від частоти пакета даних 1450A - в даному випадку на частоті f_2, а не на частоті f_1. Фактичні значення частот динамічно відображаються на карті CMTS 101 і конкретно не ідентифікуються. Таким чином, система DOCSIS3 являє собою багатофункціональне рішення, що дозволяє одному пристрою CMTS одночасно взаємодіяти з кабельним модемом або конвертером відеосигналу на декількох частотах і використовувати кілька протоколів, таких як 256 QAM або OFDM.

Замість того щоб дозволити CM і CMTS визначити, які пакети даних використовують загальний несучий канал або частоту, як це зазвичай буває в системах DOCSIS3, відповідно до описуваної безпечною динамічною мережею зв'язку і протоколом для зв'язку "Остання Миля", клієнт SDNP CM 103 вказує різні MAC-адреси призначення для забезпечення зв'язку на декількох частотах і каналах, тобто для примусового виконання операцій багаторівневого PHY-з'єднання. Оскільки пакети даних CM 103 1450A і 1450B/C передбачають різні MAC-адреси призначення, а саме MAC CMTS1 і MAC CMTS2 відповідно, пакети даних автоматично викликають багаторівневе PHY-з'єднання "Останньої Лінії". Як альтернативу, якщо CMTS дозволяє використовувати інші засоби для запиту унікального розподілу каналів, наприклад, за допомогою команди та запиту управління, використання MAC-адреси для виклику багаторівневого PHY-з'єднання може бути замінено альтернативними засобами.

Рис. 65D ілюструє послідовний потік даних від CMTS 101 до CM 103, зображуючи використання з'єднання каналів для досягнення високих швидкостей передачі даних у багатопоточному зв'язку. Як показано на Рис. , всі пакети даних вказують IP-адресу джерела "IP CMTS", IP-адресу призначення "IP CM1" і MAC-адресу призначення "MAC CM1". Багаторівневе PHY-з'єднання керується шляхом зазначення MAC-адреси джерела CMTS 101. Як показано на Рис. , пакет даних 1450G, що містить корисне навантаження SDNP G, вказує адресу джерела MAC "MAC CMTS6", відповідний зв'язку на частоті f_6, що несе дані в міні-слотах 15 і 16. Пакет даних 1450H містить корисне навантаження SDNP H і вказує адресу джерела MAC "MAC CMTS7", що відповідає зв'язку на частоті f_7, що передає дані в міні-слотах з 17 по 20. Пакет даних 1450I, що містить корисне навантаження SDNP I, визначає адресу джерела MAC "MAC CMTS8", відповідний зв'язку на частоті f_8, що передає дані в міні-слотах 21, 22 і 23. Нарешті, пакет даних 1450J, що містить корисне навантаження SDNP J, вказує адресу джерела MAC "MAC CMTS9", відповідний зв'язку на частоті f_9 з даними в міні-слотах 24 і 25. Таким чином, пов'язані та незв'язані пакети даних можуть бути одночасно відправлені з CMTS 101 в CM 103 за допомогою методів багаторівневого PHY-з'єднання без конфліктів каналів або колізій даних з відповідними висхідними даними.

Маршрутизація гіперзахищеного Call out - маршрутизація гіперзахищених викликів, здійснювана відповідно з захищеною динамічною мережею зв'язку і протоколом, може здійснюватися за допомогою одного з трьох методів управління і контролю.

- Триканальний зв'язок, за якого маршрутизація виклику або повідомлення керується за допомогою трьох наборів серверів, а саме медіасерверів SDNP для передачі аудіо, відео або файлів даних; сигнальних серверів SDNP для вибору маршрутизації виклику і сервера імен SDNP для зберігання динамічного відображення телефонних номерів за їх відповідними адресами SDNP,

- Двоканальний зв'язок, за якого керування маршрутизацією виклику або повідомлення використовує два набори серверів, а саме медіасервери SDNP для передачі аудіо, відео або

файлів даних; і сигнальні сервери SDNP для маршрутизації виклику і для виконання функції відображення телефонних номерів на відповідні адреси SDNP,

- Одноканальний зв'язок, при якому передача даних, планування маршруту і карта адрес SDNP виконуються одним набором серверів.

Загалом триканальний зв'язок забезпечує більшу захищеність від кібератак, оскільки жоден набір серверів не містить всієї інформації про виклик. У будь-якому випадку, мережа SDNP використовує розподілену обробку для обмеження інформації, що міститься на будь-якому сервері. Крім того, при передачі даних по одному, двом або трьом каналам зв'язку медіасервери SDNP з'єднуються з серверами четвертого типу - DMZ. Сервери DMZ використовуються для зберігання спільних секретів SDNP, необхідних для обробки корисного навантаження SDNP, включаючи шифрування, розділення, змішування, вставлення і видалення сміттєвих даних, а також шифрування. У процесі роботи вхідні пакети даних, отримані медіасервером, доставляються на DMZ сервер, де пакети даних модифікуються і передаються назад на медіасервер. Медіасервер не знає, як були змінені пакети даних або яка логіка або алгоритм були використані для обробки даних. Виконуваний код і таблиці, що зберігаються на сервері DMZ, зашифровані для запобігання аналізу коду. Крім того, DMZ-сервери працюють в автономному режимі без підключення до мережі або Інтернету.

Наступні графіки ілюструють приклад реалізації триканального обміну даними SDNP і послідовність, що використовується для ініціювання виклику або надсилання файлу по мережі. Робота двоканального зв'язку може розглядатися як незначна модифікація триканального зв'язку, при якій функції сервера імен SDNP об'єднуються в сигнальні сервери. Одноканальний зв'язок включає в себе інтеграцію всіх трьох операцій в мережу багатофункціональних серверів, що працюють як вузли зв'язку SDNP.

Хоча фрагментована передача даних всередині SDNP хмари зазвичай виконується з використанням динамічної сітчастої маршрутизації, зв'язок "Останньої Милі" пропонує менше варіантів маршрутизації, особливо там, де послідовні пакети даних можуть бути або (i) спрямовані на один шлюз SDNP, тобто як в одномаршрутному зв'язку "Останньої Милі" або (ii) спрямовані на кілька шлюзів SDNP, тобто як у багатомаршрутному зв'язку "Останньої Милі". Інші варіанти маршрутизації "Останньої Милі" включають динамічну адресацію джерел і багатоканальне з'єднання Останньої Лінії. Ці параметри доставки задаються в IP-пакетах даних, що генеруються сигнальними серверами. Незважаючи на те, що ці пакети даних SDNP вказують IP і MAC адреси джерела і призначення, точний шлях, по якому той чи інший пакет даних проходить Останню Милю, невідомий. Замість цього проміжний шлях визначається роботою маршрутизаторів, пристроїв, що належать операторам локальної мережі, операторам мобільного зв'язку і постачальникам мережевих послуг, які обслуговують "Останню Милю", а не сигнальними серверами SDNP. Таким чином, зв'язок "Останньої Милі" аналогічний скакалці, де два кінці зафіксовані, але їх з'єднує безліч унікальних доріжок.

Повторюючи для ясності, термін "одномаршрутний, багатомаршрутний і сітчастий зв'язок" відноситься до маршруту медіа-пакетів, тобто шлях "контент" проходить між абонентами, а терміни "триканальний, двоканальний і одноканальний зв'язок" відносяться до системи управління і контролю, що використовується для управління транспортом по мережі вузлів SDNP. З урахуванням вищевикладеного, наступний набір ілюстрацій показує послідовність кроків, тобто "процес", який використовується при здійсненні виклику або ініціюванні повідомлення відповідно до захищеної динамічною мережею зв'язку та протоколу.

Рис. 66 ілюструє абстрактне представлення одномаршрутної мережі Останньої Милі для триканального зв'язку, що включає клієнт SDNP 1600, IP маршрутизатори 1602A, 1602B і 1602C, сигнальний сервер 1603A, сервер імен SDNP 1604A і SDNP шлюз 1601. Ці комп'ютерні сервери містять вузли зв'язку SDNP, які використовуються для забезпечення мережевої взаємодії з мережевими іменами вузлів та IP-адресами, включаючи клієнт SDNP $C_{1,1}$, маршрутизатори R, сигнальний сервер SDNP вузол S, сервер імен SDNP Ns і шлюз SDNP вузол $M_{0,0}$. Мережеве з'єднання 1610 забезпечує Останню Ланку між клієнтом $C_{1,1}$ і найближчим маршрутизатором 1602A; мережеве з'єднання 1611 - між шлюзом SDNP $M_{0,0}$ і найближчим маршрутизатором 1602B; мережеве з'єднання 1612 - між шлюзом 1603A і найближчим маршрутизатором 1602C; і мережеве з'єднання 1616 - між топологічно розташованими маршрутизаторами 1602A і 1602C. Оскільки IP-адреси маршрутизаторів не використовуються в IP-датаграмах ні в якості джерела, ні в якості адреси призначення, ім'я "R" є загальним для всіх маршрутизаторів на рівні 3. У разі описів рівнів 1 і 2 кожен маршрутизатор має унікальну ідентичність, але цей аспект не має відношення до опису маршрутизації викликів на рівні 3 IP-мережі. Сигнальний сервер SDNP 1603A (вузол S) підключається до сервера імен 1604A (вузол NS) SDNP через мережеве з'єднання 1613 і до вузлів хмари $M_{0,n}$ SDNP через ряд мережевих з'єднань 1614. Сигнальний

сервер 1603A також підключається до інших сигнальних серверів (не показані) за мережевим з'єднанням 1615.

При використанні мережі SDNP для здійснення виклику, тобто встановлення "сесії", потрібна наступна послідовність кроків, ініційованих SDNP клієнтом, що здійснює виклик, тобто "викликаючим абонентом".

1. Запит на SDNP виклик (або call out).
2. Запит SDNP адреси.
3. Доставка SDNP адреси.
4. Інструкції SDNP маршрутизації.
5. Почати SDNP виклик SDNP (або call out).

Перший крок, "запит виклику" зображено на Рис. 67, де викликаючий абонент, клієнт 1600 з адресою "IP $C_{1,1}$", пов'язується з сигнальним сервером 1603A за адресою "IP S" за маршрутами 1610, 1616 і 1612 з IP-датаграмою 1620. Командне і кероване корисне навантаження датаграми 621 містить транспорт даних рівня 4 з використанням TCP для забезпечення точності даних і визначає ряд запитуваних параметрів виклику, включаючи доставку, терміновість, облікові дані безпеки і контактну інформацію викликаного абонента. У разі виклику іншого клієнта SDNP, тобто "виклику SDNP", ця контактна інформація включає конфіденційну ідентифікацію (CID) клієнта, який викликається, дані, наявні в телефонній книзі SDNP клієнта. У разі "виклику", дзвінка абоненту, який не є клієнтом SDNP, контактна інформація включає в себе номер телефону. Хоча ідентифікатор CID клієнта SDNP за своєю природою анонімний і відомий тільки серверу імен SDNP, номер телефону не маскується. Для захисту особистого життя викликаного абонента телефонний номер у блоці управління шифрується. Альтернативно можна зашифрувати все корисне навантаження системи управління 1621. Корисне навантаження 1621 може приймати вид шифрованого тексту, а IP-адреси IP-датаграми 1620 не можуть бути зашифровані, інакше маршрутизатори 1602A і 1602C не зможуть направити датаграму.

Другий крок, "Запит SDNP адреси", показаний на Рис. 68, де сигнальний сервер SDNP з адресою "IP S" зв'язується з сервером імен SDNP за адресою "IP NS" на шляху 1613 з IP-датаграмою 1622. Командне і кероване корисне навантаження датаграми визначає транспорт даних Рівня 4 як TCP і містить або CID, або зашифрований телефонний номер абонента, який викликається. У разі виклику за протоколом, SDNP сервер імен 1604A перетворює CID на SDNP адресу клієнта. У разі виклику сервер імен 1604A дешифрує і конвертує телефонний номер абонента на адресу SDNP шлюзу, розташованого найближче до абонента. Як показано на Рис. 69, сервер імен 1604A потім передає SDNP-адресу клієнта або шлюзу за IP-датаграмою 1623 від адреси джерела "IP NS" на сигнальний сервер 1603A за адресою "IP S".

Сигнальний сервер 1603A використовує SDNP-адреси абонента, який викликає абонент для маршрутизації виклику між ними або в якості гіперзахищеного з'єднання, якщо абонент, який викликається, є клієнтом SDNP, або в якості найближчого шлюзу SDNP, якщо викликаний абонент не є клієнтом SDNP. Процес, який використовується для підготовки інструкцій з маршрутизації та розповсюдження на всі медіа-вузли, необхідний для завершення з'єднання абонента, показаний на Рис. 70. Як показано на Рис. , запит абонента на доставку, що міститься в полях доставки і терміновості корисного навантаження 1621A, після звірки з даними облікового запису, використовується для вибору способу доставки датаграми, як показано в операції 1650. Методи доставки, що включають звичайну, VIP, гарантовану або спеціальну доставку, впливають на маршрутизацію пакетів або субпакетів (якщо пакети розділені або фрагментовані). Наприклад при VIP-доставці найшвидші маршрути використовуються для передачі даних, в той час як завантаження тих же маршрутів іншими клієнтами мінімізується. При гарантованій доставці дублюючі фрагменти пакетів даних відправляються по мережі, тобто з використанням надлишковості, щоб забезпечити своєчасну доставку найшвидших пакетів даних та ігнорувати пізні надходження. У поєднанні з адресними даними SDNP, отриманими від системи управління 1623A, операція 1651 відображає оптимальні маршрути від викликаючого абонента до адреси SDNP абонента, або до найближчого шлюзу, якщо абонент не є клієнтом SDNP. Дані запиту на терміновість, що містяться в документі 1621A, використовуються для вибору термінової операції 1652, включаючи порядок зменшення затримок розповсюдження - повільна доставка, нормальна доставка, пріоритетна доставка і термінова доставка.

Інформація про терміновий запит використовується для вибору маршрутизації і зон для субпакетної маршрутизації за операцією 1653. Ці параметри, поряд з будь-якими застосовними обліковими даними 1621B, об'єднуються для синтезу команд маршрутизації і пакетів управління через операцію 1660. Ці пакети керування та сертифікації доставляються на вузли зв'язку "Останньої Милі" з використанням транспорту рівня 4, зазначеного TCP, але містять інформацію про маршрутизацію, яка при доставці даних в режимі реального часу використовує

UDP як транспортний протокол рівня 4. Наприклад, маршрутизація "Останньої Милі", виконана відповідно до облікових даних зони U1, генерується як IP-датаграма 1625 з корисним навантаженням 1626 командного пункту, що використовується для маршрутизації даних з вузла клієнта $C_{1,1}$ на вузол шлюзу SDNP $M_{0,0}$. IP-датаграма 1625 доставляється клієнту SDNP за допомогою TCP передачі даних, але корисне навантаження 1626 "Маршрутизація" Останньої Милі "U1" містить дані, що використовуються для маршрутизації пакетів в режимі реального часу, що вимагає використання UDP в якості транспортного механізму рівня 4. Операція синтезу C&C пакетів SDNP 1660 також генерує безліч інших C&C повідомлень, що доставляються у вигляді пакетів даних TCP на вузли в межах хмари SDNP. Одним з прикладів пакету даних для хмарних команд є IP-датаграма 1627A, що містить корисне навантаження 1628A, що використовується для маршрутизації даних від SDNP $M_{0,0}$ до SDNP $M_{0,1}$. Як показано на Рис. 71, ці пакети інструкцій з маршрутизації SDNP розподіляються по медіа-вузлах, включаючи клієнтські вузли C1,1, по послідовних з'єднаннях 1612, 1616 і 1610 і шлюзу SDNP $M_{0,0}$ та інших вузлах в хмарі SDNP через з'єднання 1614.

Початок виклику показано на Рис. 72, де медіа SDNP датаграма 1630, що містить SDNP дані, наприклад, звук, відео, текст тощо, додається в IP-заголовок, що містить пакет даних 1626, і направляється від IP $C_{1,1}$ до IP $M_{0,0}$ від клієнта SDNP 1600 через мережеве з'єднання Останньої Лінії 1601 до маршрутизаторів 1602A і 1602B. Поля даних ідентифікаційної мітки, зони безпеки, преамбули і поля інформації SDNP разом складають корисне навантаження медіапакета SDNP, що міститься в медіа-датаграмі 1630 SDNP.

Маршрутизація вищезазначеного SDNP виклику, тобто гіперзахищеного виклику з шлюзу M0,0 SDNP на клієнт SDNP C7,1, що містить мобільний телефон 32 з встановленим додатком SDNP 1335A, показана на спрощеній мережевій схемі Рис. 73A. SDNP датаграма 1631A, що містить медіафайли корисного навантаження SDNP A і заголовок 1628A, маршрутизується між медіа-вузлами з адресами SDNP $M_{0,0}$ і $M_{0,1}$. Зверніть увагу, що SDNP шлюз 1601 має дві адреси - IP-адресу "IP $M_{0,0}$" для зв'язку на "Останній Милі" і SDNP-адресу "SDNP $M_{0,0}$" для зв'язку всередині SDNP хмари. Вміст кожної датаграми SDNP змінюється в міру проходження пакету через хмару SDNP таким чином, що вміст - звук, відео і текст, що містяться в медіафайлах SDNP, A, B і C - помітно відрізняється і може включати вміст з двадцяти різних розмов або повідомлень. Механізми маршрутизації даних і захисту пакетів всередині SDNP хмари розкриті у вищезгаданій заявці на патентування в США № 14/803,869 під назвою "Динамічна Захищена Комунікаційна Мережа і Протокол", яка описує, як вміст і шифрування пакетів даних, що анонімно рухаються через SDNP хмару, змінюється динамічно і постійно, об'єднуючись тільки на клієнтському пристрої.

Відповідно, датаграма 1631B SDNP, що містить медіаданні SDNP з корисним навантаженням B і заголовком 1628B, маршрутизується між медіа-вузлами з IP-адресами M0,4 і M0,f. Дані, що виходять з SDNP хмари через шлюз SDNP 1601B, перетворюються з датаграми SDNP в IP датаграму 1632. IP датаграма 1632 з заголовком 1628C і корисним навантаженням на носій SDNP використовує облікові дані безпеки для зони U2, яка являє собою зону, що включає в себе "Останню Милю". IP датаграма 1632 потім прямує по "Останній Милі" по дротовому або оптоволоконному каналу 24 на мережевий маршрутизатор 27, а потім по стільниковій мережі 25 і по стільниковій лінії 28 на стільниковий телефон 32. Оскільки мобільний телефон 32 є клієнтом SDNP, з'єднання по "Останній Милі" залишаються гіперзахищеними. У цьому спрощеному прикладі всі пакети даних, що виходять з хмари на "Останню Милю", направляються з одного шлюзу SDNP 1601B. Насправді, для маршрутизації даних "Останньої Милі" може використовуватися більше одного шлюзу SDNP.

"Остання Миля" зв'язку для "call out" показана на Рис. 73B. Хоча при маршрутизації через SDNP хмару використовуються ті ж датаграми SDNP 1631A і 1631B, що і при виклику клієнта SDNP, шлюз SDNP 1601B - це останній сервер з програмним забезпеченням SDNP. Зв'язок "Останньої Милі" у вихідному виклику використовує IP-датаграми з не-SDNP корисним навантаженням, тобто IP-датаграма 1635 маршрутизується від шлюзу IP $M_{0,0}$ до PSTN за IP-адресою IP $C_{7,9}$, передаючи звук у вигляді VoIP. Потім PSTN перетворює формат виклику VoIP на звичайний телефонний дзвінок з використанням номера телефону і аналогового звуку в звуковому пакеті 1636. У таких випадках зв'язок "Останньої Милі" не є гіперзахищеним з'єднанням.

У багатомаршрутному з'єднанні "Останньої Милі", показаному на Рис. 74, пакети команд і управління даними, поширювані сигнальним сервером 1603A SDNP, включають пакет команд і управління 1625X, що надсилається клієнту 1600 каналами 1612 і 1610, пакет управління 1627X, що надсилається на шлюз SDNP 1601X по лінії 1614X, і пакет управління 1627Y, що передається на шлюз SDNP по лінії даних 1614Y. Інші пакети даних (не показані)

відправляються каналами 1614X на інші сервери, на яких розміщені медіа-вузли. Контрольно-вимірювальний пакет 1625X відправляється з адреси "IP S" на адресу "IP $C_{1,1}$", що містить корисне навантаження контролера, що включає маршрутизацію Останньої Милі U1. Маршрутизація Останньої Милі U1 включає дві різні команди маршрутизації - від "IP $C_{1,1}$" до "IP $M_{0,0}$" з тегом 1 і преамбулою 1, і від "IP $C_{1,1}$" до "IP $M_{0,1}$" з тегом 2 і преамбулою 2. Як приклад можна навести пакети командно-розпорядчих даних, що відправляються на вузли зв'язку всередині SDNP хмари, в тому числі від "IP S" до " $M_{0,0}$", що містять інструкції SDNP Cloud Routing 1, і від "IP $M_{0,1}$", що містять SDNP Cloud Routing 2.

Групові SDNP виклики - маршрутизація медіа пакетів на "Останній Милі" з клієнта SDNP 1600 на кілька шлюзів SDNP, як показано на Рис. 75A, включає два пакети даних 1630X і 1630Y, що включають заголовки 1626X і 1626Y відповідно і медіа-дані SDNP X і SDNP Y. Заголовок 1626X з тегом 1 і преамбулою 1 передається з адреси "IP $C_{1,1}$" на адресу "IP $M_{0,0}$", а заголовок 1626Y з тегом 2 і преамбулою 2 – з адреси "IP $C_{1,1}$" на адресу "IP $M_{0,1}$".

Дані, що надходять у зворотному напрямку від SDNP хмари до клієнта з використанням багатоканального зв'язку, як показано на Рис. 75B, включають пакет даних 1630U, що містить заголовок 1626U, тег 8, преамбулу 8, дані SDNP U, адресу шлюзу SDNP джерела M0,0 та адресу призначення "IP $C_{0,0}$". Одночасно до складу даних також входить пакет даних 1630 B, що містить заголовок 1626 B, тег 9, преамбулу 9, дані SDNP V, адресу шлюзу SDNP джерела M0,1 та адресу призначення "IP $C_{0,0}$". Програма SDNP, запущена на клієнті SDNP 1600, потім об'єднує вхідні пакети даних SDNP Data U, SDNP Data V та інші пакети для відтворення тексту повідомлення або голосу (звуку).

Доставка C&C пакетів даних з інструкціями щодо маршрутизації може бути розширена для ініціювання тристоронніх або групових викликів, обміну груповими повідомленнями та інших мультиклієнтських комунікацій. У повідомленнях такої групи або "конференц-дзвінках" повідомлення клієнта відправляється кільком абонентам одночасно. Ця функція групи запускається абонентом, чий запит на груповий виклик спочатку визначає групу клієнтів, з якими необхідно зв'язатися, а потім сигнальний сервер, який інструктує необхідні медіа-вузли, як обробляти маршрутизацію пакетів даних, пов'язаних з певним груповим викликом. Приклад маршрутизації групових викликів наведено на Рис. 76, де сигнальний сервер 1603P передає інструкції з маршрутизації по каналу передачі даних 1614A на клієнт SDNP 1600A і 1614Z на численні медіасервери 1600Z в межах хмари SDNP.

Таким чином, пакет даних TCP 1627A з маршрутизацією Останньої Милі U1 передається з сигнального сервера 1603P за адресою "IP S1" на SDNP клієнт за адресою "IP $C_{1,1}$", щоб "налаштувати" груповий виклик з викликаючим абонентом. Пакети даних C&C, представлені типовим пакетом даних TCP 1627Z, одночасно розподіляються за SDNP хмарами для зони Z1 каналами зв'язку 1614Z від адреси сигнального сервера "IP S1" до різних адрес призначення "IP $M_{0,y}$ ", де "y" являє собою цілочисельну змінну. Інструкції з маршрутизації в хмарі SDNP встановлюють маршрутизацію пакетів від шлюзу викликаючого абонента через хмару SDNP до двох або більше шлюзів SDNP, розташованих поруч з викликаними клієнтами SDNP.

Як показано на прикладі, інші SDNP клієнти можуть перебувати в різних географічних регіонах і перебувати в межах окремих зон безпеки, наприклад, U7 і U9. У деяких випадках ці клієнти можуть бути досить далекими від сигнального сервера 1603P, щоб інший сигнальний сервер 1603Q можна було використовувати для планування пакетної маршрутизації для цих клієнтів SDNP. Сигнальний сервер 1603Q передає команди маршрутизації в зоні U9 клієнту SDNP 1600M по каналу передачі даних 1614M і клієнту SDNP 1600L по каналу передачі даних 1614L. Наприклад, C&C пакет даних 1625M передає команди маршрутизації Останньої Милі U9 від сигнального сервера на "IP S4" до клієнта SDNP 1600M за адресою "IP $C_{9,1}$". Інший C&C пакет (не показано) також надсилається клієнту SDNP за адресою "IP $C_{9,4}$". Пакет даних 1627H, що містить інструкції з маршрутизації "Останньої Милі" U7, передається по каналу 1614H від сигнального сервера 1603Q за протоколом "IP S4" на клієнт 1600H за адресою "IP $C_{7,1}$".

Сигнальні сервери 1603P і 1603Q на вузлах S1 і S4 також обмінюються інформацією у вигляді C&C пакетів даних по каналу 1613Z. Ця інформація використовується для визначення того, які частини маршрутизації повинен виконувати сигнальний сервер 1603P, а які - сигнальний сервер 1603Q, істотно поділяючи завдання маршрутизації на кілька сигнальних серверів. У наведеному прикладі вузол сигнального сервера S1 керує маршрутизацією "Останньої Милі" для зони U1 і для SDNP хмари, а сигнальний вузол S4 керує зв'язком "Останньої Милі" для зон U7 і U9.

Маршрутизація даних під час розмови або повідомлень показана на Рис. 77A, де голос, що передається SDNP даними 1 в пакеті даних 1630A, направляється заголовком 1626A від абонента з IP-адресою "IP $C_{1,1}$" до найближчого медіа-вузла шлюзу SDNP M0,0. Пакет даних

переупаковується для передачі в хмару SDNP і відправляється на шлюзи мультимедійних вузлів $M_{0,4}$ і $M_{0,8}$. Маршрутизація пакетів у межах хмари SDNP невідома жодному з учасників конференції, не має централізованого управління і динамічно змінюється залежно від умов мережі. У цьому прикладі всі пакети даних SDNP в межах хмари SDNP використовують фрагментований сітчастий транспорт даних з анонімною адресацією і динамічним шифруванням, а також динамічне шифрування, змішування, розділення, з додаванням і видаленням сміттєвих даних. У показаному прикладі хмарний механізм перенаправляє вхідні з'єднання вузла шлюзу SDNP $M_{0,0}$ на інші шлюзи, в даному випадку вузли шлюзу $M_{0,4}$ і $M_{0,8}$.

Пакет даних 1630H з голосом викликаючого абонента, тобто SDNP даними 1, виходить з вузла шлюзу $M_{0,4}$ і направляється за допомогою заголовка 1626H з медіа-вузла " IP $M_{0,4}$" на клієнт 1600H з " IP $C_{7,1}$" з використанням облікових даних системи безпеки U7. Заголовок 1626H було передано клієнту 1600A у складі пакета C&C даних 1627A до підготовки пакета медіаданих, як описано на Рис. 76. Таким чином, кожен медіа-пакет, що містить дані в режимі реального часу, може бути підготовлений без затримок, коли вміст готовий до передачі даних. У мережах реального часу високий рівень QoS залежить від своєчасної маршрутизації динамічних даних. В іншому випадку можуть виникнути неприпустимо тривалі затримки поширення.

Після маршрутизації через SDNP хмару, корисне навантаження даних SDNP-1 доставляється учасникам конференц-дзвінків зони U9, а саме SDNP-клієнтам 1600M і 1600L, від медіа-вузла шлюзу $M_{0,8}$ до клієнтських IP-адрес "IP $C_{9,1}$" і " IP $C_{9,4}$". Ці пакети даних "Останньої Милі" 1630M і 1630L містять заголовки 1626M і 1626L, що визначають ідентифікаційні теги пакетів tag8 і tag9, які використовуються для розпізнавання вмісту, пов'язаного з тією самою розмовою, преамбулу 9 інформації, що використовується для передачі вбудованих інструкцій SDNP, ключів, початкових значень тощо і поле даних "L4", що використовується для забезпечення транспортування рівня 4 як UDP. Хоча інструкції з маршрутизації даних, що передаються сигнальним сервером, використовують транспортний протокол TCP для забезпечення точності, вміст мультимедійних пакетів являє собою дані в реальному часі, тому вигідно використовувати протоколи UDP Layer 4 замість TCP.

Рис. 77B ілюструє ту ж саму розмову, де з'являється контент із зони U7 client 1600H, тобто коли починає говорити клієнт $C_{7,1}$. Для порівняння цих даних з голосовим контентом клієнта $C_{1,1}$, корисне навантаження ідентифікується у всіх пакетах даних як "SDNP дані 5". Крім унікального корисного навантаження, єдиною відмінністю від попередньої схеми є те, що IP-адреси джерела і призначення "Останньої Милі" для пакетів даних 1630H і 1630A змінюються. Зокрема, для користувача зони U7 SDNP IP-адреса джерела для пакета даних 1630H змінюється на IP $C_{7,1}$ і його призначення стає адресою шлюзу SDNP IP $M_{0,4}$. Для зони U1 IP-адреса абонента для пакета даних 1630A змінюється на IP $C_{1,1}$ і його адреса джерела стає адресою шлюзу SDNP IP $M_{0,0}$. Слід розуміти, що кілька учасників конференц-виклику можуть говорити одночасно і що пакети даних з клієнтського вузла SDNP $C_{1,1}$, які надсилаються іншим учасникам викликів, включаючи клієнтський вузол $C_{7,1}$, можуть відбуватися одночасно з клієнтським вузлом $C_{7,1}$, що відповідає на клієнтський вузол $C_{1,1}$.

На мережевому рівні 3 зв'язку "Останньої Милі" не відбувається колізій даних трафіку в протилежному напрямку. Однак на фізичному рівні і канальному рівні 1 і 2 зв'язок "Останньої Милі" може включати тимчасове мультиплексування, щоб уникнути суперечок з приводу одного і того ж каналу зв'язку. Однак таке посередництво відбувається так швидко, що зв'язок може здатися повнодуплексним без затримок у голосових пакетах. Зверніть увагу, що і на Рис. 77A, і на Рис. 77B напрямок потоку даних, що відображається для клієнтів зони U9, залишається незмінним, тобто потік даних відправляється від хмари до клієнта. На Рис. 77C, однак, починає говорити клієнтський вузол зони U9 $C_{9,1}$. У цьому випадку всі клієнтські вузли $C_{9,4}$, $C_{1,1}$ і $C_{7,1}$ стають одержувачами голосу, тобто голосових даних SDNP 6.

В альтернативному варіанті, показаному на Рис. 78, груповий виклик може включати в себе поєднання викликів SDNP клієнтам і викликів "call out" на звичайні номери телефонів. За аналогією з телефонною розмовою або повідомленнями, представленими на Рис. 77A, голос, що передається SDNP даними 1 в пакеті даних 1630A, направляється за заголовком 1626A від абонента з IP-адресою "IP $C_{1,1}$" до найближчого шлюзу SDNP, що містить медіа-вузол $M_{0,0}$. Пакет даних переупаковується для передачі в хмару SDNP і відправляється на шлюзи мультимедійних вузлів $M_{0,4}$ і $M_{0,8}$.

У наведеному прикладі хмарний механізм перенаправляє вхідні з'єднання вузла шлюзу SDNP M0,0 на інші шлюзи, в даному випадку вузли шлюзу SDNP $M_{0,4}$ і $M_{0,8}$. Пакет даних 1630H з голосом викликаючого абонента, тобто SDNP дані 1, виходить з вузла шлюзу $M_{0,4}$ і направляється за допомогою заголовка 1626H з медіа-вузла " IP $M_{0,4}$" на клієнт 1600H з " IP $C_{7,1}$" з використанням облікових даних системи безпеки зони U7. Корисне навантаження SDNP даних

1 також доставляється учасникам конференц-дзвінків через медіа-вузол шлюзу $M_{0,8}$. Зв'язок "Останньої Милі" з цим шлюзом SDNP складається з двох різних типів з'єднань, а саме гіперзахищеного з'єднання з SDNP-клієнтом 1600M і незахищеного "call out" з'єднання з PSTN 1, що включає звичайну телефонну систему без використання VoIP або пакетних протоколів. Пакет даних "Останньої Милі" 1630M доставлений в зону U9 SDNP клієнта за адресою "IP $C_{9,1}$ що містить заголовок з зазначенням ідентифікатора пакета" tag 9 ", використовуваного для розпізнавання вмісту, пов'язаного з тією ж розмовою, преамбулу 9 інформації, що використовується для передачі вбудованих інструкцій SDNP, ключів, початкових значень і поле "L4" для завдання транспорту рівня 4 в якості UDP.

Вузол шлюзу M0,8 також відправляє IP-пакет 1635 на PSTN 1 за адресою IP C7,9. Замість того, щоб нести корисне навантаження, що складається з даних SDNP 1, у цьому випадку корисне навантаження IP було перетворено на звуковий пакет VoIP, який може бути перехоплений при прослуховуванні пакетів. Телефонна комутаційна система PSTN 1 перетворює незахищений IP-пакет в аналогове телефонне POTS-з'єднання, показане POTS даними 1636, з подальшим аналоговим з'єднанням між телефоном 37 і PSTN 1. Оскільки це та будь-які інші з'єднання не є гіперзахищеними, вміст "Останньої Лінії" піддається ризику злому, прослуховування та інших методів спостереження. Якщо не реалізована деяка ієрархічна структура, що визначає права доступу клієнтів, безпека всього виклику буде поставлена під загрозу найслабшою ланкою, тобто кожен учасник групового виклику зможе все почути.

Про це свідчить таблиця на Рис. 79A, де в груповий виклик входять учасники на гіперзахищених клієнтських вузлах мережі SDNP $C_{1,1}$, $C_{7,1}$, $C_{9,1}$ і $C_{9,4}$, а також учасники телефонних викликів "Ph #1" і "Ph #2". Як показано на Рис. , клієнт SDNP $C_{1,1}$ є хостом групи, клієнти SDNP $C_{7,1}$, $C_{9,1}$ є учасниками, тобто можуть слухати і говорити, а клієнт SDNP SDNP $C_{9,4}$ - "слухачем", тобто можуть слухати дзвінок, але не можуть говорити або бути почуті учасниками. Учасник при виклику за номером телефону "Ph #1" також є учасником, здатним слухати і говорити, а уповноважений, який телефонує за номером "Ph #2", тільки як "слухач", який не має можливості говорити на груповому виклику. Хост групи призначає ці права, тобто авторизацію користувача, під час налаштування виклику.

Звертаючись до таблиці в колонці "звичайний дзвінок", зверніть увагу, що всі учасники групового дзвінка, тобто абоненти, допущені організатором, мають можливість прослуховувати дзвінок. Абоненти, які намагаються зламати виклик або не допущені хостом, не мають можливості підключитися до виклику, або навіть можливість визначити, що проходить виклик. Ті ж методи застосовні і до групових чатів, де учасники можуть читати і писати повідомлення, але тільки учасники можуть переглядати тільки коментарі, але не можуть вводити свій власний текст в чат.

Використовуючи автентифікацію і перевірку особистості для управління мережевим доступом, здійснюваним відповідно до цього розкриття, система SDNP пропонує функції конфіденційності, недоступні в звичайних групових чатах і конференц-дзвінках. Ця функція викликається вибором приватного режиму, наприклад, натисненням символом замку або іншою іконкою конфіденційності перед відправкою СМС або розмовою. У таких випадках зв'язок відправляється тільки автентифікованим клієнтам SDNP, а не клієнтам SDNP, які ще не підтвердили свою особу, або слухачам або учасникам на незахищених пристроях. Цей момент роз'яснюється у вищезгаданій таблиці, де в приватному дзвінку під колонкою "неавтентифікований клієнт SDNP" всі клієнти групових дзвінків відключають звук мікрофона і динаміка, а в колонці "Автентифікований клієнт SDNP" всі клієнти SDNP можуть слухати, учасники $C_{1,1}$, $C_{7,1}$ і $C_{9,1}$ можуть також говорити, але всі викликаючі пристрої мають свій власний мікрофон і динаміки, тоді як клієнт може тільки чути коментарі. Цей момент роз'яснюється у вищезгаданій таблиці, де в приватному дзвінку під колонкою "неавтентифікований клієнт SDNP" у всіх клієнтів групових дзвінків відключені мікрофон і динамік, тоді як в колонці "Автентифікований клієнт SDNP" всі клієнти SDNP можуть слухати, а учасники $C_{1,1}$, $C_{7,1}$ і $C_{9,1}$ також можуть говорити, але у всіх викликаючих пристроїв будуть відключені динаміки і мікрофон, щоб тільки авторизовані клієнти могли чути або коментувати в приватному режимі. Таким чином, груповий дзвінок з верифікованими клієнтами SDNP і з з'єднаннями невідомих абонентів можуть взаємно брати участь у публічній частині дзвінка, без можливості розголошення конфіденційної інформації викликаючим пристроям.

Неавтентифіковані абоненти вилучаються з приватних обговорень, якщо перед розмовою або відправкою повідомлення будь-який учасник SDNP натисне на іконку замка. Після конфіденційної розмови кнопка відпускається, і контакти знову підключаються. Під час відключення абонента, тобто коли він знаходиться в режимі очікування, система SDNP може

або відтворювати музику, мовчати, або відтворювати білий шум (наприклад, звуки океану або дощу).

Текстовими повідомленнями в груповому чаті також можна керувати подібним чином. У звичайному груповому чаті всі текстові повідомлення відправляються в програму SDNP на клієнтських пристроях SDNP і SMS всім учасникам чату. Текстові повідомлення можуть надсилатися лише учасниками. Текстові повідомлення, надіслані від "слухачів" або "тільки читаючих" учасників чату, ігноруються і не будуть пересилатися в чат-групу. Якщо перед надсиланням повідомлення учасник натискає на іконку замка, повідомлення буде надіслано тільки клієнтам SDNP, а не call out клієнтам. Для клієнтів SDNP, які отримують особисте повідомлення, якщо вони авторизовані, повідомлення буде видно для читання. Якщо вони не автентифікували свою особу, повідомлення буде приховано, закрито, або представлено іконкою, наприклад, замком, поки користувач не виконає автентифікацію для підтвердження своєї особи.

Комбінуючи автентифікацію особи з привілеями конфіденційності, регульованими мережевою авторизацією SDNP, злому пристрою буде недостатньо для відкриття тексту або прослуховування особистої розмови, навіть у групових чатах і групових викликах. Ця функція не може бути гарантована, якщо покладатися тільки на параметри безпеки пристрою - інформацію, яка може бути зламана локально. Системні параметри набагато складніше обдурити, оскільки підроблені облікові дані не будуть відповідати системним журналам і будуть відхилені як недійсні SDNP клієнти.

Додатковий ступінь конфіденційності також може бути доданий при виконанні групових дзвінків і групових чатів. Це унікальне втілення гіперзахищеного зв'язку "Останньої Милі", описане в таблиці на Рис. 79B, називається тут гіперприватний дзвінок або гіперприватний чат. Гіперконфіденційність вимагає, щоб абонент або повідомлення відповідало чотирьом критеріям:

- Всі одержувачі повідомлень у груповому виклику повинні бути клієнтами SDNP, а не call out пристроями.
- Дзвінок або текст слід вибрати як гіперприватне повідомлення, будь то дзвінок, текст, зображення тощо.
- Одержувач повідомлень щодо групового дзвінка або чату повинен засвідчити свою особу.
- Одержувач будь-якого гіперприватного повідомлення повинен бути попередньо обраний в якості "приватного" учасника або приватного слухача.

Хоча перші три критерії в основному ті ж, що і в попередньому прикладі для приватних абонентів в груповому виклику, четвертий критерій, вимога про те, щоб будь-який абонент, що має право приймати приватні дзвінки або текст, повинен завантажуватися в заздалегідь визначений список клієнтів в якості "приватного" клієнта SDNP, є унікальним і додатково обмежує доступ до важливої інформації. Наприклад, як показано в таблиці, клієнти учасника SDNP $C_{1,1}$ і $C_{7,1}$, а також клієнт слухача SDNP $C_{9,4}$ позначені як "приватні" учасники в груповому виклику. На відміну від цього клієнт SDNP $C_{9,4}$ позначений тільки як учасник, але не як приватний учасник. За визначенням, жоден учасник дзвінка або слухач не може бути зареєстрований як приватний абонент.

Як і в попередньому прикладі, під час звичайного дзвінка всі учасники, тобто клієнти SDNP $C_{1,1}$, $C_{7,1}$ і $C_{9,1}$ і call out учасник Ph1, можуть чути всі розмови і читати всі текстові повідомлення, а також говорити або надсилати повідомлення в будь-який час, а "слухачі", включаючи клієнтів $C_{9,3}$ і Ph №2, можуть чути всі розмови і бачити текст, але не можуть говорити або передавати повідомлення в групі. Однак при груповій розмові в режимі гіперприватної розмови вибір перемикача або іконки для зазначення гіперприватного повідомлення автоматично блокує не тільки всіх непідтверджених абонентів, але і відключає всіх, крім "приватних". Він також відключає всі call out з'єднання і всіх непідтверджених користувачів. Таким чином, в роботі, коли будь-який приватний учасник вибирає іконку конфіденційності, тільки приватні учасники (включаючи організатора групи) можуть бачити, читати, розмовляти або писати в групі. Мікрофони та динаміки всіх інших учасників вимкнені, а також не можуть приймати або відправляти тексти або прикріплювати до них файли. Зокрема, в гіперприватному режимі, після автентифікації, тільки клієнти $C_{1,1}$ і $C_{7,1}$ можуть як слухати і говорити, так і читати і відправляти текст, а приватний клієнт $C_{9,4}$ може тільки слухати розмову або читати текст групи.

Вищевказані можливості управління маршрутизацією "Останньої Милі" дозволяють керувати груповими викликами і груповими чатами різними способами. Наприклад, організатор групового виклику може визначити, хто може приєднатися до виклику або групи, хто може говорити і писати повідомлення, а хто може тільки слухати і читати. При стандартному закритому виклику вибір закритого режиму дозволяє всім клієнтам SDNP після автентифікації брати участь у спілкуванні з тими ж привілеями, що і при стандартному груповому спілкуванні. У

гіперприватному режимі тільки SDNP-клієнти, що визначаються як приватні учасники і приватні слухачі, можуть спілкуватися в гіперприватному режимі.

Вибір того, хто може бути кваліфікований як учасник або слухач гіперприватного спілкування, тобто хто ідентифікований як приватний учасник або слухач, а хто ні, може бути встановлений кількома способами. При разовій груповій гіперприватній комунікації організатор групи вирішує, хто є приватним абонентом, а хто ні. При "системному" груповому гіперприватному зв'язку SDNP оператор мережі SDNP заздалегідь визначає, хто є приватним абонентом, а хто ні. У заснованій на правилах групового гіперприватного зв'язку мережа SDNP визначила правила для визначення того, хто має право бути приватним абонентом, а хто ні. Ці правила можуть ґрунтуватися на списку співробітників компанії, наприклад, коли тільки віце-президент і вищестоящі особи можуть брати участь у приватних телефонних розмовах. У державних установах і службах безпеки критерії можуть встановлюватися по допуску до служби національної безпеки, номеру паспорта, номеру поліцейського бейджу і т. д. Методи зв'язку "Останньої Милі", підтримувані SDNP, описані тут, можуть підтримувати будь-який з цих прикладів або використовувати будь-які інші критерії для розділення населення на дві групи, тим самим створюючи ті, які мають доступ до гіперприватного спілкування, і ті, які не мають такого доступу.

Хоча ця концепція може бути поширена на більш ніж одну групу, критерії ієрархічного доступу, як правило, більшою мірою застосовні до професійних систем зв'язку, ніж до телефонного зв'язку. Тому застосування методів SDNP для професійних комунікацій в даному контексті далі розглядатися не буде.

Одна з проблем при групових дзвінках пов'язана з тим, що всі намагаються розмовляти в один і той же час. Накладання мови збиває з пантелику, її важко чути, а також може призвести до небажаних статичних розрядів. Цю проблему можна вирішити за допомогою функції "push-to-talk", що імітує рацію або CB радіо. У режимі PTT або push-to-talk говорити одночасно може тільки один учасник. Коли учасник бажає поговорити, натискання перемикача приглушує звук всіх інших мережевих мікрофонів, переводячи всіх інших учасників групового виклику в режим прослуховування. Як показано в таблиці на Рис. 80A, при регулярному PTT розмові при натисканні кнопки PTT, як показано в колонці Host PTT, вони мають пріоритет над груповим викликом і перевизначають всіх інших абонентів, навіть тих, хто натиснув кнопку розмови. Всі інші абоненти, включаючи телефонні з'єднання, автоматично відключають мікрофони і стають тільки слухачами. Якщо вузол не натискає кнопку PTT, як показано в стовпчику "Інший PTT", функція PTT буде передана будь-якому іншому учаснику SDNP в порядку живої черги. Вузли SDNP, призначені в якості слухачів і викликають пристроїв, таких як C9,4 і Ph1, можуть прослуховувати PTT-переговори, але їх мікрофони відключаються під час групового виклику.

Використовуючи можливість SDNP зв'язку Останньої Милі для ідентифікації абонентів, які авторизувалися в мережі, функція PTT може бути розширена до приватних функцій зв'язку. При виборі позначки конфіденційності всі непідтверджені абоненти видаляються з групового виклику, приглушаючи звук їх динаміків і мікрофонів. Викликові з'єднання за визначенням не можуть бути автентифіковані і тому вони також відключаються. Вимкнення звуку є двонаправленим, запобігаючи прослуховуванню розмови виключеними учасниками, а також відключаючи мікрофони виключених учасників. Для автентифікованих учасників операція передує звичайній PTT, коли хост має пріоритет у розмові, а будь-який автентифікований учасник може використовувати функцію PTT розмови в порядку живої черги.

Таблиця на Рис. 80B ілюструє концепцію приватного групового виклику, який може бути розширений до функції PTT. При нормальній роботі функція PTT ідентична описаному вище випадку. Але в гіперприватному режимі тільки автентифіковані особи, які раніше були визначені як приватні учасники або приватні слухачі, можуть брати участь у гіперприватних розмовах. Наприклад, у гіперприватному режимі клієнти SDNP $C_{9,1}$ і $C_{9,5}$ відрізані від розмови або прослуховування, оскільки раніше вони не були вказані як приватні учасники або слухачі. Аналогічним чином, всі підключені пристрої відключаються під час роботи в режимі гіперприватного доступу. Таким чином, доступ до різних абонентів у виклику PTT-групи можна чітко контролювати. Вимикання звуку - це процес виключення деяких учасників (наприклад, слухачів) з прийому пакетів даних, що несуть звук розмови, при цьому продовжуючи надавати пакети даних учасникам, які не відключені. У цьому методі пакети даних індивідуально відправляються всім учасникам нормальної розмови, і тільки в частину списку при відключенні звуку користувачем клієнта.

В альтернативному варіанті пакети даних відправляються в широкомовному режимі всім учасникам групового виклику, але з використанням різних методів шифрування. У разі звичайних конференц-дзвінків пакети даних відправляються всім користувачам з використанням

шифрування, де у всіх учасників є копія ключа дешифрування. У приватному режимі або в режимі вимикання звуку пакети даних, що передаються користувачам, використовують інше шифрування, при якому ключ дешифрування передається тільки обраним користувачам. Ті, у кого є ключ, можуть брати участь у розмові, а ті, у кого немає ключа, виключаються. Перевага використання широкомовного пакета полягає в тому, що він вимагає менше пропускної здатності для зв'язку "Останньої Милі", ніж для відправки окремих пакетів. В іншому варіанті на шлюз відправляється один пакет, а сигнальний сервер клонує пакет для розподілу всім учасникам в звичайному режимі виклику і вибору абонентів в приватному або беззвучному режимі.

Гіперзахищене сховище файлів - Хоча захищена динамічна комунікаційна мережа і протокол були винайдені і розроблені в якості гіперзахищеної комунікаційної системи для телефонії і передачі даних в режимі реального часу, механізми безпеки, властиві мережі і протоколу SDNP, роблять її ідеально підходящою для гіперзахищеного зберігання файлів і даних. Коротко, якщо гіперзахищений дзвінок включає анонімну фрагментарну пересилку зашифрованих даних від одного абонента до іншого, тобто наскрізне з'єднання від одного клієнта SDNP до іншого клієнта SDNP, то гіперзахищене сховище файлів і даних можна розглядати як комунікацію, яка зупиняється на півдорозі і безстроково зберігається в буфері до наступного виклику. Іншою назвою розподіленого гіперзахищеного файлового сховища є сховище дезагрегованих даних.

Спрощений опис полягає в тому, що сховище - це комунікація, яка зупиняється в середині процесу доставки пакету, і цей опис технічно більш точний, ніж може здатися на перший погляд. У наведеній вище заяві на патентування в США № 14/803,869 буферизація пакетів даних до виявлення інших пакетів була явно розкрита і описана. Незважаючи на те, що буферизація всередині вузлів хмари SDNP відбувається за мілісекунди, а не місяці, система SDNP має можливість очікувати або зберігати дані без втрати відновленої інформації для повернення початкового вмісту. Звичайно, у такій спрощеній реалізації відсутні деякі функції, необхідні для довгострокового керування файлами, такі як каталоги, меню, переробка файлів, оновлення облікових даних та інші подібні функції.

Приклад пересилання даних від клієнта до фрагментованої мережі зберігання даних представлений на Рис. 81. Як показано на Рис. , клієнт SDNP 1700A з IP-адресою IP $C_{1,1}$ передає серію пакетів даних через SDNP хмару на сервери зберігання файлів SDNP 1700H, 1700M і 1700L, з відповідними IP-адресами IP $F_{7,1}$, IP $F_{9,1}$ і IP $F_{9,4}$. У процесі роботи клієнтський вузол $C_{1,1}$ відправляє серію пакетів даних 1730X з відповідними заголовками 1726X з адреси IP $C_{1,1}$ на шлюз SDNP $M_{0,0}$. Пакети даних 1730X ілюструються пакетами даних 1730H, 1730L і 1730M з відповідними заголовками 1726H, 1726L і 1726M. Для забезпечення точності, транспорт рівень 4 використовує TCP, а не UDP. Пакети включають поштовий індекс SDNP Zip або інший ідентифікаційний тег X, який використовується для їх ідентифікації при маршрутизації, у разі пакетів даних 1730H, 1730L і 1730M, тег1, тег2 і тег3. Частина корисного навантаження кожного пакета містить унікальні дані, наприклад, у трикомпонентному фрагментованому файлі SDNP файлу 1, SDNP файлу 2 і SDNP файлу 3. Облікові дані безпеки "Останньої Милі" в зоні U1 використовуються з відповідною преамбулою 1.

Після того, як пакети даних надходять в SDNP хмару, вони направляються в різні місця призначення відповідно до їх ідентифікації та інструкцій сигнального сервера (не показані). Пакет даних 1730H з заголовком 1626H і тегом 1 з файлом SDNP 1 направляється на вузол шлюзу SDNP $M_{0,4}$. Вузол шлюзу SDNP $M_{0,4}$ потім направляє пакет 1730H на вузол сховища файлів F7,1, використовуючи облікові дані безпеки для зони U7. Між тим, пакет 1730L з ідентифікатором теґу 2 з файлом SDNP 2 незалежно маршрутизується на шлюз SDNP-вузла $M_{0,8}$. Вузол шлюзу SDNP $M_{0,8}$ потім направляє пакет 1730L на вузол сховища файлів $F_{9,4}$, використовуючи облікові дані безпеки для зони U9.

Майже одночасно пакет 1730M з ідентифікатором у вигляді теґу 3, що містить SDNP файл 3, також незалежно спрямовується на шлюз SDNP вузла $M_{0,8}$, не обов'язково використовуючи той самий сітчастий маршрут маршрутизації, що і пакет даних 1730L з ідентифікатором теґу 2. Вузол шлюзу SDNP $M_{0,8}$ також направляє пакет 1730M з тегом 3 на вузол зберігання файлів $F_{9,1}$, також використовуючи облікові дані безпеки для зони U9.

Таким чином, файл 1 SDNP передається на вузол зберігання файлів $F_{7,1}$ з використанням облікових даних безпеки для зони U7, а файли 2 і 3 SDNP передаються на вузли зберігання файлів $F_{9,4}$ $F_{9,1}$ відповідно з використанням облікових даних безпеки для зони 9. Хоча файли належать клієнтському вузлу $C_{1,1}$, клієнт не має доступу до облікових даних безпеки, які використовуються для шифрування та захисту вмісту файлів. Оскільки жоден вузол зберігання файлів не містить всіх даних, а клієнт, власник даних, не має доступу до облікових даних, що використовуються для зберігання, хакеру важко вкрасти їх вміст, оскільки (і) вони поділені на

непоєднувані і непридатні частини (ii) всі файли використовують різні облікові дані безпеки для шифрування і скремблювання даних в мережі SD (iii) вони зберігаються в різних місцях і на різних мережах "Останньої Милі" і (iv) неможливо визначити, що різні збережені дані надходять з одного і того ж вихідного файлу SDNP. Зони, що містять сервери зберігання файлів, також можна назвати зонами зберігання, що відрізняються від зони, в якій знаходиться власник файлу, тобто на протилежних сторонах SDNP хмари. За цим визначенням, зона U1 - це клієнтська зона SDNP, також звана зоною власника файлу, а зони U7 і U9 - зони зберігання.

Застосування SDNP протоколів мережевого зв'язку на файловому сховищі додатково ілюструється на Рис. 82A, що показує "операцію запису", загальні кроки, при яких клієнт SDNP і власник файлів записують дані на гіперзахищені сервери зберігання файлів. Як показано на зображенні, клієнт SDNP 1700A поділяє нерозібраний файл 1705 за допомогою дії розділення SDNP 1057 і функції парсингу 1052 для створення файлу або документа з декількох частин, як показано на прикладі файлу з трьох частин 1706A, 1706B і 1706C. Опціонально вміст файлу може бути зашифровано перед розділом. Ці три файли потім передаються мережею SDNP у вигляді незв'язаних даних або інформації. Кроки, пов'язані з маршрутизацією через SDNP-мережу до кінцевих пунктів призначення, використовують ті ж методи, що і описані вище для гіперзахищеного зв'язку "Останньої Милі" і маршрутизації в хмарі SDNP. Зокрема, пересилання даних при гіперзахищеному зв'язку "Останньої Милі" 1707 використовує облікові дані безпеки відповідно до Зони U1. Сітчаста гіперзахищена передача файлів 1708 в SDNP хмарі використовує облікові дані безпеки зони Z1. Хоча ці операції з гіперзахищеного пересилання даних представлені великими блоками, пакетний транспорт насправді відбувається через мережу маршрутизаторів, серверів і програмних комутаторів, як описано в цьому розділі, з використанням розподіленої системи, що не має майстер-ключа, центрального управління та доступу до пакетного вмісту.

У той час як маршрутизація зони U1 "Останньої Милі" може включати відправку пакетів даних через інфраструктуру з обмеженою кількістю варіантів маршрутизації, методи, описані для гіперзахищеного зв'язку "Останньою Милі", включаючи багатофункціональну маршрутизацію "Останньої Лінії", маршрутизацію послідовних пакетів на кілька шлюзів SDNP і використання динамічної адресації джерела, тобто зміну імені IP адреси клієнта, рівною мірою застосовні до операцій у гіперзахищеному сховищі файлів. Як тільки пакети даних досягають хмари SDNP, їх пересилання використовує анонімну сітчасту маршрутизацію з динамічно зашифрованими даними, що перешкоджає відстеженню вмісту файлу або навіть метаданих, пов'язаних з комунікацією. Зрештою, всі три пакети даних надходять на різні сервери зберігання файлів SDNP 1700H, 1700M і 1700L з відповідними іменами вузлів SDNP $F_{7,1}$, $F_{9,1}$ і $F_{9,4}$, розташовані в різних зонах безпеки. Після пересилання мережі розібраний файл 1 обробляється відповідно до операції безпеки файлів зони U7 1709A і зберігається на вузлі зберігання файлів SDNP $F_{7,1}$. Оброблені файли 2 і 3 аналізуються відповідно до операцій із забезпечення безпеки файлів зони U9 1709B і 1709C і зберігаються на вузлах файлового сховища SDNP $F_{9,1}$ і $F_{9,4}$. Таким чином, жоден файл не містить всіх даних, і жоден обліковий запис безпеки не може розблокувати всі файли компонентів для відтворення оригіналу.

Під час дії "читання" гіперзахищеного файлу, показаної на Рис. 82B, послідовність пересилання даних між серверами файлового сховища і SDNP-клієнтом, тобто власником файлу, змінюється на протилежну. Читання гіперзахищеного файлу означає скасування процесу, за допомогою якого файл був спочатку збережений в зворотному порядку, включаючи (i) ідентифікація оброблених файлів на кожному сервері зберігання, (ii) вилучення положень безпеки локального зберігання з кожного обробленого файлу (iii) перенесення кожного відновленого файлу назад на SDNP клієнт через хмару SDNP і гіперзахищений зв'язок "Останній Милі", (iv) збирання оброблених файлів з різних повідомлень і (v) злиття (нерозділення) і, за можливості, розбір файлів з використанням локальних облікових даних клієнта для відновлення початкового файлу.

Для подальшого опису гіперзахищеної операції "читання" файлу, відповідний вміст сервера зберігання 1700H, збережений у вузлі зберігання файлів $F_{7,1}$, обробляється за допомогою операцій 1709A Зони U7 щодо забезпечення безпеки файлів для відновлення обробленого файлу 1. Незалежно від парсингу файлів 2 або 3, парсований файл 1 передається назад на клієнтський вузол SDNP $C_{1,1}$ за допомогою хмари SDNP, показаного у спрощеній формі в гіперзахищеній операції передачі 1708, використовуючи облікові дані безпеки зони Z1, а потім зони U1 гіперзахищеного пересилання зв'язку "Останньої Милі" 1707. Паралельно з цим, відповідний вміст сервера зберігання файлів 1700M, збережений у вузлі зберігання файлів $F_{9,1}$, обробляється за допомогою операції із забезпечення безпеки файлу зони U9 1709B для відновлення розібраного файлу 2. Незалежно від парсингу файлів 1 або 3, парсований файл 2

передається назад на клієнтський вузол SDNP $C_{1,1}$ за допомогою хмари SDNP, показаного у спрощеній формі в гіперзахищеній операції пересилання 1708, використовуючи облікові дані безпеки зони Z1, а потім і зони U1 в гіперзахищеній операції пересилання зв'язку "Останньої Милі" 1707. Між тим, відповідний вміст сервера файлового сховища 1700L, збережений у вузлі файлового сховища $F_{9,4}$, обробляється за допомогою операцій із забезпечення безпеки файлів зони U9 1709C для відновлення розібраного файлу 3. Незалежно від парсингу файлів 1 або 2, парсований файл 3 передається назад на клієнтський вузол SDNP $C_{1,1}$ за допомогою хмари SDNP, показаного у спрощеній формі в гіперзахищеній операції передачі 1708, використовуючи облікові дані безпеки зони Z1, а потім і зони U1 в гіперзахищеній операції передачі зв'язку "Останньої Милі" 1707.

Незалежна пакетна маршрутизація трьох складових файлів під час операції читання показана на Рис. 83, де серверний вузол 1700H надсилає пакет даних 1731H з файлом SDNP 1 та ідентифікатором "тег 7" за допомогою TCP протоколу з адреси зберігання файлів IP $F_{7,1}$ на сервер шлюзу SDNP за адресою IP $M_{0,4}$. Пакет 1731H включає заголовок 1727H, що містить преамбулу 7 та іншу інформацію, яка в триканальному зв'язку була надана раніше в пакеті команд і управління, сигнальним сервером.

Між тим серверний вузол 1700L надсилає пакет даних 1731L з файлом SDNP 2 і ідентифікатором "тег 9", використовуючи TCP протокол з адреси зберігання файлів IP $F_{9,4}$ на сервер шлюзу SDNP за адресою IP $M_{0,8}$. Пакет 1731L включає заголовок 1727L, що містить преамбулу 9 та іншу інформацію, яка в триканальному з'єднанні була надана раніше сигнальним сервером в пакеті команд і управління. Незалежно і паралельно серверний вузол 1700M надсилає пакет даних 1731M з файлом SDNP 3 і ідентифікатором "тег 8" за допомогою TCP протоколу з адреси зберігання файлів IP $F_{9,1}$ на сервер шлюзу SDNP, також за адресою IP $M_{0,8}$.

Пакет 1731M включає в себе заголовок 1727M, містить преамбулу 9 та іншу інформацію, надану в триканальному зв'язку, раніше з використанням пакета команд і управління, наданого сигнальним сервером. Три пакети даних 1731H, 1731L і 1731M проходять через хмару SDNP, використовуючи облікові дані зони Z1, поки, нарешті, не вийдуть з шлюзу SDNP $M_{0,0}$, розміщеного на хмарному сервері 1701U SDNP, де пакети даних послідовно передаються послідовними пакетами даних 1731X, використовуючи відповідні заголовки зони 1727X і облікові дані зони U1 на клієнтський пристрій 1700A за адресою IP $C_{1,1}$.

Посилаючись на Рис. 82B, після того, як три розібраних файли 1, 2 і 3, а саме 1706A, 1706B і 1706C, будуть передані на клієнтський пристрій SDNP 1700A з незалежної маршрутизації, вони будуть об'єднані в один файл 1705 шляхом операції змішування 1061, після чого буде виконана операція дескремблювання (не показана) відповідно до повноважень безпеки зони U1.

Замість додавання додаткових операцій з файловим сервером для захисту зберігаються дані, операції 1709A, 1709B і 1709C фактично включають взаємодію гіперзахищеного зв'язку "Останньою Милі" між SDNP хмарою і відповідними серверами зберігання 1700H, 1700M і 1700L. В якості артефакту мережевого підключення третього рівня з використанням протоколу зв'язку SDNP, файлове сховище SDNP за своєю суттю є гіперзахищеним, і складається зі скрембльованих, фрагментованих, зашифрованих даних, що зберігаються на розподілених енергонезалежних дисках, включаючи використання методів маніпуляцій даними, таких як введення "сміттєвих" даних і непотрібних файлів. Крім описаних вище методів захисту даних, гіперзахищене сховище використовує анонімні імена файлів без будь-яких значущих метаданих, простежуваності до власника файлу, маршрутизації, за якою файл був доставлений, або ідентифікації будь-якого іншого сервера зберігання файлів з відсутніми компонентами з вихідного файлу.

Незважаючи на функціональну сумісність в мережі SDNP, фізичну реалізацію серверів зберігання даних, тобто їх впровадження фізичного першого рівня і транспортування другого фізичного рівня, протоколи можуть істотно відрізнятися без шкоди для функціональності зберігання, часу доступу або глобальної доступності. Рис. 84A ілюструє фізичну реалізацію серверів зберігання файлів SDNP, включаючи верхній рисунок шлюзу 1701B SDNP, підключеного до сервера зберігання файлів SDNP 1740A через маршрутизатор 27. Для підвищення продуктивності мережі і стійкості до атак рисунок посередині показує пряме з'єднання між шлюзом SDNP 1701B і сервером зберігання файлів SDNP 1740A з використанням оптоволоконного кабелю 91 без використання проміжних маршрутизаторів. Як показано в нижньому прикладі, сервер зберігання файлів може складатися з більшого обсягу пам'яті з контролером сервера 1740B і накопичувачів 1740C і 1740D. До дисків можуть відноситися будь-які носії інформації, включаючи жорсткий диск або енергонезалежну пам'ять на базі флеш-накопичувача. Для подальшого обмеження доступу шлюз SDNP і сервер зберігання файлів

SDNP можуть фізично розташовуватися в одному і тому ж місці і приміщенні з підключенням тільки оптоволоконного кабелю. Вони можуть навіть перебувати в одній кімнаті, наприклад, фізично замкненій у сховищі, з жорстко контрольованим контролем доступу і спостереженням за всіма, хто входить до приміщення.

Рис. 84B також показує, що певна частина фрагментованого файлу даних може зберігатися локально у власника файлу. Як показано на зображенні, стільниця власника файлу 36 може зберігати розподілений файл на декількох пристроях, включаючи (i) локальний сервер зберігання файлів 1740A з доступом через Wi-Fi роутер 1352, який підключений до вузла шлюзу SDNP $M_{0,0}$ на сервері 1701A, (ii) сервер зберігання файлів 1740B з доступом до вузла шлюзу SDNP $M_{0,4}$ і (iii) сервер зберігання файлів 1740C зі шлюзом $M_{0,8}$. Оскільки дані фрагментовані за розподіленими дисками 1740A, 1740B і 1740C, інші пристрої, включаючи ноутбук 35, планшет 33 і мобільний телефон 29, не мають доступу до збереженого файлу, навіть якщо локальний файловий сервер 1740A і робочий стіл власника файлу 36 будуть підключені до одного Wi-Fi 1352.

Процес зберігання кожної розібраної частини файлу унікальним чином на окремих серверах зберігання файлів, званий невибірковим гіперзахищеним відображенням файлів, показаний на Рис. 85A. Клієнтський пристрій 1700A, що включає клієнтський вузол SDNP $C_{1,1}$, зберігає оброблений файл 1706A виключно на сервері 1700H, оброблений файл 1706B виключно на сервері 1700M і оброблений файл 1706C виключно на сервері 1700L, що відповідає зіставленню файлів 1, 2 і 3 з вузлами $F_{7,1}$, $F_{9,1}$, і $F_{9,4}$, відповідно. Під час доставки файлів використовується гіперзахищений зв'язок "Останній Милі", що забезпечує пересилання даних та їх зберігання. Одним з недоліків неминучого відображення файлів є те, що втрата будь-якого з серверів зберігання файлів, як тимчасового, так і постійного, ставить під загрозу доступ до файлів і їх відновлення. У контексті цієї заяви терміни "стійкість" і "стійкий" використовуються для визначення гарантованого і своєчасного доступу до сховища даних, тобто впевненості в тому, що зберігаються дані не будуть втрачені або доступ до них буде ускладнений протягом тривалого часу. За цією ознакою, неминуче гіперзахищене відображення файлів демонструє погану стійкість, оскільки помилка однієї точки запобігає доступу до файлів. Слабка відмовність може бути подолана надлишковою системою, в якій одні й ті самі дані зберігаються на більш ніж одному сервері зберігання файлів.

Ще одним показником, що характеризує або оцінює стійкість системи зберігання даних, є показник, визначений тут як коефіцієнт надлишковості читання RRF (read redundancy factor), термін, що визначає кількість резервних систем, що забезпечують доступ до даних у разі недоступності основного сховища даних. У показаному прикладі для кожної унікальної частини даних є по одному розташуванню. Це призводить до нульового коефіцієнта надлишковості читання, математично RRF=0, що означає, що одноточкове з'єднання або збій файлового сервера може призвести до тимчасової або постійної втрати даних, оскільки файл не може бути прочитаний власником.

Альтернативне відображення файлів з коефіцієнтом надлишковості RRF=1 показано на Рис. 85B. У цьому прикладі розібраний файл 1 знаходиться на сервері зберігання файлів $F_{9,4}$ і $F_{7,1}$, розібраний файл 2 - на сервері зберігання файлів $F_{9,1}$ і $F_{7,1}$, а розібраний файл 3 - на сервері зберігання файлів $F_{9,4}$ і $F_{9,1}$. У такій реалізації, якщо сервер зберігання файлів $F_{9,1}$ став недоступним або пошкодженим, розібраний файл 3 все ще може бути доступний з сервера зберігання файлів $F_{9,4}$ і розібраний файл 2 все ще може бути доступний з сервера зберігання файлів $F_{7,1}$. Таким чином, будь-який збій одного вузла зберігання не завадить доступу на читання гіперзахищених файлів. Рис. 85C ілюструє відображення гіперзахищених файлів з RRF=2. Відображення файлових сховищ зберігає сервери 1700L, 1700M і 1700H, але додає другий набір серверів 1700J, 1700E і 1700F для реалізації серверів зберігання файлів $F_{8,2}$, $F_{4,4}$ і $F_{6,8}$ відповідно. Таким чином, сервер зберігання 1700J виконує функції резервного сервера 1700L, 1700E - функції резервного сервера 1700M, а 1700F - функції резервного сервера 1700H. Хоча наведені приклади включають файл, розібраний на 3 частини, зрозуміло, що при бажанні документ може бути розібраний на більшу кількість частин. Для забезпечення гіперзахищеного сховища оригінальний файл ніколи не повинен бути розібраний на менш ніж дві і, в ідеалі, не менше ніж три частини.

Щоб проілюструвати процес зберігання та читання надлишкових файлів за допомогою гіперзахищеного сховища файлів, корисно показати послідовність операцій обміну повідомленнями та функцій передачі файлів, накладених поверх мережі SDNP, яка використовується для забезпечення процесу зберігання. Мережа, показана на Рис. 86, наприклад, включає клієнтський пристрій 1700A, що реалізує клієнтський вузол $C_{1,1}$, маршрутизатор 1702G, сигнальний сервер 1715, що реалізує SDNP вузол S, сервер імен 1714,

що реалізує SDNP вузол NS, хмарні сервери 1701U, що реалізують SDNP вузли $M_{0,0}$, $M_{0,4}$ і $M_{0,8}$ і сервери файлового сховища SDNP 1700H, 1700F, і 1000F реалізують вузли зберігань файлів $F_{7,1}$, $F_{9,4}$ і $F_{9,1}$ відповідно.

На Рис. 87A клієнтський пристрій 1700A за адресою "IP $C_{1,1}$" виконує файл-запит на сигнальний сервер 1715 за адресою "IP S" за допомогою пакета даних 1710A, що включає корисне навантаження системи командування і управління 1711A, що містить опис розміру файлу і необхідного рівня безпеки та резервування. На Рис. 87B сигнальний сервер 1715 надсилає пакет даних 1710B на сервер 1714 із запитом IP або SDNP адрес вузлів $F_{7,1}$, $F_{9,4}$ і $F_{9,1}$ сервера зберігання файлів. Вибір вузлів файлового адресного сервера може бути вибраний випадково зі списку вузлів зберігання або географічно на основі одного вузла, доступного поруч з клієнтом або в регіонах, вільних від лих. Вибір може також базуватися на таких параметрах продуктивності, як невикористовуваний об'єм пам'яті вузла, час розповсюдження на вузол файлового сховища, ступінь надійності роботи вузла та інші подібні фактори. На Рис. 87C сервер імен 1714 надсилає на сигнальний сервер 1715 пакет даних 1710C, що містить IP або SDNP-адреси вузлів $F_{7,1}$, $F_{9,4}$ і $F_{9,1}$ сервери зберігання файлів. Сигнальний сервер 1715 обчислює "Останню Мілю" і сітчасту хмарну доставку оброблених файлів на сервери зберігання 1700H, 1700L і 1700M.

На Рис. 87D сигнальний сервер 1715 відправляє пакет даних 1710D на клієнтський пристрій 1700A, при цьому пакет маршрутизується з адреси "IP S" на "IP $C_{1,1}$" через маршрутизатор 1702G. Пакет даних 1711D містить корисне навантаження системи командування і управління 1711D, що містить маршрутизацію "Останньої Милі" для майбутньої передачі файлів у зоні U1, клієнтській зоні, а саме маршрутизацію декількох пакетів з адреси "IP $C_{1,1}$" на шлюз SDNP за "IP $M_{0,0}$" з тегом 1, тегом 2 і тегом 3 ідентифікації кожного пакета (позначені як "тег X" для зручності). Одночасно сигнальний сервер 1715 також відправляє пакет даних 1710E на шлюз SDNP 1701U, пакет передається з адреси "IP S" на "IP $M_{0,0}$". Пакет включає корисне навантаження системи командування і управління 1711E, що показує маршрутизацію SDNP хмари з використанням облікових даних зони Z1 для пакету з ідентифікаційним тегом X, в даному випадку від адреси шлюзу SDNP "SDNP $M_{0,0}$" до наступного вузла в хмарі, наприклад, за адресою "SDNP $M_{0,5}$" (не показано). Згідно з Динамічною Захищеною Комунікаційною Мережею і Протоколом, маршрутизація пакетів даних через хмару SDNP з використанням анонімної фрагментарної передачі динамічно вибирається залежно від поточного стану мережі в реальному часі. Зокрема, маршрутизація в межах SDNP хмари пакетів даних реального часу, що надходять на будь-який шлюз SDNP, залежить від затримок розповсюдження пакетів даних між вузлами в межах SDNP хмари і терміновості кожного пакета даних в режимі реального часу, призначеного сигнальними серверами.

На Рис. 87E сигнальний сервер 1715 відправляє пакети командних даних на вузли "Останньої Милі", які розташовані на боці сховища, тобто в зонах U7 і U9. Як показано на Рис. , пакет даних 1710F передається на шлюз SDNP $M_{0,4}$, пакет передається з адреси "IP S" на адресу "IP $M_{0,4}$", що містить корисне навантаження 1711F, повідомляючи, що пакет даних з тегом 1 повинен бути передбачений вузлом шлюзу $M_{0,4}$ і, при отриманні, направлений на адресу "Останньої Милі" "IP $F_{7,1}$". Другий пакет даних 1710G передається від сигнального сервера 1715 на сервер зберігання файлів 1700H за адресою "IP $F_{7,1}$". Корисне навантаження командного центру для зберігання в зоні U7 визначає вхідний пакет з ідентифікаційним тегом 1 з адреси джерела "IP $M_{0,4}$", але оскільки функція вузла - зберігання, а не зв'язок, поле призначення залишається порожнім, тобто заповненим нульовим значенням. Як тільки пакунки даних системи командування і управління будуть розподілені по мережі, можлива подальша відправка файлів.

Рис. 88 ілюструє транспорт фрагментарних даних під час гіперзахищеного зберігання файлу, коли клієнтський пристрій 1700A відправляє серію пакетів даних 1712X з файлами даних SDNP 1, 2 і 3 з адреси "IP $C_{1,1}$" на шлюз SDNP за адресою "IP M0,0" за допомогою протоколу TCP. Кожен пакет даних має унікальний ідентифікатор, а саме тег 1, тег 2 і тег 3. Потім ці файли передаються через хмару SDNP на інші шлюзи, а саме вузли шлюзу SDNP $M_{0,4}$ і $M_{0,8}$. Пакет, що містить SDNP-дані 1, що надходять на шлюз $M_{0,4}$, передається в пакеті даних 1712A з адреси "IP $M_{0,4}$" на "IP $F_{7,1}$" за TCP з обліковими даними зони U7, а пакети даних 2 і даних 3, що надходять на шлюз $M_{0,8}$, з обліковими даними зони U9 в пакетах даних 1712B і 1712C з адрес "IP $M_{0,8}$" на адресу "IP $F_{9,4}$" і "IP $F_{9,1}$" відповідно. Сховище також може включати локальне шифрування на файловому сервері для запобігання скануванню даних на диску. Цей процес шифрування є локальним і не пов'язаний із забезпеченням безпеки SDNP. Пакунки SDNP 1, SDNP 2 і SDNP 3 містять фактичні фрагментовані файли, що знаходяться на зберіганні.

Преамбула в кожному пакеті даних, наприклад преамбула 1 в пакеті даних 1712A, може також містити ключ шифрування, що поставляється клієнтом в рамках симетричного шифрування. За допомогою симетричного ключа шифрування клієнтський вузол SDNP $C_{1,1}$ створює розділений ключ, один для шифрування і його доповнення для дешифрування. Потім симетричний ключ шифрування поставляється на вузол сервера зберігання файлів $F_{7,1}$, який постачається пакетом даних 1712A в даному прикладі. У майбутньому, коли клієнт запитує читання або доступ до вмісту збереженого файлу, вузол сервера зберігання файлів $F_{7,1}$ шифрує запитуваний файл за допомогою цього ключа шифрування перед відправкою файла назад клієнту. Оскільки тільки клієнт володіє відповідним ключем дешифрування, тільки клієнт може відкрити файл для читання. Хоча цей метод забезпечує додатковий рівень захисту, його недоліком є те, що тільки один клієнт може отримати доступ до файлу для читання, запобігаючи можливості декількох власників файлу, необхідних для забезпечення надлишкового доступу в разі крадіжки, пошкодження або втрати оригінального клієнтського пристрою.

Приблизно під час процесу передачі та зберігання даних сигнальний сервер 1715 також надсилає на сервери 1700H, 1700L і 1700M інструкції щодо маршрутизації "посилання відповіді". Посилання відповіді - це пакет даних і корисне навантаження системи управління, що підтверджує клієнту, що операція запису пройшла успішно і зберігання кожного розібраного файлу завершено. Ці повідомлення надсилаються власнику файлу-клієнта незалежно від кожного сервера файлового сховища, що бере участь у зберіганні переданих розібраних файлів. Файлові сервери надсилають клієнту свої відповіді з підтвердженням запису незалежно один від одного і без відома, а відповіді з підтвердженням запису передаються з використанням незалежних облікових даних безпеки, включаючи унікальні стани, відмінні від станів, що діяли на момент запису. Маршрутизація цих повідомлень не обов'язково використовує зворотний напрямок того ж шляху маршрутизації, що і для передачі файлів. Така відповідь потенційно може бути використана кіберзлочинцями для відстеження власника файлу. Замість цього у посиланні відповіді використовується ідентифікатор пакета, щоб повідомити клієнта про те, що збережені файли є частиною одного і того ж файлу і зберігаються як частина однієї і тієї ж фрагментарної операції запису.

У процесі роботи сигнальний сервер надсилає маршрутизацію повідомлень на посилання відповіді до серверів файлового сховища, власнику клієнта і на всі проміжні вузли SDNP, що беруть участь у маршрутизації відповіді. Сигнальний сервер 1715 координує маршрутизацію повідомлень відповіді, і як показано на Рис. 89A, використовує пакети даних, що містять корисне навантаження систем команд і управління, наприклад, сервер зберігання файлів 1700H отримує пакет даних 1721G, що містить корисне навантаження систем команд і управління 1722G, що містить дані заголовка для маршрутизації "відповіді посилання 1" з адреси IP $F_{7,1}$ на адресу IP $M_{0,4}$. Вузол шлюзу SDNP $M_{0,4}$ отримує пакет даних 1712F, що містить корисне навантаження 1722F, що описує маршрутизацію пакета даних тегу 1 з адреси "SDNP $M_{0,4}$" на інший вузол всередині SDNP хмари (не показано), в даному випадку за адресою "SDNP $M_{0,4}$". Аналогічно, сигнальний сервер 1715 надсилає серверу сховища 1700M пакет даних 1721M, що містить тег "відповідь посилання 3" теґу 3 пакета з інструкціями маршрутизації "Останньої Милі" з адреси "IP $F_{9,1}$" на адресу "IP $M_{0,8}$". Хоча маршрутизація файлових пакетів даних з боку сховища "Останньої Милі" і відповідних їм відповідних повідомлень каналу зв'язку може бути ідентичною або схожою, маршрутизація відповідних повідомлень через хмару SDNP, швидше за все, відрізняється через динамічну природу хмари SDNP.

Фактична маршрутизація повідомлення посилання на відповідь з серверів файлового сховища, які приймають участь, вказана на Рис. 89B. Як показано на Рис. , сервер зберігання даних 1700H відповідає пакетом даних 1720A, ідентифікованим тегом 1 і таким, що несуть корисне навантаження "FS посилання 1". Пакет маршрутизується з адреси "IP $F_{7,1}$" на шлюз SDNP за адресою "IP $M_{0,4}$" з використанням облікових даних зони U7. Зі шлюзу SDNP пакет даних теґу 1 направляється через хмару SDNP на шлюз клієнтської сторони за адресою "SDNP $M_{0,0}$", де адреса конвертується в пакет даних "Останньої Милі" 1720X і направляється з адреси "IP $M_{0,0}$" на адресу "IP $C_{1,1}$" за допомогою TCP і облікових даних безпеки зони U1 і містить дані теґу 1, а саме преамбули 1 і FS посилання 1.

Подібним чином, сервер зберігання даних 1700L відповідає пакетом даних 1720B, ідентифікованим тегом 2 і несучим корисне навантаження "FS посилання 2". Пакет маршрутизується з адреси "IP $F_{9,4}$" на шлюз SDNP за адресою "IP $M_{0,8}$" з використанням облікових даних зони U9. З шлюзу SDNP ідентифікований пакет даних теґу 2 направляється через хмару SDNP (маршрутизація не показана) на шлюз клієнтської сторони за адресою "SDNP $M_{0,0}$", де адреса конвертується в пакет даних "Останньої Милі" 1720X і направляється з

адреси "IP $M_{0,0}$" на адресу "IP $C_{1,1}$" за допомогою TCP за обліковими даними зони U1, а саме: преамбули 2 і теги 2, для передачі даних.

Третя частина розібраного файлу, ідентифікована тегом 3 і несе корисне навантаження "FS посилання 3", відправляється з файлового сервера зберігання 1700M через пакет даних 1720C. Пакет теґу 3 маршрутизується з адреси "IP $F_{9,1}$" на шлюз SDNP за адресою "IP $M_{0,8}$" з використанням облікових даних зони U9. З шлюзу SDNP ідентифікований пакет даних теґу 3 надсилається через хмару SDNP на шлюз клієнтської сторони за адресою "SDNP $M_{0,0}$", де адреса конвертується в пакет даних "Останньої Милі" 1720X і направляється з адреси "IP $M_{0,0}$" на адресу "IP $C_{1,1}$" за допомогою TCP з використанням облікових даних зони U1 і містить дані теґу 3, а саме: преамбулу 3 і FS-з'єднання 3.

Рис. 89C ілюструє приклад вмісту пакета даних каналу FS 1720A, направленого з сервера зберігання даних 1700H назад клієнту і власнику файлу. Як показано на Рис. , пакет даних включає маршрутизацію "Останньої Милі" з адреси "IP $F_{7,1}$" на шлюз SDNP за адресою "IP $M_{0,4}$" за допомогою TCP в пакеті з ID тегом 1, створеному в безпечній зоні U7. У преамбулі відповіді 1719A міститься опис корисного навантаження 1741A, а також додаткові облікові дані безпеки, що використовуються для виконання або підвищення безпеки пакета даних 1720A, який передається клієнту, для каналу FS. Однак у триканальній комунікації облікові дані безпеки відповіді, що містяться в преамбулі відповіді 1719A, як правило, не потрібні і не пов'язані з даними, що використовуються клієнтом для подальшого доступу і відкриття гіперзахищених файлів. Посвідчення доступу, необхідні для створення посилання від клієнта на файл, що зберігається на вузлі файлового сховища F7,1, містяться в полі даних 1741A, в тому числі:

- Унікальний мережевий тег, адреса SDNP або псевдо-адреса, необхідна для ідентифікації сервера зберігання файлів, на якому зберігається ця частина фрагментованого файлу.
- Опис зони, що визначає облікові дані безпеки, що використовуються для шифрування файлу в зоні безпеки на боці сховища (не в клієнтській зоні).
- Початкове значення 1, яке може містити числовий матеріал, або час, або стан 920 під час шифрування файлу перед його збереженням.
- Початкове значення 2, яке може містити числове значення 929, що використовується для шифрування файлів в рамках операції збереження.
- Ключ 1, що містить ключ дешифрування 1030 для дешифрування шифрування на "стороні зберігання" зони U7. Цей ключ може використовуватися в поєднанні з загальними секретами, що зберігаються на сервері DMZ, що працює як частина сервера зберігання файлів, або може бути ключем часткового дешифрування, який може використовуватися тільки в поєднанні з іншими обліковими даними безпеки, такими як числовий ключ.
- Ключ 2, що містить ключ шифрування 1022, надісланий клієнту і використовується для надсилання безпечних інструкцій від клієнта на сервер зберігання файлів з використанням симетричного ключа шифрування.
- Назва файлу або інша інформація, яка використовується для того, щоб допомогти клієнтові ідентифікувати збережений файл, не показуючи, як він зберігається.

