(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년11월09일
(11) 등록번호 10-2465085
(24) 등록일자 2022년11월04일

(51) 국제특허분류(Int. Cl.)
*H04L 9/40* (2022.01) *H04L 45/24* (2022.01)
*H04L 9/14* (2006.01)
(52) CPC특허분류
*H04L 63/0428* (2013.01)
*H04L 45/24* (2022.05)
(21) 출원번호 10-2021-7035497(분할)
(22) 출원일자(국제) 2018년04월02일
심사청구일자 2021년10월29일
(85) 번역문제출일자 2021년10월29일
(65) 공개번호 10-2021-0135000
(43) 공개일자 2021년11월11일
(62) 원출원 특허 10-2019-7032459
원출원일자(국제) 2018년04월02일
심사청구일자 2021년03월23일
(86) 국제출원번호 PCT/US2018/025695
(87) 국제공개번호 WO 2018/187212
국제공개일자 2018년10월11일
(30) 우선권주장
62/480,696 2017년04월03일 미국(US)
(56) 선행기술조사문헌
US20110194692 A1
US20140201256 A1
US20160219024 A1
WO2016003525 A2

(73) 특허권자
**리스태트 리미티드**
벨리즈 벨모판 마운틴뷰 블러바드 가든 시티 플라자 스위트 5
(72) 발명자
**윌리엄스 리차드 케이.**
미국 캘리포니아주 쿠퍼티노 노르위치 애비뉴 10292
**버쥔 이브겐**
우크라이나 키에브 스테파나 반데리 애비뉴 20비
**호럽 올렉산드르**
우크라이나 키에브 스테파나 반데리 애비뉴 20비
(74) 대리인
**특허법인명신**

전체 청구항 수 : 총 30 항 심사관 : 홍기완

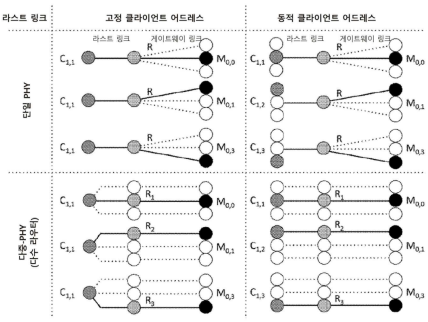
(54) 발명의 명칭 **안전한 라스트 마일 통신을 위한 방법 및 장치**

## (57) 요 약

휴대폰 또는 랩탑과 같은 클라이언트 디바이스와 네트워크 또는 미디어 노드의 클라우드 사이의 통신의 콘텐츠를 은폐하기 위한 다양한 기술이 개시된다. 그러한 기술 중에서, 통신 내의 데이터 패킷을 클라우드 내의 상이한 게이트웨이 노드들로 라우팅하고, 패킷을 이더넷 케이블 또는 WiFi 채널과 같은 상이한 물리적 미디어들을 통해서

(뒷면에 계속)

*대 표 도* - 도52c



송신하고, 상이한 소스 어드레스를 제공함으로써 패킷을 은폐한다. 또한, 컨퍼런스 콜 내의 특정 참가자를 묵음화하기 위한 기술 및 데이터 파일을 저장하는 높은 보안적 방법이 개시된다.

(52) CPC특허분류
***H04L 63/0421*** (2013.01)
***H04L 63/0464*** (2013.01)
***H04L 63/0471*** (2013.01)
***H04L 63/0478*** (2013.01)
***H04L 69/14*** (2022.05)
***H04L 9/14*** (2022.08)
*H04L 2209/42* (2013.01)
*H04L 2209/76* (2013.01)

# 명 세 서

## 청구범위

### 청구항 1

클라이언트 디바이스와 보안 동적 통신 네트워크 및 프로토콜(SDNP) 미디어 노드들의 클라우드를 포함하는 통신 네트워크로서, 상기 SDNP 미디어 노드들의 클라우드는 SDNP 게이트웨이 노드를 포함하고, 상기 클라이언트 디바이스는 SDNP 은폐 프로세스에 의해 은폐된 데이터를 해석할 수 있는 애플리케이션 프로그램을 포함하고, 상기 SDNP 은폐 프로세스는 암호화, 스크램블링, 분할, 및 정크 데이터의 삽입 중 하나 이상을 포함하며, 상기 통신 네트워크는 추가로:

상기 클라이언트 디바이스와 상기 SDNP 게이트웨이 노드 사이의 라스트 마일 연결을 횡단하는, 제1 디지털 페이로드를 포함하는 제1 디지털 데이터 패킷;

상기 SDNP 미디어 노드들의 클라우드를 동시에 횡단하는, 제2 디지털 페이로드를 포함하는 제2 디지털 데이터 패킷;

을 포함하며,

여기서 상기 제1 및 제2 디지털 데이터 패킷 각각의 데이터는 SDNP 은폐 프로세스를 사용하여 은폐되고, 여기서 상기 제1 및 제2 디지털 데이터 패킷에 대해 수행되는 상기 SDNP 은폐 프로세스는 각각 상이한 알고리즘, 시퀀스, 또는 보안 자격 증명을 포함하는, 통신 네트워크.

### 청구항 2

제1항에 있어서,

상기 제1 디지털 데이터 패킷에 대해 사용되는 상기 SDNP 은폐 프로세스는 라스트 마일 보안 구역과 연관된 보안 자격 증명을 사용하고, 라스트 마일 보안 구역과 연관된 상기 보안 자격 증명은 상기 제2 디지털 데이터 패킷이 존재하는 보안 구역과 연관된 보안 자격 증명과 상이한, 통신 네트워크.

### 청구항 3

제1항에 있어서,

상기 제1 및 제2 디지털 데이터 패킷 각각에 대해 사용되는 상기 은폐 프로세스는 각각 상태에 의해 결정되는, 통신 네트워크.

### 청구항 4

제3항에 있어서,

상기 상태는 상기 제1 및 제2 디지털 데이터 패킷 각각이 각각 생성된 시간을 포함하는, 통신 네트워크.

### 청구항 5

제3항에 있어서,

상기 제1 디지털 데이터 패킷은 상기 클라이언트 디바이스에서 상기 SDNP 게이트웨이 노드로의 방향으로 상기 라스트 마일 연결을 횡단하고, 상기 통신 네트워크는 상기 SDNP 게이트웨이 노드에서 상기 클라이언트 디바이스로의 방향으로 상기 라스트 마일 연결을 횡단하는 제3 디지털 데이터 패킷을 포함하며, 여기서 상기 제1 디지털 데이터 패킷에 대한 상기 은폐 프로세스에 사용되는 상기 상태는 상기 제3 디지털 데이터 패킷에 대한 상기 은폐 프로세스에 사용되는 상태와 상이한, 통신 네트워크.

### 청구항 6

제1항에 있어서,

상기 제1 디지털 데이터 패킷의 상기 데이터는 비디오, 음성, 이미지, 텍스트, 또는 데이터 파일, 또는 이들의

혼합을 포함하는, 통신 네트워크.

**청구항 7**

제1항에 있어서,

상기 제1 디지털 데이터 패킷은 센서 또는 변환기로부터의 데이터를 포함하는, 통신 네트워크.

**청구항 8**

제1항에 있어서,

상기 제2 디지털 데이터 패킷은 상기 SDNP 게이트웨이 노드에서 상기 클라우드의 다른 SDNP 노드로 횡단하는, 통신 네트워크.

**청구항 9**

제8항에 있어서,

상기 제1 디지털 데이터 패킷은 상기 SDNP 게이트웨이 미디어 노드가 상기 제1 디지털 데이터 패킷을 유효한 수신 데이터 패킷으로 식별할 수 있도록 하는 헤더 데이터를 포함하는, 통신 네트워크.

**청구항 10**

제1항에 있어서,

제2 클라이언트 디바이스, 제2 SDNP 게이트웨이 노드, 및 상기 제2 클라이언트 디바이스와 상기 제2 SDNP 게이트웨이 노드 사이의 라스트 마일 연결을 횡단하는 제3 디지털 데이터 패킷을 포함하고, 여기서 상기 제3 디지털 데이터 패킷의 데이터는 상기 제1 디지털 데이터 패킷의 데이터를 은폐하는 데 사용되는 상기 SDNP 은폐 프로세스의 알고리즘 또는 보안 자격 증명과 다른 알고리즘 또는 보안 자격 증명을 사용하는 SDNP 은폐 프로세스로 은폐되는, 통신 네트워크.

**청구항 11**

제10항에 있어서,

상기 제2 클라이언트 디바이스는 상기 제1 디지털 데이터 패킷의 최종 목적지이고, 여기서 상기 제1 디지털 데이터 패킷은 SDNP 은폐 프로세스를 사용하여 은폐된 상기 제2 클라이언트 디바이스의 어드레스를 포함하는, 통신 네트워크.

**청구항 12**

제10항에 있어서,

상기 제2 클라이언트 디바이스는 상기 제1 디지털 데이터 패킷의 최종 목적지이고, 상기 제1 디지털 데이터 패킷은 상기 제2 클라이언트 디바이스의 어드레스를 포함하지 않는, 통신 네트워크.

**청구항 13**

제1항에 있어서,

상기 라스트 마일 연결은 저궤도 위성, 정지궤도 위성, 셀룰러 통신 네트워크, 및 마이크로파 무선 통신을 포함하는 상이한 물리적 매체를 포함하는, 통신 네트워크.

**청구항 14**

클라이언트 디바이스 및 보안 동적 통신 네트워크 및 프로토콜(SDNP) 미디어 노드들의 클라우드를 포함하는 통신 네트워크로서, 상기 SDNP 미디어 노드들의 클라우드는 SDNP 게이트웨이 노드를 포함하고, 상기 통신 네트워크는 추가로:

하나 이상의 중간 데이터 라우터를 포함하는, 상기 클라이언트 디바이스와 상기 SDNP 게이트웨이 노드 사이의 라스트 마일 연결;

상기 하나 이상의 중간 라우터와 상기 SDNP 게이트웨이 노드 사이의 상기 라스트 마일 연결의 일부를 횡단하는 제1 디지털 페이로드를 포함하는 제1 디지털 데이터 패킷; 및

상기 SDNP 미디어 노드들의 클라우드를 동시에 횡단하는 제2 디지털 페이로드를 포함하는 제2 디지털 데이터 패킷;

을 포함하며,

상기 제1 및 제2 디지털 데이터 패킷 각각의 데이터는 SDNP 은폐 프로세스를 사용하여 은폐되며, 상기 SDNP 은폐 프로세스는 암호화, 스크램블링, 분할 및 정크 데이터의 삽입 중 하나 이상을 포함하며, 상기 제1 및 제2 데이터 패킷에 대해 각각 수행되는 상기 SDNP 은폐 프로세스는 상이한 알고리즘, 시퀀스 또는 보안 자격 증명을 포함하는, 통신 네트워크.

**청구항 15**

제14항에 있어서,

상기 하나 이상의 중간 데이터 라우터는 WiFi 라우터, 네트워크 라우터, 이더넷 라우터, 케이블 네트워크, 또는 셀룰러 네트워크를 포함하는, 통신 네트워크.

**청구항 16**

제14항에 있어서,

상기 라스트 마일 연결은 무선 부분 및 유선 부분을 포함하는, 통신 네트워크.

**청구항 17**

제16항에 있어서,

상기 하나 이상의 중간 라우터는 SDNP 펌웨어를 포함하고, 이에 의해 상기 라우터가 원격 SDNP 게이트웨이 노드로서 기능할 수 있게 하는, 통신 네트워크.

**청구항 18**

제17항에 있어서,

제3 디지털 페이로드를 포함하는 제3 디지털 데이터 패킷을 포함하고, 상기 제3 디지털 데이터 패킷은 상기 클라이언트 디바이스와 상기 하나 이상의 중간 라우터 사이의 라스트 마일 연결의 라스트 링크 부분을 횡단하며, 상기 제3 디지털 페이로드는 암호화되지만 SDNP 은폐 프로세스를 사용하여 은폐되지 않은 데이터를 포함하는, 통신 네트워크.

**청구항 19**

제18항에 있어서,

상기 클라이언트 디바이스 및 상기 적어도 하나의 중간 라우터는 상기 클라이언트 디바이스 및 상기 적어도 하나의 중간 라우터가 제3 디지털 페이로드의 데이터를 암호화 및 복호화할 수 있도록 하기 위해 동일한 암호화 키를 포함하는, 통신 네트워크.

**청구항 20**

제19항에 있어서,

상기 제3 디지털 페이로드는 보안 유선 근거리통신망(LAN: Local Area Network) 또는 WiFi 보호 액세스(WPA: WiFi Protected Access) 프로토콜에 따라 암호화되는, 통신 네트워크.

**청구항 21**

제14항에 있어서,

상기 라스트 마일은 SDNP 펌웨어를 실행하고 유선 또는 무선 SDNP 브릿지를 형성하는 2개의 라우터를 포함하는,

통신 네트워크.

**청구항 22**

제21항에 있어서,

상기 SDNP 브릿지는 이더넷 케이블 또는 WiFi 데이터 링크를 포함하는, 통신 네트워크.

**청구항 23**

제21항에 있어서,

상기 SDNP 브릿지는 동축 케이블 또는 광섬유를 사용하는 케이블 유선 연결을 포함하는, 통신 네트워크.

**청구항 24**

제21항에 있어서,

상기 SDNP 브릿지는 셀룰러 통신 네트워크를 포함하는, 통신 네트워크.

**청구항 25**

제21항에 있어서,

상기 SDNP 브릿지는 차량들 간의 무선 통신 네트워크를 포함하는, 통신 네트워크.

**청구항 26**

제21항에 있어서,

상기 SDNP 브릿지는 마이크로파 위성 링크를 포함하는, 통신 네트워크.

**청구항 27**

제26항에 있어서,

SDNP 소프트웨어로 활성화되고 위성 통신에 의해 상기 SDNP 미디어 노드들의 클라우드와 연결되는 추가의 클라이언트 디바이스를 포함하는, 통신 네트워크.

**청구항 28**

제27항에 있어서,

상기 추가의 클라이언트 디바이스는 선박, 비행기 또는 기차를 포함하는, 통신 네트워크.

**청구항 29**

제28항에 있어서,

상기 추가의 클라이언트 디바이스 중 적어도 하나는 다수의 사람과 디지털 데이터 패킷을 교환하기 위한 근거리 통신망의 형태인, 통신 네트워크.

**청구항 30**

제25항에 있어서,

상기 클라이언트 디바이스는 다수의 사람과 디지털 데이터 패킷을 교환하기 위한 근거리 통신망의 형태인, 통신 네트워크.

## *발명의 설명*

### *기 술 분 야*

[0001] **관련 출원에 대한 상호 참조**

[0002] 본원은 2017년 4월 3일자로 출원된 미국 가출원 제62/480,696호의 우선권을 주장하고, 2015년 1월 26일자로 출원된 미국 가출원 제62/107,650호의 우선권을 다시 주장하는, 2015년 7월 20일자로 출원된 "Secure Dynamic Communication Network And Protocol"이라는 명칭의 미국 출원 제14/803,869호의 부분-계속 출원이다.

[0003] 전술한 출원의 각각의 전체가 본원에서 참조로 포함된다.

[0004] 본 발명은 장치와 네트워크 또는 클라우드에 대한 게이트웨이 사이의 하이퍼보안 "라스트 마일" 통신을 촉진하기 위한 방법 및 장치에 관한 것이다.

## *배 경 기 술*

[0005] 통신의 개선 수단은 인류의 초기 발단으로부터 문명의 진전에 연료를 공급했다. 도보 또는 말을 타고 여행하는 배달자 및 메신저의 사용으로부터, 기차, 트럭, 및 비행기에 의한 우편 전달을 통해, 전보 및 전신, 전화, 라디오, 텔레비전, 컴퓨터, 휴대폰, 인터넷, 이메일 및 월드 와이드 웹의 출현까지, 최근에는 소셜 미디어, 인터넷 전화, 기계-대-기계(M2M: machine-to-machine) 연결성, 사물 인터넷(IoT: Internet of Things), 및 만물 인터넷(IoE: Internet of Everything)을 통해 더 많은 정보를 얻을 수 있다. 그리고 만물 인터넷의 통신은 항상 시대의 최신 기술의 개발에 주도적 역할을 했다. 사용된 각각의 새로운 통신 기술에 따라, 연결된 사람수와 정보가 전송되는 비율도 증가되었다.

[0006] 이러한 추세의 영향은 역사 상 그 어느 때보다도 사람들이 더 많이 연결되어, 사람들은 그들이 접촉하고자 의도한 사람에게만 그 사적, 개인, 가족, 및 금융 정보를 안전하고 신뢰성 있게 전달하기 위해 통신 기술을 신뢰하고 의존하고 있다. 지식과 정보는 이제 수백만 명의 사람들에게 수 초 만에 배포될 수 있으며, 친구와 가족은 버튼을 누르는 것만큼이나 일상적으로 세계 곳곳에서 중간에 서로 접촉할 수 있다. "세상은 매우 작은 장소가 되었다"라고 종종 말한다.

[0007] 이러한 진보는 모든 사람에게 대단히 유익하지만, 기술에 대한 우리의 의존도가 높다는 부정적인 결과도 있다. 예를 들어 지진이나 악천후 중에 통신 시스템이 수행을 실패하였을 때, 일시적일지라도 "언플러그드(unplugged)"에 의해 사람들이 혼란스럽거나 당황하게 된다는 것은 놀라운 일이 아니다. 따라서 통신 시스템 또는 미디어의 서비스 품질(QoS: quality of service)는 통신 네트워크의 성능의 중요한 측정치이다. 사람들의 마음의 평화, 금융 자산, 신원, 심지어 그들의 삶까지도 믿을 수 있고 안전한 통신에 의존한다.

[0008] 통신 네트워크의 다른 주요 고려 사항은 프라이버시, 안전, 및 보안을 이를 사용하는 클라이언트에게 보장하는 능력이다. 통신 기술이 진화함에 따라, 장난을 유발하고, 시스템을 혼란시키며, 돈을 훔치거나, 우연히 또는 악의적으로 타인에게 해를 입히고자 의도하는 범죄자 및 "해커(hacker)"의 정교함도 진화했다. 신용카드 사기, 도난당한 암호, 신분 도용, 및 기밀 정보, 개인 사진, 파일, 이메일, 텍스트 메시지, 개인적인 트윗의 무단 공개(당황스럽게 하거나 피해자를 협박하는 도용)는 단지 현대 사이버-범죄의 몇 개의 예에 불과하다.

[0009] 오늘날의 개방형 통신 네트워크에서 보안 문제의 유행 비율을 밝히기 위해, 본 특허출원 당시의 프라이버시 침해 및 사이버 범죄의 주목할 만한 사례는 다음과 같다(시간 순서대로 나열).

[0010] * "표적: 도난당한 정보가 최소한 7천만 명에 이른다". CNBC, 2014년 1월 10일

[0011] * "해커가 스마트 프릿지(fridge)를 만들고 TV가 악의적인 이메일을 보냈다". BGR(www.bgr.com), 2014년 1월 20일

[0012] * "해킹된 서모스탯으로 네스트 구글 프라이버시 행 재개(Nest Google Privacy Row Resumes)", 슬래시 기어(Slash Gear(www.slashgear.com)), 2014년 1월 24일

[0013] * "계정 도용은 퀘스천 라인(Question Line)에 라인의 데이터 보안을 요구한다. 무료 통화 및 메시징 애플리케이션인 라인(Line)은 최근 데이터 보안 위반에 휩싸였다. 상기 애플리케이션은 계정 사용자가 아닌 다른 사람에 의해 불법적으로 액세스한 수백 개의 사용자 계정을 보았다". 닛케이 아시안 리뷰(Nikkei Asian Review), 2014년 7월 2일

[0014] * "NSA 데이터 스윕(NSA Data Sweep)에 포착된 보통의 미국인이 클레임을 보고하였다". 에이피(AP), 2014년 7월 6일

[0015] * "스마트 LED 전구가 WiFi 패스워드를 누설한다." BBC 뉴스, 2014년 7월 8일

[0016] * "6명의 사람들이 스터브허브 스캠(StubHub Scam)에 프라임 티켓(prime ticket)을 부과했다. 스터브허브는 도

난당한 패스워드 및 신용카드 번호로 팝뮤직 콘서트와 양키스 게임을 위해 수천 장의 티켓을 사고파는 해커들의 표적이 되었다고 뉴욕 당국은 말했다". 블룸버그(Bloomberg), 2014년 7월 24일

[0017] * "연구는 해킹에 매우 민감한 '사물 인터넷'을 나타내고 있다. "인터내셔널 비즈니스 타임즈(www.ibtimes.com), 2014년 8월 4일

[0018] * "러시아 해커는 10억 개의 인터넷 패스워드를 모았다". 뉴욕 타임즈 2014년 8월 5일

[0019] * "미국 비밀 정부 결정판(U.S. Secrets, Government Concludes)을 나타내는 뉴 리커(New Leaker)" CNN, 2014년 8월 6일

[0020] * "15초의 해커 루트 구글의 네스트 서모 스탯", 더 인콰이어러(The Enquirer)(www,theinquirer.net), 2014년 8월 11일

[0021] * "표적을 타격하는 동일한 맬웨어에 의해 해킹된 유제품 여왕", 크리스티앙 사이언스 모니터(Christian Science Monitor), 2014년 8월 29일

[0022] * "누드 사진 유출의 유명인 희생자- 아이클라우드(iCloud) 계정의 보안 취약성", CBS 뉴스, 2014년 9월 1일

[0023] * "홈 디포(Home Depot)는 신용카드 분쟁의 최신 표적일 수 있다. 홈 디포 분쟁은 표적보다 더 클 수 있다.(3주에 걸쳐 도난당한 40M 카드)", 포춘(Fortune), 2014년 9월 2일

[0024] * "신비한 가짜 핸드폰 타워가 미국 전역에 걸쳐 전화를 가로채고 있다. "비즈니스 인사이더(Business Insider), 2014년 9월 3일

[0025] * "해킹 공격, 은행에서 소매업으로, 사이버 전쟁의 징후?" 야후 파이낸스(Yahoo Finance), 2014년 9월 3일

[0026] * "홈 디포는 미국과 캐나다 상점에서 해킹당한 지불 시스템을 확인한다". 폭스 뉴스(Fox News), 2014년 9월 9일

[0027] * "야후는 감시에 대해 미국 정부와 다투고 있다. "CBS/AP, 2014년 9월 11일

[0028] * "당신의 의료 기록은 해커에게 당신의 신용카드보다 더 가치 있다. "로이터 통신, 2014년 9월 24일

[0029] * "레드 얼럿(Red Alert): HTTP S가 해킹당했다. SSL/TLS(BEAST) 공격에 대한 브라우저 활용은, 수억 명의 사람들이 매일 의존하는 브라우저 연결을 손상시키기 때문에 최악의 해킹에 속할 것이다". 인포월드(InfoWorld), 2014년 9월 26일

[0030] * "소니 사이버 공격, 첫 번째 골칫거리, 신속하게 화염에 빠져 들었다". 뉴욕 타임즈, 2014년 12월 30일

[0031] 사이버 범죄, 보안 침해, 신분 절도, 및 프라이버시 침해가 점증하고 있는 것처럼 보이는 가운데, "이러한 모든 사이버-공격은 어떻게 가능하며, 이를 막기 위해 무엇이 실행될 수 있을까?"라는 질문이 제기된다. 사회가 더 높은 프라이버시 및 보안을 추구하는 동시에, 소비자 또한 더 나은 연결성, 더 저렴한 고품질 통신, 및 금융 거래 수행 시의 더욱 편리함을 원한다.