Наведений вище пакет даних використовується в ілюстративних цілях і не повинен розглядатися як щось, що обмежує вміст пакету даних точними елементами або форматом, як показано в прикладі. FS посилання 1720X, отримані клієнтським вузлом SDNP $C_{1,1}$ після того, як вони отримані від серверів зберігання файлів, що беруть участь у зберіганні фрагментованого файлу, потім обробляються для створення файлового з'єднання для пристрою клієнта.

Як показано на Рис. 89D, ця операція об'єднує посилання FS 1741A, 1741B і 1741C за допомогою операції змішування 1753 для створення сукупного FS "посилання читання файлового сховища" 1754. Посилання на файлове сховище 1754 розміщене в клієнтському гіперзахищеному текстовому месенджері чи системі управління файлами, що надає можливість викликати гіперзахищений файл одним натисканням кнопки. Гіперзахищені операції невидимі для користувача. Власника файлу не повинен турбувати той факт, що файл насправді фрагментований, закодований і зберігається в розподіленій системі зберігання файлів. Виклик файлу відбувається так, ніби файл розташований локально. Тому FS посилання є ключовим елементом для доступу до будь-якого файлу, що зберігається в розподіленій файловій системі зберігання.

Спрощений перегляд FS посилання показано на Рис. 90A, де всі три сервери зберігання файлів надсилають свої відповідні FS посилання на клієнтський вузол $C_{1,1}$ і відповідний клієнтський пристрій 1700A, а саме сервер зберігання файлів 1700H відправляє FS посилання 1, сервер зберігання файлів 1700M відправляє FS посилання 2, а сервер зберігання файлів 1700L відправляє FS посилання 3. У клієнтському пристрої 1700A програмне забезпечення програми SDNP на клієнтському вузлі $C_{1,1}$ об'єднує три вхідні FS-посилання 1, 2 і 3 для

формування посилання на збережений файл. Це комбіноване посилання відображається в SDNP-месенджері як підтвердження наявності файлового сховища. При керуванні невибірковими файлами інформація про FS-посилання відправляється тільки на клієнтський пристрій. Для керування власними файлами посилання можна назвати або в момент запиту на файлове сховище, або після отримання повідомлення з підтвердженням.

Оскільки посилання на файлове сховище надсилається клієнту безпосередньо з серверів зберігання файлів, а не через сигнальний сервер, доступ до файлу має тільки клієнт з посиланням. Це FS посилання є необхідним для виклику та читання фрагментованого файлу. Без посилання збережений файл і його вміст буде втрачено назавжди і стане безповоротно безповоротним. Щоб знизити ризик втрати FS посилання, альтернативний підхід надсилає FS посилання на два клієнтські пристрої - клієнтський пристрій і додатковий пристрій.

Додатковий пристрій може бути другим пристроєм, що належить клієнту, або, в ділових випадках, другим пристроєм, що належить компанії. Альтернативно, другий пристрій може складатися з іншого сервера з власним логіном безпеки і перевіркою особи користувача.

Надлишковий доступ через посилання до фрагментованих розподілених файлів, створених відповідно до цього винаходу, може застосовуватися як до надлишкових систем зберігання файлів, тобто RRF 1, так і до не надлишкових. Використання надлишкового посилання в системі розподіленої гіперзахищеної пам'яті без надлишковості читання (RRF=0) показано на Рис. 90B. У таких системах, відображення файлів між розібраними файлами 1706A, 1706B і 1706C та відповідними серверами зберігання даних 1700H, 1700M і 1700L не є надлишковим. Як показано на Рис. , FS посилання 1, 2 і 3 відправляються на два клієнтські пристрої, а саме: 1700A хостинг SDNP клієнтського вузла $C_{1,1}$ і додатковий клієнтський пристрій 1700B хостинг резервного клієнта $C_{2,1}$. У разі втрати або недоступності з будь-якої причини одного з FS-посилань, для відновлення файлів можна використовувати FS-посилання на клієнті резервного копіювання. У зв'язку з цим розподілена система зберігання SDNP описує реалізацію невибіркового читання з резервуванням по одному каналу, тобто RRF=0 і LRF=1.

Приклад гіперзахищеної пам'яті з резервуванням посилань показано на Рис. 90C, де розібрані файли 1, 2 і 3 співставленні з двома серверами зберігання файлів, тобто для реалізації коефіцієнта надлишковості RRF=1, при цьому кожне FS посилання відправляється на два клієнти для досягнення коефіцієнта надлишковості каналу LRF=1. Несприйнятливість системи зберігання до збоїв читання і з'єднання означає, що систему можна розглядати як істинно резервовану систему управління гіперзахищеними файлами із загальним коефіцієнтом надлишковості SRF=1. Ми визначаємо фактор надлишковості сховища SRF, рівний найменшим значенням RRF і LRF. Наприклад, якщо RRF=0 і LRF=1, SRF=0, якщо RRF=3 і LRF=2, то загальна надлишковість сховища - SRF=2. Для реалізації загальної системи SRF=3 кожен файл повинен зберігатися на чотирьох окремих серверах зберігання файлів (як показано раніше на Рис. 85C) і FS посилання слід надіслати на чотири окремі клієнти.

Таким чином, загальний коефіцієнт надлишковості сховища SRF є прямим заходом стійкості розподіленої системи зберігання від збоїв. Цей принцип узагальнено на Рис. 91, де абсцис описує кількість файлових серверів зберігання, які використовуються в системі зберігання даних, а ордината описує кількість FS посилань, що відправляються окремим клієнтам. Як показано на зображенні, один сервер зберігання файлів не має надлишковості, тобто RRF=0. Збільшення кількості пристроїв зберігання файлів покращує надлишковість читання, але не впливає на надлишковість посилань. Навпаки, відправлення посилання на одного клієнта не забезпечує надлишковості каналу, тобто LRF=0 незалежно від кількості доступних серверів зберігання файлів. У будь-якому випадку, тобто для одного сервера зберігання або одного клієнтського з'єднання, загальний коефіцієнт надлишковості SRF=0, що означає відсутність стійкості файлової системи зберігання, як показано графічно в області L-подібної форми.

Як показано на Рис. , зберігання трикомпонентного парсованого файлу на 3-х серверах зберігання призводить до надлишковості читання RRF=1. Якщо принаймні два клієнти отримують FS-посилання, досягається резервування посилання LRF 1. Поєднання LRF=1, або RRF=1 дає L-подібну область 1724B, де SRF=1, тобто забезпечує деяку ступінь стійкості системи. Зауважте, що навіть при використанні 6 серверів, якщо FS посилання надсилаються лише двом клієнтам, система все одно демонструє лише обмежений ступінь стійкості, тобто SRF=1.

Посилаючи FS посилання на 3 клієнта і зберігаючи надлишковість даних на 6 серверах зберігання, регіон 1724C визначає умови, при яких SRF=2 забезпечує досить високу ступінь стійкості системи зберігання. Регіон 1724D ілюструє подальше підвищення стійкості, коли SRF=3 з використанням шести серверів зберігання файлів і чотирьох клієнтів, які отримують

ключі. Таким чином, найнижчий ряд і лівий стовпчик мають найнижчу відмовостійкість, а найвищий правий - найвищу.

Розподілене гіперзахищене файлове сховище, створене відповідно до цього розкриття, забезпечує довгострокову стійку безпеку за рахунок адаптації, тобто повторного використання, численних новаторських елементів зв'язку SDNP. Ці інноваційні елементи включають в себе:

- Парсинг файлу та розповсюдження його фрагментованого вмісту за кількома незв'язаними мережевими серверами зберігання файлів,

- Передача файлів між клієнтським сервером і сервером зберігання файлів за допомогою наскрізного гіперзахищеного з'єднання, що містить динамічно шифрований зашифрований анонімний фрагментарний транспорт даних SDNP без використання майстер-ключа,

- Зберігання фрагментованих файлів на серверах таким чином, щоб сервери зберігання не мали доступу до облікових даних безпеки клієнтів, які використовувалися для початкової фрагментації і шифрування даних, тобто щоб сервер зберігання файлів не мав "клієнтської сторони" облікових даних безпеки "Останньої Милі" для дешифрування, доступу або читання файлу.

- Опціональне шифрування фрагментованих файлів на серверах виконується таким чином, щоб клієнт (власник файлу) не мав облікових даних безпеки, необхідних для дешифрування зберігаючих даних, за винятком безпечного з'єднання, тобто коли клієнтська сторона "Останньої Милі" не володіє обліковими даними безпеки "сторони зберігання" "Останньої Милі", які використовуються для локального дешифрування файлів.

- Обмеження кількості посилань на файлове сховище, необхідних для знаходження і відкриття файлу, і обмеження доступу користувача до таких посилань на клієнтський пристрій власника файлу разом з резервними або бекапними пристроями,

- Вимога багатофакторної автентифікації та перевірки особи клієнта для створення посилання на файл та виконання операції читання або видалення,

- Використання анонімної маршрутизації пакетів даних та анонімних імен файлів, де навіть при використанні посилання для виклику даних не відображається інформація про місце розташування або шифрування гіперзахищеного сховища і де, не рахуючи посилання, не зберігається інформація про маршрутизацію в мережі SDNP або гіперзахищеній системі зберігання файлів,

- Розподіл фрагментованого файлу по декількох серверах зберігання за допомогою нерозкритих розташувань файлових серверів, за винятком посилання на файлове сховище, з використанням анонімних імен, невідомих клієнтові, мережі SDNP або інших серверів зберігання,

- Використання триканального зв'язку, коли сигнальні сервери SDNP, що використовуються для планування маршрутизації файлів для розподіленого зберігання, не мають доступу до вмісту фрагментованих файлів або облікових даних безпеки, що використовуються для шифрування файлів і де у вузлах SDNP, які використовуються для транспортування файлів, використовуються пакети даних SDNP одного хопу без ідентифікації або адреси клієнта або сервера зберігання файлів,

- Регулярне використання динамічного перейменування файлів і переміщення даних після багаторазового доступу до файлів, відновлення облікових даних безпеки під час операції перезапису файлів; і

- Локальне шифрування директорії сервера зберігання файлів для запобігання аналізу файлів.

З урахуванням вищесказаного, відсутність будь-якої видимої ідентифікації файлу, використання фрагментованого файлу, розподіленого по мережі (можливо, в глобальному масштабі), та використання облікових даних безпеки для конкретних зон унеможливлює доступ до гіперзахищеного файлу та його реконструкції без доступу до посилання на сховище файлів. Такі FS посилання, обмежені за кількістю і поширювані тільки через систему зв'язку SDNP, додатково захищені перевіркою особи.

Виконання вищеперерахованих функцій для файлового гіперзахищеного сховища може бути представлено схематично так само, як і взаємодія гіперзахищеного зв'язку, використовуючи функціональні символи, показані раніше на Рис. 9A. Для спрощення, як показано на верхній ілюстрації Рис. 92, будь-яка комбінація з функції скремблінгу 926, вставки "сміттєвих" даних 1053, парсингу 1052 і розділення 1057 і шифрування 1026 за станом або часом 926C може бути представлена у вигляді функції шифрування SDNP 1750. Аналогічним чином, функція дешифрування 1751 включає в себе дешифрування 1032, змішування 1061, видалення "сміттєвих" даних 1053B і дескремблювання 928 з використанням стану або часу 926B.

Використовуючи вищезгадані захисні функції, верхня ілюстрація на Рис. 93A показує процес розподіленого зберігання файлів з шифруванням на боці клієнта. Як показано на Рис. , файл 1705 розібрано 1052 і розділено 1057 для створення розібраного файла 1706 на клієнтському пристрої 1700A, який використовується для реалізації SDNP клієнта $C_{1,1}$. Отримані фрагменти файлів потім шифруються за допомогою облікових даних зони U1 операцією SDNP шифрування 1750B для зв'язку "Останньої Милі" відповідно до методів, описаних у цій заяві. Фрагменти файлу, які передаються послідовним або багатомаршрутним каналом зв'язку "Останній Милі", потім приймаються шлюзом SDNP $M_{0,0}$ і дешифруються за допомогою операції дешифрування SDNP 1751C відповідно до даних безпеки зони U1, що дозволяє відновити оброблений файл 1706. Оброблений файл 1706 потім повторно шифрується операцією шифрування SDNP 1750C відповідно до даних безпеки зони Z1 хмари SDNP. Під час сітчастого пересилання, після серії операцій дешифрування і шифрування зон Z1 в хмарі SDNP (не показано), остаточні пакети даних надходять на відповідні шлюзи SDNP, включаючи, наприклад, шлюз $M_{0,8}$, де операція дешифрування SDNP 1751D відновлює розібраний файл 1706, потім повторно шифрує його за допомогою операції шифрування SDNP 1750D згідно з вимогами безпеки зон U9. У показаному прикладі 1706 розібраний файл розбитий на два файли, а розібрані файли 2 і 3 розібраного файла 1706 відновлюються за допомогою функції дешифрування SDNP 1751E і зберігаються на сервері зберігання файлів 1740B і 1740C відповідно. У цьому методі файли даних, що зберігаються на серверах файлового сховища, фрагментовані, але в іншому випадку (за винятком шифрування локального диска) файли будуть доступні при кібератаці на дані диска. Таким чином, безпека досягається фрагментацією файлів та розподіленим зберіганням.

Більш високий рівень захисту файлів досягається за рахунок використання процесу, показаного на нижній ілюстрації Рис. 93A, який демонструє процес розподіленого зберігання файлів з повним шифруванням на клієнтській стороні. Як показано на Рис. , файл 1705 обробляється операцією шифрування 1750A SDNP для створення скрембльованого, зашифрованого, розібраного файлу 1706 на клієнтському пристрої 1700A, який використовується для реалізації клієнта SDNP $C_{1,1}$. Операція 1750A також включає в себе поділ 1706 файлів на три фрагментовані файли 1, 2 і 3. Потім фрагментовані файли 1, 2 і 3 шифруються за допомогою облікових даних зони U1 операцією шифрування SDNP 1750B для зв'язку Останньої Милі, що виконується відповідно до методів, описаних у цій заяві. Фрагменти файлу, що передаються послідовним або багатомаршрутним каналом зв'язку "Останній Милі", потім приймаються шлюзом SDNP $M_{0,0}$ і дешифруються за допомогою операції дешифрування SDNP 1751C відповідно до облікових даних зони U1, що дозволяє відновити скрембльований, шифрований, оброблений файл 1706. Оброблений файл 1706 потім повторно шифрується операцією шифрування SDNP 1750C відповідно до даних безпеки зони Z1 хмари SDNP.

Під час сітчастого пересилання, після серії операцій дешифрування і шифрування зони Z1 в хмарі SDNP (не показано), остаточні пакети даних надходять на відповідні шлюзи SDNP, включаючи, наприклад, шлюз $M_{0,8}$, де операція SDNP дешифрування 1751D відновлює скрембльований, шифрований, оброблений файл 1706, потім повторно шифрує його, використовуючи операції шифрування SDNP 1750D відповідно до облікових даних зони U9. Фрагментовані файли 2 і 3 скрембльованого, зашифрованого і розібраного 1706 файлу відновлюються за допомогою функції дешифрування SDNP 1751E і зберігаються відповідно на сервері 1740B і 1740C файлової пам'яті. Тому файл захищений не тільки фрагментованим розподіленим сховищем, а й комбінацією скремблювання, "сміттєвих" даних і шифрування, відомою тільки клієнтській зоні безпеки. Таким чином файл 1 передається через SDNP хмару на шлюз $M_{0,4}$, де він зберігається у файловому сховищі 1700H в зоні U7, як показано з пакетом 1712A на Рис. 88.

В обох прикладах, описаних вище, більш високий рівень безпеки може бути досягнутий шляхом виключення останньої операції дешифрування SDNP 1751E, показаної на ілюстраціях Рис. 93B. Таким чином, файли, що зберігаються на серверах файлового сховища, залишаються зашифрованими за допомогою операції шифрування SDNP 1750D з використанням облікових даних безпеки зони U9. На верхньому Рис. файли фрагментовані клієнтом, але зашифровані відповідно до облікових даних безпеки сторони зберігання для зони U9. На нижньому Рис. файли шифруються відповідно до облікових даних безпеки U1 на боці клієнта, а потім шифруються вдруге відповідно до облікових даних безпеки на стороні зберігання для зони U9. Такий подвійний зашифрований файл, крім захисту фрагментованим розподіленим файловим сховищем, є вкладеним гіперзахищеним сховищем, оскільки файл, зашифрований обліковими даними зони U9, містить файл, зашифрований обліковими даними системи безпеки U1.

Перевага вкладеної безпеки полягає в тому, що ні клієнт, ні сервер зберігання не мають необхідної інформації для відкриття збереженого файлу.

Короткий опис показових методів впровадження дезагрегованого гіперзахищеного зберігання файлів наведено на Рис. 94. У наведених прикладах шифрування та дешифрування, які використовуються для гіперзахищеного зв'язку та хмарної маршрутизації SDNP, видалено, що дає тільки кінцевий ефект від шифрування файлів. У верхньому лівому куті показано приклад фрагментації клієнтської зони, коли документ фрагментовано відповідно до облікових даних зони U1, але без будь-яких додаткових заходів безпеки з боку мережевого сховища. У нижньому лівому куті показано приклад шифрування клієнтської зони, де документ зашифрований операцією 1750B, тобто скрембльований, забезпечений "сміттєвими" файлами, фрагментований, зашифрований відповідно до облікових даних зони U1, але без введення будь-яких заходів безпеки на боці мережевого сховища.

У правому верхньому куті показано випадок фрагментації клієнтської зони U1, але де додатковий крок шифрування SDNP, тобто скремблювання, вставлення "сміттєвих" файлів, фрагментація і шифрування, вводиться на боці зберігання відповідно до зони U9. У правому нижньому куті представлено приклад повного вкладеного файлового гіперзахищеного сховища, де файл шифрується і фрагментується відповідно до операції шифрування SDNP 1750B з боку U1 облікових даних клієнта, а потім файл шифрується повторно відповідно до даних безпеки зони U9 на боці сховища "Останньої Милі".

Щоб відкликати і прочитати файл, при відкликанні даних повинні використовуватися захисні операції, що включають в себе антифункції, виконувані в точному зворотному порядку, як показано на Рис. 95. У верхньому лівому куті для відкликання фрагментованих даних клієнтської зони, розібраний файл 1706, викликаний з різних серверів зберігання файлів, комбінується за допомогою операції злиття 1061 для відновлення вихідного файлу 1705. У нижньому лівому куті відкликання клієнтської зони зашифрованих даних, розібраний файл 1706 відкликаний з різних серверів зберігання файлів відновлюється для доступу до вихідного файлу 1705 за допомогою операції дешифрування SDNP 1751H, точної антифункції операції розділення 1750B, включаючи змішування, дешифрування, дескремблювання. У правому верхньому куті, де зображено сховище шифрованих, фрагментованих клієнтською зоною файлів, зворотна операція спочатку проводить операцію дешифрування SDNP 1751F для скасування наслідків операцій захисту зони U9 для відновлення розібраного файлу 1706, потім операцію об'єднання файлів 1061 для скасування ефекту операції розділення файлів 1057 відповідно до облікових даних зони Z1.

У нижньому прикладі справа для читання повністю вкладеного гіперзахищеного файлу, дані, що зберігаються на різних серверах зберігання, дешифруються операцією дешифрування SDNP 1751D з використанням облікових даних зони U9 для відновлення файлу 1706, який як і раніше скрембльований, забезпечений "сміттєвими" даними, розібраний, і зашифрований відповідно до облікових даних зони Z1. Операція дешифрування SDNP в зоні Z1 1751H потім виконує послідовні анти-функції кодування 1750B, що включають змішування, дешифрування і дескремблювання для відкликання вихідного файлу 1705. Операція виконання послідовної антифункції відновлення файлу повинна виконуватися в зворотному порядку порівняно з послідовністю, яка використовується для його створення. Наприклад, якщо шифрування включає поділ, потім скремблювання, а потім шифрування, антифункція, тобто дешифрування, повинна включати операційну послідовність дешифрування, потім дескремблювання, а потім змішування. Якщо, однак, кодування послідовно включає в себе скремблювання, потім шифрування, а потім поділ пакета, то антифункція, тобто декодування, повинна включати послідовність змішування, дешифрування і нарешті дескремблювання пакетів даних.

Для відкликання або читання файлів клієнт натискає на посилання "Читати файлове сховище", щоб ініціювати кроки, необхідні для відкликання та читання файлів, що зберігаються в гіперзахищеній системі зберігання системи. Процес читання включає наступні етапи, як показано на Рис. 96A:

- Власник файлу і клієнт 1700A або авторизований користувач натискає на посилання читання файлового сховища в програмі SDNP, такому як гіперзахищений месенджер 1196 з підтримкою SDNP, файловий менеджер або інший інтерфейс з підтримкою SDNP.
- Використовуючи діалоговий інтерфейс 1765 або командний рядок, клієнт 1700A вказує запит файлу 1761, включаючи читання файлу, редагування файлу (створення копії файлу з правами запису), видалення файлу (видалення), оновлення посилання (перевипуск облікових даних) або перерозподіл файлу (переміщення фрагментів файлу на різні сервери зберігання і випуск нового посилання для читання власником файлу або клієнтами).

- У операції "верифікація клієнтів" 1762, сигнальний сервер SDNP 1715 підтверджує особу клієнта або клієнтів, які запитують файл (автентифікацію). У діалоговому вікні 1767 клієнт повинен підтвердити свою особу за допомогою PIN-коду і, за бажанням, другого фактора, який визначає пристрій або токен безпеки. Альтернативно, SMS повідомлення може бути відправлено на інший пристрій, що належить тому ж клієнтові. У файлах, що потребують схвалення доступу з боку декількох клієнтів, необхідно перевірити особу кожного користувача (мульти-автентифікація).

- У операції "Перевірка привілеїв" 1763, сигнальний сервер 1715 підтверджує, що запитувач 1700A має право доступу до запитаного файлу з правами читання або читання/видалення (авторизація). Результат відображається у діалоговому вікні 1768 перед підтвердженням того, що користувач ще хоче завантажити або прочитати файл. Якщо особа не підтверджена, запитувачу може бути дано вказівку повторити спробу. Після певної кількості невдалих спроб адміністратор файлу 1700Z (якщо такий є) буде поінформований про невдалі спроби, і акаунт буде заблоковано. Діалогове вікно може проінформувати користувача про проблему з проханням зв'язатися з адміністратором файлу або, у разі підозр на злам, вікно може залишитися порожнім або навіть "викинути" користувача з програми SDNP.

- У процесі адміністрування запиту документа 1764 сигнальний сервер 1715 SDNP інформує адміністратора файлового сховища 1700Z про запит доступу до файлів і характер запиту (адміністрування). Цей адміністративний крок може (i) бути пропущений повністю, (ii) зареєструвати запит на доступ до файлів в обліковому записі адміністратора файлового сховища, (iii) надіслати повідомлення адміністратору файлового сховища, негайно поінформувавши його про спробу доступу до файлів, або (iv) запросити роздільну здатність адміністратора файлового сховища через діалогове вікно 1769 до надання доступу клієнтові.

Після цих кроків автентифікації, авторизації та адміністрування (AAA), після схвалення, клієнт робить запит на доступ до файлу, використовуючи кроки, показані на блок-схемі на Рис. 96B, яка використовується як ілюстрація запиту на читання. Ці кроки включають наступне:

- При виконанні запиту читання 1770 запитувач 1700A надсилає запит на читання файлу на сигнальний сервер 1715 SDNP.

- У режимі запиту імені сервера зберігання 1771 сигнальний сервер 1715 SDNP надсилає запит імені сервера зберігання файлів на сервер імен 1714 SDNP, запитуючи поточні адреси SDNP відповідних серверів зберігання файлів, наприклад, сервера зберігання файлів 1700M. Відповідно до методу SDNP адреса SDNP для клієнтів SDNP (включаючи файлові сервери) змінюється не рідше одного разу на день, щоб запобігти можливості довготривалого відстеження клієнта.

- У операції доставки імені сховища 1772, сервер імен SDNP 1714 передає запитувані імена файлів "FS адреси" на сигнальний сервер SDNP 1715, за допомогою чого сигнальний сервер SDNP прокладає маршрутизацію відкликання файлів.

- У операції маршрутизації 1773, сигнальний сервер SDNP надсилає інструкції щодо маршрутизації файлів клієнту 1700A, вузлам у хмарі SDNP, таким як сервер 1700U, і серверам зберігання файлів із зональними обліковими даними, таким як сервер зберігання файлів 1700M з обліковими даними безпеки зони U9, включаючи стан або час 920, цифровий ключ 923, ключ шифрування 1030 і додатковий ключ шифрування 1022 (використовується в режимі зв'язку зашифрованої симетричним ключем).

- У операції відновлення локальних файлів 1774, використовуючи відповідні облікові дані безпеки, включаючи інформацію про стан або час створення файлу, сервер DMZ на кожній стороні зберігання дешифрує і відновлює розібраний файл і впорядковує дані в один або кілька пакетів даних у процесі підготовки до пересилання.

- При доставці файлів 1775, кожен розібраний файл доставляється запитувачу з використанням незалежної доставки по мережі SDNP відповідно до інструкцій маршрутизації сигнального сервера SDNP, наприклад, коли сервер зберігання файлів 1700M відправляє файл клієнту 1700A.

- Вхідні розібрані файли даних дешифруються відповідно до облікових даних клієнтської зони, а аналізований файл об'єднується для відтворення вихідного файлу, готового для перегляду або передачі.

Кроки представлені в наступній послідовності ілюстрацій. На Рис. 97A клієнтський пристрій за адресою "IP $C_{1,1}$" робить запит на читання файлу на сигнальний сервер 1715 за адресою "IP S" за допомогою пакета даних 1810A, який включає корисне навантаження 1811A із зазначенням TCP, інформацію заголовка файлу і два або більше FS-посилання. FS посилання анонімно описують розташування збережених фрагментів файлів, використовуючи теги або псевдо-адреси, які повинні бути перетворені на SDNP-адреси або IP-адреси для маршрутизації.

Сигнальний сервер 1715, однак, не знає поточну SDNP-адресу для цих іменованих ідентифікаторів користувачів і повинен запитувати поточну інформацію з сервера імен 1714 SDNP. На Рис. 97B сигнальний сервер 1715 надсилає пакет даних 1810B на сервер 1714 із запитом IP або SDNP адрес вузлів $F_{7,1}$, $F_{9,4}$ і $F_{9,1}$ сервера зберігання файлів. На Рис. 97C сервер імен 1714 передає сигнальному серверу 1715 пакет даних 1810C, що містить IP або SDNP адреси серверних вузлів зберігання файлів $F_{7,1}$, $F_{9,4}$ і $F_{9,1}$. Сигнальний сервер 1715 обчислює після цього "Останню Милю" і сітчасте хмарне пересилання розібраних файлів на сервери зберігання даних.

На Рис. 97D сигнальний сервер 1715 відправляє пакети даних системи управління і командування на вузли "Останньої Милі", розташовані на боці сховища, тобто в зони U7 і U9. Як показано на Рис. , пакет даних 1810G передається з сигнального сервера 1715 за адресою S на сервер зберігання даних 1700H за адресою "IP $F_{7,1}$" з корисним навантаженням, що включає "Інструкцію з читання файлу 1" 1811G. Цей пакет інструктує сервер зберігання файлів надсилати файл з ідентифікаційним тегом 1 з адреси "IP $F_{7,1}$" на шлюз SDNP за адресою "IP $M_{0,4}$", використовуючи облікові дані безпеки U7. Одночасно пакет даних відправляється на шлюз SDNP, пакет передається з адреси "IP S" на "IP $M_{0,4}$", що містить корисне навантаження 1811F, повідомляючи, що пакет даних з тегом 1 повинен бути передбачений вузлом шлюзу $M_{0,4}$ і при отриманні перенаправлений в хмару SDNP, використовуючи облікові дані безпеки Z1, наприклад, для адреси SDNP $M_{0,31}$.

Другий пакет даних 1810I відправляється з сигнального сервера 1715 SDNP за адресою "IP S" на сервер зберігання даних 1700M за адресою "IP $F_{9,1}$", що містить корисне навантаження 1811I, що містить "Інструкцію з читання файлу 3". Ця інструкція вказує серверу зберігання файлів 1700M надіслати файл з ідентифікаційним тегом 3 на шлюз SDNP адреси IP $M_{0,8}$ за допомогою облікових даних зони U9. Інші пакети команд і керування (не показано) також надсилаються на інші сервери зберігання файлів і шлюзи, такі як вузли $F_{9,4}$ і $M_{0,8}$, а також вузли в SDNP хмарі.

На Рис. 97E сигнальний сервер 1715 відправляє пакет даних 1810D на клієнтський пристрій 1700A, при цьому пакет маршрутизується з адреси "IP S" на "IP $C_{1,1}$" через маршрутизатор 1702G. Пакет даних 1810D містить корисне навантаження системи команд і управління 1811D, яка інформує клієнта про те, що від шлюзу SDNP 1701U за адресою "IP $M_{0,0}$" за допомогою облікових даних зони U1 можна очікувати кілька вхідних пакетів даних з тегом 1, тегом 2 тощо. Одночасно сигнальний сервер 1715 також відправляє пакет даних 1810E на шлюз SDNP 1701U, пакет надсилається з адреси "IP S" на "IP $M_{0,0}$". Цей пакет включає корисне навантаження системи команд і управління 1811E для маршрутизації "Останньої Милі" в зоні U1, яка застосовна для вхідних пакетів даних, ідентифікованих як пакети тегів 1, 2 і 3, що передаються з SDNP хмари.

Після того, як пакунки даних команд і керування буде розподілено по мережі, можна пересилати файли. Перший етап передачі показано на Рис. 98, де пакет даних 1741R, що включає FS посилання 3, надає інформацію щодо операції дешифрування SDNP 1751R, включаючи приклад стану 920, цифровий ключ 929, ключ дешифрування 1030, і ключ шифрування 1022. Від імені дії дешифрування SDNP 1751R ця інформація обробляється сервером DMZ 1752 для виконання функцій, пов'язаних із загальними секретами, такими як дешифрування пакетів 1032R, змішування 1061R, видалення "сміттєвих" файлів 1053R і дескремблювання 928R, все виконується в стані 920, у якому файл, що обробляється, було зашифровано востаннє. Зауважте, що ключ шифрування 1022 не потрібен спеціально для дешифрування файлу, але може бути використано в симетричному шифруванні для пересилання парсованого файлу назад клієнту і власнику файлу.

Маршрутизація файлів і пересилання даних показано на Рис. 99, включаючи пакет даних TCP 1720A, що містить файл 1 з адресою "IP $F_{7,1}$" до "IP $M_{0,4}$" з використанням облікових даних U7, пакет даних TCP 1720B з адресою "IP $F_{9,4}$" до "IP $M_{0,8}$" з обліковими даними U9, пакет даних TCP 1720C з адресами "IP F_9" і пакет даних $U_{1,0}$ з обліковими даними $M_{8,3}$ до "IPF_9". Після пересилання через SDNP хмару (не показано), серія пакетів даних 1720X доставляється від шлюзу SDNP за адресою "IP $M_{0,0}$" на адресу клієнта "IP $C_{1,1}$".

У процесі читання дані завантажуються в програму SDNP у формі "тільки читання". Поки файл знаходиться в ізольованому середовищі в додатку SDNP, він захищений функціями програми і мережі SDNP і не залежить від процедур входу в систему і недостатніх заходів безпеки операційної системи пристрою. У бізнесі широко поширена необхідність мати доступ до приватних документів для читання. Файли, підготовлені фінансовими, юридичними, виробничими, інженерно-технічними та контрольними підрозділами, ілюструють приклади матеріалів, які часто містять інформацію, доступну тільки для читання. У багатьох випадках ці

конфіденційні файли компанії повинні бути передані, тобто поширені в електронному вигляді, керівникам компаній для ознайомлення до їх розповсюдження.

Випадкове або передчасне розкриття переданої інформації може мати катастрофічні наслідки, спричинити за собою важкі економічні і навіть правові наслідки для компанії і персональну відповідальність її посадових осіб. Наприклад, неопублікований фінансовий звіт публічної компанії є суворо конфіденційним до його видання. У Сполучених Штатах правило "сумлінного розкриття" означає, що інформація повинна бути оприлюднена для загального доступу одночасно для всіх і без будь-яких преференцій. Якщо будь-яка зовнішня сторона отримає доступ до цієї інформації до її оприлюднення, це є порушенням правила "сумлінного розкриття". Якщо суд встановить, що порушення положення "сумлінного розкриття" відбулося через недбалість компанії у виконанні своїх обов'язків щодо збереження та забезпечення конфіденційності документа, то компанія може бути покарана за його порушення, а її посадові особи можуть бути притягнуті до персональної відповідальності, навіть якщо за виборчим розкриттям інформації не послідував інсайдерський трейдинг.

У додатку SDNP отриманий файл розділений на частини (в ізольованому середовищі) для запобігання перенесенню даних з одного облікового запису на інший, тобто файли не можуть бути перенесені між особистими і бізнес-акаунтами. Залежно від прав доступу читача користувачеві може бути дозволено або не дозволено завантажувати витягнутий файл з програми SDNP і зберігати його в незашифрованому вигляді в пам'яті пристрою. Завантаження файлу за межі програми з підтримкою SDNP ставить під загрозу безпеку файлу і даних, що містяться в ньому. Для даних, що зберігаються в програмі SDNP, доступ контролюється, дії користувача обмежені, і як пристрій, так і мережа SDNP повинні перевіряти особу користувача. Таку багаторівневу багаторівневу і багатофакторну аутентифікацію обійти набагато важче, ніж звичайний 4-значний пін-код, необхідний для відкриття телефону. Однак, як тільки файл завантажується в комп'ютер, планшет або мобільний телефон, практично неможливо запобігти несанкціонованому доступу, визначити, хто має доступ або хто зробив копію файлу.

Таким чином, використовуючи SDNP комунікацію, власник файлу може заблокувати, тобто розділити конфіденційні документи і файли на частини, щоб інші могли їх читати, але не завантажувати в свій телефон. Для запобігання знімків екрану або фотографій ЖК-дисплея можна виконати додаткові заходи. В інших випадках, коли безпека або конфіденційність не потрібні, передача файлів з програми SDNP в пам'ять телефону дозволена і доступна для використання без обмежень.

Під час редагування форма файлу завантажується в пристрій і передається до програми, необхідної для обробки файлу. Для запиту файлу та обміну даними у мережі SDNP немає принципової різниці між запитом на читання файлу і запитом на редагування файлу, крім як у роботі клієнтської програми SDNP - з точки зору передачі даних по мережі SDNP, ці операції функціонально еквівалентні. Отже, відмінності між операціями читання та редагування можуть розглядатися в першу чергу як відмінності у виконанні операцій на рівнях від 5 до 7, що включають файли певних програм.

Для редагування отриманого файла програмою може бути (i) програмою, вбудованою в пристрій (наприклад, Simpletext), спочатку використовуваною операційною системою пристрою, але працює поза програмою SDNP, (ii) сторонньою програмою, що працює поверх ОС пристрою, але поза програмою SDNP, наприклад, Microsoft Word, Adobe Acrobat тощо або (iii) захищеною програмою, що працює всередині програми SDNP і не доступна безпосередньо з його ОС. Наприклад, корпоративний прес-реліз можна відредагувати в пісочниці програми SDNP, але його не можна завантажити в пам'ять телефону. В якості додаткової умови для забезпечення безпеки будь-якого файлу, що належить компанії, тобто знаходиться в пісочниці у відділенні бізнес-акаунта SDNP, не можна передавати в особистий акаунт SDNP, навіть якщо обидва профілі працюють в одному і тому ж SDNP додатку.

Після редагування, збереження відредагованого файлу назад на серверах зберігання SDNP не перезаписує існуючі дані, якщо тільки власник файлу спеціально не попросить про це. Замість цього друга версія зберігається на додаток до першої і усунення попередньої версії вимагатиме від користувача виконання операції видалення. Оскільки гіперзахищене сховище файлів незмінно вимагає перевірки справжності, процес збереження відредагованого файлу може включати унікальні системні функції, недоступні зі сховища файлів без спеціальної мережевої взаємодії з гіперзахищеною мережею. У цьому випадку такою унікальною особливістю є функція перевірки підпису, яка використовується для підпису і дати (в Азії для друку/вибору і дати) файлу. Функція підпису може включати зареєстровану розписку, надіслану власнику документа і творцеві оригінального документа.

Для гіперзахищеного сховища даних, створеного згідно з цим винаходом, операція видалення включає перезаписування всіх існуючих парсованих файлів випадковими числами і опціональний перезапис через годину для подальшого приховування невеликих, але потенційно помітних змін електричного або магнітного поля збереженого біта. Запис файлу також буде перезаписано, щоб зробити процес запису файлу на диск даних більш заплутаним. Після видалення даних і запису файлу посилання на клієнтський пристрій знищується за допомогою функції самознищення повідомлення системи SDNP, а всі залишки FS посилання видаляються з системи SDNP. Однак якщо адміністратор системи файлів відстежує активність бази користувачів за допомогою стороннього програмного забезпечення, він може зберігати метадані про історію файлу, включаючи його власника, дату створення, хто і коли отримав доступ до файлу, коли і як він був видалений, навіть якщо у нього немає доступу до самого файлу.

Мережа SDNP і функції гіперзахищеного зв'язку "Останньої Милі" також можуть підтримувати різні функції і операційні процедури для корпоративних облікових записів, а не тільки особистих акаунтів. Як описано вище, операція видалення на особистому акаунті включає в себе перезапис "сміттєвих" даних у файл, очищення індексного запису диска про існування файлу і знищення всіх FS посилань на попередні місця зберігання файлу за допомогою повідомлень самознищення. Для корпоративних облікових записів, однак, адміністратору сховища може знадобитися їх попередня роздільна здатність для остаточного знищення файлу, наприклад, за допомогою процесу затвердження, аналогічного діалоговому вікну 1769 на Рис. 96A, але надісланий адміністратору, а не власнику файла.

Якщо адміністратор файлів компанії не дозволяє вилучення файлів, може відбутися декілька сценаріїв, включаючи (i) сповіщення власника файла про те, що (i) файл не буде вилучено і посилання для читання зберігається в програмі SDNP або історії повідомлень SDNP програми, (ii) сповіщення власника файла про те, що вилучення файла не буде виконано, тобто файл буде збережено для "архівних потреб", але їх особисте посилання на читання файла буде вилучено з програми SDNP за допомогою самознищуваних повідомлень системи SDNP, тобто при спробі видалення файла тільки адміністратор файлового сховища зможе його відновити, або (iii) посилання на читання файла буде вилучено з програми SDNP власника файла за допомогою самознищених повідомлень системи SDNP, але вони не будуть повідомлені про це компанією, оскільки файл був збережений.

Через те, що гіперзахищеному зв'язку "Останньої Милі" притаманне функціонування розкритої анонімної фрагментованої розподіленої системи зберігання файлів, без "посилання читання файлового сховища" збережені файли не можуть бути відновлені навіть адміністратором системи.

Для того, щоб адміністратор міг отримати доступ до файлу, при кожному збереженні або редагуванні файлу має існувати відповідне посилання на читання з файлового сховища. Хоча такий рівень контролю можливий для корпоративного облікового запису, величезна кількість даних, що генеруються при відстеженні кожної зміни в кожному файлі, неминуче перевантажить будь-яку систему управління файлами. Інтелектуальний фільтр, доступний у системі SDNP, дозволяє відстежувати тільки спроби видалення файлів. При такому підході адміністратор не відстежує процес створення файлів, а відстежує тільки спроби їх видалення. Щоразу, коли власник файлу намагається видалити файл, посилання на читання файлового сховища передається в базу даних або консоль адміністратора для затвердження або архівування.

Розмір бази даних може бути додатково мінімізований шляхом визначення конкретних співробітників і підрядників, щодо яких потрібне спостереження. Наприклад, якщо компанія залучена у фінансовий аудит або патентний процес, сторони, як правило, інформуються про те, що вони не видаляють відповідні дані і не стирають файли. За допомогою функцій керування файлами, передбачених системою зберігання файлів SDNP, будь-які спроби співробітників, причетних до розслідування, можуть бути відстежені шляхом запису спроб видалення або надсилання копії посилання на файлове сховище адміністратору або, залежно від обставин, незалежному слідчому. Такий метод корисний, оскільки він обмежує обсяг даних, що підлягають моніторингу, і природно попереджає керівництво про підозрілу діяльність, що передбачає спробу приховування протиправних дій. Щоб запобігти випадковій або зловмисній втраті посилання на файлове сховище в результаті руйнування самого пристрою клієнтом і власником файлу, необхідно використовувати резервні посилання на файлове сховище, описані вище. У корпоративному сегменті резервна копія може зберігатися на комп'ютері, розташованому в захищеному офісі, або на централізованому сервері компанії.

В умовах крайньої міри захищеності, наприклад, з метою забезпечення національної безпеки, видалення файлу може включати багатоетапний метод, що включає: i) перезапис файлу випадковими даними, ii) копіювання всіх інших файлів з накопичувача на інший пристрій

зберігання даних; iii) виконання масового видалення диску; iv) переформатування диску; v) перезапис полів зберігання випадковими номерами; vi) копіювання збережених файлів. На відміну від звичайного перезапису файлу, процес об'ємного видалення впливає на сам носій даних, автоматично змінюючи його електричні, магнітні або оптичні властивості у випадковому порядку на молекулярному рівні. Для масового видалення на магнітному накопичувачі може використовуватися великий електромагніт, масове видалення на flash-накопичувачі може призвести до підвищення температури мікросхем і, можливо, піддати їх іонізуючому випромінюванню при підвищеній робочій напрузі. Масове видалення на магнітооптичних накопичувачах може бути вироблено за допомогою високочастотних магнітних полів. Масове видалення на перезаписуваних оптичних дисках може бути зроблено за допомогою яскравого скануючого лазера, що сканує доріжки диска. У будь-якому випадку, масове видалення являє собою винятковий випадок, коли носій інформації після видалення або повністю позбавляється даних, або знаходиться під загрозою пошкодження, що може призвести до неможливості його повторного використання.

Ще одним важливим фактором у системі розподіленого гіперзахищеного сховища файлів є збереження цілісності файлових даних і доступу за посиланнями. Щоб не допустити випадкової втрати посилання, корисно час від часу відновлювати, тобто підтверджувати посилання на файлове сховище і перевипускати облікові дані. Цей процес, названий командою "оновити посилання", може бути ініційований клієнтом або зроблений автоматично, а також може бути ініційований з сервера зберігання файлів через певний проміжок часу. Для запитів, ініційованих клієнтом, сигнальний сервер SDNP пов'язує пакети команд і управління з відповідними серверами. Після ініціалізації оновлення посилання, як показано на Рис. 100, файли зчитуються і дешифруються операцією дешифрування SDNP 1751F в стані 320X, "старому" стані за часом t_1, в якому вони були раніше створені з використанням облікових даних зони U9. Потім файл повторно шифрується операцією шифрування 1750D SDNP з використанням нового стану 920Y за часом t_2 і зберігається на накопичувачі. Оновлене посилання на сховище, наприклад, посилання 3 FS, потім відправляється по мережі SDNP назад власнику файлу, клієнтському пристрою 1700A. Отриманий файл містить зашифровані дані, оновлені обліковими даними зони U9 під час t_2. Однак облікові дані клієнта в зоні U1, які використовуються для створення та аналізу файлу, спочатку не оновлюються. Для читання файлу операція зчитування повинна спочатку дешифрувати його, використовуючи облікові дані зони U9 в стані, відповідному часу t_2, а потім, після перенесення на клієнтський вузол $C_{1,1}$, дешифрувати файл, використовуючи облікові дані зони Z1, пов'язані з часом створення файлу.

Як ще один засіб для підвищення безпеки, операція перерозподілу переміщує кожен парсований файл певного посилання на сховище нового або іншого сервера зберігання файлів. Операція може надсилати розібрані файли на абсолютно нові сервери, або файли можуть бути перерозподілені між існуючими вузлами зберігання. У кожному випадку оновлюються облікові дані і видається нове FS-посилання на файл, яке відправляється клієнту або клієнтам, що мають доступ до файлу. Ця операція показана на Рис. 101, де вміст вузла файлового сховища SDNP $F_{7,1}$ в зоні U7 дешифрується операцією дешифрування SDNP 1751H у стані 920X, стані t_1 на момент створення файлу. Потім файл передається по мережі SDNP (не показано) на файлове сховище SDNP-вузла $F_{9,4}$, де піддається операції шифрування SDNP 1750L з використанням облікових даних зони U9 при стані 920Y, відповідне часу t_2. Потім файл зберігається, а власнику файлу та іншим клієнтам, які мають доступ до файлів, надсилається оновлене FS посилання.

Одночасно з вищезгаданою передачею файлів вміст сховища SDNP-вузла $F_{9,4}$ в зоні U9 піддається операції дешифрування SDNP 1751L з використанням стану 920X, стан, який спостерігався під час створення файлу t_1. Потім файл переноситься по мережі SDNP (не показано) на файлове сховище SDNP-вузла $F_{9,1}$, де він зашифрований операцією шифрування SDNP 1750M з використанням облікових даних зони U9, при стані 920Y який відповідає часу t_2. Потім файл зберігається, а власнику файлу та іншим клієнтам, які мають доступ до файлів, надсилається оновлене FS посилання 3. Подібним чином, вміст файлового сховища SDNP-вузла $F_{9,1}$ в зоні U9 дешифрується операцією дешифрування SDNP 1751M з використанням стану 920X, який спостерігався на момент створення файлу t_1. Потім файл переноситься по мережі SDNP (не показано) на файлове сховище SDNP-вузла $F_{7,1}$, де він шифрується операцією шифрування SDNP 1750H за обліковою записом зони U7 в стані 920Y, відповідне часу t_2. Потім файл зберігається, а власнику файлу та іншим клієнтам, які мають доступ до файлів, надсилається оновлене FS посилання 1. Таким чином, всі три файли переміщуються і отримують нові облікові дані безпеки, а клієнтам з правами доступу видаються нові посилання для читання файлового сховища на основі оновлених FS посилань 1, 2 і 3.

Ще однією необхідною функцією підтримки, яка виконується гіперзахищеною системою зберігання файлів, є перевірка файлів, які не мають прямих посилань, тобто "Зомбі-файлів". Ця операція аналогічна операції оновлення посилання, за винятком того, що сервер файлового сховища, а не клієнт або власник файлу ініціює її. У процесі роботи кожен сервер зберігання файлів відстежує час, що минув з моменту останнього звернення до файлу. Якщо остання операція з файлом перевищує вказаний інтервал часу, наприклад, місяць без активності, сервер файлового сховища зв'язується з клієнтом або клієнтами для підтвердження того, що посилання все ще активне. Сервер файлового сховища може зв'язатися з клієнтом, використовуючи той самий метод, що і для відправки FS-посилання. Під час зберігання файлу сервер сховища зберігає поштовий індекс SDNP Zip або псевдо-адресу клієнта.

Якщо протягом вказаного інтервалу часу не буде ніяких дій, сервер сховища файлів зв'яжеться з сигнальним сервером SDNP і попросить підтвердити, що зв'язок залишається активним. Потім сигнальний сервер SDNP планує маршрут доставки запиту на перевірку FS посилання для кожного приймаючого участь сервера зберігання файлів. Потім кожен сервер файлового сховища надсилає запит клієнту по мережі SDNP. Кожен клієнтський вузол SDNP, який бере участь у процесі, відповідає підтвердженням того, що посилання на файл все ще присутнє на пристрої. Якщо посилання на файл буде підтверджено, клієнт матиме можливість оновити посилання. Якщо, однак, жоден пристрій не відповів, тобто активне посилання на читання файлу не збереглося, то сервер сховища повідомляє про зникнення або втрату файлу, а через деякий час, наприклад через місяць-три, незатребуваний файл буде остаточно і безповоротно вилучений.

Зареєстрована комунікація - Ще однією особливістю SDNP-комунікацій, створеною відповідно до цього винаходу, є здатність мережі доставляти або зберігати "зареєстровані комунікації". Зареєстрована комунікація включає в себе гіперзахищену доставку інформації або гіперзахищене сховище файлів у вигляді повідомлень підписаних тимчасовою печаткою, включаючи можливість електронного підпису та електронного перезапису для цілей встановлення юридичної сили повідомлення. Зареєстрована комунікація також включає в себе можливість надсилання "сертифікованого повідомлення" способом рукостискання, що підтверджує отримання документа або файлу з використанням підписаної відповіді з відміткою часу. Вся зареєстрована комунікація, ініційована додатком SDNP на клієнтському пристрої, сертифікується за допомогою комунікації "Останньої Милі", тобто зв'язку "Останньої Милі" мережі SDNP. Будь-яка спроба клієнта шахрайським чином змінити підпис підтвердження призведе до невідповідності між повідомленням і мережевим записом підтвердження, тобто звітом про отримання.

Через використання "стану" в комунікації SDNP, тобто часу та інших унікальних змінних, що використовуються для створення спеціальних облікових даних, що забезпечують безпеку повідомлень в комунікаціях і сховищі файлів, маркування часу є невід 'ємною частиною зв'язку SDNP. Прикладом може служити вікно 1800 програми SDNP, показане на Рис. 102, де кожне надіслане і отримане текстове повідомлення має відповідний набір часових міток 1801A і 1801B, що показують, коли повідомлення було надіслано, коли воно було отримано і коли воно було прочитано. Інформація про час, що містить покажчик на загальний час, встановлений сигнальним сервером SDNP, доставляється клієнту по мережі "Останньої Милі". Потім клієнтський додаток SDNP інтегрує мітку часу в інформаційний дисплей.

У зареєстрованій комунікації, комюніке генерує офіційний штамп. Один з прикладів процесу зареєстрованої комунікації показаний на Рис. 103, де гіперзахищене повідомлення виконується, починаючи з опціонального кроку вкладення файла 1802, що включає діалогове вікно 1803, де клієнт, який надсилає повідомлення або файл, тобто відправник, вибирає, чи вкласти файл у повідомлення, за допомогою переглядача каталогу для пошуку файла. Діалогове вікно 1804 використовується для надсилання зареєстрованого повідомлення відповідно до діалогового вікна 1805, в якому вибирається спосіб доставки - звичайна або зареєстрована. Потім повідомлення відправляється за допомогою гіперзахищеного зв'язку, підготовленого відповідно до цього винаходу.

На кроці "Повідомлення прийнято" 1806 одержувач виконує ряд кроків, необхідних для підтвердження особи для отримання доступу до повідомлення і відправлення автентифікованої довідки, що підтверджує прийняття вхідного повідомлення і файлу. Цей процес починається з операції автентифікації прийому 1807, коли одержувача просять підтвердити його особу. Без автентифікації одержувач не зможе отримати доступ до повідомлення, повідомлення буде знищено, а відправник буде повідомлений про невдалий процес автентифікації. Таким чином, відправник може бути попереджений про те, що одержувач, можливо, вкрав його пристрій. Після підтвердження особи одержувачу задається питання при операції авторизації отримання

1808, чи хочуть вони прийняти вхідне повідомлення або вкладення і відхилити його. Якщо повідомлення відхилено - відправник буде повідомлений.

Якщо одержувач приймає повідомлення, вибираючи варіант "так", він повинен виконати адміністративний крок 1809, щоб підписати його, вибравши електронний підпис (e-sign) та/або вибравши друк/штамп (e-chop). Відправник може вказати необхідні параметри. У деяких країнах і штамп, і підпис повинні бути юридично обов'язковими. Наступне діалогове вікно (не показано) вказує користувачеві на те, щоб він знайшов свій підпис або штамп у каталозі файлів пристрою. Як підтвердження можна також використовувати аудіо/відеозапис. Отримувач буде проінструктований про те, що читати під час запису. Після підписання повідомлення воно стає видимим для отримувача, а вкладений файл стає доступним для перегляду і, можливо, для завантаження залежно від вимог відправника.

Під час прийняття документа повідомлення про отримання повідомлення із зазначенням часом 1811, ідентифікуючого одержувача повідомлення, отриманий текст і вкладене ім'я файлу, дані та час отримання повідомлення, підпис, що включає електронний підпис або штамп, аудіо-відео запис або їх комбінацію, надсилається відправнику на підтвердження операції 1810. У параметрі архівного повідомлення про отримання повідомлення 1812 відправник має можливість зберегти копію підписаного повідомлення з позначкою часу 1811 у файлову гіперзахищену систему зберігання, для якої відправник отримає посилання для читання файла 1813, необхідне для відкликання повідомлення. У якості альтернативи, повідомлення про отримання повідомлення 1811 може бути доступне для завантаження на пристрій відправника.

Проблеми з безпекою, заснованою на шифруванні - Державні органи безпеки стверджують, що в сучасному світі корпоративного шахрайства, крадіжки інтелектуальної власності, кіберзлочинності, хакерства, злочинних угруповань, наркокартелів, мафії, якудзи, джихадистів і терористів, будь-яка система зв'язку, що забезпечує невідслідковуваний анонімний зв'язок, тобто систему з шифруванням для захисту даних і приховування особистості, є безвідповідальною бізнес-практикою для операторів мереж, розробників додатків і виробників девайсів.

На жаль, комунікація, заснована на шифруванні для забезпечення безпеки, дійсно захищає як злочинців, так і законослухняних громадян. Як згадувалося раніше, ця тема стала предметом незліченних новин про злочинну діяльність терористів ІДІЛ та їхні напади на Париж і Бельгію за допомогою телефонного додатку "Telegram". Ця програма забезпечує безпечний зв'язок за допомогою наскрізного шифрування, також відомого як кінцеве шифрування. Оскільки ключі дешифрування зберігаються тільки у двох сторін, а не в мережі або у оператора, що здійснює втручання, наскрізне шифрування значно ускладнює життя службам безпеки. Силові структури, які виступають проти Telegram, стверджують, що наскрізне шифрування становить загрозу національній і навіть глобальній безпеці, дозволяючи терористам таємно працювати, використовуючи відкриті засоби зв'язку. Аргументи на користь Telegram підтримують недоторканність приватного життя будь-якою ціною.

Суперечки про конфіденційність знову виникли у зв'язку зі стрілянином 2 грудня 2015 року в Сан-Бернардіно, Каліфорнія, в результаті якої 14 людей загинули і 22 отримали поранення, коли федеральний суддя виніс рішення на користь ФБР, який наказав Apple допомогти "відкрити" закритий телефон, що ймовірно належав стрілку. У статті, опублікованій 17 лютого 2016 року в газеті Washington Post, названій "Apple клянеться протистояти вимогам ФБР зламати iPhone, пов'язаний з атаками на Сан-Бернардіно". Компанія Apple та їх генеральний директор назвали кілька причин, через які вони відмовилися виконувати постанову суду. З текстом статті можна ознайомитися в Інтернеті за адресою (https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html),

Зокрема, компанія Apple неухильно стверджувала, що не змогла розблокувати свій новий iPhone для правоохоронних органів, навіть коли співробітники поліції отримують ордер, оскільки вони сконструйовані таким чином, що ключ дешифрування відсутній у розпорядженні Apple, що, по суті, породжує ще один приклад проблеми наскрізного шифрування. Apple стверджує, що розблокувати телефон зможе тільки користувач телефону або той, хто знає пароль. Уряд спростував той факт, що вони не потребують розблокування функції шифрування, просто відключивши функції, що стирають пам'ять телефону після десяти невдалих спроб входу. В онлайн-зверненні генеральний директор Apple Тім Кук протиставив такий крок небезпечному зниженню рівня безпеки iPhone. "Створений метод, - писав він, - можна буде використовувати знову і знову, на будь-якій кількості пристроїв. У фізичному світі він буде еквівалентний майстер-ключу, здатному відкрити сотні мільйонів замків - від ресторанів і банків до магазинів і будинків. Жодна розумна людина не вважатиме це прийнятним ". Він продовжив: "Протидія

цьому наказу - справа не з легких. Ми вважаємо, що повинні висловитися перед обличчям того, що ми вважаємо надмірним втручанням уряду США".

Остання теза, висунута компанією Apple про те, що Міністерство юстиції США перевищило свої повноваження, є юридичним аргументом, а не технічною позицією, який повторює думку конституціоналістів і захисників приватного життя про те, що держава не має законного права контролювати повідомлення або зазіхати на приватне життя людини без достатніх підстав. Хоча конкретна справа Сан-Бернардіно явно відповідає вимогам ймовірної причини, ідея створення універсального бекдору, який може відкрити будь-який комунікаційний пристрій, як стверджується, спонукає до зловживань з боку влади. У своїй статті 23 лютого 2016 року видання The Atlantic погодилося з тим, що "Apple має рацію: ФБР хоче зламати купу телефонів". Того ж дня The Guardian повідомила, що "ФБР шукає доступ до дюжини iPhone, стверджує Apple".

Як не дивно, та ж позиція на користь конфіденційності була зайнята Конгресом Сполучених Штатів. 1 березня в продовження історії Guardian під назвою "Конгрес повідомляє ФБР, що примус Apple до розблокування iPhone є дурним дорученням", американські законодавці звинуватили Міністерство юстиції США в перевищенні повноважень і підриві конфіденційності. "Шлях до пекла починається з бекдору", - сказав генеральний юрисконсульт Microsoft Бред Сміт на конференції RSA в Сан-Франциско. Сміт кинув виклик індустрії комп'ютерної безпеки, представленої на зборах, щоб виступити разом з Apple в цій важливій справі".

Під час палкої дискусії багато експертів з безпеки, включаючи викривача NSA Едварда Сноудена, оприлюднили позицію, згідно з якою розблокувати телефон не так складно, як передбачалося ФБР. Звертаючись по відеозв'язку з Москви до проекту програм "Спільна справа" на конференції Великої демократії (8-9 березня), Сноуден сказав: "ФБР каже, що Apple має "ексклюзивні технічні засоби" для розблокування телефону. З усією повагою, це нісенітниця собача". ФБР повідомило, що ще до того, як справа дійшла до суду, вони вже знайшли спосіб зламати заблокований iPhone. 29 березня 2016 року в статті в журналі "Фортуна" йшлося: "ФБР може не повідомити Apple, як їм вдалося зламати iPhone."

Правові та геополітичні наслідки у справі Apple-ФБР довгострокові. Слідуючи ініціативі ФБР, очікується, що інші країни будуть наполягати на бекдорах всіх комунікаційних пристроїв, підключених до їх мережі, включаючи телефони громадян США, які виїжджають за кордон. Більш того, тепер, коли iPhone був успішно зламаний, злочинці обов'язково виявлять або заново винайдуть ці методи для участі в нових формах кіберзлочинності і крадіжки особистих даних. Щоб не бути ошуканими злочинцями, уряди можуть прагнути використовувати одні й ті самі методи для розширення спостереження і шпигунства, і навіть різні департаменти всередині одного уряду можуть використовувати ці методи для шпигунства за діяльністю один одного. У відповідних статтях представники різних державних органів розглядають можливість обмеження рівня шифрування, що використовується в наскрізній комунікації.

У сукупності ці події чітко підтверджують усвідомлення того, що ніяке наочне поєднання існуючих в даний час в суспільному надбанні методів забезпечення безпеки і конфіденційності, принаймні без надання допомоги злочинцям і терористам, не забезпечує ні безпеки, ні конфіденційності. Проблема виникає через виняткову залежність від шифрування для досягнення мережевої безпеки або наскрізного зв'язку, а також пов'язаної з цим конфіденційності інформації. Підвищення безпеки тексту, голосу або файлів за рахунок збільшення розміру біта ключа шифрування робить будь-яке спілкування більш безпечним і важким для злому. Посилена безпека захищає бізнес і законослухняних громадян у забезпеченні безпеки та конфіденційності, а також у боротьбі з розкраданням особистих даних. На жаль, таке ж зміцнення безпеки невибірково захищає злочинців і терористів від виявлення, дозволяючи їм діяти приховано і безкарно.

Цей аспект ілюструється на Рис. 104A, де викликаючий абонент 1825A телефонує до приймаючого виклик абонента 1825Q через незахищену мережу, таку як Інтернет 1821, яка схильна до різних способів кібератак, тобто має велику "поверхню атаки" вразливості. Для зменшення "поверхні атаки" шифрування 1026 і дешифрування 1032 використовуються для формування зашифрованого каналу або тунелю 1820 з меншою "поверхнею атаки", ніж мережа 1821. Проблема полягає в тому, що слід використовувати великий ключ шифрування. Як показано в таблиці 1824, чим більший ключ шифрування, тим більше комбінацій існує і тим складніше зламати ключ шифрування. Шифрування використовується для двох цілей: (i) забезпечення мережевої безпеки для запобігання атакам типу "людина посередині" і (ii) забезпечення конфіденційності даних викликаючого абонента через наскрізну систему безпеки. Як видно з рядка 1823, будь-яке поліпшення мережевої безпеки призводить до еквівалентного збільшення наскрізної безпеки. Високий рівень мережевої безпеки корисний для запобігання

атакам з боку зловмисників, проте надмірне наскрізне шифрування - це обопільний меч. Якщо використовується великий розмір ключа, наприклад, AES256 або AES512, система забезпечує "надсекретну" продуктивність мережі і, природно, такий же рівень безпеки для викликаючих абонентів. Однак у разі, якщо абонент підозрюється у злочині або тероризмі, ні оператор мережі, ні уряд не зможуть виявити або проконтролювати його діяльність.

Компроміс розміру ключів є комплексним. Якщо ключ шифрування занадто малий, зловмисники можуть атакувати мережу і її користувачів. Якщо ключ шифрування занадто великий, злочинці можуть використовувати мережу, щоб приховати свою незаконну діяльність і перешкодити зусиллям слідчого з виявлення триваючого шахрайства і неправомірних дій. У корпоративних умовах політика безпеки компанії може повністю відмовитися від наскрізного шифрування, оскільки вона перешкоджає відстеженню дій співробітників або дотриманню вимог корпоративних розслідувань і судових позовів щодо захисту інтелектуальної власності.

Навіть визначення того, який розмір ключа може бути зламаним, а який - безпечним, є складним завданням, що змінюється з розвитком технологій. Посилаючись на таблицю 1824, кількість можливих комбінацій, які повинні бути проаналізовані при атаці "грубою силою", обчислюється як функція розміру ключа шифра. Тоді як ключ 16-біт має тільки 65 тисяч комбінацій, ключ 56-біт має 10^{16} комбінацій, і ключ 128-біт має більш 10^{38} комбінацій. 256-бітовий ключ має комбінації, що перевищують 128-бітовий ключ на 39 порядків величини. Ігноруючи використання функції розпізнавання образів, атака грубою силою намагається зламати код будь-якою комбінацією. У статті EETimes, озаглавленій "Наскільки надійно AES захист від атак 'грубою силою'?" (http://www.eetimes.com/document.asp? doc _ id=1279619), автори вирахували що суперкомп'ютер 2012 року, здатний виконувати атаку "грубою силою" зі швидкістю близько 10,5 петафлопс в секунду. Петафлопс - це тисяча трильйонів, або 10^{15} операцій з плаваючою комою в секунду, або тисяча терафлопсів. Таким чином, 56-бітний ключ вимагає всього 399 секунд, 128-бітний ключ вимагає $1,02 \times 10^{18}$ років, 192-бітний ключ вимагає $1,872 \times 10^{37}$ років, а 256-бітний ключ вимагає $3,31 \times 10^{56}$ років.

Час, необхідний для проведення атаки грубою силою, також змінюється. З моменту написання статті швидкість найшвидшого у світі комп'ютера вже потроїлася. Про це йдеться в статті BBC від 30 липня 2015 року, названій "Суперкомп'ютери: Обама замовляє найшвидший у світі комп'ютер ", дослідники повідомили, що цільова швидкість суперкомп'ютера наступного покоління у двадцять разів вища, ніж у машини-рекордсмена, тобто машини, здатної виконувати один ексафлоп або мільярд операцій з плаваючою комою в секунду. Це означає, що час, необхідний для злому шифрування, з кожним роком скорочується. Іншим, більш новим, підходом до злому шифрування є масова паралельна обробка, аналогічна методу видобутку біткойнів. Замість того, щоб використовувати один суперкомп'ютер, використання тисяч або мільйонів комп'ютерів одночасно дозволить атакувати одночасно, пропорційно скорочуючи час атаки "грубою силою". Сьогодні найшвидші мікропроцесори вже зламали 1,1 терафлопс, тому тридцять тисяч кращих у своєму класі мікропроцесорів, що працюють разом, практично дорівнюють найшвидшим комп'ютерам у світі. Тільки один мільйон мікропроцесорів необхідний для реалізації ексафлопс комп'ютера. Спеціальні ASIC можуть ще більше послабити безпеку, тоді як квантові обчислення обіцяють змінити обчислювальну потужність на багато порядну величину.

У висновку слід зазначити, що шифрування за допомогою великого ключа наскрізного шифрування не є хорошим рішенням для забезпечення конфіденційності та безпеки в комунікаціях. Альтернативний підхід, підтримуваний мережами SDNP і гіперзахищеним зв'язком "Останньої Милі", поділяє наскрізне шифрування і мережеву безпеку, як описано в цьому документі. Як показано на Рис. 104B, зв'язок між клієнтами SDNP 1700A і 1700Q, що представляють абонента, який дзвонить і викликається відповідно, здійснюється по мережі SDNP 1831. Невелика поверхня атаки мережі реалізується анонімним, багатомаршрутним і сітчастим трафіком передачі даних з використанням динамічного шифрування, фрагментації, вставок "сміттєвих" даних, шифрування на кожному хопі, маршрутизованого триканального зв'язку для контролю. Хоча обмін даними "Останньої Милі" і кожен перехід (хопі) всередині SDNP хмари пов'язаний з динамічною зміною облікових даних, цей процес представлений у спрощеній формі за допомогою операції шифрування SDNP 1832 і операції дешифрування SDNP 1833.

Як описано в таблиці 1834 і проілюстровано лінійним сегментом 1830, ці методи в різних комбінаціях забезпечують безпеку, еквівалентну стандартам секретного або надсекретного шифрування, не покладаючись виключно на шифрування. Оскільки лінійний сегмент 1830 рівний, це означає відсутність взаємозалежності між наскрізним шифруванням, показаним на осі Y, і мережевою безпекою, показаною на осі X. Замість цього, рівень мережевої безпеки може

бути скоригований від випадку A до випадку D за допомогою різних методів безпеки SDNP. Ці захисні операції виконуються програмним забезпеченням SDNP таким чином, що абонент, який телефонує і викликається, не знають облікових даних безпеки, що використовуються для транспортування пакетів даних по мережі SDNP 1831 і її різним зонам безпеки. Зокрема, співрозмовники свідомо не беруть участі ні в якому обміні ключами мережі "Останньої Милі". У розподіленій мережі, використання шифрування в SDNP хмарі не пов'язане з безпекою "Останньої Милі", і майстер-ключів для системи не існує. Таким чином, безпека мережі SDNP 1831 не залежить від наскрізного шифрування, виконуваного шифруванням 1026 і дешифруванням 1032 для створення шифрованого каналу або тунелю 1820.

У шифруванні, що використовується SDNP-мережею 1831, не обов'язково використовувати ключі того ж розміру, що і при шифруванні наскрізного тунелю 1820. Як показано на графіку, комерційні та корпоративні програми для забезпечення безпеки наскрізного шифрування можуть використовувати 128-бітовий ключ шифрування (наприклад, AES128), показаний пунктирною лінією 1835, навіть якщо при однохоповому динамічному шифруванні в SDNP хмарі використовується AES256. Насправді, наскрізне шифрування може використовувати RSA або інші шифри без шкоди для мережевої безпеки. Мережа SDNP 1831 все ще захищена шифруванням AES відповідно до військового стандарту FIPS140-2, навіть якщо тунель шифрування 1820 не є наскрізним. Як описано вище, мережа SDNP 1831 захищає від усіх зовнішніх кібератак і атак типу "людина посередині". Наскрізний шифрований тунель 1820 захищає абонентів від втручання оператора мобільного зв'язку та інших хакерських атак. У зв'язку з цим наскрізне шифрування в даному розкритті в першу чергу використовується для забезпечення конфіденційності викликаючого абонента, а не для забезпечення безпеки передачі пакетів даних.

Оскільки наскрізне шифрування може бути збільшено або зменшено в потужності або навіть усунуто без ризику для безпеки мережі, цей метод може бути адаптований для широкого кола програм. Наприклад, якщо шифрування 128-бітового ключа, показане пунктирною лінією 1835, є занадто складним для невеликих компаній або особистого користування, кількість біт може бути зменшено без шкоди для безпеки. У військових або державних додатках довжина ключа шифрування може бути збільшена до 192 біт, 256 біт або навіть 512 біт у міру необхідності. У зв'язку з цим описана SDNP система усуває недоліки сучасного шифрованого зв'язку, пропонуючи функції, недоступні для будь-якого альтернативного додатку, пристрою або мережі.

Адміністрування безпеки - Ще однією ключовою особливістю зв'язку SDNP є унікальний підхід до адміністрування безпеки. Адміністрування безпеки необхідне в багатьох випадках, у тому числі:

- Відстеження комунікацій співробітників відповідно до кадрової політики або розслідувань, що проводяться співробітниками.
- Відстеження та запис звернень співробітників у рамках фінансового аудиту, криміналістичного бухгалтерського обліку або фінансової звітності.
- Документування внутрішньокорпоративних комунікацій в рамках угоди з поглинання і злиття,
- Документування внутрішньофірмових комунікацій в рамках судових розглядів у галузі інтелектуальної власності або корпоративних спорів.
- Виконання вимог про надання комюніке та документів відповідно до повісток до суду та кримінальних розслідувань.
- Виконання правових приписів щодо облікової інформації, відстеження дзвінків і повідомлень, а також доступу до файлів з питань національної безпеки.

За наявності відповідної авторизації адміністратор мережі SDNP може забезпечити доступ мережевого трафіку SDNP призначеному "агенту безпеки SDNP" з метою відстеження зв'язку і контролю даних. Процес створення та включення агента безпеки SDNP включає багаторівневий процес затвердження та автентифікації, який обов'язково виконується до початку спостереження. Для запобігання зловживань ніхто не може самостійно почати спостереження, навіть адміністратор мережі SDNP. Через динамічну природу SDNP як розподілену мережу, позбавлену централізованого управління, що не має ключів провідної мережі і використовує динамічне шифрування і дешифрування SDNP, виконувані з використанням спеціальних облікових даних безпеки зони, що працюють автономно в DMZ серверах, відсутній механізм відновлення даних і виклику розмови постфактум. Дані зберігаються в мережі SDNP тільки протягом короткого періоду часу, зазвичай менше 100 мілісекунд. Будучи розподіленою системою, мережа SDNP за своєю суттю не має централізованого управління, без якого навіть метадані попередніх викликів недоступні. Таким чином, мережа SDNP підтримує відстеження

безпеки тільки апріорі, тобто відстеження призначеним агентом безпеки SDNP має бути здійснено до перехоплення інформації.

Більш того, через динамічну природу фрагментованого зв'язку всередині SDNP хмари, жоден SDNP вузол всередині хмари, тобто за межами шлюзу SDNP, не несе пакетів даних повної розмови. Більшість вузлів передають не більше 5 % даних і зазвичай тільки 10 мс за раз до зміни маршрутизації. Згідно з протоколом SDNP, динамічна маршрутизація постійно перенаправляє комунікацію через різні медіа сервери. Тому хмарний доступ як такий не корисний для відновлення або моніторингу інформації. Хоча пакети даних SDNP хмари можуть бути перехоплені, вони являють собою поєднання незв'язаних звуків, даних, розмов і "сміттєвих" даних. Замість цього, відстеження за допомогою призначеного агента безпеки SDNP може продуктивно здійснюватися тільки в "Останній Милі", де весь набір відповідних пакетів даних обов'язково проходить або всередині клієнтського пристрою, або, переважно, в шлюзі SDNP.

Приклад маршрутизації пакетів даних в рамках спостереження в цілях безпеки схематично показаний на Рис. 105A, де агент безпеки SDNP 1840 контролює взаємодію між клієнтським пристроєм SDNP 1600A і клієнтським пристроєм SDNP 1600H. У той час як розмова відбувається за допомогою пакетів даних, що відправляються з клієнтського пристрою SDNP 1600A через маршрутизатор "Останньої Милі" 1602G на шлюз SDNP 1701U і через хмару SDNP, пакети даних, що відправляються з клієнтського пристрою 1600A закриваються шлюзом SDNP 1700U і надійно направляються до назначеного агента безпеки SDNP 1840. Зокрема, при передачі по UDP пакет даних "Останньої Милі" передає дані SDNP 1 від клієнта SDNP за адресою "IP $C_{1,1}$" на шлюз SDNP за адресою "IP $M_{0,0}$", який виходить з шлюзу SDNP за адресою "IP $M_{0,4}$" і передається по зоні U7 "Останньої Милі" на адресу клієнта SDNP "IP $C_{7,1}$". Під час авторизованого спостереження клоновані дані SDNP-1 надійно передаються агенту безпеки SDNP 1840 за адресою SDNP "IP SA". Клонований пакет даних для спостереження 1841 працює так само, як і груповий виклик SDNP, за винятком того, що дублікати клонів даних невидимі для абонентів. Тому ті, хто дзвонить, не знають, що за ними ведеться спостереження.

Відстеження з метою забезпечення безпеки працює і для вхідних викликів. На Рис. 105B дані SDNP-7 передаються з клієнтського пристрою 1600H з адресою "IP $C_{7,1}$" на шлюз SDNP за адресою "IP $M_{0,4}$". Після передачі через хмару SDNP дані зі шлюзу SDNP доставляються за адресою "IP $M_{0,0}$" у два пункти призначення. Перший пункт призначення, клієнт 1600A за адресою "IP $C_{1,1}$", отримує пакет даних 1640A, що містить дані SDNP 7. Другий пункт призначення, агент безпеки SDNP 1840, отримує ідентичне корисне навантаження, що містить клоновані дані "SDNP data 7" через пакет даних 1842. Доставка пакета даних 1842 невидима для абонентів, тому вони не знають, що за ними ведеться спостереження.

Такий же метод можна застосувати і для спостереження за фрагментованим розподіленим сховищем файлів. Однак замість того, щоб перехоплювати фрагментовані файли даних, агент з безпеки повинен отримати тільки копію відповідних FS посилань. Наприклад, на Рис. 106 показано, що пристрій зберігання файлів SDNP 1700H відправляє пакет даних 1740H, що містить FS посилання 1 з адреси "IP $F_{1,1}$" на адресу шлюзу "IP $M_{0,4}$", який після маршрутизації через хмару SDNP передається клієнту 1600A по пакету даних 1740A. Клоноване корисне навантаження "FS посилання 1" також передається агенту безпеки SDNP 1840 за адресою "IP SA" по пакету даних 1843, відправленим з адреси шлюзу "IP $M_{0,0}$". Як і в разі комунікації в режимі реального часу, власник файлу, клієнт 1600A, не знає про те, що за ним стежить агент безпеки SDNP.

Той же самий механізм спостереження працює для багатомаршрутного зв'язку "Останньої Милі", коли пакети даних надходять і залишають SDNP хмару через більш ніж один шлюз SDNP. Цей випадок ілюструється на Рис. 107, де зв'язок "Останньої Милі" з клієнтського пристрою 1600A включає роздільні пакети даних 1630A, що містять дані корисного навантаження SDNP 1, і пакет даних 1630B, що містить дані корисного навантаження SDNP 2, що надходять в хмару через SDNP шлюзи 1701U і 1701V відповідно. Після хмарної маршрутизації SDNP пакети даних рекомбінуються і відображаються такими, що виходять з хмари у вигляді єдиного пакета даних 1630L з корисним навантаженням, що містить комбіновані дані даних SDNP 3. У процесі роботи шлюзи SDNP з адресами "IP $M_{0,0}$" і "IP $M_{0,11}$" передаються сигнальним сервером для створення клонів вхідних даних SDNP 1 і SDNP 2 з клієнтського вузла $C_{1,1}$ і направлення їх на агента безпеки SDNP 1840 за адресою "IP SA". Клоновані дані відправляються в пакетах даних 1841A і 1841B з використанням тих же методів гіперзахищеного зв'язку, що і для всіх видів передачі даних SDNP, за винятком того, що агент безпеки працює у своїй власній унікальній зоні безпеки, тобто зоні SA, використовуючи облікові дані, недоступні

для будь-якого іншого пристрою. Таким чином, немає жодних записів або доказів того, що призначений агент служби безпеки коли-небудь стежив за тією чи іншою розмовою.

Оскільки дії SDNP зі спостереження є таємними і по суті еквівалентні невидимому конференц-дзвінку, дуже важливо, щоб система SDNP використовувала незалежні перевірки для схвалення і підтвердження використання мережевого спостереження, а також для призначення і підтвердження агента безпеки SDNP, уповноваженого на здійснення спостереження. Агентом безпеки SDNP може бути будь-який клієнт SDNP, крім мережевого адміністратора. Для захисту від пошкодження системи будь-який оператор мережі SDNP або адміністратор SDNP не має права виступати як агент безпеки SDNP, тобто ті, хто управляє мережею, не можуть порушити її можливості для власного користування, навіть якщо їм загрожують або шантажують.

Агентом безпеки SDNP може бути фізична особа, державний агент, уповноважений представник уряду або посадова особа, що займається питаннями законодавства. Конкретні необхідні кваліфікації призначеного агента безпеки варіюються залежно від компанії або країни відповідно до застосованого місцевого законодавства. Агент безпеки SDNP може включати комунікаційний пристрій або комп'ютерний сервер з можливістю запису, зберігання даних і комплексної розшифровки даних. Всі повідомлення, що відправляються з мережі SDNP уповноваженому агенту безпеки SDNP, передаються за допомогою того ж самого гіперзахищеного зв'язку, що і самі повідомлення клієнта, і тому спостереження для забезпечення безпеки не порушує конфіденційність дзвінка або конфіденційність абонента, за винятком спостереження, здійснюваного уповноваженим агентом безпеки.

Більш того, реалізація відстеження і дозволених можливостей авторизованого агента SDNP ні в якому разі не ставить під загрозу цілісність і безпеку мережі. Ніякі операційні подробиці або загальні секрети DMZ не розголошуються оператору мережі або будь-яким агентам безпеки — робота системи SDNP відбувається автоматично і автономно, без втручання або участі людини-оператора, в той час як сервери DMZ забезпечують безпеку, використовуючи облікові дані, специфічні для зони, недоступні через онлайн-доступ. Таким чином, відстеження в цілях безпеки не знижує рівень безпеки системи і не робить мережу SDNP вразливою для кібератак.

Корисне навантаження даних доставляється агенту безпеки SDNP в тій же формі, в якій вона створюється абонентом, що дзвонить. У рамках доставки агенту безпеки SDNP все мережеве шифрування SDNP дешифрується таким чином, щоб у доставлених пакетах даних не було положень про мережеву безпеку. Однак, якщо клієнт використовує наскрізне шифрування, агент безпеки SDNP повинен буде зламати наскрізне шифрування клієнта, якщо тільки клієнт заздалегідь не погодиться поділитися з мережею ключами наскрізного шифрування або використовувати незалежний сервер ключів, доступний в мережі SDNP. Такі наскрізні ключі шифрування і дешифрування в першу чергу включені в метод SDNP для цілей конфіденційності і не пов'язані з якимось шифруванням, що використовується в функції динамічного шифрування SDNP.

Для мінімізації ризику зловживання відстеженням, адміністрування SDNP, що використовується для створення і авторизації призначеного агента безпеки SDNP для відстеження клієнта або групи клієнтів, являє собою багатоетапний процес. Тоді як система SDNP включає положення для здійснення спостереження, за законне застосування цієї функції відповідають оператор мережі, адміністратор мережі, а також уповноважене агентство або агенти. Разом ці сторони несуть персональну відповідальність за те, щоб спостереження здійснювалося на законних підставах і відповідно до законодавства країни, в якій здійснюється спостереження.

Потреба в спостереженні може виникнути в результаті будь-якого числа ситуацій. У компанії скарга інформатора або заява про сексуальне домагання може стати приводом для проведення кадрового розслідування або прискорення судово-медичної експертизи. Повістка до суду, пов'язана з судовим розглядом (потенційно включає постанову про нерозголошення), також може вимагатися у відстеженні. У корпоративних справах спілкування з використанням мережі SDNP компанії, як правило, обмежується корпоративними повідомленнями і не поширюється на приватні та особисті повідомлення. У більшості країн особисті повідомлення захищені, за винятком випадків, коли є підозри в злочинному умислі. У випадках національної безпеки або дій правоохоронних органів, як державні, так і приватні облікові записи SDNP викликаючого абонента можуть підлягати відстеженню. У таких випадках корпоративний оператор мережі SDNP компанії буде здійснювати спостереження за комунікаціями компанії, в той час як незалежний телекомунікаційний оператор мережі SDNP буде єдиним провайдером, здатним здійснювати спостереження за приватними комунікаціями абонента. У деяких країнах уряд повинен представляти затверджену суддею повістку до суду, щоб почати спостереження за

приватними громадянами, в той час як в інших країнах уряд може затверджувати право здійснювати спостереження за будь-якою приватною комунікацією де-факто. У випадках міжнародних комунікацій складніше визначити, які закони застосовні і якою має бути позиція мережі щодо вирішення відстеження дзвінків.

Один з прикладів процесу AAA, який використовується для включення спостереження, проілюстрований на Рис. 108. Процес затвердження спостереження за клієнтом включає в себе мережевого адміністратора 1850, що використовується для організації спостереження, агента безпеки 1840, що відповідає за спостереження за клієнтом, і трьох уповноважених агентів 1851A, 1851B і 1851C, що використовуються для затвердження процесу спостереження, які переважно працюють автономно і незалежно від оператора мережі або мережевого адміністрування. Процес починається з того, що мережевий адміністратор 1850 шукає запит на проведення спостереження 1862 у відповідь на запит про проведення розслідування або постанови суду. Використовуючи командне діалогове вікно 1862, адміністратор визначає номер телефону особи, щодо якого запитується відстеження. Якщо запит на проведення спостереження стосується групи осіб, вони можуть бути введені по одному в систему файлу, в якому перераховані всі сторони, і їх відповідні телефонні номери можуть бути завантажені в систему.

На етапі авторизації 1863 мережевий адміністратор 1850 визначає кандидатуру агента безпеки 1840, рекомендованого для виконання функції спостереження, використовуючи діалогове вікно 1864. У корпоративних справах фізичною особою може бути керівник відділу кадрів, юридичний консультант, член комітету з аудиту та представник незалежної аудиторської фірми, а також незалежний слідчий. У юридичних справах агентом безпеки може бути співробітник юридичної служби, окружний прокурор, агент ФБР або інший належним чином призначений член слідчого комітету, наприклад, у випадках зловживань з боку уряду, таких як спеціальна слідча колегія комітету з розслідування. Потім система перевіряє сервер імен SDNP 1714, щоб упевнитися, що у агента безпеки є обліковий запис SDNP і що він дотримується правил, встановлених компанією або оператором мережі. У деяких випадках, пов'язаних з національною безпекою, до їх затвердження може бути проведено подальше розслідування щодо облікових даних і судимостей агентів безпеки.