[0032] 현대의 통신 네트워크, 데이터 저장소 및 연결된 디바이스의 성능 제한과 취약점을 이해하기 위해, 오늘날의 전자, 라디오, 및 광 통신이 파일, 이메일, 텍스트, 오디오, 및 비디오 영상을 포함하는 데이터를 어떻게 동작, 전송, 및 저장하는지를 이해하는 것이 제일 중요하다.

[0033] **회선 교환형 전화망 동작**

[0034] 전자 통신은 와이어, 라디오, 마이크로파 또는 광섬유 링크의 네트워크 내에 연결된 다양한 하드웨어 구성요소 또는 디바이스를 포함하고 있다. 정보는 이 네트워크를 통해 전기 또는 전자기 에너지를 전송하고, 또한 데이터 스트림 내에 정보 "콘텐츠"를 매립 또는 인코딩하기 위해 다양한 방법을 사용함으로써, 하나의 디바이스로부터 다른 디바이스로 전송된다. 이론적으로, 물리학의 법칙은 이러한 네트워크의 최대 데이터 전송률을 빛의 속도로 설정하지만, 그러나 대부분의 경우에 데이터 인코딩, 라우팅 및 트래픽 제어, 신호 대 노이즈 품질, 및 전기, 자기 및 광학 노이즈, 불필요한 기생의 극복에 대한 실질적인 제한 사항은 통신 네트워크의 기능을 이상적인 성능의 일부로 제한하는 정보 흐름을 방해하거나 억제한다.

[0035] 역사적으로, 전자 데이터 통신은 전기적으로 연결된 2개 또는 그 이상의 디바이스 사이 또는 이들 사이에서 통신 "회로"를 형성하는 전용 "하드와이어형(hardwired)" 전기 연결을 사용하여 먼저 달성되었다. 전신의 경우에 있어서, 직류(DC) 수동으로 전기 회로를 만들고 끊기 위해, 기계적 스위치가 사용되었으며, 솔레노이드를 자화

시키고 다시 금속 레버를 움직여, 청취 디바이스 또는 "릴레이"가 발신자가 스위치를 누른 동일한 패턴으로 동일한 위치에서 클릭되게 한다. 그 후, 정보를 펄스 스트림으로 인코딩하기 위해, 상기 발신자는 합의된 언어, 즉 모스 부호(Morse code)를 사용하였다. 청취자는 마찬가지로 점(dot)과 대시(dash)라고 불리는 일련의 길고 짧은 펄스인 모스 부호를 이해하여, 메시지를 해석할 필요가 있다.

[0036] 나중에, 알렉산더 그레이엄 벨(Alexander Graham Bell)은 전기적 연결을 통해 소리를 전달하기 위해, 이제 교류 전류(AC)로 언급되는 "기복 전류(undulating current)"의 개념을 사용하여 최초의 전화기를 개발하였다. 전화 네트워크는 전기 회로에 의해 연결되는 2개의 자기 변환기로 구성되며, 각각의 자기 변환기는 고정된 영구자석 인클로저에 의해 둘러싸인 가동형 다이어프램 및 코일 또는 "음성 코일(voice coil)"로 구성된다. 변환기에서 말할 때, 소리로부터의 공기 압력의 변화는, 음성 코일을, 코일에 AC 전류를 유도하는 둘러싸고 있는 자기장 내에서 전후로 이동시킨다. 청취자 쪽에서, 음성 코일에 흐르는 시변-전류(time-varying)는 파형 및 둘러싸는 자기장에 대향하는 동일한 파형 및 시변-자기장을 유도하여, 음성 코일을 소리를 포착하는 변환기와 동일한 방식으로 전후로 이동시킨다. 결과적인 이동은 소리를 포착하는 디바이스와 유사한 방식으로 소리를 재생한다. 현대 토착어에 있어서, 변환기가 소리를 전류로 변환할 때, 이는 마이크로서 동작하며, 또한 변환기가 전류를 소리로 변환할 때, 이는 스피커로서 동작한다. 또한, 전도된 전기 신호는 공기 중에서 요소 압력파, 즉 소리로서 운반되는 오디오 파형과 유사하기 때문에, 오늘날 이러한 전기 신호는 아날로그 신호 또는 아날로그 파형으로 지칭된다.

[0037] 전술한 바와 같이, 변환기는 말하기와 듣기 모두에 사용되기 때문에, 대화의 두 당사자는 모두 말할 때와 들을 때를 알아야만 한다. 이러한 시스템에서 스트링(string)에 의해 연결된 2개의 주석 캔과 유사하게, 발신자는 동시에 말하고 들을 수 없다. 반이중(half-duplex)" 모드로 불리는 이러한 단방향 동작은 고풍으로 들릴 수도 있지만, 이는 현대의 워키토키(walkie-talkies)에서, 그리고 "푸시 투 토크(push-to-talk)" 또는 PTT 라는 이름으로 현대의 전화기술에서 무선 통신에 아직도 실제로 사용되고 있다.

[0038] 나중에, 별도의 마이크 및 스피커를 구비한 전이중(full-duplex)(즉, 양방향 또는 송수신) 전화가 일상적으로 되어, 당사자들은 동시에 말하고 들을 수 있다. 그러나 현대라 해도, 피드백, 수신자의 소리가 그 마이크에 의해 수신되어 발신자에게 피드백되고 또한 발신자에게 피드백되어, 혼란스러운 에코와 때로는 불편한 휘파람 소리가 발생하는 상태-특히, 장거리 전화 통신을 괴롭히는 문제를 방지하기 위해, 전이중 전화 통신을 동작하는데에도 주의가 요구된다.

[0039] 초기의 전신 및 전화 시스템은 다른 문제, 프라이버시 중 하나로 어려움을 겪었다. 이들 초기의 통신 네트워크의 화신(incarnation)에 있어서, 네트워크에 연결된 모든 사람들은 원하지 않더라도, 회선 상에 통신되는 모든 것을 들었다. 농촌의 전화 네트워크에서, 이들 공유 라인은 "당사자 회선(party line)"으로 알려져 있었다. 그 후, 전화 시스템은 전용 회선이 전화 지점 사무실을 개별적인 클라이언트의 전화에 직접 연결한 다중-회선 네트워크로 급속하게 발전했다. 지점 교환 사무실 내에서, 시스템 운영자는 점퍼 케이블을 사용하여 교환대를 통해 발신자를 서로 수동으로 연결하고, 또한 첫 번째 "장거리"전화 통화 서비스를 형성하기 위해 한 지점을 다른 지점에 연결하는 능력도 가졌다. 전화 "스위치" 네트워크를 형성하는 큰 릴레이 뱅크(bank of relay)는 점진적으로 인간 운영자를 대체했으며, 이는 이어서 진공관을 포함하는 전자 스위치로 대체되었다.

[0040] 벨 연구소(Bell Laboratories)가 1950년대 후반에 트랜지스터를 개발한 후, 전화 스위치와 지점 교환은 그 취약하고 뜨거운 진공관을, 트랜지스터 및 궁극적으로 집적 회로를 포함하는 차가운 고체-상태 디바이스로 대체하였다. 네트워크가 커짐에 따라, 전화번호는 국제 전화를 처리하기 위해 7단위의 접두어와 개인 번호로부터 지역 코드 및 궁극적으로 국가 코드를 포함하도록 단위가 확장되었다. 곧 음성 통화를 운반하는 구리 케이블이 전세계를 커버하고 바다를 건넜다. 네트워크의 크기에도 불구하고, 동작 원리는 일정하게 유지되었으며, 그 통화는 아날로그 신호에 의해 운반되는 음성을 구비한 발신자와 전화 스위치에 의해 결정되는 통화의 라우팅 사이에 직접적인 전기 연결 또는 "회로"를 표시하였다. 이러한 전화 시스템은 결국 "회선 교환형 전화망"으로 알려지거나 또는 구어체로 일반 구식 전화 시스템 또는 POTS로서 알려지게 되었다. 회선 교환형 전화기술은 1980년대에 절정에 이르렀고, 그 이후로 다음 섹션에 기재되는 "패킷 교환형 전화기술"로 가차 없이 대체되었다.

[0041] 전화 네트워크와 거의 평행하게 진화하면서, 정규 라디오 통신이 1920년대에 라디오 방송으로 시작되었다. 상기 방송은 단방향이었고, 지정의 정부-허가를 받은 주파수의 라디오 방송국으로부터 송출되었으며, 또한 지정의 방송 주파수 또는 라디오 방송국에 맞춰진 임의의 많은 라디오 수신기에 의해 수신된다. 방송된 신호는 진폭 변조(amplitude modulation)(AM)를 사용하거나 또는 나중에 허가된 라디오 스펙트럼의 전용 부분 상의 각각의 주파수 변조(frequency modulation)(FM) 방법에 의해, 아날로그 신호를 운반하였다. 미국에서, 연방 통신위원회 또

는 FCC는 이러한 허가된 대역의 할당 및 규제를 관리하도록 발전했다. 방송 컨셉은 처음에 흑백 콘텐츠를, 후에 컬러를 포함하는 무선 전송을 사용하는 공용 텔레비전 프로그램으로 확장되었다. 나중에, 마이크로파 위성 접시에 의해 또는 동축 케이블을 통해 사람들의 가정에 텔레비전 신호도 운반될 수 있었다. 지정 방송 주파수에 맞춰진 임의의 청취자가 방송을 수신할 수 있기 때문에, 이러한 단방향 다중-청취자 통신을 위해 이제 "멀티캐스트(multicast)"라는 용어가 사용되고 있다.

[0042] 라디오 방송의 출현과 동시에, 첫 번째 양방향 통신이 상업용 및 군용 해양 선박에서 시작되었으며, 또한 2차 세계 대전 당시 라디오는 워키-토키 손 파지형 라디오 송수신기, 송신기와 수신기를 단일의 유닛으로 조합한 디바이스로 발전했다. 전화기술과 마찬가지로, 초기의 양방향 라디오 송신은 "단방향(simplex)" 모드로 동작하여, 다른 것은 듣기만 하고 오직 하나의 라디오만 단일의 라디오 채널 상에 방송하는 것을 허용하였다. 상이한 주파수에서 송신기와 수신기를 조합함으로써, 라디오 링크의 각각의 단부에서 동시 송신 및 수신이 가능하게 되어, 두 당사자 사이에 전이중 모드 통신을 가능하게 했다.

[0043] 그러나 다중 당사자로부터의 중복 전송을 방지하기 위해, 반이중 또는 PTT(push-to-talk)라 불리는 프로토콜이 채널 관리를 위해 일반적으로 사용되어, 선착순에 기초하여 누구나 지정 채널 상에 독점적으로 전송하게 한다. 아날로그 변조를 사용하는 산업 표준 라디오 유형은 아마추어(햄 또는 CB) 라디오, 해양 VHF 라디오, 항공 교통 제어를 위한 UNICOM, 및 개인용 워키-토키 통신을 위한 FRS를 포함한다. 이들 양방향 라디오 네트워크에 있어서, 라디오는 그 데이터를 지정 주파수 "채널"에 대해 중앙 라디오 타워(radio tower)에 송신하며, 상기 라디오 타워는 타워가 신호를 증폭하고 반복하여, 이를 전체 라디오 네트워크에 송신한다. 방송 구역에 대해 정보를 운반하는 사용 가능한 주파수의 번호는, 시스템의 총 대역폭 및 라디오 네트워크 상에서 한 번에 독립적으로 통신할 수 있는 사용자 수를 설정한다.

[0044] 많은 수의 발신자를 취급하도록 라디오 네트워크의 전체 용량을 확장하기 위해, 넓은 면적이 작은 부분 또는 라디오 "셀"로 분리된 셀룰러 네트워크의 개념이 1970년대에 입증되고, 그 후 10년 내에 널리 보급되었다. 상기 셀룰러 개념은 라디오 타워의 방송 범위를 더 작은 구역, 즉 더 짧은 거리로 제한하고, 따라서 동일한 주파수 대역을 재사용하여, 상이한 셀에 존재하는 상이한 발신자를 동시에 취급할 수 있게 하는 것이었다. 그렇게 하기 위해, 하나의 셀로부터 인접한 셀 내를 지나가는 발신자의 핸드오프(handoff)를 "누락(dropping)" 없이 그리고 갑자기 통화를 분리하지 않고 관리하도록, 소프트웨어가 생성되었다. 라디오 및 텔레비전 방송과 마찬가지로, POTS, 양방향 라디오처럼, 초기의 셀룰러 네트워크는 사실상 아날로그였다. 통화 라우팅을 제어하기 위해, 적절한 무선 전기 연결을 결정하도록 전화번호 시스템이 채택되었다. 이 선택은 또한 새로운 무선 셀룰러 네트워크를 "유선" 일반 구형 전화 시스템에 원활하게 연결하여, 두 시스템을 통해 상호 연결 및 상호 작용을 제공한다는 이점을 갖고 있었다.

[0045] 1980년대에 시작되어, 라디오 및 TV 방송과 함께 전화 및 라디오 통신은 전력 소비를 줄이고 배터리 수명을 늘리기 위해, 더 좋은 신호 대 노이즈 비율로 품질을 향상시키기 위해, 그리고 데이터 및 텍스트를 음성과 함께 운반할 필요성의 어드레싱을 시작할 필요성에 의해 구동되는 아날로그에서 디지털로의 통신 방법 및 포맷으로의 냉혹한 이전을 시작하였다. 일 대 일(one-to-one), 일 대 다(one-to-many), 및 다 대 다(many-to-many) 통신 모드를 동시에 사용할 수 있는, EDACS 및 TETRA 와 같은 라디오 포맷이 나왔다. 또한, 셀룰러 통신은 TV 방송이 그랬던 것처럼, GPRS 와 같은 디지털 포맷으로 신속히 전환되었다.

[0046] 2010년대까지, 대부분의 국가는 모든 아날로그 TV 방송을 중단했거나, 또는 중단 과정에 있었다. 방송 텔레비전과 달리, 케이블 TV 캐리어는 디지털 포맷으로 전환할 것이 요구되지 않고, 2013년까지 아날로그 및 디지털 신호의 하이브리드 합성물을 유지하였다. 디지털로의 그 궁극적인 이전은 정부 표준에 의해서가 아니라, 그 네트워크의 허용 가능한 채널의 수를 확장하고, HD 및 UHD 콘텐츠를 전달할 수 있고, 더 많은 페이퍼 뷰(payper-view)(PPV, "유니캐스트(unicast)"로도 알려짐)를 제안하고, 그리고 그 클라이언트에게 고속 디지털 연결서비스를 가능하게 하기 위한 상업적인 이유에 의해 유발되었다.

[0047] 인터넷의 출현으로, 더 구체적으로는 인터넷 프로토콜(IP)의 광범위한 채택으로, 아날로그로부터 디지털 포맷으로 글로벌 통신 네트워크의 이전을 동일시하는 것이 일반적이지만, 디지털 포맷으로의 전환은 전화기술에서 IP의 상업적 수용을 선행하여, IP 및 "패킷-교환형 네트워크"(다음 섹션에 기재된)로의 보편적인 이전을, 촉진시키지는 않았지만, 가능하게 하였다.

[0048] 회선-교환형 전화기술의 결과적인 진화는 "공공 교환 전화망" 또는 유사하지 않은 기술을 각각 포함하는 라디오, 셀룰러, PBX, 및 POTS 연결 및 서브-네트워크의 합병을 포함하는 PSTN으로서 개략적으로 존재한다. 네트워크는 고 대역 트렁크 라인에 의해 연결되고, 예를 들어 유선 연결을 통해 POTS 게이트웨이, 셀룰러 네트워

크, 기지국 PBX, 및 양방향 무선 네트워크에 연결된 PSTN 게이트웨이를 포함한다. 각각의 서브-네트워크는 독립적으로 동작하여, 유사한 종류의 디바이스를 구동한다.

[0049] 또한, PSTN은 AMPS, CDMA, 및 GSM 아날로그 및 디지털 프로토콜을 실행하는 기지국(17)을 거쳐 회선 교환형 셀룰러 네트워크에 연결된다. 셀룰러 타워를 통해, 회선 교환형 셀룰러 네트워크 기지국은 셀룰러 링크의 표준화된 셀룰러 무선 주파수를 이용하여 휴대폰과 같은 모바일 디바이스에 연결한다. GSM의 개선인 GPRS 네트워크의 경우, 회선 교환형 셀룰러 네트워크 기지국은 저속 데이터 및 음성을 동시에 전달하는 태블릿에도 연결할 수 있다. TETRA 및 EDACS 와 같은 양방향 무선 네트워크는 고-전력 무선 타워 및 셀룰러 링크를 통해 PSTN을 손 파지형 라디오 및 대형의 인-대시 및 데스크탑 라디오에 연결한다. 경찰차, 구급차, 구급 의료대원, 소방서, 및 심지어 항만 당국에 의해 통상적으로 사용되는 이러한 양방향 라디오 네트워크는, 전문 통신 네트워크 및 서비스로도 지칭되며, 소비자보다는 정부, 지방자치 당국, 및 응급 대응자를 표적으로 한다(참고: 여기에 사용되는 바와 같이, "데스크탑" "태블릿" 및 "노트북"이라는 용어는 이들 이름을 갖는 컴퓨터의 약식 참조로서 사용된다).

[0050] 통화 라우팅을 완료하기 위한 전형적인 전화번호를 사용하는 POTS 게이트웨이, 셀룰러 네트워크 기지국, 및 PBX와는 달리, 양방향 라디오 네트워크는 타워와 이것이 작용하는 모바일 디바이스 사이에 무선 링크를 설정하기 위해, (전화번호보다는) 전용의 RF 라디오 채널을 사용한다. 따라서 전문적인 무선 통신 서비스 가 뚜렷하게 존재하며, 또한 소비자 셀룰러 전화기 네트워크와는 독특하게 다르다.

[0051] 따라서, PSTN 네트워크는 다양한 기술의 서브 네트워크들을 유연하게 상호 연결한다. 오늘날의 회선 교환형 네트워크의 고유의 약점인 서브-네트워크 간 상호 동작 능력을 형성하는 것은 매우 다양하다. 다양한 서브-네트워크가 임의의 통상적인 제어 프로토콜 또는 언어와 통신하지 않기 때문에, 또한 각각의 기술이 데이터 및 음성의 전송을 상이하게 취급하기 때문에, PSTN 백본 또는 트렁크 라인(trunk line)을 통해 전화를 걸 수 있는 그 제한된 능력을 제외하고는, 다양한 시스템이 기본적으로 호환되지 않는다. 예를 들어, 뉴욕시의 세계 무역 센터에 대한 9월 11일 테러 공격 중, 재난과의 싸움에 도움을 주기 위해, 단지 그 라디오 통신 시스템 및 워키-토키를 배우기 위해, 맨해탄으로 집결한 미국 전역의 많은 응급 요원들은 다른 주 및 도시의 자원 봉사자들과 호환할 수 없었기 때문에 구호 노력에 대한 중앙 명령 및 통제를 관리하는 것을 불가능하게 하였다. 그 라디오의 통신 프로토콜에 표준화가 없기 때문에, 라디오는 서로 간단히 연결할 수 없었다.