Після затвердження агента безпеки на етапі авторизації 1865 запит на проведення спостереження направляється уповноваженим агентам 1851A, 1851B та 1851C, які переглядають інформацію, подану в діалоговому вікні 1866, включаючи ім'я опису предмета, ім'я або посаду агента безпеки, на якого покладено завдання проведення спостереження, очікувану тривалість спостереження і причину проведення спостереження. Кожен уповноважений агент може прийняти або відхилити запит. Правила мережевого оператора або компанії визначають, чи буде операція спостереження схвалена на основі одноголосного схвалення авторизованих агентів або простою більшістю голосів. Особа уповноважених агентів може бути відома, а в корпоративних справах, або в кримінальних справах їх особа може залишатися анонімною, захищеною анонімними засобами зв'язку мережі SDNP.

Після того, як спостереження було схвалено, на кроці адміністрування 1867, база даних 1868 клієнтів оновлюється на сервері імен 1714 для позначки клієнта SDNP, за яким необхідно спостереження, і для ідентифікації клієнта SDNP, авторизованого як агента безпеки, в даному прикладі використовується заштрихований рядок даних. Адреси SDNP у цій базі даних оновлюються щодня, коли адреси SDNP перетасовуються для підтримки відносин між клієнтом, за яким ведеться спостереження, і призначеним агентом безпеки. Після закінчення терміну дії перевірки канал спостереження автоматично розривається. На адміністративному етапі 1869, агенту безпеки SDNP 1840 надсилається посилання, що дозволяє йому отримувати весь поточний зв'язок ідентифікованого клієнта, за яким ведеться спостереження. Використання цієї інформації не є питанням роботи мережі SDNP. Несанкціоноване розголошення агентом безпеки особистої інформації особи може являти собою злочин, за який агент безпеки несе повну відповідальність.

Завдяки цьому інноваційному методу спостереження мережа SDNP здатна, таким чином, надавати підтримку в проведенні кримінальних розслідувань за фактом протиправних дій і потенційної терористичної діяльності, забезпечуючи при цьому безпечне середовище зв'язку для законослухняних громадян. Мережа SDNP здатна безпечно надавати владі приватну комунікацію клієнтів відповідно до законних судових постанов, не ризикуючи конфіденційністю невинних цивільних осіб і не ставлячи під загрозу безпеку глобальної комунікаційної мережі SDNP. Оскільки для виконання судових приписів не використовується бекдор або майстер-ключ, подальший зв'язок по мережі SDNP залишається анонімним і гіперзахищеним. Таким чином, захищена мережа і протокол динамічної комунікації та його гіперзахищений зв'язок

"Останньої Милі" здатні запропонувати функції безпеки, недоступні жодними іншими способами, і повністю виключають ризик сприяння криміналу і тероризму, що виникає в результаті надмірної залежності від наскрізного шифрування, використовуваного OTG і практично всіма додатками для обміну повідомленнями.

Подолання вразливостей протоколу SS7 - Якщо раптом розбіжності ФБР і Apple могли здатися такими, що недостатньо доносять існуючу проблематику у сфері телекомунікацій і безпеки, то ролик "Зламати за 60 хвилин" (http://www.cbsnews.com/news/60-minutes-hacking-your-phone/) наочно продемонстрував серйозну вразливість в області безпеки протоколу сигналізації 7 або SS7, каналом управління сигналом для звичайної бездротової телефонії. Як було наочно продемонстровано на відео, вразливість SS7 піддає кожен смартфон і підключений пристрій потенційному ризику прослуховування пакетів і здійснення кібератак, дозволяючи прослуховувати розмови по бездротовому зв'язку і переглядати SMS-повідомлення, прикріплені файли і картинки, просто знаючи номер телефону людини.

Загальноканальна система сигналізації № 7 — це протокол телефонної сигналізації, розроблений в 1975 році і використовуваний у всіх формах цифрової телефонії в усьому світі. Він включає в себе частину передачі повідомлень або "MTP", що працює на фізичному рівні 1, канальному рівні 2 і мережевому рівні 3 для обробки маршрутизації викликів. Керування наскрізною маршрутизацією здійснюється за допомогою керуючої частини сигнального з'єднання або "SCCP", що працює на транспортному рівні 4. Протокол також включає низку функцій прикладного рівня 7, пов'язаних з тарифікацією, роумінгом і авторизацією викликів. Протокол SS7, хоча і вимушено необхідний, він надзвичайно вразливий для атак і являє собою серйозний ризик для забезпечення безпеки звичайної телефонії.

У квітні 2016 року (https:/ /en.wikipedia.org/wiki/Signalling_System_No._7) комітет з нагляду Конгресу США повідомив, що "використання вразливості, практично, безмежні: від злочинців, які відстежують окремі цілі, до іноземних організацій, що здійснюють економічне шпигунство за американськими компаніями, до національних штатів, які відстежують урядових чиновників США. [...] Вразливість має серйозні наслідки не тільки для приватного життя окремих осіб, а й для американських інновацій, конкурентоспроможності та національної безпеки. [...] Багато інновацій в області цифрової безпеки, такі як багатофакторна автентифікація з використанням текстових повідомлень, можуть виявитися марними."

Кібератаки на протокол SS7, по суті, належать до категорії прослуховування пакетів, перехоплення як контенту, так і метаданих з використанням специфічного форматування інформації SS7 в якості інструкцій. Протокол SS7, по суті, надає інформаційний шаблон, за допомогою якого пакетна інформація може бути інтерпретована. Як показано на Рис. 109, проблема починається з SIM-карти або "модуля ідентифікації абонента", що містить різні види особистої інформації про абонента і його рахунок. Як показано на Рис. , SIM-карта оператора мобільного зв'язку 1880, як правило, видається оператором мобільного зв'язку, використовується для ідентифікації телефону 32 в стільниковій мережі, проілюстрованій антенами 25A, 25B і 25C з відповідними радіоканалами 28A, 28B і 28C. Кожна SIM-карта включає унікальний ідентифікатор, ICCID або "ID карти інтегральної схеми" 18- або 19-значний номер, що використовується для міжнародної ідентифікації SIM-карти. Міжнародний ідентифікатор абонента мобільного зв'язку або IMSI ідентифікує мережу індивідуального оператора, тобто внутрішню мережу, на якій працює SIM-карта. Постачальник послуг місцевої мережі використовує номер IMSI для зв'язку з SIM-картою з метою здійснення дзвінків.

SIM-карта також включає в себе тризначний "мобільний код країни" (mobile country code, MCC) для ідентифікації країни, в якій була виготовлена SIM-карта. При здійсненні міжнародних дзвінків з мобільного телефону, MCC потрібна як частина послідовності набору номера. Приклади MCC включають: 310-316 для США, 234-235 для Великобританії, 460 для Китаю, 208 для Франції, 250 для Росії, 262 для Німеччини, 302 для Канади і 724 для Бразилії. MCC використовується разом з "кодом мобільної мережі" (mobile network code, MNC) для ідентифікації постачальника мережі, який випустив SIM-карту. Повний список кодів наведено на сайті https://en.wikipedia.org/wiki/Mobile_country_code. SIM-карта також включає 15-значний "міжнародний номер абонента мобільної станції" або MSISDN для унікального визначення абонента і типу мережі, в якій працює SIM-карта. На SIM-карті також є телефонний номер абонента і текстовий довідник SMS із записом вхідних і вихідних дзвінків і відправлених текстів, а також інформація про час і дату. В останні роки оператори зв'язку почали використовувати спеціалізовані SIM-картки з так званими захищеними елементами для зберігання реквізитів кредитних карток з метою спрощення мобільних платежів.

Оскільки коди MCC, MNC і MSISDN передаються як частина процесу підключення, країна походження і носій будь-якої SIM-карти і пов'язаний з нею телефонний номер абонента можуть

бути легко ідентифіковані за допомогою впровадження через протокол SS7 і прослуховування пакетів. Передані дані 1881 можуть бути легко використані для відстеження особи викликаючого абонента за допомогою телефонних довідників, онлайн-інформації або соціальних мереж, тобто за допомогою профілювання. Після ідентифікації та зіставлення, номер телефону і SIM-карта можуть бути використані для моніторингу діяльності абонента незалежно від того, куди він може піти. Шифрування не захищає основну інформацію про дзвінки або метадані. Навіть при наскрізному шифруванні пакети даних можуть бути легко ідентифіковані як пакети однієї і тієї ж розмови, перехоплені і збережені для подальших спроб дешифрування.

Крім метаданих і вмісту, місце розташування викликаючого абонента також схильне до ризику вразливості SS7. У будь-якій стільниковій мережі телефон посилає повідомлення на місцеві вишки стільникового зв'язку, визначаючи, чи доступний він у конкретній стільниковій мережі. Ці пакети реєстрації відправляються через регулярні проміжки часу. Моніторинг цих пакетів дозволяє визначити місце розташування телефону з певною SIM-картою, навіть якщо телефон не використовується і GPS вимкнений. Таким чином, місце розташування і пересування абонента можна відстежити без його відома.

Незважаючи на властиві SS7 вразливості, гіперзахищена комунікація "Останньої Милі", виконана відповідно до захищеної динамічної мережі і протоколу, відбиває атаки на SS7 шляхом маскування важливих даних про дзвінки по "Останній Лінії". Зокрема, гіперзахищена комунікація "Останньої Милі" пропонує значні переваги в галузі безпеки порівняно зі звичайною телефонією або OTT-інтернет комунікаціями, включаючи такі як:

- Гіперзахищена комунікація "Останньої Милі" не розкриває номер телефону або IP-адресу викликаючої або викликаної сторін, навіть якщо ця сторона не є SDNP клієнтом.

- Гіперзахищена комунікація "Останньої Милі" не визначає, чи є послідовні пакети даних частиною одного і того ж виклику або являють собою незв'язані пакети даних з різним призначеннями.

- Приховуючи специфіку викликів пакетів даних, гіперзахищена комунікація "Останньої Милі" приховує метадані про час виклику.

- Гіперзахищена комунікація "Останньої Милі" динамічно кодує корисне навантаження, запобігаючи несанкціонованому доступу до вмісту пакетів і захищаючи конфіденційність голосового, відео- та текстового зв'язку, а також зображень, файлів та іншого вмісту.

Отже, як було описано вище, взаємодія за допомогою описаної захищеної динамічної мережі та протоколу і гіперзахищеної комунікації "Останньої Милі" не схильна до впливу вразливості SS7. Оскільки SDNP-комунікація відбувається за пропрієтарним протоколом і здійснюється за допомогою кодованого корисного навантаження, дані виклику або вміст не можуть бути витягнуті з SDNP-пакету даних навіть для пакетів, що передаються по відкритому незашифрованому каналу, такому як 2G, 3G або 4G/LTE-телефонія. Таким чином, прослуховування пакетів неефективне при проведенні кібератак при SDNP шифруванні і фрагментованій передачі даних.

SDNP маскування - Враховуючи вищесказане, єдиний вплив, який вразливість SS7 надає на SDNP-комунікацію, полягає у виявленні місця розташування викликаючого абонента. Оскільки номер телефону в SIM-карті оператора пов'язаний з ідентифікацією кожного користувача, при включенні мобільного телефону він обов'язково зв'язується з найближчими вишками стільникового зв'язку, навіть якщо не відбувається телефонного дзвінка. Ця інформація про вежі стільникового зв'язку може бути використана для тріангуляції місця розташування користувача і відстеження подорожей абонента навіть при вимкненому GPS. Оскільки таке несанкціоноване відстеження покладається на протокол SS7, пристрої, що використовують SIM-карти звичайного оператора, вразливі для відстеження місця розташування, навіть ті, які працюють в якості SDNP-клієнтів.

Як показано на спрощеній мережевій схемі на Рис. 110, удосконалення гіперзахищеної комунікації "Останньої Милі", згадуваної тут як "SDNP маскування", перешкоджає відстеженню абонента в цілому. Для реалізації цієї функції звичайна SIM-карта оператора 1880 замінюється на SDNP SIM-карту 1882. SIM-карта SDNP зареєстрована на ім'я оператора мережі SDNP, а не на ім'я абонента, тому на SIM-карті SDNP 1882 не міститься ніякої персональної інформації про абонента. SIM-карта SDNP 1882 аналогічна SIM-карті передплаченого мобільного зв'язку в тому, що вона має доступ до мережі, але не містить особистих даних. Замість цього особисті дані власника облікового запису надійно зберігаються на серверах імен SDNP і недоступні для хакерів або не схильні до кібератак.

У процесі експлуатації SDNP маскування приховує справжню особистість власника, використовуючи SIM-карту 1882, відому тільки оператору мережі SDNP. Таким чином, номер телефону, що знаходиться всередині SIM-карти, використовується для встановлення зв'язку 1-

го рівня і з' єднання 2-го рівня 28B між мобільним телефоном 32 і мобільною вишкою 25B, але не для забезпечення маршрутизації. Замість цієї адреси джерела і призначення пакетів даних для маршрутизації "Останньої Милі" керуються програмою SDNP 1335A і шлюзом SDNP 1601A відповідно до інструкцій сигнального сервера SDNP 1603A.

При проходженні через SDNP-шлюз 1601A виклики з програми SDNP відображаються з номером, відмінним від номера SIM-карти. Цей переклад з номера фізичної SIM-карти на номер телефону SDNP виконується сервером імен SDNP 1604A, який під час маршрутизації викликів перетворює номер телефону SDNP на номер SIM-карти відповідно до таблиці перекладу 1885, тим самим маскуючи фізичний номер SIM-карти під будь-якого користувача. При використанні SDNP маскування справжня особистість власника телефону повністю ховається. Щоб зробити дзвінок клієнту SDNP, зовнішні абоненти роблять дзвінок з SDNP #, навіть якщо вони самі не є клієнтами SDNP. Мережа SDNP автоматично направляє виклик клієнту SDNP, ніколи не розкриваючи номер телефону на SIM-карті. Аналогічним чином, клієнт SDNP відправляє виклик абоненту, який не є клієнтом SDNP, а одержувач виклику бачить вхідний виклик з SDNP #, а не з номера SIM-карти. Таким чином, SDNP виконує в телефоні функції, аналогічні функціям шлюзу NAT в інтернет-комунікації, за винятком того, що система SDNP є мережею реального часу, а Інтернет - ні.

Оскільки справжня особистість користувача телефону 32 ніколи не розкривається дзвінком 28B, тріангуляція місцезнаходження телефону не корисна, оскільки його користувач і все спілкування залишаються анонімними. Як таке, відстеження місцезнаходження невпізнаних мобільних телефонів не вигідно хакерам, але вирішує проблему вразливості протоколу SS7. У разі, якщо клієнт SDNP подорожує по всьому світу, мандрівник може придбати місцеву передплачену SIM-карту і прив'язати її до свого SDNP номера. Абонент SDNP все одно буде отримувати дзвінки на свій SDNP номер, але "Остання Лінія" буде відбуватися з використанням місцевої SIM-карти, що дозволить уникнути плати за роумінг. Таким чином, один телефонний номер SDNP функціонує як глобальний номер без витрат на міжміський зв'язок.

SDNP підмережі - Використовуючи свої унікальні комутатори на основі програмних вузлів зв'язку, хмара зв'язку SDNP може бути розгорнута віддалено в будь-якій мережі взаємопов'язаних комп'ютерів, як приватних, так і публічно розміщених. Прикладами серверних мереж можуть служити приватні публічно орендовані мережі, наприклад, розміщені на серверах Microsoft, Google і Amazon. На Рис. 111 показано дві хмари SDNP, розгорнуті у двох окремих серверних мережах. Як показано на Рис. , у хмарі SDNP, що складається з серверів 1901A, 1901B, 1901C і 1901D, розміщені вузли зв'язку SDNP $M_{0,0}$, $M_{0,4}$, $M_{0,7}$ і $M_{0,8}$, відповідно. Друга хмара SDNP, що складається з серверів 1902A, 1902B і 1902C, розміщує SDNP вузли $M_{10,0}$, $M_{10,1}$ і $M_{10,2}$ відповідно. Оскільки вони використовують окремі облікові дані безпеки, зони Z0 і Z10 відповідно, обидві хмари SDNP повністю відрізняються одна від одної і не можуть безпосередньо обмінюватися інформацією. Один SDNP клієнт, показаний у вигляді мобільного телефону 32 із запущеним додатком SDNP 1335, може, однак, з належною авторизацією отримати доступ до обох "хмар", навіть якщо вони розміщуються у різних провайдерів з оренди комп'ютерних серверів. Як показано в прикладі, клієнт SDNP $C_{1,1}$ має доступ до SDNP вузла шлюзу $M_{0,7}$ в хмарі зони Z0 за допомогою взаємодії гіперзахищеної "Останньої Милі" через маршрутизатор 1910 і доступ до SDNP вузла шлюзу $M_{10,0}$ в хмарі зони Z10 за допомогою взаємодії гіперзахищеної "Останньої Милі" через той самий маршрутизатор 1910 без ризику змішування розмов чи пакетів даних.

Доступ до двох незалежних хмар здійснюється через загальний комунікаційний додаток UI/UX 1920. Доступ до кожної хмари поділено на окремі діалогові "пісочниці" 1921A і 1921B. Хоча інформація може бути завантажена з персонального аккаунта "пісочниці" 1921A в телефон, експорт даних з бізнес-аккаунта "пісочниці" 1921B залежить від бізнесу та адміністрації безпеки компанії.

Підключення пристрою до хмар SDNP вимагає встановлення програми SDNP, у вигляді програмного забезпечення або мікропрограми, в пристрій. Встановлення включає в себе (i) завантаження програми (ii) підтвердження ідентифікації пристрою за допомогою згенерованого в мережі SDNP коду авторизації (iii) встановлення ідентифікаційних даних і (iv) отримання дозволу на підключення до конкретної "хмари" SDNP. Після активації програма SDNP створює гіперзахищене з'єднання "Останньої Милі" до незалежної SDNP хмари. У багатьох випадках перевірка автентифікація користувача для облікового запису підприємства більш складна, ніж та, яка необхідна для доступу до особистого облікового запису, і може вимагати застосування багатофакторних методів автентифікації.

У зв'язку з тим, що зв'язок SDNP заснований на програмному забезпеченні, з різними і окремими обліковими записами безпеки для кожної хмари зв'язку, відсутня взаємодія між будь-

якими встановленими мережами зв'язку SDNP, навіть якщо вони розміщені на одних і тих же серверах. Оскільки облікові дані безпеки, що відносяться до конкретних зон, унікальним чином визначають кожну налаштовану хмару SDNP, ніякі дві хмари SDNP не схожі одна на одну і, отже, не можуть безпосередньо обмінюватися даними. Перевагою є те, що кілька SDNP хмар можуть співіснувати в межах однієї серверної мережі без ризику витоку даних. Доступ до бізнес-мережі контролюється відповідно до вимог власника хмари. Таким чином, об'єднання двох облікових записів і хмар зв'язку заборонено при спільному використанні загальних хост-серверів, що працюють з однаковою безпекою, як якщо б для підключення до двох окремих мереж потрібно було б два різних телефони. Автономія зональних хмар SDNP, або "підмереж", додатково демонструється на Рис. 112, де сервери 1901A, 1901B, 1901C і 1901D розміщують одночасно дві хмари - одна хмара, що складається із зональних вузлів зв'язку Z0 SDNP $M_{0,0}$, $M_{0,4}$, $M_{0,7}$ и $M_{0,8}$ відповідно, і друга, що складається з зональних вузлів зв'язку SDNP Z7 $M_{7,0}$, $M_{7,4}$, $M_{7,7}$ и $M_{7,8}$, відповідно. Незважаючи на роботу всередині одних і тих же серверів, гіперзахищена комунікація за допомогою встановлених SDNP протоколів запобігає будь-якому прямому обміну даними. Доступ, таким чином, управляється комунікацією "Останньої Милі", а не за допомогою прямого обміну даними між хмарами.

SDNP зв'язок не обмежується приватними орендованими публічно доступними серверами, але також може бути налаштований для різних типів корпорацій або державних установ. В основному, приватні корпорації часто воліють розміщувати свої власні мережі, особливо в критично важливих для бізнесу додатках. Прикладами приватних мереж є FedEx, Walmart, IBM тощо. З метою забезпечення конфіденційності мережі, що використовуються науково-дослідними інститутами, університетами та медичними центрами, також часто воліють розміщувати самостійно. Мережі приватних серверів також використовуються для розміщення глобальних хмарних бізнес-додатків, таких як SalesForce.com, Box.com, Dropbox, eTrade, SAP тощо; платформ електронної комерції та мереж порівняльного шопінгу, таких як eBay, Amazon.com, Priceline.com, e-Insurance; потокових медіа-послуг, таких як YouTube, Amazon Prime, Netflix, Hulu, Comcast Xfinity; а також соціальних медіа, таких як Facebook, Twitter і Snapchat.

У більш великих корпораціях IT-відділ може прийняти рішення про управління окремими мережами для материнської компанії та її дочірніх компаній. Однак у багатьох приватних компаніях витрати на інфраструктуру вважаються важливим фактором при проектуванні мереж. Замість підтримки двох абсолютно різних апаратних систем, система SDNP надає компанії можливість розгортати свої мережі, використовуючи комбінацію окремих і спільно використовуваних серверних ресурсів. Як показано на Рис. 113, дві юридичні особи, наприклад материнська корпорація та її дочірня компанія, спільно розміщують мережу серверів, що складається як з окремих, так і із загальних серверів. Зокрема, на серверах 1903, 1904B, 1904C і 1904D розміщені відповідні вузли зв'язку зони Z7 $M_{7,0}$, $M_{7,4}$, $M_{7,7}$ і $M_{7,8}$ відповідно для материнської корпорації, а на серверах 1901A, 1901B, 1901C і 1903 розміщені відповідні вузли зв'язку зони Z0 $M_{0,0}$, $M_{0,4}$, $M_{0,7}$ і $M_{0,8}$ для місцевої дочірньої компанії. Як показано на прикладі, на сервері 1903 розміщено два вузли зв'язку SDNP, а саме вузол $M_{7,0}$ для головної компанії і вузол $M_{0,8}$ для дочірньої компанії. Через їх різні політики безпеки, ніякі дані не передаються безпосередньо між батьківським і дочірнім SDNP хмарами, навіть якщо сервер 1903 та інші (не показані) спільно використовуються обома організаціями. Хоча співробітники, як правило, обмежені доступом тільки до "хмар" свого роботодавця, у разі корпоративних співробітників може знадобитися доступ до обох "хмар". Правильно авторизовані користувачі, як показано в додатку SDNP UI/UX 1920, включають окремі діалогові "пісочниці" 1921C і 1921D для різних юридичних осіб. Таким чином, один мобільний телефон або планшет може отримати доступ до кількох SDNP хмар різних юридичних осіб без ризику змішування даних, як якщо б у користувача було кілька телефонів.

Багатопрофільна функція програми SDNP, що використовує облікові дані безпеки гіперзахищеної "Останньої Милі" для дозволу або заборони доступу до декількох SDNP хмар, підтримує необмежену кількість профілів облікових записів з однієї програми SDNP. На Рис. 114, наприклад, клієнт SDNP $C_{1,1}$ може здійснювати глобальні дзвінки без плати за міжміський зв'язок по зоні Z99 глобального телекомунікаційного вузла SDNP, що складається з серверів 1909A-1909E, що хостують SDNP-вузли M99,1-M99,5 відповідно, а також отримувати доступ до інших хмар, наприклад, до хмари гіперзахищенної "Останньої Милі", яка забезпечує доступ до декількох облікових записів, таких як, наприклад, корпоративна хмара зони Z9, що включає сервери 1905A, 1905B і 1905C, що хостують SDNP-вузли $M_{9,0}$, $M_{9,4}$ і $M_{9,8}$, а також для виклику абонентів хмари зони Z0 через сервери 1901A, 1901B і 1901C, що хостують SDNP-вузли $M_{0,0}$, $M_{0,4}$ і $M_{0,8}$ відповідно. Привілеї доступу до будь-якої цієї хмари реалізуються через комунікацію

"Останньої Милі" до шлюзу SDNP і керуються сигнальним сервером SDNP системи і сервером імен SDNP, що використовується для адміністрування авторизованих користувачів.

SDNP зв'язок рівною мірою застосовний у мережах з високою безпекою і обмеженим доступом, необхідних для уряду і безпеки. Наприклад, у США зв'язок з обмеженим доступом необхідний різним відомствам, включаючи місцеві правоохоронні органи і правоохоронні органи штату, ФБР, Національну гвардію США, Агентство національної безпеки США, збройні сили США (окремо і спільно), державний департамент США, а також мережі серверів Конгресу і законодавчих органів. В інших країнах також існують окремі мережі для різних державних установ.

Для підтримки доступу до конкретної хмари за принципом "у міру необхідності", вкладені архітектури підмережі можуть бути реалізовані з використанням методів і технологій зв'язку SDNP. Наприклад, на Рис. 115 вкладена хмарна структура SDNP включає захищену хмару, що складається з орендованих комп'ютерних серверів 1907A і 1907D, що хостують вузли зв'язку SDNP $M_{0,0}$, $M_{0,4}$, $M_{0,5}$ і $M_{0,9}$ відповідно. Зв'язок у цій зовнішній мережевій "оболонці" включає облікові дані безпеки зони Z0 і відображається в діалоговому вікні "секретного" рівня в "пісочниці" 1912E, як показано в SDNP комунікаторі 1920. Вкладена "хмара" також включає в себе внутрішнє ядро підвищеної безпеки з обліковими даними безпеки зони Z8, що складається з розміщених урядом серверів 1906A, 1906B і 1906C і відповідних SDNP серверних вузлів $M_{8,0}$, $M_{8,2}$ і $M_{8,4}$. Для того щоб клієнт $C_{1,1}$ отримав доступ до ядра зони Z8, він повинен мати "цілком секретний" допуск до секретної інформації, і спілкуватися через захищену комунікаційну "пісочницю" 1921F. Одним із прикладів застосування цієї технології в уряді є Держдепартамент США, де надсекретна комунікація в зоні Z8 обмежена доступом послів і держсекретаря, в той час як інші співробітники посольств США по всьому світу обмежені "секретною" гіперзахищеною комунікацією за допомогою політик безпеки зони Z0.

ФОРМУЛА ВИНАХОДУ

1. Спосіб передачі з клієнтського пристрою в хмару пакетів даних, що складаються з пакетів даних, які входять в комунікацію, хмара складається з множини медіа-вузлів і множини вузлів шлюзу, в якому:

клієнтський пристрій передає запит на дзвінок на сигнальний сервер, при цьому запит на дзвінок містить контактну інформацію щодо сторони, яку потрібно викликати;

сигнальний сервер розробляє маршрути для комунікації, спрямовані щодо сторони, яку потрібно викликати, перший маршрут містить перший вузол шлюзу, а другий маршрут містить другий вузол шлюзу;

ні перший вузол шлюзу, ні другий вузол шлюзу, ні будь-який інший медіа-вузол не мають інформації, що описує або перший, або другий маршрут в цілому;

сигнальний сервер передає пакети інструкцій маршрутизації на клієнтський пристрій, перший вузол шлюзу та другий вузол шлюзу, відповідно; й

у відповідь на пакет інструкцій маршрутизації клієнтський пристрій передає перший пакет даних у комунікації з клієнтського пристрою на перший вузол шлюзу та другий пакет даних у комунікації з клієнтського пристрою на другий вузол шлюзу.

2. Спосіб за п. 1, який **відрізняється** тим, що включає передачу першого пакета даних з клієнтського пристрою на перший вузол шлюзу через перше фізичне середовище та передачу другого пакета даних і з клієнтського пристрою на другий вузол шлюзу через друге фізичне середовище.

3. Спосіб за п. 2, який **відрізняється** тим, що перше фізичне середовище складається зі стільникового телефонного зв'язку, а друге фізичне середовище складається з Wi-Fi-каналу. 4. Спосіб за п. 2, який **відрізняється** тим, що включає забезпечення першого пакета даних з першою IP-адресою джерела та забезпечення другого пакета даних з другою IP-адресою джерела.

5. Спосіб за п. 2, який **відрізняється** тим, що перше фізичне середовище містить стільниковий телефонний зв’язок, модульований з використанням першої несучої частоти, а друге фізичне середовище містить стільниковий телефонний зв'язок, модульований з використанням другої несучої частоти.

6. Спосіб за п. 2, який **відрізняється** тим, що перше фізичне середовище містить канал Wi-Fi, модульований з використанням першої несучої частоти, а друге фізичне середовище містить канал Wi-Fi, модульований з використанням другої несучої частоти.

7. Спосіб за п. 1, який **відрізняється** тим, що включає забезпечення першого пакета даних з першою IP-адресою джерела та забезпечення другого пакета даних з другою IP-адресою джерела.

8. Спосіб за п. 7, який **відрізняється** тим, що клієнтський пристрій передає перший та другий пакети даних на перший та другий вузли шлюзу відповідно через маршрутизатор, при цьому спосіб додатково включає забезпечення першого пакета даних з першою MAC-адресою джерела та забезпечення другого пакета даних з другою MAC-адресою джерела.

9. Спосіб за п. 1, який **відрізняється** тим, що перед тим, як сервер сигналізації передає пакети інструкцій маршрутизації на клієнтський пристрій, перший вузол шлюзу та другий вузол шлюзу, відповідно, сигнальний сервер зв'язується з сервером імен з контактною інформацією щодо сторони, яку потрібно викликати.

10. Спосіб за п. 9, який **відрізняється** тим, що контактна інформація щодо сторони, яку потрібно викликати, включає конфіденційну ідентифікацію сторони, яку потрібно викликати, і в якому сервер імен перетворює конфіденційну ідентифікацію в SDNP-адресі сторони, яку потрібно викликати, при цьому сигнальний сервер використовує SDNP-адресу сторони, яку потрібно викликати, при розробці маршрутів для комунікації від клієнтського пристрою до сторони, яку потрібно викликати.

11. Спосіб за п. 9, який **відрізняється** тим, що контактна інформація щодо сторони, яку потрібно викликати, містить номер телефону, і в якому сервер імен перетворює номер телефону в адресу вузла шлюзу, найближчого до місця розташування сторони, яку потрібно викликати, при цьому сигнальний сервер використовує адресу вузла шлюзу, найближчого до місця розташування сторони, яку потрібно викликати, при розробці маршрутів зв'язку від клієнтського пристрою до сторони, яку потрібно викликати.

12. Спосіб за п. 9, який **відрізняється** тим, що клієнтський пристрій передає інформацію серверу імен кожного разу, коли пристрій під'єднується до мережі.

13. Спосіб за п. 1, який **відрізняється** тим, що пакет інструкцій маршрутизації, який сигнальний сервер відправляє на клієнтський пристрій, містить першу інструкцію маршрутизації для відправки першого пакета даних на перший вузол шлюзу та другу інструкцію маршрутизації для відправки другого пакета даних на другий вузол шлюзу.

14. Спосіб за п. 13, який **відрізняється** тим, що кожний з першого вузла шлюзу та другого вузла шлюзу має першу адресу для зв'язку з клієнтським пристроєм і другу адресу для зв'язку всередині хмари.

15. Спосіб за п. 1, який **відрізняється** тим, що включає забезпечення множини сигнальних серверів, у якому сигнальні сервери розподіляють завдання маршрутизації пакетів від клієнтського пристрою до сторони, яку потрібно викликати, і в якому жоден сигнальний сервер не має інформації, що описує всю маршрутизацію пакета.

16. Спосіб за п. 1, який **відрізняється** тим, що додатково включає приховування вмісту щонайменше одного з першого пакета даних і другого пакета даних з використанням комбінації способів приховування, причому способи приховування включають шифрування, скремблювання, введення небажаних даних, розділення та/або змішування й основується на стані.

17. Спосіб за п. 16, який **відрізняється** тим, що стан включає час, номер вузла, ідентифікацію мережі або місце розташування GPS.

18. Спосіб передачі від клієнтського пристрою в хмару пакетів даних, що складаються з пакетів даних, які входять в комунікацію; хмара складається з множини медіа-вузлів і множини вузлів шлюзу, який включає:

передачу першого пакета даних з клієнтського пристрою на перший вузол шлюзу через щонайменше один маршрутизатор;

забезпечення першого пакета даних з першою IP-адресою джерела та першою MAC-адресою джерела;

передачу другого пакета даних від клієнтського пристрою на другий вузол шлюзу через щонайменше один маршрутизатор; і

забезпечення другого пакета даних з другою IP-адресою джерела та другою MAC-адресою джерела.

19. Спосіб за п. 18, який **відрізняється** тим, що включає передачу першого пакета даних від клієнтського пристрою на перший вузол шлюзу через перше фізичне середовище та передачу другого пакета даних і з клієнтського пристрою на другий вузол шлюзу через друге фізичне середовище.

20. Спосіб за п. 19, який **відрізняється** тим, що перше фізичне середовище складається зі стільникового телефонного зв'язку, а друге фізичне середовище складається з Wi-Fi-каналу.

21. Спосіб за п. 19, який **відрізняється** тим, що перше фізичне середовище містить стільниковий телефонний зв'язок, модульований з використанням першої несучої частоти, а друге фізичне середовище містить стільниковий телефонний зв'язок, модульований з використанням другої несучої частоти.

22. Спосіб за п. 19, який **відрізняється** тим, що перше фізичне середовище містить канал Wi-Fi, модульований з використанням першої несучої частоти, а друге фізичне середовище містить канал Wi-Fi, модульований з використанням другої несучої частоти.

23. Спосіб за п. 18, який **відрізняється** тим, що додатково включає приховування вмісту щонайменше одного з першого пакета даних і другого пакета даних з використанням комбінації способів приховування, причому способи приховування включають шифрування, скремблювання, введення небажаних даних, розділення та/або змішування й основується на стані.

24. Спосіб за п. 23, який **відрізняється** тим, що стан включає час, номер вузла, ідентифікацію мережі або місце розташування GPS.

25. Спосіб передачі від клієнтського пристрою в хмару через щонайменше один маршрутизатор пакетів даних, що складаються з пакетів даних, які входять в комунікацію; хмара складається з множини медіа-вузлів і множини вузлів шлюзу, який включає:

забезпечення першого пакета даних з першою IP-адресою джерела та першою MAC-адресою джерела; та

забезпечення другого пакета даних з другою IP-адресою джерела та другою MAC-адресою джерела.

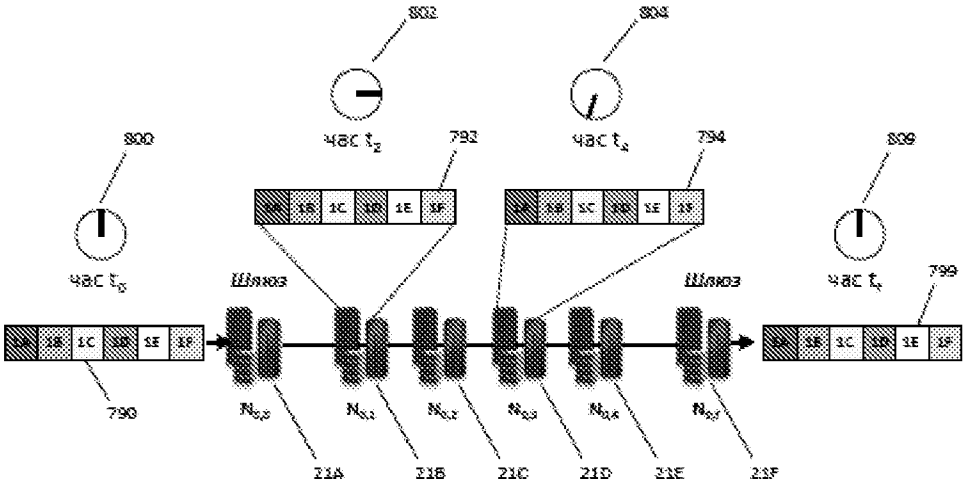


Рис. 1

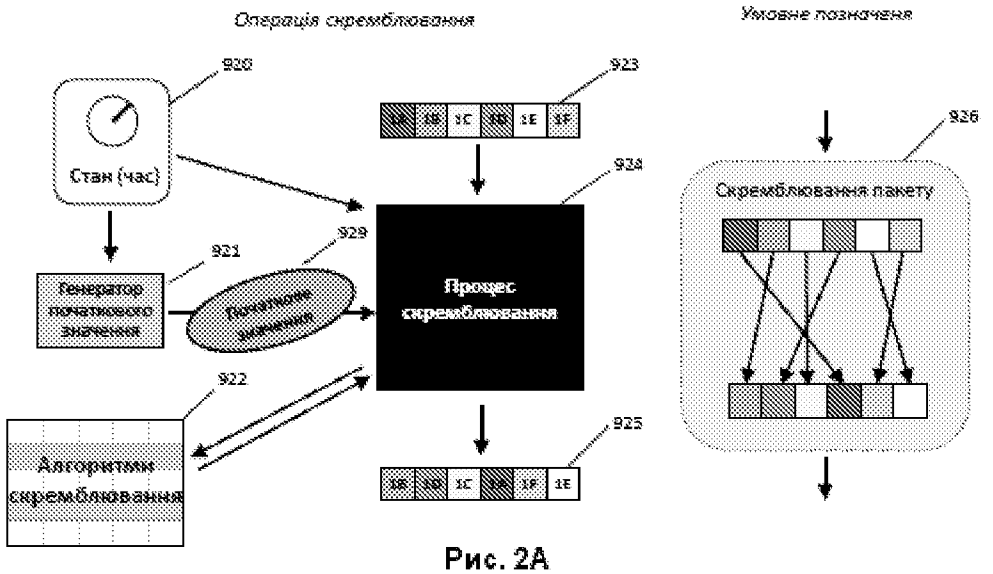


Рис. 2A

Дескремблювання пакету

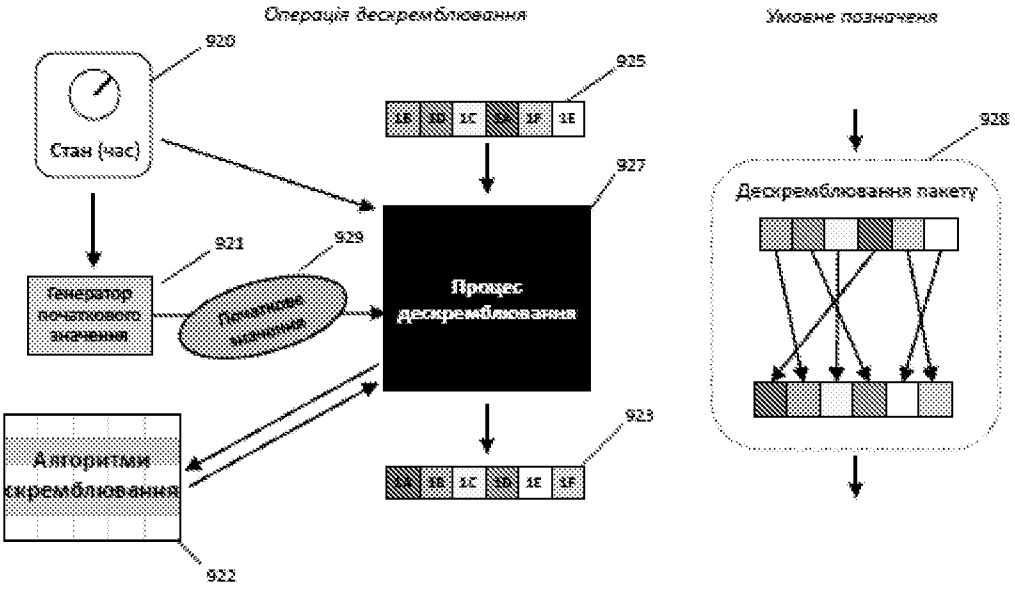


Рис. 2B

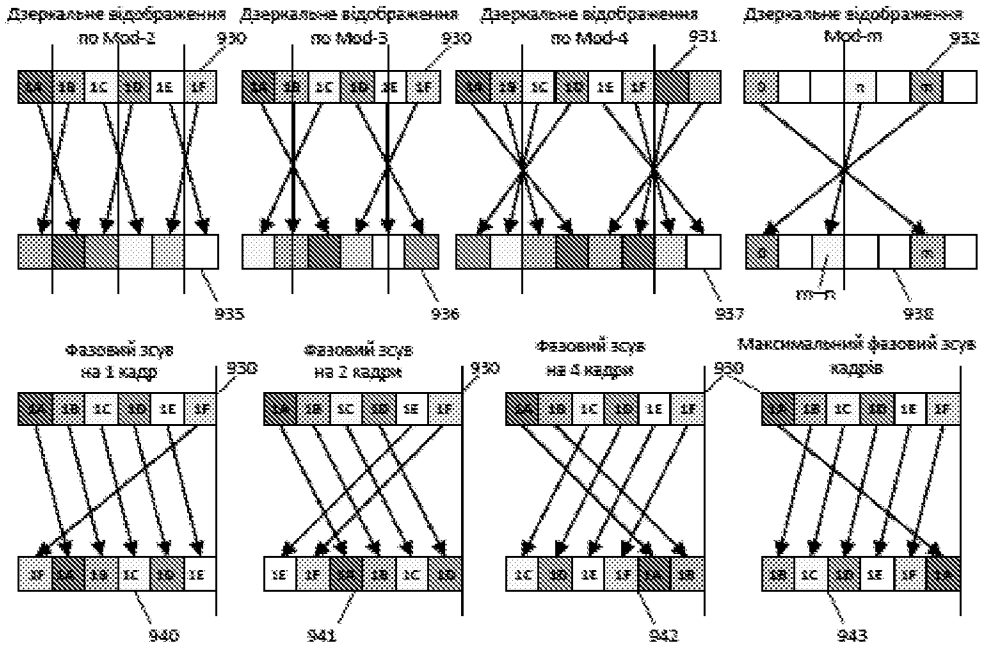

Дзеркальне відображення по Mod-2
930
Дзеркальне відображення по Mod-3
930
Дзеркальне відображення по Mod-4
931
Дзеркальне відображення Mod-m
932
935
936
937
m−n
938
Фазовий зсув на 1 кадр
930
Фазовий зсув на 2 кадри
930
Фазовий зсув на 4 кадри
930
Максимальний фазовий зсув кадрів
940
941
942
943

Рис. 2C

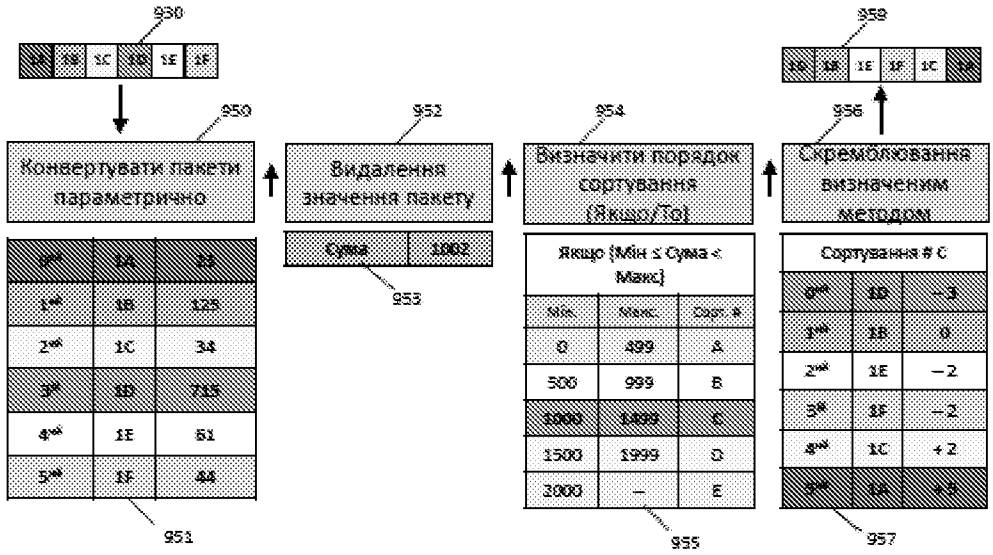

930
950
Конвертувати пакети параметрично
952
Видалення значення пакету
Сума
1002
953
954
Визначити порядок сортування (Якщо/То)
Якщо (Мін ≤ Сума < Макс)
Мін.
Макс.
Сорт. #
0
499
A
500
999
B
1000
1499
C
1500
1999
D
2000
–
E
955
956
Скремблювання визначеним методом
958
Сортування # C
0x00
1B
−3
0x01
1B
0
0x02
1E
−2
0x03
1F
−2
0x04
1C
+2
0x05
1A
+3
951
957

Рис. 2D

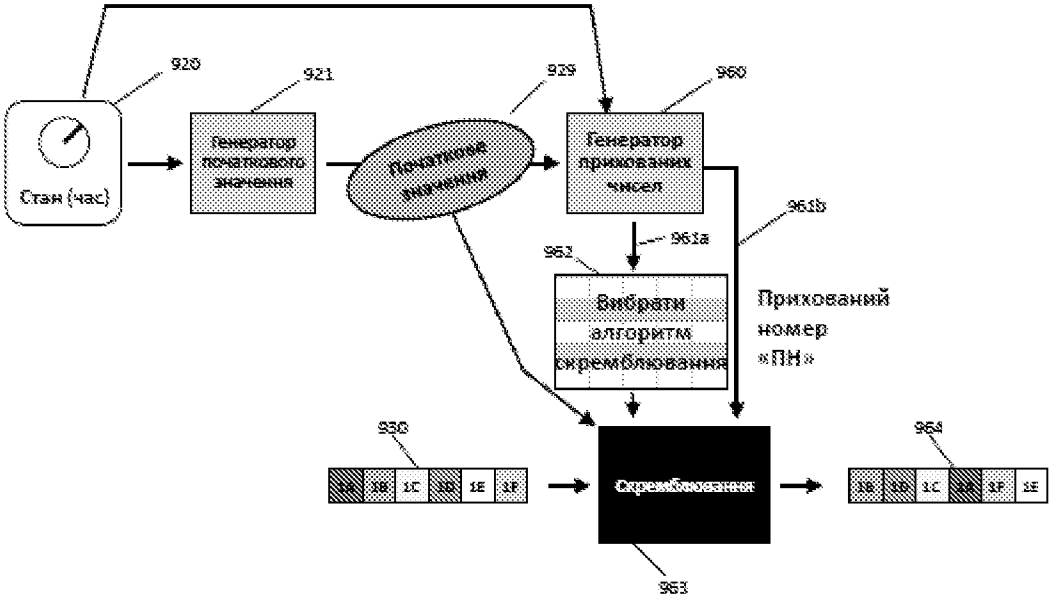

920
921
929
960
961b
961a
962
Стан (час)
Генератор початкового значення
Початкове значення
Генератор прихованих чисел
Вибрати алгоритм скремблювання
Прихований номер «ПН»
930
964
Скремблювання
963

Рис. 2E

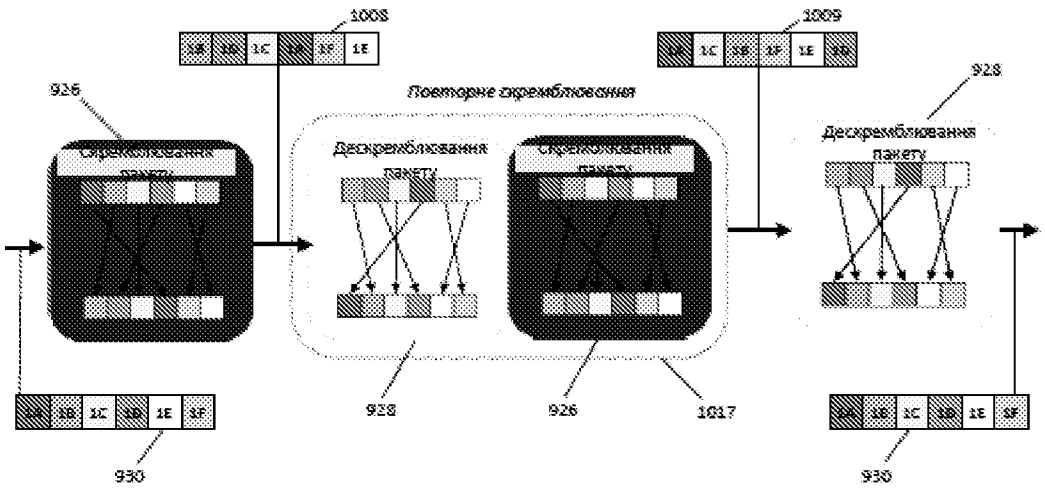

1008
1009
926
Повторне скремблювання
Дескремблювання пакету
928
928
926
1017
930
930

Рис. 3

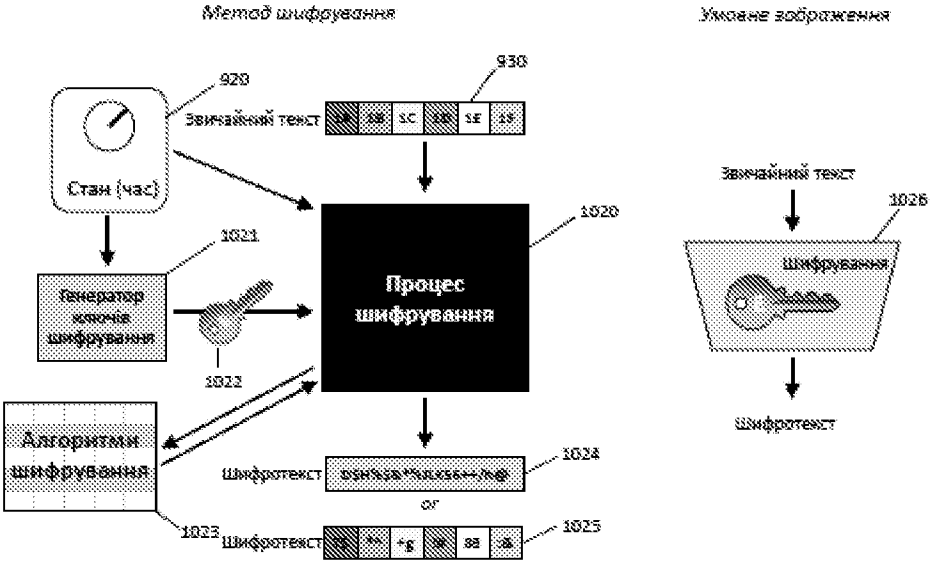


Рис. 4A

Дешифрування пакету

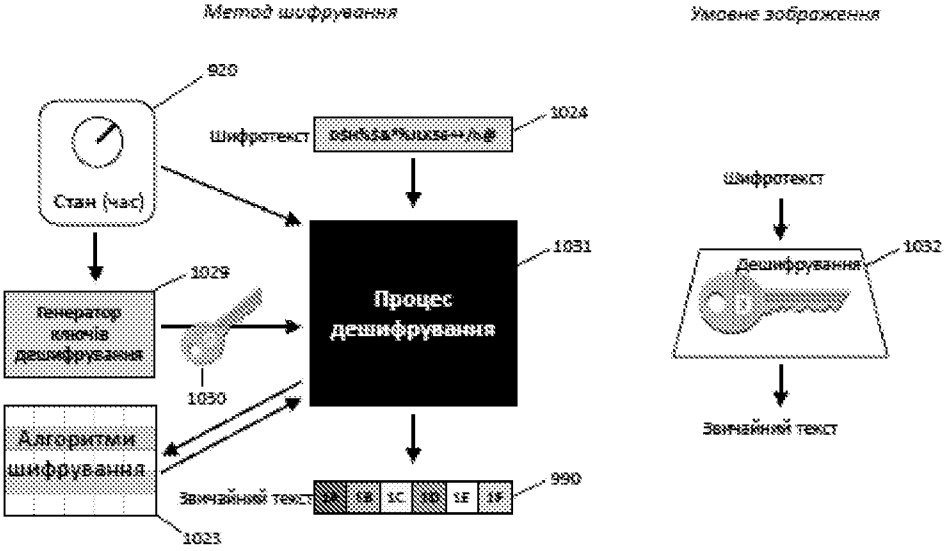


Рис. 4B

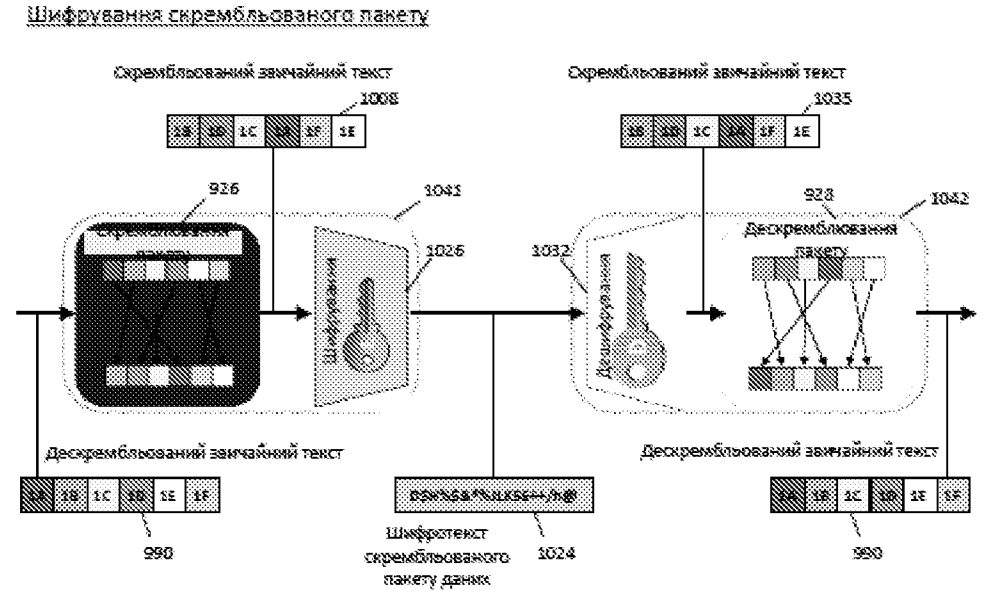

Шифрування скрембльованого пакету
Скрембльований звичайний текст
1008
926
1041
1026
Шифрування
Скрембльований звичайний текст
1035
928
1042
Дескремблювання пакету
1032
Дешифрування
Дескремблюваний звичайний текст
990
Шифротекст скрембльованого пакету даних
1024
Дескремблюваний звичайний текст
990

Рис. 5

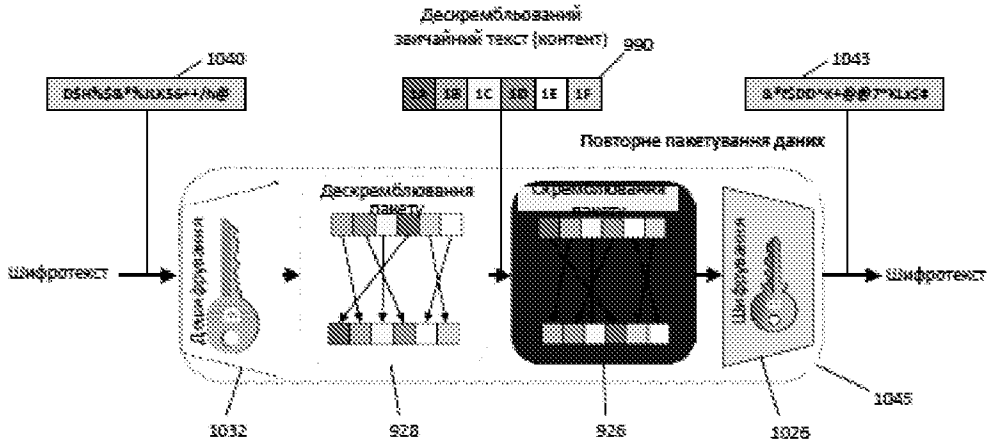

Дескремблюваний звичайний текст (контент)
990
1040
1043
Повторне пакетування даних
Дескремблювання пакету
Шифротекст
Дешифрування
Шифрування
Шифротекст
1045
1032
928
926
1026

Рис. 6

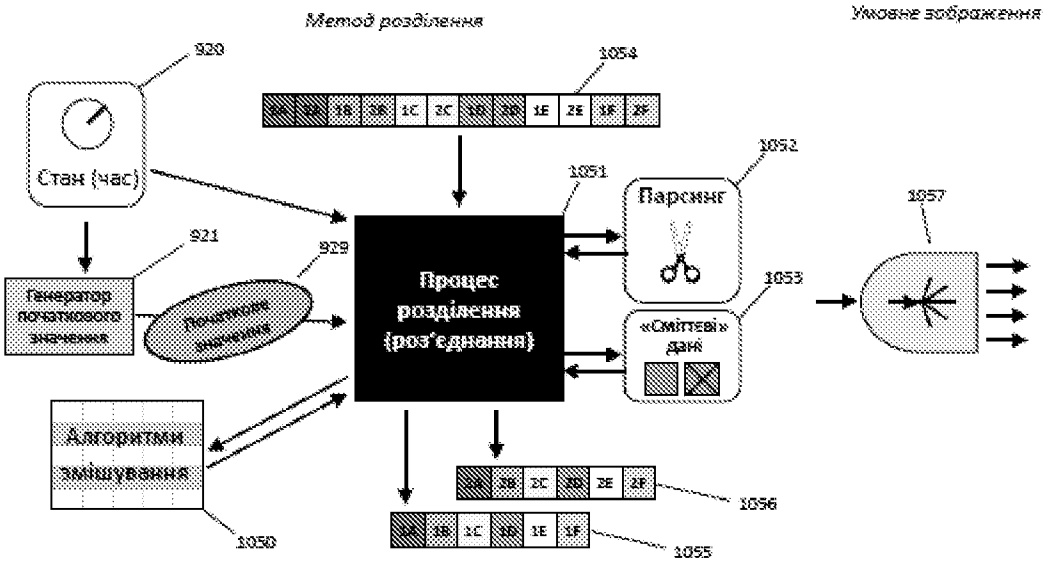

Метод розділення
Умовне зображення
920
Стан (час)
1054
1052
Парсинг
1051
1057
921
929
Генератор початкового значення
початкове значення
Процес розділення (роз'єднання)
1053
«Сміттєві» дані
Алгоритми змішування
1056
1055
1050

Рис. 7A

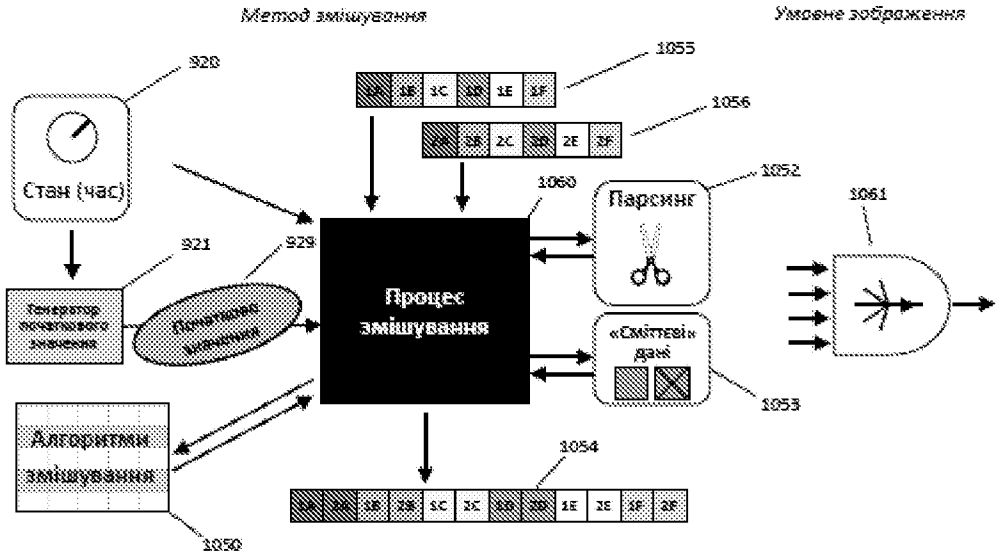

Метод змішування
Умовне зображення
920
1055
1056
Стан (час)
1060
1052
Парсинг
1061
921
929
Генератор початкового значення
початкове значення
Процес змішування
«Сміттєві» дані
1053
Алгоритми змішування
1054
1050

Рис. 7B

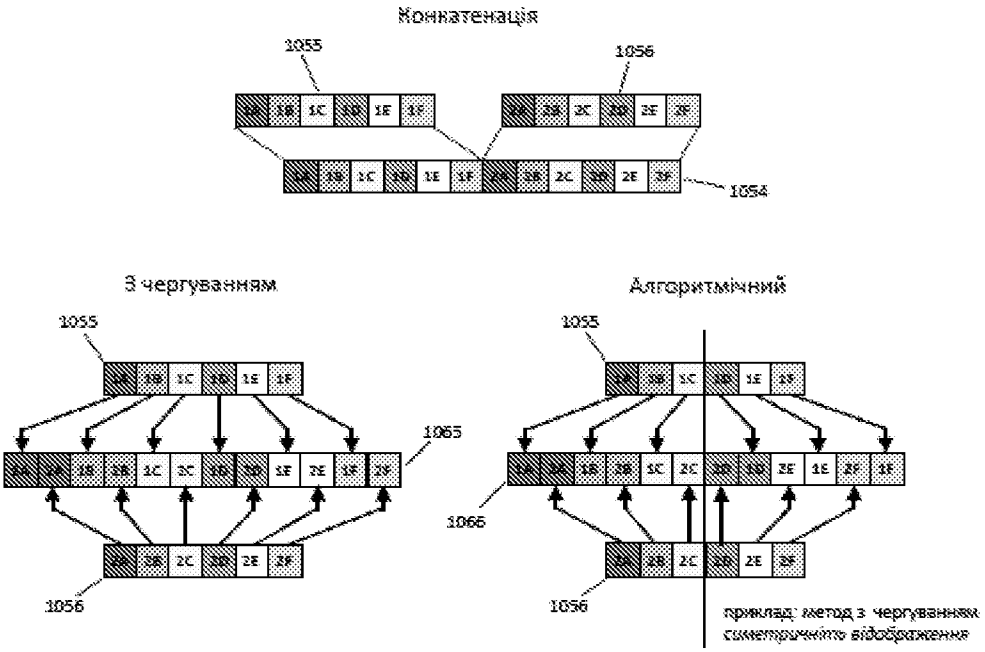

Конкатенація
1055
1056
1054
З чергуванням
Алгоритмічний
1055
1065
1066
1056
1056
приклад: метод з чергуванням
симетричного відображення

Рис. 8

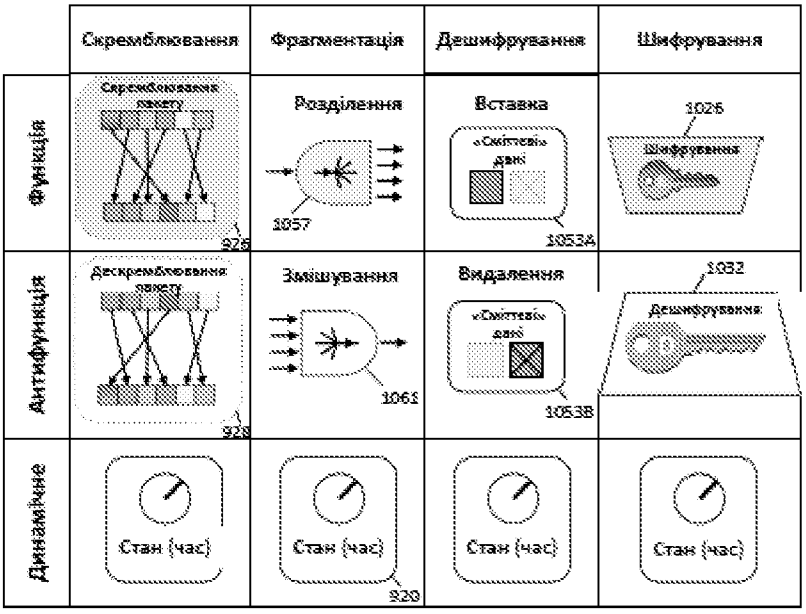

Скремблювання
Фрагментація
Дешифрування
Шифрування
Функція
Антифункція
Динамічне
Скремблювання пакету
Розділення
Вставка
1026
Шифрування
1057
«Сигнальні» дані
1053A
926
Дескремблювання пакету
Змішування
Видалення
1032
Дешифрування
1061
«Сигнальні» дані
1053B
928
Стан (час)
Стан (час)
Стан (час)
Стан (час)
929

Рис. 9A

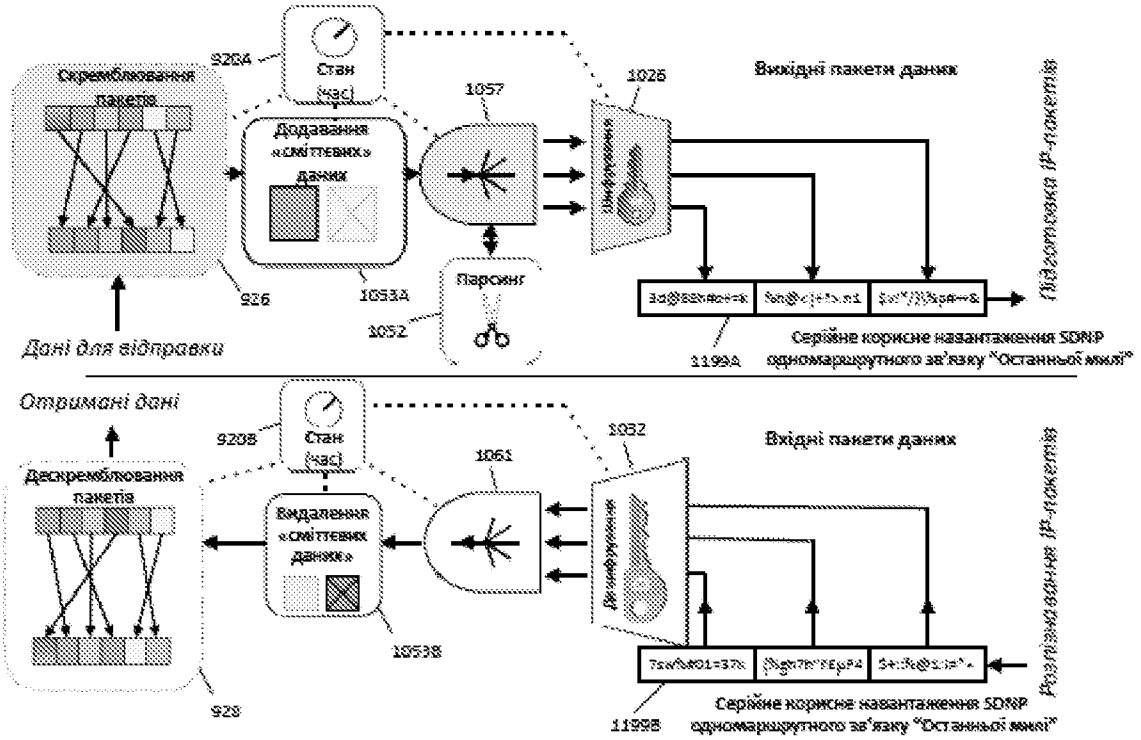

Скремблювання пакетів
920A
Стан (час)
1057
1026
Вихідні пакети даних
Додавання «сміттєвих» даних
Шифрування
Підготовка IP-пакетів
1053A
Парсинг
926
1052
Дані для відправки
1199A
Серійне корисне навантаження SDNP одномаршрутного зв'язку "Останньої милі"
Отримані дані
920B
Стан (час)
1052
1061
Вхідні пакети даних
Дескремблювання пакетів
Видалення «сміттєвих» даних
Дешифрування
Розпізнавання IP-пакетів
1053B
928
1199B
Серійне корисне навантаження SDNP одномаршрутного зв'язку "Останньої милі"

Рис. 9B

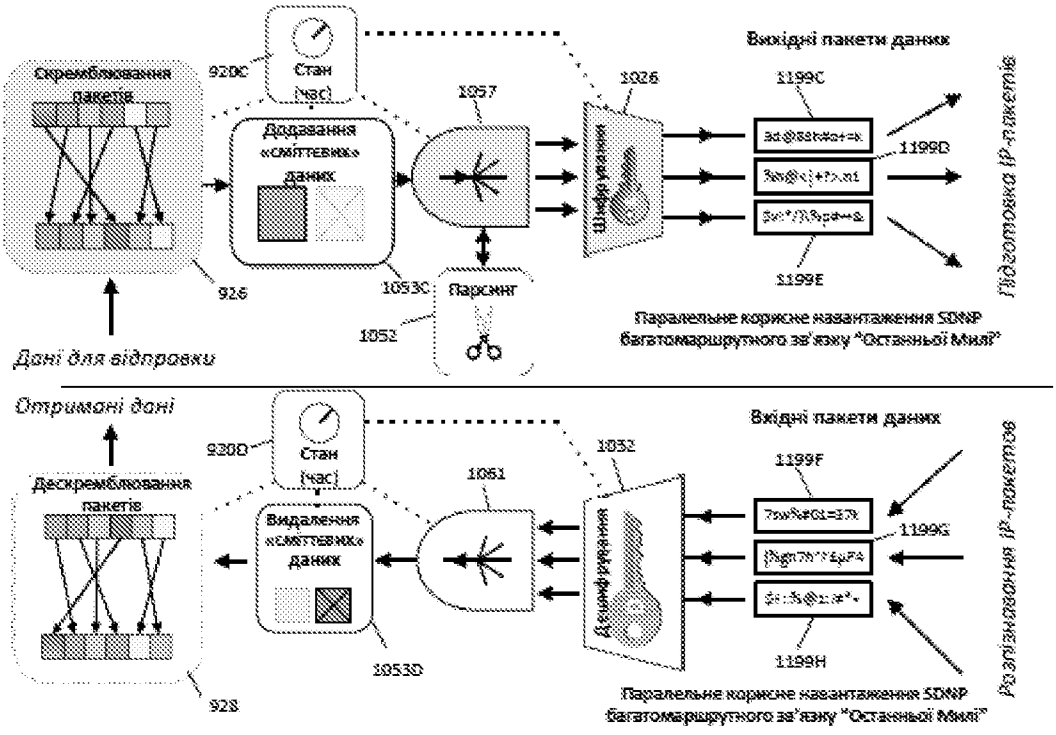

Скремблювання пакетів
920C
Стан (час)
1057
1026
Вихідні пакети даних
1199C
Додавання «сміттєвих» даних
Шифрування
Підготовка IP-пакетів
1199D
1053C
Парсинг
926
1052
Дані для відправки
1199E
Паралельне корисне навантаження SDNP багатомаршрутного зв'язку "Останньої Милі"
Отримані дані
920D
Стан (час)
1052
1061
Вхідні пакети даних
1199F
Дескремблювання пакетів
Видалення «сміттєвих» даних
Дешифрування
Розпізнавання IP-пакетів
1199G
1053D
928
1199H
Паралельне корисне навантаження SDNP багатомаршрутного зв'язку "Останньої Милі"

Рис. 9C

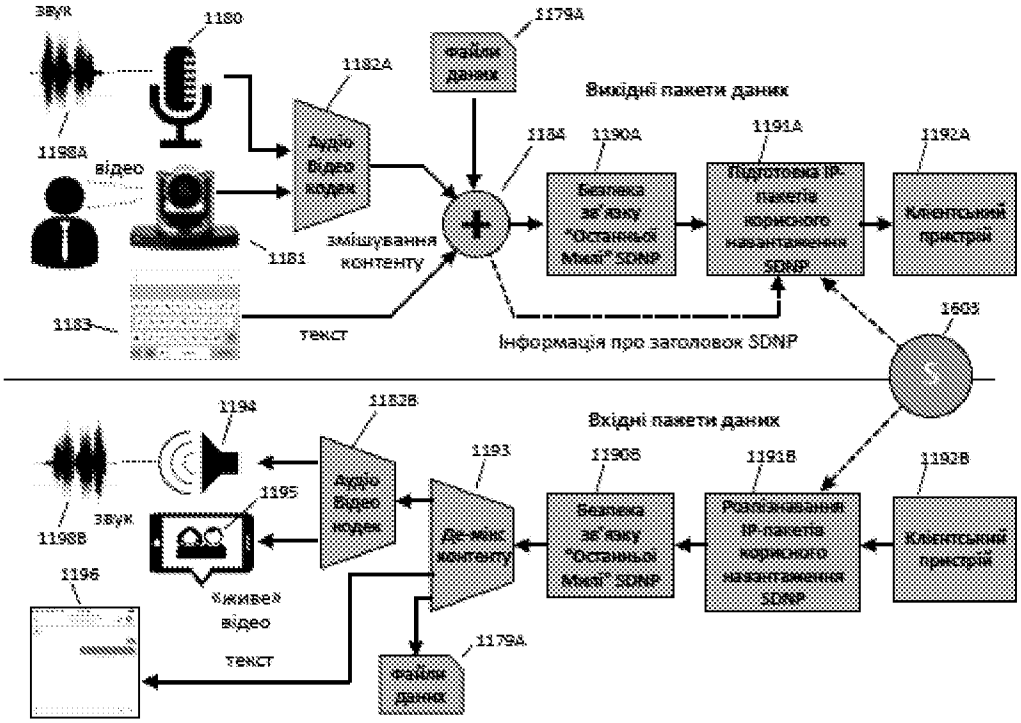

звук
1180
1179A
1182A
файли даних
Вихідні пакети даних
1188A
відео
1184
1190A
1191A
1192A
Аудіо Відео кодек
Безпека зв'язку "Остання Миля" SDNP
Підготовка IP пакета корисного навантаження SDNP
Клієнтський пристрій
1181
змішування контенту
1183
текст
Інформація про заголовок SDNP
1603
1194
1182B
Вхідні пакети даних
1193
1190B
1191B
1192B
1195
звук
1188B
Де-мікс контенту
Безпека зв'язку "Остання Миля" SDNP
Розпізнавання IP пакета корисного навантаження SDNP
Клієнтський пристрій
1196
"живе" відео
текст
1179A
файли даних

Рис. 9D

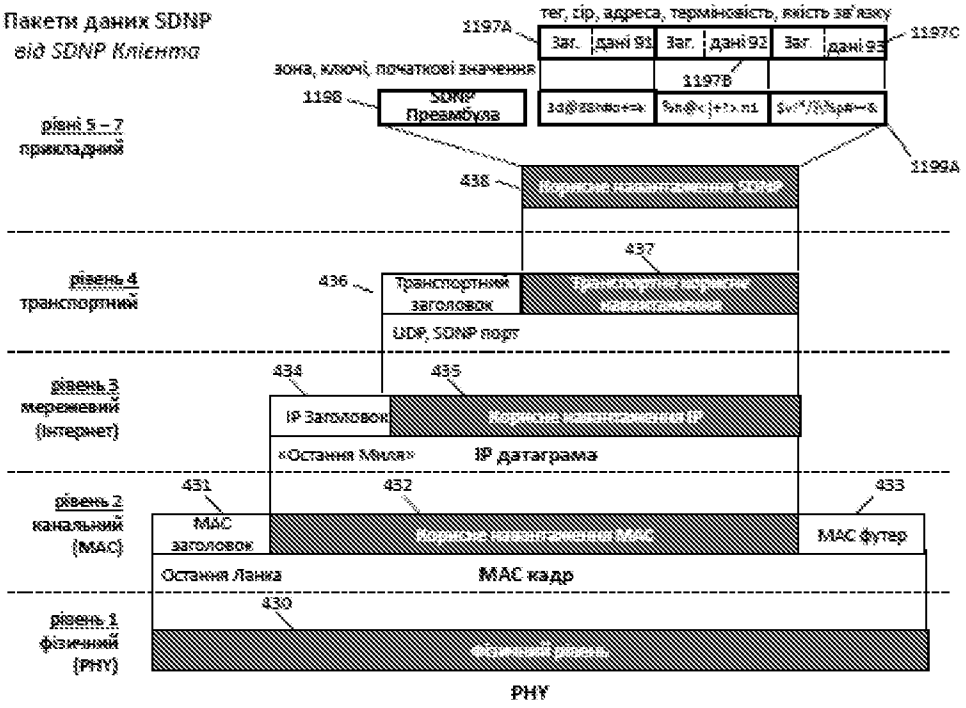
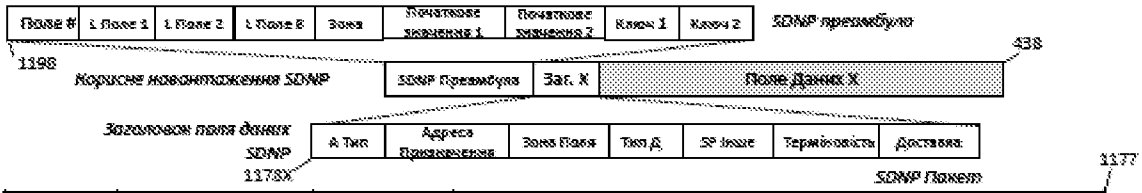

Пакети даних SDNP
від SDNP Клієнта
тег, cip, адреса, терміновість, якість зв'язку
1197A
Заг.
дані 91
Заг.
дані 92
Заг.
дані 93
1197C
зона, ключі, початкові значення
1197B
1198
SDNP Преамбула
1199A
рівні 5 – 7
прикладний
438
рівень 4
транспортний
437
436
Транспортний заголовок
UDP, SDNP порт
рівень 3
мережевий
(Інтернет)
434
435
IP Заголовок
«Остання Миля»
IP датаграма
рівень 2
канальний
(MAC)
431
432
433
MAC заголовок
MAC футер
Остання Ланка
MAC кадр
рівень 1
фізичний
(PHY)
430
PHY

Рис. 9E



Рівень	Поле Пакету	Розмір	Функція
3	Поле #	4b	Кількість полів
3	L поле 1, 2, X	4B	Довжина поля даних 1, 2, ..., 8
3	Зона	12b	Поточна зона SDNP (одна із 4096 зон)
5	Початкове значення 1, 2	8B, 8B	Два 32-бітні вихідні значення (для скремблювання, змішування, і т.д.)
6	Ключ 1, 2	64B, 64B	Два 512-бітні ключі (для шифрування)
3	Тип А (Адреса)	2b	Тип адреси призначення (тег, SDNP Zip, IPv6, NAT, POTS #)
3	Адрес призначення	1B до 12B	Тег, IP адреса, SDNP адреса, NAT адреса, SDNP ZIP, телефонний #
3	Зона поля	12b	SDNP зона переносу (одна із 4096 зон)
4	Тип Д (Даних)	2b	Тип даних (голос, текст, відео, дані, ПЗ...)
6	Інше поле	8B	Поле розширення, поле інформацій дескремблювання, і т.д.
4	Терміновість	2b	Терміновість підпакета (повільна, нормальна, пріоритетна, термінова)
4	Доставка	2b	Маркер якості зв'язку (нормальна, надлишкова, особлива, VIP...)
5 до 7	Дані в Пакеті X	0 до 2008	Дані до 2008 на субпакет, 8 субпакетів макс.

Рис. 9F

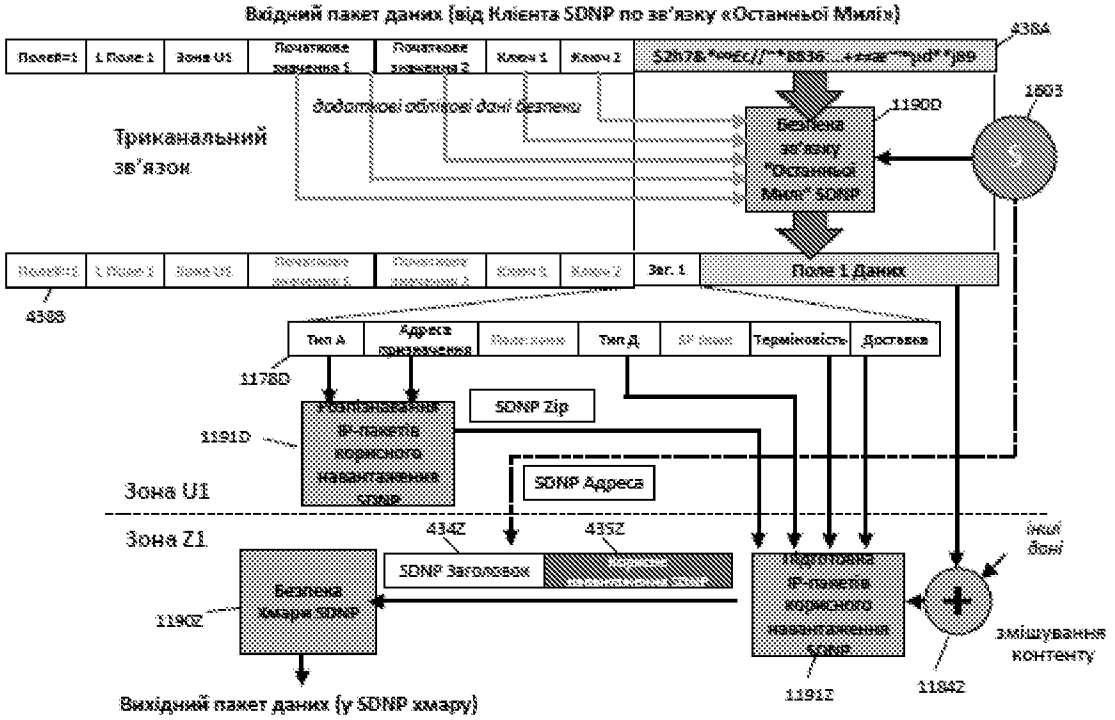


Рис. 9G

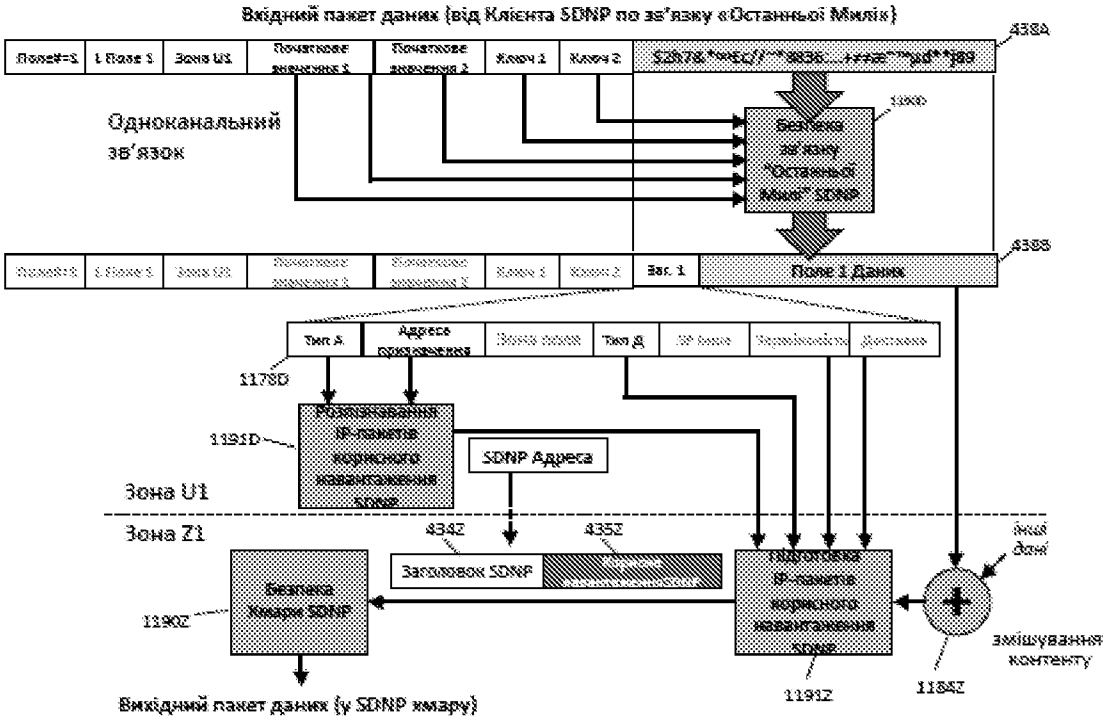

Вхідний пакет даних (від Клієнта SDNP по зв'язку «Останньої Милі»)
Одноканальний зв'язок
Безпека зв'язку "Останньої Милі" SDNP
Поле 1 Даних
Розпізнавання IP-пакета корисного навантаження SDNP
SDNP Адреса
Зона U1
Зона Z1
Заголовок SDNP
Безпека Хмари SDNP
Підготовка IP-пакета корисного навантаження SDNP
інші дані
змішування контенту
Вихідний пакет даних (у SDNP хмару)

Рис. 9H

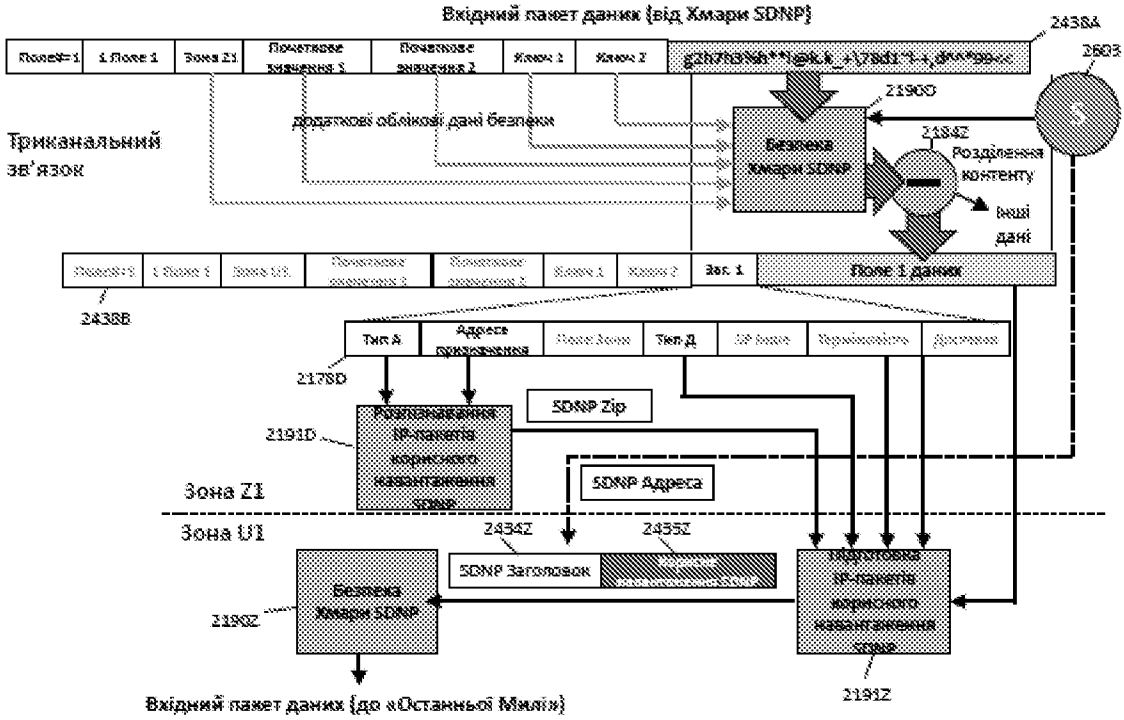

Вхідний пакет даних (від Хмари SDNP)
додаткові облікові дані безпеки
Триканальний зв'язок
Безпека Хмари SDNP
Розділення контенту
інші дані
Поле 1 даних
SDNP Zip
SDNP Адреса
Зона Z1
Зона U1
SDNP Заголовок
Безпека Хмари SDNP
Підготовка IP-пакета корисного навантаження SDNP
Вхідний пакет даних (до «Останньої Милі»)

Рис. 9I

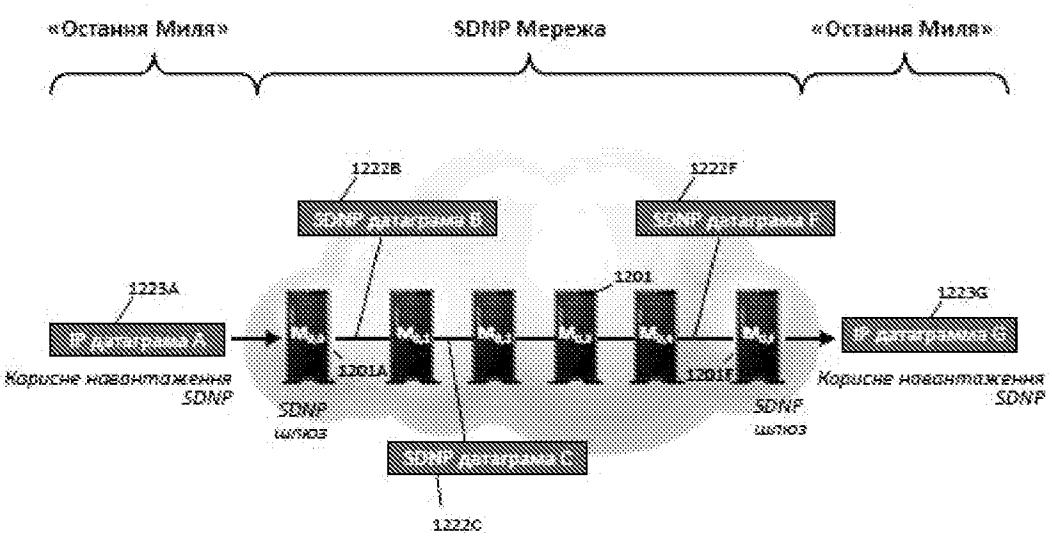

«Остання Миля»
SDNP Мережа
«Остання Миля»
1222B
1222F
1223A
1201
1223G
Корисне навантаження SDNP
1201A
1201B
SDNP шлюз
SDNP шлюз
Корисне навантаження SDNP
1222C

Рис. 10

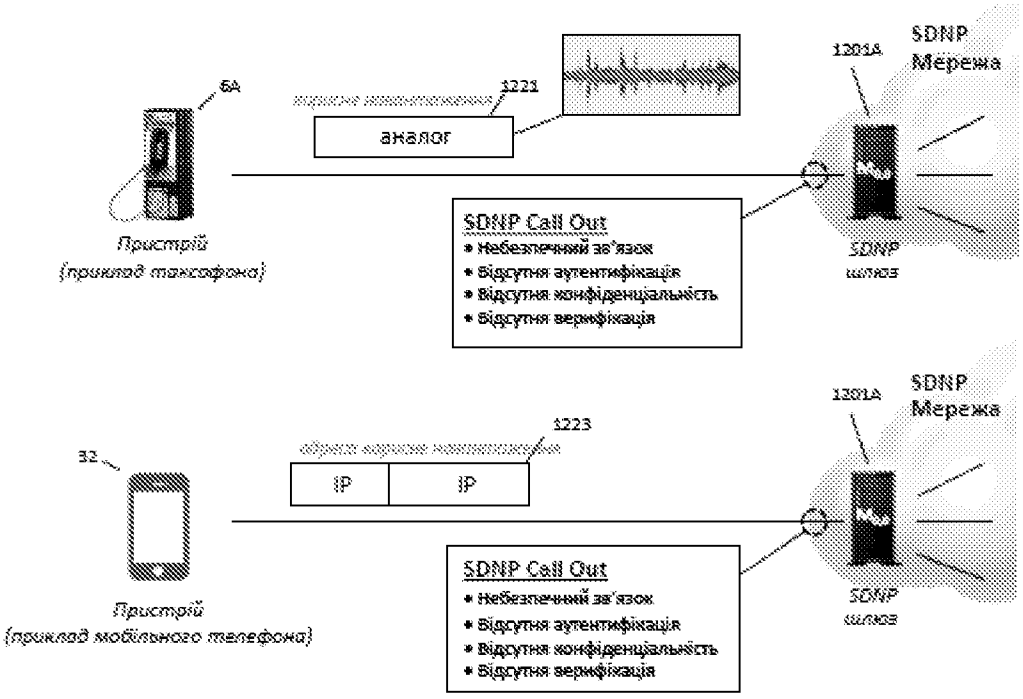

6A
1221
аналог
1201A
SDNP Мережа
Пристрій
(приклад таксофона)
SDNP Call Out
• Небезпечний зв'язок
• Відсутня аутентифікація
• Відсутня конфіденціальність
• Відсутня верифікація
SDNP шлюз
32
1223
IP
IP
1201A
SDNP Мережа
Пристрій
(приклад мобільного телефона)
SDNP Call Out
• Небезпечний зв'язок
• Відсутня аутентифікація
• Відсутня конфіденціальність
• Відсутня верифікація
SDNP шлюз

Рис. 11

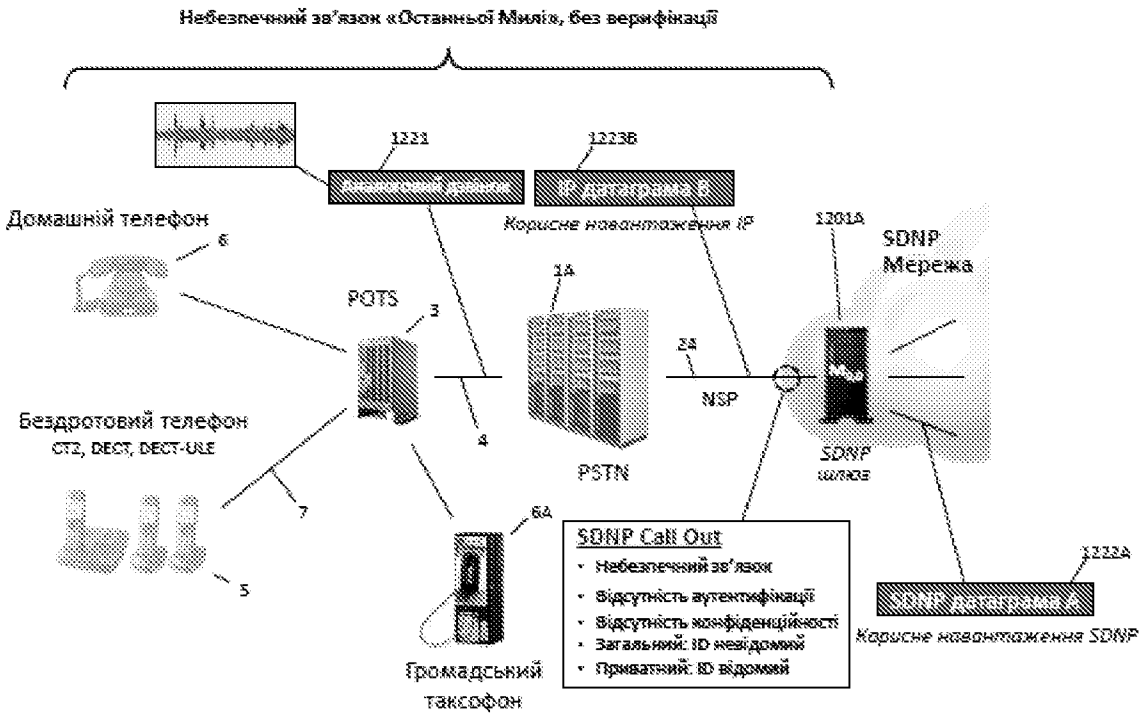

Небезпечний зв'язок «Останньої Милі», без верифікації
1221
1223B
Корисне навантаження IP
1201A
SDNP
Мережа
Домашній телефон
6
POTS
3
1A
24
NSP
Бездротовий телефон
CT2, DECT, DECT-ULE
7
4
PSTN
SDNP
шлюз
5
6A
SDNP Call Out
Небезпечний зв'язок
Відсутність аутентифікації
Відсутність конфіденційності
Загальний: ID невідомий
Приватний: ID відомий
1222A
Корисне навантаження SDNP
Громадський
таксофон

Рис. 12

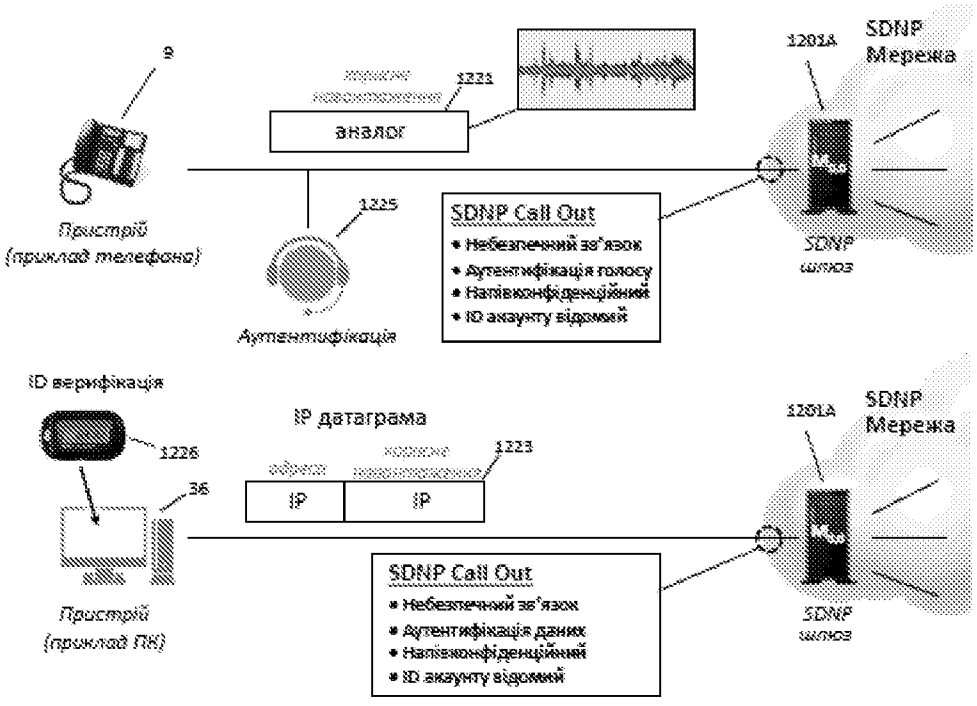

9
1221
аналог
1201A
SDNP
Мережа
Пристрій
(приклад телефона)
1225
SDNP Call Out
Небезпечний зв'язок
Аутентифікація голосу
Напівконфіденційний
ID акаунту відомий
SDNP
шлюз
Аутентифікація
ID верифікація
IP датаграма
1226
1223
36
IP
IP
1201A
SDNP
Мережа
SDNP Call Out
Небезпечний зв'язок
Аутентифікація даних
Напівконфіденційний
ID акаунту відомий
SDNP
шлюз
Пристрій
(приклад ПК)

Рис. 13

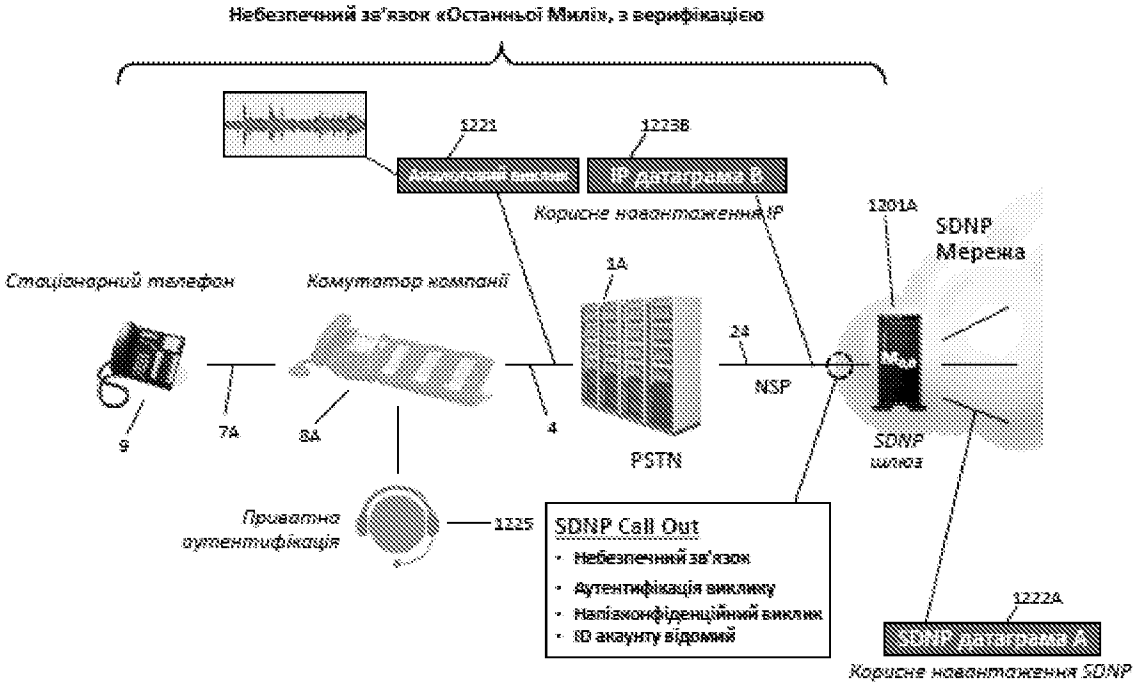

Небезпечний зв'язок «Останньої Милі», з верифікацією
1221
1223B
Аналоговий вихід
IP датаграма B
Корисне навантаження IP
1201A
SDNP
Мережа
Стаціонарний телефон
Комутатор компанії
3A
24
NSP
9
7A
8A
4
PSTN
SDNP
шлюз
Приватна
аутентифікація
1225
SDNP Call Out
Небезпечний зв'язок
Аутентифікація виклику
Напівконфіденційний виклик
ID акаунту відомий
1222A
SDNP датаграма A
Корисне навантаження SDNP

Рис. 14

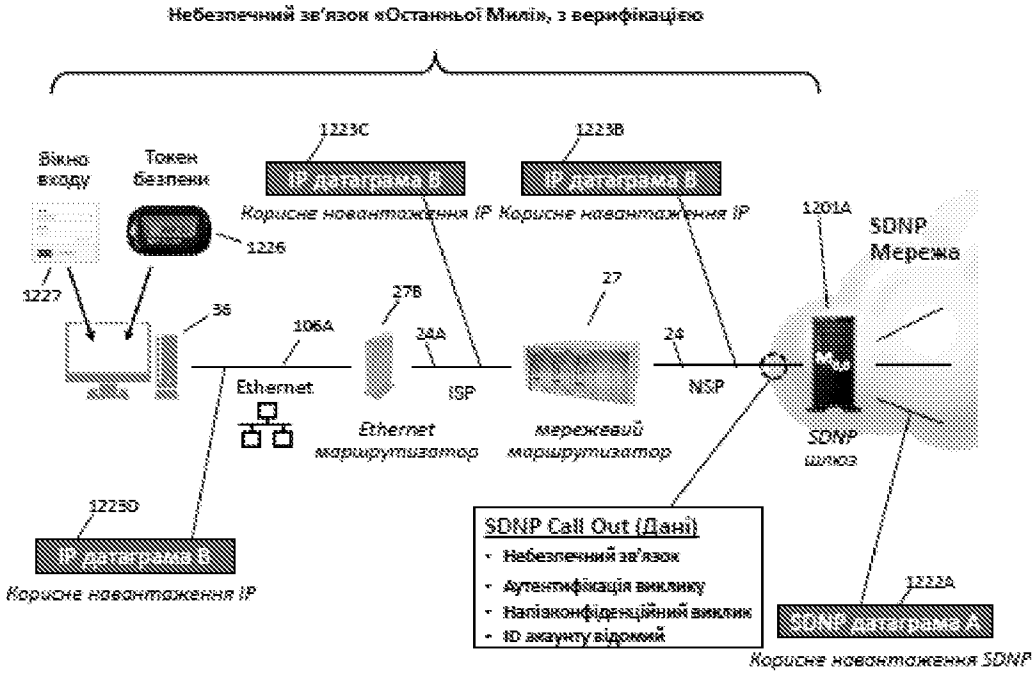

Небезпечний зв'язок «Останньої Милі», з верифікацією
1223C
1223B
Вікно
входу
Токен
безпеки
IP датаграма B
IP датаграма B
Корисне навантаження IP
Корисне навантаження IP
1201A
SDNP
Мережа
1226
1227
36
106A
27B
34A
27
24
Ethernet
ISP
NSP
Ethernet
маршрутизатор
мережевий
маршрутизатор
SDNP
шлюз
1223D
IP датаграма B
Корисне навантаження IP
SDNP Call Out (Дані)
Небезпечний зв'язок
Аутентифікація виклику
Напівконфіденційний виклик
ID акаунту відомий
1223A
SDNP датаграма A
Корисне навантаження SDNP

Рис. 15

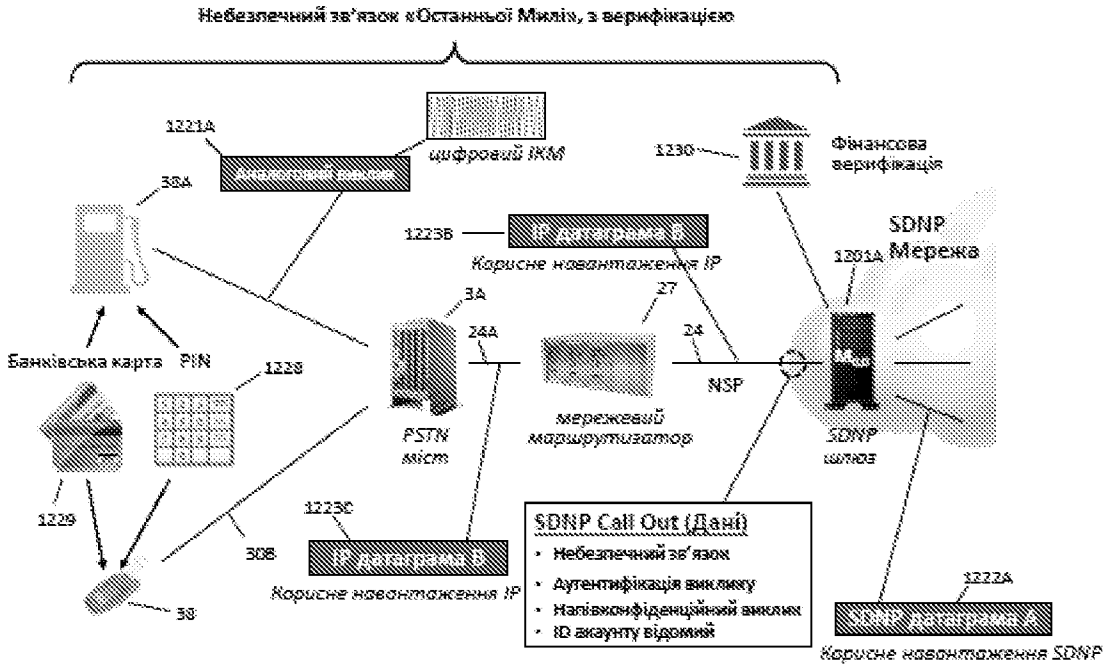

Небезпечний зв'язок «Останньої Милі», з верифікацією
1221A
цифровий ІКМ
1230
Фінансова верифікація
38A
1223B
IP датаграма 2
Корисне навантаження IP
SDNP Мережа
1291A
3A
27
24A
24
Банківська карта
PIN
1228
NSP
PSTN міст
мережевий маршрутизатор
SDNP шлюз
1229
1223C
SDNP Call Out (Дані)
Небезпечний зв'язок
Аутентифікація виклику
Напівконфіденційний виклик
ID акаунту відомий
1222A
SDNP датаграма 2
Корисне навантаження SDNP
38B
IP датаграма 2
Корисне навантаження IP
38

Рис. 16

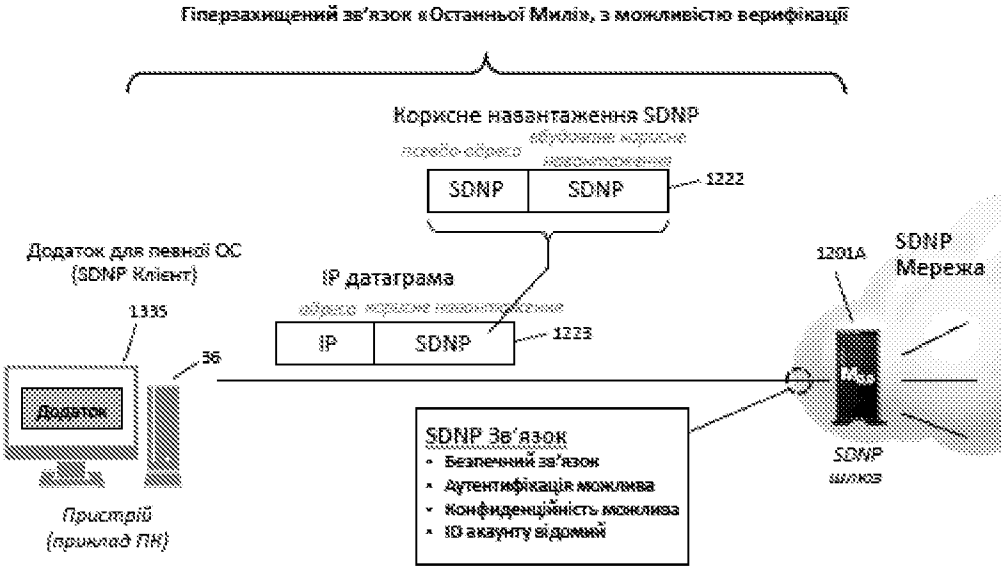

Гіперзахищений зв'язок «Останньої Милі», з можливістю верифікації
Корисне навантаження SDNP
SDNP
SDNP
1222
Додаток для певної ОС
(SDNP Клієнт)
IP датаграма
1291A
SDNP Мережа
1335
IP
SDNP
1223
36
Додаток
SDNP Зв'язок
Безпечний зв'язок
Аутентифікація можлива
Конфіденційність можлива
ID акаунту відомий
SDNP шлюз
Пристрій
(приклад ПК)

Рис. 17

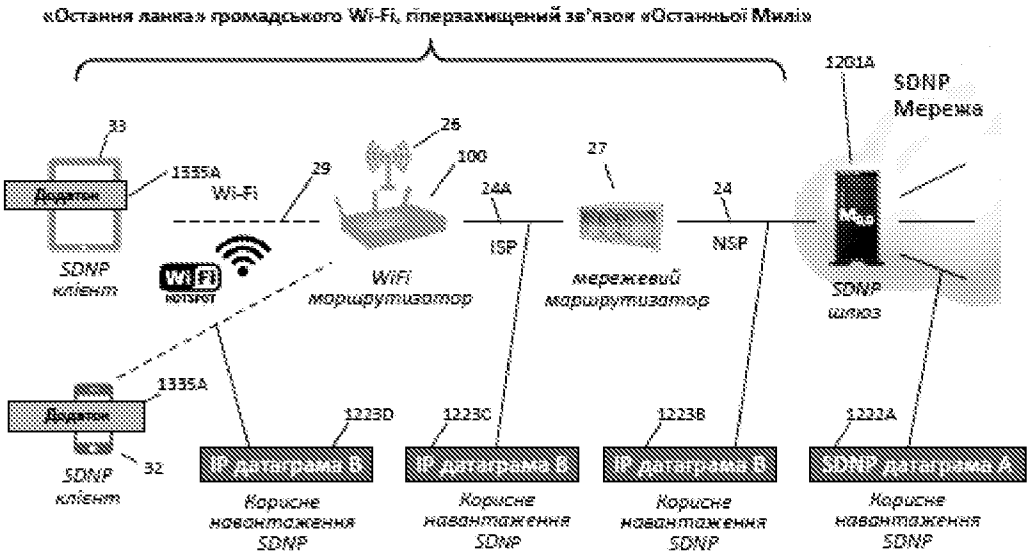

«Остання ланка» громадського Wi-Fi, гіперзахищений зв'язок «Останньої Милі»
1201A
SDNP
Мережа
33
1335A
Додаток
SDNP
клієнт
Wi-Fi
29
26
100
WiFi
маршрутизатор
24A
ISP
27
мережевий
маршрутизатор
24
NSP
SDNP
шлюз
1335A
Додаток
32
SDNP
клієнт
1223D
1223C
1223B
1223A
IP датаграма B
IP датаграма B
IP датаграма B
SDNP датаграма A
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP

Рис. 18

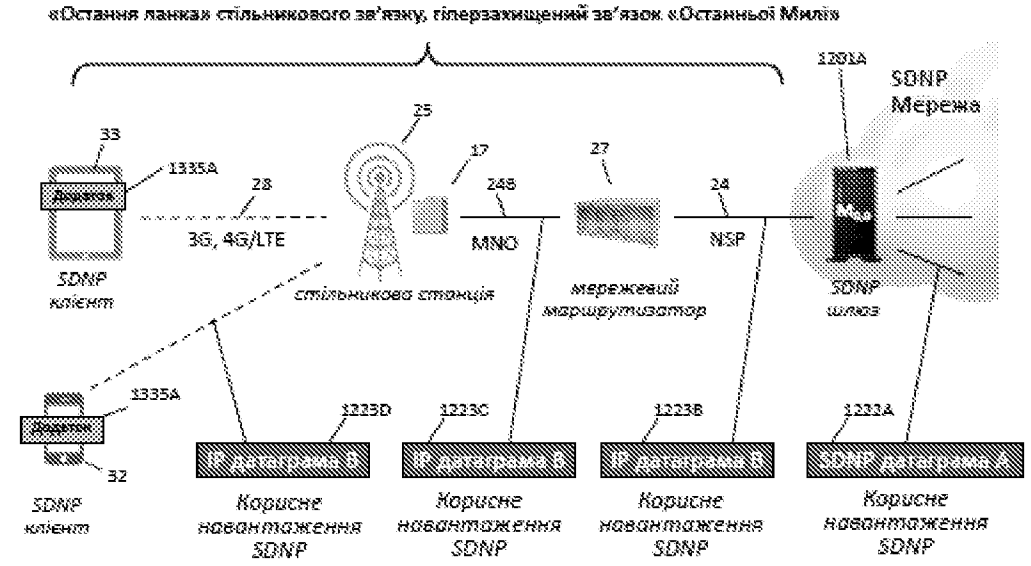

«Остання ланка» стільникового зв'язку, гіперзахищений зв'язок «Останньої Милі»
1201A
SDNP
Мережа
33
1335A
Додаток
SDNP
клієнт
28
3G, 4G/LTE
25
17
стільникова станція
24B
MNO
27
мережевий
маршрутизатор
24
NSP
SDNP
шлюз
1335A
Додаток
32
SDNP
клієнт
1223D
1223C
1223B
1223A
IP датаграма B
IP датаграма B
IP датаграма B
SDNP датаграма A
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP

Рис. 19

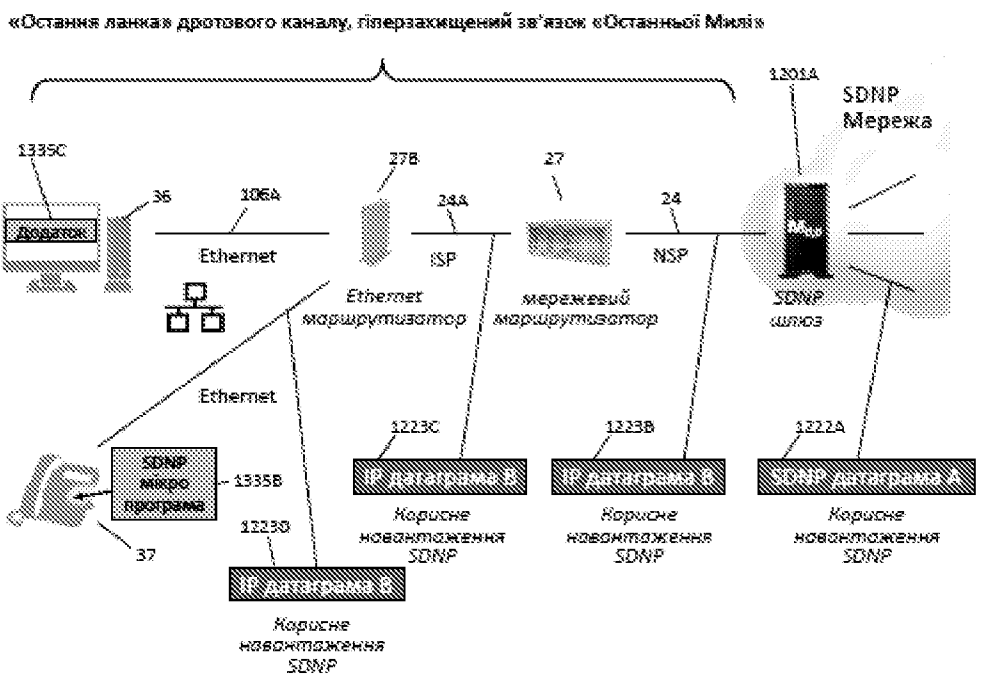

«Остання ланка» дротового каналу, гіперзахищений зв'язок «Останньої Милі»
1201A
SDNP
Мережа
1335C
Додаток
36
106A
Ethernet
27B
ISP
24A
27
NSP
24
SDNP
шлюз
Ethernet
маршрутизатор
мережевий
маршрутизатор
Ethernet
SDNP
мікро
програма
1335B
37
1223C
IP датаграма B
1223B
IP датаграма B
1222A
SDNP датаграма A
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP
1223D
IP датаграма B
Корисне
навантаження
SDNP

Рис. 20

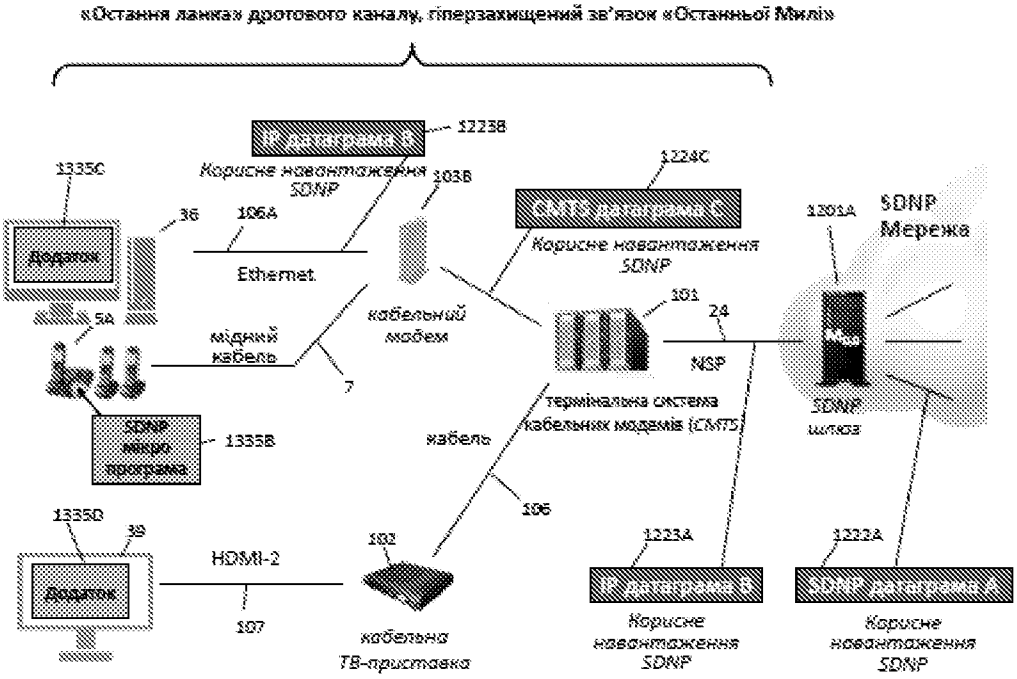

«Остання ланка» дротового каналу, гіперзахищений зв'язок «Останньої Милі»
IP датаграма B
1223B
Корисне навантаження
SDNP
1335C
Додаток
36
106A
Ethernet
103B
кабельний
модем
1224C
CMTS датаграма C
Корисне навантаження
SDNP
1201A
SDNP
Мережа
101
24
NSP
SDNP
шлюз
5A
мідний
кабель
7
SDNP
мікро
програма
1335B
термінальна система
кабельних модемів (CMTS)
кабель
106
1335D
39
Додаток
HDMI-2
107
102
кабельна
ТВ-приставка
1223A
IP датаграма B
1222A
SDNP датаграма A
Корисне
навантаження
SDNP
Корисне
навантаження
SDNP

Рис. 21

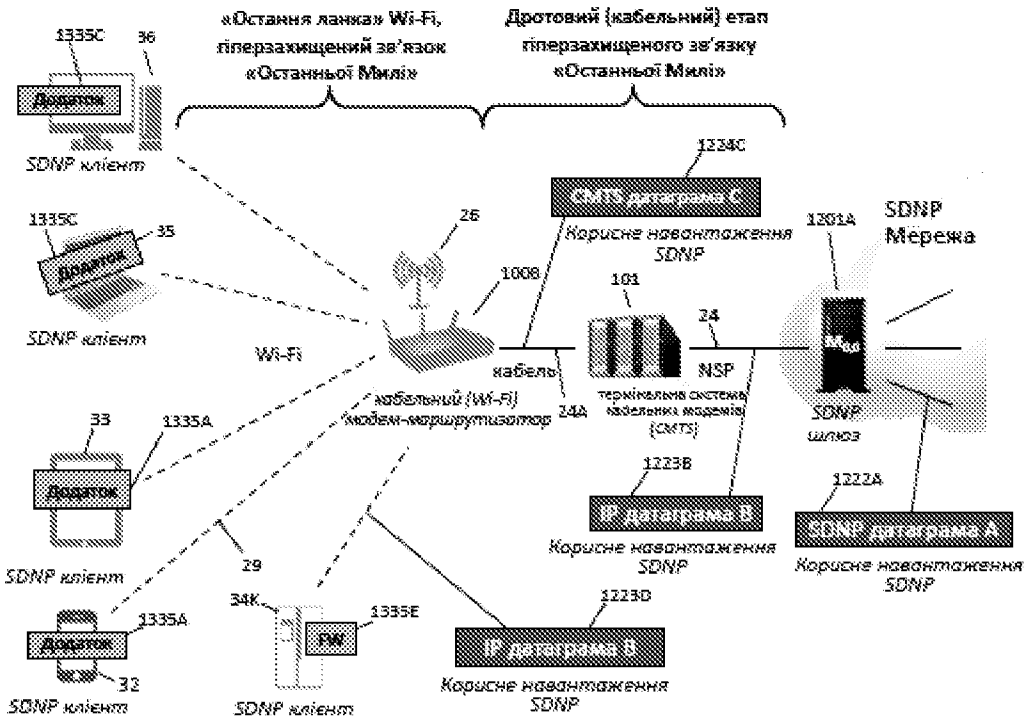

«Остання ланка» Wi-Fi, гіперзахищений зв'язок «Останньої Милі»
Дротовий (кабельний) етап гіперзахищеного зв'язку «Останньої Милі»
SDNP клієнт
Wi-Fi
кабельний (Wi-Fi) модем-маршрутизатор
кабель
NSP
термінальна система кабельних модемів (CMTS)
SDNP шлюз
SDNP Мережа
Корисне навантаження SDNP
IP датаграма B
SDNP датаграма A
IP датаграма D
FW

Рис. 22


Ідентифікатор останнього з'єднання захищеної локальної мережі
Гіперзахищений етап зв'язку «Останньої Милі» з перевіркою особистості
корисне навантаження SDNP
IP датаграма
SDNP
IP
Без SDNP клієнта
Пристрій (прилад ПК)
віддалений шлюз SDNP
SDNP Мережа
SDNP шлюз
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
LAN Підключення
• Ethernet
• Wi-Fi
• Інші протоколи
• Парні пристрої

Рис. 23

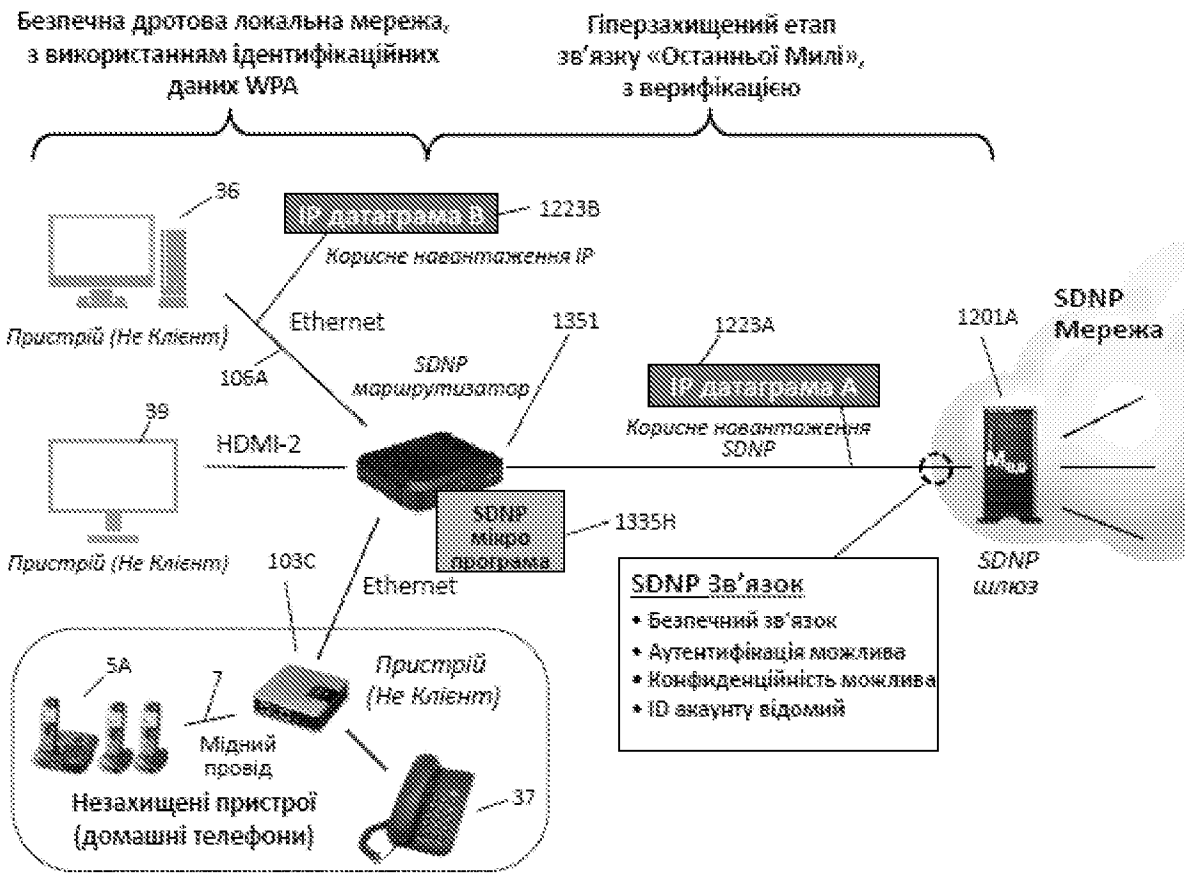

Безпечна дротова локальна мережа, з використанням ідентифікаційних даних WPA
Гіперзахищений етап зв'язку «Останньої Милі», з верифікацією
36
IP дейтаграма B
1223B
Корисне навантаження IP
Пристрій (Не Клієнт)
Ethernet
1351
1223A
1201A
SDNP Мережа
106A
SDNP маршрутизатор
39
HDMI-2
IP дейтаграма A
Корисне навантаження SDNP
SDNP мікро програма
1335R
Пристрій (Не Клієнт)
103C
Ethernet
SDNP шлюз
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
5A
7
Пристрій (Не Клієнт)
Мідний провід
37
Незахищені пристрої (домашні телефони)

Рис. 24

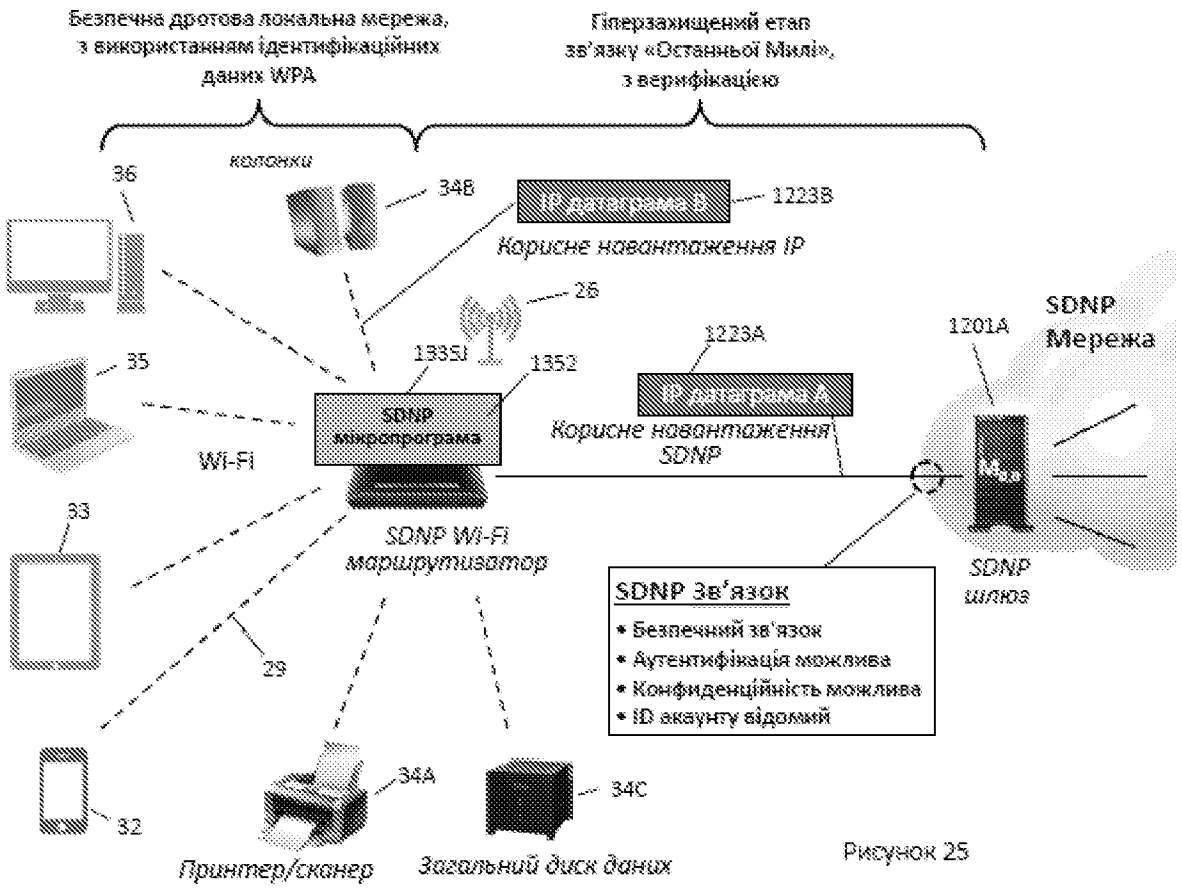

Безпечна дротова локальна мережа, з використанням ідентифікаційних даних WPA
Гіперзахищений етап зв'язку «Останньої Милі», з верифікацією
колонки
36
34B
IP датаграма B
1223B
Корисне навантаження IP
26
35
1335J
1352
1223A
1201A
SDNP Мережа
SDNP мікропрограма
Wi-Fi
Корисне навантаження SDNP
33
SDNP Wi-Fi маршрутизатор
SDNP шлюз
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
29
34A
34C
32
Принтер/сканер
Загальний диск даних
Рисунок 25

Рис. 25

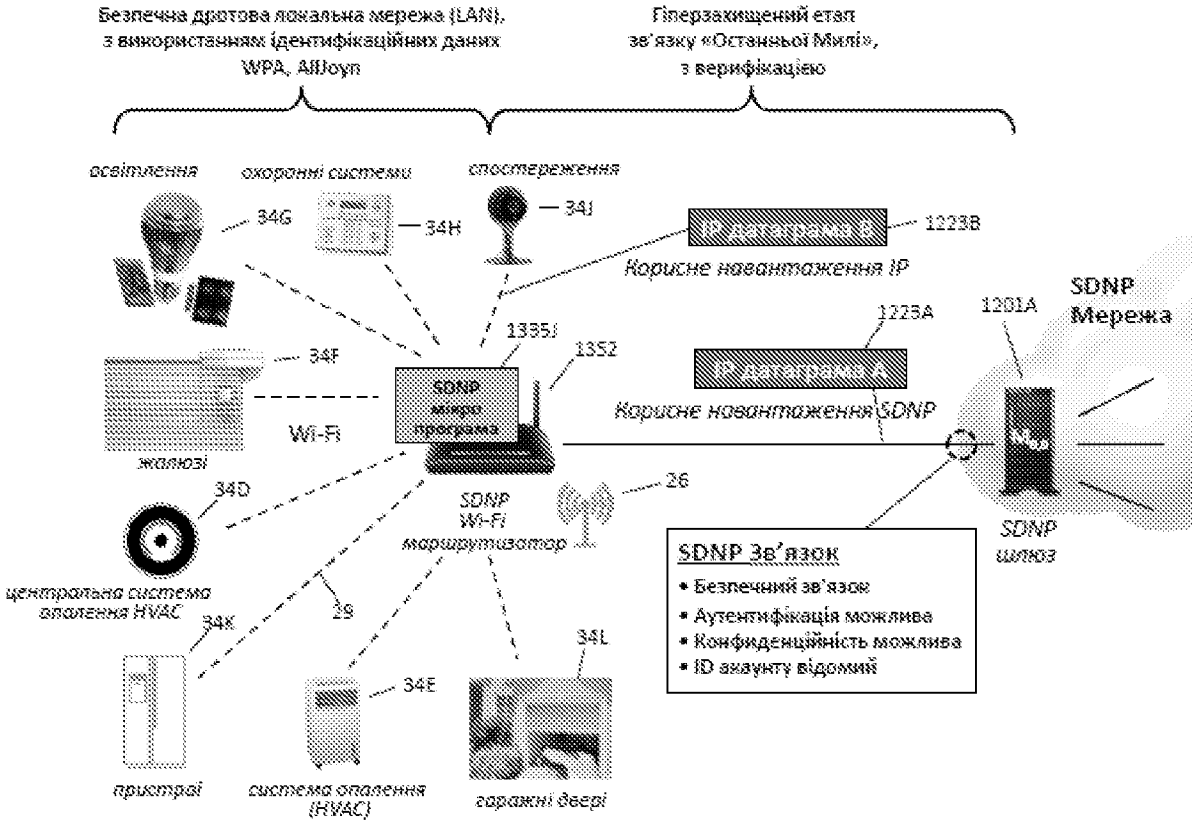

Безпечна дротова локальна мережа (LAN), з використанням ідентифікаційних даних WPA, AllJoyn
Гіперзахищений етап зв'язку «Останньої Милі», з верифікацією
освітлення
охоронні системи
спостереження
34G
34H
34J
IP датаграма B
1223B
Корисне навантаження IP
1223A
1201A
SDNP Мережа
1335J
1352
34F
SDNP мікропрограма
Wi-Fi
Корисне навантаження SDNP
жалюзі
34D
26
SDNP Wi-Fi маршрутизатор
SDNP шлюз
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
центральна система опалення HVAC
29
34K
34L
34E
пристрої
система опалення (HVAC)
гаражні двері

Рис. 26

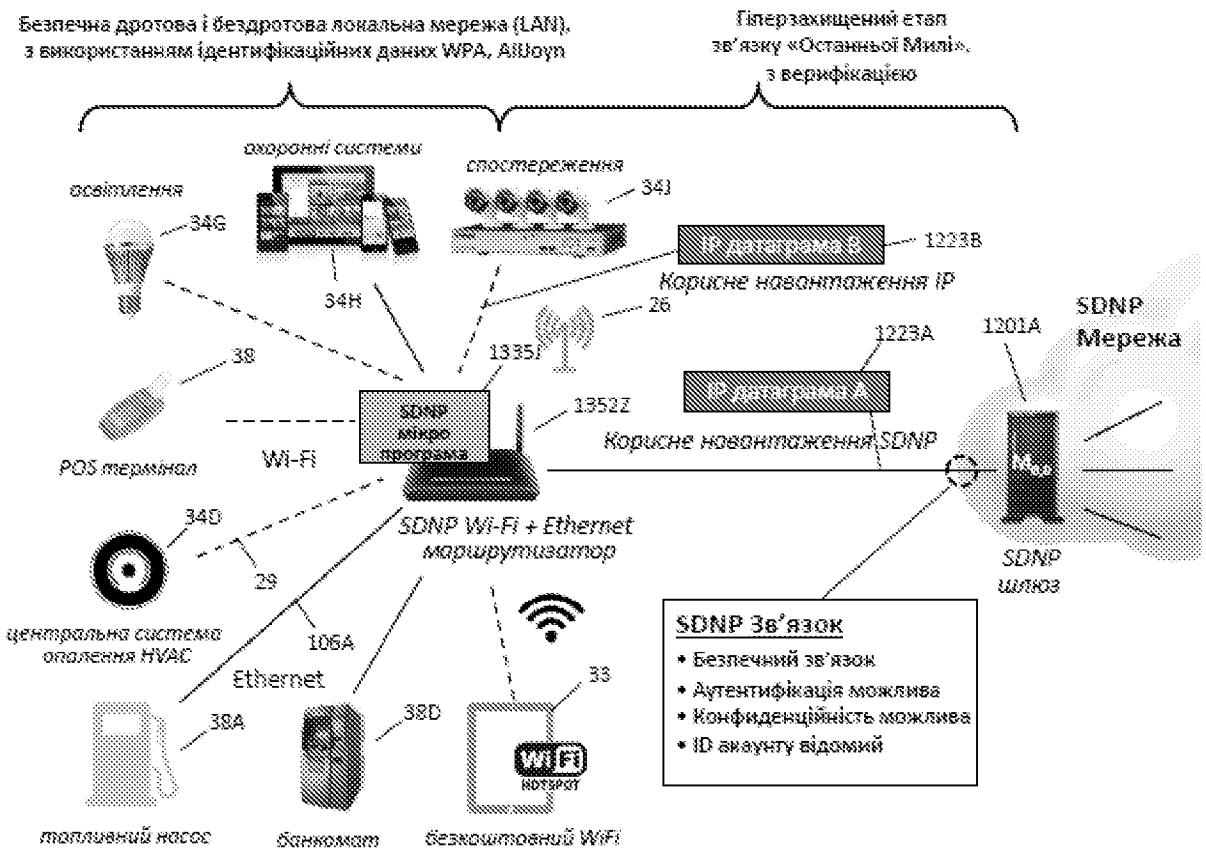

Безпечна дротова і бездротова локальна мережа (LAN),
з використанням ідентифікаційних даних WPA, AllJoyn
Гіперзахищений етап
зв'язку «Останньої Милі»,
з верифікацією
охоронні системи
спостереження
освітлення
34J
34G
34H
IP Антенна B
1223B
Корисне навантаження IP
26
1335J
1223A
1201A
SDNP
Мережа
38
SDNP
мікро
програма
1352Z
Корисне навантаження SDNP
Wi-Fi
POS термінал
SDNP Wi-Fi + Ethernet
маршрутизатор
34D
29
SDNP
шлюз
центральна система
опалення HVAC
106A
Ethernet
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
33
38A
38D
Wi Fi
HOTSPOT
паливний насос
банкомат
безкоштовний WiFi

Рис. 27

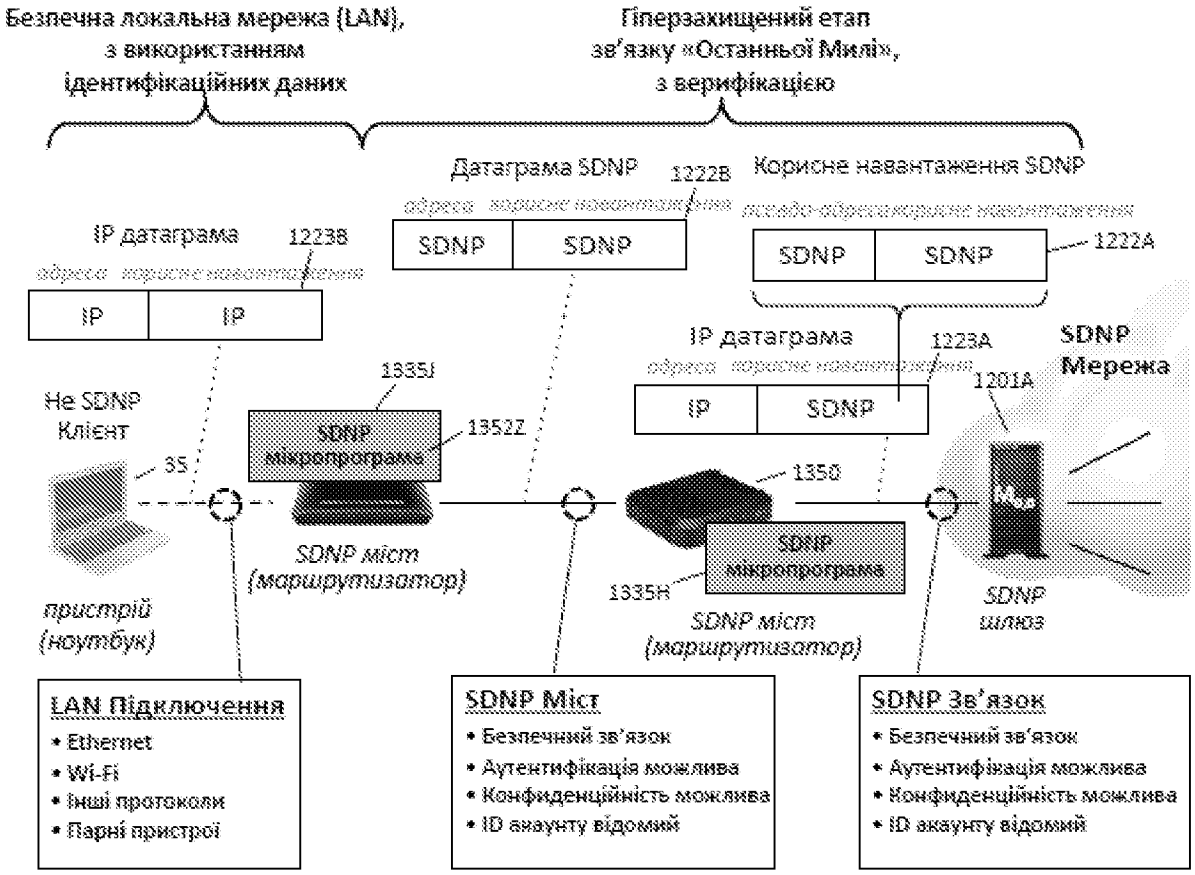

Безпечна локальна мережа (LAN),
з використанням
ідентифікаційних даних
Гіперзахищений етап
зв'язку «Останньої Милі»,
з верифікацією
Датаграма SDNP
1222B
Корисне навантаження SDNP
адреса
корисне навантаження
IP датаграма
1223B
SDNP
SDNP
1222A
IP
IP
IP датаграма
1223A
SDNP
Мережа
1335J
Не SDNP
Клієнт
SDNP
мікропрограма
1352Z
IP
SDNP
1201A
35
1350
SDNP міст
(маршрутизатор)
SDNP
мікропрограма
1335H
SDNP міст
(маршрутизатор)
SDNP
шлюз
пристрій
(ноутбук)
LAN Підключення
• Ethernet
• Wi-Fi
• Інші протоколи
• Парні пристрої
SDNP Міст
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий
SDNP Зв'язок
• Безпечний зв'язок
• Аутентифікація можлива
• Конфіденційність можлива
• ID акаунту відомий

Рис. 28

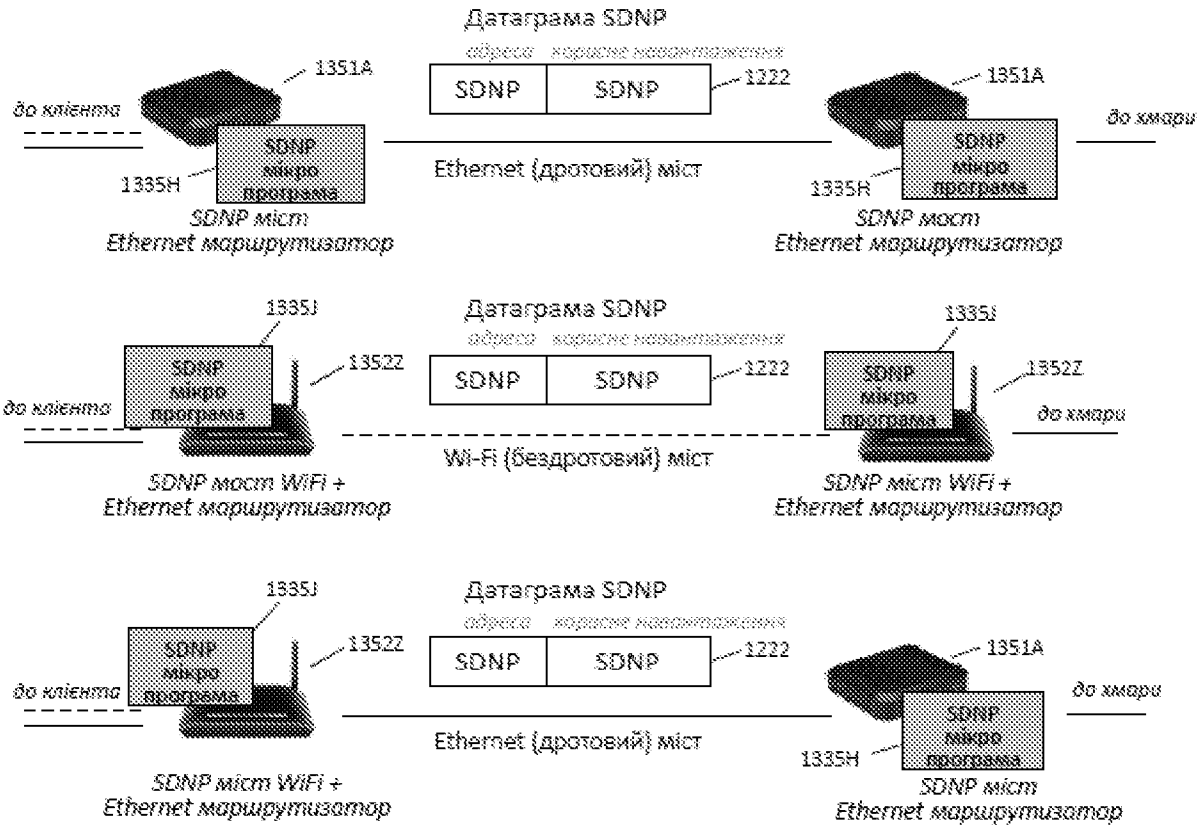


Рис. 29A

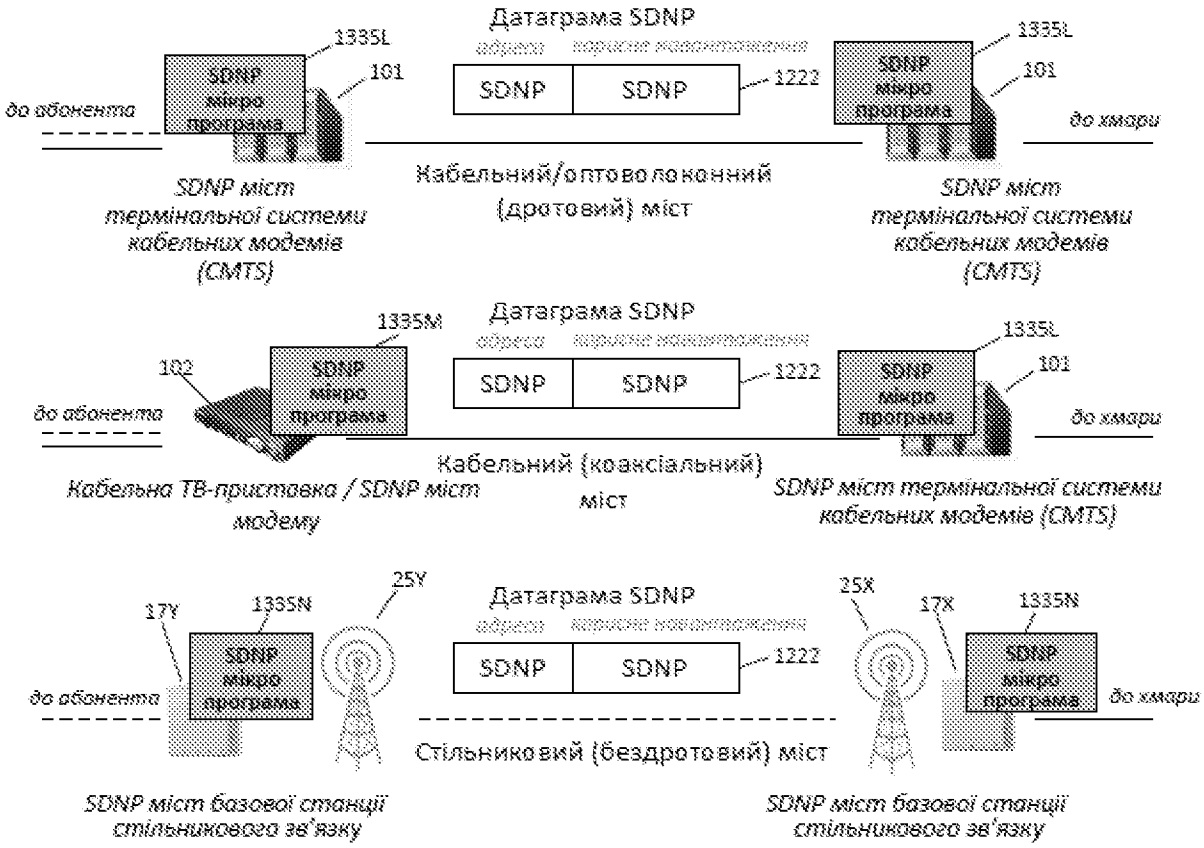


Рис. 29B

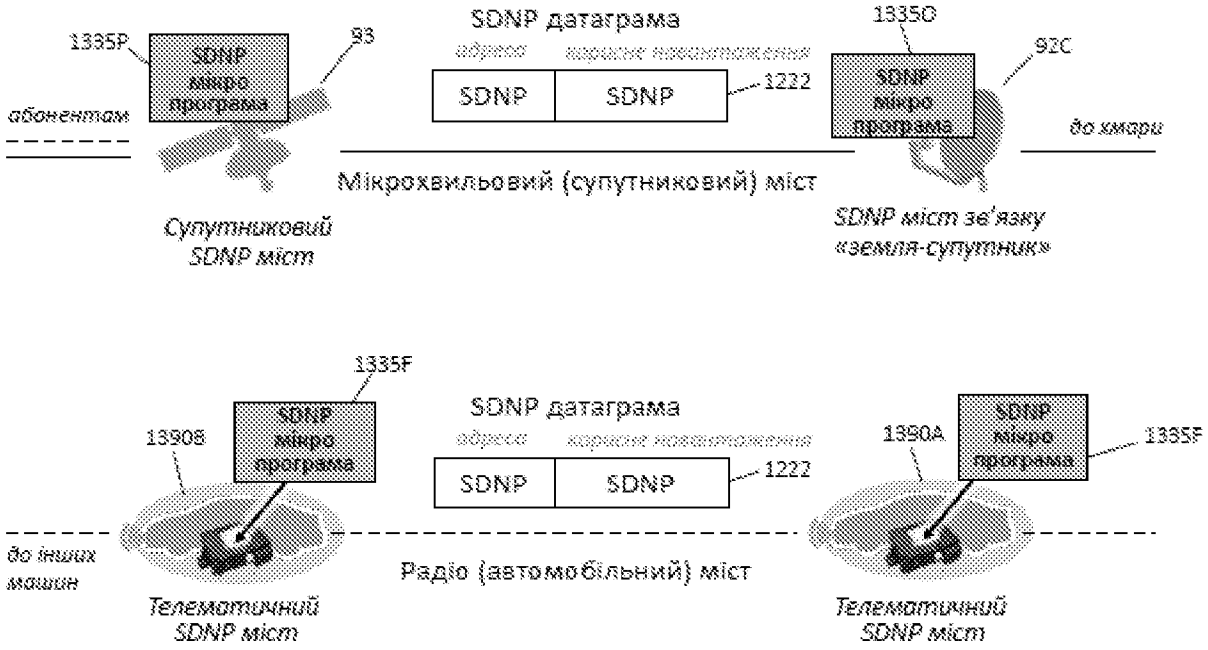


Рис. 29C

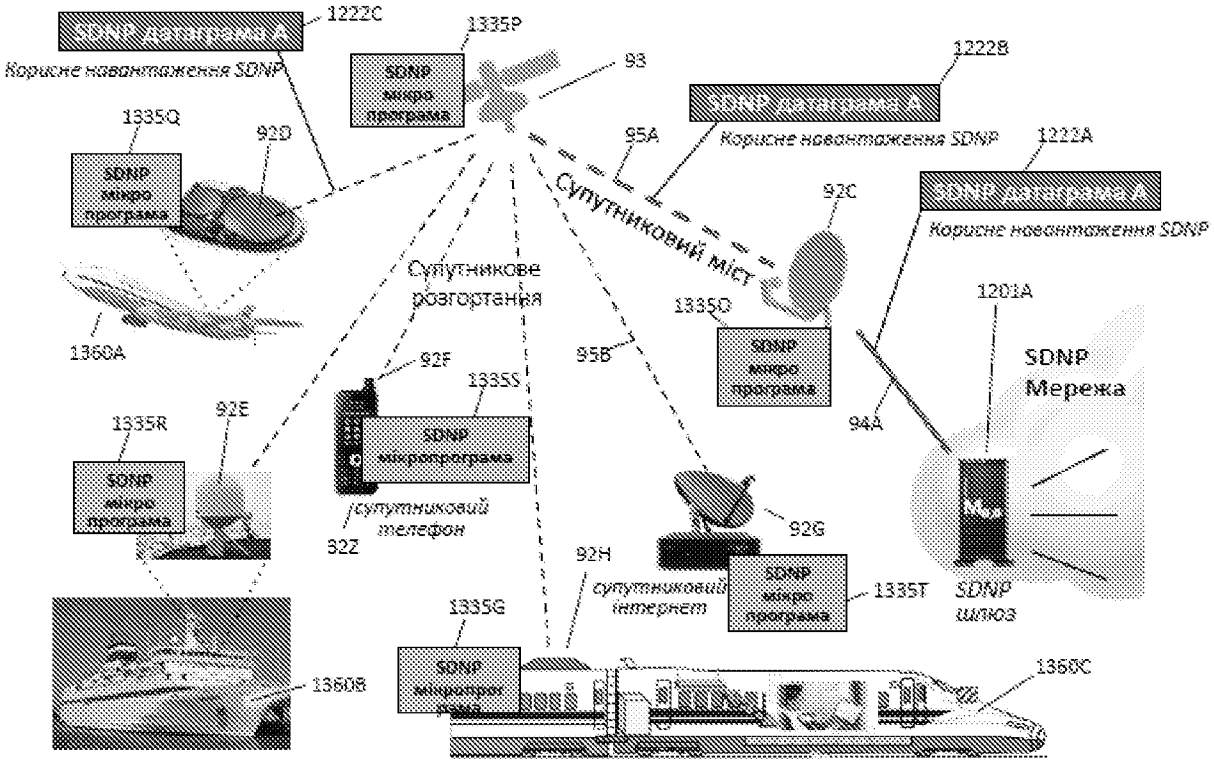


Рис. 30

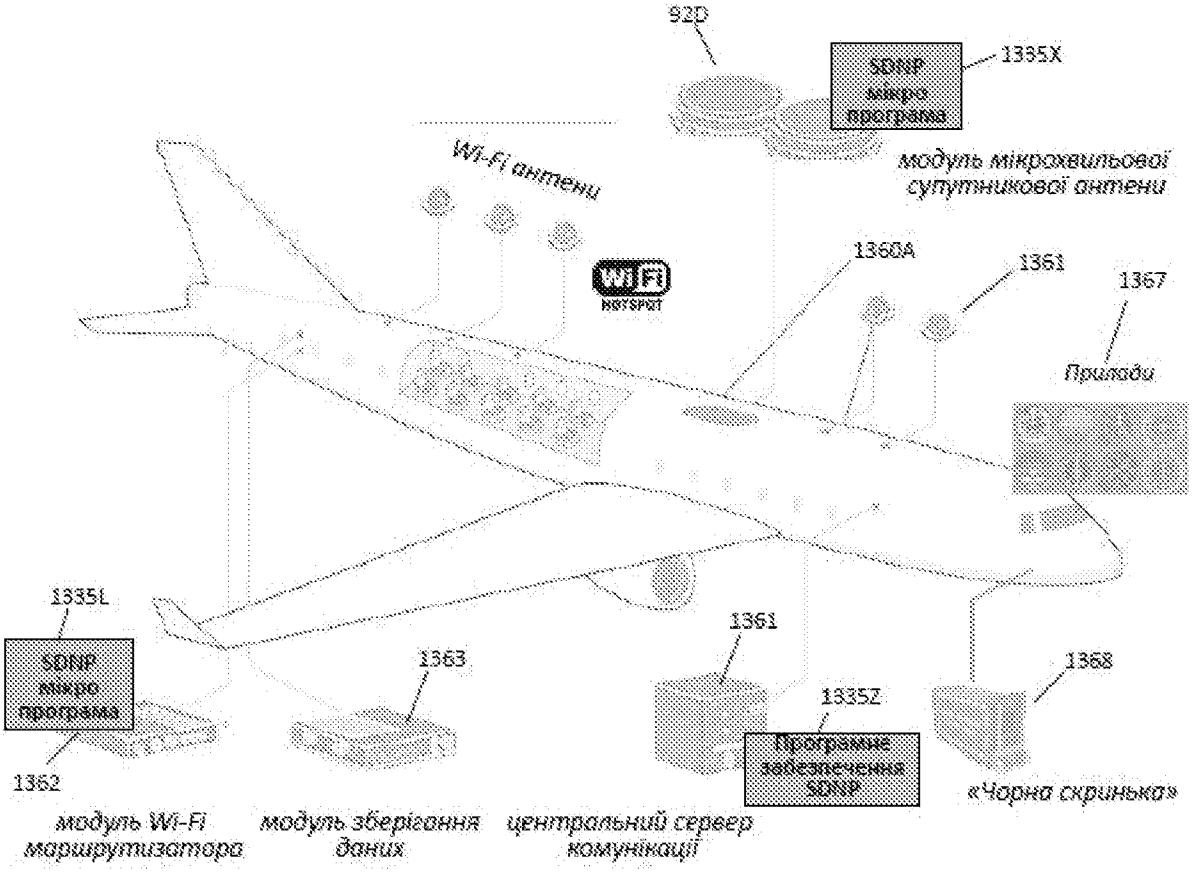


Рис. 31A

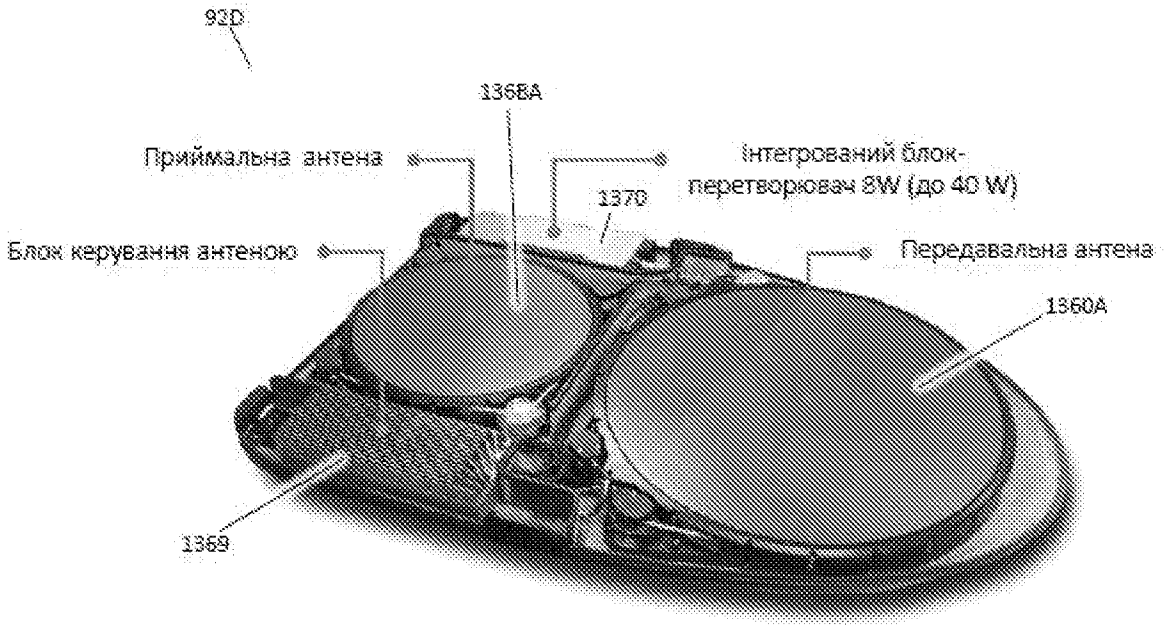


Рис. 31B

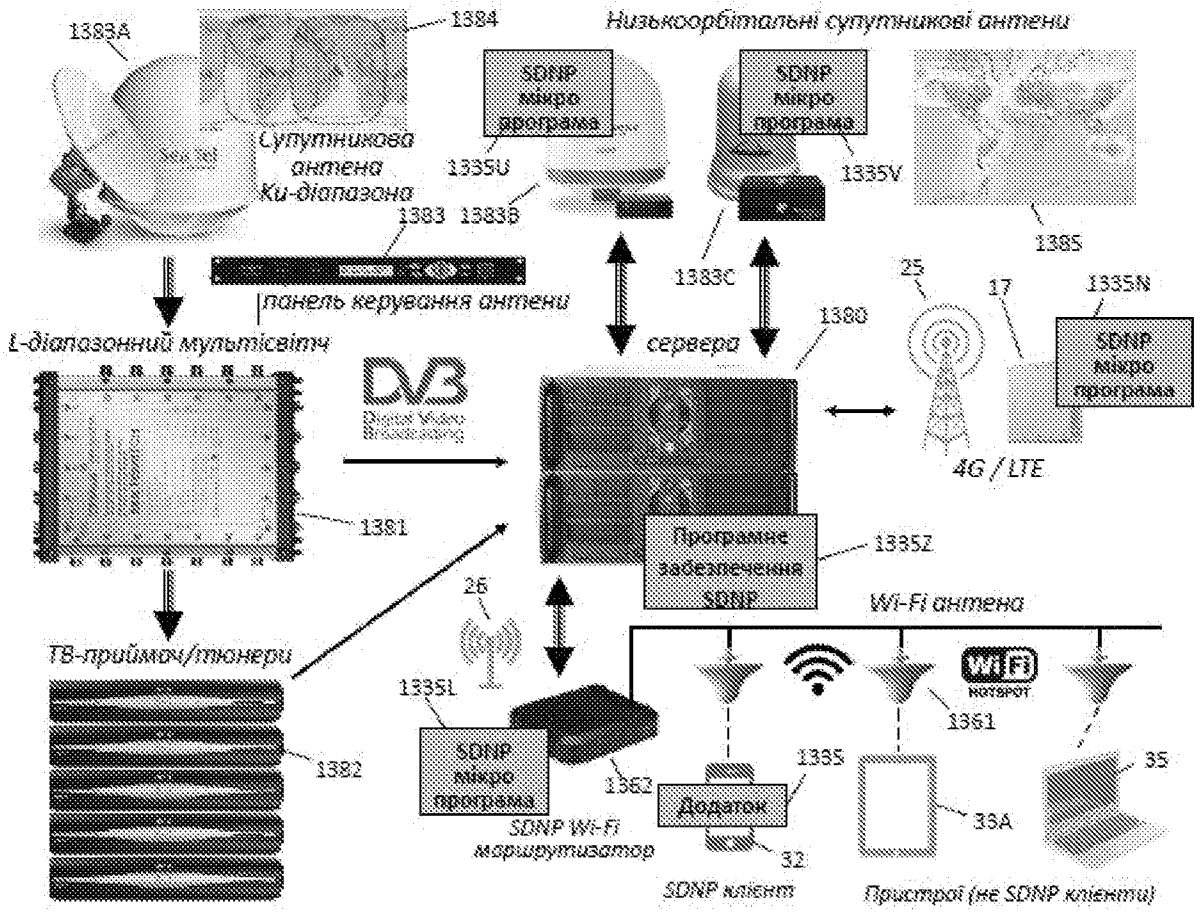

1383A
1384
Низькоорбітальні супутникові антени
SDNP мікро програма
1335U
SDNP мікро програма
1335V
1385
Супутникова антена Ku-діапазона
1383
1383B
1383C
панель керування антени
25
17
1335N
L-діапазонний мультисвітч
сервера
1380
SDNP мікро програма
4G / LTE
1381
Програмне забезпечення SDNP
1335Z
26
Wi-Fi антена
ТВ-приймач/тюнери
1335L
1361
1382
SDNP мікро програма
1362
1335
35
Додаток
36A
SDNP Wi-Fi маршрутизатор
32
SDNP клієнт
Пристрої (не SDNP клієнти)

Рис. 32

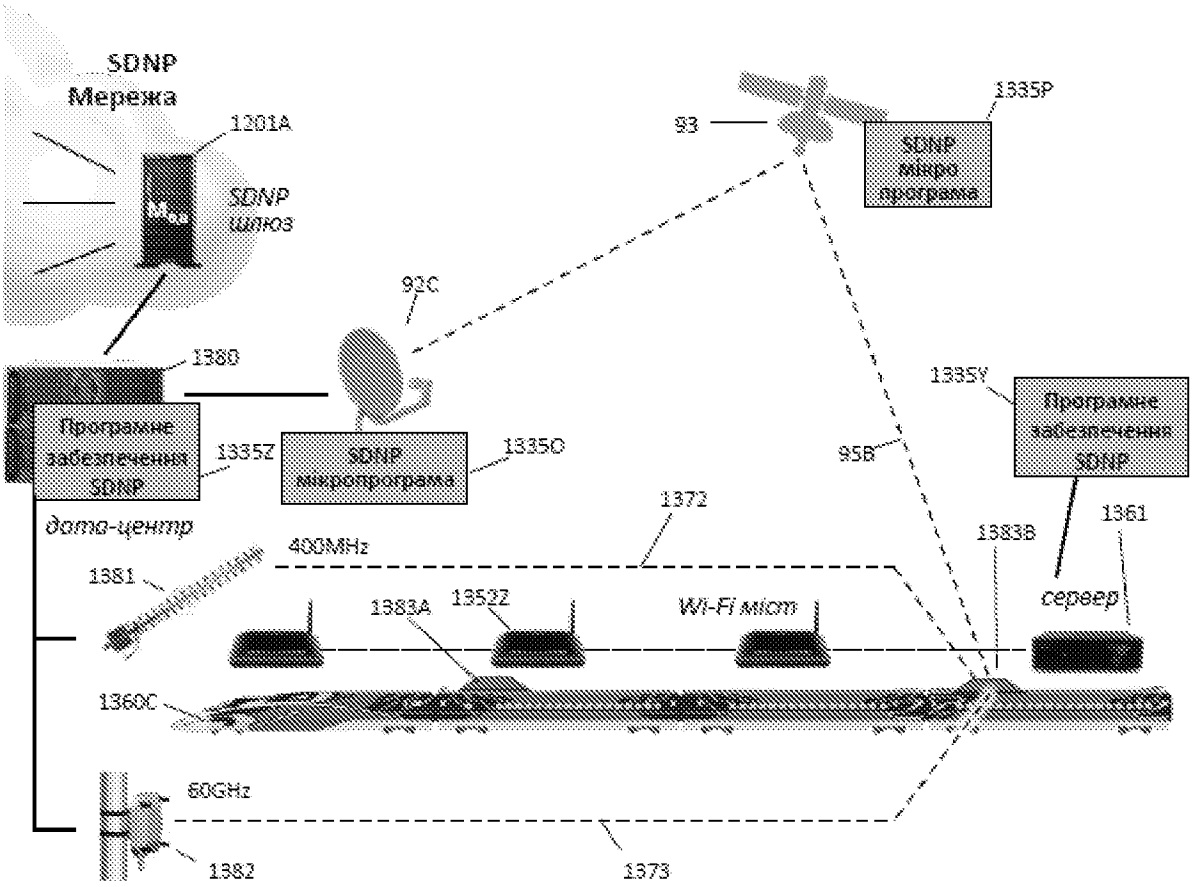

SDNP
Мережа
1201A
SDNP
шлюз
93
1335P
SDNP
мікро
програма
92C
1380
Програмне
забезпечення
SDNP
1335Z
SDNP
мікропрограма
1335O
95B
1335Y
Програмне
забезпечення
SDNP
дата-центр
1372
400MHz
1361
1383B
1381
1383A
1352Z
Wi-Fi міст
сервер
1360C
60GHz
1382
1373