[0052] 더욱이, 특히 아날로그 또는 비 보안 디지털 프로토콜을 사용하는 회선 교환형 전화 네트워크의 직접적인 전기 및 RF 연결에 의해, RF 스캐너를 구비한 해커가 활성 통신 채널을 찾고 그 당시에 발생하는 대화를 스니핑, 샘플링, 청취, 또는 차단하는 것은 간단한 일이다. 통신하는 당사자 사이에 PSTN 이 "지속적으로 연결된" 링크 또는 회로를 형성하기 때문에, 연방 법원이 주문한 도청 하에 동작하는 정부에 의해 합법적으로, 또는 불법적인, 금지된, 또는 공인되지 않는 감시를 수행하는 사이버 범죄 또는 정부에 의해 형사법적으로, 해커가 연결을 식별하고 "도청"하기에 충분한 시간이 있다. 합법적인 그리고 불법적인 스파이 행위 및 감시의 정의와 네트워크 운영자에 의한 협력 준수 의무는 국가마다 크게 다르며, 또한 국제적 경계를 넘어서 운영되고 있는 구글, 야후, 애플과 같은 글로벌 기업 사이의 논쟁이 가열되고 있다. 통신 네트워크 및 인터넷은 글로벌하며, 또한 국경이나 경계도 없지만, 이러한 전자 정보를 지배하는 법률은 당시 국내 및 국제적인 통신 및 상업을 제어하는 정부의 관할권에 국한되어 있다.

[0053] 적법성이나 윤리와 관계없이, 오늘날 모든 도로 또는 지하철의 거리 모서리 및 위에 있는 유비쿼터스 보안 카메라의 모니터링부터 다양한 국가의 국가 보안국 및 기관에 의해 수행되는 정교한 해킹 및 코드 균열에 이르기까지의 범위에 속하는 전자 도청 및 감시는 일상적인 것이다. 모든 네트워크가 취약하지만, PSTN의 오래된 그리고 취약한 보안 규정은 이들을 해킹에 특히 용이하게 한다. 따라서 심지어 현대의 보안 모뎀 네트워크에 연결된 PSTN은 전체 시스템에서의 약점을 나타내어, 보안 위반 및 사이버 범죄에 약점을 생성한다. 그럼에도 불구하고, 수십 년은 아니더라도, 글로벌 PSTN 네트워크를 퇴역시키고 이를 IP-기반 패킷 교환형 통신으로 완전히 대체하는데 수 년이 걸릴 것이다. 이러한 패킷-기반 네트워크(이하에 기재됨)는 PSTN 보다는 현대적이지만, 여전히 안전하지 않으며, 보안 파괴, 해킹, 서비스 거부 공격, 및 프라이버시 침해에 노출된다.

[0054] **패킷 교환형 통신 네트워크 동작**

[0055] 스트링에 의해 연결된 2개의 주석 캔이 현대의 회선 교환형 전화의 동작에 대한 은유를 나타낸다면, 우체국은 패킷 교환형 통신 네트워크에 대한 유사한 은유를 나타낸다. 이러한 접근법에 있어서, 텍스트, 데이터, 음성, 및 비디오는 파일 및 디지털 데이터의 스트림으로 변환되고, 이런 데이터는 그 후 데이터의 양자화된 "패킷"으로 파싱되어 네트워크를 통해 전달된다. 전달 메커니즘은 데이터 패킷이 어디로 가고 어디에서 왔는지를 독특하게 식별하는 전자 어드레스에 기초하고 있다. 또한, 포맷 및 통신 프로토콜은 이것이 사용될 프로그램 또는 애

플리케이션, 및 패킷을 운반하는 물리적 링크 및 전기 또는 라디오 연결을 촉진시키는 하드웨어에 지정한 콘텐츠를 포함하는 패킷에 포함된 데이터의 특성에 따라 정보를 포함하도록 설계된다.

[0056] 1960년대에 태어난 패킷 교환형 네트워크의 개념은 스푸트니크(Sputnik) 냉전의 편집 시대에 생성되었다. 그때 미 국방부(US Department of Defense, DoD)는 우주-기반 핵 미사일 발사가 미국의 전체 통신 기반시설을 분쇄하여, USSR 선제 공격에 대처할 능력을 상실할 수 있고, 또한 이런 공격에 대한 취약성이 실제로 하나를 도발시킬 수 있다는 우려를 표명했다. 따라서 DoD는 군대 시설 간에 정보를 전달할 수 있는 네트워크의 능력이 지정 데이터 링크 또는 심지어 네트워크 내의 수많은 링크를 파괴함으로써 방해받을 수 없는 중복 통신 시스템 또는 격자형(grid-like) "네트워크"의 개발을 후원했다. ARPANET으로 알려진 이 시스템은 인터넷의 부모와 현대 디지털 통신의 유명한 모태가 되었다.

[0057] 패킷 교환형 네트워크의 생성에도 불구하고, 인터넷의 폭발적인 성장은 처음 사용하기 쉬운 웹 브라우저인 Mosaic, 하이퍼텍스트 정의 웹 페이지의 출현, 월드 와이드 웹(World Wide Web)의 신속한 채택, 및 이메일의 광범위한 사용이 인터넷 플랫폼의 글로벌 수용을 전체적으로 확산시켰을 때의 1990년대까지는 발생하지 않았다. 어느 나라나 정부도 이를 중지시킬 수 없기 때문에(또는 심지어 그 글로벌 연계를 완전히 인식하지 못했기 때문에), 또한 그 사용자 기반은 그 새로이 획득된 개인용 컴퓨터를 사용하는 소비자를 포함하고 있기 때문에, 그 기본적인 견해, 중앙 제어의 결여, 또는 중앙 메인프레임에 대한 필요성 중 하나는 부분적으로는 인터넷을 유비쿼티(ubiquity)로 추진하였다.

[0058] 인터넷 성장의 다른 의미 있는 영향은 네트워크를 통해 데이터 패킷을 라우팅하는데 사용된 인터넷 프로토콜(IP)의 표준화였다. 1990년대 중반까지, 인터넷 사용자들은 데이터를 운반하는데 사용될 수도 있음을 인식하였으며, 바로 그 후 "Voice over Internet Protocol" 또는 VoIP 가 탄생했다. 그 개념은 이론적으로 인터넷을 갖는 누구라도 자유롭게 인터넷에 대해 음성에 의해 통신할 수 있게 했지만, 네트워크를 횡단하는 보급 지연, 즉 대기 시간(latency)은 음성 품질을 빈약하게 하였으며, 또한 자주 난해하게 하였다. "라스트 마일(lastmile)"에서의 연결 품질을 개선하도록 고속 이더넷 링크, 고속 WiFi 연결성, 4G 데이터의 채택으로 지연 시간이 개선되었지만, 인터넷 자체는 데이터 패킷의 정확한 전달을 보장하기 위해 생성되었으며, 패킷을 전달하는데 필요한 시간을 보장하지 않으며, 즉 인터넷은 실시간 네트워크로서 운영되도록 생성되지 않았다.

[0059] 따라서 값 비싼 장거리 통신 캐리어 또는 "텔코(telco)"를 대체하기 위해 인터넷을 사용하려는 꿈은 스카이프(Skype), 라인(Line), 카카오 톡(Kakao Talk), 바이퍼(Viper), 등과 같은 "오버 더 탑(over-the-top)"(OTT) 제공업체의 유용성에도 불구하고 크게 미흡한 실정이다. OTT 전화기술은 제어되지 않은 네트워크 대기 시간, 불량한 음질, 통화 끊김, 에코, 잔향, 피드백, 고르지 못한 소리, 및 때로는 통화를 시작할 수 없음으로부터 나타나는 낮은 서비스 품질(QoS)로 고통 받고 있다. OTT 통신의 빈약한 성능은 본질적으로 VoIP 기반 프로토콜의 약점이 아니라, OTT 캐리어가 데이터가 취하는 경로 또는 통신이 만나는 지연을 제어할 수 없는 네트워크 자체의 약점이다. 본질적으로, OTT 캐리어는 성능 또는 QoS를 보장할 수 없으며, 그 이유는 OTT 통신이 인터넷 히치하이커로서 동작하기 때문이다. 역설적으로, 오늘날 VoIP 기반 통신을 가장 잘 활용할 수 있는 회사는 전용의 낮은 대기 시간 하드웨어-기반 네트워크를 갖는 장거리 전화 캐리어며, 바로 텔코가 그렇게 하기 위한 최소의 동기를 갖고 있다.

[0060] 그 고유의 네트워크 중복을 제외하고, 패킷 교환형 통신의 가장 큰 강점 중 하나는, 데이터가 인터넷 프로토콜과 일치하는 패킷으로 배치되고, 또한 통신 디바이스가 인터넷에 연결되고 링크되어 있는 한, 임의의 소스로부터 임의의 목적지로 정보를 운반하는 그 능력이다. 인터넷 프로토콜은, 어떤 정보가 운반되는지 또는 어떤 애플리케이션이 이를 사용할 것인지에 대한 관심이나 염려 없이, 페이로드를 그 목적지로 전달하기 위해 네트워크의 능력을 관리하여, 맞춤형 소프트웨어 인터페이스 및 비싼 독점 하드웨어에 대한 임의의 필요성을 모두 피한다. 많은 경우에, 예를 들어 메일 읽기, 브라우저 상에서 웹 페이지 열기, 사진 또는 비디오 보기, 플래시 파일 보기, 또는 PDF 문서 읽기, 등을 위해 심지어 애플리케이션 관련 페이로드조차도 미리 정의된 포맷을 설정한다.

[0061] 다용도의 파일 포맷이 독점적인 또는 회사-지정의 소프트웨어에 대한 의존을 피하기 때문에, 인터넷은 "컴퓨터"로부터 휴대폰으로, 차량으로부터 가전기기의 범위에 속하는 지금까지 연결된 가장 광범위한 디바이스와 통신할 수 있는 "오픈 소스" 통신 플랫폼으로 간주될 수 있다. 이런 보편적인 연결성을 설명하는 가장 최근의 문구는 "만물 인터넷(IoE)" 이다.

[0062] 도시된 바와 같이, 고속 클라우드 서버 및 클라우드 데이터 스토리지를 포함하는 큰 컴퓨터 어레이는, 인터넷 클라우드를 형성하기 위해, 셀 수 없는 다른 서버(도시되지 않음) 사이에서 고 대역폭 연결부, 전형적으로 광섬유에 의해 상호 연결된다. 어떤 서버가 클라우드의 일부로 간주되고 어떤 서버가 그렇지 않은지를 정의하는 잘

정의된 경계가 없기 때문에, 클라우드 은유가 적절하다. 1일 및 심지어 분 단위로, 서버는 인터넷의 기능이나 성능에 영향을 주지 않고 유지 관리를 위해 오프라인으로 전환될 수 있을 동안, 온라인으로 있다. 이는 실제 중복 분산 시스템의 이점이며, 단일의 제어 지점이 없으며, 따라서 단일의 실패 지점도 없다.

[0063] 클라우드는 임의의 다양한 유선, WiFi 또는 무선 링크를 통해 사용자 또는 연결된 디바이스에 연결될 수 있다. 무선 패킷 교환형 가능한 전화 통신은 4G/LTE(또는, long-term evolution) 뿐만 아니라 HSUPA 및 HSDPA를 포함하는 셀룰러 프로토콜 3G를 포함하며, 심지어 셀이 다른 프로토콜로 동작하더라도 한 셀로부터 다른 셀로 전화 통화를 끊김 없이 핸드오프하는 능력을 포함하여 다양한 셀룰러 프로토콜과의 상호 작용성을 보장하는 네트워크 표준을 지칭한다. 참고: 정의 상, 여기에 사용된 "라스트 마일"은 태블릿, 데스크탑 또는 휴대폰과 같은 임의의 유형의 클라이언트 디바이스와 클라우드 서버 사이의 링크를 지칭한다. 방향 상, "퍼스트 마일(first-mile)"이라는 용어는 때로는 데이터 전송을 시작하는 디바이스와 클라우드 서버 사이의 연결을 지정하는데 사용되기도 한다. 이러한 경우에, 상기 "라스트 마일" 링크는 "퍼스트 마일" 링크이기도 하다.

[0064] 근거리 통신을 위해, WiFi 액세스 포인트는 스마트폰, 태블릿, 노트북, 데스크탑 또는 연결된 기기에 연결되며, 또한 가정, 카페, 레스토랑, 및 사무실의 로컬 무선 애플리케이션에 사용될 수 있다. WiFi는 단일 반송파 주파수 사양 802.11a, 802.11b, 802.11g, 802.11n을 위한 그리고 가장 최근에는 이중 주파수 대역 802.11ac 포맷을 위한 IEEE 정의된 표준에 따라 동작하는 통신을 포함한다. 간단한 고정 로그인 키에 기초하는 WiFi 보안은, 주로 연결의 무단 액세스를 방지하는데 사용되지만, 그러나 스니핑(sniffing) 또는 해킹으로부터 데이터를 무한정으로 보호하는 것으로는 의도되지 않는다.

[0065] 유선 분배 유닛 즉, 라우터는 광섬유, 동축 케이블, 또는 이더넷에 의해 노트북, 데스크탑, 전화, 텔레비전에, 또는 비틀린 구리 와이어 쌍 전화선에 의해 호텔, 공장, 사무소, 서비스 센터, 은행, 및 가정을 포함하는 부동의 또는 고정된 유선을 작용하는 판매 터미널의 지점에 연결될 수 있다. 유선 연결은 고속 데이터(high-speed data)(HSD) 연결을 WiFi, 이더넷, 또는 비틀린 구리 와이어 쌍으로 변환하기 위해 모뎀을 통해 로컬로 연결된 가정, 사무소, 공장, 또는 비즈니스에 광섬유 또는 동축 케이블의 분배를 포함할 수 있다. 광섬유 또는 케이블이 사용될 수 없는 원격 지역에 있어서, 디지털 가입자 라인(digital subscriber line)(DSL) 연결이 여전히 사용되지만, 그러나 데이터 전송률과 연결 안정성이 크게 양보된다. 무선, WiFi, 및 유선 연결을 통한 액세스를 계산하면, 인터넷에 연결된 개체의 수는 2020년까지 전 세계적으로 200억에 도달할 것으로 예상된다.

[0066] 디바이스 간 직접 연결을 설정하고 유지하는 상기 회선 교환형 네트워크와는 달리, 패킷 교환형 통신은 패킷을 인터넷을 통해 그 목적지에 "라우팅"하기 위해 어드레스를 사용한다. 따라서 상기 패킷 교환형 통신 네트워크에서, 통신 디바이스 사이의 연결을 유지하는 단일의 전용 회선이 없으며, 인터넷을 통해 이동하는 데이터는 단일 일관된 경로로 이동하지도 않는다. 각각의 패킷은 그 목표 목적지에 도달하기 위해 상호 연결된 컴퓨터의 미로(maze)를 통해 그 길을 찾아야만 한다.

[0067] 패킷 교환형 네트워크 통신을 사용한 노트북으로부터 데스크탑으로 IP 패킷 라우팅에서, 예를 들어 노트북으로부터 무선 연결부를 통해 로컬 WiFi 라우터에 전송된 제1 데이터 패킷은 DNS 서버의 어레이를 향하여 지향되며, DNS는 도메인 네임 서버의 약자이다. DNS 서버의 어레이의 목적은, 이 경우에 데스크탑인, 목적지 디바이스의 텍스트 이름 또는 전화번호를, IP 어드레스로 변환하는 것이다. 일단 식별되면, IP 어드레스는 DNS 서버의 어레이로부터 소스 어드레스로, 즉 노트북으로 다시 통과된다. 통신 장치를 명확하게 식별하는 이러한 어드레스는 네트워크를 통한 데이터 패킷의 라우팅에서 사용된다.

[0068] 그 후에, 노트북은 그 IP 데이터 패킷을 조립하고, 이들을 그 목적지로 연속해서, 예를 들어 처음에 WiFi 라디오를 통해 로컬 WiFi 라우터로 송신하기 시작하며, 그 후에 중간 라우터로서 작용하는 라우터 및 서버의 네트워크를 통해 그 목적지로 송신한다. 라우터 및 컴퓨터 서버는 함께 인터넷의 노드로서 또는 존재 포인트, 또는 POP, 즉 인터넷에 액세스할 수 있는 제한된 연결성의 게이트웨이로서 네트워크 동작한다. POP로서 동작하는 일부 라우터 또는 서버는 소수의 인접한 디바이스를 통해 인터넷에 연결되지만, 다른 서버는 다수의 디바이스에 상호 연결되며, 또한 때로는 "슈퍼 POP"으로서 지칭된다. 명확함을 위해, 네트워크 토착어에서 POP 라는 용어는 애플리케이션 이름 POP, 또는 이메일 애플리케이션에 사용되는 보통의 오래된 우체국과 혼동해서는 안 되는 것을 인식해야 한다.

[0069] 각각의 라우터 또는 라우터로서 동작하는 서버는 그 메모리 파일에, 어드레스 할 수 있는 IP 어드레스 및 가능하기로는, 그 위의 라우터가 어드레스할 수 있는 어드레스를 식별하는 라우팅 표를 포함한다. 이들 라우팅 표는 인터넷에 처음 연결될 때 모든 라우터에 자동으로 다운로드되어 설치되며, 또한 일반적으로 네트워크를 통해 패킷을 라우팅하는 부분으로서 로딩되지 않는다. IP 패킷이 라우터, POP 또는 슈퍼 POP에 들어왔을 때, 그 목적지

로의 여정 상에서 패킷을 어디로 지향시킬지를 알기 위해, 라우터는 일반적으로 어드레스의 최상위 자릿수인 충분한 IP 어드레스를 읽는다. 예를 들어, 뉴욕으로부터 도쿄로 향하는 패킷은 먼저 시카고로 라우팅되며, 그 후 도쿄로 연결되기 전에 샌프란시스코, 로스앤젤레스, 또는 시애틀의 서버를 통한다.

[0070] 패킷이 횡단하는 라우터의 수, 및 라우터 간 연결 각각의 사용 가능한 데이터 전송률은 인프라에 의해서 그리고 네트워크 트래픽 및 로딩에 의해 달라지기기 때문에, 어떤 경로가 가장 빠른지 또는 가장 좋은지를 선험적으로 결정할 방법이 없다.

[0071] 패킷 교환형 데이터로 클라이언트 사이에 직접 연결을 설정하고 유지하는 회선 교환형 전화 통신과는 달리, 어떤 경로가 최적인지, 적절한지, 또는 더 빠른 경로인지를 결정하여, 패킷을 라우팅하기 위해 인터넷을 감시하면서 패킷을 라우팅하는데 가장 적합한 경로를 결정하는 범용 인텔리전스는 없고, 또한 2개의 연속한 패킷이 심지어 동일한 경로를 취할 것이라는 보장도 없다. 따라서 패킷은 패킷이 횡단하는 라우터 및 서버를 동작하는 회사의 우선순위에 기초하여 인터넷을 통해 그 길을 "발견"한다. 각각의 라우터는, 본질적으로, 네트워크 상태에 따라 그 바람직한 경로를 정의하는 어떤 라우팅 표 및 라우팅 알고리즘을 포함한다. 예를 들어, 라우터의 선호는 동일한 회사에 의해 소유된 다른 라우터로 패킷 전송하는 우선시할 수 있어, 인접 라우터와의 연결 사이에 트래픽을 평형시키고, 다음 라우터로의 가장 짧은 지연을 찾고, 최소화하거나 비즈니스를 전략적 비즈니스 파트너에게 지향시키거나, 가능한 한 중간 라우터를 스킵함으로써 VIP 클라이언트를 위한 고속 차선을 생성한다. 패킷이 라우터에 들어갈 때, 지정 POP 에 의해 이루어진 라우팅 선택이 발신자 또는 네트워크 서버 운영자에게 가장 관심 있게 이루어졌는지의 여부를 아는 방법은 없다.

[0072] 따라서 어떤 의미에서, 패킷이 취하는 루트는 타이밍과 운의 문제이다. 이전의 New York to Tokyo 라우팅 예에 있어서, 라우팅 및 결과적인 QoS는 경로의 작은 혼란, 즉 비선형 방정식에서 소위 "나비 효과"에 기초하여 실질적으로 변할 수 있다. 뉴욕으로부터의 패킷이 시카고의 "라우터 A"를 통과하는 경우를 생각하면, 캘리포니아에 일시적으로 높은 트래픽이 많기 때문에, 이는 캘리포니아보다는 멕시코시티로 포워딩된다. 그 후, 멕시코시티 라우터는 다시 IP 패킷을 싱가포르로 포워딩하고, 그로부터 이는 마지막으로 도쿄로 송신된다. 송신된 바로 다음 패킷은 시카고 "라우터 B"를 통해 라우팅되고, 이는 그 시점에서 낮은 트래픽 때문에, 상기 패킷을 샌프란시스코로 보내고, 그 후 직접 도쿄로 2홉만으로 지향시킨다. 이런 경우에, 제2 패킷은 제1 패킷이 더 길고 에두르는 경로를 통해 라우팅되기 전에 도쿄에 도착할 수 있다. 이 예는 라이브 비디오 스트리밍이나 VoIP 와 같은 실시간 통신을 위해 인터넷을 사용하는 문제, 즉 전달 시간을 보장하거나 또는 전달 수행 시 네트워크 지연을 제어하도록 인터넷이 설계되지 않았음을 강조한다. 대기 시간은 패킷이 단지 2개의 서버를 통해 또는 15개를 통해서만 라우팅되는지의 여부에 따라 50 ms 내지 1초 이상까지 변할 수 있다.