Рис. 33

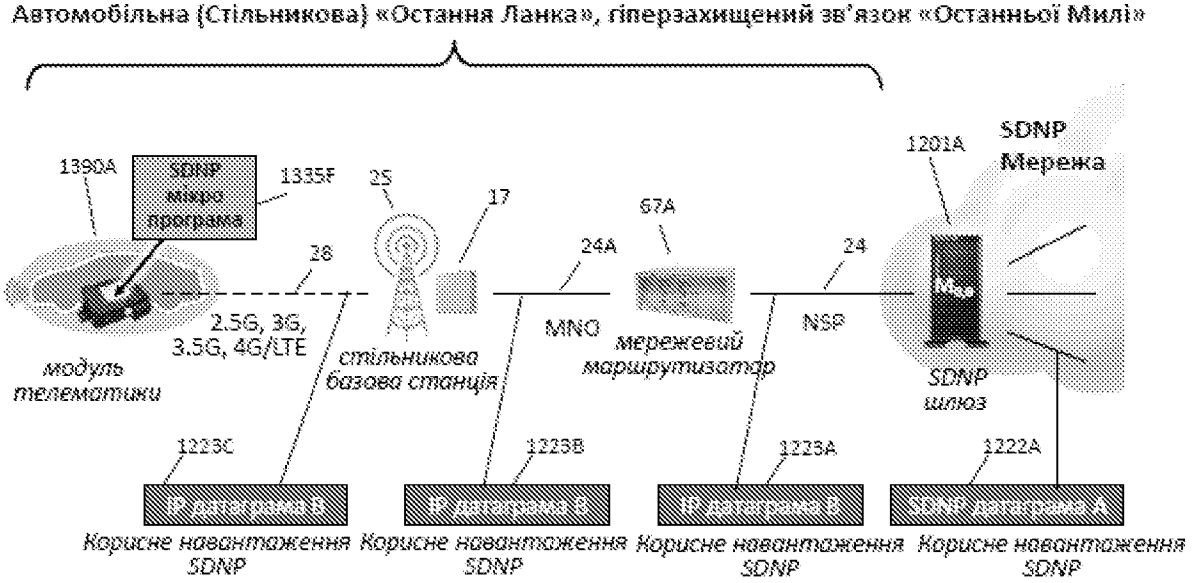

Автомобільна (Стільникова) «Остання Ланка», гіперзахищений зв'язок «Останньої Милі»
1390A
SDNP
мікро
програма
1335F
25
17
67A
1201A
SDNP
Мережа
28
24A
24
2.5G, 3G,
3.5G, 4G/LTE
MNO
NSP
модуль
телематики
стільникова
базова станція
мережевий
маршрутизатор
SDNP
шлюз
1223C
1223B
1223A
1222A
IP датаграма B
IP датаграма B
IP датаграма B
SDNP датаграма A
Корисне навантаження
SDNP
Корисне навантаження
SDNP
Корисне навантаження
SDNP
Корисне навантаження
SDNP

Рис. 34

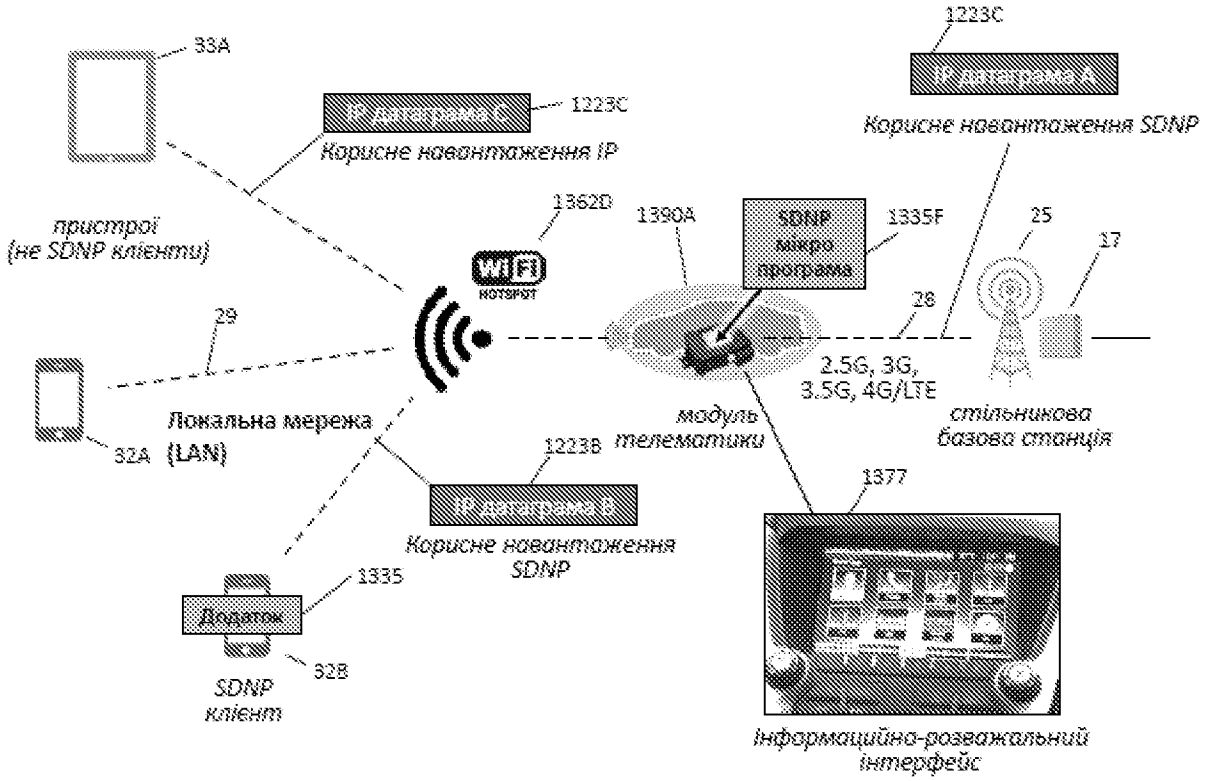

1223C
IP датаграма A
Корисне навантаження SDNP
33A
IP датаграма C
1223C
Корисне навантаження IP
пристрої
(не SDNP клієнти)
1362D
WiFi
HOTSPOT
1390A
SDNP
мікро
програма
1335F
25
17
28
29
2.5G, 3G,
3.5G, 4G/LTE
32A
Локальна мережа
(LAN)
модуль
телематики
стільникова
базова станція
1223B
IP датаграма B
Корисне навантаження
SDNP
1377
1335
Додаток
32B
SDNP
клієнт
інформаційно-розважальний
інтерфейс

Рис. 35

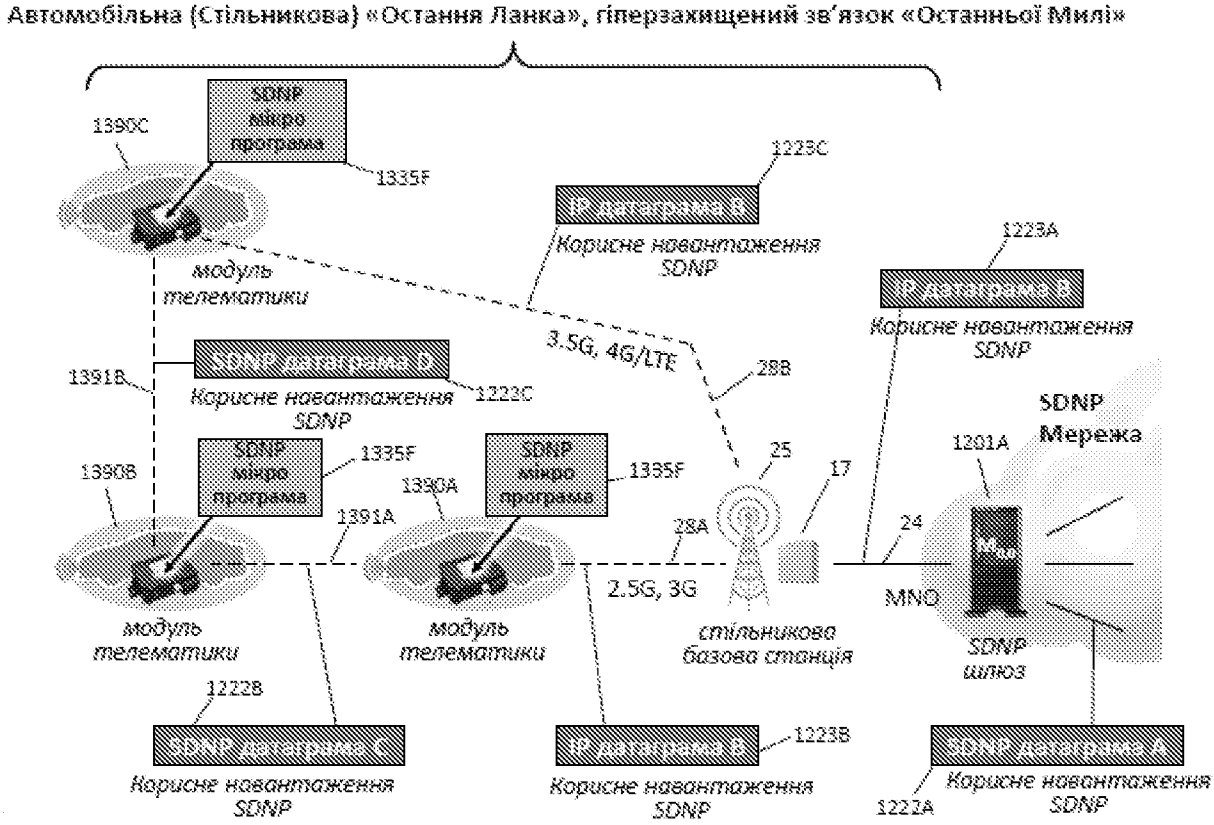

Автомобільна (Стільникова) «Остання Ланка», гіперзахищений зв'язок «Останньої Милі»
SDNP
мікро
програма
1390C
1335F
модуль
телематики
1223C
IP датаграма B
Корисне навантаження
SDNP
1223A
IP датаграма A
Корисне навантаження
SDNP
3.5G, 4G/LTE
28B
1391B
SDNP датаграма D
1222C
Корисне навантаження
SDNP
SDNP
Мережа
1201A
1390B
1390A
1391A
28A
25
17
24
2.5G, 3G
MNO
модуль
телематики
модуль
телематики
стільникова
базова станція
SDNP
шлюз
1222B
SDNP датаграма C
Корисне навантаження
SDNP
IP датаграма B
1223B
Корисне навантаження
SDNP
1222A
SDNP датаграма A
Корисне навантаження
SDNP

Рис. 36

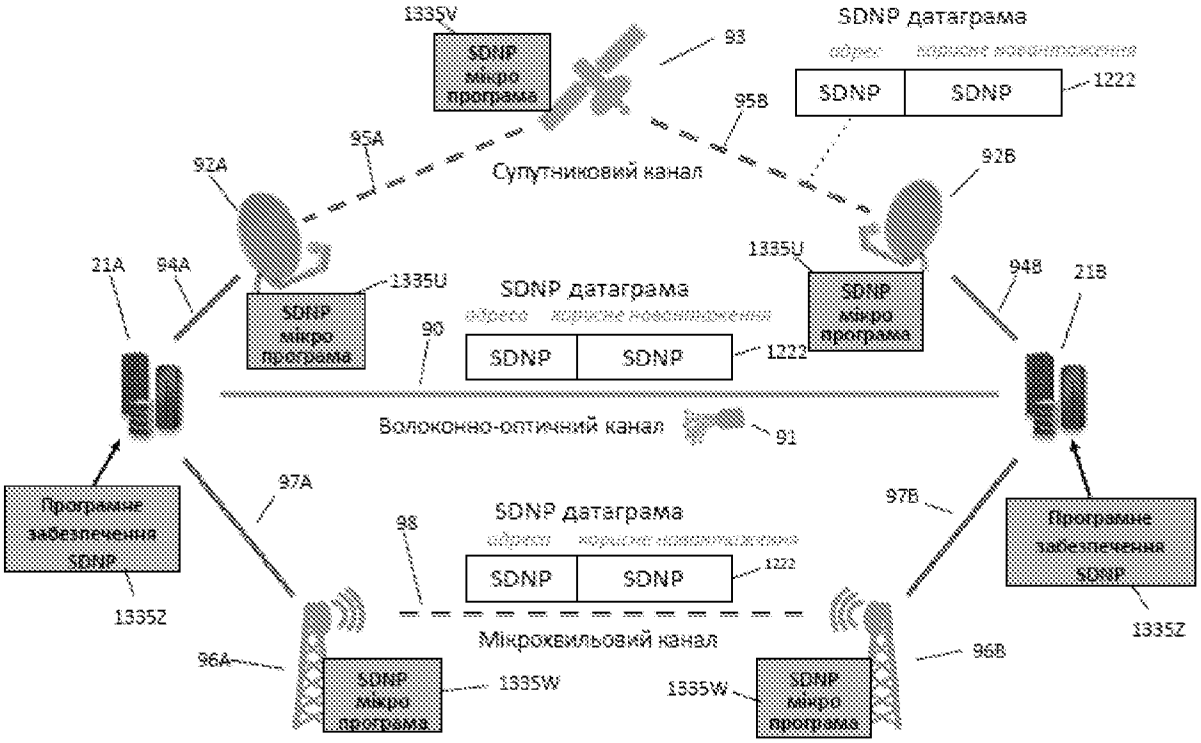

1335V
SDNP мікро програма
93
SDNP датаграма
адреса корисне навантаження
SDNP SDNP
1222
95B
95A
Супутниковий канал
92A
92B
21A
94A
1335U
SDNP мікро програма
SDNP датаграма
адреса корисне навантаження
SDNP SDNP
1222
90
1335U
SDNP мікро програма
94B
21B
Волоконно-оптичний канал
91
97A
97B
Програмне забезпечення SDNP
1335Z
98
SDNP датаграма
адреса корисне навантаження
SDNP SDNP
1222
Мікрохвильовий канал
Програмне забезпечення SDNP
1335Z
96A
SDNP мікро програма
1335W
1335W
SDNP мікро програма
96B

Рис. 37

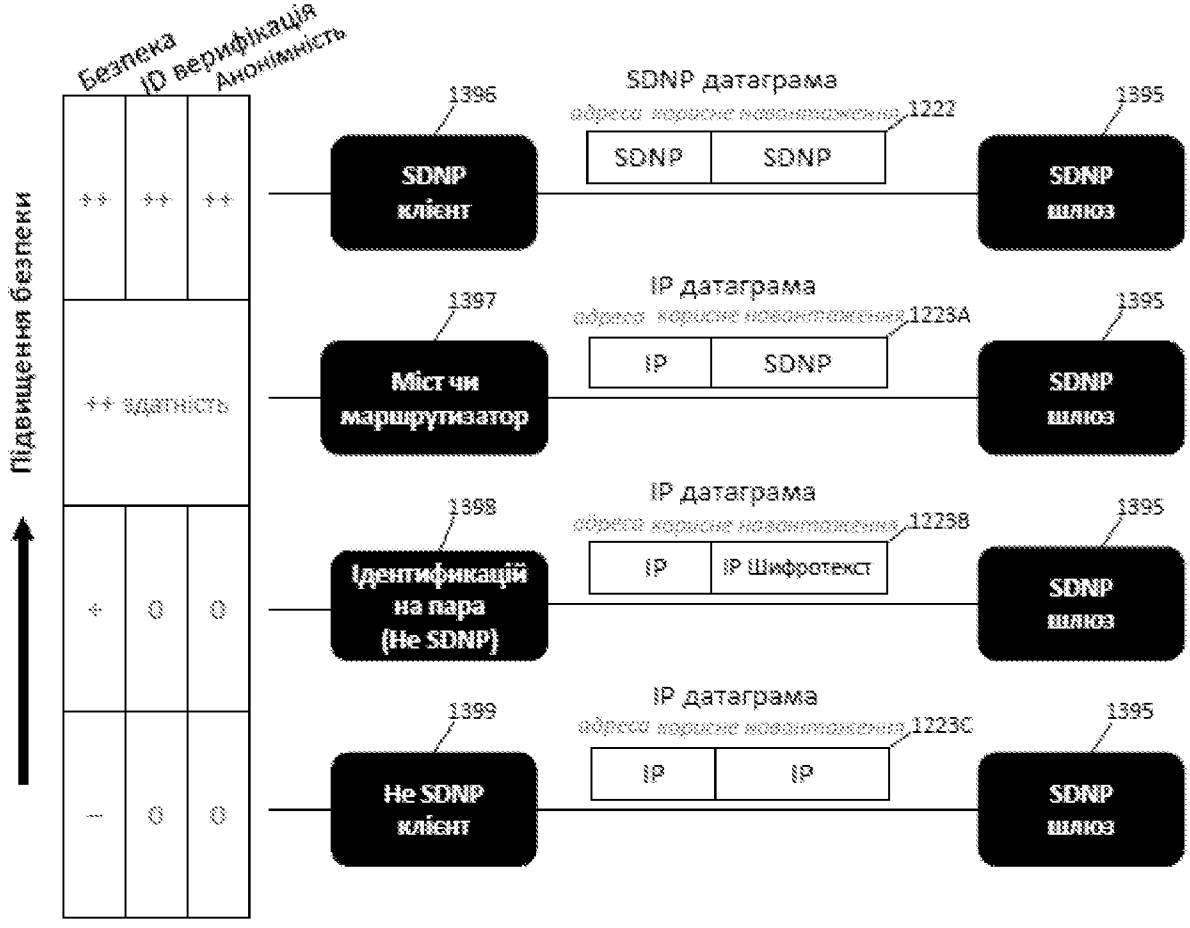

Безпека
ID верифікація
Анонімність
Підвищення безпеки
++
++
++
++ вдатність
+
0
0
–
0
0
1396
SDNP клієнт
SDNP датаграма
адреса корисне навантаження
SDNP SDNP
1222
1395
SDNP шлюз
1397
Міст чи маршрутизатор
IP датаграма
адреса корисне навантаження
IP SDNP
1223A
1395
SDNP шлюз
1398
Ідентифікаційна пара (Не SDNP)
IP датаграма
адреса корисне навантаження
IP IP Шифротекст
1223B
1395
SDNP шлюз
1399
Не SDNP клієнт
IP датаграма
адреса корисне навантаження
IP IP
1223C
1395
SDNP шлюз

Рис. 38

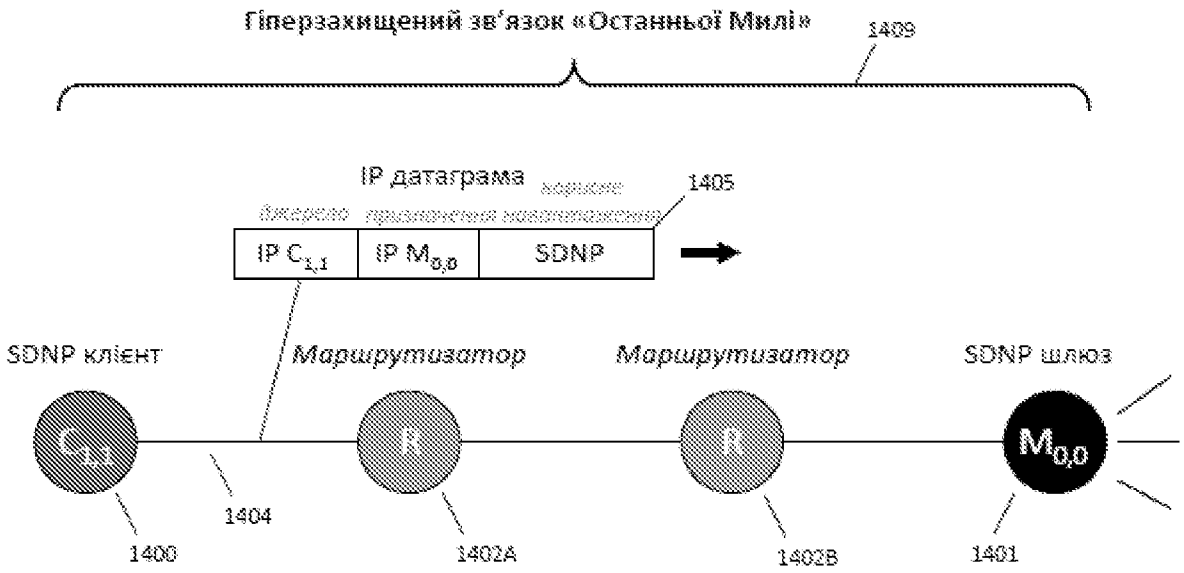


Рис. 39

Одномаршрутний зв'язок SDNP «Останньої Милі», статична адресація

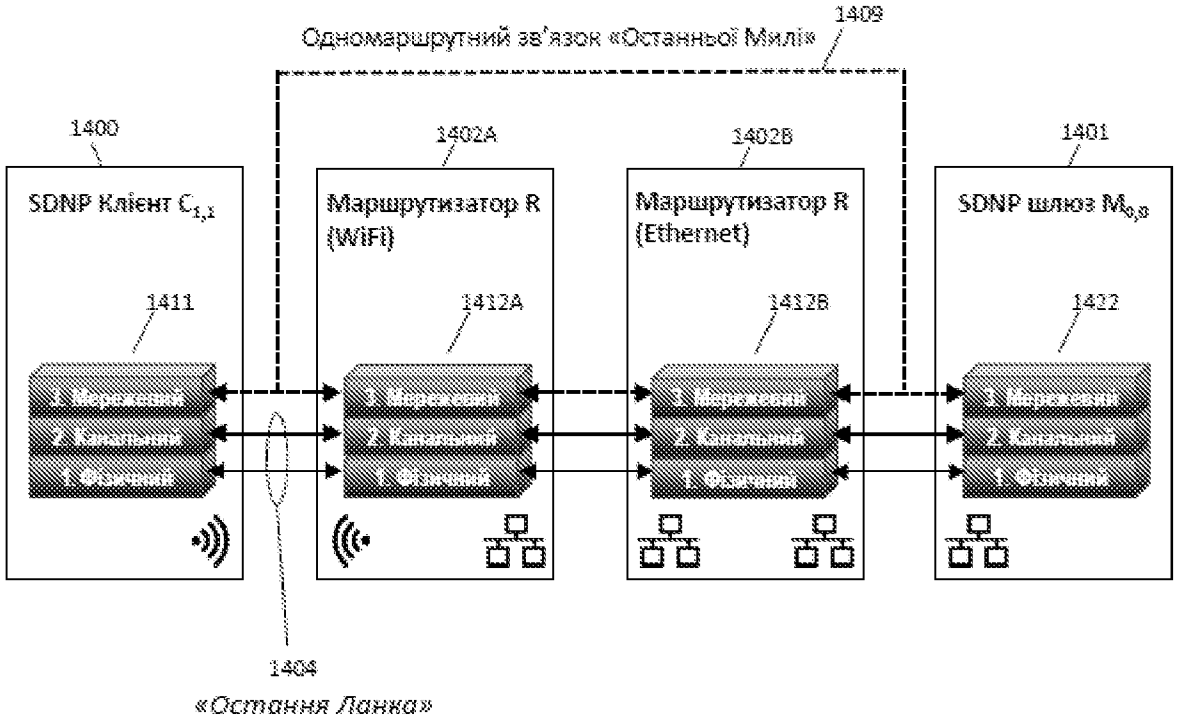


Рис. 40А

Одномаршрутний зв'язок SDNP «Останньої Милі», статична адресація клієнта

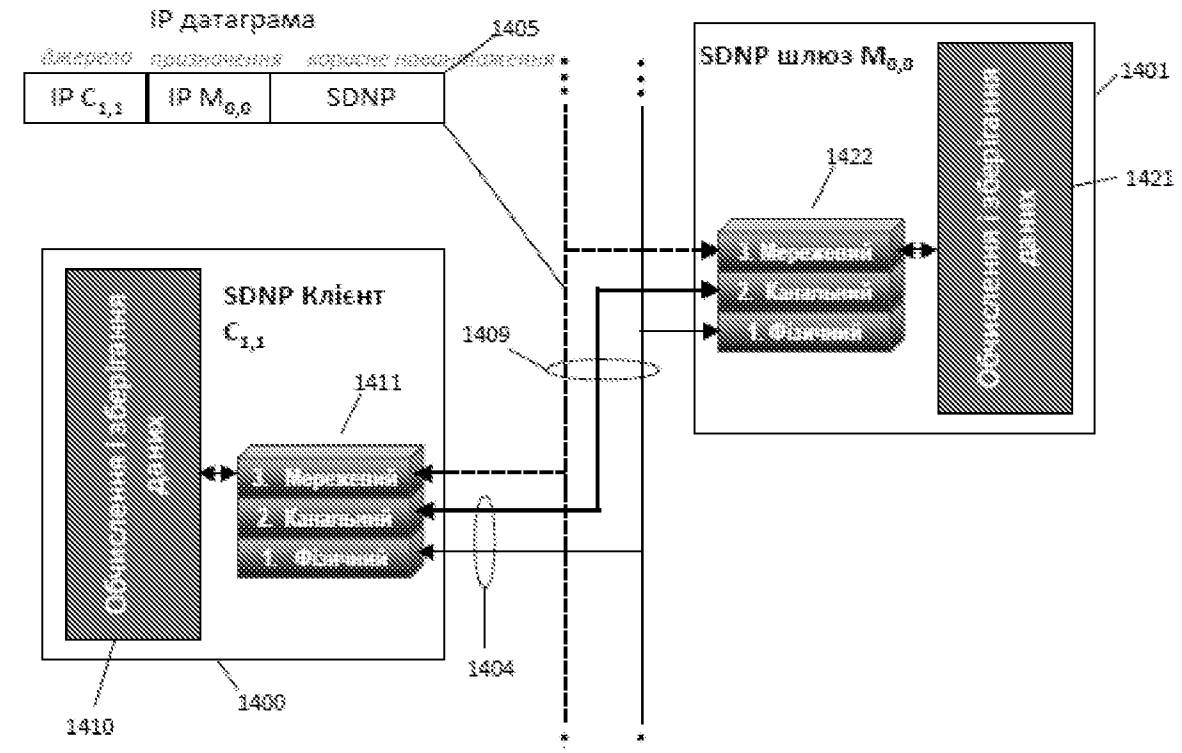


Рис. 40В

Одномаршрутний зв'язок SDNP «Останньої Милі», динамічна адресація клієнта

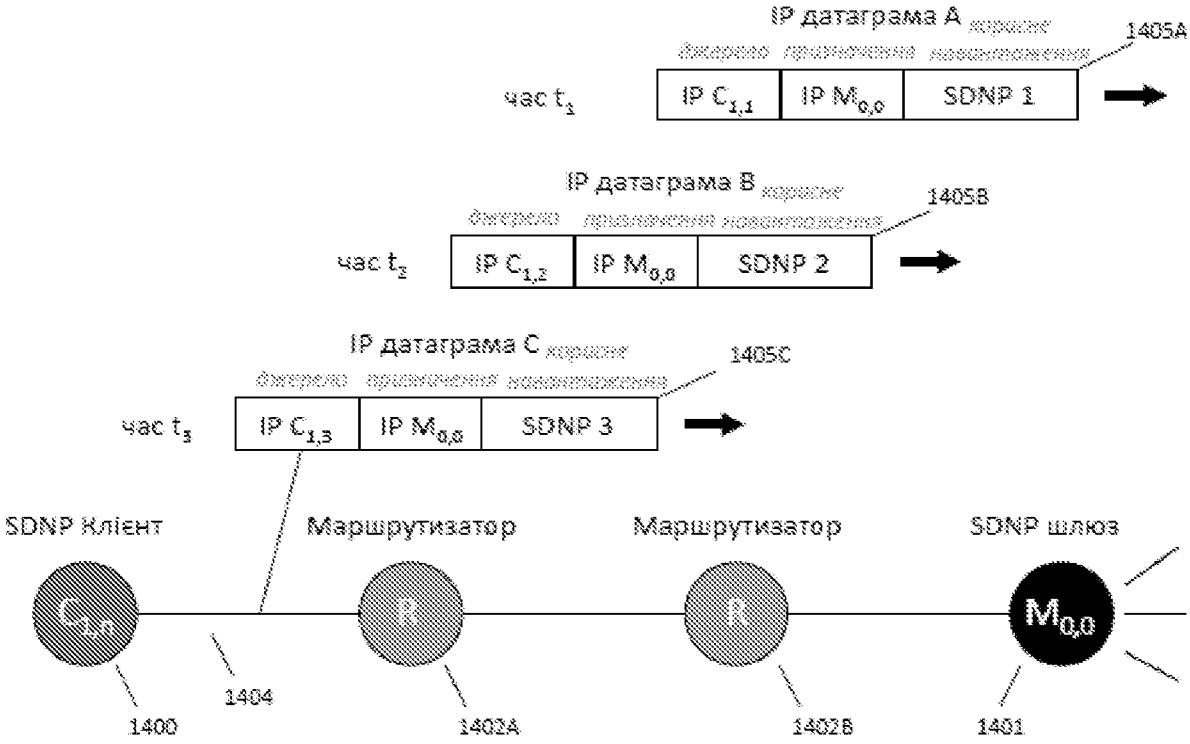
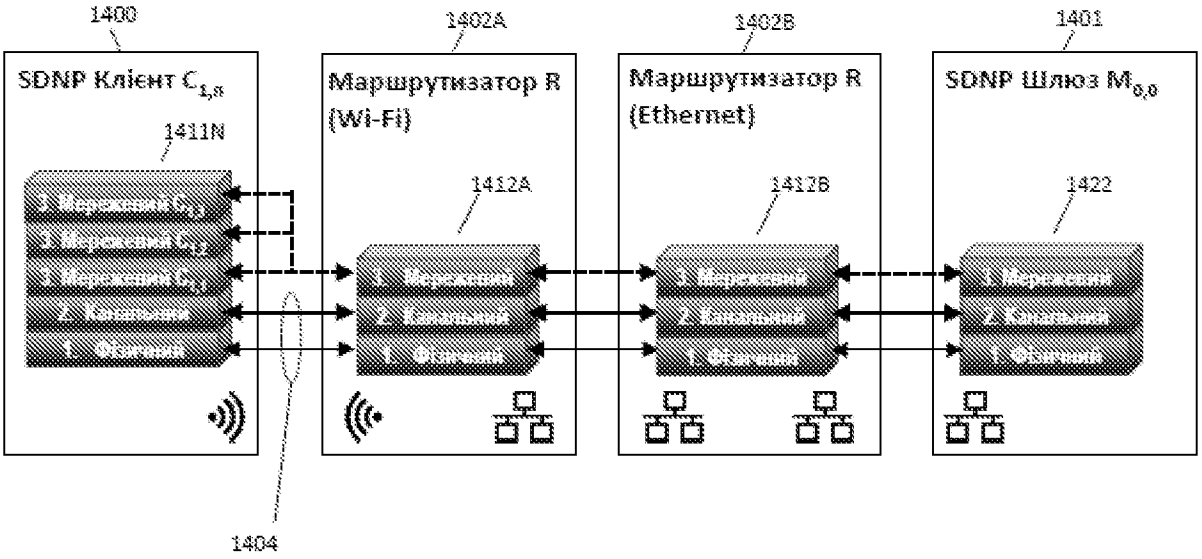


Рис. 41

Одномаршрутний зв'язок SDNP «Останньої Милі», динамічна адресація клієнта



Одноріневе PHY-з'єднання «Останньої Лінії"

Рис. 42A

Одномаршрутний зв'язок SDNP «Останньої Милі», динамічна адресація клієнта

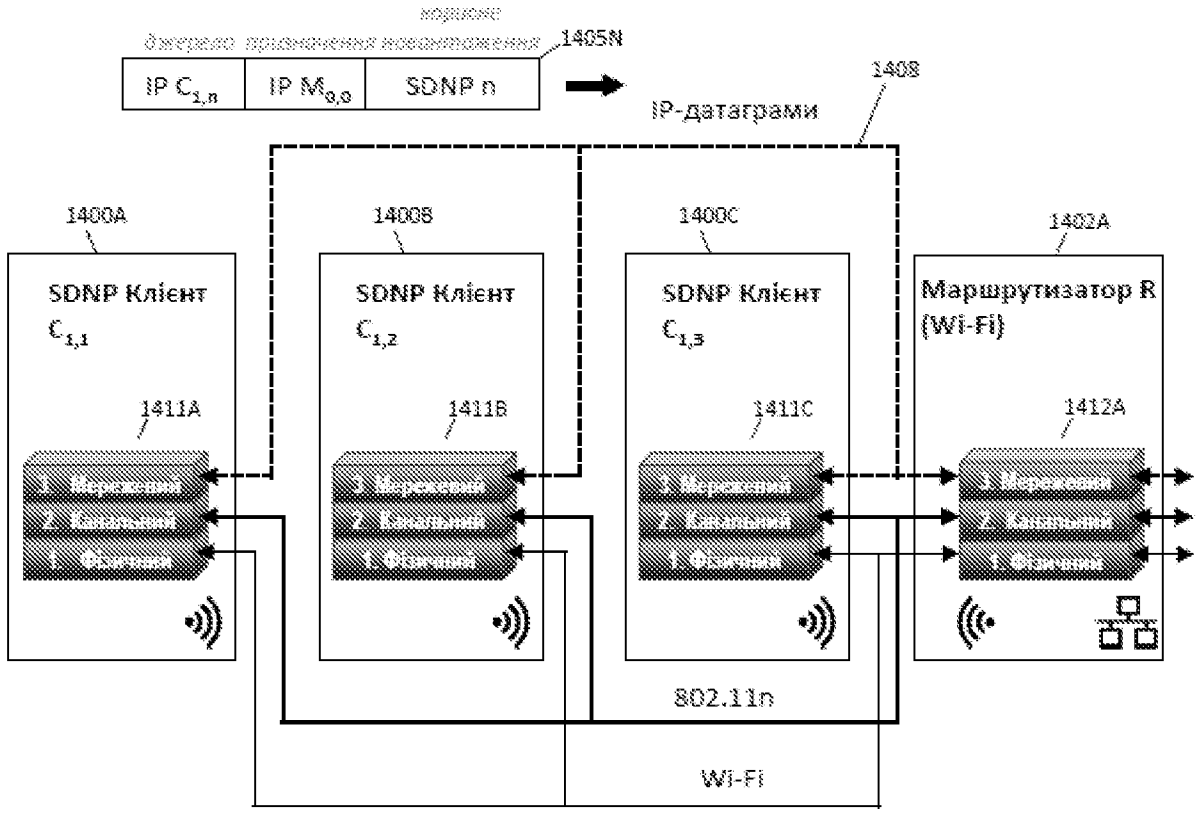


Рис. 42B

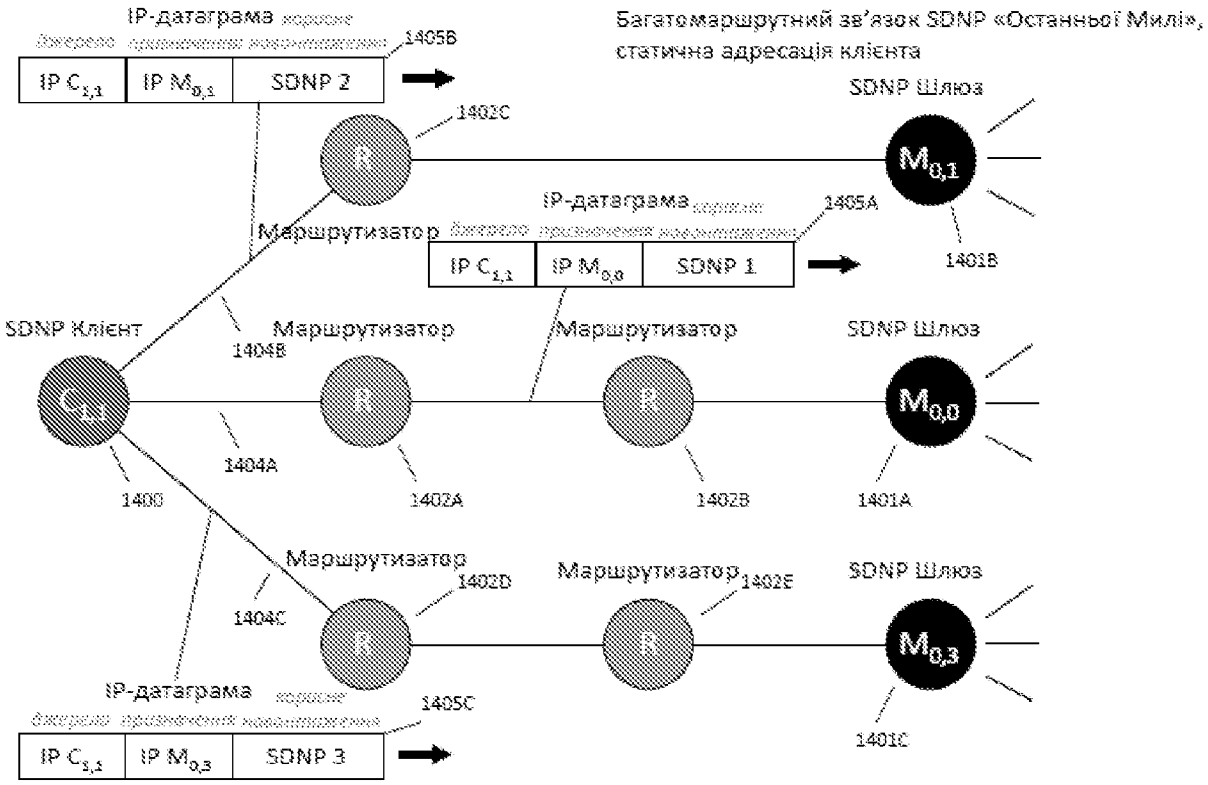


Рис. 43

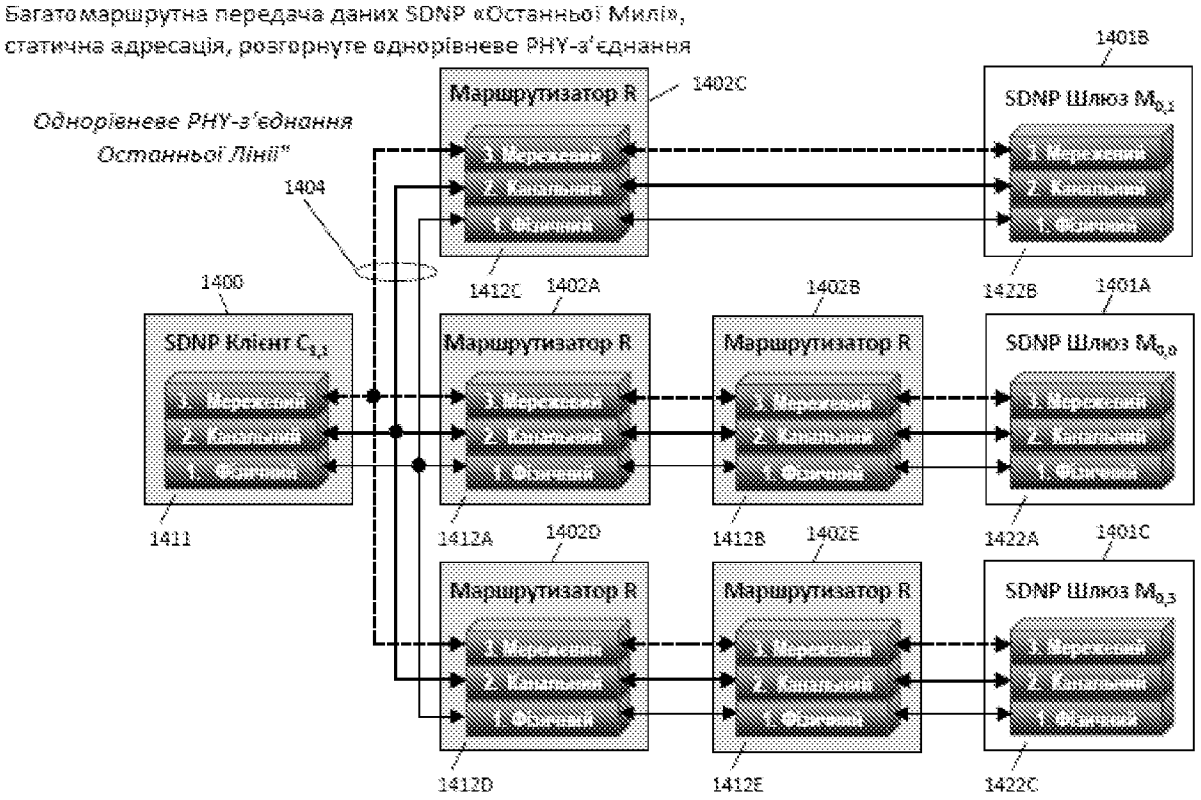


Рис. 44A

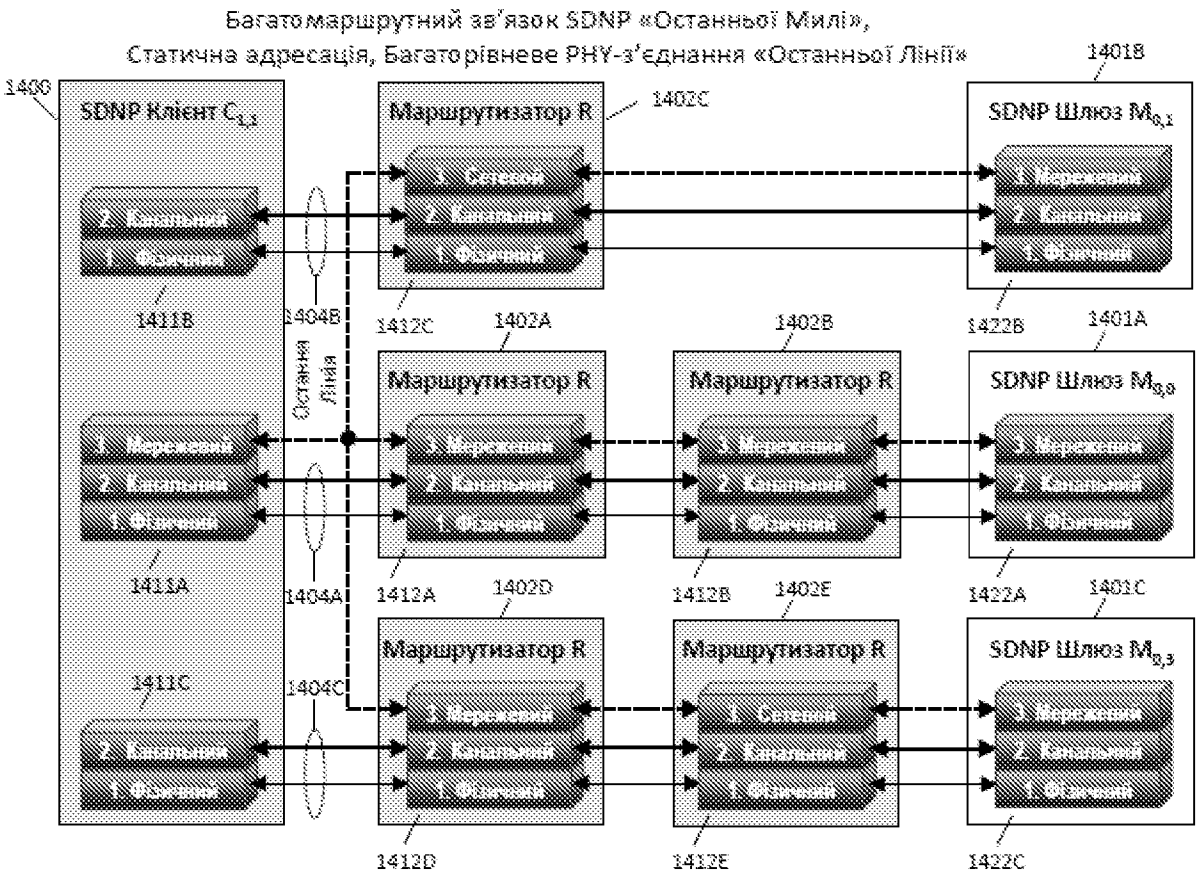

Багатомаршрутний зв'язок SDNP «Останньої Милі»,
Статична адресація, Багаторівневе PHY-з'єднання «Останньої Лінії»
1400
SDNP Клієнт $C_{1,1}$
1411B
1411A
1411C
1404B
1404A
1404C
Остання Лінія
Маршрутизатор R
1402C
1412C
1402A
1412A
1402D
1412D
1402B
1412B
1402E
1412E
SDNP Шлюз $M_{0,1}$
1401B
1422B
SDNP Шлюз $M_{0,0}$
1401A
1422A
SDNP Шлюз $M_{0,3}$
1401C
1422C

Рис. 44B

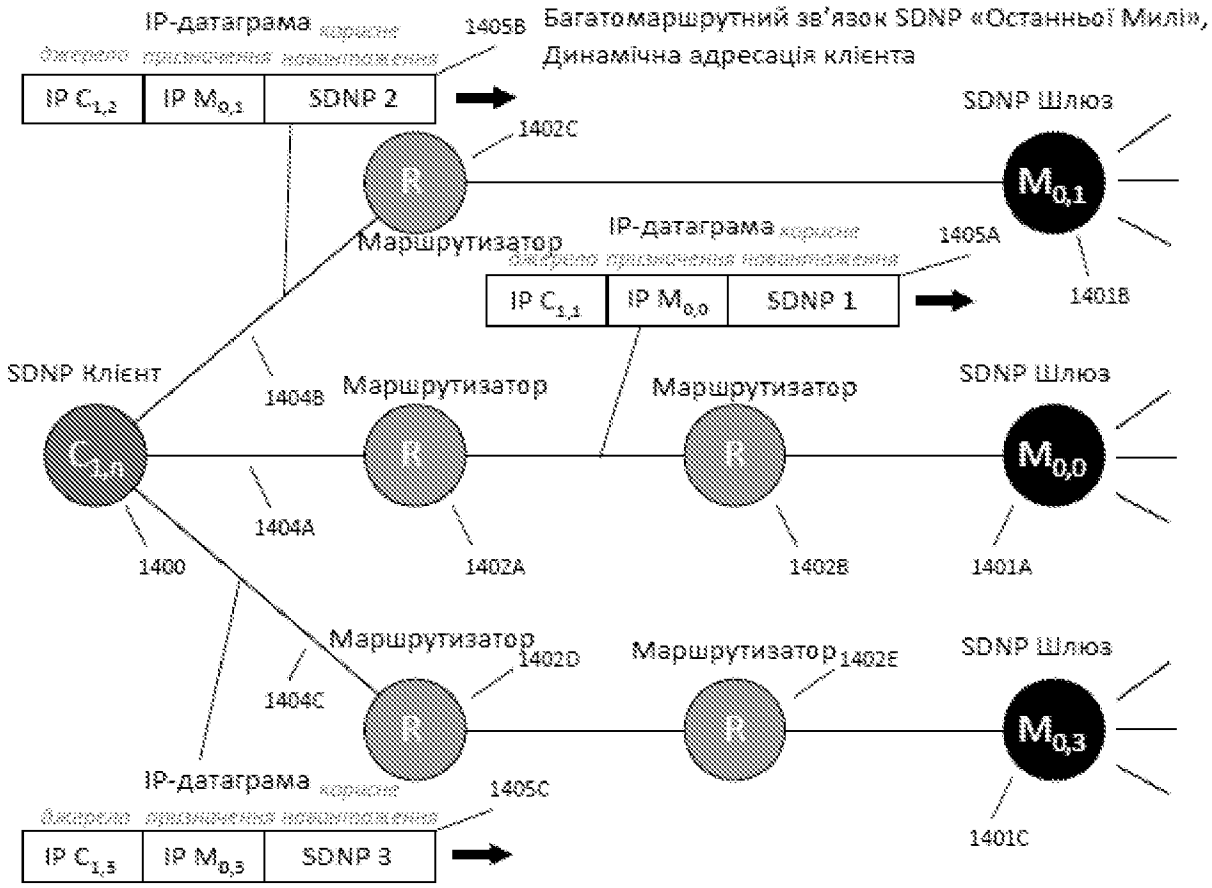

IP-датаграма
1405B
Багатомаршрутний зв'язок SDNP «Останньої Милі»,
Динамічна адресація клієнта
IP $C_{1,2}$
IP $M_{0,1}$
SDNP 2
SDNP Шлюз
1402C
R
$M_{0,1}$
Маршрутизатор
IP-датаграма
1405A
IP $C_{1,1}$
IP $M_{0,0}$
SDNP 1
1401B
SDNP Клієнт
1404B
Маршрутизатор
Маршрутизатор
SDNP Шлюз
$C_{1,0}$
R
R
$M_{0,0}$
1404A
1400
1402A
1402B
1401A
Маршрутизатор
1402D
Маршрутизатор
1402E
SDNP Шлюз
1404C
R
R
$M_{0,3}$
IP-датаграма
1405C
IP $C_{1,3}$
IP $M_{0,3}$
SDNP 3
1401C

Рис. 45

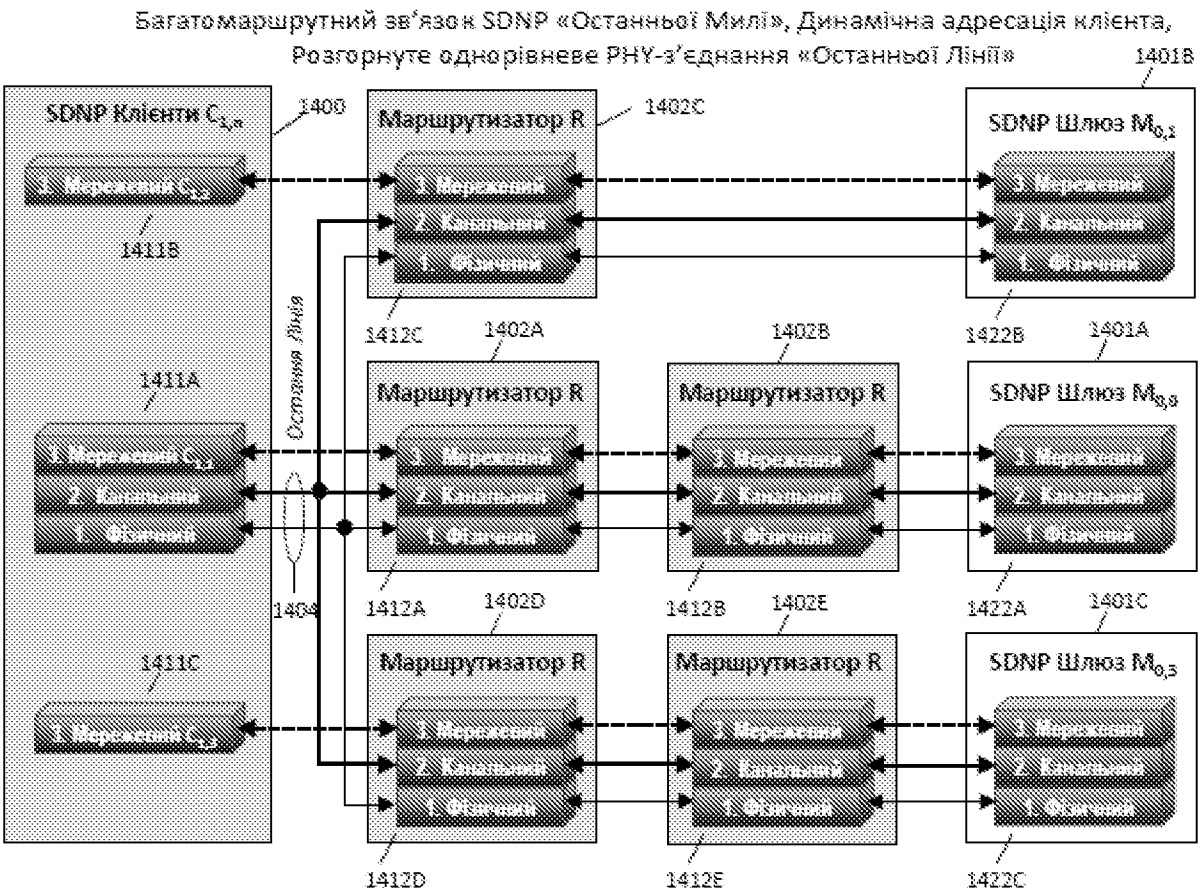

Багатомаршрутний зв'язок SDNP «Останньої Милі», Динамічна адресація клієнта,
Розгорнуте одноріневе PHY-з'єднання «Останньої Лінії»
SDNP Клієнти $C_{1,n}$
1400
Маршрутизатор R
1402C
SDNP Шлюз $M_{0,1}$
1401B
1411B
1412C
1402A
1422B
1401A
1411A
Остання Лінія
Маршрутизатор R
Маршрутизатор R
SDNP Шлюз $M_{0,0}$
1404
1412A
1402D
1412B
1402E
1422A
1401C
1411C
Маршрутизатор R
Маршрутизатор R
SDNP Шлюз $M_{0,3}$
1412D
1412E
1422C

Рис. 46A

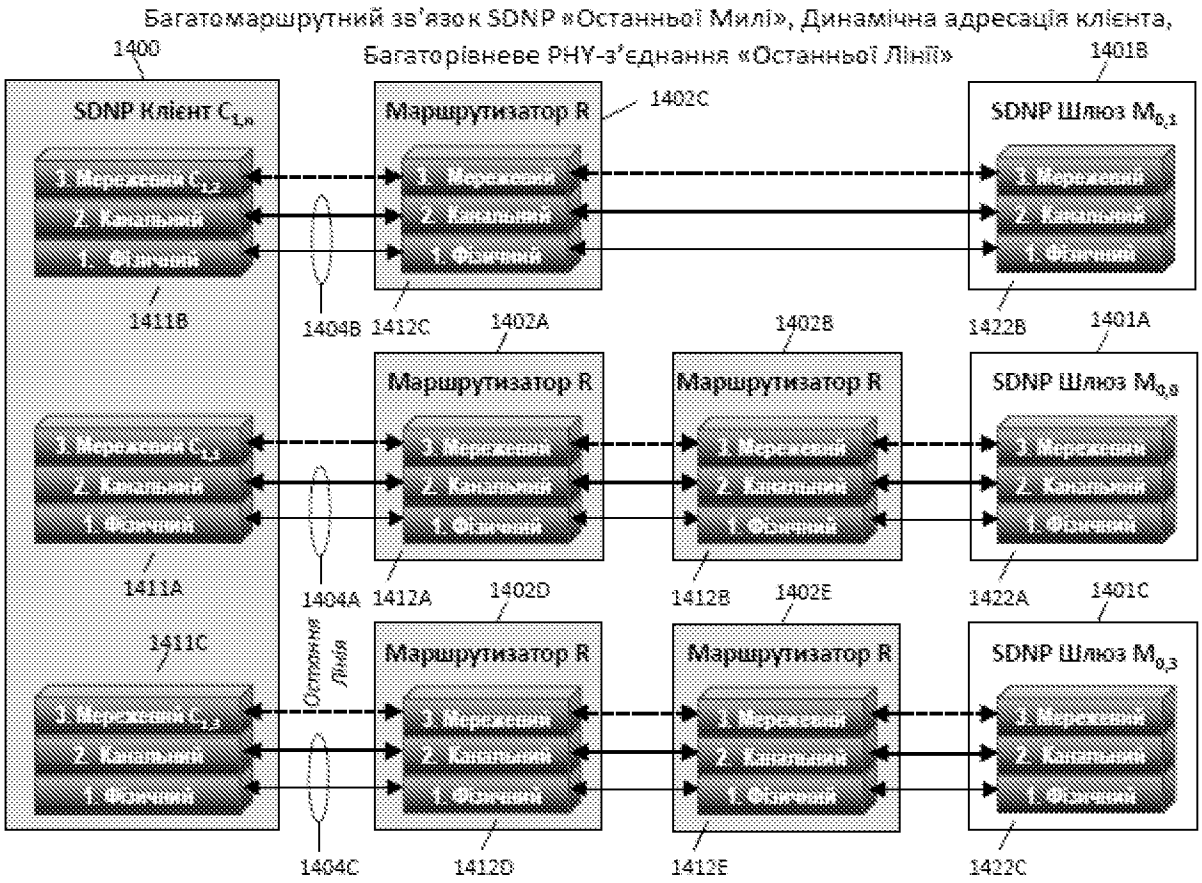

Багатомаршрутний зв'язок SDNP «Останньої Милі», Динамічна адресація клієнта,
Багаторівневе PHY-з'єднання «Останньої Лінії»
1400
SDNP Клієнт $C_{1,n}$
Маршрутизатор R
1402C
SDNP Шлюз $M_{0,1}$
1401B
1411B
1404B
1412C
1402A
1422B
Маршрутизатор R
Маршрутизатор R
SDNP Шлюз $M_{0,2}$
1401A
1411A
1404A
1412A
1402D
1412B
1402E
1422A
1401C
1411C
Остання Лінія
Маршрутизатор R
Маршрутизатор R
SDNP Шлюз $M_{0,3}$
1404C
1412D
1412E
1422C

Рис. 46B

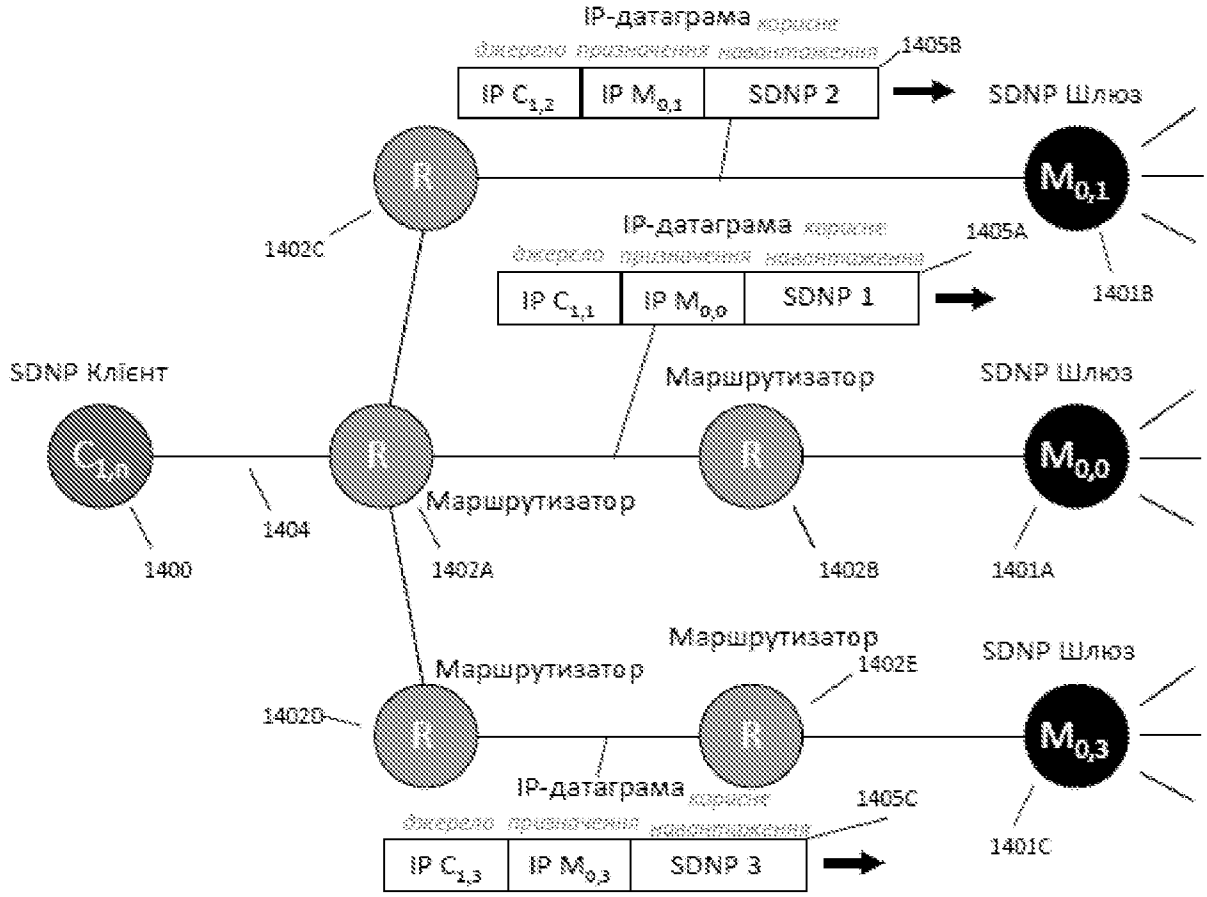

IP-датаграма
1405B
IP C1,2
IP M0,1
SDNP 2
SDNP Шлюз
R
M0,1
1402C
IP-датаграма
1405A
IP C1,1
IP M0,0
SDNP 1
1401B
SDNP Клієнт
Маршрутизатор
SDNP Шлюз
C1,0
R
R
M0,0
1404
Маршрутизатор
1400
1402A
1402B
1401A
Маршрутизатор
1402E
Маршрутизатор
SDNP Шлюз
1402D
R
R
M0,3
IP-датаграма
1405C
IP C1,3
IP M0,3
SDNP 3
1401C

Рис. 47

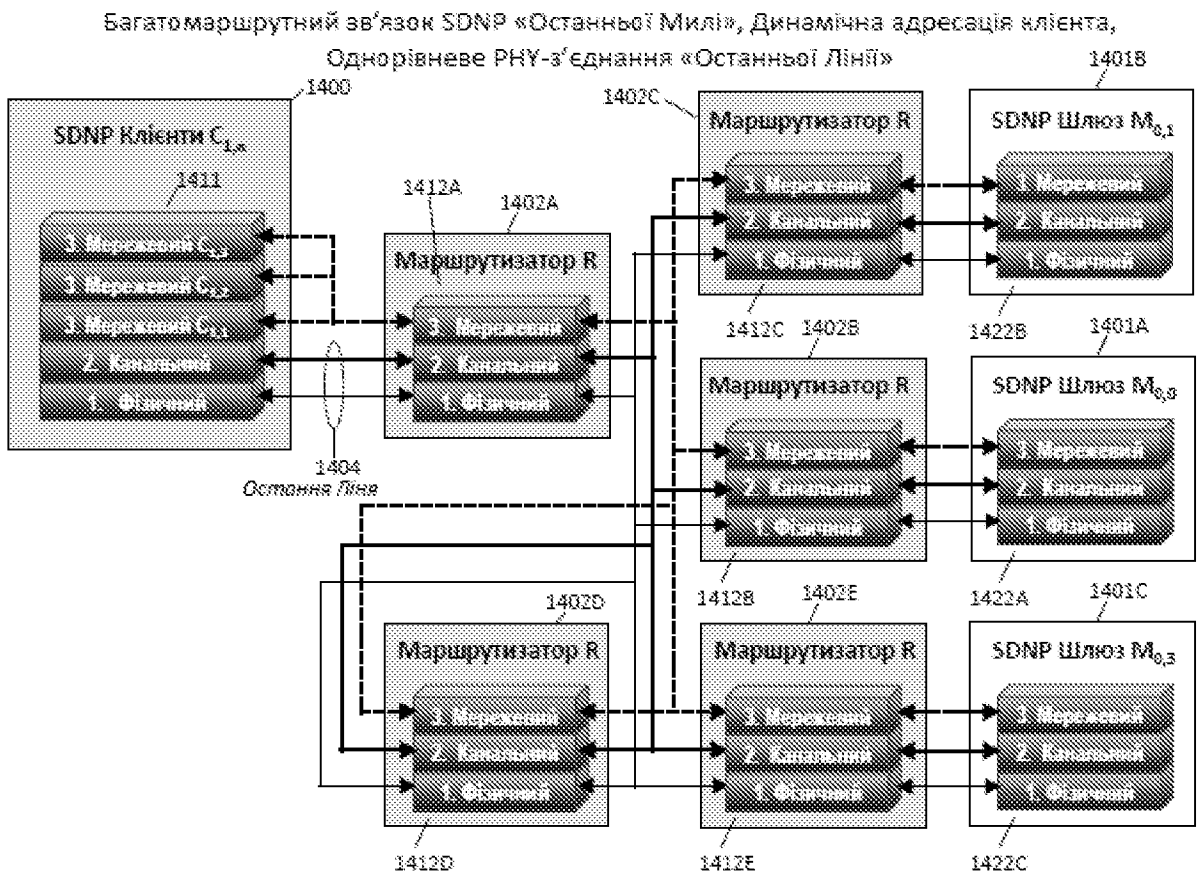

Багатомаршрутний зв'язок SDNP «Останньої Милі», Динамічна адресація клієнта,
Однорівневе PHY-з'єднання «Останньої Лінії»
1400
SDNP Клієнти $C_{1,x}$
1411
1412A
1402A
Маршрутизатор R
1404
Остання Лінія
1402C
Маршрутизатор R
1412C
1402B
Маршрутизатор R
1412B
1402D
Маршрутизатор R
1412D
1402E
Маршрутизатор R
1412E
1401B
SDNP Шлюз $M_{0,1}$
1422B
1401A
SDNP Шлюз $M_{0,2}$
1422A
1401C
SDNP Шлюз $M_{0,3}$
1422C

Рис. 48

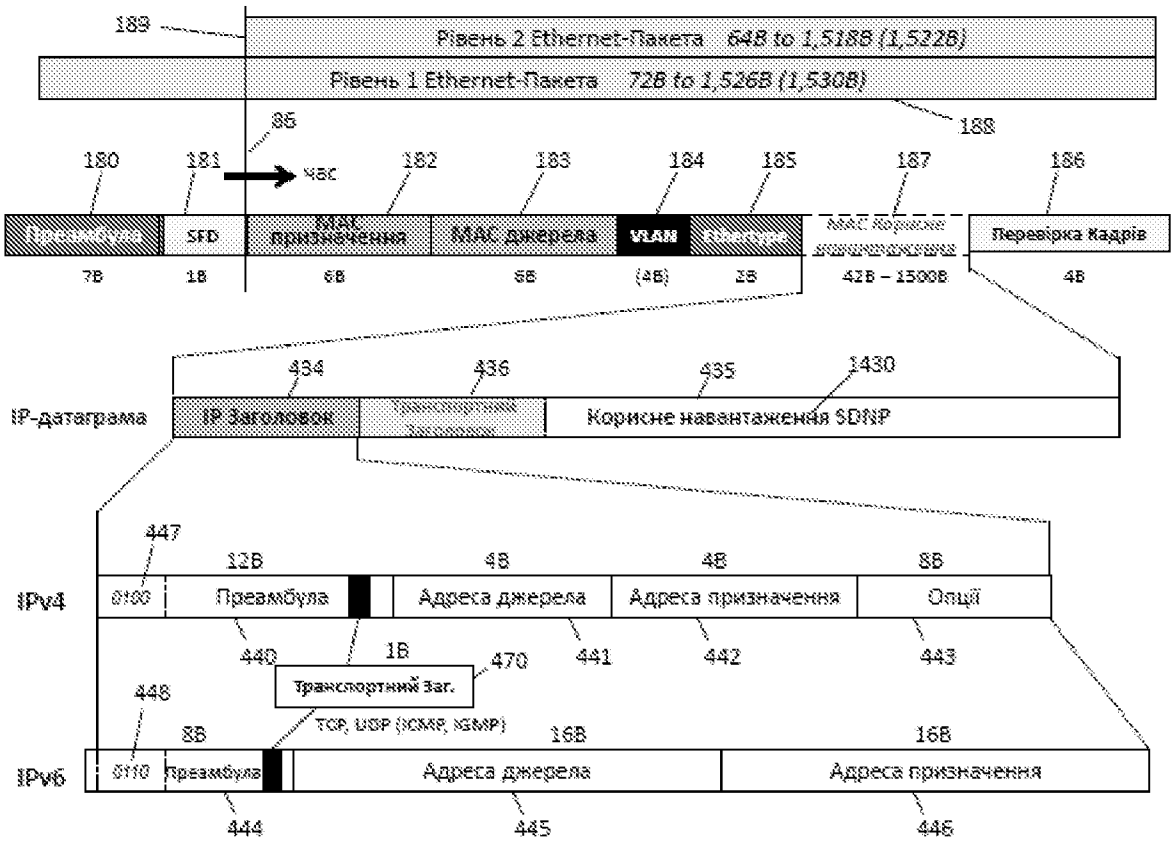


Рис. 49



Остання Лінія Ethernet-пакета (Від Клієнта до Хмари SDNP)

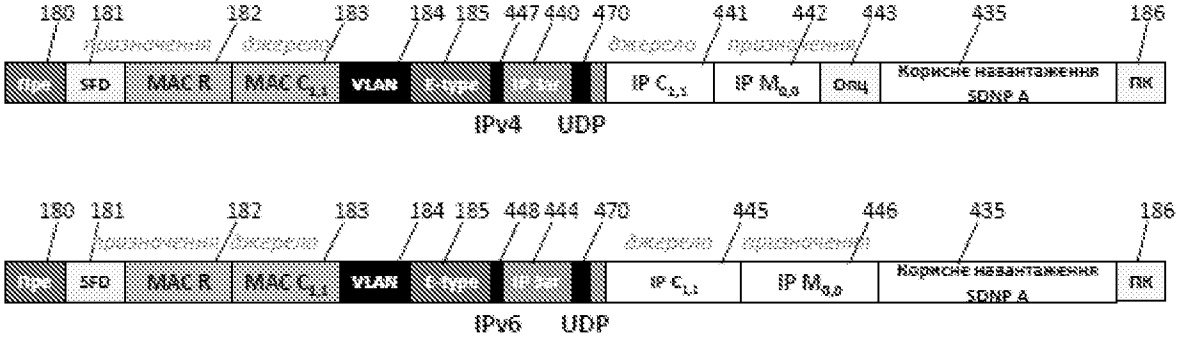
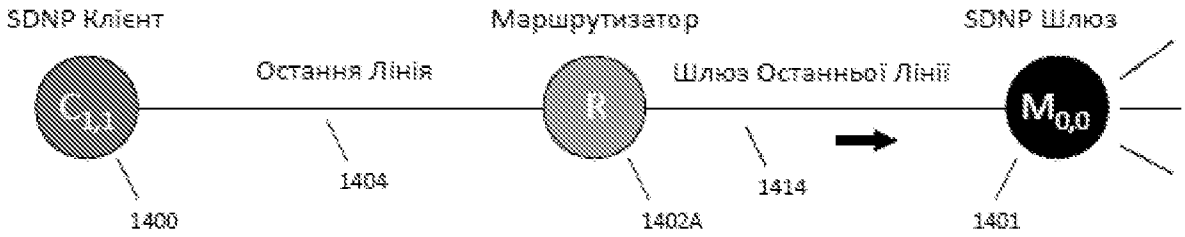
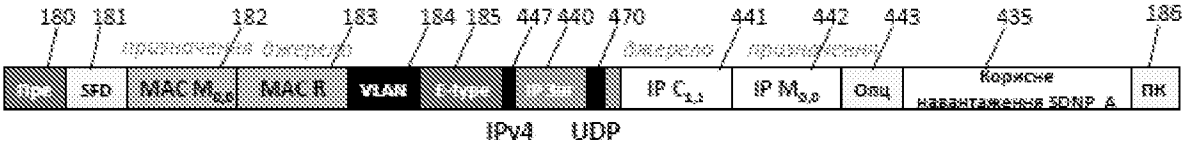


Рис. 50A



Шлюз Останньої Лінії Ethernet-пакета (Від Клієнта до Хмари SDNP)



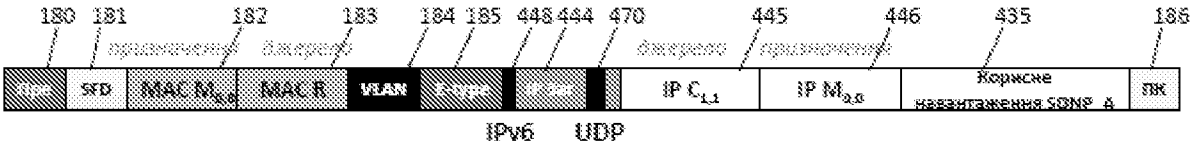
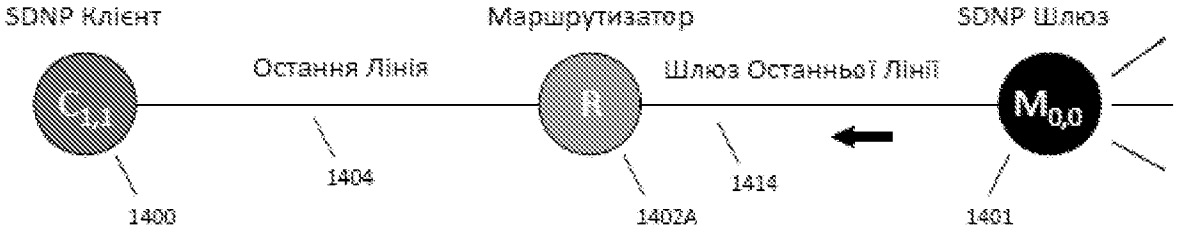
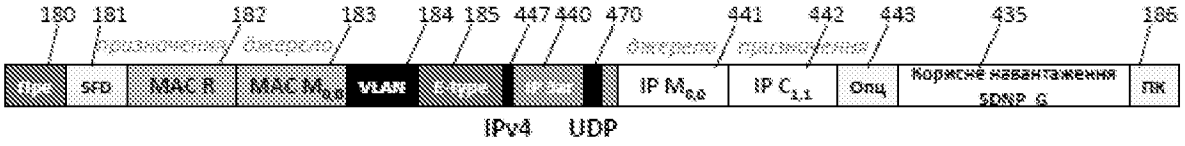


Рис. 50B



Шлюз Останньої Лінії Ethernet-пакета (Від Хмари SDNP до Клієнта)



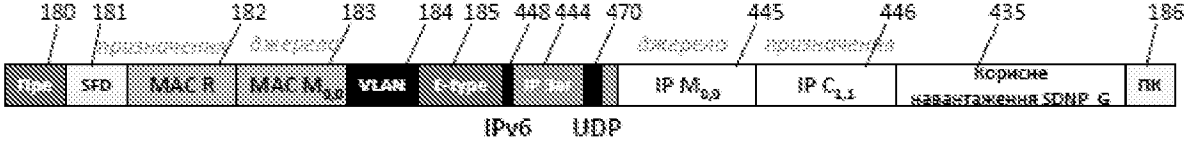
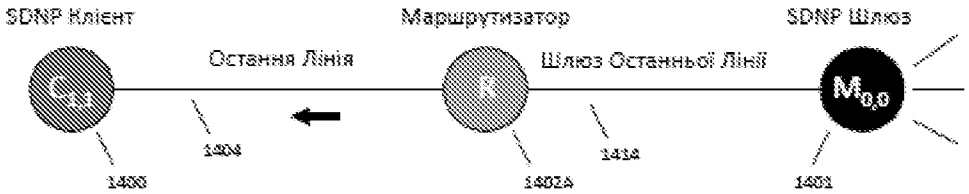


Рис. 50C



Остання Лінія Ethernet Пакета (Від SDNP Хмари до Клієнта)

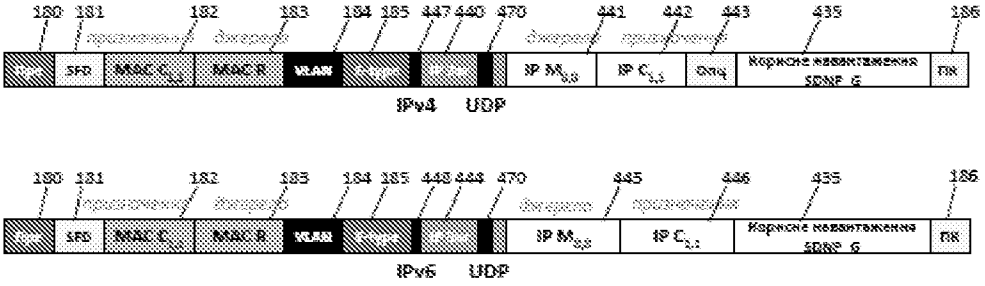
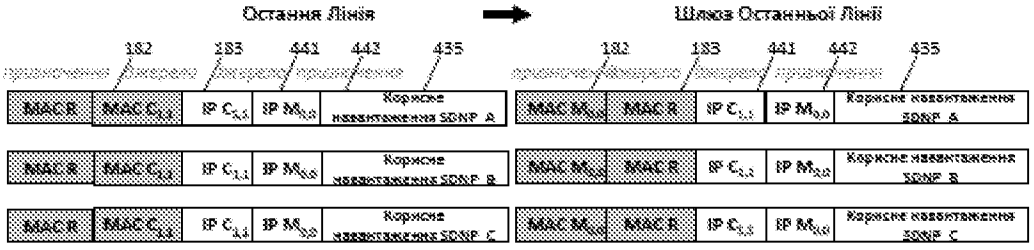


Рис. 50D

Одномаршрутний зв'язок «Останньої Милі» SDNP, Статична адресація клієнта, Одноріневе PHY-з'єднання «Останньої Лінії»



Одномаршрутний зв'язок «Останньої Милі» SDNP, Статична адресація клієнта, Багаторіневе PHY-з'єднання «Останньої Лінії»

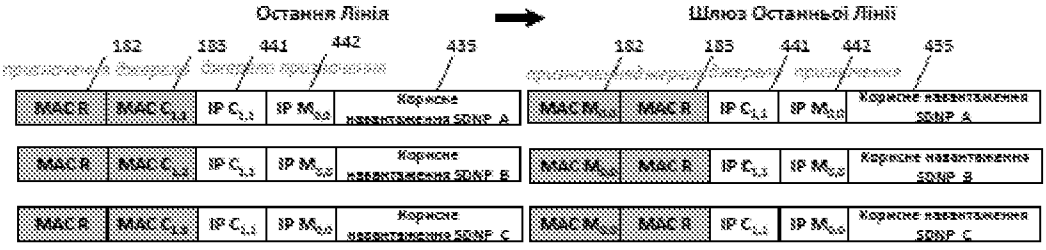
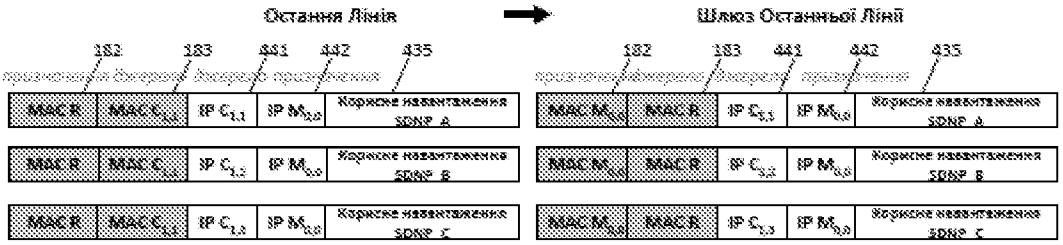


Рис. 51A

Одномаршрутний зв'язок «Останньої Милі» SDNP, Динамічна адресація клієнта,
Одноріневе PHY-з'єднання «Останньої Лінії»



Одномаршрутний зв'язок «Останньої Милі» SDNP, Динамічна адресація клієнта,
Багаторівневе PHY-з'єднання «Останньої Лінії»

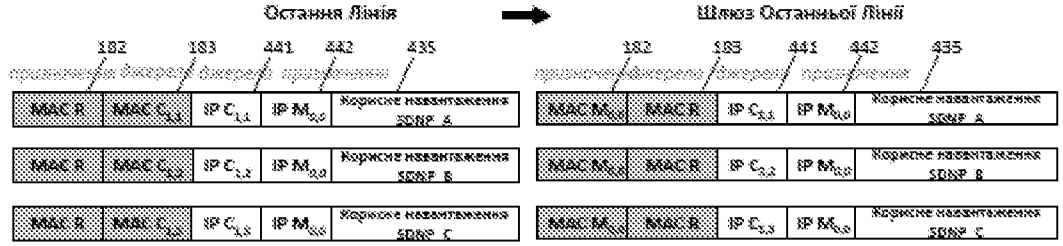
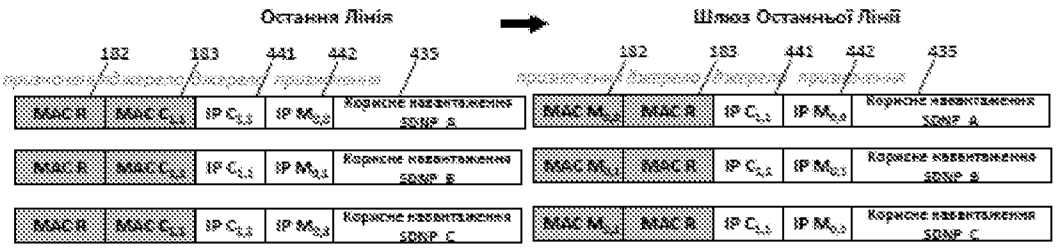


Рис. 51B

Багатомаршрутний зв'язок «Останньої Милі» SDNP, Статична адресація клієнта,
Одноріневе PHY-з'єднання «Останньої Лінії»



Багатомаршрутний зв'язок «Останньої Милі» SDNP, Статична адресація клієнта,
Многорівневе PHY-з'єднання «Останньої Лінії»

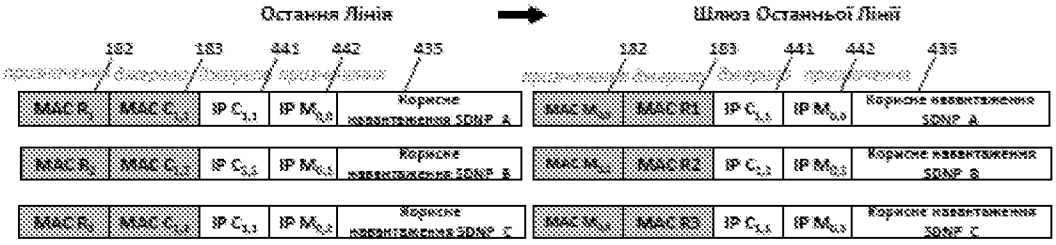


Рис. 51C

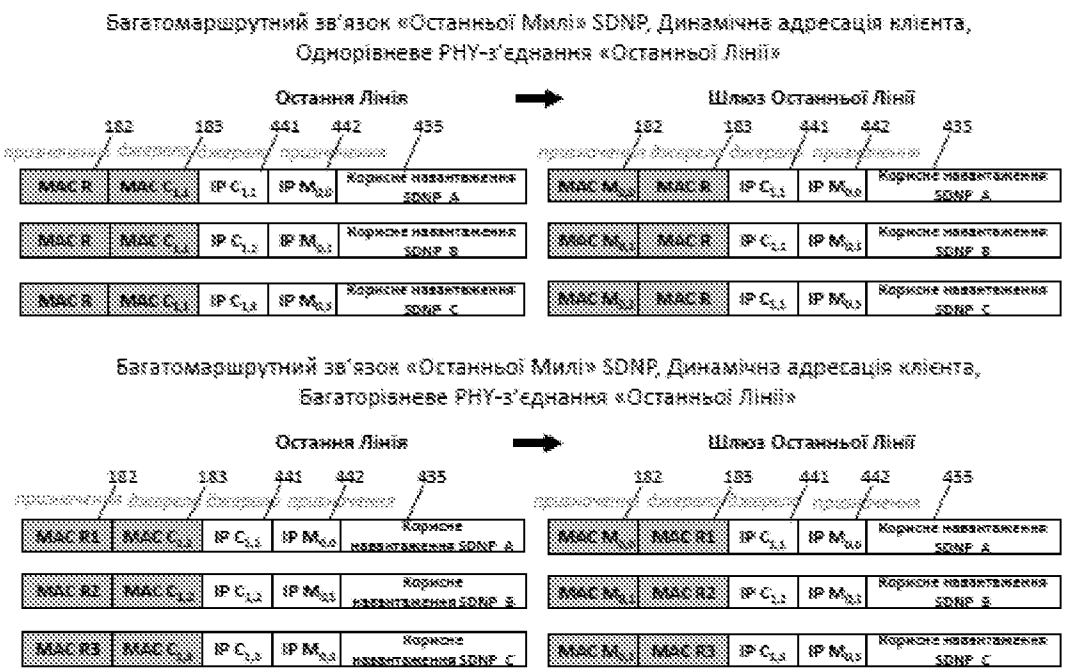


Рис. 51D

Ethernet маршрутизація даних SDNP «Останньої Милі»