[0073] 인터넷의 라우팅 제어의 결여는 실시간 애플리케이션에 문제가 있으며, 또한 특히 OTT 캐리어-인터넷 인프라의 상부 상에 무임 승차를 포획함으로써 인터넷 기반 전화를 제공하려고 노력하는 캐리어에 대해 취약한 QoS의 문제가 된다. OTT 캐리어가 라우팅을 제어하지 않기 때문에, 그들은 지연 또는 네트워크 대기 시간을 제어할 수 없다. 패킷 교환형 통신의 다른 문제점은 검출되지 않고 데이터를 빼내기 쉽다는 점이다. 해적이 패킷을 가로채서 소스 또는 목적지 IP 어드레스를 식별한다면, 그들은 중재 라우터로부터의 데이터를 가로채고 자신의 해적 네트워크를 통해 트래픽을 스니핑하거나 재지향시켜, 대화를 염탐하거나 또한 심지어 암호화된 파일을 해독시키기 위해 다양한 방법을 사용수 있다.

[0074] 패킷을 라우팅하는데 사용되는 소스 및 목적지 IP 어드레스 및 다른 중요한 정보(및 패킷을 난도질하기 위해 해적에 의해 사용되기도 하는)는, IP 패킷, IP 데이터그램, 또는 TCP/IP 패킷으로 지칭되는 디지털 데이터의 스트링으로 지정된다. 상기 IP 패킷은 디바이스 사이의 물리적 연결을 정의하는 디지털 정보, 디바이스를 함께 링크하도록 데이터가 조직화되는 방법, 패킷의 네트워크 라우팅, 유용한 데이터(페이로드)가 정확하게 전달되었는지 그리고 어떤 종류의 데이터가 페이로드에 있는지, 그리고 그 후 페이로드 데이터 자체가 다양한 애플리케이션에 의해 사용되는지를 보장하기 위한 수단을 포함하고 있다.

[0075] IP 패킷은 일련의 디지털 비트의 스트링으로서 순차적으로 송신 및 수신되며, 또한 그 중에서도 인터넷 엔지니어링 태스크 포스(Internet Engineering Task Force)를 포함하는 다양한 표준 위원회에 의해 설정된 인터넷 프로토콜이라고 불리는 지정 방식으로 조직된다. 이 표준은 규정된 프로토콜을 따르는 임의의 IP 패킷이 동일한 IP 표준을 준수하는 임의의 연결된 디바이스에 의해 통신하고 이해될 수 있음을 보장한다. 인터넷에 연결된 디바이스 및 애플리케이션의 통신 및 상호 작용성을 보장하는 것은 인터넷의 특징이며, 또한 회사, 정부 또는 개인이 인터넷을 제어하거나 액세스 가능성을 또는 그 기능성을 제한하는 것을 방지하기 위해, 오픈 소스 이니셔티브(Open Source Initiative) 또는 OSI의 안내 원리를 나타낸다.

[0076] 기능성의 7개 계층을 포함하는 추상적인 개념인 OSI 모델은 IP 패킷의 형식, 및 패킷의 각 세그먼트가 사용되는 것을 정확하게 규정한다. IP 패킷의 각 부분 또는 "세그먼트"는 특정 OSI 계층 4의 기능에 적용하는 데이터에 대응한다. 7개의 OSI 계층의 역할은 다음과 같다 :

[0077] * 계층 1, 물리 계층 또는 PHY 계층은 통신의 물리적 특성을 전기, RF, 및 광 신호로 표현하는 하드웨어 지정 정보와, 이들 신호를 통신 시스템에서 사용하기 위해 비트로 변환될 수 있는 방법을 포함한다. WiFi 라디오, 이더넷, 직렬 포트, 광섬유, 3G 또는 4G 셀룰러 라디오, 비틀린 쌍의 구리선 상의 DSL, USB, 블루투스, 케이블 또는 위성 TV, 또는 오디오, 비디오, 또는 멀티미디어 콘텐츠의 디지털 방송을 비트 스트림으로 변환하는 것은 PHY 계층의 동작이다. IP 패킷에서 프리앰블은 계층 1 데이터를 나타내며, 그리고 전체 데이터 패킷 또는 "프레임"을 이를 송수신하는 하드웨어로 동기화하는데 사용된다.

[0078] * 계층 2, 데이터 링크 계층은 프레임으로서 배열된 비트를 포함하고, PHY 계층 1로부터 전달된 비트 스트림이 해석 가능한 데이터로 변환되는 규칙 및 수단을 정의한다. 예를 들어, WiFi 라디오 기반 비트 스트림은 802.11a, b, g, n 및 ac를 포함하는 임의의 개수의 IEEE 정의 표준을 준수할 수 있으며; 3G 무선 통신은 고속 패킷 액세스 방법인 HSDPA 또는 HSUPA를 사용하여 변조될 수 있으며; 광섬유에서 변조된 광 또는 동축 케이블 상의 전기 신호는, DOCSIS 3 표준에 따라 데이터로 디코딩될 수 있다. IP 패킷에서, 계층 2 데이터는 그 페이로드를 선행 "데이터 링크 헤더" 및 후행 "데이터 링크 트레일러"와 함께 데이터그램으로 캡슐화하고, 캡슐화된 전송되는 페이로드가 전송 프로세스에서 손실된 것이 없음을 보장하는 것처럼 시작 및 중지한다. 계층 2 데이터의 하나의 핵심 요소는 지정 이더넷 어드레스, RF 링크, 또는 하드웨어지정 송수신기 링크로 또는 이로부터 데이터 트래픽을 지향시키는데 사용되는 MAC 또는 미디어 액세스 어드레스이다.

[0079] * 계층 3, 네트워크 또는 인터넷 계층은, 패킷이 패킷 내에 포함된 페이로드의 특성에 관한 정보뿐만 아니라 IPv4 또는 IPv6 데이터 및 대응하는 소스와 목적지 IP 어드레스를 포함하는지의 여부, 즉 사용된 전송 프로토콜의 유형이 전송 제어 프로토콜(Transmission Control Protocol)(TCP), 사용자 데이터그램 프로토콜(User Datagram Protocol)(UDP), 또는 다른 어떤 것을 포함하는지의 여부를 포함하는, IP 패킷을 라우팅하는데 사용되는 인터넷 프로토콜(IP) 정보를 포함하는 "데이터그램"으로 불리는 패킷을 포함한다. 또한, 계층 3은 IP 패킷이 전달되지는 않지만 결코 죽지 않는 불사(immortal)를 방지하는 기능을 포함한다. 지정 유형의 계층 3 패킷인 ICMP는 잘 알려진 "핑(ping)"기능을 포함하여 네트워크의 상태를 진단하는데 사용된다. IP 패킷에서, 상기 계층 3은 "IP 헤더"(82)를 포함하며, 또한 전송 및 상위 계층 세그먼트를 포함하는 자신의 페이로드를 캡슐화한다.

[0080] * 계층 4, 전송 계층은 통신 디바이스 사이의 연결 특성을 정의하는 데이터의 세그먼트를 포함하며, 여기서 UDP는 비 연결형 통신을 위한 페이로드의 최소 설명, 즉 페이로드가 얼마나 큰지, 손실된 임의의 비트가 있는지, 그리고 어떤 애플리케이션 서비스(포트)가 전달된 데이터를 사용하는지를 정의한다. 상기 UDP는 페이로드의 전달을 확인하지 않고, 애플리케이션 상에서 에러 또는 손실 데이터를 확인하는 것에 의존하기 때문에 비 연결성으로 간주된다. 상기 UDP는 전형적으로 패킷을 재전송하는 것이 선택사항이 아닌, 방송, 멀티캐스팅, 및 스트리밍과 같은 시간 민감형 통신에 사용된다. 이와는 달리, TCP는 패킷을 확인함으로써 가상 연결을 보장하며, 다음 패킷이 송신되기 전에 페이로드가 안정적으로 전달되며, 그리고 누락된 패킷을 재송신한다. 또한, TCP는 체크섬(checksum)을 사용하여 전달된 패킷의 데이터 무결성을 체크하며, 또한 그 본래 순서대로 순서가 잘못된 패킷을 재조립하는 기능을 포함한다. TCP 와 UDP 모두는 소스 및 목적지 포트, 상위 계층 서비스 또는 애플리케이션, 예를 들어 계층 4 페이로드 내에 포함된 정보와 관련된 웹 서버 또는 이메일 서버의 설명을 정의한다. IP 패킷에 있어서, 계층 4는 TCP/UDP 헤더를 포함하며, 또한 상위 OSI 계층 5, 6, 7 에 의해 사용되는 콘텐츠를 포함하는 데이터/페이로드를 캡슐화한다.

[0081] * 계층 5, 6, 7, 상위 또는 애플리케이션 계층은 인터넷에 의해 전달된 콘텐츠를 데이터/페이로드로서 설명한다. 계층 7, "애플리케이션" 계층은 OSI 모델에서 가장 높은 레벨을 나타내며, 또한 오픈 소스 및 독점 애플리케이션 소프트웨어를 모두 지원하기 위해 6개의 하부 OSI 계층에 의존한다. 통상적으로 사용되는 레벨 7 애플리케이션은 SMTP, POP 또는 IMAP를 사용하는 이메일, HTTP(크롬, 사파리, 익스플로러, 파이어폭스)를 사용하는 웹 브라우징, FTP를 사용한 파일 전송, 및 텔넷을 사용하는 터미널 에뮬레이션을 포함한다. 독점적인 애플리케이션은 마이크로소프트 오피스 제품군(워드, 액셀, 파워포인트), 어도브 일러스트레이터, 및 포토샵, 오라클 및 SAP 데이터베이스 애플리케이션; 퀴켄(Quicken), 마이크로소프트 머니(Microsoft Money), 및 퀵북(QuickBooks) 금융 소프트웨어; 이에 더하여, 어도브 아크로뱃 리더(Adobe Acrobat Reader) 및 애플 프리뷰(Apple Preview)와 같은 문서 판독기뿐만 아니라, (아이튠(iTunes), 퀵타임(QuickTime), 리얼 미디어 플레이어, 윈도우 미디어 플레이어, 플래시(Flash)와 같은) 오디오 및 비디오 플레이어를 포함한다. 레벨 7 애플리케이션은, 암호화와 같은 보안 기능과 함께, 일반적으로 텍스트, 그래픽 및 그림, 소리 및 비디오, XML 또

는 PDF와 같은 문서 프리젠테이션을 포함하는 레벨 6, "프리젠테이션" 계층에 의해 구문적으로 정의된 매립형 개체를 이용한다. 레벨 5, "세션"계층은 하나의 개체를 다른 프로그램 파일로 가져 오는 것과 같은 애플리케이션 간 연결성을 설정하고, 또한 세션을 시작하고 종료하는 것을 제어한다.

[0082] 설명된 바와 같이, OSI 7 계층 모델은 각각의 계층의 기능을 정의하고, 대응하는 IP 패킷은 서로에 대한 데이터를 캡슐화한다(바부시카(babushka) 또는 러시아 중첩 인형과 유사한 방식으로 하나가 다른 것의 내부에 있는, 하나의 인형 내에 다른 인형이 있는, 그리고 이것이 계속되는 나무 인형). 외부 패킷 또는 계층 1 PHY는 모든 상위 레벨과 관련된 정보를 포함하는 전체 IP 프레임을 정의한다. 이 PHY 데이터 내에서, 상기 계층 2 데이터 프레임은 데이터 링크 계층을 설명하며, 계층 3 네트워크 데이터그램을 포함한다. 이 데이터그램은 다시 인터넷 계층을, 전송 계층을 설명하는 계층 4 세그먼트 데이터를 구비한 그 페이로드로서 설명한다. 전송 계층은 상위 계층 데이터를, 계층 5, 6, 7 콘텐츠를 포함하는 페이로드로서 전달한다. 7 계층 캡슐화는 때로는 애플리케이션, 프리젠테이션, 세션, 전송, 네트워크, 데이터 링크, 및 물리 계층으로서 위에서부터 아래로 7개의 OSI 계층을 연속적으로 나열하는 "모든 사람들이 데이터 처리를 필요로 하는 것처럼 보인다"라는 연상기호에 의한 것으로 지칭된다.

[0083] 낮은 물리 계층과 링크 계층이 하드웨어에 지정한 반면에, 네트워크 및 전송 정보를 설명하는 IP 패킷 내에 캡슐화된 중간 OSI 계층은, 통상적으로 IP 패킷을 통신하고 전달하고 전달하는데 사용되는 하드웨어에 완전히 불가지론적이다. 더욱이, 전송 계층의 페이로드로서 캡슐화된 상위 계층은, 패킷이 인터넷을 통해 어떻게 라우팅되거나 전달된 바와는 완전히 독립적으로 적용되고 동작되는 애플리케이션에만 지정한다. 이 구획화는 각각의 계층이 본질적으로 독립적으로 감시될 수 있게 하여, 패킷 포맷팅의 관리 승인이나 패킷 페이로드의 유효성 검사에 대한 필요성 없이, 수많은 기술 및 사용자 조합을 지원할 수 있다. 불완전하거나 부적절한 IP 패킷은 단순히 폐기된다. 이러한 방식으로, 상기 패킷 교환형 네트워크는 임의의 인터넷 연결된 디바이스 또는 개체 사이에서 일관된 형태로 이질적인 통신 미디어에 대해 다양한 애플리케이션 관련 정보를 라우팅, 전송, 및 전달할 수 있다.

[0084] 결론적으로, 교환형 회선 네트워크는, 패킷 교환형 네트워크 통신이 문서, 소리, 비디오, 및 텍스트를 여러 개의 패킷으로 분할하고, 복수의 네트워크 경로(정확한 시간 내에 전달을 제공하기 위한 최선의 노력을 사용하여 우체국과 유사한)를 통해 이들 패킷을 전달하고, 그 후 본래의 콘텐츠를 재조립하고, 그 과정에서 손실된 것이 없음을 확인할 동안, 2개 또는 그 이상의 당사자 통신(한 세기 전 일반 구현 전화기 시스템과 유사) 사이에서 단일의 직접 연결을 요구한다. 회선 교환형 PSTN과 패킷 교환형 VoIP 사이의 비교가 이하의 표에 요약되어 있다.

*표 1*

[0085]

| 네트워크 | PSTN | 인터넷 |
|---|---|---|
| 기술 | 회선 교환형 | 패킷 교환형 |
| 연결 | 전용 전기 연결 | 각 패킷이 인터넷을 통해 라우팅 됨 |
| 데이터 전달 | 실시간(회선) | 최선 전송(패킷) |
| 신호 | 아날로그 또는 디지털 | 디지털, IP, VoIP |
| 콘텐츠 | 음성 | 음성, 텍스트, 데이터, 비디오 |
| 데이터 전송률 | 낮음 | 높음 |
| 에러 체킹 | 없음, 또는 최소 | 광범위 |
| 끊긴 라인의 영향 | 끊긴 또는 짧은 통화 | 통화 재라우팅 |
| 정전의 영향 | 네트워크가 전력 전달 | 배터리 백업 필요 |

[0086] PSTN이 실시간 전기 회선 연결을 사용하여 동작할 동안, 패킷 교환형 네트워크는 그 도착이 늦었더라도 궁극적으로 메일을 전달하기 위해 상이한 트럭 및 우편 집배원을 사용하는 우체국과는 달리, 패킷 및 페이로드를 전달하는 방법을 찾기 위해 "최상의 노력" 방법을 사용하여 콘텐츠를 전달한다는 점을 인식해야 한다. 패킷 교환형 네트워크의 동작 및 통신이, 본 개시 내용이 부분-계속인 "Secure Dynamic Communication Network and Protocol"이라는 명칭의 관련 특허출원의 배경 항목에서 더 구체적으로 설명된다.네트워크의 성능을 고려할 때, 아래의 몇 가지 요소가 고려된다.

[0087] * 데이터 속도, 즉 대역폭

[0088] * 서비스의 품질

[0089] * 네트워크 및 데이터 보안

[0090] * 사용자 프라이버시

[0091] 위의 고려 사항 중, 데이터 전송률은 초당 수백만 비트 또는 Mbps로 쉽게 계량된다. 반면 서비스 품질 또는 QoS는 대기 시간, 음질, 네트워크 안정성, 간헐적인 동작 또는 빈번한 서비스 중단, 동기화 또는 연결 실패, 낮은 신호 강도, 지연된 애플리케이션, 및 긴급 상태 중 기능적인 네트워크 이중화를 포함하는 여러 가지 요소를 포함한다. 사이버 보안 및 사이버 프라이버시는 네트워크 상에서의 공격을 방지하고, 사이버 범죄, 사이버 감시, IP 패킷 스니핑, 포트 심문 및 서비스 공격 거부, 프로파일링, 사기, 패킷 하이재킹, 사이버-감염, 감시, 해적 관리 및 침입을 포함하는, 데이터 트래픽 및 콘텐츠에 대한 미승인 접속을 방해한다.

[0092] **서비스 품질**

[0093] 서비스 품질은 용량, 대역폭, 대기 시간, 데이터 전송률, 확장성, 음질 데이터 무결성, 데이터 비트 에러율에서의 네트워크의 성능을 설명한다. 프로그램, 파일 및 보안 관련 검증에 대해, 데이터 정확성이 중요한 요소이다. 어떤 요소가 중요한지는 패킷 교환형 네트워크를 통해 운반되는 페이로드의 특성에 달려 있다. 이와는 대조적으로, 실시간 애플리케이션을 구성하는 음성 및 비디오에 대해, 패킷 전달 시간에 영향을 미치는 요소가 중요하다. 품질 요소 및 이들이 비디오, 음성, 데이터 및 텍스트와 같은 다양한 애플리케이션에 어떻게 영향을 미치는지는 적용예에 따라 달라진다. 일정한 고속 데이터 IP 패킷 파형에 의해 전형적인 양호한 네트워크 상태는, 최소의 시간 지연, 명확한 강한 신호 강도, 신호 왜곡 없음, 안정된 동작, 및 패킷 전송 손실 없음이다.

[0094] 간헐성을 갖는 낮은 데이터 전송률 패킷 파형을 갖는 간헐적인 네트워크는 비디오 기능에 가장 큰 영향을 끼쳐, 고통스럽게 느린 비디오 다운로드를 유발하고 비디오 스트리밍을 수용할 수 없게 한다. IP 패킷 파형에 의해 예시되는 짧은 주기의 차단으로 보다 낮은 유효 데이터 처리율로 동작하는 혼잡한 네트워크는, 덜컥거리는 간헐적인 운동, 퍼지(fuzzy) 영상, 부적절한 색깔 및 밝기에 의해 비디오를 심각하게 저하시킬 뿐만아니라, 왜곡, 에코, 그리고 심지어는 전체 문장이 대화나 소리 트랙으로부터의 누락에 의해 음성 또는 음성통신을 저하시킨다. 그러나 혼잡한 네트워크에 있어서, 재방송에 대한 반복된 요청에 의해 TCP를 사용하여 데이터가 여전히 전달될 수 있다.

[0095] 극단적으로, 불안정한 네트워크는 예측할 수 없는 주기의 많은 데이터 정지로 낮은 데이터 처리율을 나타낸다. 또한, 불안정한 네트워크는 파형(610D)에서 어두운 음영 패킷으로 표현되는 바와 같이 손상된 IP 패키지를 포함하며, 이는 TCP 기반 전송에서 재전송되어야만 하며 또한 UDP 전송에서는 단순히 변질되거나 부적절한 데이터로서 폐기되어야만 한다. 네트워크 열화의 레벨에 있어서, 심지어 이메일은 간헐적으로 되어, IMAP 파일 동기화가 실패한다. 그 경량 데이터 포맷 때문에, 대부분의 SMS 및 텍스트 메시지는 비록 심각한 네트워크 혼잡에도 불구하고 약간의 전달 지연으로 배달되지만, 그러나 첨부물은 다운로드되지 않을 것이다. 불안정한 네트워크에서 모든 애플리케이션은 실패하여, 컴퓨터나 휴대폰의 정상 동작이 중단되어 예상 파일이 전달될 때까지 기다림으로 나타날 수 있다. 이러한 경우에는 비디오가 멈추고, 소리가 고르지 않게 되어 이해하기 어려워지고, VoIP 연결은 몇 분 내에 12번 이상 반복적으로 끊어지며, 어떤 경우에는 완전히 연결되지 않는다. 마찬가지로, 이메일은 컴퓨터 아이콘이 끊임 없이 둥글게 회전하면서 멈추거나 지연된다. 진행률 막대가 모두 중단된다. 심지어 텍스트 메시지도 반송되고 "전달할 수 없다".

[0096] 선택한 서버 또는 네트워크 상의 서비스 거부 공격의 심각한 거부 중 주요 서버 및 슈퍼 POP의 전력 장애, 과부하된 통화 용량, 대용량 데이터 파일 또는 UHD 영화의 전송을 포함하여, 여러 가지 요인이 네트워크 불안정성의 원인이 될 수 있지만, 네트워크의 QoS를 추적하는데 사용된 주요한 요인은 그 패킷 손실 속도 및 패킷 대기 시간이다. 누락된 패킷은 IP 패킷이 전달될 수 없어 영구적으로 "타임 아웃"될 때, 또는 라우터나 서버가 IP 패킷 헤더의 체크섬 에러를 검출한 경우에 발생한다. UDP를 사용하는 패킷의 경우, 패킷이 손실되고, 계층 7 애플리케이션은 무엇이 손상되었는지를 알 수 있을 정도로 똑똑해야 한다. TCP 가 계층 4 전송에 사용되는 경우, 패킷은 재전송 요청을 받을 것이며, 추가로 잠재적으로 이미 오버로드된 네트워크에 로딩을 추가한다.

[0097] QoS, 전파 지연을 결정하는 다른 요소는 노드 대 노드로부터의 IP 패킷의 지연 또는 소스로부터 목적지로의 단방향으로, 또는 대안적으로 다시 소스로부터 목적지로의 왕복 지연과 같은 여러 가지 방법으로 정량적으로 측정될 수 있다. 패킷 전달 상의 전파 지연의 효과는 UDP 및 TCP 전송 프로토콜을 사용하는 것과 상이하다. 통합형 네트워크 전파 지연이 증가함에 따라, VoIP 대화와 같은 왕복 통신을 수행하는데 필요한 시간이 증가한다. UDP 전송의 경우, 왕복 지연은 전파 지연에 따라 선형적으로 증가한다. 긴 전파 지연이 더 높은 비트 에러율과 관련되기 때문에, 손실된 UDP 패킷의 수가 증가하지만 그러나 UDP는 손실된 패킷의 재전송을 요청하기 때문에, 왕복

시간은 증가 된 지연으로 선형으로 유지된다. TCP 전송은 패킷 전달을 확인하는데 요구되는 핸드세이킹 때문에, UDP 보다 송신된 각 패킷에 대해 실질적으로 더 긴 왕복 시간을 나타낸다. 비트 에러율이 낮고 또한 대부분의 패킷이 재전송을 요구하지 않으면, TCP 전파 지연은 통합된 전파 지연에 따라 선형적으로 증가한다. 그러나 통신 네트워크가 전파 지연이 증가함에 따라 불안정해지면, 누락된 패킷의 재전송에 대한 프로토콜의 필요성 때문에 TCP 전송에 기인한 왕복 시간이 기하급수적으로 증가한다. 따라서 TCP는 VoIP 및 비디오 스트리밍과 같이 시간에 민감한 애플리케이션에 대해서는 금기 사항이다.

[0098] 모든 패킷 통신이 동일한 전파 시간을 갖는 두 패킷이 없는 통계적이기 때문에, 네트워크의 단일 방향 대기 시간을 추정하는 가장 좋은 방법은 많은 수의 비슷한 크기의 IP 패킷의 왕복 시간을 측정함으로써, 그리고 단일 방향 대기 시간을 추정하기 위해 2로 나눔으로써 이루어진다. 100 ms까지의 지연 시간이 현저하며, 200 ms 까지는 상당히 매우 좋은 것으로 간주되며, 300 ms 까지는 여전히 허용 가능한 것으로 간주된다. 인터넷 상에서 동작되는 OTT 애플리케이션에 의해 쉽게 접하는 500 ms의 전파 지연에 대해, 상기 지연은 사용자에게 불편해지며 또한 정상적인 대화를 방해한다. 음성 통신에 있어서, 특히 이런 긴 전파 지연은 "나쁜" 소리를 내고 또한 반향으로 나타날 수 있어, "틱(twangy)" 또는 금속성 소리를 생성하여, 상대방이 그 마지막 순간까지 당신의 응답을 얻기 위해 기다릴 동안 정상적인 대화를 중단하여, 아마도 자신의 마지막 의견에 대한 응답을 기다리는 동안 정상적인 대화를 방해하고 아마도 왜곡되거나 이해할 수 없는 스피치로 나타날 수 있다.

[0099] 명확함을 위해서, 통신의 단방향 대기 시간은, 부분적으로는 ICMP 패킷이 일반적으로 실제 IP 패킷에 비해 경량이기 때문에, 핑 테스트가 TCP의 "재송신 요청"을 사용하지 않기 때문에, 및 인터넷의 공공 네트워크에 대한 보상이 없기 때문에, 핑 테스트의 루트가 실제 패킹 루트와 매칭된다는 점에서, 계층 3 ICMP 유틸리티(HTTP://www.speedtest.net 에서의 무료 네트워크 테스트와 같은)에 의해 수행된 핑 테스트와는 상이하다. 본질적으로, 핑이 오랜 지연을 경험할 때, 네트워크 또는 디바이스와 네트워크 사이의 일부 링크, 예를 들어 WiFi 라우터 또는 라스트 마일에 무언가 문제가 있지만, 그러나 그 자체의 좋은 핑 결과는 실제 패킷의 낮은 전파 지연을 보장 할 수 없다.

[0100] 네트워크 보안을 향상시키기 위해, 암호화 및 확인 방법은 해킹, 스니핑, 또는 스파이를 방지하도록 자주 사용된다. 그러나 과도한 암호화와 다중 키 암호화 프로토콜은 대화 상대의 신원을 끊임없이 재확인하여, 추가적인 지연을 야기하며 이렇게 함으로써 효과적인 네트워크 대기 시간을 증가시키며, 보안을 향상시키는 비용에서 QoS를 저하시킨다.

[0101] **사이버 보안 및 사이버 프라이버시**

[0102] 통신의 다른 2가지 주요 고려 사항은 사이버 보안 사이버 프라이버시이다. 관련이 있지만, 상기 2가지 문제는 다소 상이하다. "네트워크 보안, 컴퓨터 보안, 및 보안 통신을 포함한 사이버 보안은 컴퓨터 또는 통신 네트워크, 네트워크 액세스 가능 자원, 또는 네트워크 연결된 디바이스 내에 포함된 데이터의 무단 액세스, 오용, 수정, 또는 거부를 모니터링, 차단, 및 방지하는데 사용되는 방법을 포함한다. 데이터는 개인 사진 이미지 및 비디오 기록물뿐만 아니라, 개인 정보, 생체 인식 데이터, 재무 기록, 건강 기록, 개인 통신 및 기록물을 포함할 수 있다. 네트워크 연결된 디바이스는 포인트 오브 세일(point of sale)(POS) 단말기, 가스 펌프, ATM 등과 같이 개인에 의해 사용되는 공공적으로 공유되는 디바이스뿐만 아니라, 휴대폰, 태블릿, 노트북, 데스크탑, 파일 서버, 이메일 서버, 웹 서버, 데이터베이스, 개인 데이터 저장소, 클라우드 저장소, 인터넷 연결된 디바이스, 연결된 자동차를 포함한다.

[0103] 명백히, 보안 정보에 대해 무단 액세스를 시도하는 사이버 범죄자와 컴퓨터 해커가 범죄를 저지르고 있다. 불법적으로 얻어진 데이터가 개인 정보를 포함하고 있다면, 공격은 피해자의 개인 프라이버시의 침해이다. 그러나 역으로, 사이버 범죄에 대한 필요성 없이 프라이버시 침해가 발생할 수 있으며, 또한 실제로 막을 수도 없다. 오늘날의 네트워크 연결된 세계에 있어서, 개인의 정보의 무단 사용은 보안 침입의 필요성 없이 발생할 수 있다. 많은 경우에 있어서, 하나의 목적을 위해 데이터를 수집하는 회사는 다른 목적을 위해 데이터를 사용하고자하는 다른 클라이언트에게 자신의 데이터베이스를 판매할 수 있다. 심지어 마이크로소프트 구매 핫메일일지라도, 잠재적 클라이언트에게 스팸을 보내는데 관심이 있는 광고주에게 메일 목록이 판매된 것으로 잘 알려져 있다. 그러한 행동이 사이버 프라이버시 침해로 간주되어야 하는지의 여부는 의견의 문제로 남는다.

[0104] 인터넷 프라이버시, 컴퓨터 프라이버시, 및 사적 통신을 포함하는 "사이버 프라이버시"는 다른 사람과 정보의 수집, 저장, 표시, 또는 공유를 포함하여 그 사적인 그리고 개인의 정보 및 그 권리를 제어하기 위해, 개개인의 사적인 권리 또는 또는 의무를 포함한다. 개인 정보는 신장, 체중, 나이, 지문, 혈액형, 운전 면허증 번호, 여권 번호, 사회 보장 번호, 또는 그 이름을 알지 못하고 개개인을 식별하는데 유용한 임의의 개인 정보를 포함하

여, 개인 식별 정보를 포함할 수 있다. 미래에는 개인의 DNA 지도조차도 법적 기록물로 남을 수 있다. 개인 식별 정보 외에도, 비개인적 사적 정보에는 우리가 구입하는 옷의 브랜드, 자주 방문하는 웹 사이트, 담배를 피우는지, 술을 마시는지, 또는 총을 소유하는지, 어떤 종류의 차를 운전하는지, 우리가 인생에서 걸릴 수 있는 질병이 무엇인지, 우리 가족이 어떤 질병이나 질병의 병력을 가지고 있는지, 심지어 어떤 종류의 사람들이 우리에게 끌리는 지 등을 포함할 수 있다.

[0105] 이런 개인 정보는 개인 소득, 세금, 재산 증서, 범죄 기록, 교통 위반 및 소셜 미디어 사이트에 게시된 모든 정보와 관련된 공개 기록과 결합하여 이해 당사자를 위한 강력한 데이터 세트를 형성한다. 인구 통계, 개인, 금융, 생물 의학, 및 행동 정보를 캡처하고 패턴, 추세, 및 통계적 상관관계에 대한 데이터를 수집하는 대규모 데이터 세트를 의도적으로 수집하는 것은 "빅 데이터(big data)"로서 알려져 있다. 보험 회사, 헬스케어 제공업체, 제약 회사, 심지어는 의료 변호사를 포함하는 헬스케어 산업은 빅 데이터로서 저장된 개인 정보에 강력하게 관심을 갖고 있다. 자동차 및 소모품 회사도 마찬가지로 시장 전략 및 광고 예산을 관리하기 위해 이러한 데이터베이스에 대한 액세스를 원한다. 최근의 선거에서, 정치인조차도 유권자의 의견과 회피해야 할 정치적 쟁점을 더 잘 이해하기 위해 빅 데이터를 바라보기 시작했다.

[0106] 사이버 프라이버시의 문제는 오늘날 빅 데이터가 개인 정보(이미 표준 절차 임)를 캡처하고 있는지의 여부가 아니라, 상기 데이터 세트가 당신의 이름 또는 알지 못하더라도 당신을 식별할 수 있는 충분한 개인 신원 정보를 보유하고 있는지의 여부이다. 예를 들어, 본래 미국 정부는 일단 개인 의료 계정이 설정되었다면, 적정가 케어법안(Affordable Care Act)에 가입하기 위해 사용된 healthcare.gov 웹 사이트에 의해 수집된 개인 정보가 파괴될 것이라고 말했다. 그 후, 최근의 게시에서, 미국 정부를 위해 데이터 수집을 촉진시키는 제3의 회사는 수집한 데이터를 보유하고 사용할 수 있는 권리를 부여하는 정부 계약서에 이전에 서명했으므로, 미국 정부에 누설된 개인적인 사적 정보는 실제로 사적인 것이 아니라고 밝혔다.

[0107] 마지막으로, 유사한 기술적 방법을 사용하여 정부와 범죄 조직 모두에 의해 감시가 실시되고 있음을 언급해야만 한다. 범죄자들이 이러한 데이터를 수집 할 법적 권리가 분명히 없지만, 허가받지 않은 정부 감시의 사례는 더욱 애매하여, 나라마다 극적으로 다양하다. 예를 들어, 미국 NSA는 클라우드, 데이터베이스에 대한 액세스를 제공하기 위해 애플, 구글, 마이크로소프트 및 기타 업체에 반복해서 압력을 가했다. 정부 관리조차도 그들의 대화와 발표를 도청하고 가로챘다. 마이크로소프트의 한 부서 인 스카이프가 발신자의 콘텐츠를 모니터링하는지 묻는 질문에 스카이프 최고 정보 책임자(CIO)가 갑자기 "코멘트 없음"이라고 대답했다.

[0108] ***사이버 범죄 및 사이버 감시 방법*** - 사이버 보안의 주제에 초점을 맞추어, 사이버 범죄를 저지르고 보안 네트워크에 인가되지 않은 침입을 달성하는데 사용되는 다양한 맬웨어 및 해커 기술을 포함하는, 디바이스, 네트워크, 및 컴퓨터 데이터에 무단으로 액세스하기 위한 수많은 수단이 존재한다.

[0109] 예를 들어, 인터넷 연결된 태블릿을 사용하는 개인은 사무실 전화에 전화를 걸거나, TV에 메시지를 보내거나, 전화기로 라인 교환된 POTS 네트워크를 여전히 사용하는 나라의 친구에게 전화를 걸거나, 또는 웹 스토리지로부터 파일을 다운로드하거나, 또는 이메일 서버를 통해 이메일을 전송할 수 있다. 모든 애플리케이션이 인터넷의 정상적인 애플리케이션과 글로벌 상호 연결성을 나타내지만, 전체 네트워크를 통해 감시, 사이버 범죄, 사기, 및 신원 도용에 대해 많은 기회가 존재한다.

[0110] 예를 들어, 셀룰러 라디오 안테나 및 LTE 셀룰러 기지국을 통해 또는 단거리 무선 안테나 및 공용 WiFi 기지국을 통해 네트워크에 연결하는 태블릿에 대해, 인증되지 않은 침입자는 무선 링크를 모니터링할 수 있다. 마찬가지로, 셀룰러 링크를 통한 LTE 통화는 차단형 라디오 수신기 또는 스니퍼에 의해 모니터링되거나 "스니핑"될 수 있다. 동일한 스니퍼는 WiFi 링크를 모니터링하고 케이블 CMTS와 케이블 모뎀 사이에서 케이블 상의 수신 단부 상에서 조정될 수 있다.

[0111] 일부 경우에 있어서, LTE 통화는 해적 모조 타워(pirate faux tower)에 의해 차단되어, 태블릿과 셀룰러 타워 사이에서 전환된 통신 경로를 설정할 수 있다. 패킷 교환형 네트워크를 통해 라우터, 서버, 서버, 및 클라우드 스토리지로 송신된 통신은 중간자 공격에 종속될 수도 있다. 유선 탭은 PSTN 게이트웨이로부터 전화로의 POTS 라인 상의 통화 및 PBX 서버와 사무실 전화 사이의 협동 PBX 라인 상의 통화를 가로챌 수 있다.

[0112] 일련의 보안 침해를 통해, 스파이웨어는 그 자체를 태블릿 또는 노트북 상에, 라우터 상에, PSTN 브릿지 상에, 클라우드 스토리지 상에, 케이블 CMTS 상에, 또는데스크탑 컴퓨터 상에 설치할 수 있다. 트로이 목마 소프트웨어는 패스워드를 피싱하기 위해 자체를 태블릿 또는데스크탑 상에 설치할 수 있다. 웜은 특히 컴퓨터가 가능한 액티브 X 기능을 사용하는 마이크로소프트 운영 체제를 실행하는 경우, 데스크탑을 공격할 수도 있다. 마지막으

로, 서비스 공격의 거부를 론칭하기 위해, 바이러스는 서버, 데스크탑, 및 태블릿을 포함하는 네트워크-연결된 임의의 수의 디바이스를 공격할 수 있다.

[0113] 그에 따라, 맬웨어가 통신 네트워크 및 사회 기반 시설의 상이한 부분들에서 동작될 수 있고, 사이버 공격은 바이러스, 중간자 공격, 정부 감시, 및 서비스 공격의 거부를 포함할 수 있다. 통신 네트워크의 라스트 마일은 세 구역으로 분할된, 로컬 텔코/네트워크, 라스트 링크, 및 디바이스로 분할된 맬웨어 및 사이버 공격에 대해 심지어 더욱 광범위한 기회를 제안한다. 도시된 바와 같은 로컬 텔코/네트워크는 고속 유선 또는 광섬유 링크, 라우터, 케이블 CMTS, 케이블/광섬유, 케이블 모뎀, WiFi 안테나 및 LTE 라디오 네트워크를 포함한다. 네트워크의 이러한 부분에서, 라디오 스니퍼, 스파이웨어, 바이러스, 및 중간자 공격이 모두 가능하다.

[0114] 라스트 링크에 있어서, 디바이스에 대한 로컬 연결에서, 네트워크 연결은 스파이웨어, 라디오 스니퍼, 유선탭(wiretap), 및 모조 타워에 노출되는 유선 연결, WiFi 링크, 및 LTE/라디오 셀룰러 링크를 포함한다. 예를 들어 태블릿, 노트북, 데스크탑, 스마트폰, 스마트 TV, POS 단말기 등을 포함하는 디바이스 자체는 스파이웨어, 트로이 목마, 바이러스, 및 웜을 포함하는 많은 공격에 노출된다.

[0115] 이더넷 근거리 네트워크 상의 트래픽을 모니터링하기 위해 사용되는 디바이스, WiFi 데이터를 모니터링하기 위한 디바이스, 및 셀룰러 통신 감시를 위한 디바이스를 포함하는 이러한 감시 방법 및 스파이 디바이스는 상업 및 온라인 시장에서 용이하게 사용될 수 있다. 광섬유 클라우드 연결의 스니핑이 초기에 위협으로서 확인되지는 않았지만, 최근에 광통신에 대한 비-침입적 데이터 스니퍼가 출현하였고, 즉 광섬유를 끊을 필요가 없는 또는 그 정상적인 동작을 심지어 일시적으로 손상시킬 필요가 없는 데이터 스니퍼가 현재 존재한다.

[0116] 해킹 및 감시 방법을 사용하는 것 외에도, 휴대폰 대화 및 인터넷 통신을 모니터링하기 위해, 다양한 상업용 스파이웨어가 쉽게 사용될 수 있다. 오늘날, 상업적으로 이용 가능한 스파이웨어 프로그램은, 당신의 직원, 당신의 자녀, 및 당신의 배우자를 유익하게 감시하는 능력과 같은 많은 특징을 광고하고 있다. 이러한 특징의 세트는 사이버 프라이버시를 놀라울 정도로 설득력 있게 위반하는 많은 방법을 함께 포함하여, 전화, 사진 및 비디오, SMS/MMS 텍스트 메시지, 타사 인스턴트 메시징, 이메일, GPS 위치 추적, 인터넷 사용, 어드레스 북, 캘린더 이벤트, 도청, 제어 애플리케이션, 및 심지어 원격 제어 기능에 대한 감시를 포함하여 놀라울 정도로 포괄적이다. 실제로, 사이버 공격은 이제 너무 빈번해지고, 이들은 매일 추적된다. 사이버 공격을 시작하기 위해서는 일반적으로 다음과 같은 여러 단계 또는 기술의 조합이 필요하다.

[0117] * IP 패킷 스니핑

[0118] * 포트 심문

[0119] * 프로파일링

[0120] * 사기꾼

[0121] * 패킷 도용

[0122] * 사이버 감염

[0123] * 감시

[0124] * 해적 관리

[0125] ***IP 패킷 스니핑(Packet Sniffing)*** - 라디오 모니터링 디바이스를 사용하여, 사이버 범죄자는 사용자, 그 거래, 및 그 계정에 대한 중요한 정보를 얻을 수 있다. 패킷 스니핑에서, IP 패킷의 콘텐츠는 두 사용자 사이의 경로 어디에서나 얻을 수 있거나 또는 "스니핑"될 수 있다. 예를 들어, 사용자가 파일, 예를 들어 사진 또는 텍스트를 IP 패킷으로 그의 노트북으로부터 그 친구의 전화기로 송신할 때, 사이버 해적은 송신자의 라스트 링크를 가로챔으로써, 송신자의 로컬 네트워크를 가로챔으로써, 클라우드를 가로챔으로써, 수신자의 로컬 텔코를 가로챔으로써, 또는 수신자의 라스트 링크를 가로챔으로써, 임의의 많은 장소에서 IP 패킷을 발견할 수 있다. 가로챈 IP 패킷에 포함된 관찰 가능한 데이터는, 통신에 사용된 디바이스의 계층 2 MAC 어드레스, 수신측의 송신자의 계층 3 어드레스, 즉 전송 프로토콜, 예를 들어 UDP, TCP 등을 포함하는 패킷의 목적지를 포함한다. 또한, IP 패킷은 요청되는 서비스의 유형을 잠재적으로 정의하는 송신 및 수신 디바이스의 계층 4 포트 번호 및 데이터 파일 자체도 포함한다. 파일이 암호화되지 않았다면, 파일에 포함된 데이터는 사이버 해적에 의해서 직접 판독될 수도 있다.