#	Маршрут	Адреса Клієнта	Остання Лінія	IP Джерела	IP Призначення	MAC Клієнта
1	Багато	Динамічний	Багаторівн.	Змінюваний $C_{1,n}$	Багато Шлюзів $M_{0,n}$	MAC $C_{1,n}$ и R_n
2	Багато	Динамічний	Багаторівн.	Змінюваний $C_{1,n}$		MAC $C_{1,n}$ и R
3	Багато	Динамічний	Одноріжн.	Змінюваний $C_{1,n}$		MAC $C_{1,1}$ и R
4	Багато	Статичний	Багаторівн.	Закріплений $C_{1,1}$		MAC $C_{1,n}$ и R_n
5	Багато	Статичний	Багаторівн.	Закріплений $C_{1,1}$		MAC $C_{1,n}$ и R
6	Багато	Статичний	Одноріжн.	Закріплений $C_{1,1}$		MAC $C_{1,1}$ и R
7	Одно	Динамічний	Багаторівн.	Змінюваний $C_{1,n}$	Єдиний Шлюз $M_{0,0}$	MAC $C_{1,n}$ и R
8	Одно	Динамічний	Одноріжн.	Змінюваний $C_{1,n}$		MAC $C_{1,1}$ и R
9	Одно	Статичний	Багаторівн.	Закріплений $C_{1,1}$		MAC $C_{1,n}$ и R
10	Одно	Статичний	Одноріжн.	Закріплений $C_{1,1}$		MAC $C_{1,1}$ и R

Рис. 52A

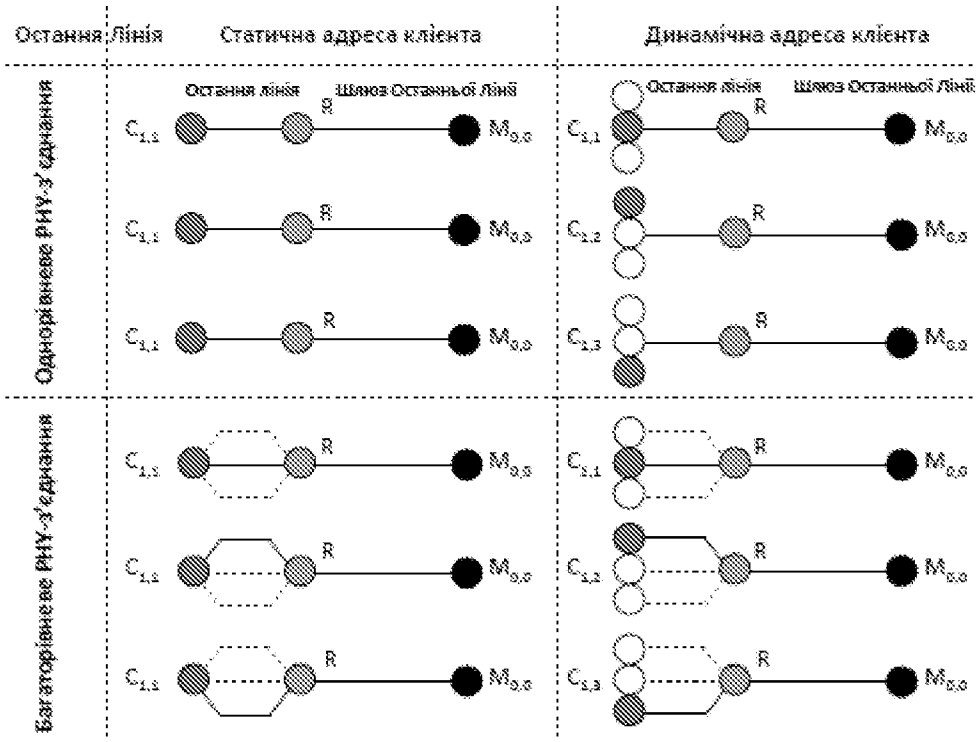


Рис. 52B

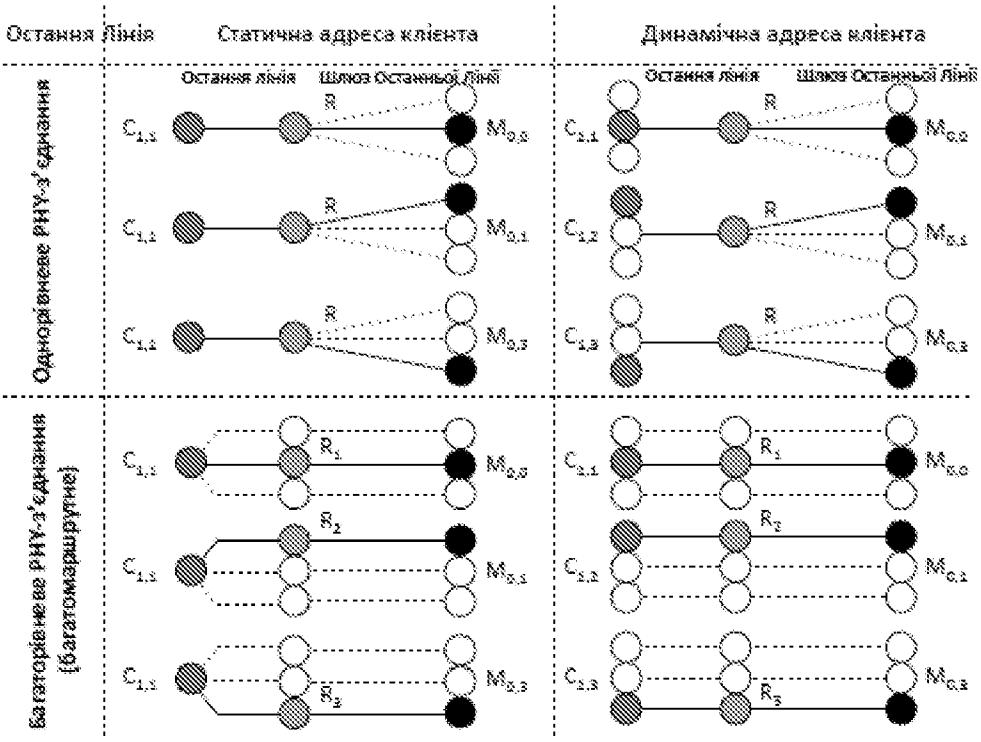


Рис. 52C

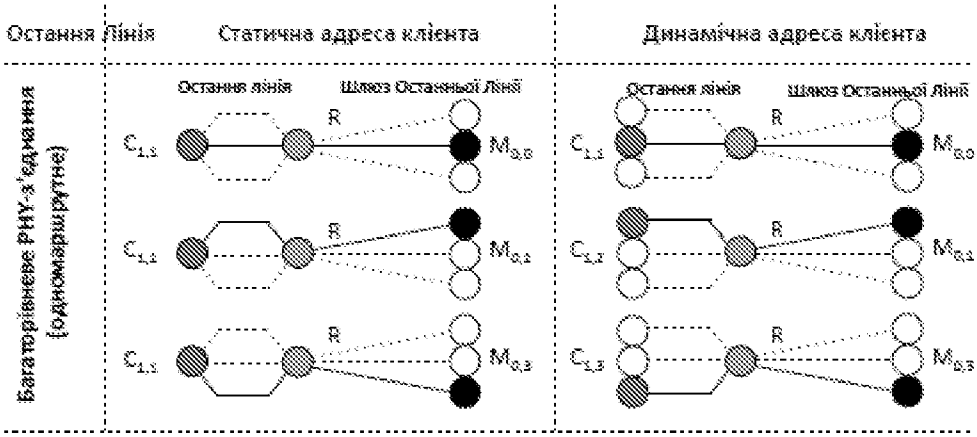


Рис. 52D

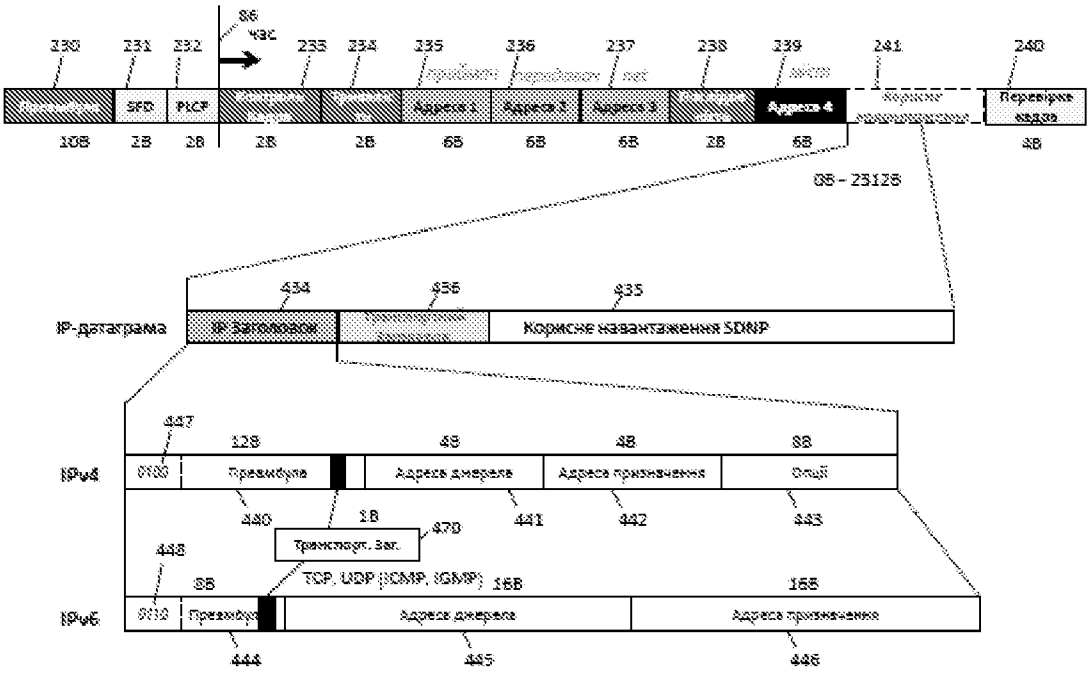
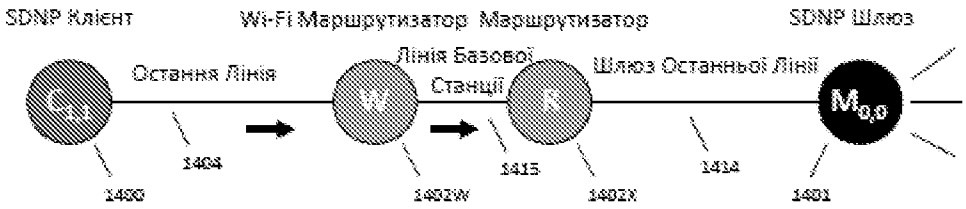


Рис. 53



Остання Лінія / Лінія Базової Станції Wi-Fi пакета (Від Клієнта до Хмари SDNP)

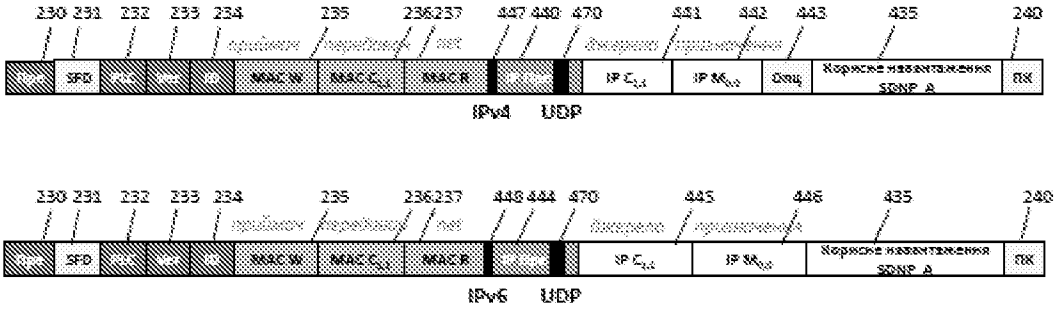
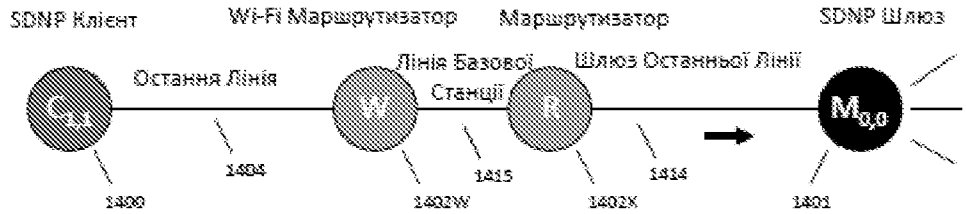


Рис. 54A



Шлюз Останньої Лінії Ethernet пакета (Від Клієнта до Хмари SDNP)

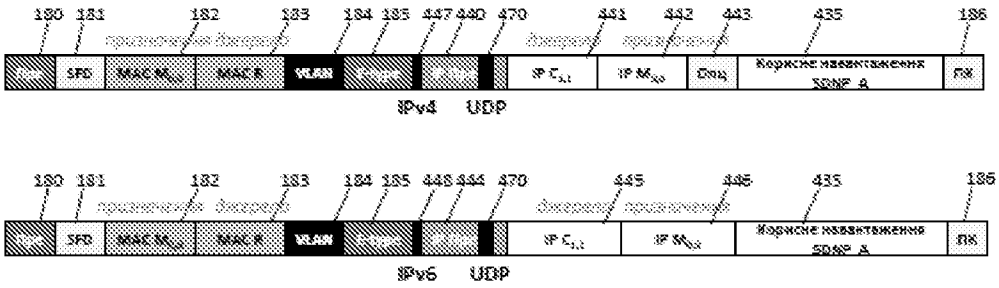
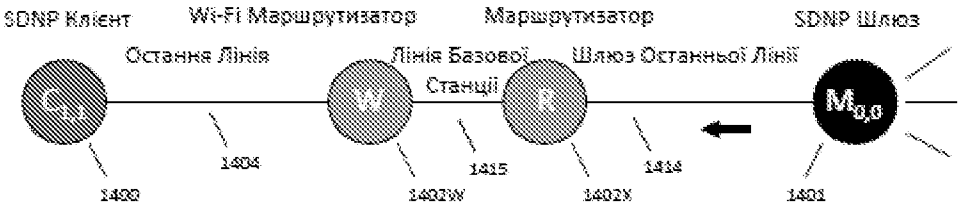
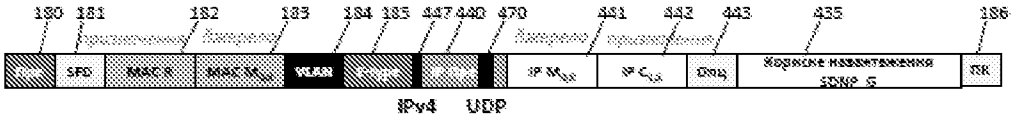


Рис. 54B



Шлюз Останньої Лінії Ethernet пакета (Від Хмари SDNP до Клієнта)



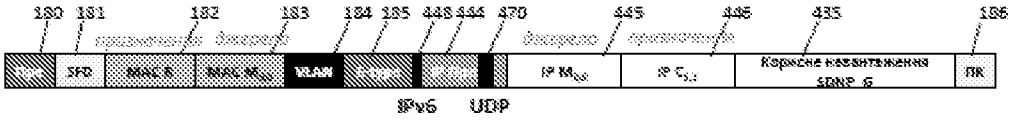
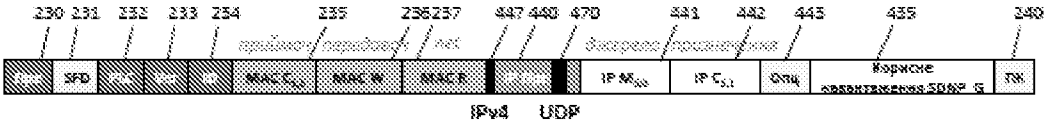


Рис. 54C



Лінія Базової Станції / Остання Лінія Wi-Fi Пакета (Від Хмари SDNP до Клієнта)



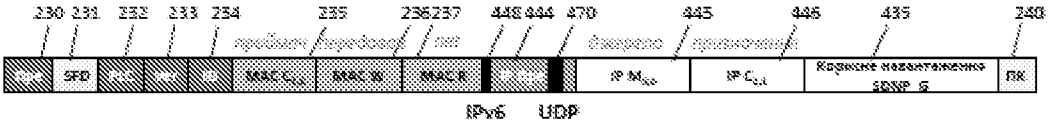


Рис. 54D

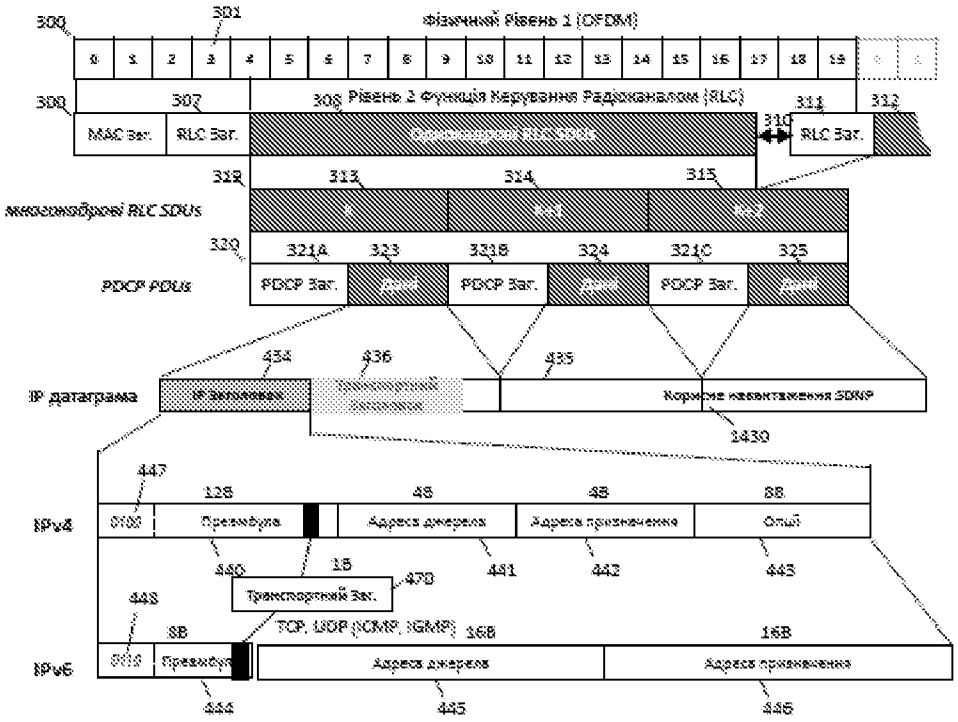
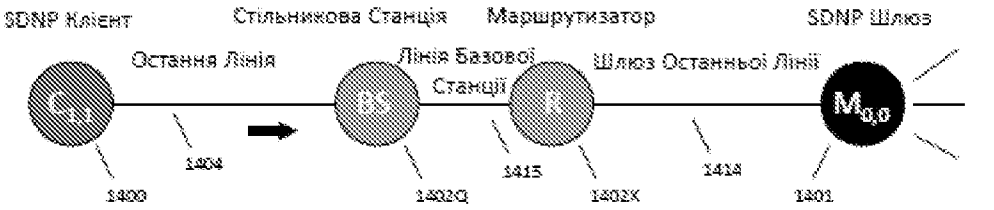


Рис. 55



Остання Лінія/ Стільникова Лінія Базової Станції 4G Пакета (Від Клієнта до Хмари SDNP)

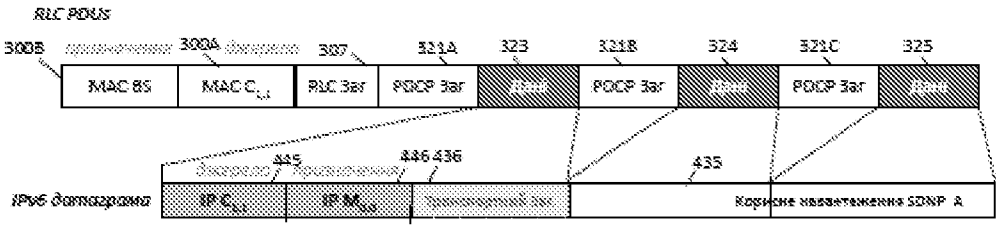
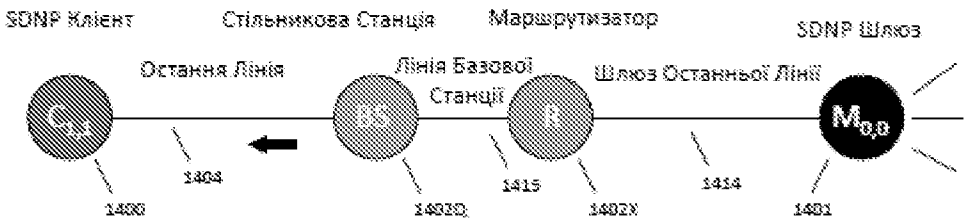


Рис. 56A



Остання Лінія/ Стільникова Лінія Базової Станції 4G Пакета (Від Клієнта до Хмари SDNP)

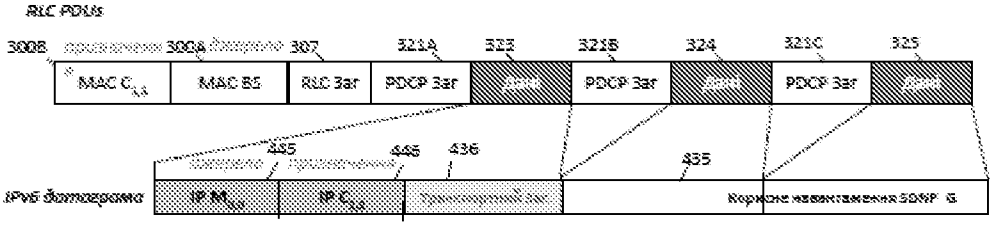


Рис. 56B

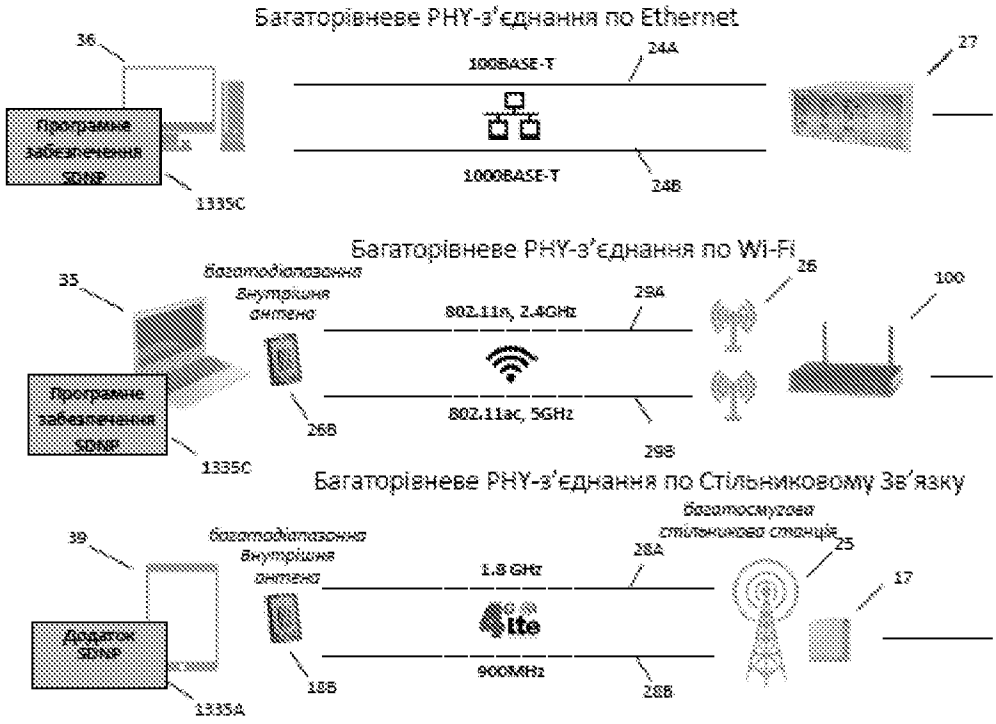


Рис. 57A

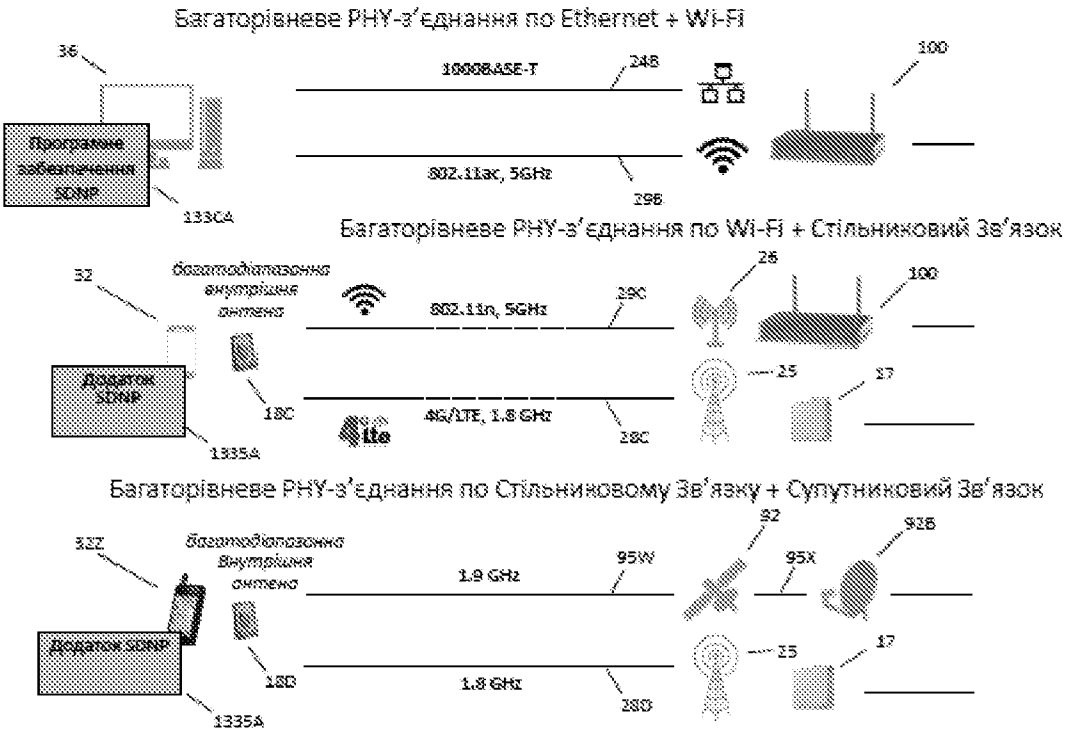


Рис. 57B

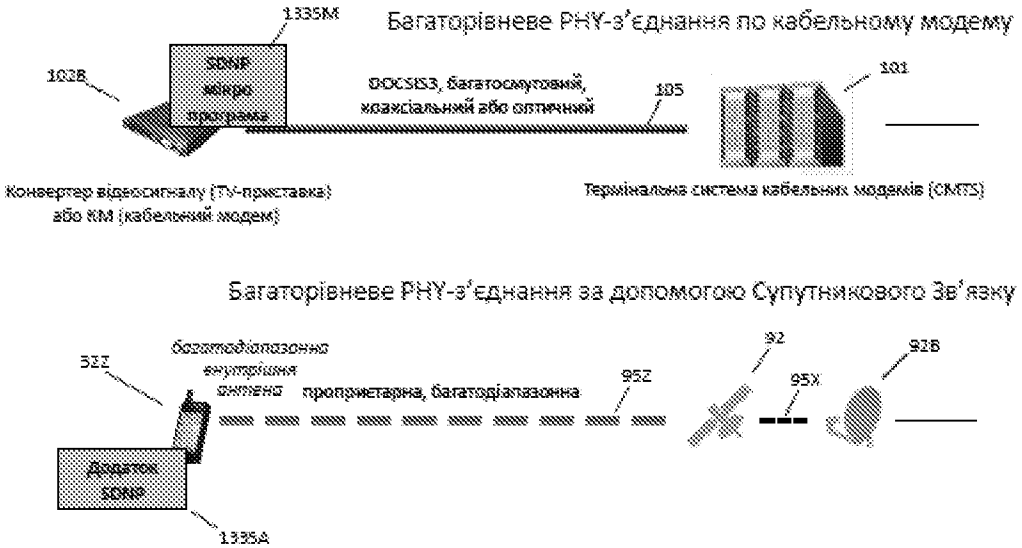


Рис. 57C

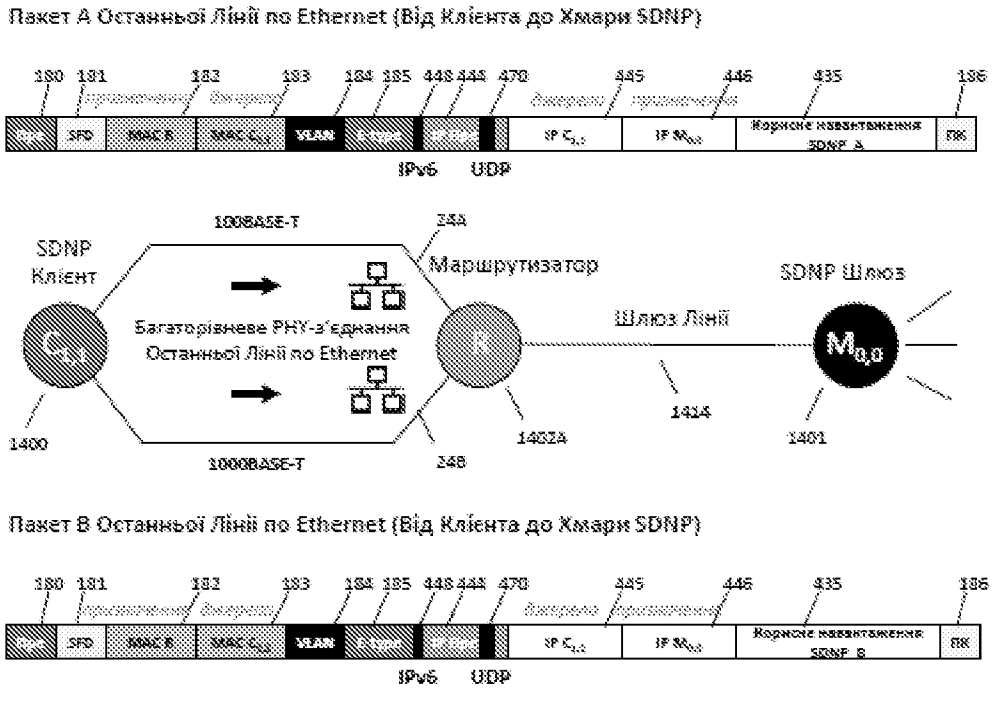

Пакет А Останньої Лінії по Ethernet (Від Клієнта до Хмари SDNP)
180 181 182 183 184 185 448 448 470 445 446 435 186
Преамбула SFD MAC R MAC $C_{x,y}$ VLAN Тип/Довжина IP Заголовок IP $C_{x,y}$ IP $M_{x,y}$ Корисне навантаження SDNP_A ПК
IPv6 UDP
SDNP Клієнт
100BASE-T
248A
Маршрутизатор
SDNP Шлюз
Багаторівневе PHY-з'єднання Останньої Лінії по Ethernet
Шлюз Лінії
$C_{1,1}$
R
$M_{0,0}$
1400
1402A
1414
1401
100BASE-T
248
Пакет В Останньої Лінії по Ethernet (Від Клієнта до Хмари SDNP)
180 181 182 183 184 185 448 448 470 445 446 435 186
Преамбула SFD MAC R MAC $C_{x,y}$ VLAN Тип/Довжина IP Заголовок IP $C_{x,y}$ IP $M_{x,y}$ Корисне навантаження SDNP_B ПК
IPv6 UDP

Рис. 58

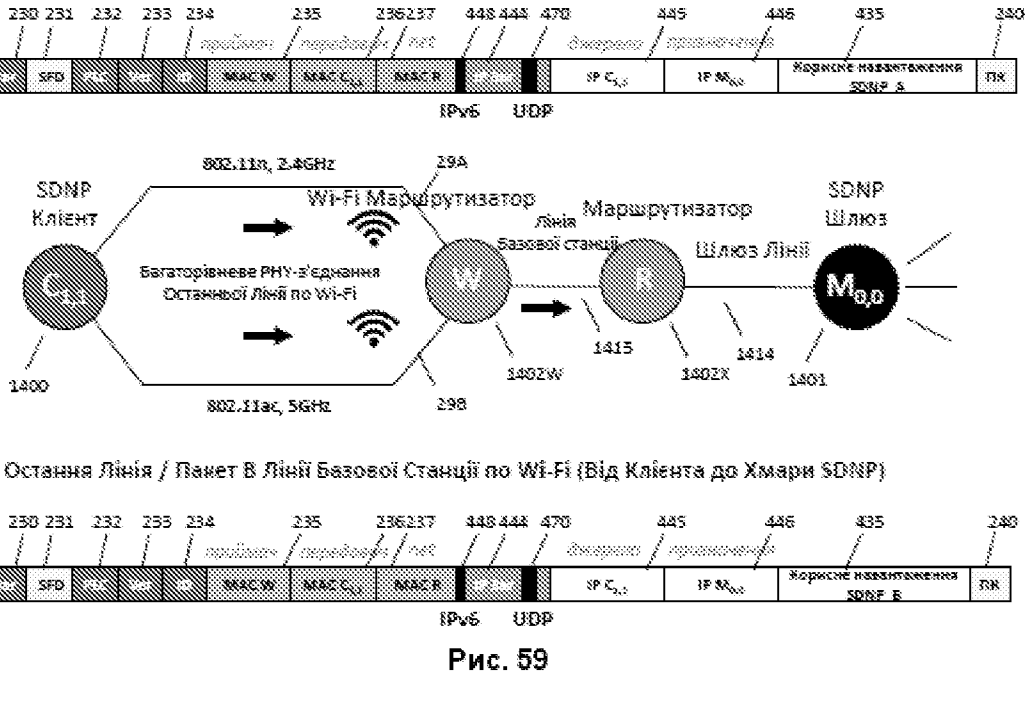

Остання Лінія / Пакет А Лінії Базової Станції по Wi-Fi (Від Клієнта до Хмари SDNP)
230 231 232 233 234 235 236 237 448 448 470 445 446 435 240
Преамбула SFD Тип MAC W MAC $C_{x,y}$ MAC R Заголовок IP $C_{x,y}$ IP $M_{x,y}$ Корисне навантаження SDNP_A ПК
IPv6 UDP
802.11n, 2.4GHz
298A
SDNP Клієнт
Wi-Fi Маршрутизатор
Лінія Базової станції
Маршрутизатор
SDNP Шлюз
Багаторівневе PHY-з'єднання Останньої Лінії по Wi-Fi
Шлюз Лінії
$C_{1,1}$
W
R
$M_{0,0}$
1400
1402W
1415
1402X
1414
1401
802.11ac, 5GHz
298
Остання Лінія / Пакет В Лінії Базової Станції по Wi-Fi (Від Клієнта до Хмари SDNP)
230 231 232 233 234 235 236 237 448 448 470 445 446 435 240
Преамбула SFD Тип MAC W MAC $C_{x,y}$ MAC R Заголовок IP $C_{x,y}$ IP $M_{x,y}$ Корисне навантаження SDNP_B ПК
IPv6 UDP

Рис. 59

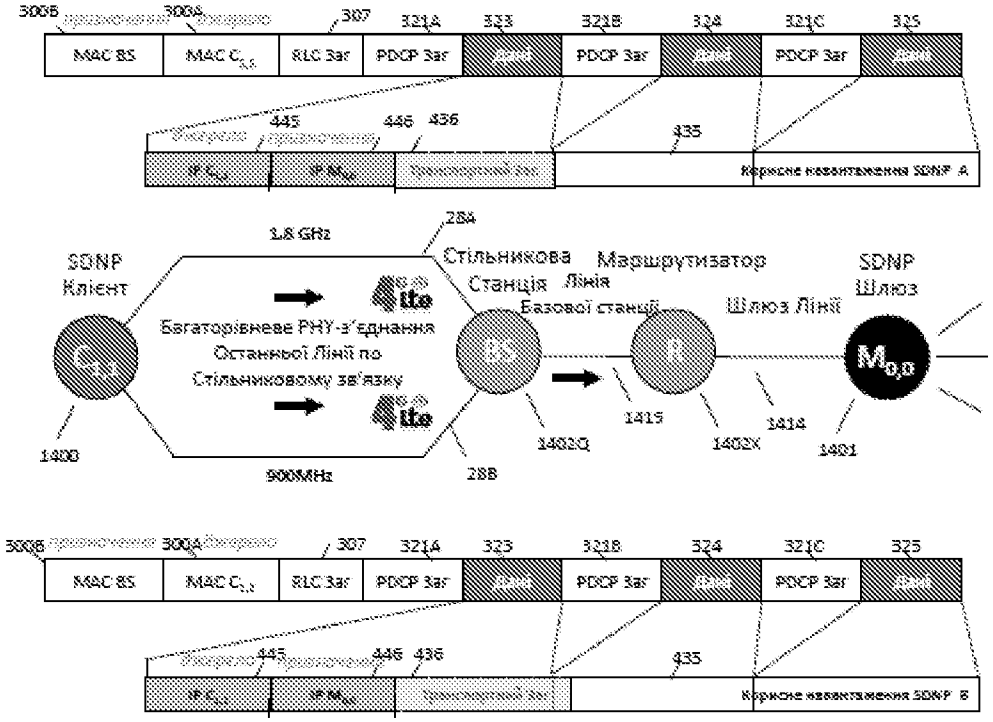
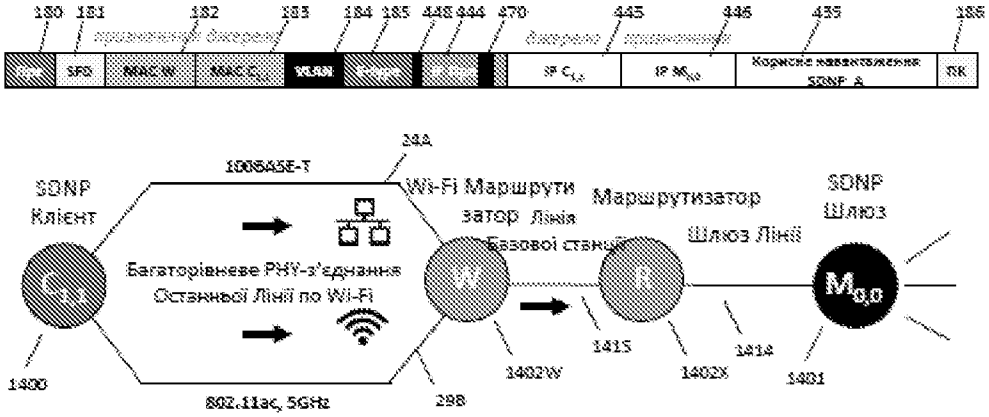


Рис. 60

Пакет A Останньої Лінії по Ethernet (Від Клієнта до Хмари SDNP)



Остання Лінія / Пакет B Лінії Базової Станції по Wi-Fi (Від Клієнта до Хмари SDNP)

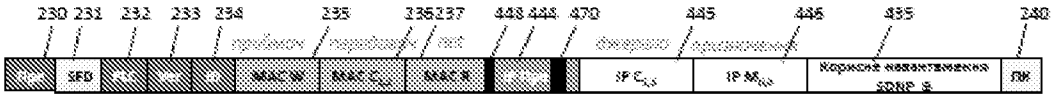
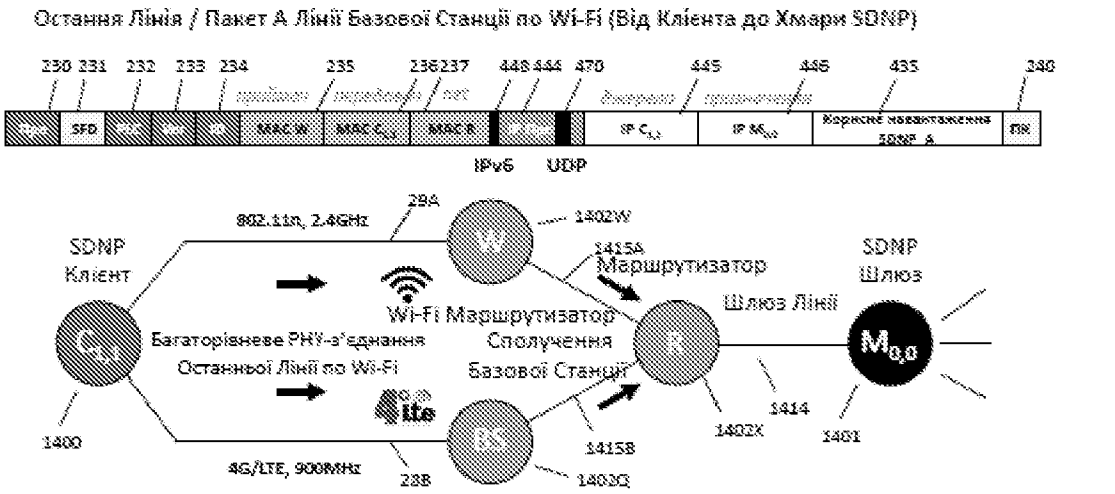


Рис. 61


Остання Лінія / Пакет А Лінії Базової Станції по Wi-Fi (Від Клієнта до Хмари SDNP)
IPv6
UDP
802.11n, 2.4GHz
SDNP
Клієнт
Wi-Fi Маршрутизатор
Сполучення
Базової Станції
Маршрутизатор
Шлюз Лінії
SDNP
Шлюз
Багаторівневе PHY-з'єднання
Останньої Лінії по Wi-Fi
4G/LTE, 900MHz
1400
1402W
1402X
1402Z
1414
1401
1415A
1415B
28A
28B

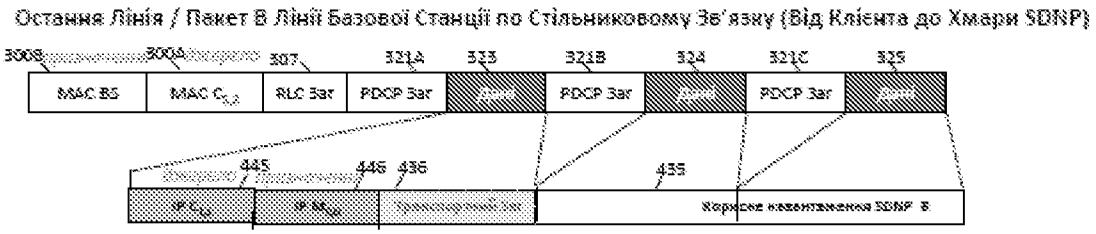

Остання Лінія / Пакет В Лінії Базової Станції по Стільниковому Зв'язку (Від Клієнта до Хмари SDNP)
MAC BS
RLC Заг
PDCP Заг
Дані
Корисне навантаження SDNP B

Рис. 62

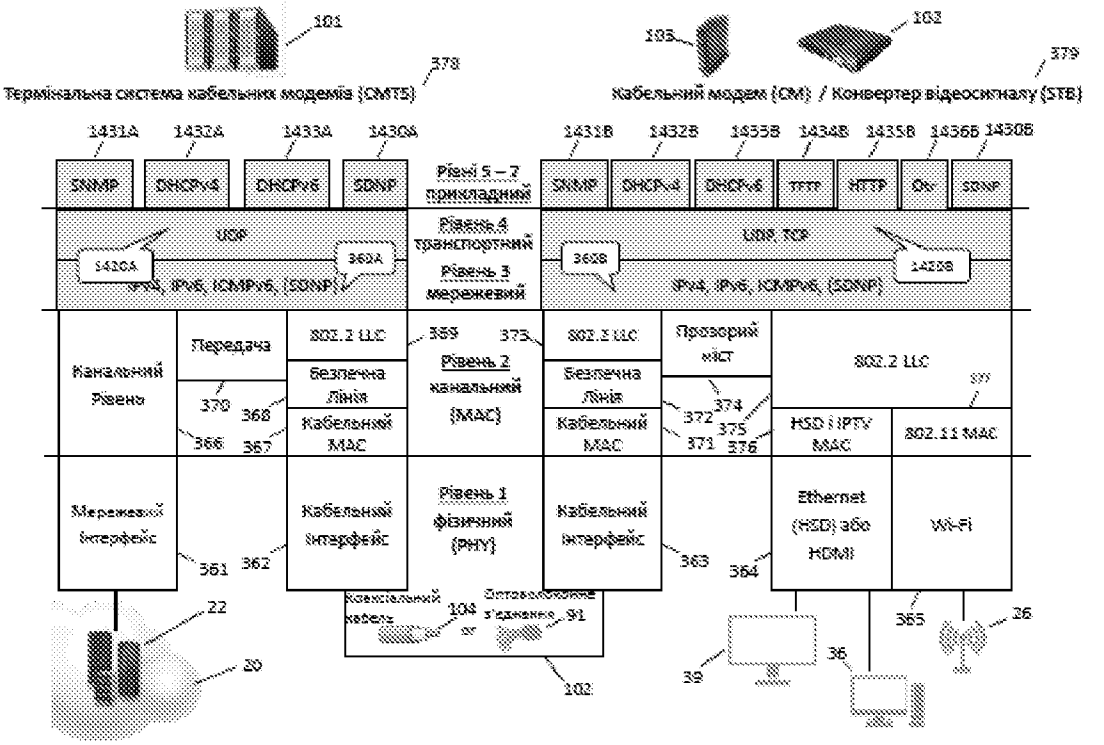

Термінальна система кабельних модемів (CMTS)
Кабельний модем (CM) / Конвертер відеосигналу (STB)
SNMP
DHCPv4
DHCPv6
SDNP
Рівні 5 – 7 прикладний
Рівень 4 транспортний
Рівень 3 мережевий
UDP
UDP, TCP
IPv4, IPv6, ICMPv6, (SDNP)
Передача
802.2 LLC
Безпечна Лінія
Кабельний MAC
Рівень 2 канальний (MAC)
Прозорий міст
HSD і IPTV MAC
802.11 MAC
Канальний Рівень
Мережевий інтерфейс
Кабельний інтерфейс
Рівень 1 фізичний (PHY)
Ethernet (HSD) або HDMI
Wi-Fi
Коаксіальний кабель
Оптоволоконне з'єднання
22
20
104
91
102
39
36
365
26

Рис. 63

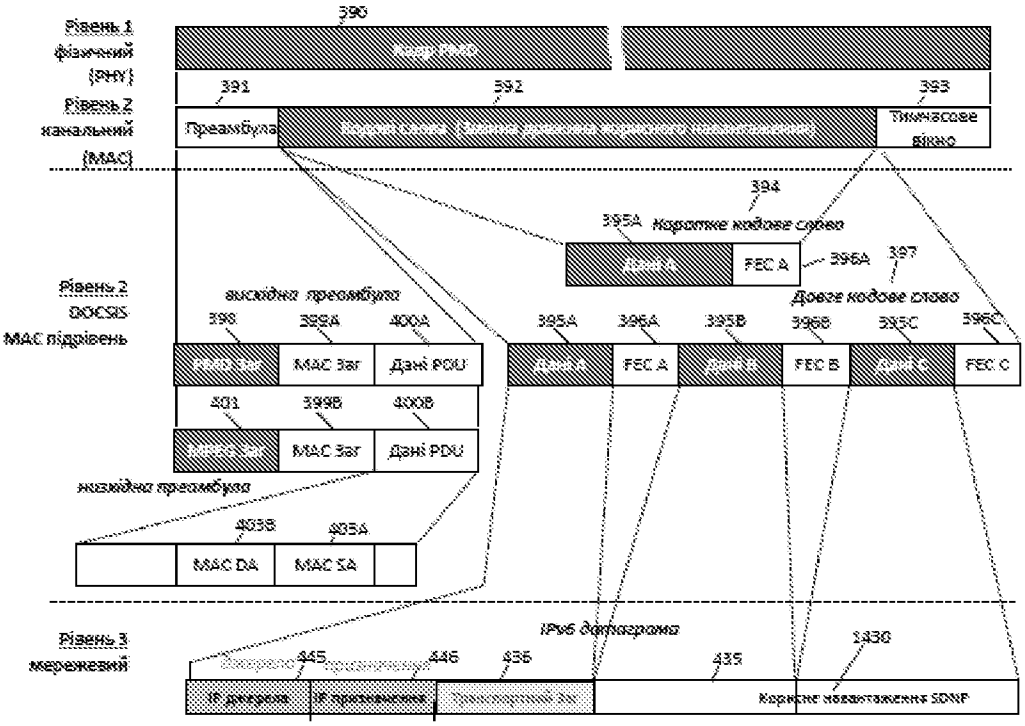


Рис. 64

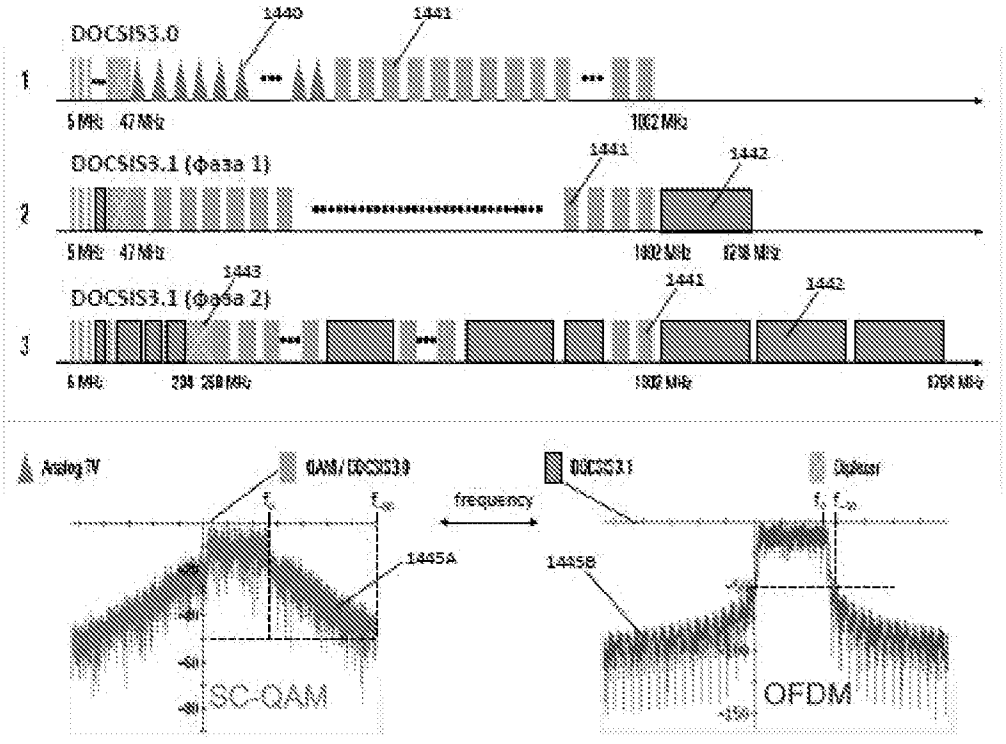


Рис. 65A

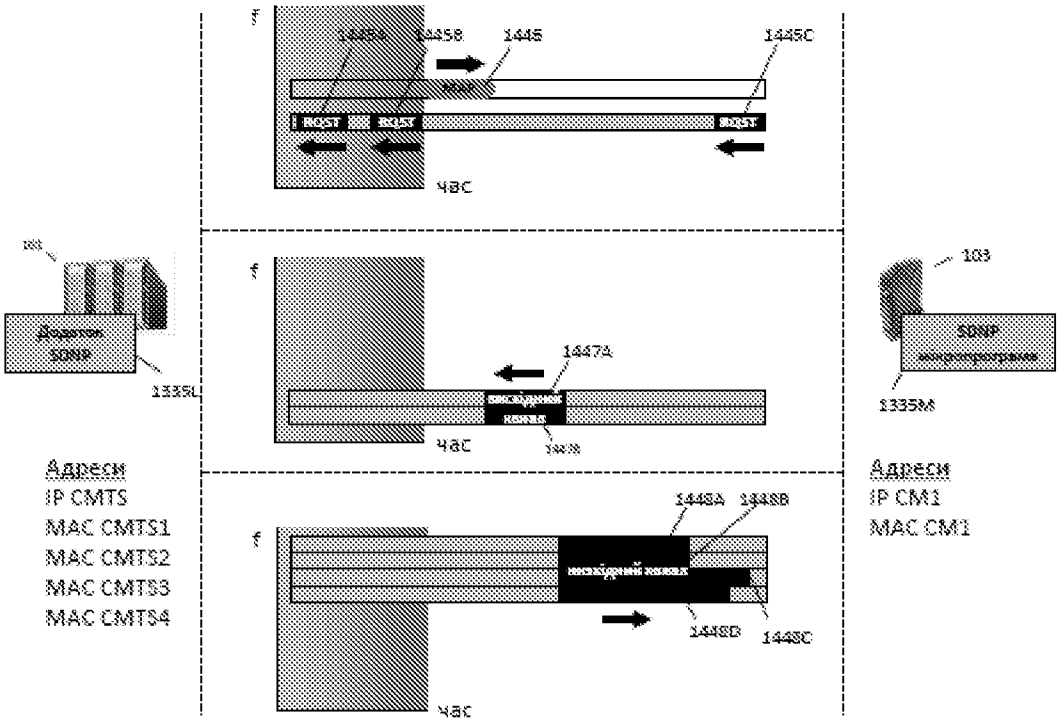


Рис. 65B

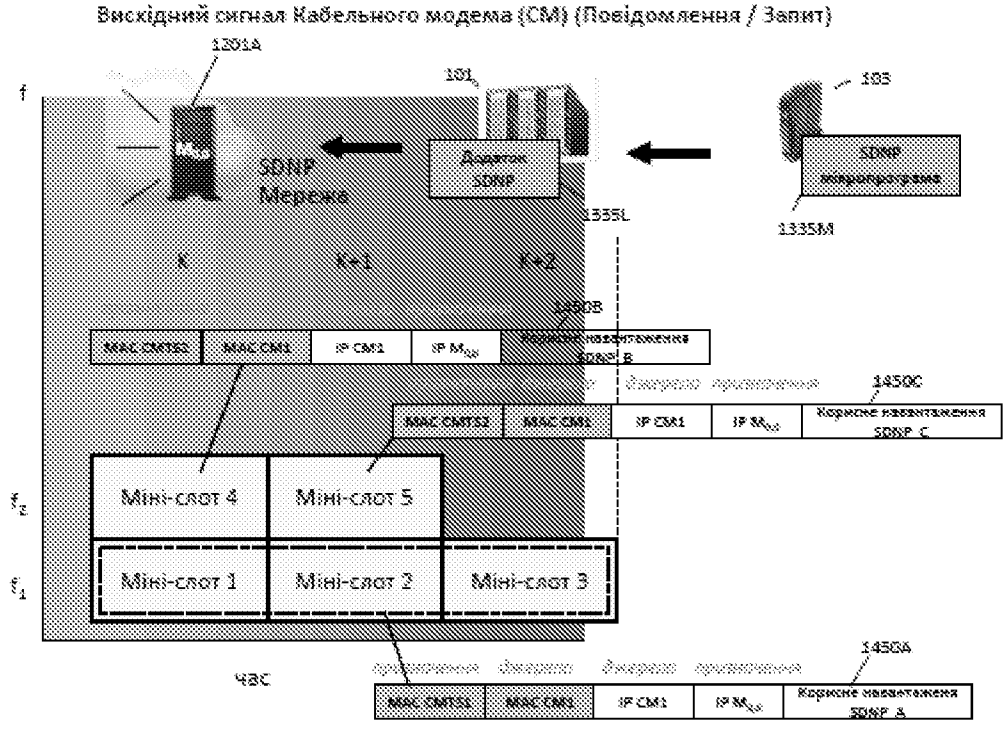


Рис. 65C

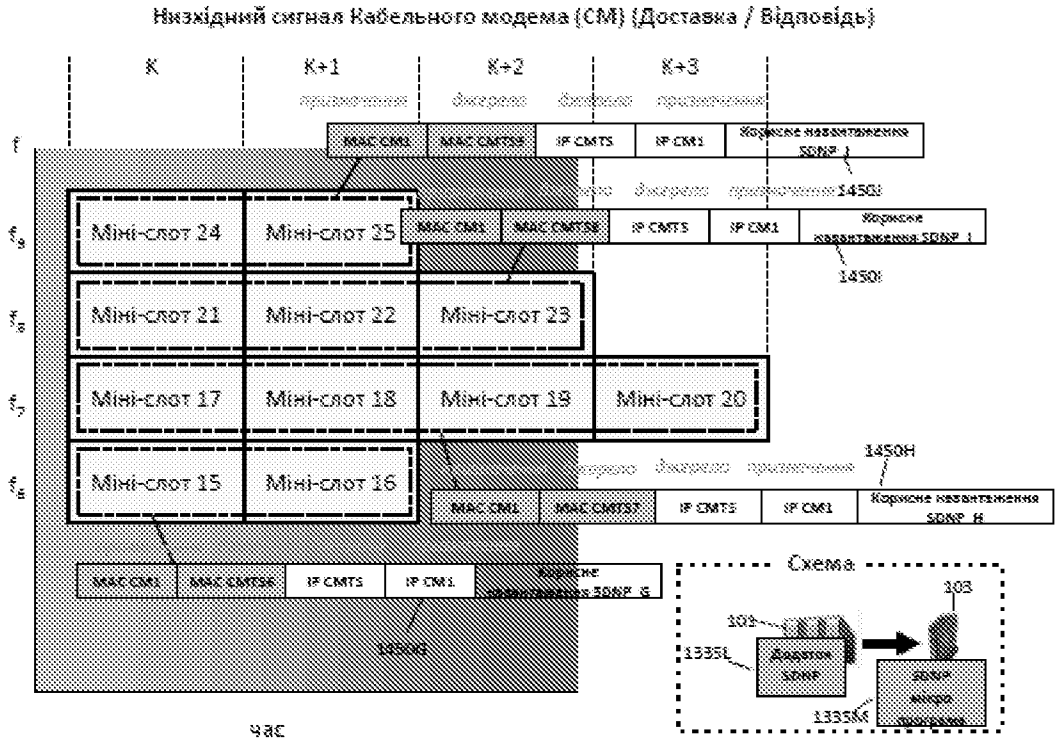


Рис. 65D

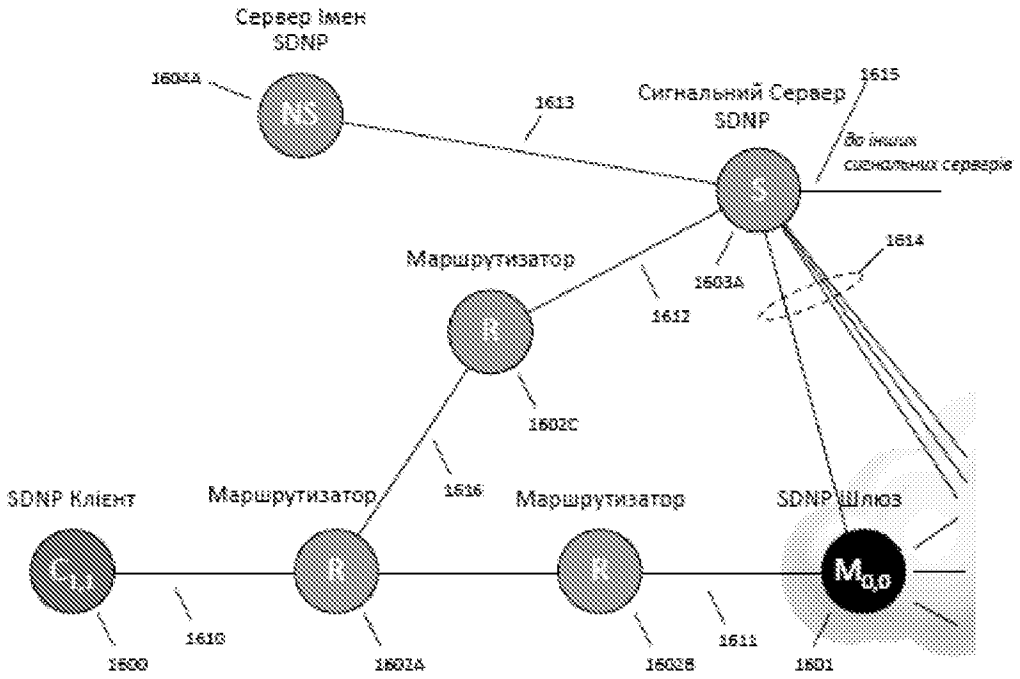


Рис. 66

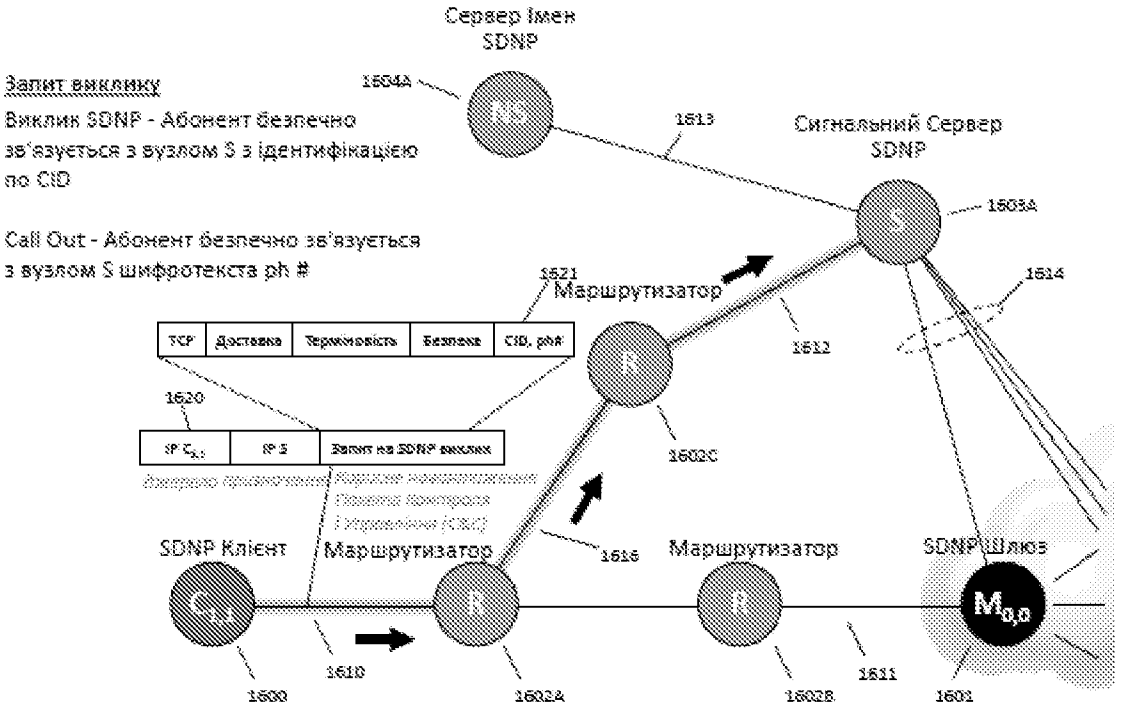

Сервер Імен SDNP
Запит виклику
Виклик SDNP - Абонент безпечно зв'язується з вузлом S з ідентифікацією по CID
Call Out - Абонент безпечно зв'язується з вузлом S шифротекста ph #
1604A
1613
Сигнальний Сервер SDNP
1603A
1614
1621
Маршрутизатор
TCP
Доставка
Термінальність
Безпека
CID, phN
1612
1620
IP S
Запит на SDNP виклик
1602C
SDNP Клієнт
Маршрутизатор
1616
Маршрутизатор
SDNP Шлюз
1600
1610
1602A
1602B
1611
1601

Рис. 67

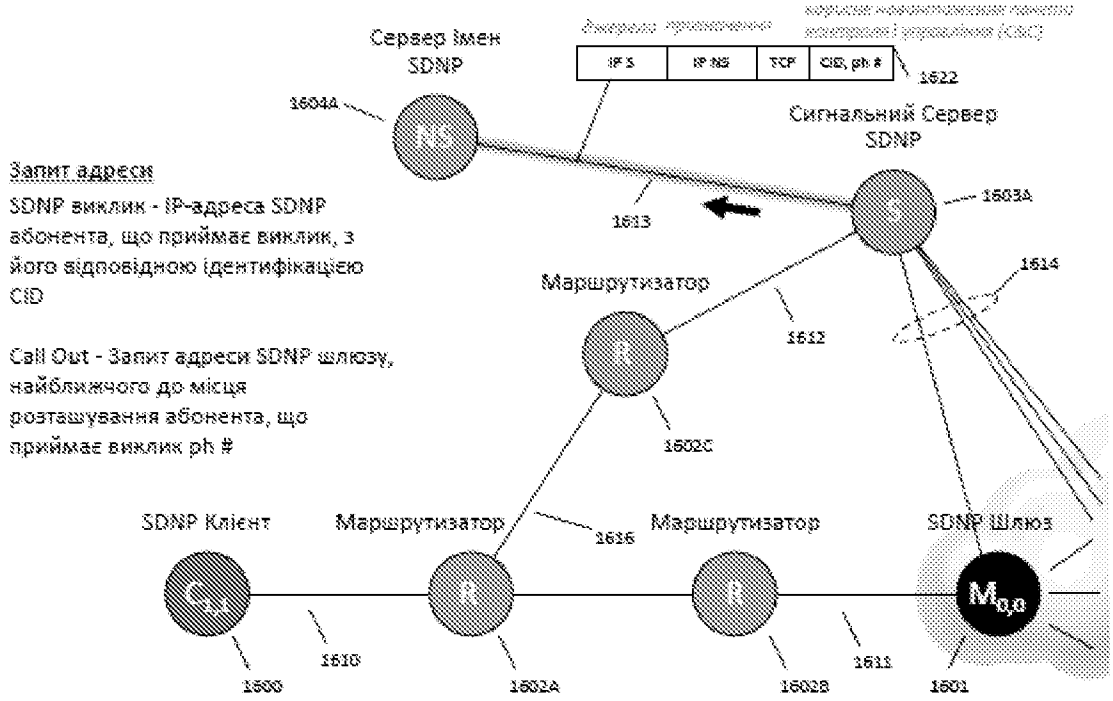

Сервер Імен SDNP
IP S
IP NS
TCP
CID, ph #
1622
1604A
Сигнальний Сервер SDNP
Запит адреси
SDNP виклик - IP-адреса SDNP абонента, що приймає виклик, з його відповідною ідентифікацією CID
1613
1603A
1614
Маршрутизатор
1612
Call Out - Запит адреси SDNP шлюзу, найближчого до місця розташування абонента, що приймає виклик ph #
1602C
SDNP Клієнт
Маршрутизатор
1616
Маршрутизатор
SDNP Шлюз
1600
1610
1602A
1602B
1611
1601

Рис. 68

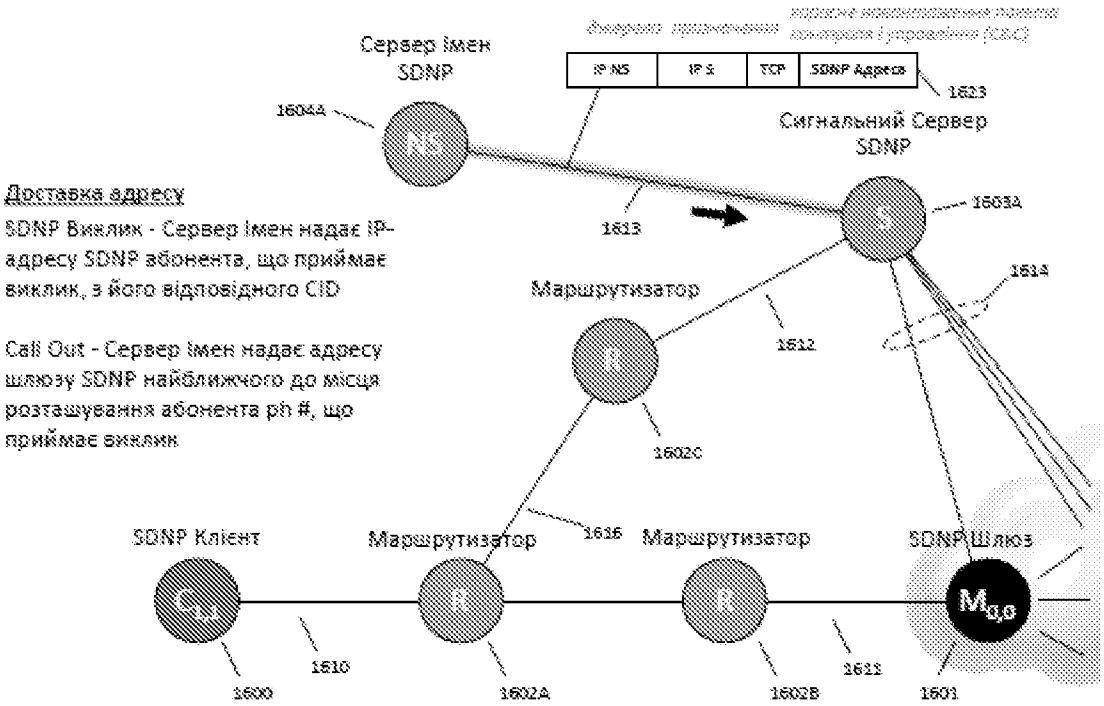

Сервер імен SDNP
IP NS
IP S
TCP
SDNP Адреса
1623
1604A
NS
Сигнальний Сервер SDNP
1603A
S
1613
Доставка адресу
SDNP Виклик - Сервер імен надає IP-адресу SDNP абонента, що приймає виклик, з його відповідного CID
Call Out - Сервер імен надає адресу шлюзу SDNP найближчого до місця розташування абонента ph #, що приймає виклик
Маршрутизатор
1614
1612
R
1602C
SDNP Клієнт
Маршрутизатор
1616
Маршрутизатор
SDNP Шлюз
1610
1600
1602A
1602B
1611
1601

Рис. 69

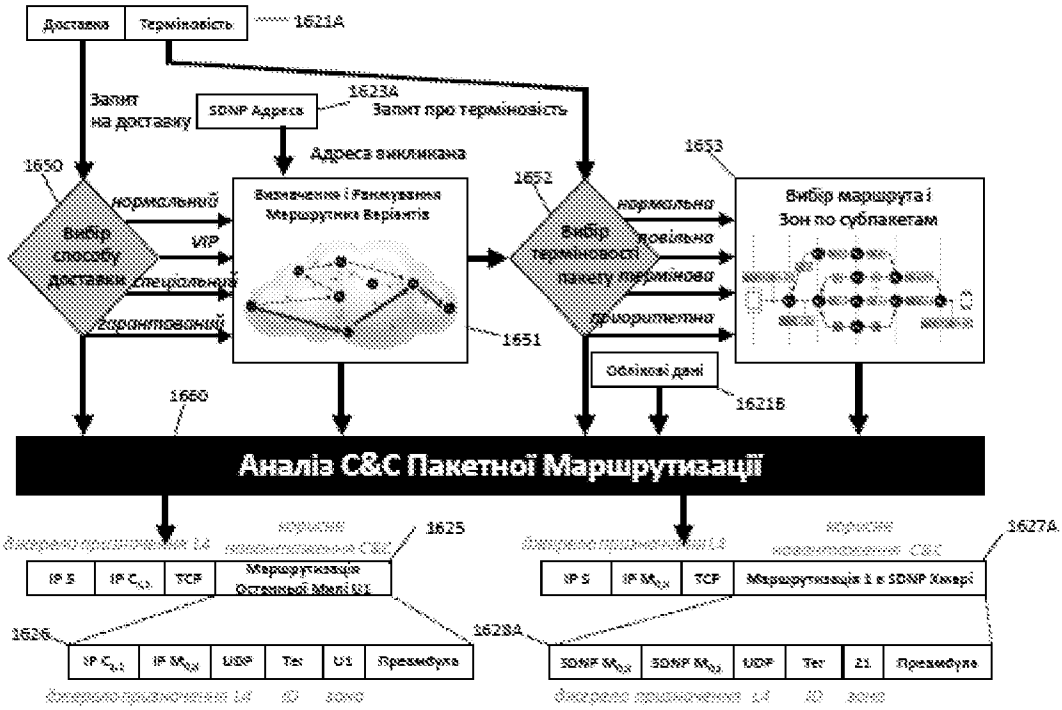

Доставка
Терміновість
1621A
Запит на доставку
SDNP Адреса
1623A
Запит про терміновість
Адреса виклика
1650
1652
1653
Вибір способу доставки
нормальний
VIP
Спеціальний
Зашифрований
Визначення і Ранжування Маршрутних Варіантів
1651
Вибір терміновості пакету
нормально
терміново
пріоритетно
Вибір маршруту і Зон по субпакетам
Облікові дані
1621B
1650
Аналіз C&C Пакетної Маршрутизації
1625
1627A
1626
1628A

Рис. 70

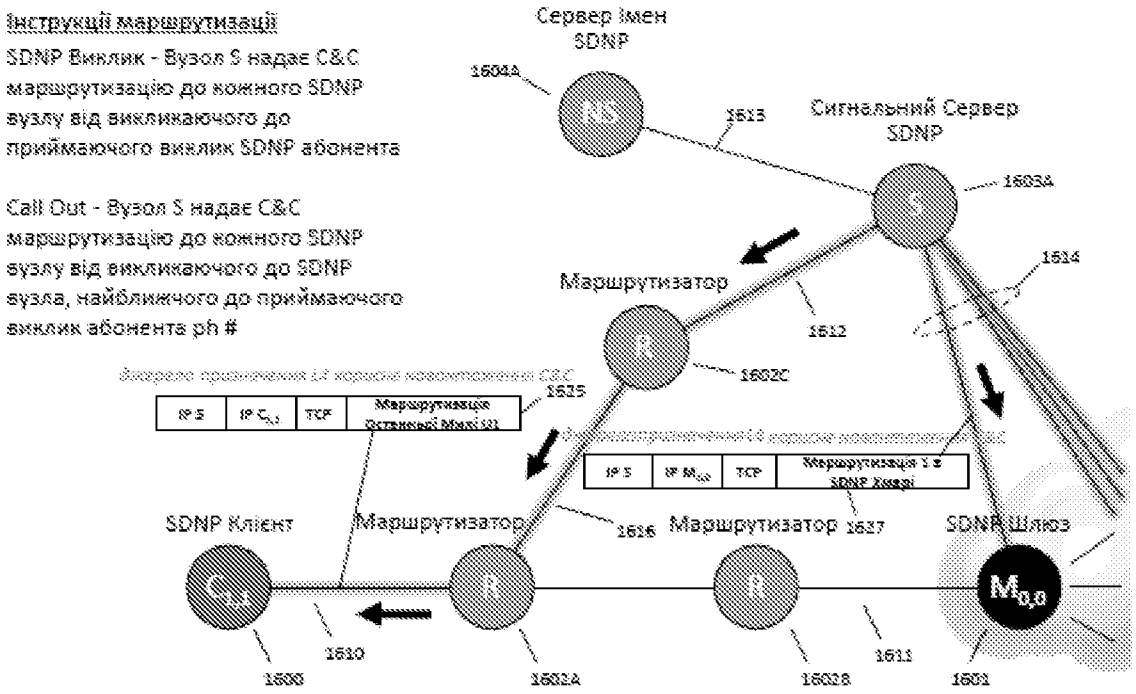

Інструкції маршрутизації
SDNP Виклик - Вузол S надає C&C маршрутизацію до кожного SDNP вузлу від викликаючого до приймаючого виклик SDNP абонента
Call Out - Вузол S надає C&C маршрутизацію до кожного SDNP вузлу від викликаючого до SDNP вузла, найближчого до приймаючого виклик абонента ph #
Сервер Імен SDNP
NS
1604A
1613
Сигнальний Сервер SDNP
S
1603A
1614
Маршрутизатор
R
1612
1602C
1625
IP S
TCP
1616
1627
SDNP Клієнт
Маршрутизатор
Маршрутизатор
SDNP Шлюз
1610
1600
1602A
1602B
1611
1601

Рис. 71

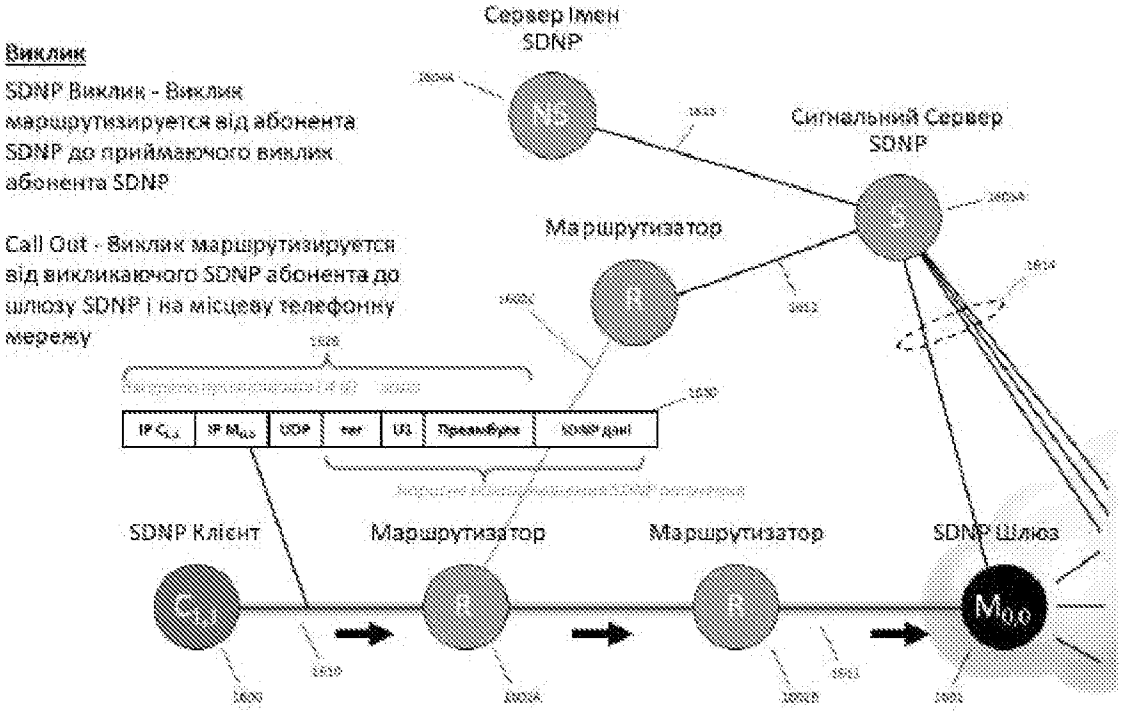

Виклик
SDNP Виклик - Виклик маршрутизируется від абонента SDNP до приймаючого виклик абонента SDNP
Call Out - Виклик маршрутизируется від викликаючого SDNP абонента до шлюзу SDNP і на місцеву телефонну мережу
Сервер Імен SDNP
Сигнальний Сервер SDNP
Маршрутизатор
SDNP Клієнт
Маршрутизатор
Маршрутизатор
SDNP Шлюз