[0126] 페이로드가 암호화되지 않았다면, 계정 번호, 로그인 순서, 및 패스워드와 같은 텍스트 정보가 판독될 수 있으

며, 또한 가치 있다면, 범죄 목적을 위해 도난당하거나 도용될 수 있다. 페이로드가 비디오 또는 그림문자(pictographic) 정보가 포함되어 있다면, 콘텐츠가 사용하는 계층 6 애플리케이션 포맷을 결정하기 위해 몇가지 추가 동작이 필요하지만, 그러나 일단 식별되었다면 상기 콘텐츠는 공개적으로 보여질 수 있거나, 게시될 수 있으며, 또는 아마도 통신 당사자 중 하나 또는 둘 모두를 협박하는데 사용할 수 있다. 이러한 사이버 공격은 사이버 해적이 개인적으로 통신 당사자를 알지 못하기 때문에 "중간자 공격"으로서 지칭된다.

[0127] 이미 기재된 바와 같이, 클라우드에서의 IP 패킷 라우팅이 예측할 수 없기 때문에, 클라우드의 모니터링이 더욱 어려운데, 그 이유는 사이버 해적이 IP 패킷의 중요한 정보가 처음 나왔을 때 이를 캡처해야만 하기 때문에, 이후의 패킷이 동일한 루트 및 스니핑된 패킷을 따를 수 없기 때문이다. 라스트 마일에서의 데이터를 가로채는 것은 동일한 대화를 포함하는 일련의 관련 패킷을 관찰할 더 큰 가능성을 가지며, 그 때문에 로컬 라우터는 패킷이 클라이언트 자신의 반송파 외부의 POP 에 도달할 때까지 로컬 라우터가 지정된 라우팅 표를 정상적으로 따르기 때문이다. 예를 들어 컴캐스트의 클라이언트는, 패킷이 컴캐스트의 도달 범위 및 클라이언트 서비스 영역을 넘어 지리적으로 이동할 때까지, 전적으로 컴캐스트 소유 네트워크를 사용하여 IP 패킷을 라우팅 체인까지 통과할 것이다.

[0128] 동일한 2개의 IP 어드레스 사이에서 패킷의 연속이 충분히 오랜 시간 동안 발생한다면, 전체 대화를 단편적으로 재생성할 수 있다. 예를 들어, SMS 텍스트 메시지가 라스트 마일에서 동일한 네트워크에 대해 통과되었다면, 사이버 해적은 IP 어드레스 및 포트 번호를 통해, 텍스트를 운반하는 다중 IP 패킷이 동일한 2개의 디바이스, 즉 휴대폰과 노트북 사이의 대화를 나타내는지를 식별할 수 있다. 따라서 계정 번호와 패스워드가 서로 다른 메시지로 텍스트가 기재되거나 또는 많은 패킷에 대해 불완전하게 보급된 경우라도, 패킷 식별자의 일관성은 여전히 사이버 해적이 대화를 재구성하고 계정 정보를 도용할 수 있게 한다. 일단 계정 정보가 도난당했다면, 이들은 해외 은행으로 돈을 이체하거나 또는 심지어 계좌 암호 및 보안 질문을, 즉 일시적으로 도용을 식별하는, 변경함으로써 계정 권한을 빼앗을 수 있다.

[0129] 페이로드가 암호화 되더라도, IP 어드레스 및 포트 #를 포함하는 나머지 IP 패킷은 암호화되지 않는다. 많은 수의 IP 패킷을 반복적으로 스니핑한 후, 충분한 계산 능력에 액세스할 수 있는 사이버 해적은 이들이 암호화 패스워드를 파괴할 때까지 잔인한 전단력에 의해 모든 조합을 체계적으로 시도할 수 있다. 일단 키가 파괴되었다면, 패킷 및 모든 후속 패킷이 해독되어 사이버 해적에 의해 사용될 수 있다. "패스워드 추측"에 의한 로그인 패스워드를 해독시킬 확률은 아래에 기재된 패킷 스니핑이 사용자 및 계정 "프로파일링"과 결합되면 크게 향상된다. "중간자 공격"에서 통신 디바이스는 사이버 해적이 이들에 직접 액세스할 수 없기 때문에 일반적으로 포함되지 않는다.

[0130] ***포트 심문(Port Interrogation)*** - 디바이스에 침입하는 다른 방법은 많은 계층 4 포트를 심문하고 임의의 요청이 응답을 수신하는지의 여부를 확인하기 위해 그 IP 어드레스를 사용하는 것이다. 일단 사이버 해적이 패킷 스니핑 또는 다른 수단으로부터 표적 디바이스의 IP 어드레스를 식별하면, 사이버 해적은 비보안 또는 개방 포트, 서비스 및 유지 관리 포트, 또는 애플리케이션 백도어를 찾기 위해서 디바이스 상의 포트에 대해 일련의 심문을 시작할 수 있다. 해커의 심문 프로그램이 모든 포트 #를 체계적으로 순환할 수 있는 반면에, 공격은 일반적으로 핑을 위한 포트 # 7, FTP를 위한 포트 # 21, 텔넷 터미널 에뮬레이션을 위한 포트 # 23, 간단한 이메일을 위한 포트 # 25 등과 같이 악명 높은 취약 포트에 집중한다. 디바이스가 응답하는 패킷을 해적이 송신할 때마다, 해적은 표적 디바이스의 운영 체제에 대해 더 많은 것을 학습한다.

[0131] 포트 심문 과정에서, 사이버 해적은 그 실제 신원을 노출시키길 원치 않으며, 그에 따라 그들은 개인적으로 추적될 수 없는, 메시지를 수신하기 위한 위장된 의사 어드레스를 사용할 것이다. 대안적으로, 사이버 범죄자가 도난당한 컴퓨터 및 계정을 사용할 수 있으므로, 다른 누군가가 표적 디바이스를 해킹하려고 시도하는 것처럼 보이며, 추적한다면, 조사자를 그들이 아닌 무고한 사람으로 되돌린다.

[0132] ***프로파일링(Profiling)*** - 사용자 및 계정 프로파일링은 암호를 해독시키고, 계정을 식별하고, 및 자산을 결정하기 위해, 사이버 해적이 공개적으로 사용 가능한 정보를 사용하여 표적, 그 계정, 그 개인 기록에 대해 학습하는 프로세스이다. 일단 해커가 스니핑이나 다른 방법을 사용하여 표적의 IP 어드레스를 얻었다면, 디바이스의 계정의 DNS 서버를 찾기 위해 추적 루트 유틸리티가 사용될 수 있다. 그 후, 인터넷 상의 "Who is" 기능을 이용함으로써, 계정 소유자의 이름이 발견될 수 있다. 프로파일링에서, 사이버 범죄자는 인터넷을 검색하여 계정 소유자의 모든 사용 가능한 정보를 수집한다. 정보의 소스는 재산 증서, 자동차 등록, 결혼 및 이혼, 세금 유치권, 주차 위반 티켓, 교통 위반, 범죄 기록 등과 같은 공공 기록을 포함한다. 많은 경우에 있어서, 대학 및 전문 사회로부터의 웹 사이트는 집 어드레스, 이메일 어드레스, 전화번호, 및 개인의 생년월일을 포함한다. 페

이스북, 링크드인, 트위터 및 기타와 같은 소셜 미디어 사이트를 조사함으로써, 사이버 범죄자는 창피한 사건, 가족의 비밀, 및 개인적인 적을 포함하여, 사진 및 비디오 파일뿐만 아니라, 가족 및 친구, 애완동물의 이름, 이전 집 주소, 동급생, 다른 사람의 주요 사건, 사진 등 중요한 정보를 수집할 수 있다.

[0133] 사이버 해적의 다음 단계는 이 프로필을 사용하여, 그 프로필에 기초하는 사용자의 암호를 "추측"하여, 표적 디바이스 및 동일한 개인의 다른 계정을 해킹하는 것이다. 일단 사이버 범죄자가 하나의 디바이스 패스워드를 해독하였다면, 사람들은 암기하기 쉽도록 암호를 재사용하는 경향이 있기 때문에, 이들이 다른 계정으로 침입할 가능성이 크다. 그 시점에서, 사람의 신원을 훔치고, 돈을 송금하고, 이들을 경찰 수사의 대상으로 삼아, 그 모든 재산을 훔쳐 다른 사람의 생명을 근본적으로 파괴하는 것이 가능하다. 예를 들어, 도난당한 계정으로부터 긴 암호 목록을 모으는 본 발명의 서두에 기재된 바와 같이, 사이버 범죄자는 동일한 패스워드와 로그인 정보를 사용하여 콘서트 및 스포츠 이벤트에 수백만 달러의 프리미엄 티켓을 불법적으로 구매하기 위해 동일한 패스워드를 사용했다.

[0134] ***사기범(imposters)*** - 인증된 사람 또는 디바이스인 것처럼 위장하여 통신 및 파일에 액세스하기 위해서 사이버 해적이 누군가를 사칭하거나 불법적으로 획득한 사이버 보안 자격을 사용할 때, 사이버 해적은 "사기범"으로서 행동한다. 사이버 공격의 사기범 유형은, 사이버 범죄자가 피해자의 계정을 빼앗기 위해서 개인의 계정에 관한 충분한 정보 또는 액세스를 갖고, 그들을 대신하여 메시지를 보내고, 해킹된 계정의 소유자로서 그들을 허위로 전달한다. 최근에, 예를 들어 발명가 중 한 명의 개인 친구가 "라인" 개인 메신저 계정을 해킹당했다. 계좌를 인계받은 후, 사이버 범죄자는 "그녀가 자동차 사고로 긴급 대부금으로 돈을 필요로 했다"고 허위 진술하고 돈을 어디로 보내라는 지령을 보내는 것을 포함하는 메시지를 그녀의 친구에게 전했다. 계정이 해킹당했다는 사실을 알지 못하고, 그녀의 친구의 요청이 실제라고 생각되어 즉각적으로 재정적 도움을 주었다. 의심을 피하기 위해 각 친구에게 보낸 요청은 1,000 달러 이하였다. 다행히 돈을 송금하기 직전에, 그녀의 친구 중 한 명이 그녀에게 유선 정보를 다시 확인하라고 전화를 걸었고 사기가 밝혀졌다. 전화가 없었다면, 그 누구도 요청이 사기범으로부터 왔음을 전혀 알지 못했을 것이며, 또한 라인 계정 소유자는 전신 송금이 보내졌거나 요청되었다는 것을 결코 알지 못했을 것이다.

[0135] 다른 형태의 허위 진술은 디바이스가 보안 권한을 부여 받고 서버 또는 다른 네트워크 연결된 디바이스와 정보를 교환할 수 있을 때 발생하며, 또한 어떻게든 사이버 해적 디바이스가 허가된 서버로 위장하고, 그에 의해서, 피해자의 디바이스는, 서버가 사기범이라는 것을 인식하지 못하고, 해적 서버에 파일 및 정보를 기꺼이 넘겨준다. 이 방법은 백업 클라우드가 사기범이라는 점을 제외하고는, 유명 인사가 아이클라우드로 개인 사진 파일을 백업하도록 유도하는데 사용되었다.

[0136] 사기의 다른 형태는 사람의 전화나 열린 브라우저에 물리적으로 액세스하는 사람이 이메일 송신, 전화 응답, 다른 사람의 계정이나 디바이스에서 텍스트 메시지 보내기와 같은 사기 행위를 수행할 때 발생한다. 수신 당사자는 이들이 알려진 디바이스 또는 계정에 연결되어 있어 해당 디바이스 또는 계정을 운영하는 사람이 소유자임을 전제로 한다. 사기는 페이스북에 난처한 댓글을 게시하는 친구와 같은 장난이거나 또는 누군가의 배우자가 개인 전화에 응답하거나 개인 성격의 개인 텍스트 메시지를 가로채는 보다 개인적인 성격을 띠고 있을 수 있다. 무단 액세스의 결과는 질투심, 이혼, 및 복수의 법적 절차로 나타날 수 있다. 사무실이나 카페에서 디바이스가 잠시 감시되지 않는 상태가 되면, 예를 들어 화장실에 가면, "감염"이라는 제목의 다음 섹션에서 설명하는 바와 같이, 사기범이 개인 정보 또는 회사 정보에 빠르게 액세스하거나, 허가되지 않은 이메일을 송신하거나, 파일을 전송하거나, 맬웨어의 일부 형태를 디바이스에 다운로드할 다른 위험이 있다.

[0137] 사기범-기반의 사이버 공격은 디바이스가 도난당한 경우에도 중요하다. 이러한 경우에, 디바이스가 로그아웃 되더라도, 도둑은 로그인 코드를 파괴하는데 충분한 시간을 할애한다. 컴퓨터에 있는 도난당한 디바이스를 찾아내고 사이버 해적이 디바이스에 처음 로그온 할 때 컴퓨터 파일을 지우는 "내 컴퓨터 찾기"기능은, 기술에 익숙한 범죄자들이 현재 셀룰러 또는 WiFi 연결이 없는 디바이스만 활성화한다는 것을 알고 있기 때문에 더 이상 동작하지 않는다. 이 위험은 특히 패스 라인 보안이 간단한 4자리 개인 ID 번호 또는 PIN 인 휴대폰의 경우에 특히 크다. 9999 가지 가능한 조합만 있기 때문에 PIN을 깨는 것은 시간 문제이다.

[0138] 디바이스를 안전하게 유지하기 위한 주요한 문제는 사기범에 대한 액세스를 방지하는 것이다. 사기범을 방지하는 것은 일정한 간격으로 사용자의 신원을 인증하고 필요한 정보와 권한 만 액세스할 수 있는 권한이 있는지 확인하는 강력한 수단을 요구한다. 디바이스 보안은 종종 체인에서 가장 약한 링크이다. 일단 디바이스의 보안이 무너졌다면, 강력한 네트워크 보안에 대한 고려할 가치가 없다.

[0139] ***패킷 하이잭킹(Packet Hijacketing)*** - 패킷 하이잭킹은 네트워크를 통한 정상적인 패킷 흐름이 적대적인 디바이

스를 통해 우회되는 사이버 공격을 포함한다.

[0140] 예를 들어, 라우터의 무결성이 사이버 해적으로부터의 사이버 공격에 의해 손상된 경우에, 라우터를 통과하는 IP 패킷이 개정된 IP 패킷으로 재작성될 수 있고, IP 패킷을 사이버 해적 디바이스의 다른 목적지 어드레스 및 포트 #로 전환할 수 있다. 이어서, 사이버 해적 디바이스는 IP 패킷의 페이로드로부터 필요로 하는 모든 정보를 얻고 IP 패킷의 페이로드의 콘텐츠를 변경할 수 있다. 사기성 페이로드는 임의의 수의 사기 범죄를 저지르고, 정보를 수집하고, 휴대폰에 맬웨어를 다운로드하는데 사용될 수 있으며, 이에 대해서는 이후의 "감염"항목에서 설명된다.

[0141] 이어서, 하이잭킹된 패킷은, 패킷이 새롭고 다른 경로를 통과하는 것을 제외하고, 원래의 IP 패킷의 소스 IP 어드레스와 같이 보이도록 재개조된다. 대안적으로, 하이잭킹된 IP 패킷은 손상된 라우터로 되돌아갈 수 있고 이어서 이전에서와 같이 클라우드로 송신될 수 있다. 패킷 하이잭킹의 범죄 이득을 최대화하기 위해, 사이버 해적은 패킷 하이잭킹에서 그들의 신원을 은폐할 필요가 있고, 그러한 이유로 IP 패킷의 실제 라우팅을 위장하고, 그에 따라 계층 3 ICMP 기능인 "추적 루트" 조차도 통신의 실제 경로를 식별하는데 어려움을 가질 것이다. 그러나 하이잭킹이 패킷 라우팅에서 현저한 지연을 부가하는 경우에, 비정상적인 대기 시간은 네트워크 운영자에 의해 즉각적으로 조사될 수 있다.

[0142] ***사이버 감염(Cyber-infections)*** - 사이버 공격의 가장 교활한 범주 중 하나는 정보를 수집하고, 사기를 치고, 트래픽을 재지향시키고, 다른 디바이스를 감염시키고, 시스템을 손상시키거나 차단하고, 또는 서비스 실패의 거부를 유발시키도록 이에 의해 표적 디바이스 또는 디바이스 내에 맬웨어를 설치하는 "사이버 감염"이다. 사이버 감염은 이메일, 파일, 웹 사이트, 시스템 확장, 애플리케이션 또는 네트워크를 통해 확산될 수 있다. 맬웨어의 하나의 일반적인 분류인 "스파이웨어"는 모든 종류의 처리 정보를 수집하여 이를 사이버 해적에 전달한다. "피싱"의 경우에, 친숙한 로그인 페이지처럼 보이는 웨(wen) 페이지나 애플리케이션 쉘이 계정 로그인 또는 개인 정보에 대한 정보를 묻고 사이버 해적에 정보를 전달한다. 다른 맬웨어 감염은 하드웨어를 제어할 수 있으며, 예를 들어 전술한 패킷 하이잭킹을 실행하도록 라우터를 제어한다. 이들 경우에 있어서, 사이버 해적은 그 자신의 목적을 위해 정보를 얻거나 이익을 제어하려고 한다.

[0143] 바이러스, 웜, 및 트로이 목마를 포함하는 다른 등급의 사이버-감염은 중요한 파일을 덮어쓰거나 또는 무의미한 기능을 반복적으로 실행하여, 디바이스가 정상적인 동작을 수행하는 것을 방지하도록 설계되었다. 기본적으로, 서비스를 거부하거나, 성능을 저하시키거나 디바이스를 완전히 죽인다. 이들 악의적인 감염은 본질적으로 파괴적이며, 악의의 목적을 위해서 사용되며, 그에 따라 경쟁 업체의 비즈니스가 정상적으로 동작하지 못하게 하거나, 또는 해커가 가능한지 확인하기 위해서 단순히 재미를 위한 동기에 기인한다.

[0144] ***감시(Surveillance)*** - 침입 및 감시는 사이버 범죄를 넘어선다. 이러한 경우, 개인 탐정이나 지인은 디바이스나 프로그램을 표적의 개인 디바이스에 설치하여 음성 대화, 데이터 교환, 및 위치를 모니터링하도록 고용되거나 강제된다. 대상이 알지 못하는 상태에서 탐정이 표적 디바이스에 일시적으로 액세스하여야 하기 때문에, 이는 잡힐 위험이 더 크다. 예를 들어, 휴대폰의 네트워크 액세스 권한을 복사할 수 있는 SIM 카드가 상업적으로 사용될 수 있지만, 동시에 표적의 통화 및 데이터 트래픽을 모니터링하는 사이버 범죄자에게 정보를 전송할 수 있다.

[0145] 감시의 다른 형태는, 카지노에 있는 것과 마찬가지로, 비밀의 비디오 카메라를 사용하여 사람의 모든 행동과 전화 통화를 모니터링하는 것을 포함한다. 비디오 모니터링을 통해, 로그인 과정 중 사용자의 키 입력을 관찰함으로써, 디바이스의 패스워드 또는 PIN을 간단하게 알 수 있다. 충분한 카메라가 제 위치에 있다면, 결국 로그인 프로세스가 기록된다. 의심의 여지없이 카메라 네트워크에 액세스하기 위해, 사이버 해적은 건물, 상점 또는 거리의 기존 카메라 감시 시스템을 해킹하고 다른 사람의 네트워크에 액세스하여 의심하지 않는 희생자의 행동을 모니터링할 수 있다. 비디오 감시와 패킷 스니핑의 조합은, 후속 사이버 공격을 시작하기 위한 보다 더 포괄적인 데이터 세트를 제공한다.

[0146] ***해적 관리(침입)(Pirate Administration(Infiltration)***-사이버 해적들이 정보를 얻기 위해 할 수 있는 다른 하나의 수단은 해킹하여 디바이스, 서버 또는 네트워크의 시스템 관리 권한에 대한 액세스 권한을 얻는 것이다. 따라서 하나의 사용자의 계정에 무단으로 액세스하기보다는, 시스템 관리자의 로그인을 해킹함으로써, 시스템 이용자가 알지 못하는 상태에서 사이버 해적은 상당한 액세스 및 권한을 이용할 수 있다. 시스템 관리자가 시스템의 경찰 역할을 하기 때문에, 본질적으로 그 범죄 행위를 포착할 사람은 아무도 없으며, 본질적으로 부패한 관리자가 있는 시스템 또는 네트워크에서는 경찰을 감독할 사람이 아무도 없다.

[0147] ***결론*** - 인터넷, 패킷 교환형 네트워크 및 7 계층 오픈 소스 이니셔티브 네트워크 모델의 거의 보편적인 채택으로 인한 편재성과 상호 운용성은 지난 20년 동안 전세계 통신이 비할 수 없을 정도로 확장되고 스마트폰으로부터 태블릿, 컴퓨터, 스마트 TV, 자동차, 가전제품 및 전구에 이르기까지 다양한 범위의 디바이스를 제공했다. 이더넷, 셀룰러, WiFi 및 케이블 TV 연결을 위한 기반으로 인터넷 프로토콜 또는 IP의 전 세계적인 채택은 통일된 통신뿐만 아니라 해커 및 사이버 범죄자가 가능한 많은 디바이스 및 시스템에 침입하려는 도전을 상당히 간단하게 만들었다. 현재의 통신 네트워크를 공격할 수 있는 많은 소프트웨어 및 하드웨어 방법을 감안한다면, 단일의 방어로서의 단일 보안 방법은 충분하지 않다. 대신에 모든 디바이스, 최종 링크, 로컬 텔코/네트워크 및 클라우드 네트워크를 보호하여 정교한 사이버 공격에 대한 그 보호를 보장하기 위해 체계적인 접근법이 요망되고 있다. 활용되는 방법은 QOS, 네트워크 대기 시간, 비디오 또는 음질을 희생시키지 않으면서 본질적인 사이버 보안 및 사이버 프라이버시를 제공해야만 한다. 암호화는 보안 통신 및 데이터 저장 분야에서 이러한 차세대 개발의 중요한 요소로 남아 있어야 하지만, 네트워크의 보안은 암호화 방법론에만 의존해서는 안 된다.

## *발명의 내용*

### *해결하려는 과제*

### *과제의 해결 수단*

[0148] 본 발명에 따라, (텍스트, 오디오, 비디오, 그래픽 및 모든 다른 종류의 디지털 정보 또는 파일을 포함하도록 광범위하게 정의된) 데이터는 보안 동적 통신 네트워크 및 프로토콜(SDNP) 네트워크 또는 "클라우드"를 통해 전송된다. "SDNP " 클라우드는 전 세계 어디에나 위치되는 서버 또는 다른 유형의 컴퓨터 또는 디지털 장비(통칭하여 여기에서는 "서버"로서 지칭됨) 상에 개별적으로 호스트된 "미디어 노드"로도 지칭되는 다수의"노드"를 포함한다. 2개 또는 그 이상의 노드가 단일 서버에 위치되는 것이 가능하다. 전형적으로, 데이터는 광섬유 케이블을 통해 운반되는 광에 의해, 라디오 또는 마이크로파 스펙트럼에서 라디오 전파(radiowave)에 의해, 구리선 또는 동축 케이블 상에 전도된 전기 신호에 의해, 또는 위성 통신에 의해 미디어 노드 사이에서 전송되지만, 본 발명은 디지털 데이터가 한 지점으로부터 다른 지점으로 전송되는 것을 광범위하게 의미한다. SDNP 네트워크는 SDNP 클라우드와 휴대폰, 태블릿, 노트북 및 데스크탑 컴퓨터, 모바일 소비자전자 기기 및 인터넷 등의 디바이스와 같은 클라이언트 디바이스 사이의 "라스트 마일" 링크뿐만 아니라, 사물 인터넷 디바이스 및 전자기기, 자동차, 및 다른 차량뿐만 아니라 SDNP 클라우드를 포함한다. 또한, 라스트 마일 통신은 휴대폰 타워, 가정용 케이블 또는 광섬유, 및 공공 WiFi 라우터를 포함한다. 라스트 마일에서, 클라이언트 디바이스와 가장 근거리의 셀 폰 타워 또는 다른 재-전송기 사이의 링크는 "라스트 링크"로 지칭된다.

[0149] SDNP 클라우드의 미디어 노드 사이 전송 시, 데이터는 고정된 또는 가변 길이일 수 있는 디지털 비트의 개별 스트링인 "패킷" 형태이며, 또한 데이터는 이하의 기술, 즉 스크램블링(scrambling), 암호화 또는 분할(splitting) 또는 그 역프로세스, 언스크램블링(unscrambling), 해독 및 혼합(주: 여기에 사용되는 바와 같이, 문맥에서 달리 표시하지 않는 한, "또는"이라는 단어는 결합적인(및/또는) 의미로 사용된다)을 사용함으로써 위장된다.

[0150] 스크램블링은 데이터 패킷 내의 데이터를 재정렬하는 것을 수반하며; 예를 들어, 패킷에서 그 순서로 나타나는 데이터 세그먼트 A, B 및 C는 시퀀스 C, A 및 B로 재배열된다. 스크램블링 동작의 반대는 "언스크램블링"으로서 지칭되고, 위의 예에서 A, B 및 C가 처음 등장한 순서에 대한 패킷 내에 데이터를 재배치하는 단계를 수반한다. 데이터 패킷을 언스크램블한 후 스크램블링하는 조합된 동작은 "재스크램블링(re-scrambling)"으로서 지칭된다. 이미 스크램블링된 패킷을 재스크램블링하는 경우, 상기 패킷은 이전의 스크램블링 동작과 동일한 또는 상이한 방식으로 스크램블될 수 있다.

[0151] 두 번째 동작인 "암호화"는 패킷의 데이터를 암호문(ciphertext)이라고 지칭되는 형식으로 인코딩하는 것으로, 이는 송신자 및 다른 인증된 사람, 그리고 그렇게 하기 위해 역동작-"해독"-을 수행해야만 하는 사람에 의해서만 이해될 수 있다. 암호문 데이터 패킷을 해독과 이를 다시 암호화하는 조합된 동작은, 전형적으로, 그러나 이를 이미 암호화하는데 사용된 방법과는 상이한 방법을 사용하는 것이 필수적이지는 않게, 여기에서는 "재암호화(re-encryption)"라고 지칭된다.

[0152] 세 번째 동작인 "분할"은 이름에서 알 수 있듯이 패킷을 2개 또는 그 이상의 작은 패킷으로 분할하는 것을 의미한다. 역동작인 "혼합(mixing)"은 둘 이상의 패킷을 단일 패킷으로 재조합하는 것으로서 정의된다. 이전에 분리

되고 그 후 혼합된 패킷을 분할하는 것은 이전의 분할 동작과 동일하거나 상이할 수 있다. 조작 순서는 역전 가능하며, 이에 따라 혼합에 의해 분할이 실행되지 않을 수 있으며, 또한 반대로 다중 입력을 하나의 출력으로 혼합하는 것은 분할하여 구성요소를 복구하기 위해 분할에 의해 이루어지지 않을 수 있다(주: 스크램블링 및 언스크램블링, 암호화 및 해독, 그리고 분할 및 혼합은 역프로세스이기 때문에, 이를 수행하는데 사용된 알고리즘 또는 방법에 대한 지식이 그 반대를 수행하기 위해 필요하다. 따라서 여기에서 특별한 스크램블링, 암호화, 또는 분할 알고리즘과 관련하여, 그 알고리즘에 대한 지식이 역프로세스를 수행하는 것을 허용한다는 인식해야 한다.)

[0153] 본 발명에 따라, SDNP 클라우드를 통과하는 데이터 패킷은 스크램블링되거나 또는 암호화되며, 또는 분할과의 조합 시 이들 동작 중 하나 또는 둘 모두를 거친다. 또한, 패킷을 해독하기가 더 어렵게 하거나 또는 패킷을 필요로 하는 길이에 맞추기 위해, 패킷에 "정크(junk)"(즉, 의미 없는) 데이터가 추가될 수 있다. 더욱이, 패킷은 파싱될 수 있으며, 즉 별개의 단편으로 분리될 수 있다. 컴퓨팅 언어에 있어서, 파싱한다는 것은 컴퓨터 언어 구문, 컴퓨터 명령, 또는 데이터 파일을 컴퓨터에 유용하게 사용할 수 있는 부분으로 나누는 것이다. 파싱은 명령 또는 데이터 패킷의 목적을 모호하게 하거나 또는 지정된 데이터 길이를 갖는 데이터 패킷으로 데이터를 배열하는데 사용될 수도 있다.

[0154] 데이터 패킷의 포맷이 인터넷 프로토콜에 따르더라도, SDNP 클라우드 내에서, 미디어 노드의 어드레스는 표준 인터넷 어드레스가 아니며, 즉 이들은 임의의 인터넷 DNS 서버에 의해 식별될 수 없다. 따라서 미디어 노드가 인터넷을 통해 데이터 패킷을 기술적으로 수신할 수는 있어도, 상기 미디어 노드는 어드레스를 인식하지 못하거나 질의에 응답하지 않는다. 더욱이, 인터넷 사용자가 미디어 노드에 접촉하더라도, 그들은 미디어 노드 내의 데이터가 SDNP 미디어 노드로서 필요한 식별 자격 증명이 없는 사기꾼으로 미디어 노드를 인식할 수 있기 때문에, 미디어 노드 내부의 데이터에 액세스하거나 검사할 수 없다. 특히, 미디어 노드가 SDNP 네임 서버 또는 이와 그 동등한 기능의 적격 서버에서 실행중인 유효한 SDNP 노드로 등록되지 않는 한, 그 노드로부터 다른 SDNP 미디어 노드로 송신된 데이터 패킷은 무시되고 폐기될 것이다. 유사한 방식으로, SDNP 네임 서버에 등록된 클라이언트만 SDNP 미디어 노드에 접촉할 수 있다. 등록되지 않은 서버와 마찬가지로, 등록된 SDNP 클라이언트 이외의 소스로부터 수신된 데이터 패킷은 무시되어 즉시 폐기될 것이다.

[0155] "단일 루트"로서 지칭된 비교적 간단한 실시예에 있어서, 데이터 패킷은 SDNP 클라우드에서 일련의 미디어 노드를 통해 단일 경로를 횡단하며, 이는 이것이 클라우드에 들어가는 미디어 노드에서 스크램블링되고, 또한 패킷이 클라우드를 나가는 미디어 노드에서 언스크램블링된다(이들 두 노드는 "게이트웨이 노드" 또는 "게이트웨이 미디어 노드"로서 지칭된다). 약간 더 복잡한 실시예에 있어서, 패킷은 이전의 미디어 노드에서 사용된 바와는 상이한 스크램블링 방법을 사용하여 각 미디어 노드에서 재스크램블링된다. 다른 실시예에 있어서, 패킷은 이것이 클라우드에 들어가는 게이트웨이 노드에서 암호화되고 그리고 이것이 클라우드를 나가는 게이트웨이 노드에서 해독되며, 또한 상기 패킷은 클라우드에서 통과하는 각 미디어 노드에서 재암호화될 수 있다. 주어진 노드가 패킷을 스크램블링하거나 암호화할 때마다 동일한 알고리즘을 사용하기 때문에, 이 실시예는 "고정"스크램블링 및 암호화로서 기재된다.

[0156] 패킷이 2개 또는 그 이상의 동작을 받는 경우, 예를 들어 스크램블링되고 암호화되는 경우, 역동작은 바람직하게는 동작 자체의 반대 순서로, 즉 역순으로 수행된다. 예를 들어, 패킷이 스크램블링되고 그 후 미디어 노드를 떠나기 전에 암호화되었다면, 이는 먼저 해독되고 그 후 이것이 이하의 미디어 노드에 도착하였을 때 언스크램블링된다. 상기 패킷은 미디어 노드 내에 있는 동안에만 그 본래의 형태로 재생성된다. 패킷이 미디어 노드 사이로 전송되는 동안, 이는 스크램블링되거나, 분할되거나, 혼합되거나, 또는 암호화된다.

[0157] "다중 루트" 데이터 전송으로서 지칭되는 다른 실시예에 있어서, 패킷은 게이트웨이 노드에서 분리되고, 또한 결과적인 다중 패킷은 일련의 "병렬" 경로로 클라우드를 횡단하며, 게이트웨이 노드를 제외하고 그 어떤 경로도 다른 경로와 미디어 노드를 공유하지 않는다. 다중 패킷은 통상적으로 출구 게이트웨이 노드에서 본래의 패킷을 재생성하도록 혼합된다. 따라서 해커가 단일 패킷의 의미를 이해할 수 있더라도, 그들은 전체 메시지의 일부만 가질 것이다. 상기 패킷은 이것이 분할되기 전에 또는 후에 게이트웨이 노드에서 스크램블링되고 암호화될 수도 있으며, 상기 다중 패킷은 그들이 통과하는 각각의 미디어 노드에서 재스크램블링되거나 재암호화될 수 있다.

[0158] 다른 실시예에 있어서, 패킷은 SDNP 클라우드에서 오직 단일 경로 또는 일련의 병렬 경로를 통해 이동하지 않으며, 오히려 패킷은 다수의 경로를 통해 이동할 수 있으며, 이들 중 다수는 서로 교차한다. 이 실시예에 가능한 경로의 그림이 메시(mesh)를 닮았기 때문에, 이는 "메시형 전송(meshed transport)"으로 지칭된다. 전술한 실시예에서처럼, 패킷은 이들이 SDNP 클라우드에서 개별적인 미디어 노드를 통과할 때, 스크램블링되고,

암호화되고, 그리고 분할되거나 또는 혼합될 수 있다.

[0159] SDNP 네트워크를 통한 패킷의 경로는, 시그널링 기능에 의해 결정되며, 이는 전용 시그널링 서버 상에서 동작하는 별도의 시그널링 노드에 의해 미디어 노드 자체의 세그먼트 또는 바람직하게는 "이중 채널"로 또는 "3중 채널" 실시예로 수행될 수 있다. 상기 시그널링 기능은 네트워크의 조건(예를 들어, 전파 지연) 및 통화의 우선순위와 긴박성에 기초하여 이것이 전송 클라이언트 디바이스(예를 들어, 휴대폰)를 떠날 때 각각의 패킷의 루트를 결정하고, 이것이 패킷을 수신하는 루트를 따라 각각의 미디어 노드를 알려주며, 또한 이를 전송할 노드를 명령한다. 각각의 패킷은 태그에 의해 식별되며, 상기 시그널링 기능은 각각의 미디어 노드가 이것이 송신하는 각 패킷 노드에 어떤 태그를 적용할지를 명령한다. 일 실시예에 있어서, 상기 데이터 태그는 SDNP 헤더 또는 서브 헤더에, 서브-패킷을 식별하는데 사용된 각각의 데이터 서브-패킷에 첨부된 데이터 필드를 포함한다. 각각의 서브-패킷은 패킷에서 지정한 데이터 "슬롯"에 저장된 하나 또는 다중 소스로부터 데이터 세그먼트를 포함할 수 있다. 임의의 2개의 미디어 노드 사이로 데이터 전송 중 하나의 큰 데이터 패킷 내에 다중 서브-패킷이 존재할 수 있다.

[0160] 라우팅 기능은 분할 및 혼합 기능과 정렬되는데, 그 이유는 일단 패킷이 분할되면, 분할된 각각의 서브-패킷의 각각의 경로가 결정되어야 하고, 서브-패킷이 재조합되는 노드가 그들을 혼합하도록 명령을 받아야만 하기 때문이다. 패킷은 다중 루트 실시예에서처럼 일단 분할되고 나서 혼합될 수 있으며, 또는 SDNP 네트워크를 통해 게이트웨이 노드를 나감에 따라 여러 번 분할되고 혼합될 수 있다. 어떤 노드에서 패킷이 분할될 것인지, 얼마나 많은 서브-패킷이 분할될 것인지, 서브-패킷의 각 경로 및 본래의 패킷을 재생성하기 위해 어떤 노드에서 서브-패킷이 혼합될 것인지의 결정은 이것이 별도의 시그널링 서버에 의해 수행되는지의 여부와는 관계없이 모두 시그널링 기능의 제어 하에 있다. 분할 알고리즘은 통신에서 어느 데이터 세그먼트가 각각의 서브-패킷에 포함될 것인지, 그리고 서브-패킷의 데이터 세그먼트의 순서 및 위치를 지정할 수 있다. 혼합 알고리즘은 본래 패킷을 재생성하기 위해 서브-패킷이 혼합된 노드에서 이 프로세스를 역으로 수행한다. 물론, 시그널링 기능에 의해 그렇게 지시되었다면, 그 노드는 또한 분할 프로세스가 발생하는 시간 또는 상태에 대응하는 상이한 분할 알고리즘에 따라 패킷을 다시 분할할 수 있다.

[0161] 미디어 노드가 시그널링 기능에 의해, 네트워크를 통해 "다음 홉(hop)"상의 특별한 목적지 미디어 노드에 복수의 패킷을 전송하도록 명령 받았을 때, 이들 패킷은 분할 패킷(서브-패킷)인지, 또는 이들이 상이한 메시지에 속하는지, 미디어 노드는 특히 다중 서브-패킷이 그들의 다음 홉에 대한 공통 목적지 미디어 노드를 공유할 때(단일 어드레스에 대해 의도된 글자 그룹을 박스 내에 두고 상기 박스를 어드레스로 보내는 우체국과 유사하게), 패킷을 단일의 큰 패킷으로 결합할 수 있다.

[0162] 본 발명의 "동적"실시예에 있어서, SDNP 클라우드의 개별적인 미디어 노드는 이들을 통과하는 연속적인 패킷 상에서 동일한 스크램블링, 암호화, 또는 분할 알고리즘 또는 방법을 사용할 수 없다. 예를 들어, 주어진 미디어 노드는 특별한 스크램블링, 암호화 또는 분할 알고리즘을 사용하여 하나의 패킷을 스크램블, 암호화 또는 분할하고, 그 후 다른 스크램블링, 암호화, 또는 분할 알고리즘을 사용하여 다음 패킷을 스크램블, 암호화, 또는 분할할 수 있다. "동적" 동작은 해커가 당면할 수 있는 어려움을 크게 증가시키는데, 그 이유는 그들이 패킷의 의미를 이해할 수 있는 짧은 시간(예를 들어, 100 msec)만 가지고 있기 때문이며, 또한 그들이 성공했다고 해도, 그 지식의 유용성은 수명이 짧을 것이다.

[0163] 동적 실시예에 있어서, 각각의 미디어 노드는 "DMZ 서버"로서 알려진 것과 관련이 있으며, 이는 데이터 전송 포트로부터 격리된 노드의 부분으로서 관찰될 수 있으며, 또한 이는 미디어 노드가 나가는 패킷에 적용할 수 있는 가능한 스크램블링, 암호화 및 분할 알고리즘의 목록 또는 표("선택기(selector)")를 포함하는 데이터베이스를 갖고 있다. 상기 선택기는 "공유된 비밀"로서 지칭되는 정보 본문의 일부인데, 그 이유는 정보는 미디어 노드에도 알려지지 않았으며, 또한 모든 DMZ 서버는 지정된 시점에 동일한 선택기를 사용하기 때문이다.

[0164] 미디어 노드가 스크램블링된 패킷을 수신할 때, 동적 실시예에 있어서, 이는 또한 패킷을 언스크램블링하는데 어떤 알고리즘이 사용될 것인지를 수신 노드에 표시하는데 사용되는 "시드(seed)"를 수신한다. 시드는 그 자체로 의미가 없지만 그러나 패킷이 종래의 미디어 노드에 의해 스크램블링된 시간과 같이 끊임없이 변화하는 상태에 기초하고 있는 위장된 수치이다. 상기 종래의 노드가 패킷을 스크램블했을 때, 그 관련 DMZ 서버는 상태에 기초하여 시드를 생성했다. 물론, 그 상태는 패킷을 스크램블링하는데 사용된 알고리즘의 선택 시 그 관련 DMZ 서버에 의해 사용되었으며, 이는 패킷을 어떻게 스크램블할지에 대한 명령의 형태로 송신 미디어 노드로 송신되었다. 따라서 상기 송신 노드는 패킷을 스크램블링하는 방법에 관한 명령과 다음 미디어 노드로 송신될 시드를 모두 수신했다. DMZ 서버 내에서 동작하는 시드 생성기는 프로세스가 실행될 때의 상태에 기초한 알고리즘을 사

용하여 시드를 생성하였다. 시드 생성기 및 그 알고리즘이 미디어 노드의 공유된 비밀 중 일부이더라도, 생성된 시드는 수치 시드가 의미를 갖지 않는 알고리즘에 액세스하지 않기 때문에 비밀이 아니다.

[0165] 따라서 패킷의 루트 상의 다음 미디어 노트는 스크램블링된 패킷 및 상기 패킷과 관련된 상태로부터 유도된 시드(예를 들어, 이것이 스크램블링된 시간)를 수신한다. 상기 시드는 패킷 자체에 포함될 수 있거나, 또는 패킷과 동일한 루트를 따라 또는 시그널링 서버를 통하는 것과 같은 일부 다른 경로를 통해 패킷 전에 수신 노드로 전송될 수 있다.

[0166] 이것이 시트를 수신하는 방법과는 관계없이, 상기 수신 노드는 시드를 DMZ 서버로 송신한다. 그 DMZ 서버가 공유 비밀의 일부이며 따라서 송신 노드의 DMZ 서버에서의 선택기와 동일한 스크램블링 알고리즘의 선택기 또는 표를 가지고 있기 때문에, 이는 패킷을 스크램블링하는데 사용되었던 알고리즘을 식별하기 위해 상기 시드를 사용할 수 있으며, 또한 패킷을 어떻게 언스크램블할지를 수신 노드에 명령할 수 있다. 따라서 상기 수신 노드는 그 언스크램블링된 형태로 패킷을 재생성하며, 이에 따라 본래의 데이터를 복원한다. 전형적으로, 상기 패킷은 다른 노드로 전송되기 전에 다른 스크램블링 알고리즘에 따라 다시 스크램블될 것이다. 만일 그렇다면, 상기 수신 노드는 스크램블링 알고리즘 및 시드를 획득하기 위해 DMZ 서버와 협력하고, 프로세스는 반복된다.