Рис. 72

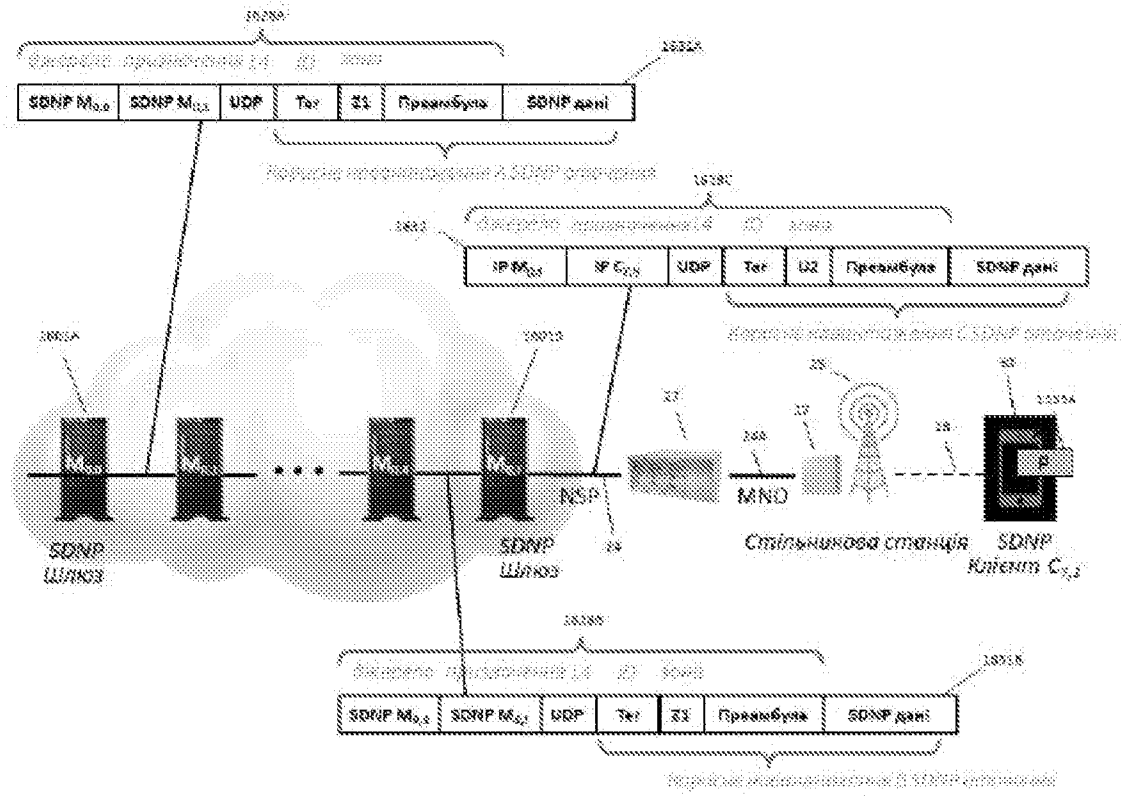


Рис. 73A

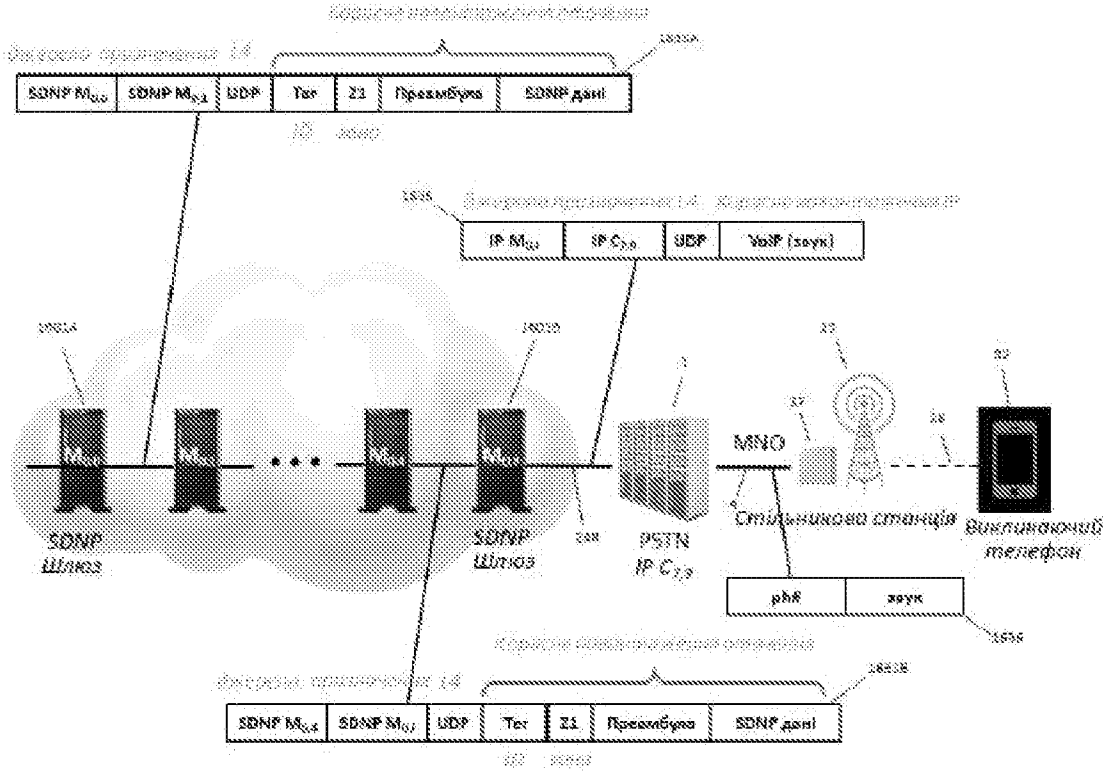


Рис. 73B

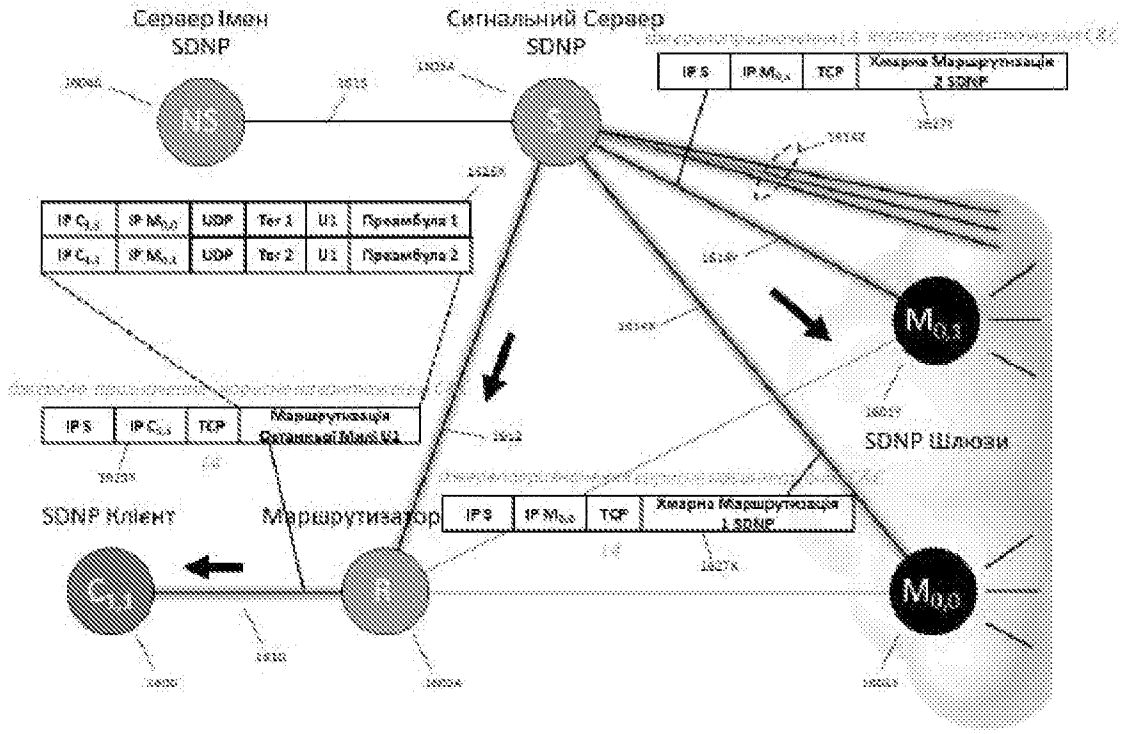


Рис. 74

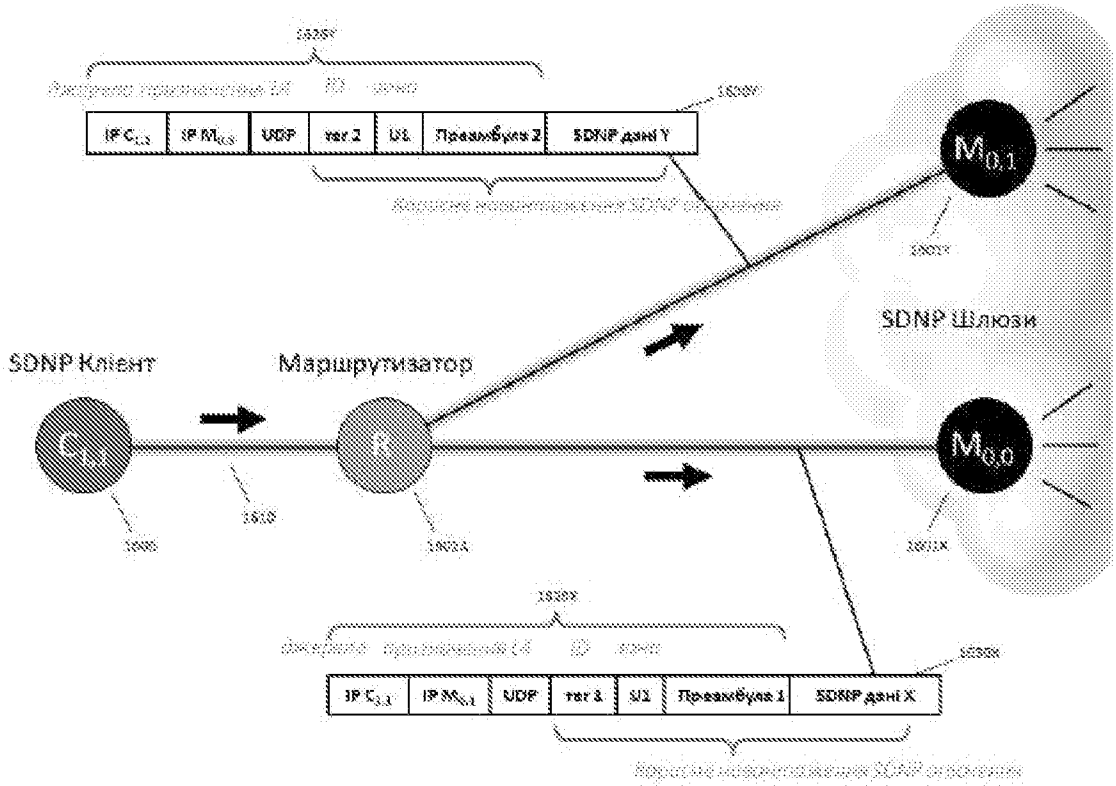


Рис. 75А

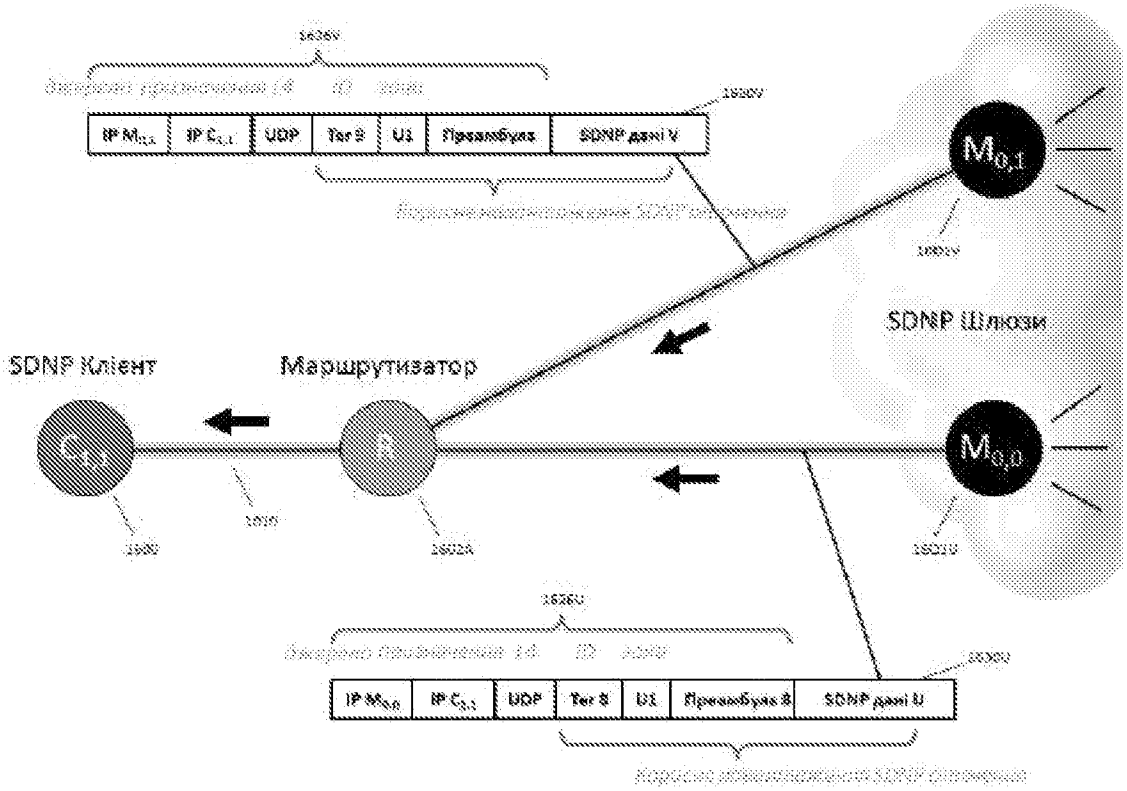


Рис. 75B

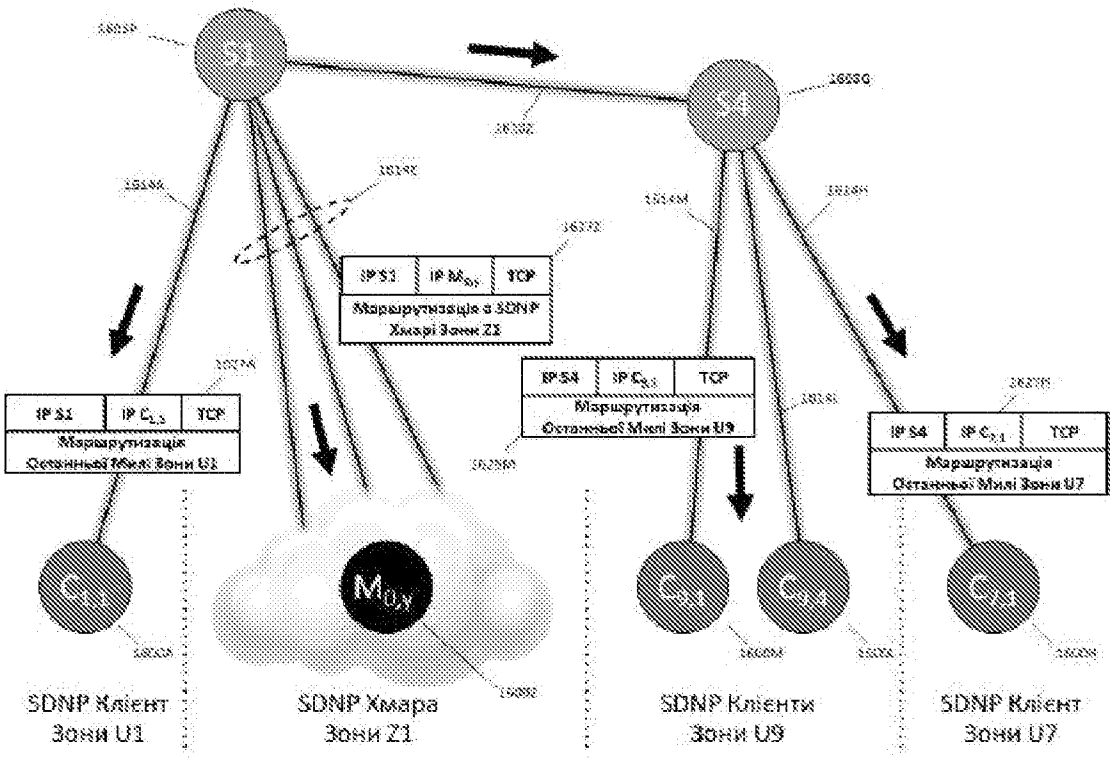


Рис. 76

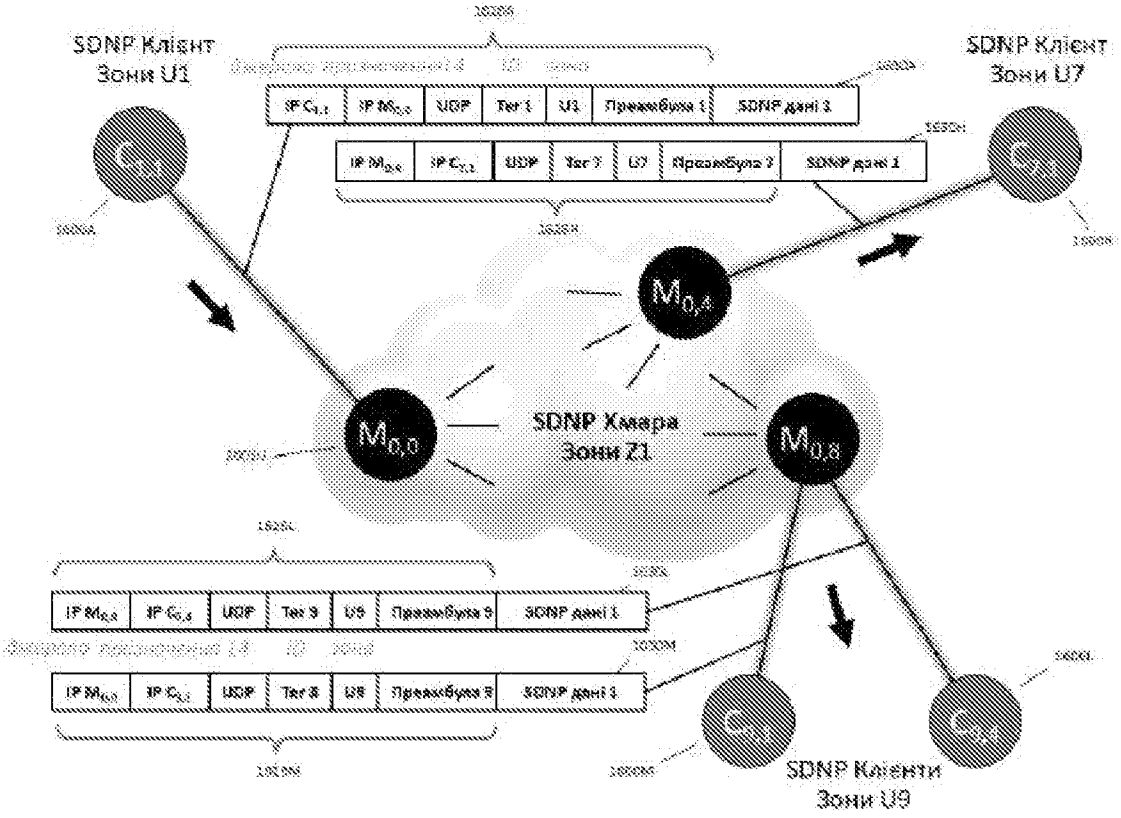

SDNP Клієнт
Зони U1
SDNP Клієнт
Зони U7
SDNP Хмара
Зони Z1
SDNP Клієнти
Зони U9

Рис. 77А

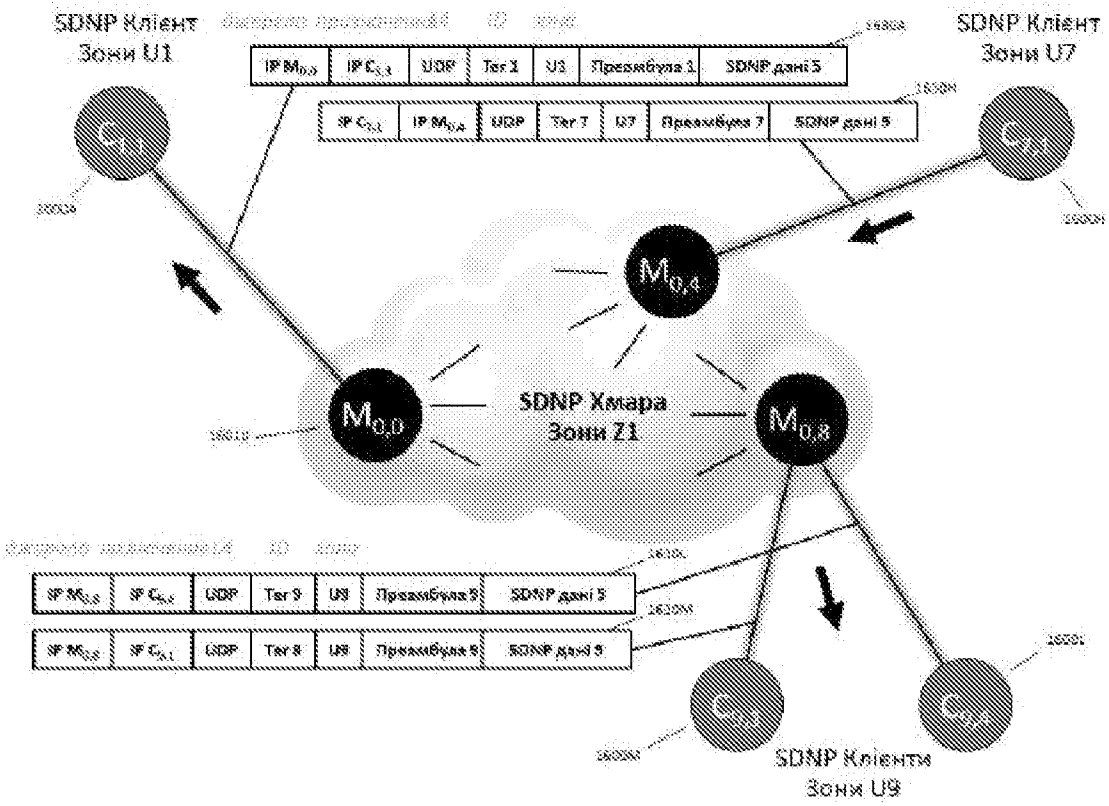

SDNP Клієнт
Зони U1
SDNP Клієнт
Зони U7
SDNP Хмара
Зони Z1
SDNP Клієнти
Зони U9
UDP
Тег 1
Преамбула 1
SDNP дані 5
UDP
Тег 7
Преамбула 7
SDNP дані 5
UDP
Тег 9
Преамбула 9
SDNP дані 5
UDP
Тег 8
Преамбула 8
SDNP дані 5

Рис. 77B

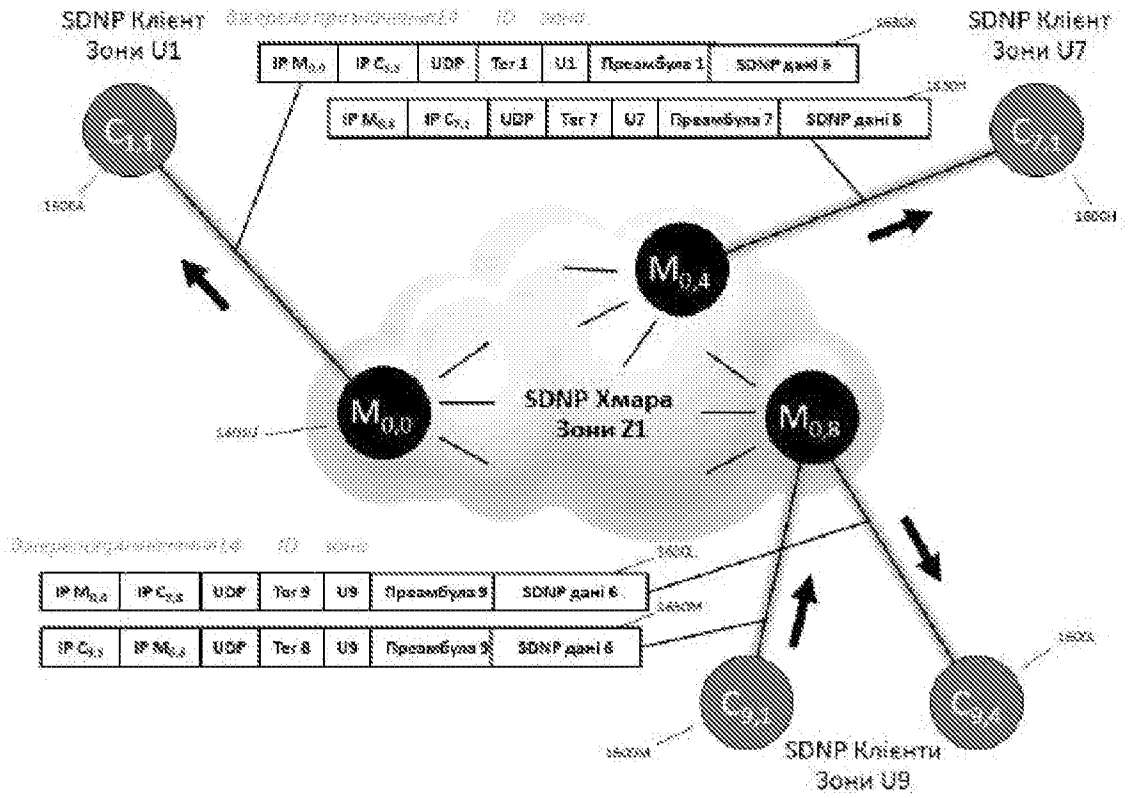


Рис. 77C

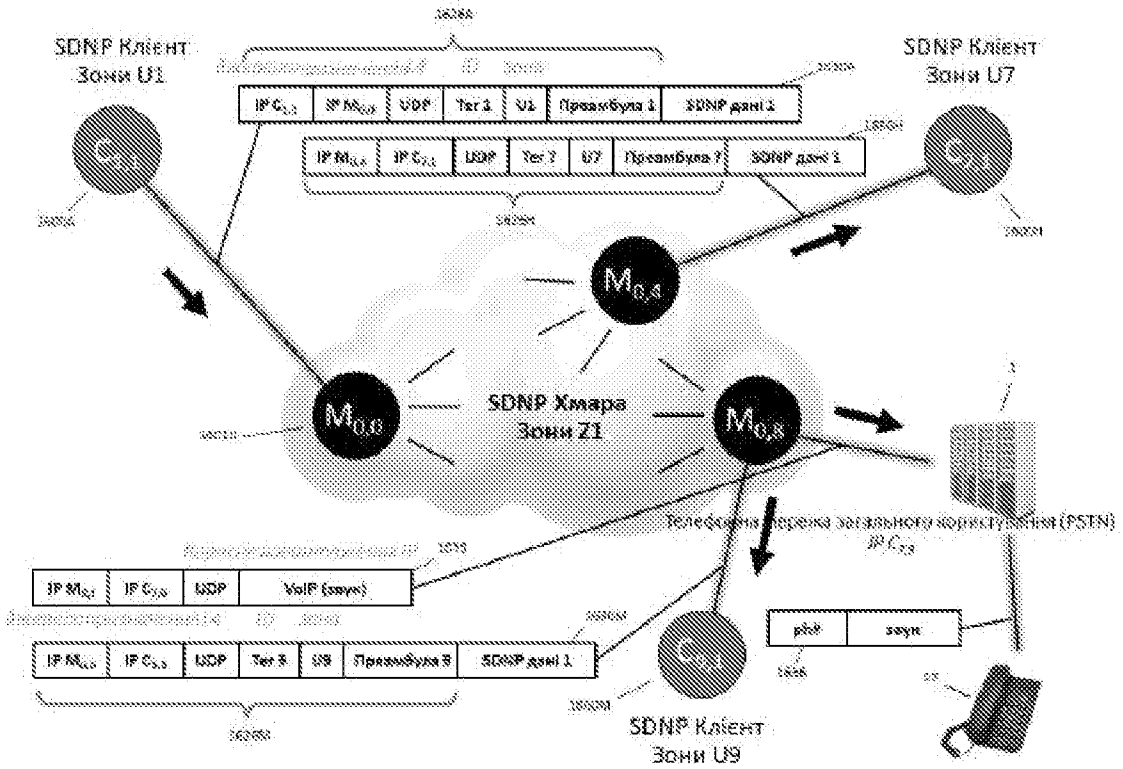


Рис. 78

Клієнт Групового Дзвінка		Звичайний Дзвінок	Приватний Дзвінок	
Вузли Мережі	Авторизація Користувача	Всі Учасники	Аутентифікований клієнт SDNP	Неаутентифікований клієнт SDNP
$C_{8,1}$	SDNP Клієнт *Хост Групи*	Слухати, Говорити	Слухати, Говорити	–
$C_{7,1}$	SDNP Клієнт *Учасник*	Слухати, Говорити	Слухати, Говорити	Мікрофон і Динамік Відключені
$C_{9,1}$	SDNP Клієнт *Учасник*	Слухати, Говорити	Слухати, Говорити	
$C_{9,2}$	SDNP Клієнт *Слухач*	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
Ph #1	Call Out *Учасник*	Слухати, Говорити	Мікрофон і Динамік Відключені	
Ph #2	Call Out *Слухач*	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	

Рис. 79A

Клієнт Групового Дзвінка		Звичайний Дзвінок	Гіперприватний Дзвінок	
Вузли Мережі	Авторизація Користувача	Всі Учасники	Аутентифікований клієнт SDNP	Неаутентифікований клієнт SDNP
$C_{1,1}$	SDNP Клієнт *Хост Приватної Групи*	Слухати, Говорити	Слухати, Говорити	–
$C_{7,1}$	SDNP Клієнт *Приватний Учасник*	Слухати, Говорити	Слухати, Говорити	Мікрофон і Динамік Відключені
$C_{9,1}$	SDNP Клієнт *Учасник*	Слухати, Говорити	Мікрофон і Динамік Відключені	
$C_{9,4}$	SDNP Клієнт *Приватний Слухач*	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
$C_{9,2}$	SDNP Клієнт *Слухач*	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	
Ph #1	Call Out *Учасник*	Слухати, Говорити	Мікрофон і Динамік Відключені	
Ph #2	Call Out *Слухач*	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	

Рис. 79B

PTT Клієнт Групового Дзвінка		Звичайний Push-to-Talk		Приватний Push-to-Talk		
Вузол Мережі	Авторизація Користувача	Хост PTT	Інший PTT	Аутентифікований Хост PTT	Аутентифікований Інший PTT	Неаутентифікована Сторона
C_{11}	SDNP Клієнт Хост Групи	**Говорити,** Пріоритет Відключення	Тільки Слухати, Мікрофон Відключений	**Говорити,** Пріоритет Відключення	Тільки Слухати, Мікрофон Відключений	--
C_{12}	SDNP Клієнт Учасник	Тільки Слухати, Мікрофон Відключений	**Говорити,** Відключити Інших	Тільки Слухати, Мікрофон Відключений	**Говорити,** Відключити Всіх Інших	Мікрофон і Динамік Відключені
C_{13}	SDNP Клієнт Учасник	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
C_{14}	SDNP Клієнт Слухач	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
C_{15}	SDNP Клієнт Слухач	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
Ph 81	Call Out	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	Мікрофон і Динамік Відключені	

Рис. 80A

PTT Клієнт Групового Дзвінка		Звичайний Push-to-Talk		Гіперприватний Push-to-Talk		
Вузол Мережі	Авторизація Користувача	Хост PTT	Інший PTT	Аутентифікований Хост PTT	Аутентифікований Інший PTT	Неаутентифікована Сторона
C_{21}	SDNP Клієнт Хост Групи	**Говорити,** Пріоритет Відключення	Тільки Слухати, Мікрофон Відключений	**Говорити,** Пріоритет Відключення	Тільки Слухати, Мікрофон Відключений	--
C_{22}	SDNP Клієнт Приватний Учасник	Тільки Слухати, Мікрофон Відключений	**Говорити,** Відключити Інших	Тільки Слухати, Мікрофон Відключений	**Говорити,** Відключити Інших	Мікрофон і Динамік Відключені
C_{23}	SDNP Клієнт Учасник	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	Мікрофон і Динамік Відключені	
C_{24}	SDNP Клієнт Приватний Слухач	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	
C_{25}	SDNP Клієнт Тільки Слухати	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	Мікрофон і Динамік Відключені	
Ph 8	Call Out	Тільки Слухати, Мікрофон Відключений	Тільки Слухати, Мікрофон Відключений	Мікрофон і Динамік Відключені	Мікрофон і Динамік Відключені	

Рис. 80B

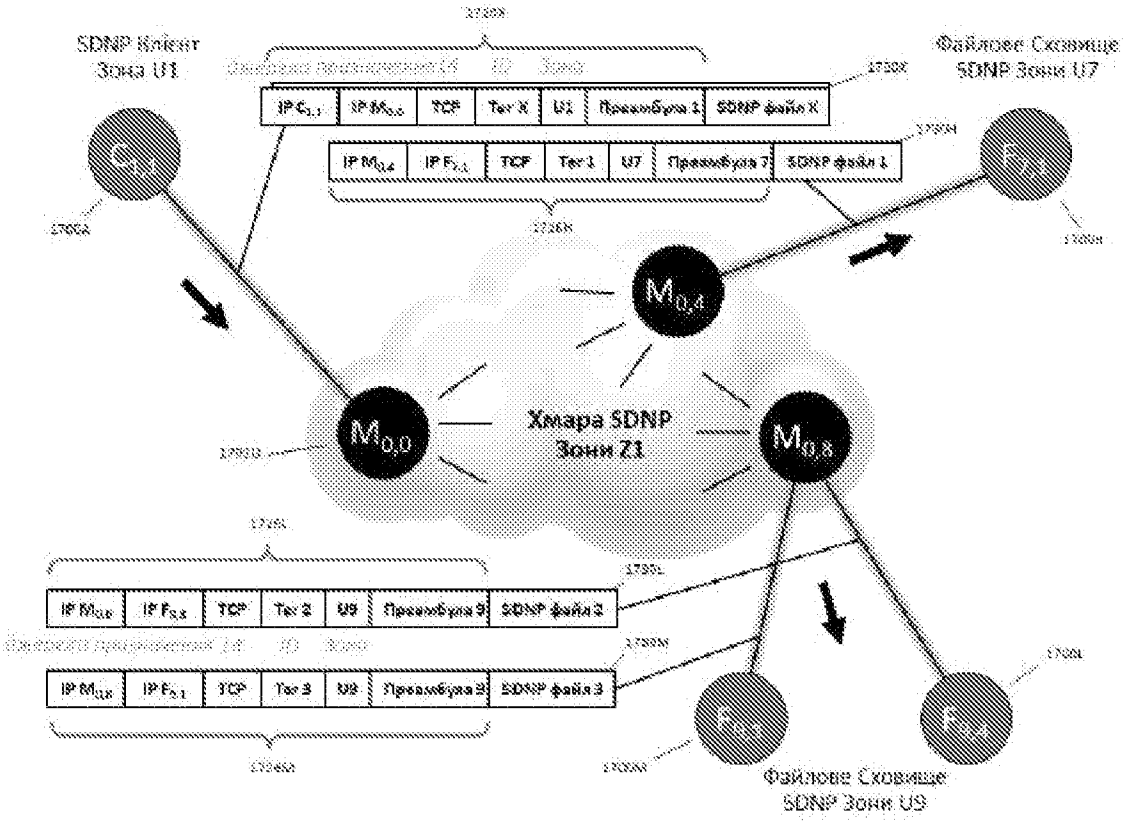


Рис. 81

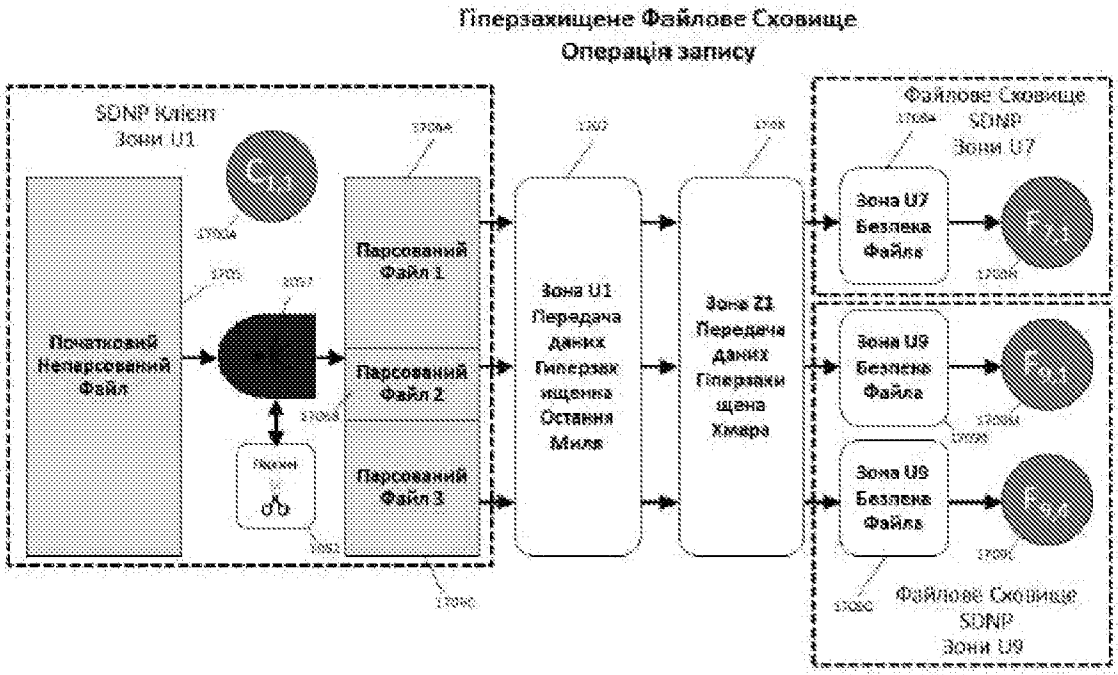


Рис. 82А

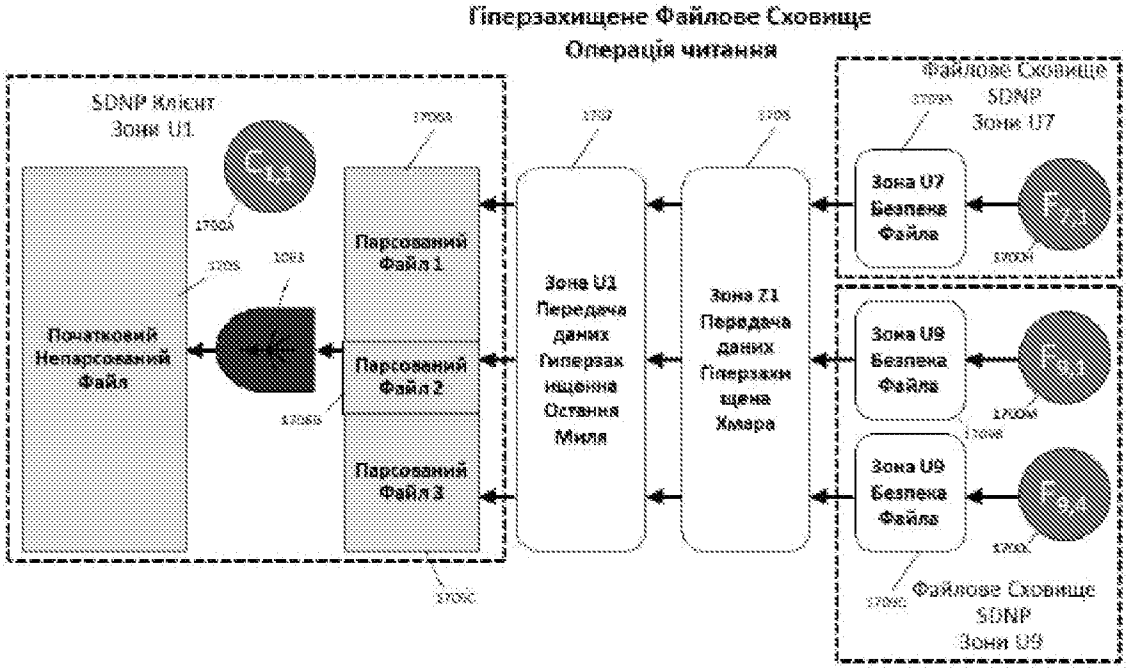


Рис. 82B

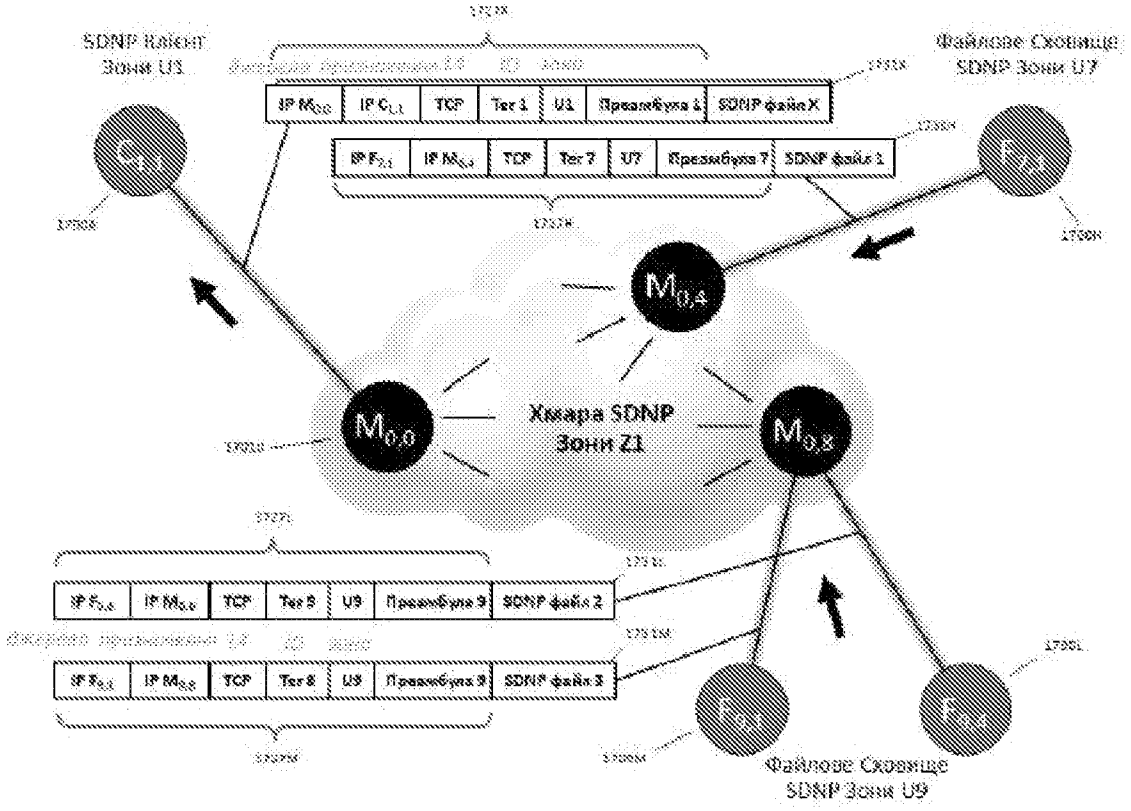


Рис. 83

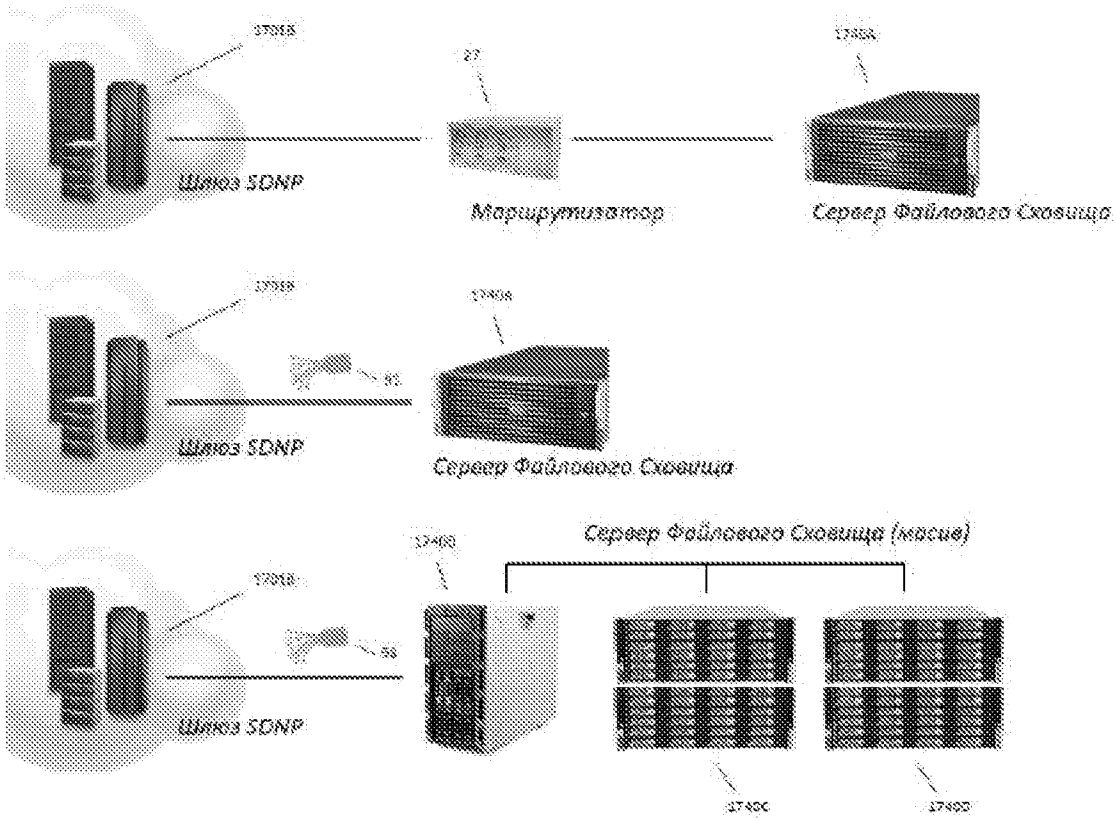


Рис. 84A

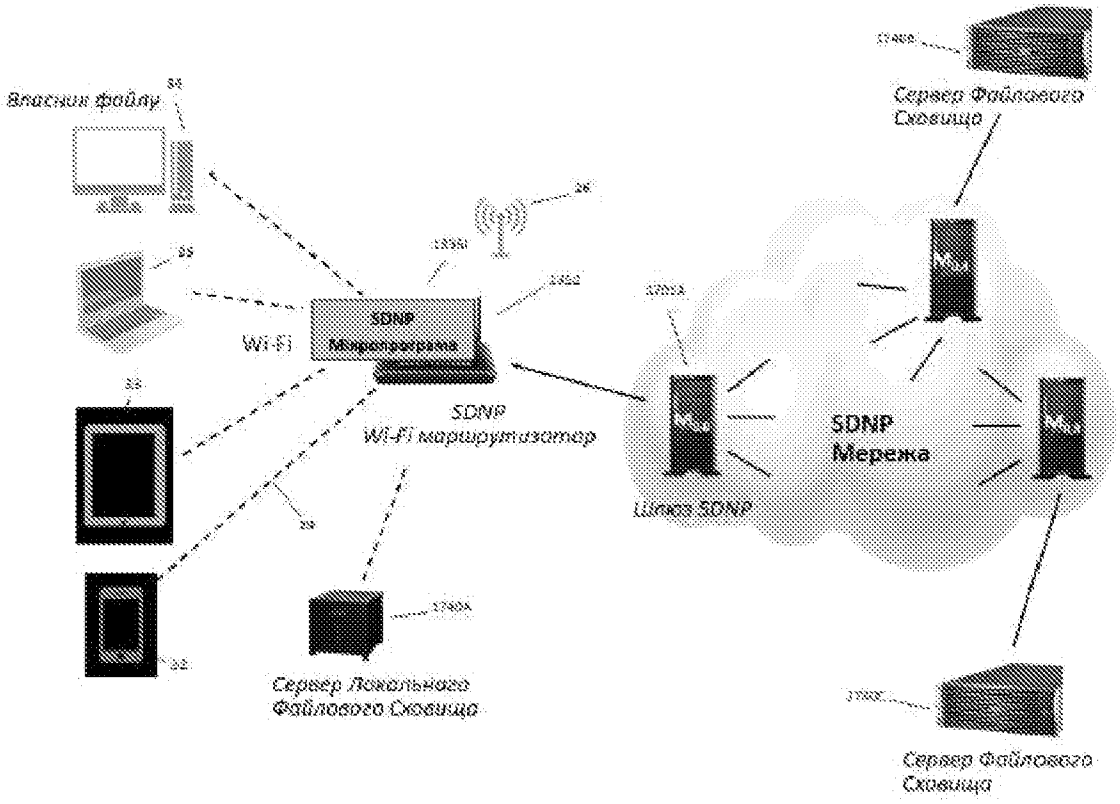


Рис. 84B

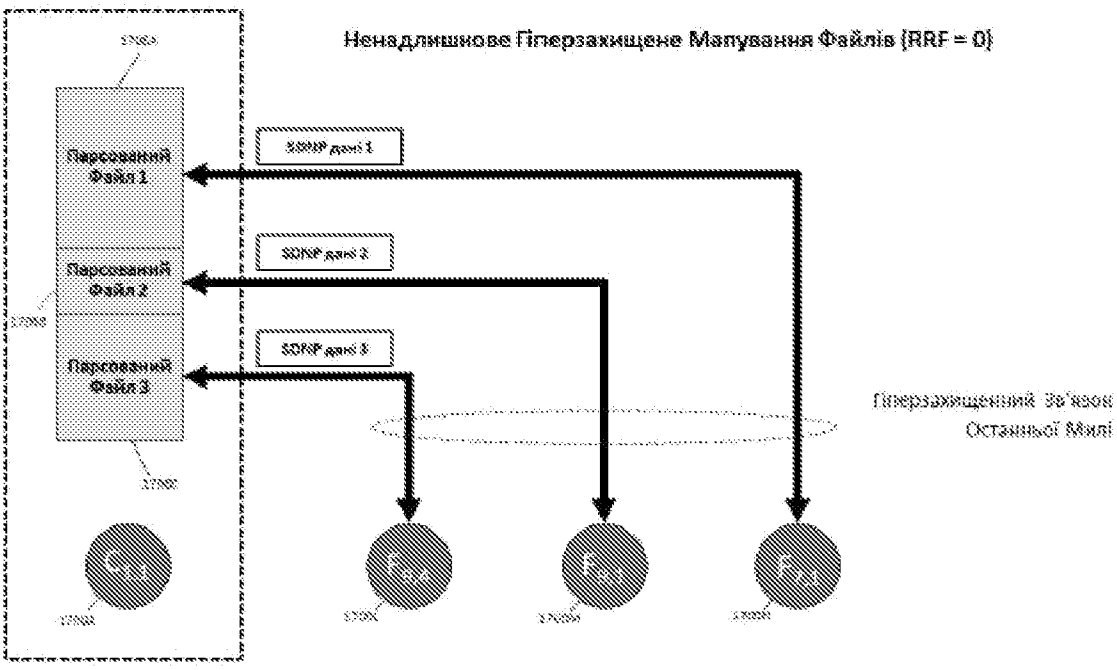


Рис. 85A

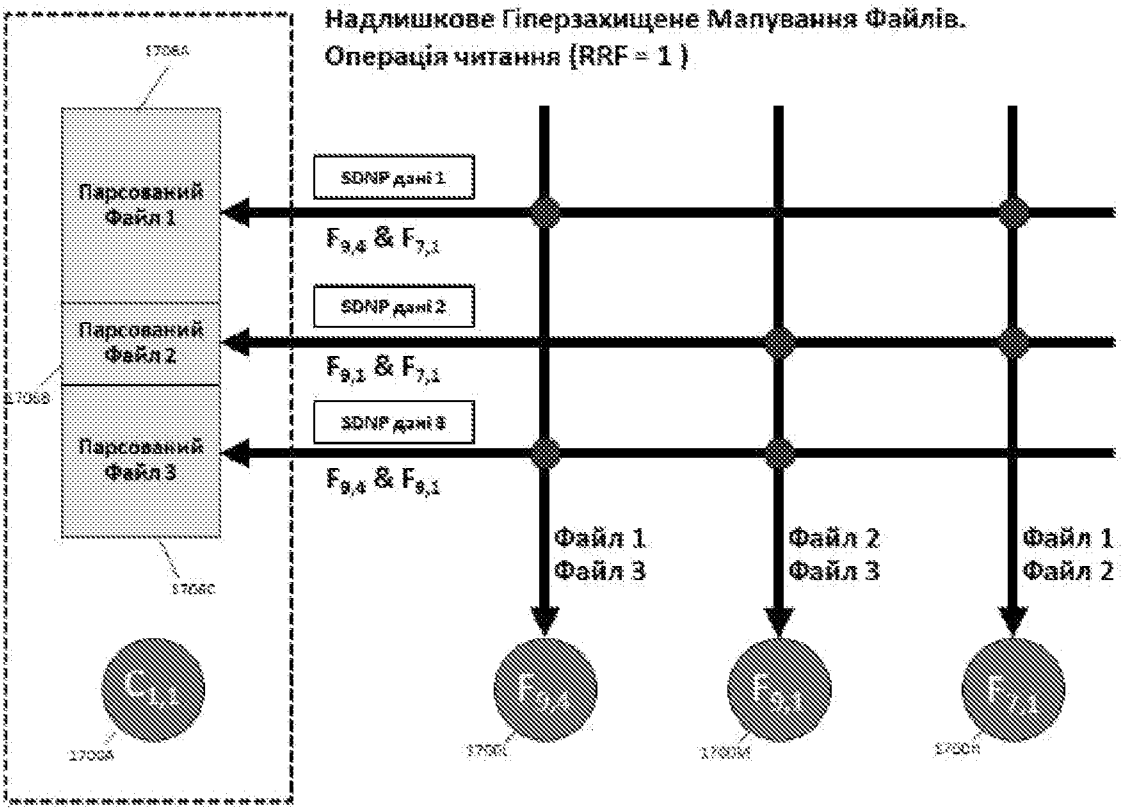


Рис. 85B

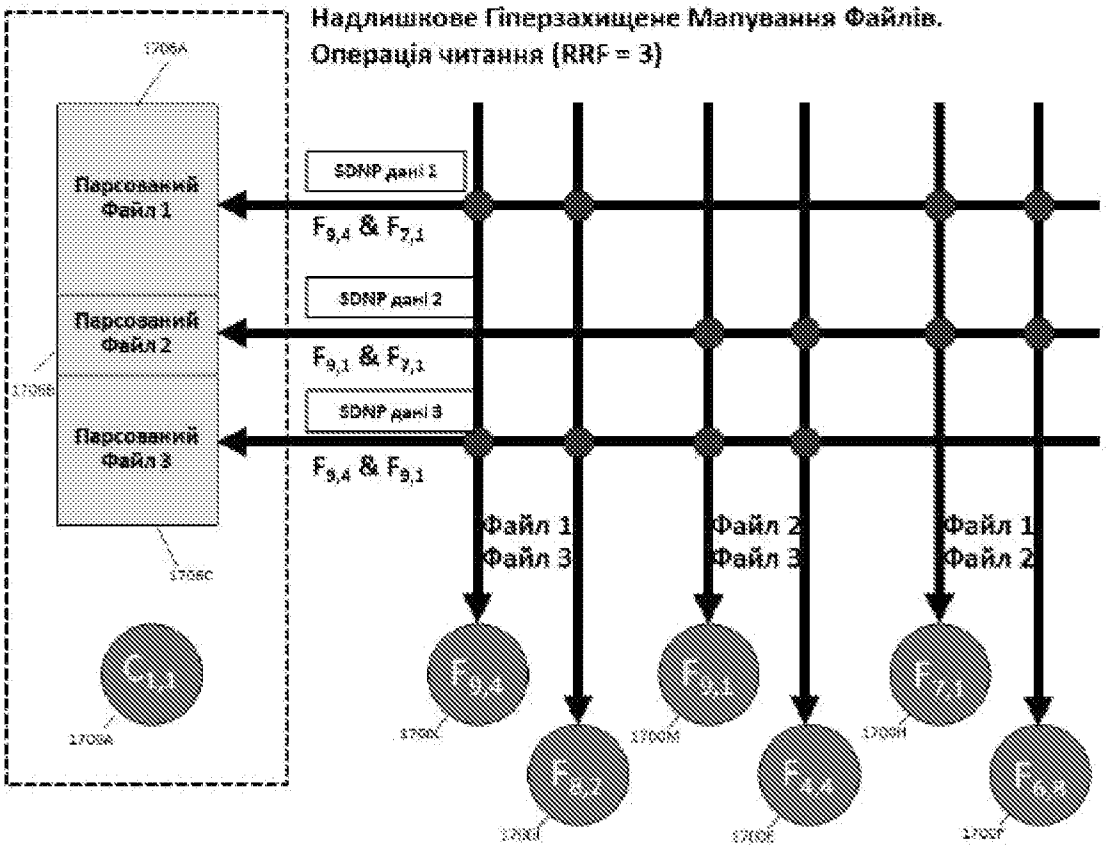

Надлишкове Гіперзахищене Мапування Файлів.
Операція читання (RRF = 3)
Парсований Файл 1
Парсований Файл 2
Парсований Файл 3
SDNP дані 1
SDNP дані 2
SDNP дані 3
$F_{9,4}$ & $F_{7,1}$
$F_{9,1}$ & $F_{7,1}$
$F_{9,4}$ & $F_{9,1}$
Файл 1
Файл 3
Файл 2
Файл 3
Файл 1
Файл 2

Рис. 85C

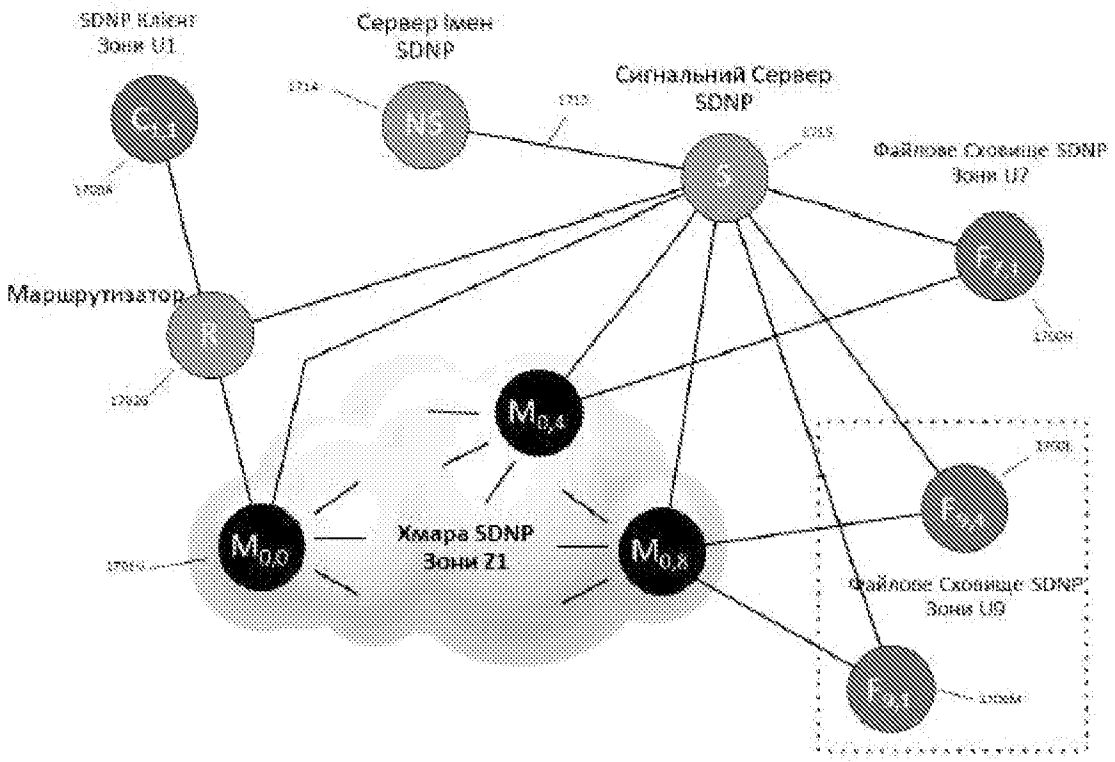


Рис. 86

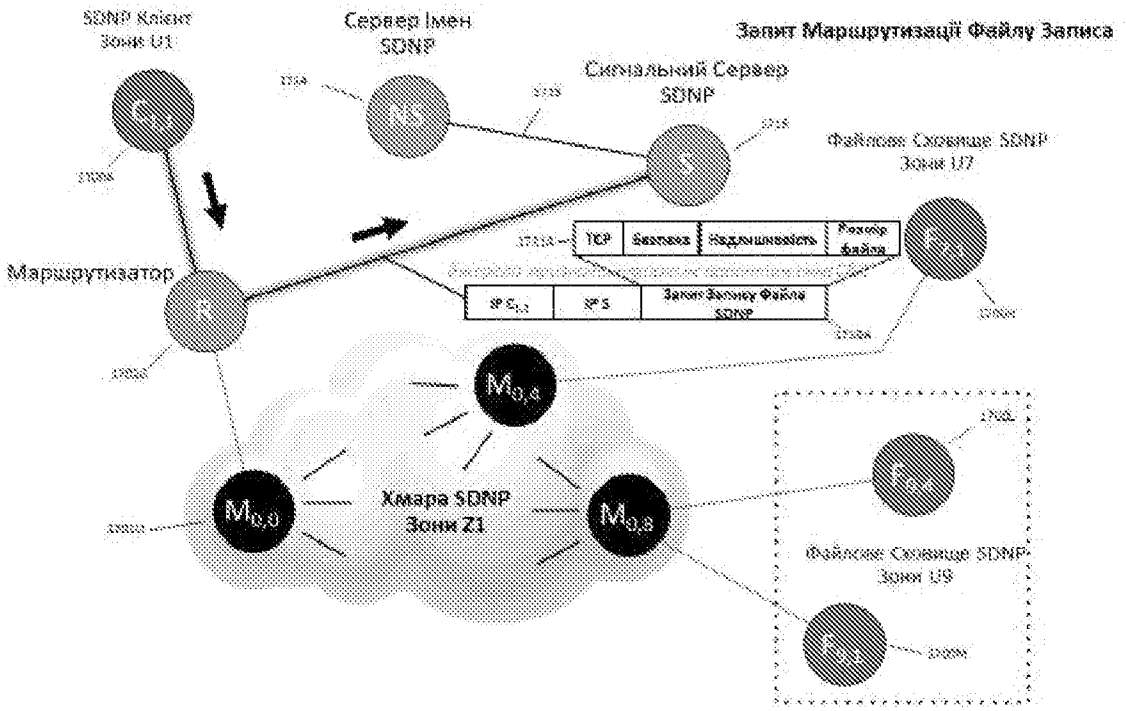


Рис. 87А

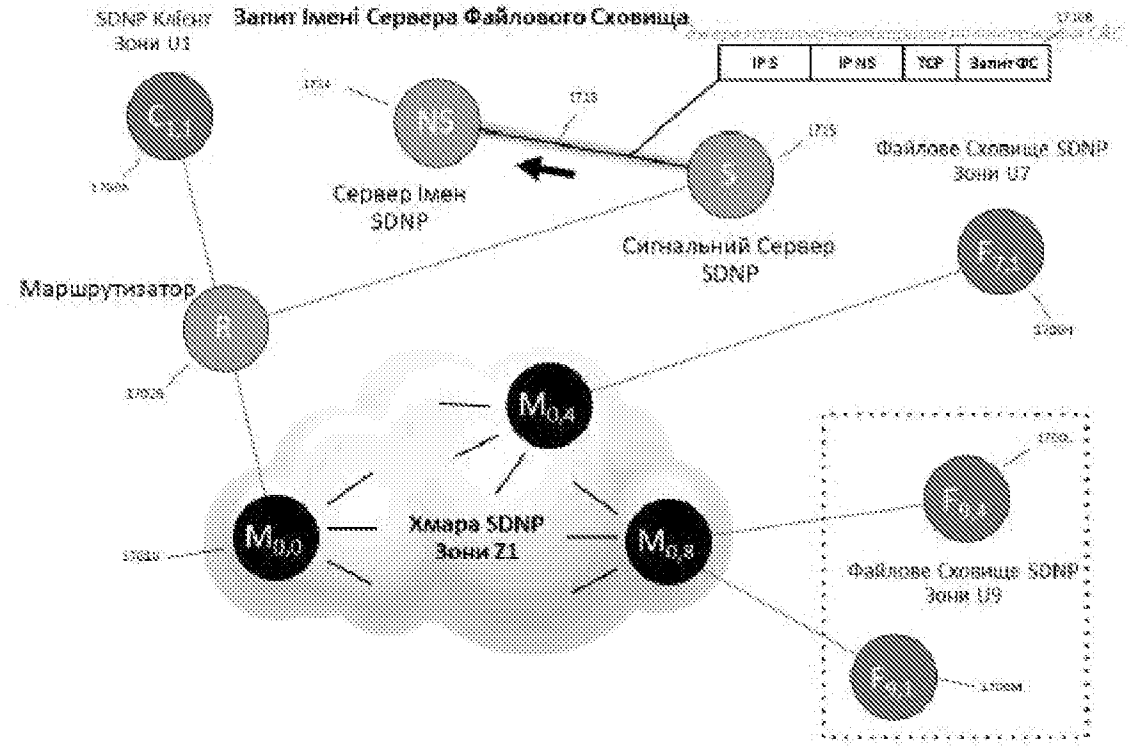


Рис. 87B

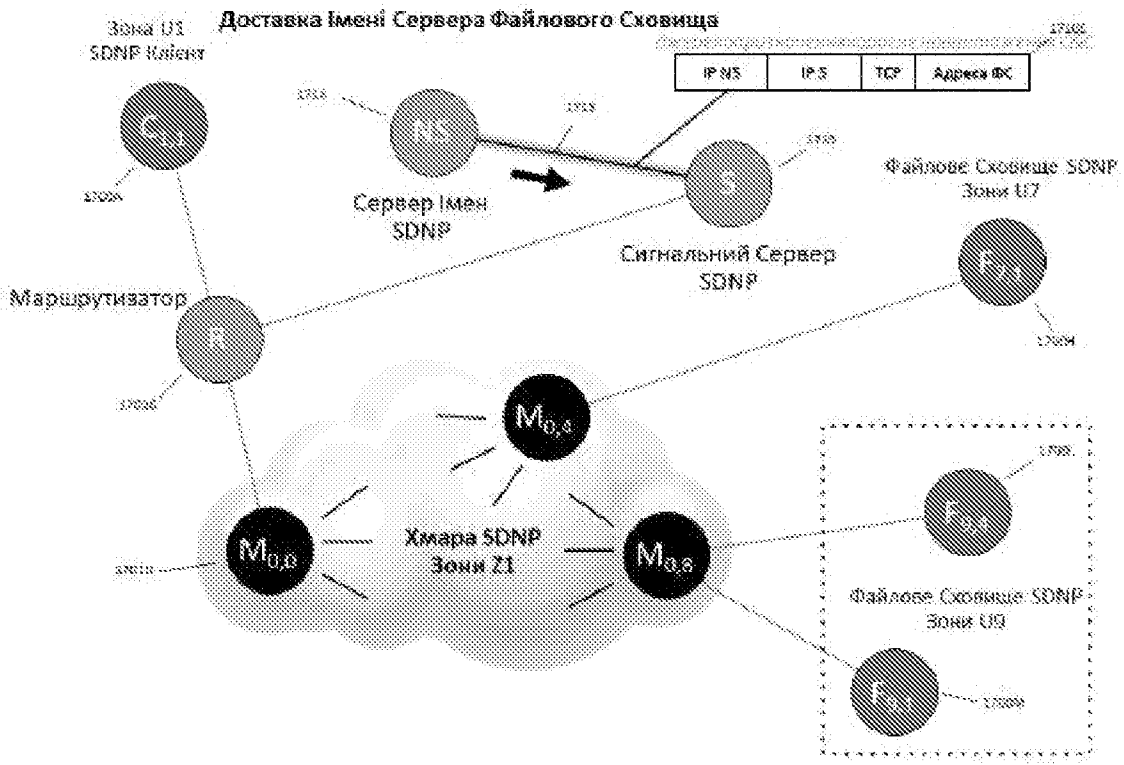


Рис. 87C

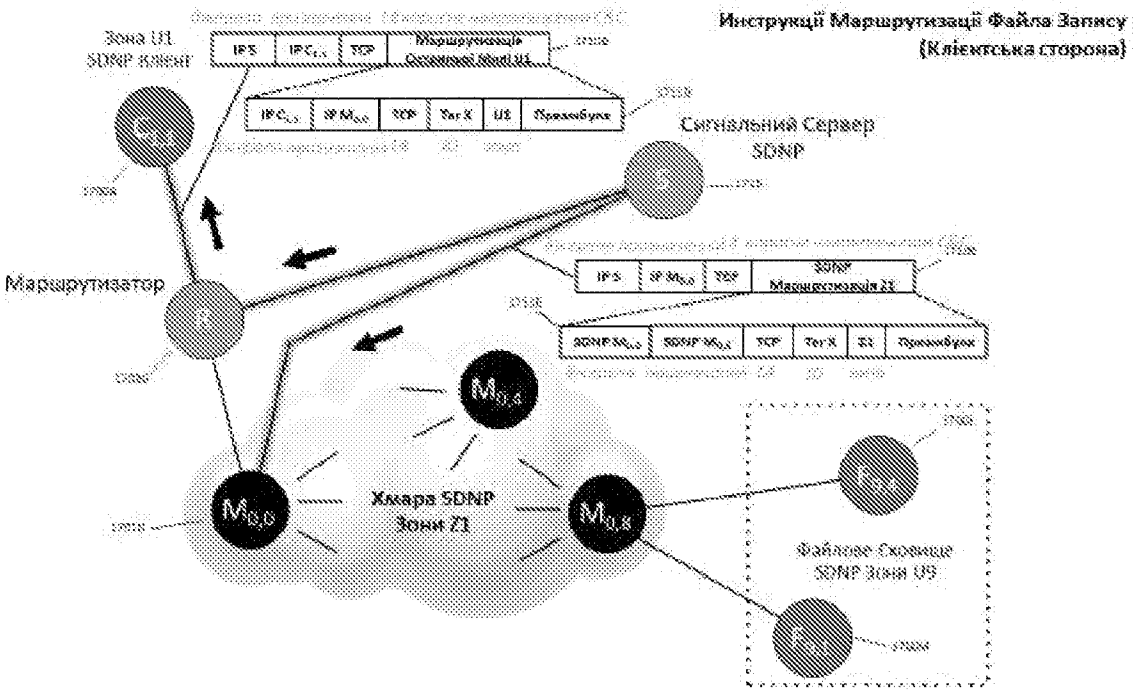


Рис. 87D

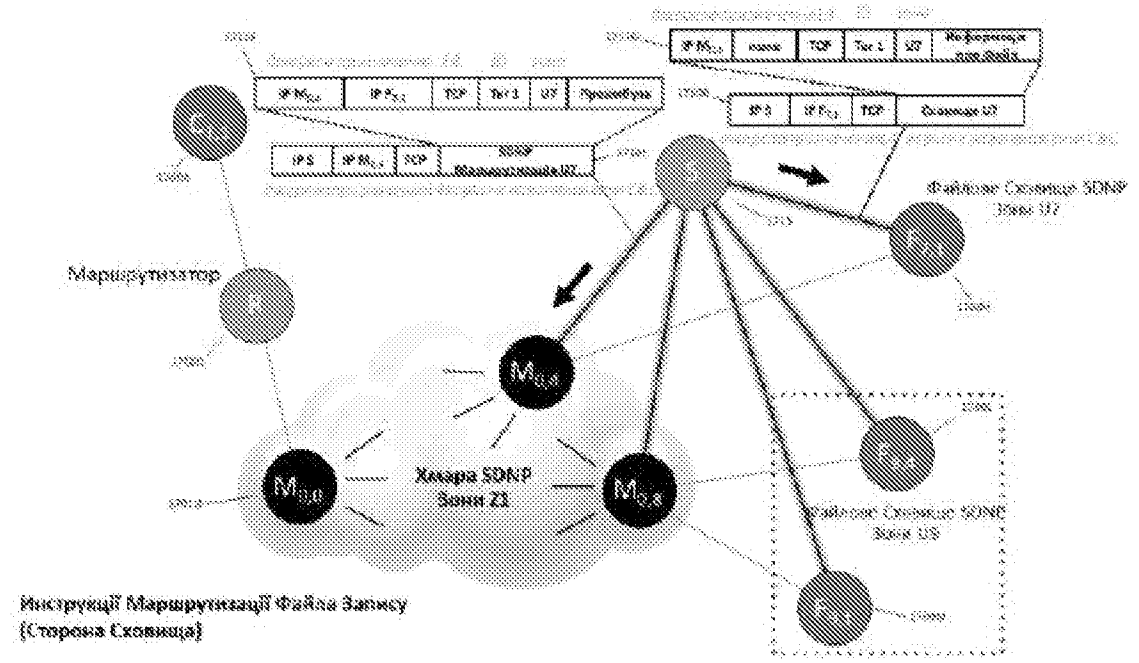


Рис. 87E

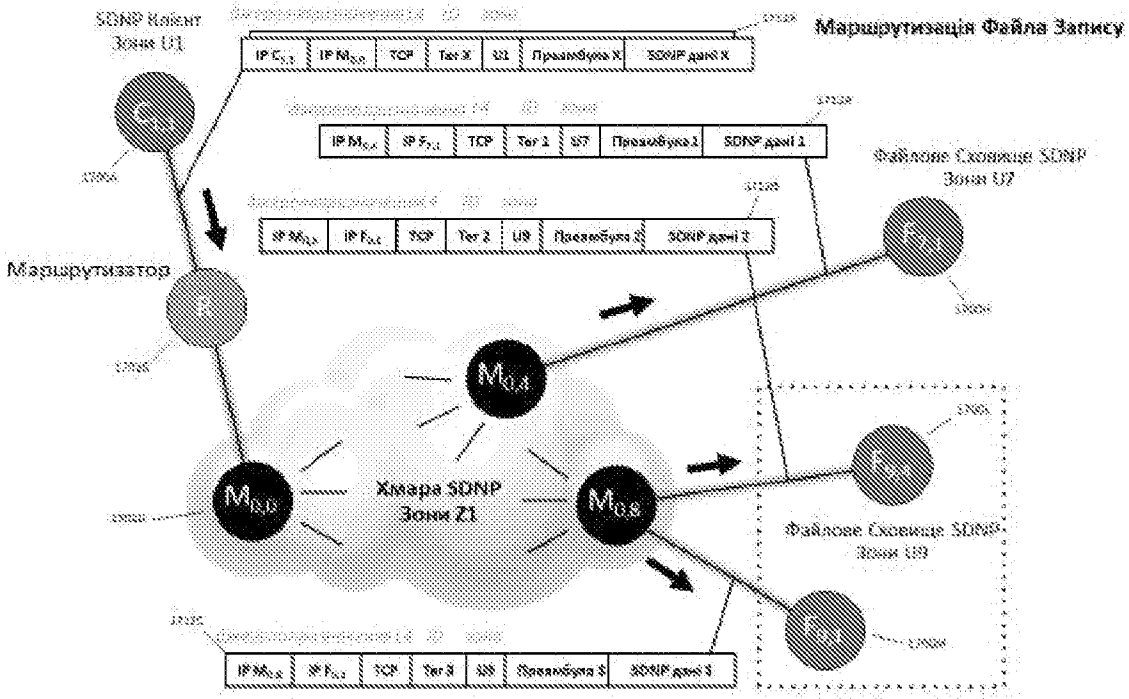


Рис. 88

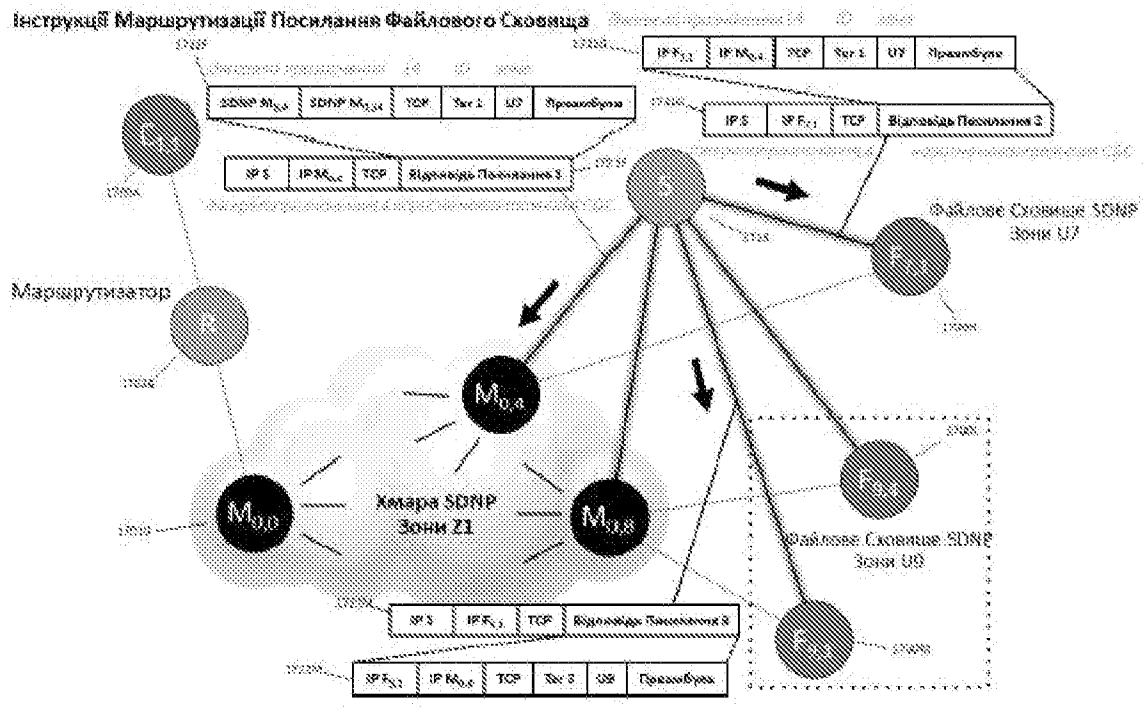


Рис. 89А

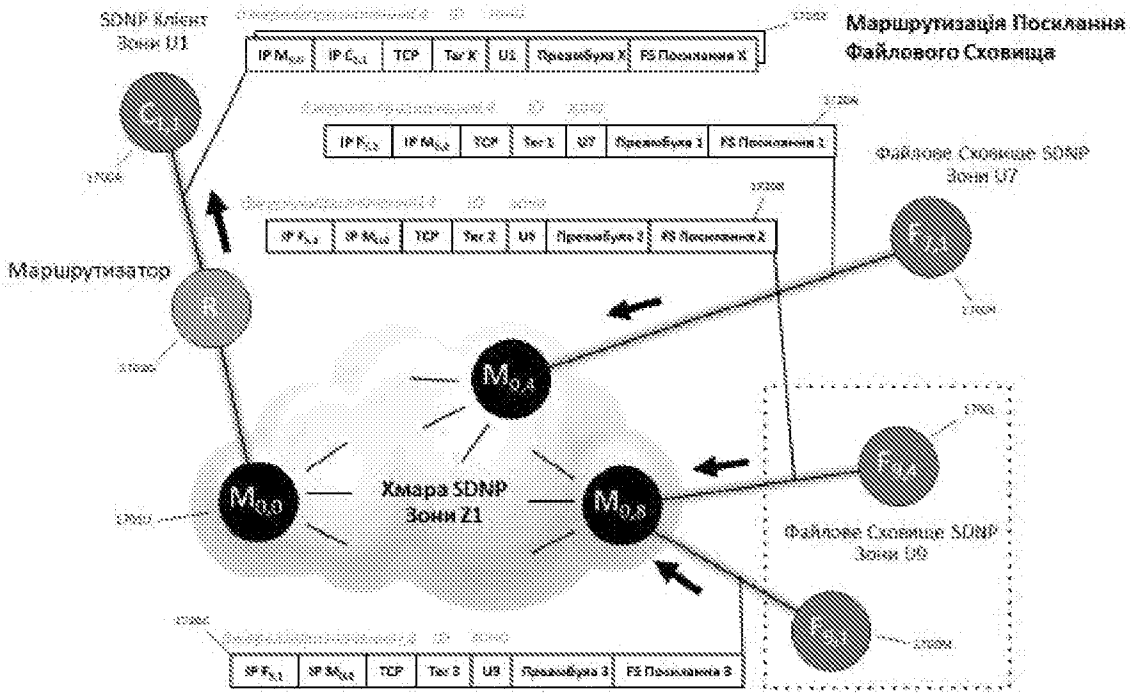


Рис. 89B

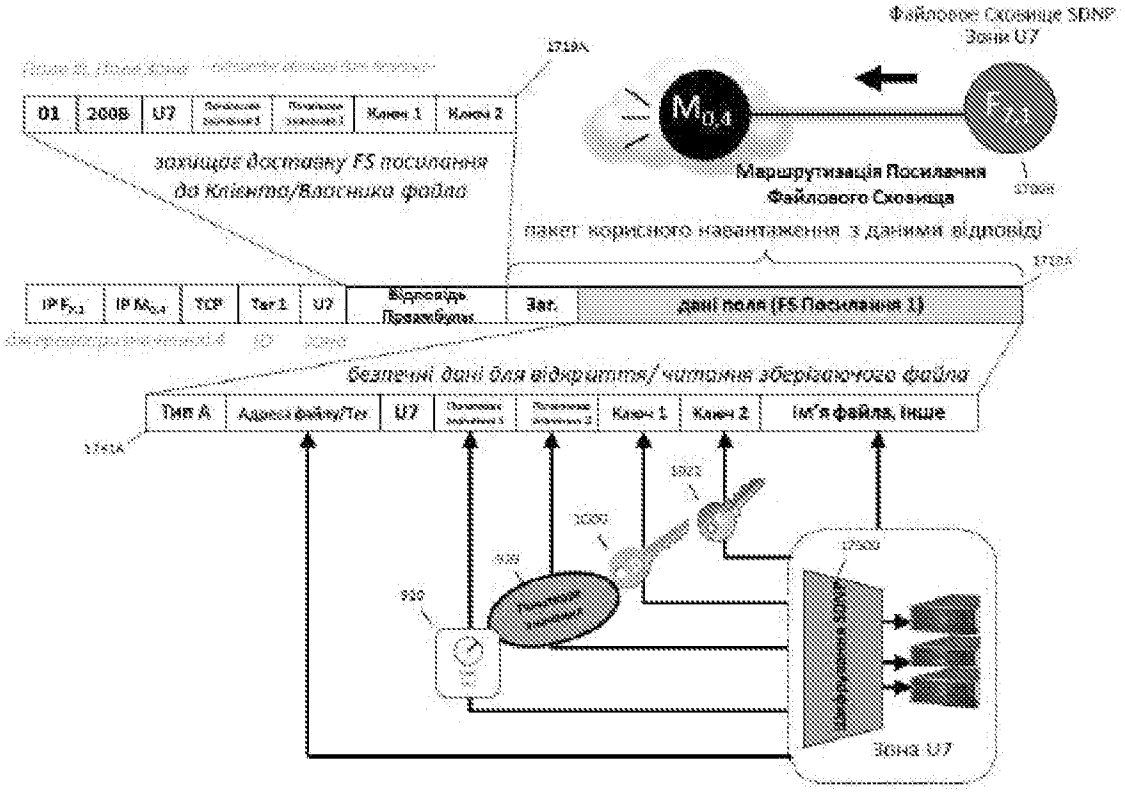


Рис. 89C

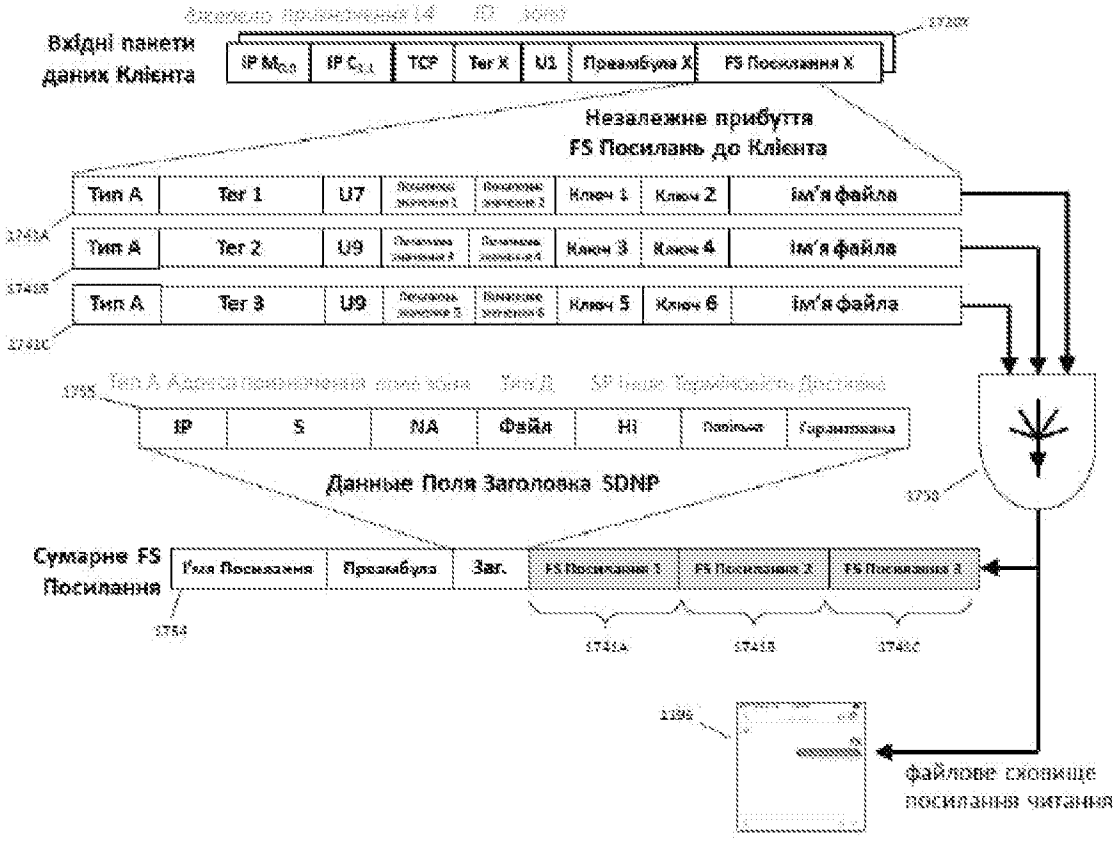


Рис. 89D

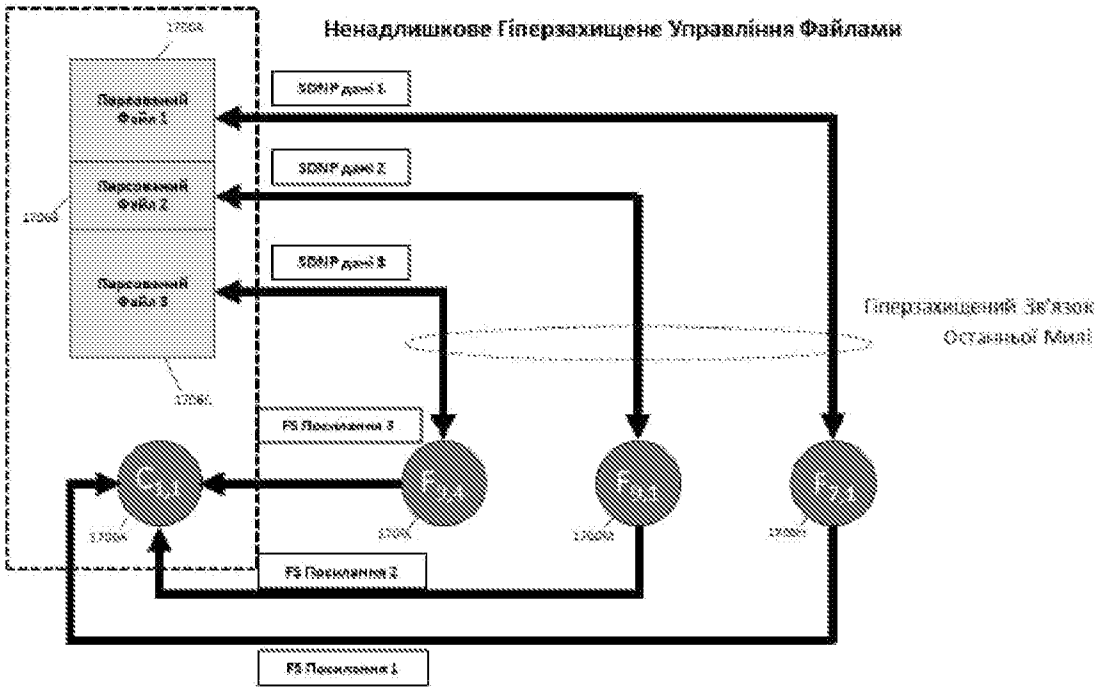


Рис. 90A

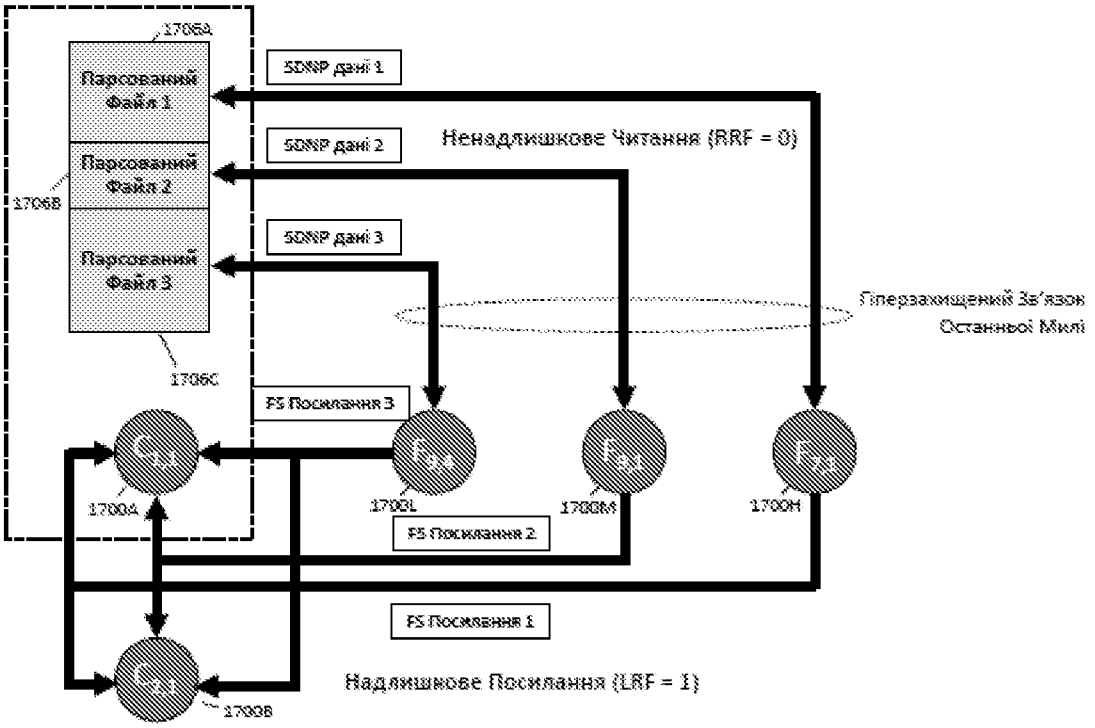


Рис. 90B

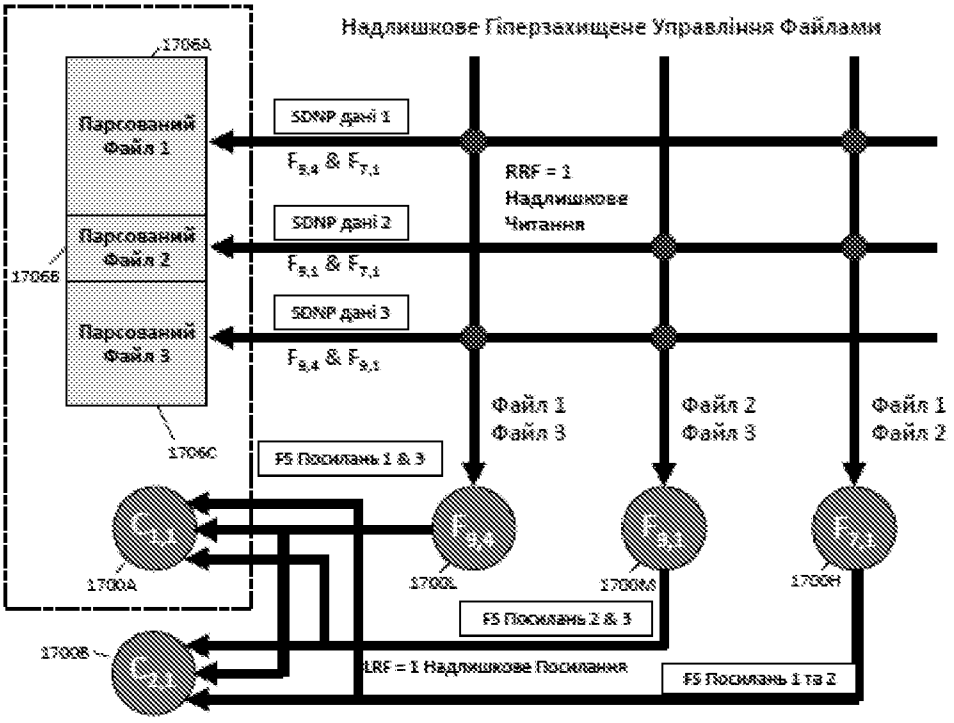


Рис. 90C

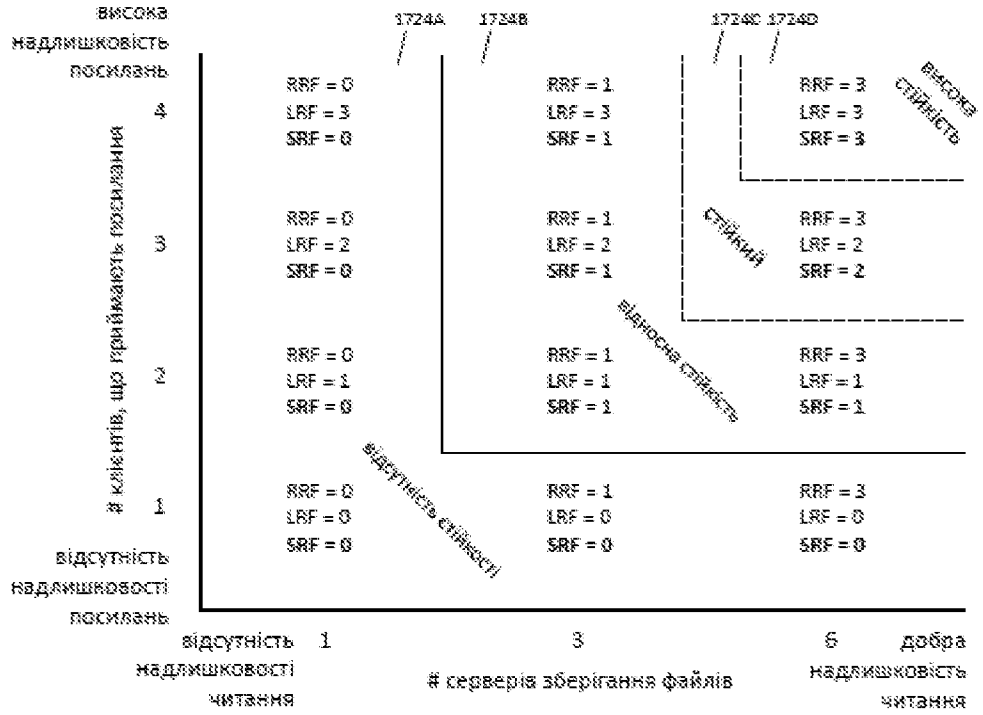

ВИСОКА НАДЛИШКОВІСТЬ ПОСИЛАНЬ
КЛІЄНТІВ, ЩО ПРИЙМАЮТЬ ПОСИЛАННЯ
4
3
2
1
ВІДСУТНІСТЬ НАДЛИШКОВОСТІ ПОСИЛАНЬ
1724A
1724B
1724C
1724D
RRF = 0 LRF = 3 SRF = 0
RRF = 1 LRF = 3 SRF = 1
RRF = 3 LRF = 3 SRF = 3
ВИСОКА СТІЙКІСТЬ
RRF = 0 LRF = 2 SRF = 0
RRF = 1 LRF = 2 SRF = 1
RRF = 3 LRF = 2 SRF = 2
СТІЙКИЙ
ВІДНОСНА СТІЙКІСТЬ
RRF = 0 LRF = 1 SRF = 0
RRF = 1 LRF = 1 SRF = 1
RRF = 3 LRF = 1 SRF = 1
ВІДСУТНІСТЬ СТІЙКОСТІ
RRF = 0 LRF = 0 SRF = 0
RRF = 1 LRF = 0 SRF = 0
RRF = 3 LRF = 0 SRF = 0
відсутність надлишковості читання
1
3
6
добра надлишковість читання
серверів зберігання файлів

Рис. 91

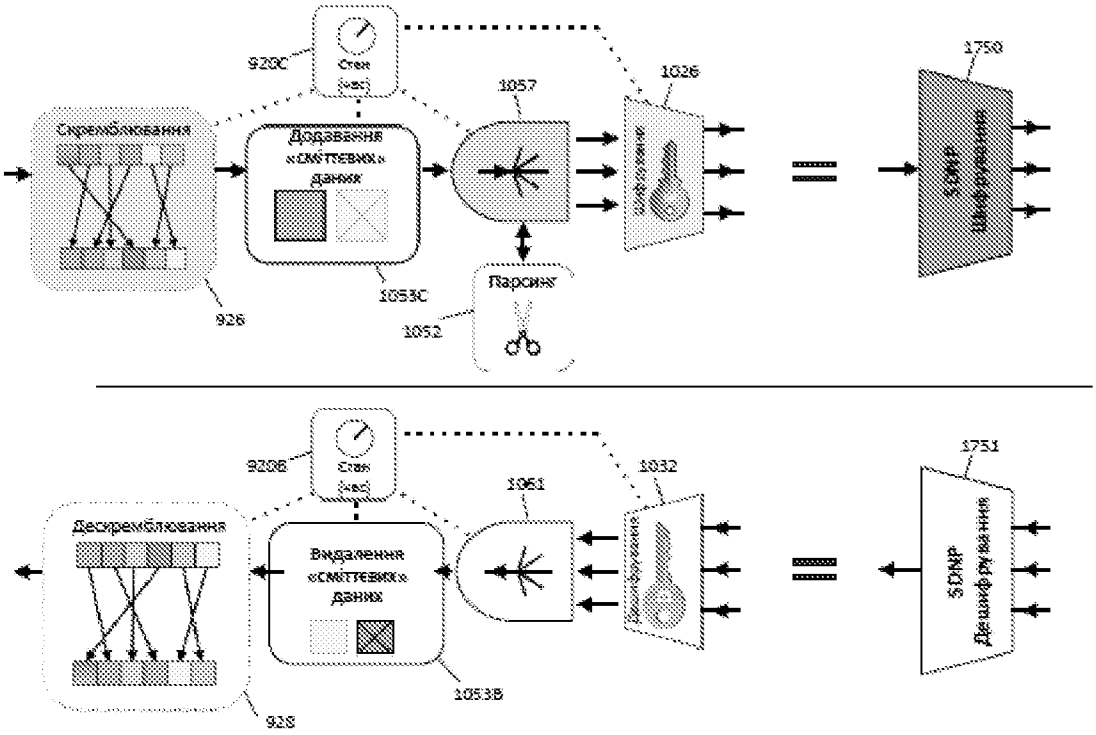

Скремблювання
926
Додавання «сміттєвих» даних
1053C
Парсинг
1052
Стан (час)
920C
1057
1026
1750
SDNP Шифрування
Дескремблювання
928
Видалення «сміттєвих» даних
1053B
1051
1032
1751
SDNP Дешифрування

Рис. 92

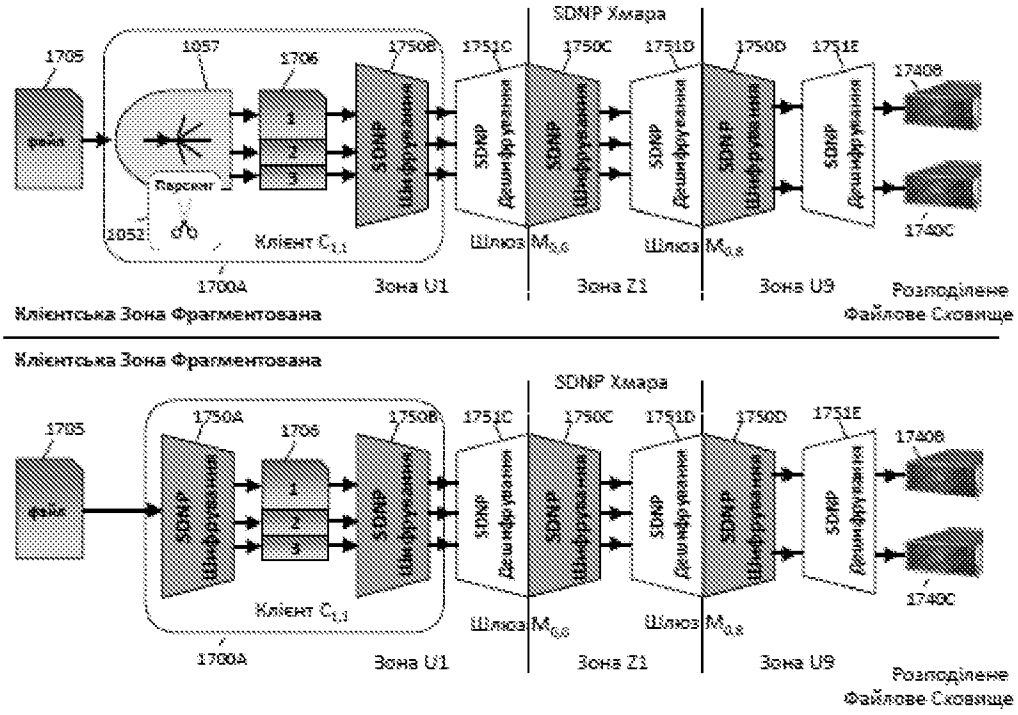


Рис. 93A

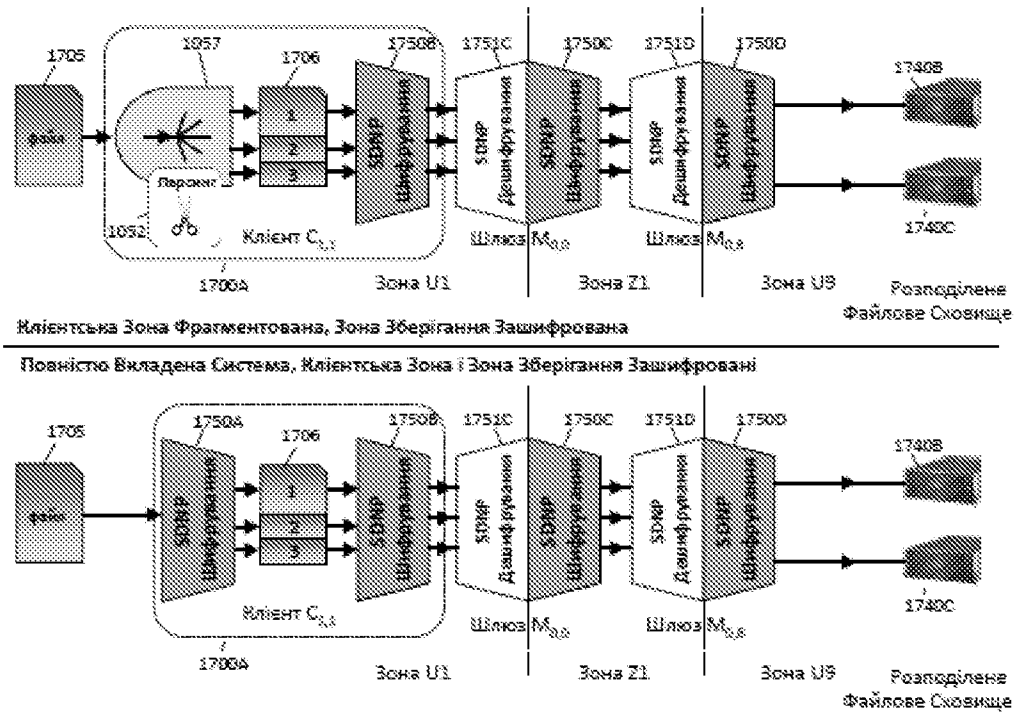


Рис. 93B

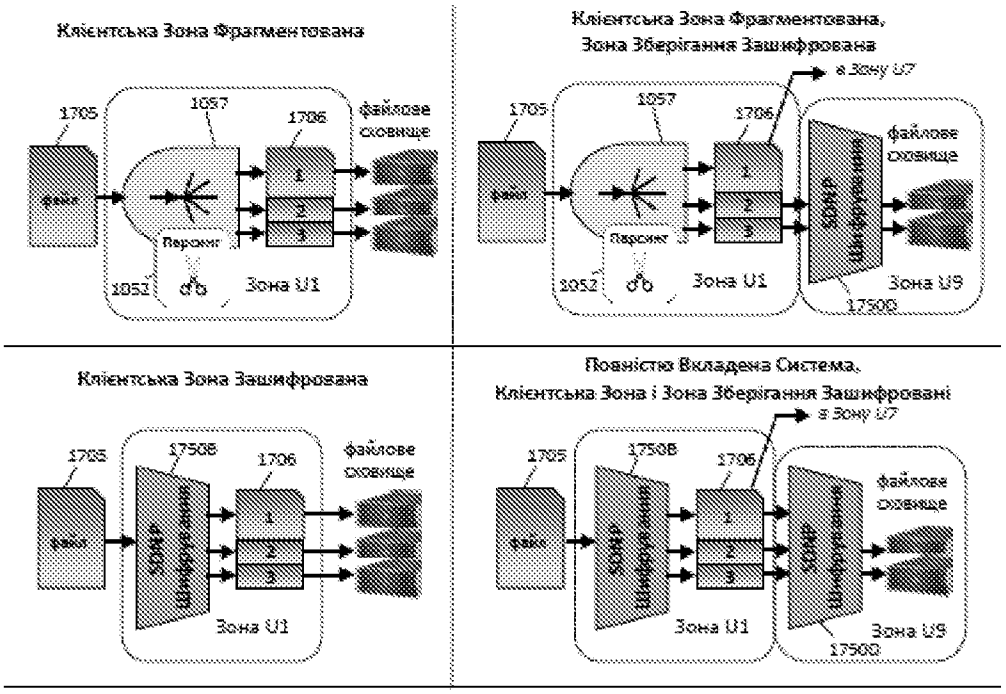

Клієнтська Зона Фрагментована
Клієнтська Зона Фрагментована,
Зона Зберігання Зашифрована
в Зону U7
Клієнтська Зона Зашифрована
Повністю Вкладена Система,
Клієнтська Зона і Зона Зберігання Зашифровані
файлове сховище
Зона U1
Зона U9

Рис. 94

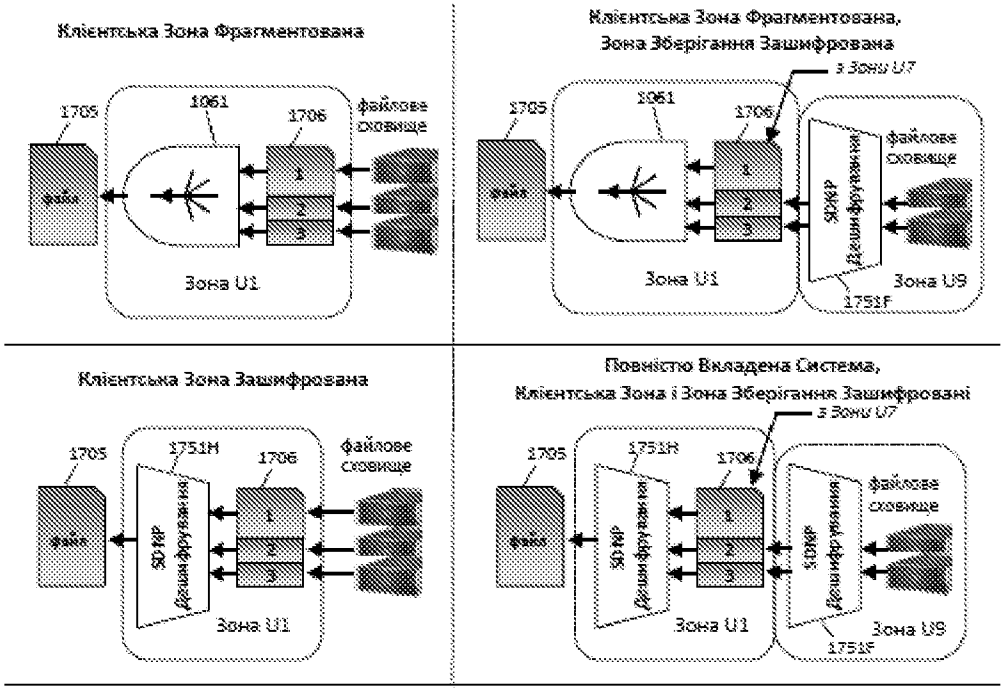

Клієнтська Зона Фрагментована
Клієнтська Зона Фрагментована,
Зона Зберігання Зашифрована
в Зону U7
Клієнтська Зона Зашифрована
Повністю Вкладена Система,
Клієнтська Зона і Зона Зберігання Зашифровані
файлове сховище
Зона U1
Зона U9

Рис. 95

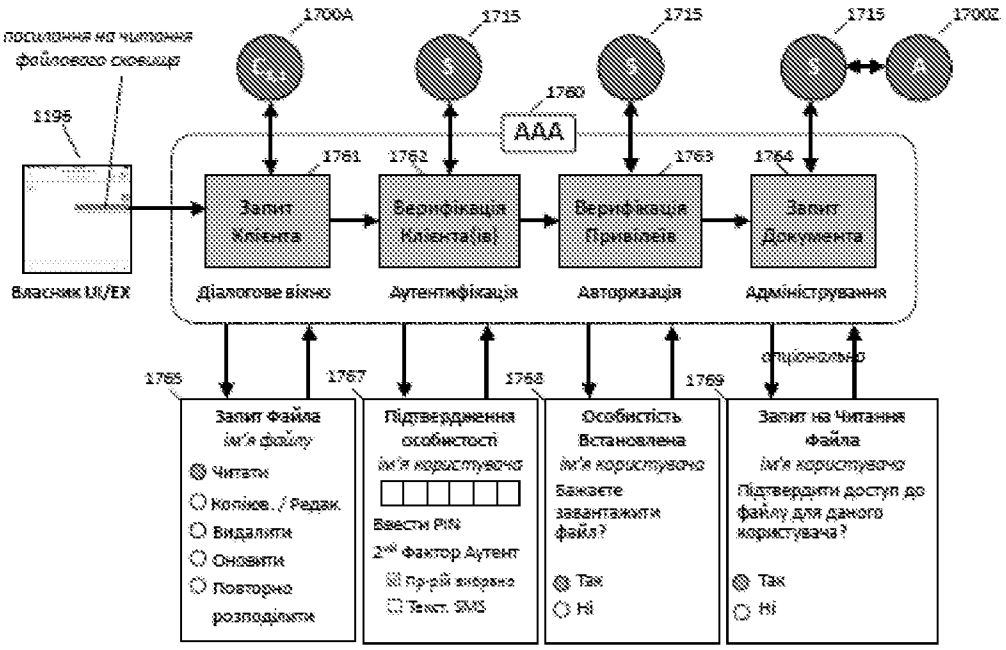


Рис. 96A

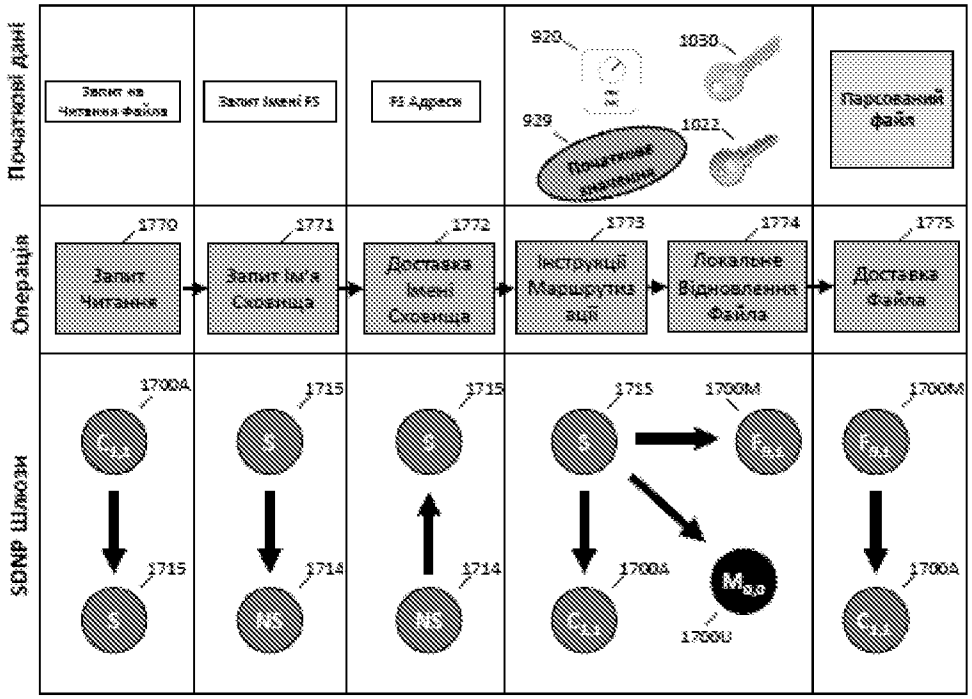


Рис. 96B

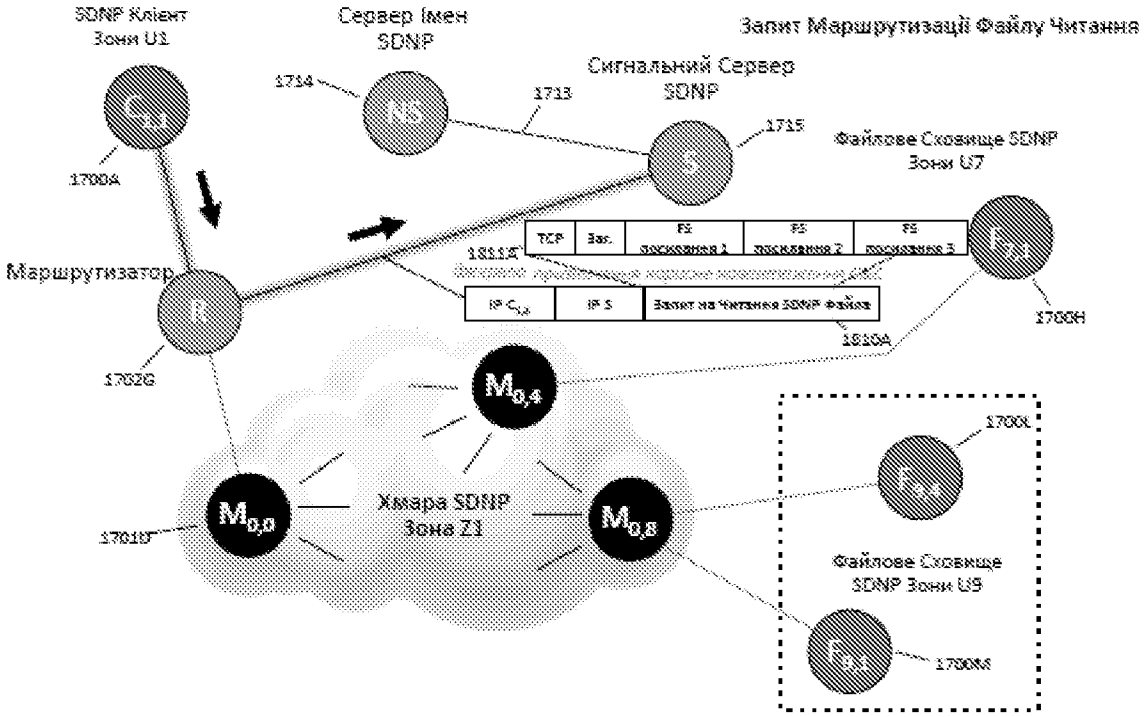


Рис. 97A

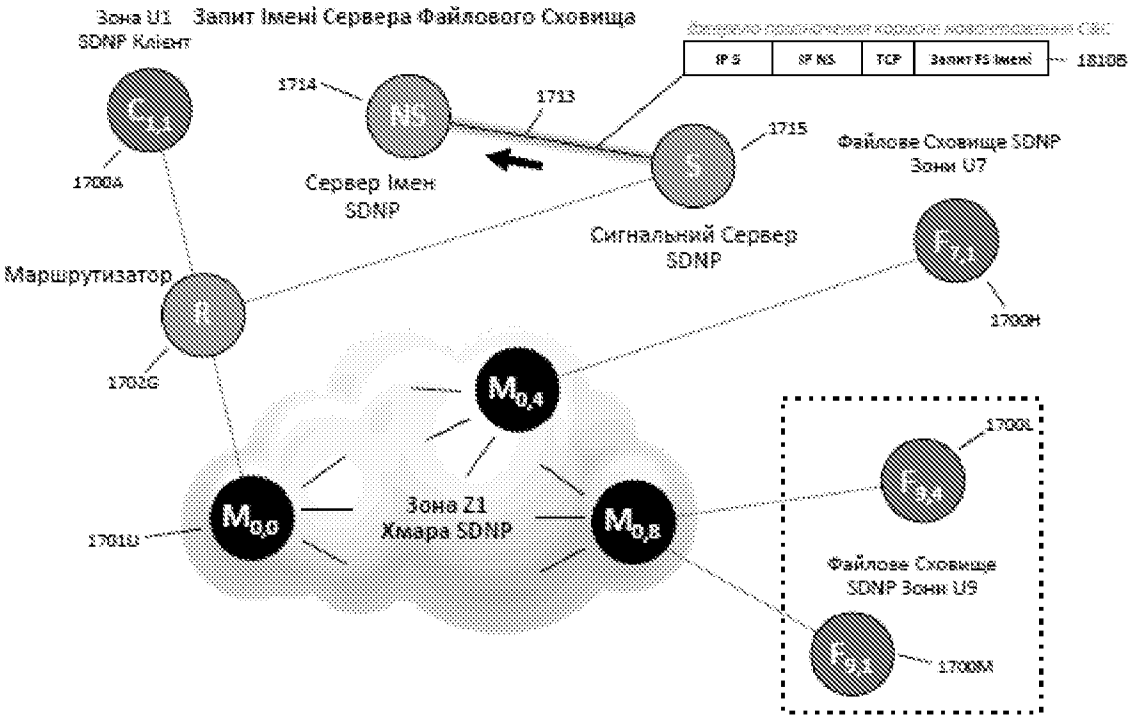


Рис. 97B

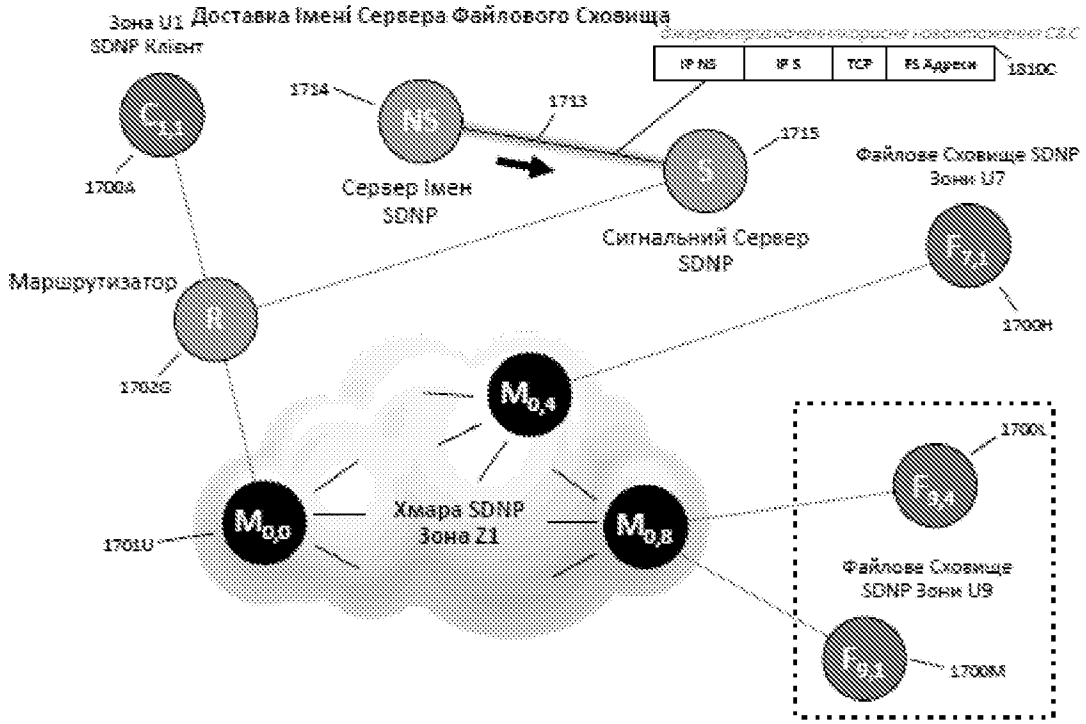


Рис. 97C

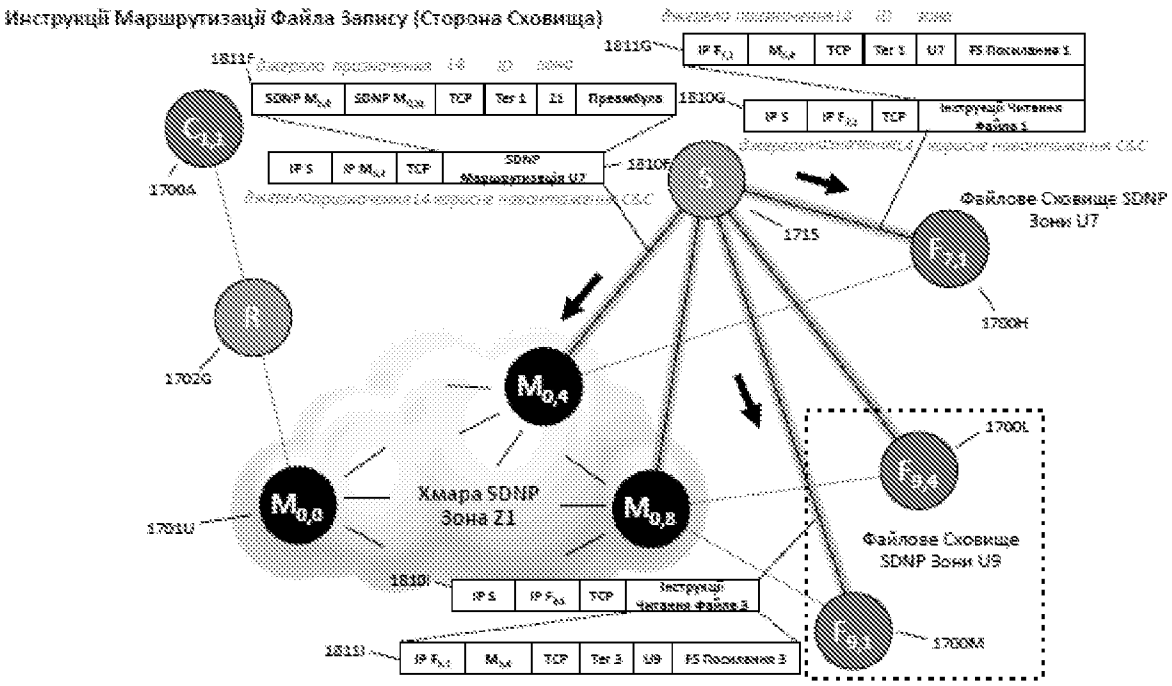


Рис. 97D

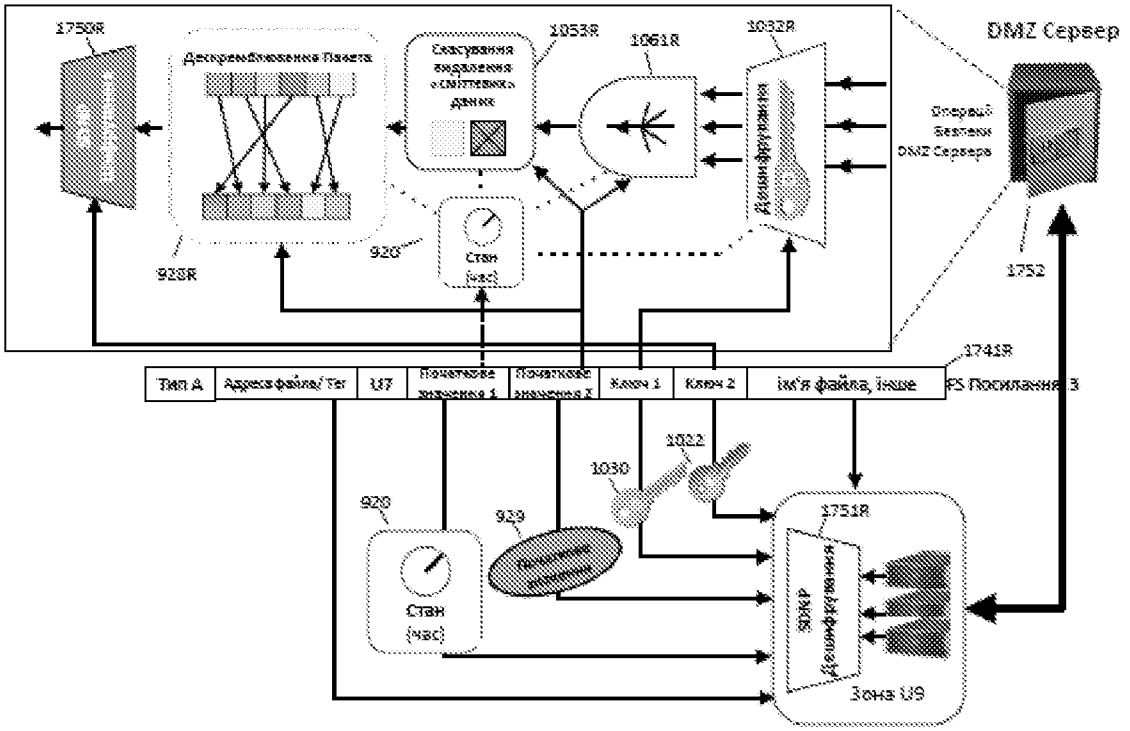

DMZ Сервер
Операції безпеки DMZ Сервера
Дешифрування
Дешифрування
Ствн (чвс)
Ствн (чвс)
Тип А
Адреса файлу/ Тег
U7
Ключ 1
Ключ 2
ім'я файла, інше
Зона U9

Рис. 98

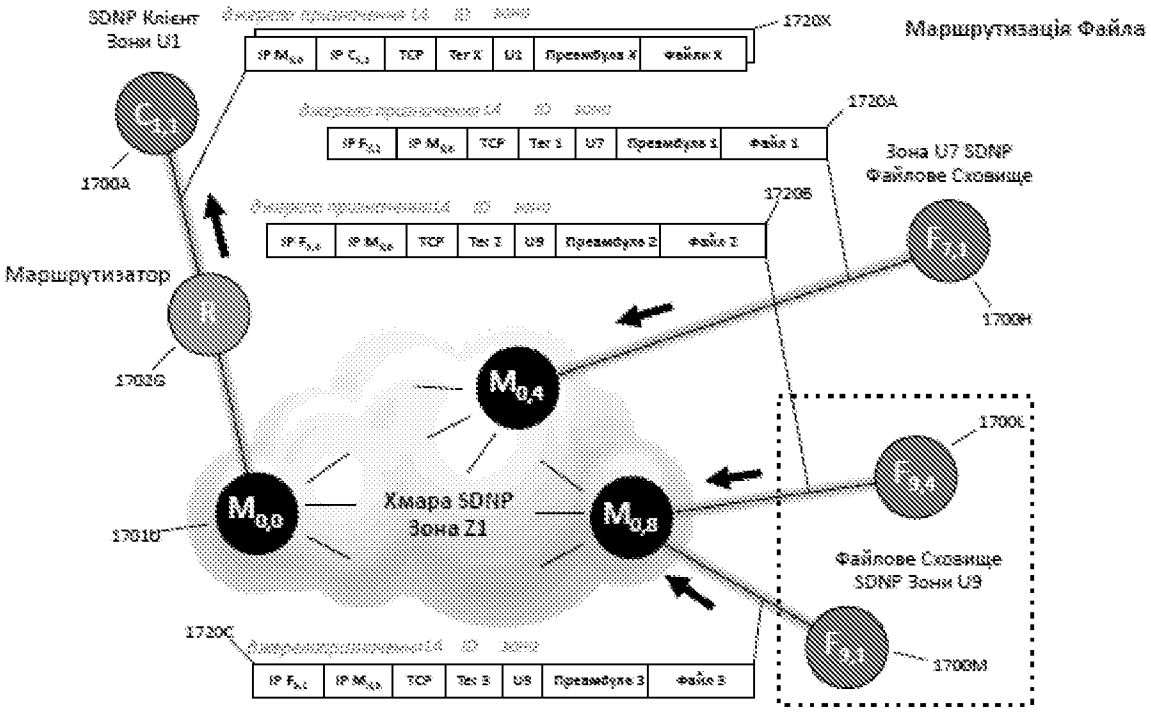

SDNP Клієнт Зони U1
Маршрутизація Файла
Маршрутизатор
Зона U7 SDNP Файлове Сховище
Хмара SDNP Зона Z1
Файлове Сховище SDNP Зони U9
IP
TCP
Тег X
Тег 1
Тег 2
Тег 3
U1
U7
U9
Преамбула X
Преамбула 1
Преамбула 2
Преамбула 3
Файли X
Файл 1
Файл 2
Файл 3

Рис. 99

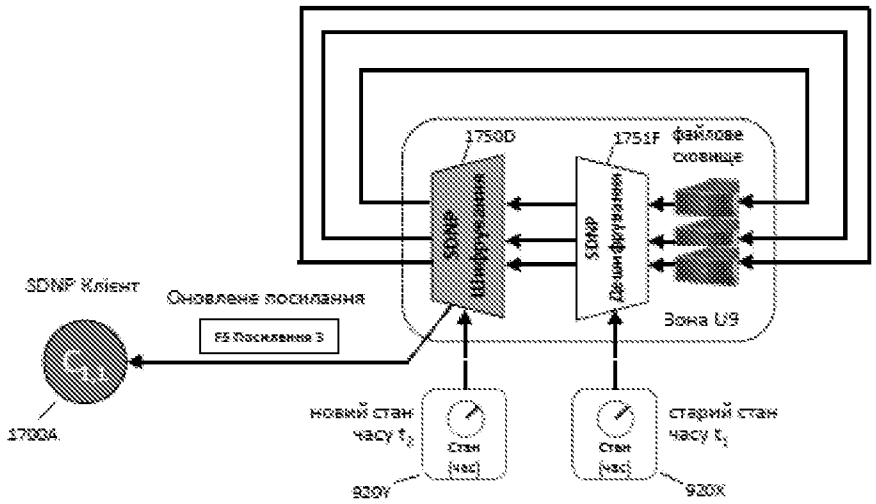


Рис. 100

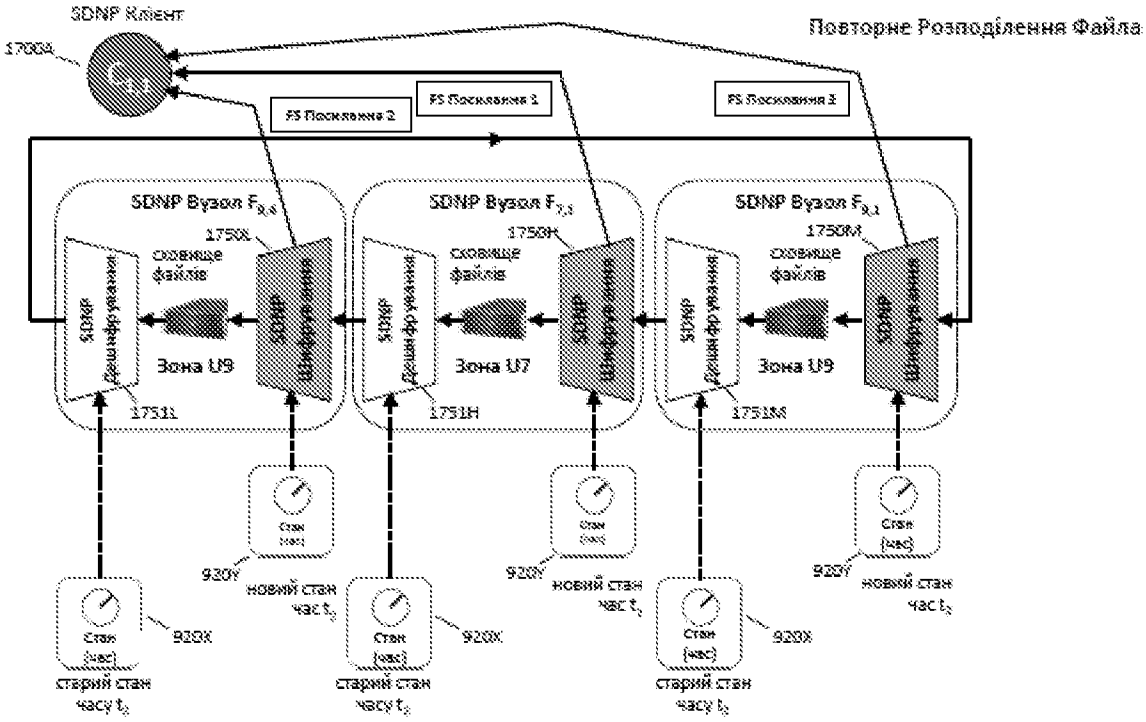


Рис. 101



Рис. 102

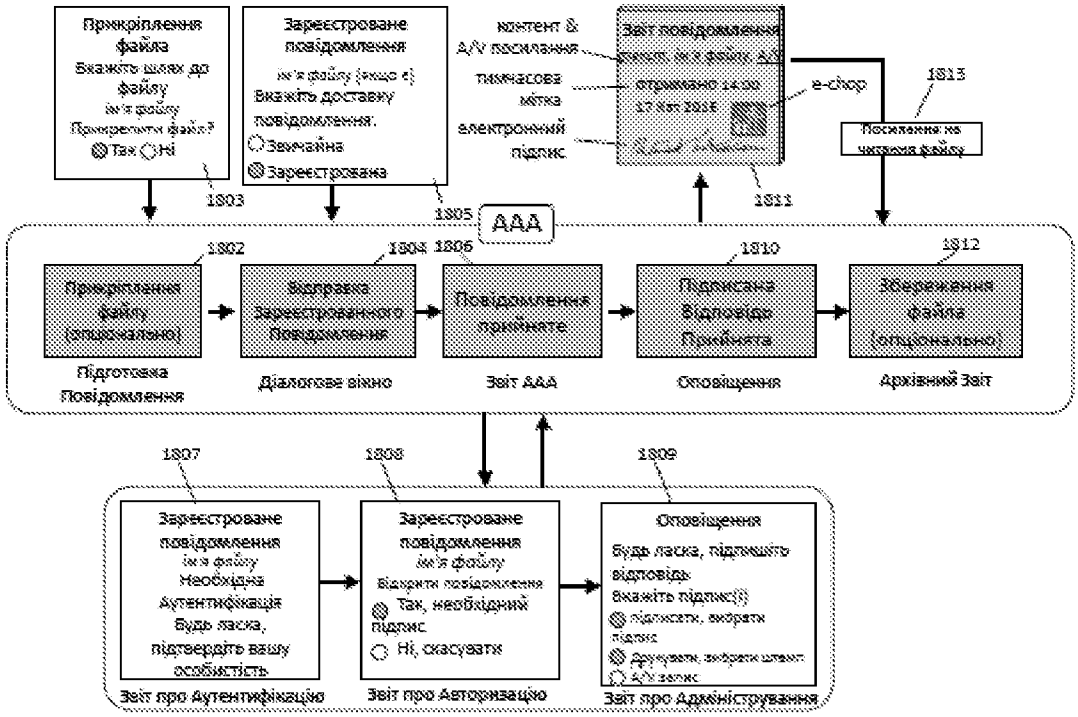


Рис. 103

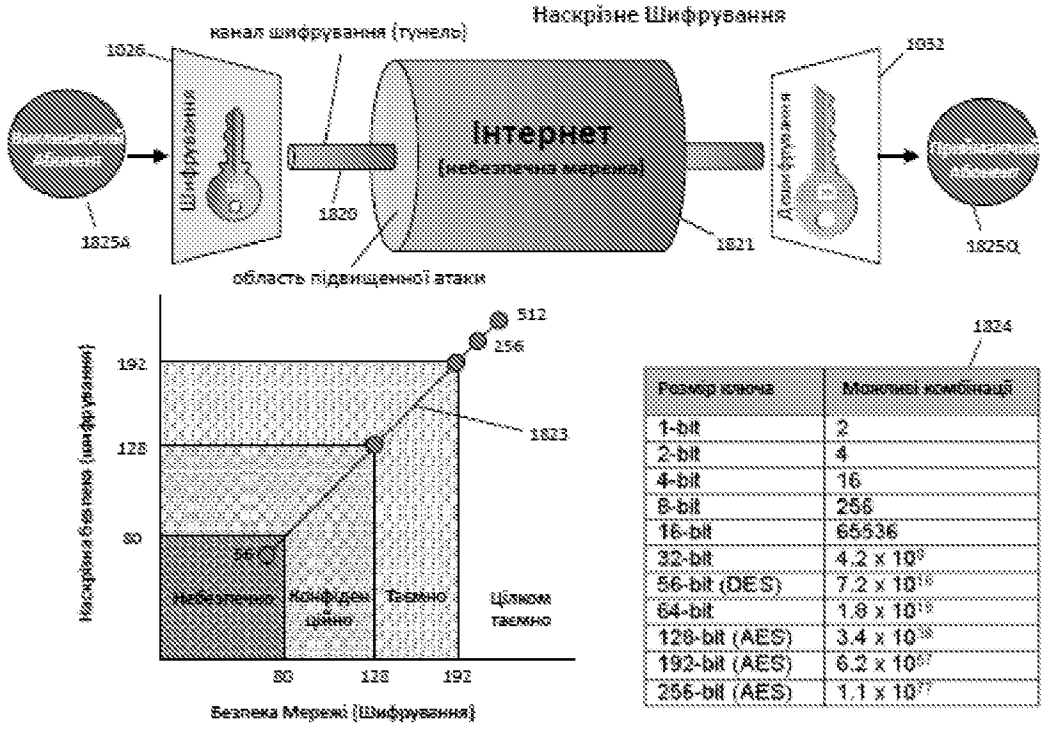


Рис. 104A

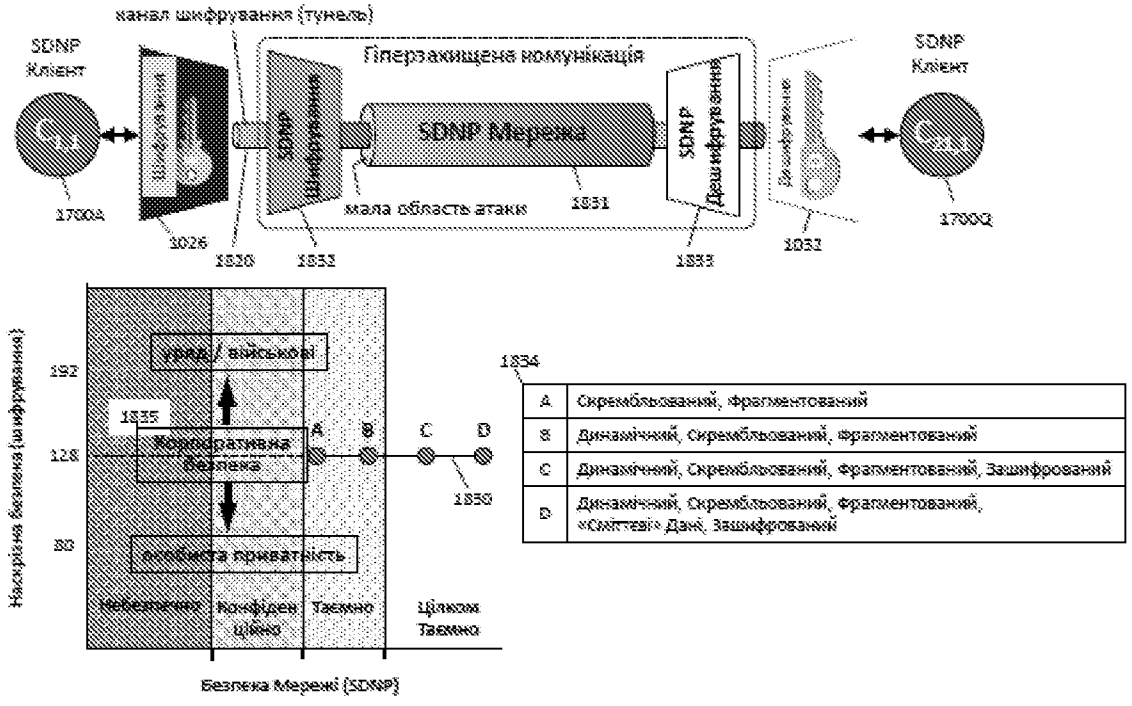


Рис. 104B

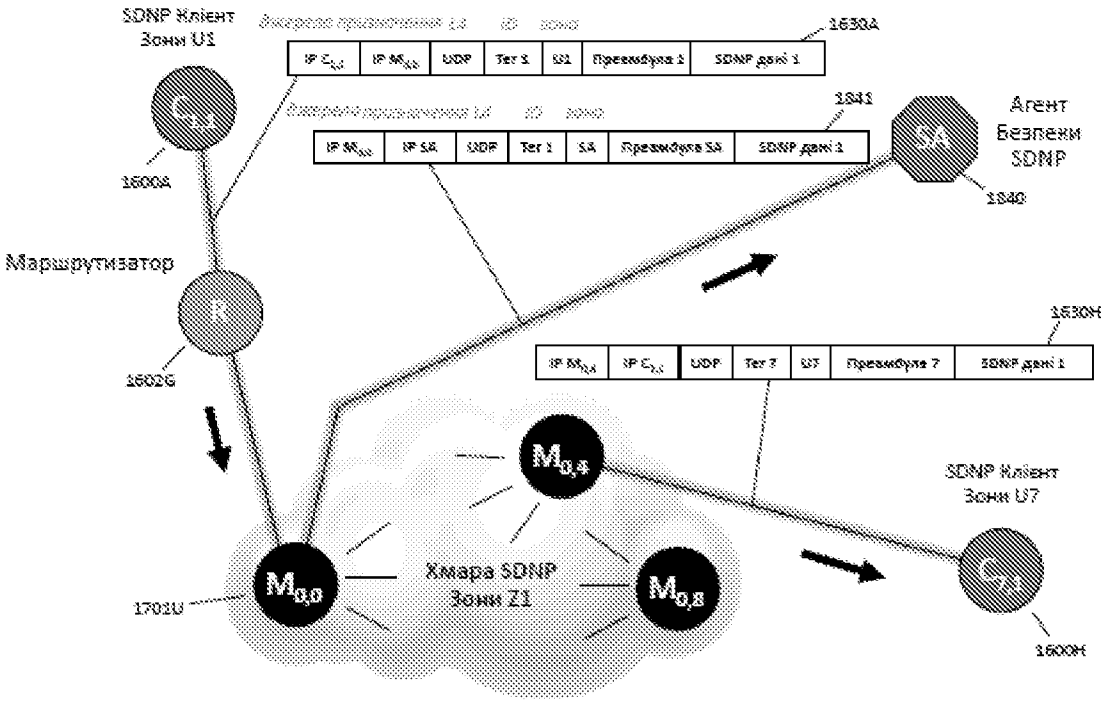


Рис. 105A

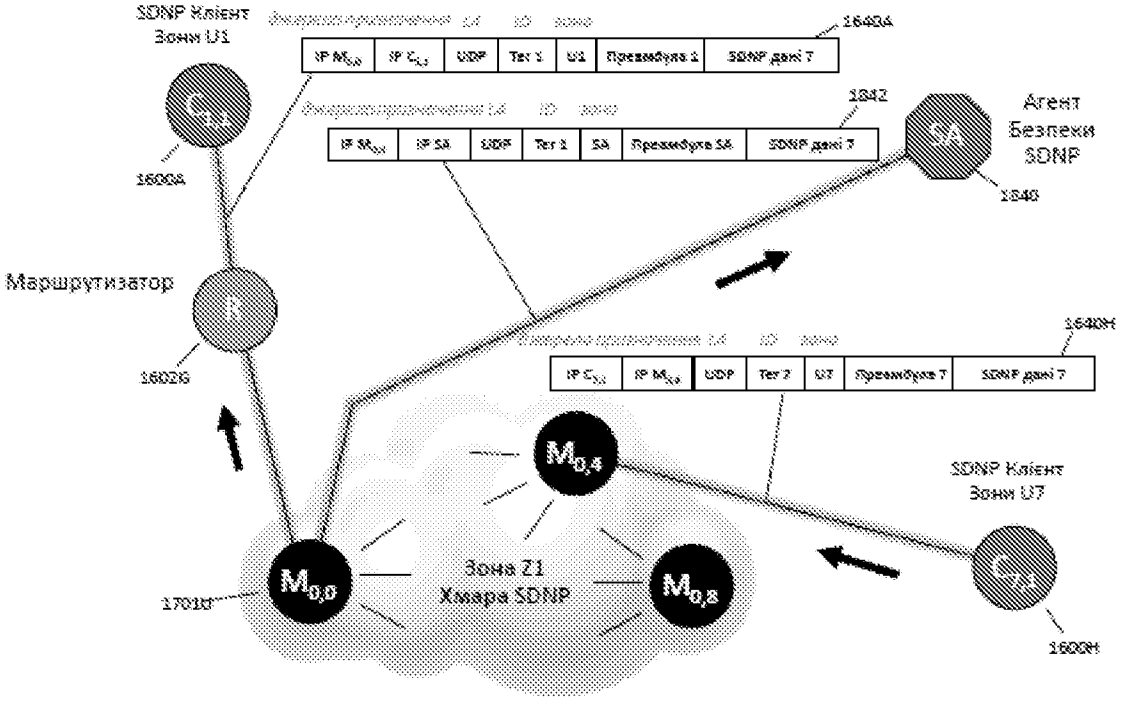


Рис. 105B

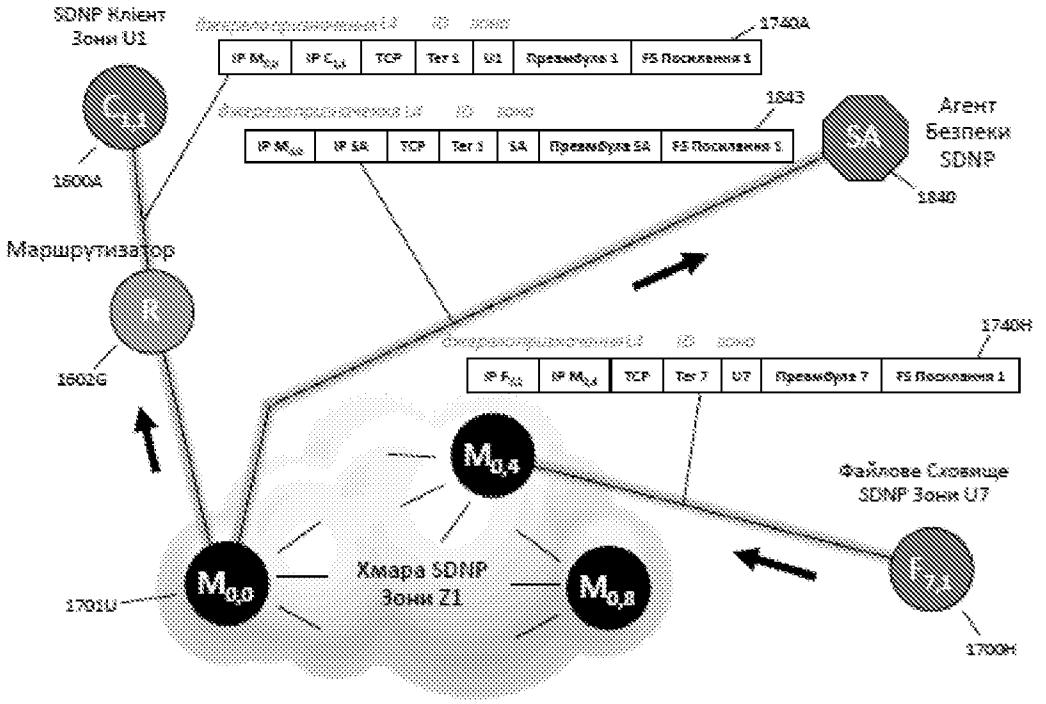


Рис. 106

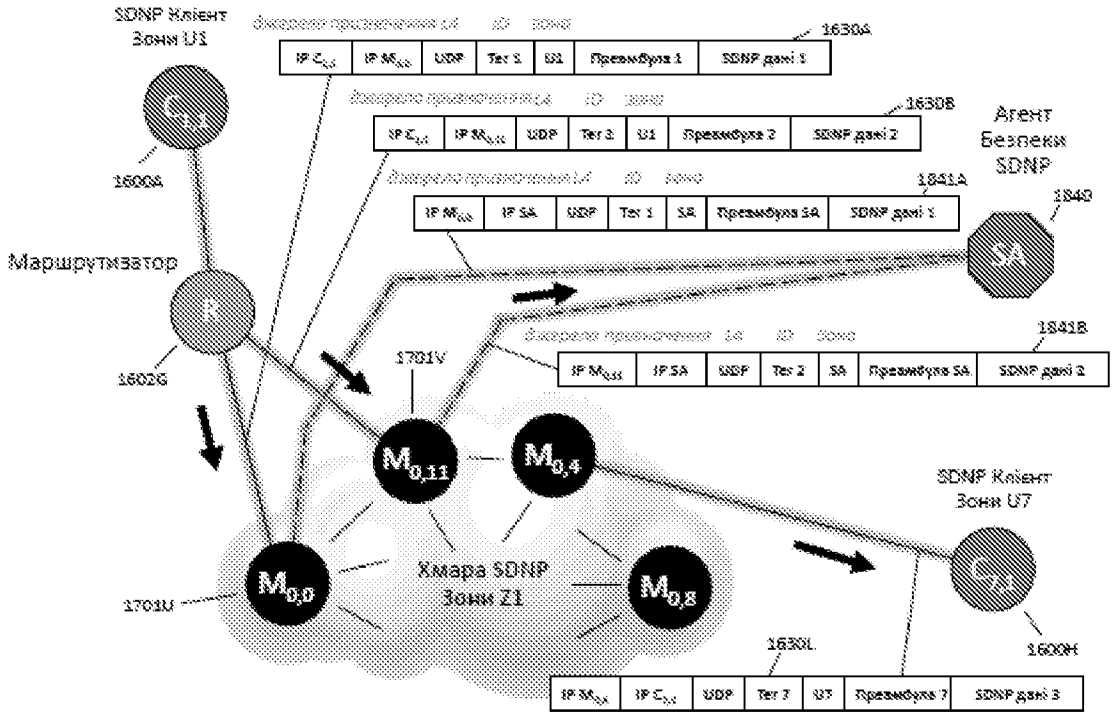


Рис. 107

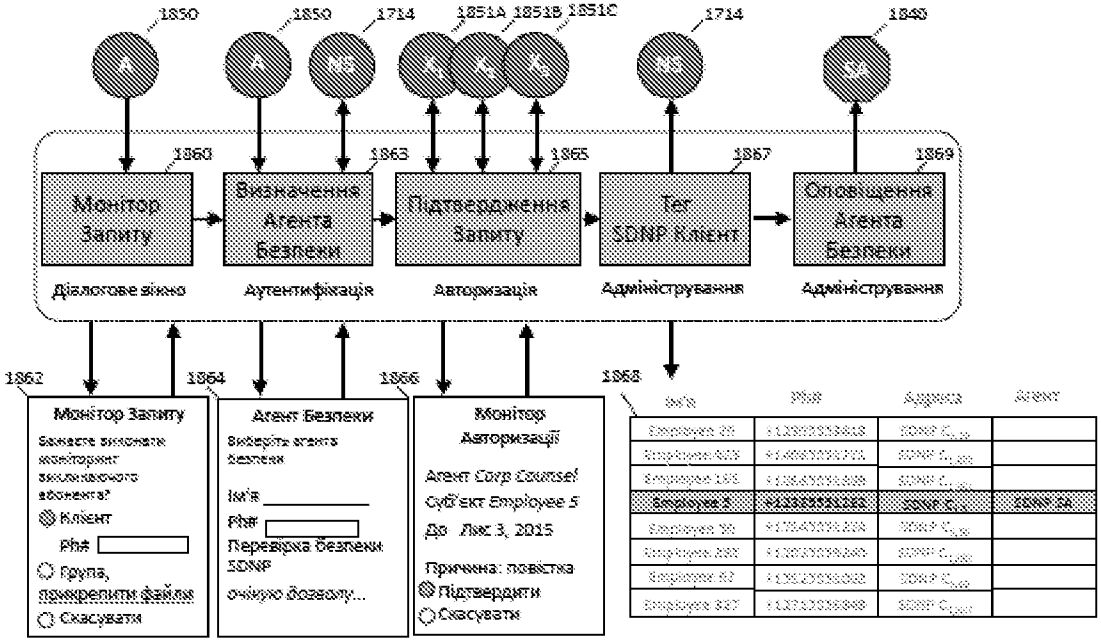


Рис. 108

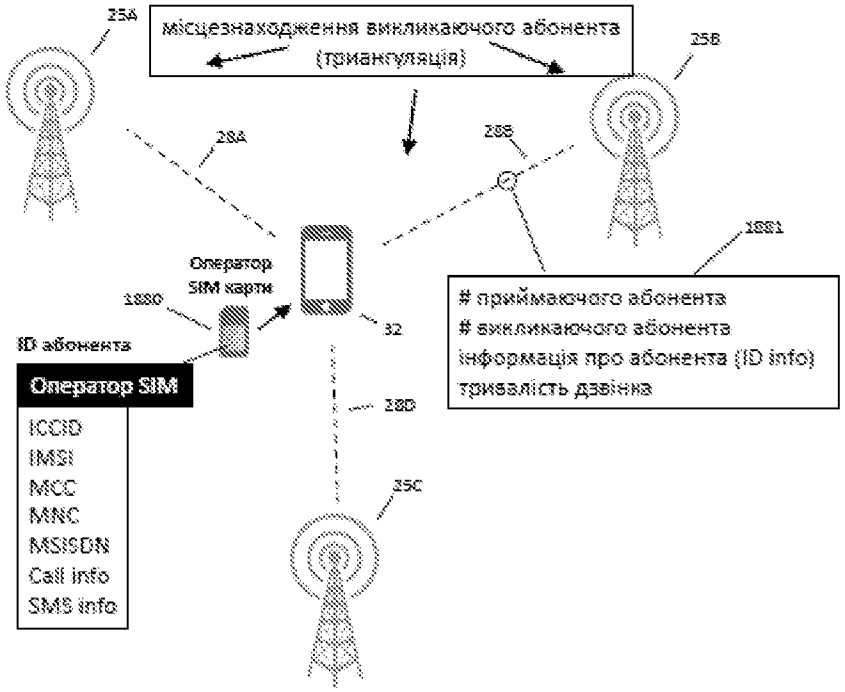


Рис. 109

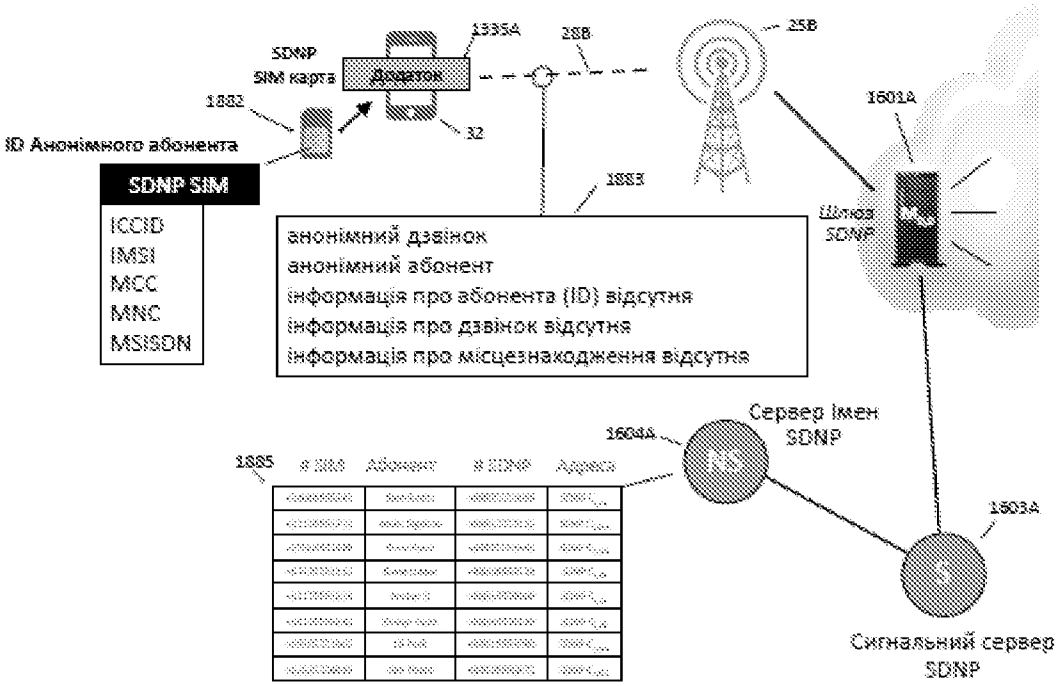


Рис. 110

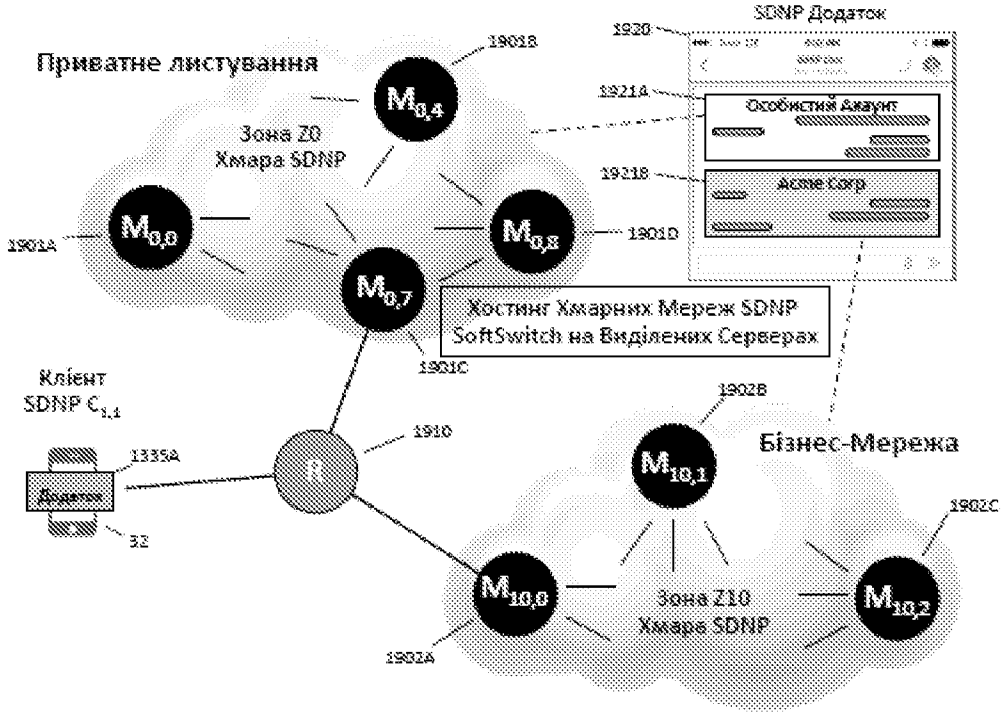


Рис. 111

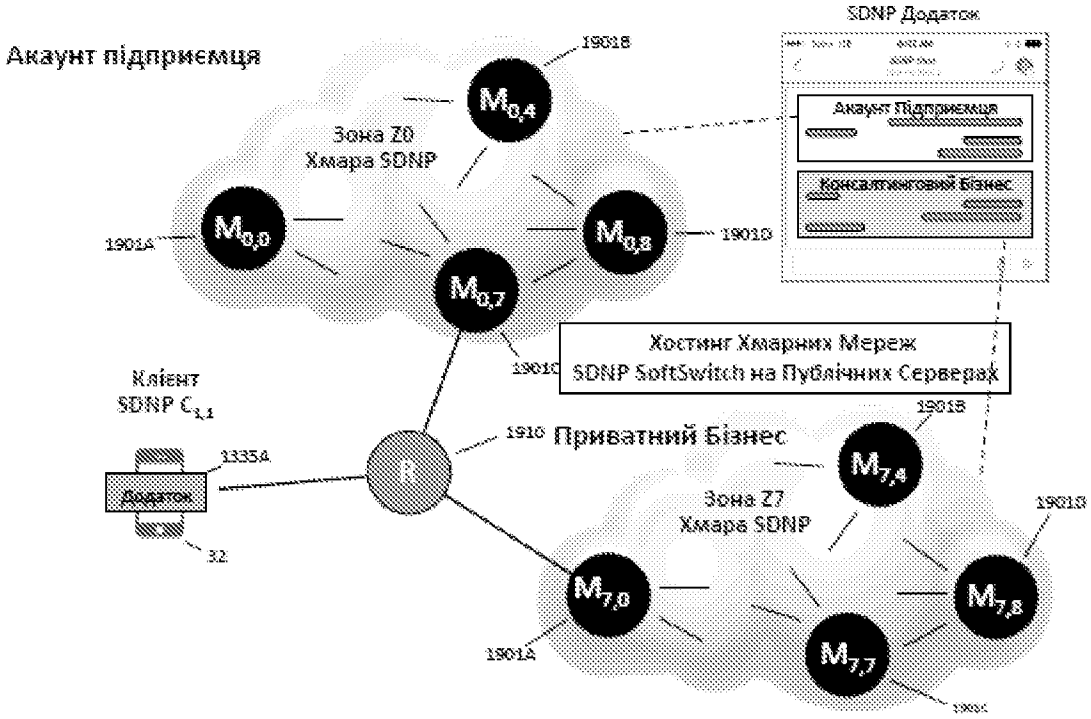


Рис. 112

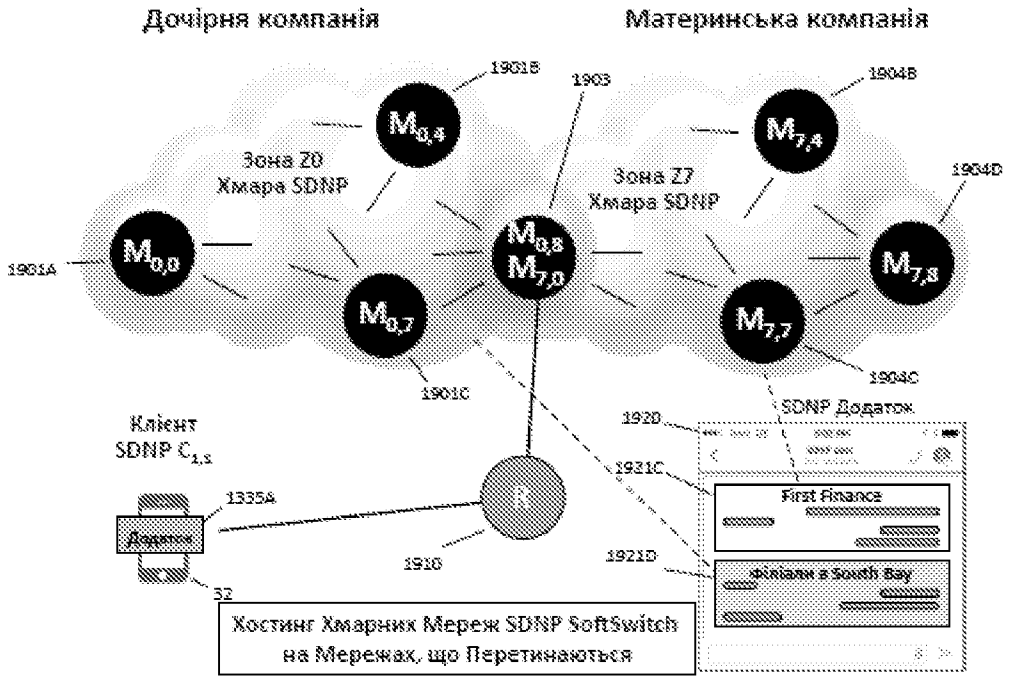


Рис. 113

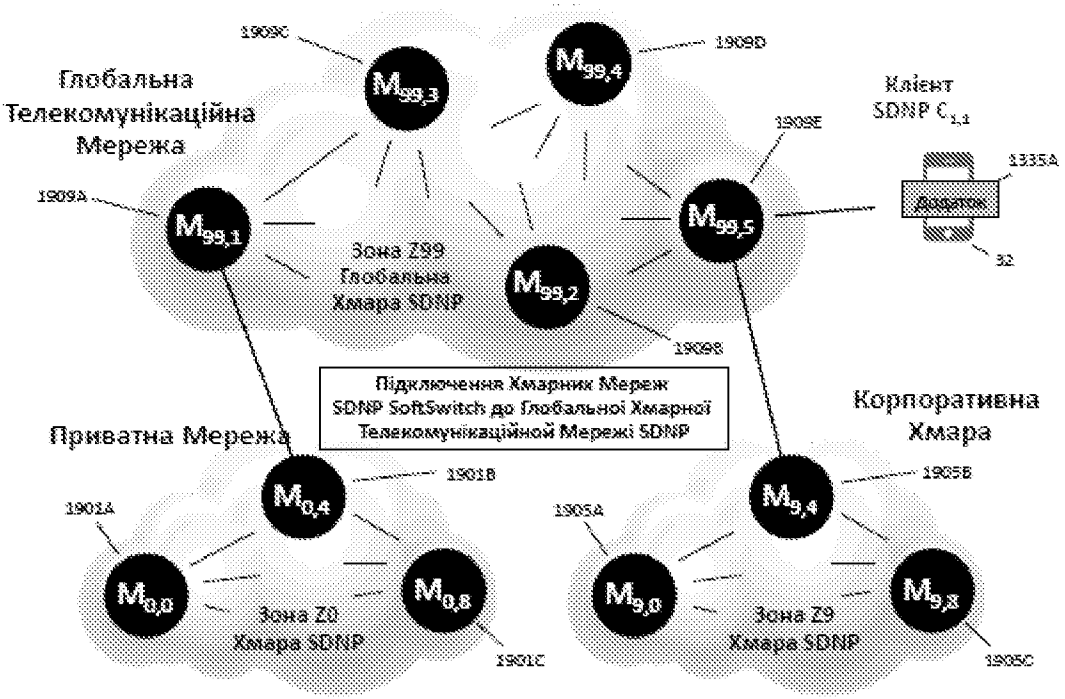


Рис. 114

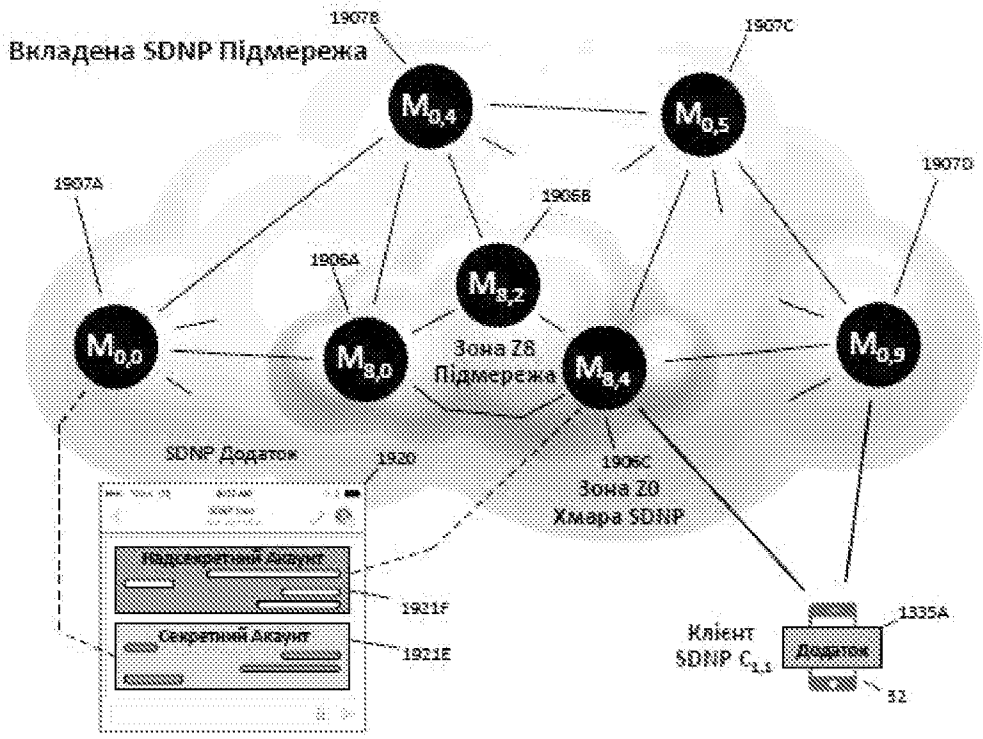


Рис. 115

Комп'ютерна верстка В. Мацело

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601