[0167] 따라서 패킷이 SDNP 네트워크를 통해 진행됨에 따라, 이는 각각의 노드에 의해 상이한 스크램블링 알고리즘에 따라 스크램블링되며, 다음 노드가 패킷을 언스크램블링할 수 있게 하는 새로운 시드가 각 노드에서 생성된다.

[0168] 본 발명의 대안적인 실시예에 있어서, 실제 상태(예를 들어, 시간)가 노드 사이에 전송될 수 있다(즉, 송신 노드는 수신 노드에 시드를 전송할 필요가 없다). 송신 및 수신 미디어 노드 모두와 관련된 DMZ 서버는 주어진 시점에서 동일한 알고리즘을 포함하는 은폐 숫자 생성기(다시 말하면, 공유된 비밀의 일부)를 포함한다. 송신 노드와 관련된 DMZ 서버는, 은폐 숫자와 은폐 숫자를 발생시켜 가능한 스크램블링 알고리즘의 선택자 또는 표로부터 스크램블 알고리즘을 결정하기 위해, 상태를 사용한다. 전송 노드는 상태를 수신 노드로 전송한다. 시드와 달리, 은폐 숫자는 네트워크를 통해 절대 전달되지 않지만, 그러나 미디어 노드와 그 DMZ 서버 사이에는 독점적인 사적 통신이 유지된다. 수신 미디어 노드가 들어오는 데이터 패킷의 상태를 수신하였을 때, 은폐 숫자 생성기 및 그 관련 DMZ 서버는 동일한 은폐 숫자를 발생시키기 위해 상태를 사용하며, 이는 그 후 패킷의 언스크램블링에 사용될 알고리즘을 식별하기 위해 선택기 또는 표에 사용된다. 상기 상태는 패킷에 포함될 수 있거나 또는 패킷 전에 또는 일부 다른 경로를 통해 송신 노드로부터 수신 노드로 전송될 수 있다.

[0169] 동적 암호화 및 분할에 사용된 기술은 동적 스크램블링에서 사용된 기술과 유사하지만, 그러나 동적 암호화에서는 시드 대신에 "키"가 사용된다. DMZ 서버에 의해 보유된 공유 비밀은 암호화 및 분할 알고리즘 및 키 생성기의 선택기 또는 표를 포함한다. 대칭 키 암호화의 경우, 송신 노드는 패킷을 암호화하는데 사용된 알고리즘을 식별하고 이에 따라 파일을 해독하기 위해, 수신 노드의 DMZ 서버에 의해 사용된 수신 미디어 노드에 키를 전송한다. 비대칭 키 암호화의 경우에, 정보를 요청하는 미디어 노드, 즉 수신 노드는 먼저 송신될 데이터 패킷을 포함하는 노드에 암호화 키를 보낸다. 그 후, 송신 미디어 노드는 그 암호화 키에 따라 데이터를 암호화한다. 암호화 키를 생성하는 수신 미디어 노드만이 대응하는 해독 키, 및 암호화 키를 사용하여 생성된 암호문을 해독하는 능력을 보유한다. 중요하게도, 비대칭 암호화에서, 암호화를 위해 사용되는 암호화 키에 대한 액세스는 데이터 패킷을 해독하는 방법에 대한 임의의 정보를 제공하지 않는다.

[0170] 분할의 경우, 패킷이 분리된 미디어 노드는 결과적인 서브-패킷이 혼합될 미디어 노드에 시드를 전송하고, 또한 혼합 노드와 관련된 DMZ 서버는 분할 알고리즘 및 이에 따라 서브-패킷을 혼합 시 사용될 알고리즘을 식별하기 위해 그 시드를 사용한다.

[0171] 전술한 바와 같이, 이중 또는 3중 채널 실시예에 있어서, 시그널링 기능은 시그널링 서버로서 알려진 별도의 서버 그룹에서 동작하는 시그널링 노드에 의해 수행된다. 이러한 실시예에 있어서, 시드 및 키는 송신 미디어 노드로부터 수신 미디어 노드로 직접 송신하는 대신에 시그널링 서버를 통해 전송될 수 있다. 따라서 송신 미디어 노드는 시그널링 서버에 시드 또는 키를 송신할 수 있고, 상기 시그널링 서버는 상기 시드 또는 키를 수신 미디어 노드에 포워딩할 수 있다. 전술한 바와 같이, 시그널링 서버는 패킷의 경로를 설계하는 역할을 하므로, 시그널링 서버는 각 패킷이 지향되는 다음 미디어 노드를 알고 있다.

[0172] 해커가 되는 것을 더 어렵게 하기 위해, 선택자에서 가능한 스크램블, 분할, 또는 암호화 방법의 목록 또는 표는 특별한 시드에 대응하는 방법 또는 키를 바꾸는 방식으로 주기적으로(예를 들어, 시간별로 또는 일별로) "셔플"될수 있다. 따라서 제1 일에 시간(t1)에 생성된 패킷에 주어진 미디어 노드에 의해 적용되는 암호화 알고리즘은 제2 일에 동일한 시간(t1)에 생성된 패킷에 이것이 적용하는 암호화 알고리즘과는 상이할 수 있다.

[0173] 각 DMZ 서버는 전형적으로 동일한 "서버 팜"에서 하나 또는 그 이상의 미디어 노드와 물리적으로 연관되어 있다. 전술한 바와 같이, 미디어 노드는 그 관련 DMZ 서버에 시드 또는 키를 제공함으로써(예를 들어, 패킷이 생성된 시간 또는 상태에 기초하여) 이것이 수신된 패킷에 무엇을 해야 할지에 대한 명령을 요청할 수 있지만, 그러나 미디어 노드는 공유된 비밀 또는 DMZ 서버 내의 임의의 다른 데이터 또는 코드에 액세스할 수 없다. DMZ 서버는, 미디어 노드가 패킷을 언스크램블링, 해독, 또는 혼합할 때 사용해야만 하는 방법을 결정하기 위해, 시드 또는 키를 사용함으로써 이러한 요청에 응답할 수 있다. 예를 들어, 패킷이 스크램블링되고 미디어 노드가 이를 언스크램블링하는 방법을 알기를 원한다면, 상기 DMZ 서버는 시드에 해당하는 지정 알고리즘을 찾기 위해, 스크램블 알고리즘 목록(또는 선택자)을 조사할 수 있다. 그 후, DMZ는 그 알고리즘에 따라 패킷을 언스크램블링하도록 미디어 노드에 지시한다. 즉, 미디어 노드는 시드 또는 키에서 실시되는 질의를 DMZ 서버에 전송하고, DMZ 서버는 이들 질의에 지침으로 응답한다.

[0174] 미디어 노드가 인터넷을 통해 액세스할 수 있지만(이들이 DNS 인식된 IP 어드레스를 갖고 있지 않아도), 상기 DMZ 서버는 와이어 또는 광섬유를 통해 네트워크 연결된 미디어 서버에 오직 로컬 네트워크 연결을 갖는 인터넷으로부터 완전히 격리된다.

[0175] "단일 채널" 실시예에 있어서, 시드 및 키는 데이터 패킷 자체의 일부로서 송신 미디어 노드와 수신 미디어 노드 사이에서 송신되거나, 이들은 동일한 루트상의 데이터 패킷 이전에 데이터 패킷으로서 분리 패킷에서 전송될 수 있다. 예를 들어, 패킷을 암호화할 때, 미디어 노드 # 1은 암호화가 수행된 시간에 기초하여 암호화 키를 패킷에 포함할 수 있다. 패킷이 미디어 노드 # 2에 도착하였을 때, 미디어 노드 # 2는 키를 그 관련 DMZ 서버로 전송하고, DMZ 서버는 그 선택기에서 해독 방법을 선택하고 해독을 수행하기 위해, 키를 사용할 수 있다. 미디어 노드 # 2는 미디어 노드 # 3으로 전송하기 전에 패킷을 다시 암호화해야 하는 방법을 DMZ 서버에 요청할 수 있다. 다시, 상기 DMZ 서버는 선택기와 상의하여, 패킷 암호화 시 어떤 방법을 사용해야 할 지를 미디어 노드 # 2 에 알려주며, 그리고 미디어 노드 # 2 에 암호화 방법에 대응하는 상태를 반영하는 키를 전달한다. 미디어 노드 # 2는 암호화를 수행하고 암호화된 패킷 및 키(별도로 또는 패킷의 일부로서)를 미디어 노드 # 3에 전송한다. 그 후, 키는 패킷을 해독하기 위해 미디어 노드 # 3 에 의해 유사한 방식으로 사용될 수 있다. 결과적으로 해커가 패킷을 해독하는데 사용할 수 있는 단일의 고정 해독 방법은 없다.

[0176] 시드 또는 키에 실시될 스크램블링 암호화 또는 분할 방법의 결정 요인으로서 상기 예에서의 시간 또는 동적 "상태" 조건의 사용은 단지 예시적일 뿐이다. 임의의 변화하는 매개변수, 예를 들어 패킷이 통과 한 노드의 수는 사용될 지정 스크램블링, 암호화, 또는 분할 방법을 선택하기 위해 시드 또는 키의 "상태"로서 사용될 수도 있다.

[0177] "이중 채널" 실시예에 있어서, 시드 및 키는 미디어 노드 사이에서 직접 전송되기 보다는, 시그널링 서버로 이루어진 제2 "명령 및 제어" 채널을 통해 미디어 노드 사이로 전송될 수 있다. 시그널링 노드는 또한 라우팅 정보를 미디어 노드에 제공하고, 또한 패킷이 다른 패킷으로 어떻게 쪼개지거나 혼합되는지 패킷 루트를 따라 미디어 노드에 알릴 수도 있으며, 또한 이들은 다음 미디어 노드(들)가 패킷(들)을 인식할 수 있도록 각 미디어 노드에 식별 "태그"를 적용하여 전송된다. 시그널링 서버는 바람직하게는 주어진 미디어 노드에 네트워크를 통과하는 패킷의 최종 및 다음 미디어 노드만 공급한다. 개별 미디어 노드는 SDNP 클라우드를 통해 패킷의 전체 루트를 알 수 없다. 일부 실시예에 있어서, 라우팅 기능은 2개 또는 그 이상의 시그널링 서버 사이에서 분할될 수 있으며, 하나의 시그널링 서버는 특별한 미디어 노드에 대한 루트를 결정하고, 제2 시그널링 서버는 그로부터 다른 미디어 노드로의 그리고 출구 게이트웨이 노드로의 루트를 결정한다. 이러한 방식으로, 단일의 시그널링 서버는 데이터 패킷의 완전한 라우팅을 알지 못한다.

[0178] "3중 채널" 실시예에 있어서, "네임 서버"라 불리는 서버의 제3 그룹은 SDNP 클라우드 내의 요소를 식별하고 또한 SDNP 클라우드에 연결된 디바이스 및 그 대응하는 IP 또는 SDNP 어드레스에 관한 정보를 저장하는데 사용된다. 또한 상기 네임 서버는 SDNP 클라우드의 미디어 노드를 지속적으로 모니터링하여, 클라우드의 모든 미디어 노드의 조합 사이에 활성 미디어 노드의 현재 목록과 전파 지연 표를 유지한다. 통화를 위치시키는 첫 번째 단계에서, 태블릿과 같은 클라이언트 디바이스는 IP 패킷을 네임 서버에 송신하여, 목적지 또는 사람이 통화되기 위한 어드레스 및 기타 정보를 요청한다. 또한, 디바이스가 클라우드 상에 처음 연결, 예를 들어 등록할 때마다 별도의 전용 네임 서버가 제1 접촉으로서 동작하는데 사용된다.

[0179] 보안상 추가적인 이점으로서, 다른 선택기, 시드 및 키 생성기, 그리고 다른 공유 비밀을 갖는 별도의 보안 "구역"이 하나의 SDNP 클라우드 내에 설정될 수 있다. 인접한 구역은 브릿지 미디어 노드에 의해 연결되며, 이는 두 구역의 공유 비밀을 보유하고 또한 한 구역의 규칙에 따라 포맷된 데이터를 다른 구역에 대한 규칙에 따라

서식이 지정된 데이터로 변환하거나 또는 그 역으로 변환할 수 있다.

[0180] 유사하게, 상이한 서비스 제공자에 의해 호스트된 상이한 SDNP 클라우드 사이의 통신을 위해, 각 클라우드의 인터페이스 브릿지 서버 사이에 전이중(즉, 양방향) 통신 링크가 형성된다. 각 인터페이스 브릿지 서버는 각 클라우드에 대해 관련의 공유 비밀 및 기타 보안 항목에 액세스할 수 있다.

[0181] 개시된 발명의 중요한 이점은, SDNP 네트워크에서 제어의 단일 지점이 없고 또한 주어진 통신이 어떻게 발생하는지 또는 그것이 어떻게 동적으로 변할 수 있는지에 대해 완전한 그림이 네트워크의 노드 또는 서버에 없다는 점이다.

[0182] 예를 들어, 시그널링 서버 상에서 실행되는 시그널링 노드는 통신이 발생하는 루트(또는 경우에 따라서는 오직 일부 경로만)를 알고 있지만, 그러나 이들은 통신되고 있는 데이터 콘텐츠에 액세스하지 못하고, 그리고 실제 발신자 또는 클라이언트 누군지를 알지 못한다. 더욱이, 시그널링 노드는 미디어 노드의 DMZ 서버의 공유 비밀에 액세스할 수 없으므로, 전송 중인 데이터 패킷이 암호화, 스크램블, 분할, 또는 혼합되는 방식을 알지 못한다.

[0183] SDNP 네임 서버는 발신자의 실제 전화번호 또는 IP 어드레스를 알고 있지만, 그러나 통신 중인 데이터나 또는 다양한 패킷 및 서브-패킷의 라우팅에 액세스할 수 없다. 시그널링 노드와 마찬가지로, 상기 네임 서버는 미디어 노드의 DMZ 서버의 공유 비밀에 액세스하지 않으므로, 전송 중인 데이터 패킷이 암호화, 스크램블, 분할, 또는 혼합되는 방법을 알지 못한다.

[0184] 실제로 미디어 콘텐츠를 전송하는 SDNP 미디어 노드는, 통신하는 발신자가 누구인지를 알지 못하며 또한 다양한 단편화된 서브-패킷이 SDNP 클라우드를 통해 취하고 있는 루트를 알지 못한다. 실제로, 각각의 미디어 노드는 도착할 데이터 패킷(그 태그 또는 헤더에 의해 식별되는), 및 이들을 다음에 전송할 곳, 예를 들어"다음 홉"만 알고 있지만, 그러나 상기 미디어 노드는 데이터가 암호화되는, 스크램블링되는, 혼합 또는 분할되는 방법을 알지 못하며 또한 상태, 수치 시드, 또는 키를 사용하여 알고리즘을 선택하거나 파일을 해독하는 방법을 알고 있지 않다. 들어오는 데이터 패킷의 데이터 세그먼트를 올바르게 처리하는데 요구되는 노하우는 그 공유 비밀, 네트워크를 통해 또는 미디어 노드 자체에 의해 액세스할 수 없는 알고리즘을 사용하여 DMZ 서버에만 알려져 있다.

[0185] 개시된 본 발명의 다른 독창적인 양태는, 네트워크 대기 시간을 줄이고 전파 지연을 최소화하여 데이터 패킷의 크기를 제어함으로써 보다 우수한 품질의 서비스(QoS)를 제공하고 에코 또는 누락된 통화를 제거할 수 있는 능력, 즉 하나의 고 대역폭 연결에 의존하기보다 클라우드를 통해 보다 작은 데이터 패킷을 병렬로 전송하는 것이다. SDNP 네트워크의 동적 라우팅은 네트워크의 노드 대 노드 전파 지연에 대한 지식을 사용하여, 그 순간에 임의의 통신에 대한 최상의 루트를 동적으로 선택한다. 다른 실시예에 있어서, 우선순위가 높은 클라이언트에 대해, 네트워크는 레이스 라우팅을 촉진시킬 수 있으며, 원음 또는 데이터 콘텐츠를 복구하기 위해 가장 빠른 데이터만을 선택하는 SDNP 클라우드를 통해 단편화된 형태로 중복 메시지를 전송할 수 있다.

[0186] 본 발명에 따른 SDNP 시스템의 많은 이점 중에서, 병렬 및 "메시형 전송"실시예에 있어서, 패킷은 이들이 SDNP 클라우드를 통과할 때 단편화될 수 있어, 잠재적인 해커가 개별적인 서브-패킷 또는 서브-패킷 그룹을 해독할 수 있다 해도 메시지를 이해하는 것을 방지하며, 또한 "동적" 실시예에 있어서 패킷에 적용되는 스크램블링, 암호화, 및 분할 방법은 끊임없이 변화하여, 주어진 시점에서 패킷을 성공적으로 해독으로부터 잠재적인 해커가 임의의 중요한 이익을 취하는 것을 거부한다. 본 발명의 실시예의 많은 추가적인 이점은 이하의 설명의 검토로부터 본 기술분야의 숙련자에게 쉽게 명확해질 것이다.

[0187] 유사한 보안 기술들이 일반적으로 SDNP 클라우드와 클라인언트 디바이스, 예를 들어 휴대폰 또는 태블릿 사이의 "라스트 마일"에서 적용될 수 있다. 클라이언트 디바이스는 일반적으로 클라우드부터 분리된 보안 구역 내에 배치되고, 이는 먼저 인증된 SDNP 클라이언트가 될 수 있고, 단계가, 전형적으로 SDNP 관리 서버로부터의 다운로드를 통해서, 디바이스의 보안 구역에 특정된 소프트웨어 패키지를 클라이언트 디바이스에 설치하는 것을 포함한다. 클라이언트 디바이스는 클라우드 내의 (종종 단지 "게이트웨이"로 지칭되는) 게이트웨이 미디어 노드를 통해서 SDNP 클라우드에 링크된다. 게이트웨이 미디어 노드는 클라우드 및 클라이언트의 디바이스의 보안 구역 모두와 관련된 공유 비밀에 대한 액세스를 가지나, 클라이언트 디바이스는 SDNP 클라우드와 관련된 공유 비밀에 대한 액세스를 가지지 않는다.

[0188] 부가된 보안 레벨로서, 클라이언트 디바이스들은 시그널링 서버를 통해서 서로 시드 및 키를 직접적으로 교환할 수 있다. 따라서, 전송 클라이언트 디바이스는 시드 및/또는 키를 수신 클라이언트 디바이스에 직접적으로 송신

할 수 있다. 그러한 실시예에서, 수신 클라이언트 디바이스에 의해서 수신된 패킷은 송신 클라이언트 디바이스를 떠나는 패킷과 동일한 스크램블링된 또는 암호화된 형태일 것이다. 그에 따라, 수신 클라이언트 디바이스는, 패킷을 언스크램블링하거나 해독하기 위해서 송신 클라이언트 디바이스로부터 수신하는 시드 또는 키를 이용할 수 있다. 클라이언트 디바이스들 사이의 직접적인 시드 및 키의 교환은 SDNP 네트워크의 자체적인 동적 스크램블링 및 암호화에 부가되고, 그에 따라 네스트형 보안으로 지칭되는 부가된 보안 레벨을 나타낸다.

[0189] 또한, 클라이언트 디바이스 또는 클라이언트 디바이스가 통신에 이용하는 게이트웨이 노드는, 패킷이 SDNP 네트워크에 도달하기 전에, 동일한 종류의 데이터 - 예를 들어, 보이스 패킷, 텍스트 메시지 파일, 문서, 소프트웨어의 단편, 또는 상이한 유형의 정보를 나타내는 것, 예를 들어 하나의 보이스 패킷 및 하나의 텍스트 파일, 하나의 텍스트 패킷, 및 하나의 비디오 또는 사진 이미지 - 를 나타내는 패킷들을 혼합할 수 있고, 출구 게이트웨이 노드 또는 목적지 클라이언트 디바이스가 혼합된 패킷을 분할하여 원래의 패킷을 복원할 수 있다. 이는, SDNP 네트워크에서 발생되는 임의의 스크램블링, 암호화 또는 분할에 부가된다. 그러한 경우에, 송신 클라이언트 디바이스는, 송신 클라이언트 디바이스 또는 게이트웨이 미디어 노드에서 혼합된 원래의 패킷을 재생하기 위해서 패킷을 어떻게 분할하는지를 설명하는 시드를 수신 클라이언트 디바이스에 송신할 수 있다. 성공적인 혼합 및 분할의 실시는 동작의 선형 시퀀스를 포함할 수 있거나, 대안적으로 네스트형 아키텍처를 이용하고, 여기에서 클라이언트는 그 자체의 보안 수단을 실행하고 그에 따라 SDNP 클라우드도 실행한다.

[0190] 있을 수도 있는 해커를 더 혼동시키기 위해서, 클라이언트 디바이스는 단일 통신에서 연속적인 패킷들(또는 서브-패킷들)을 상이한 게이트웨이 노드들에 전송할 수 있고, 및/또는 클라이언트 디바이스는 이들을 상이한 물리적 미디어 링크(셀룰러, WiFi, 이더넷 케이블 등)를 통해서 전송할 수 있다 - 본원에서 "다중-PHY" 전송으로 종종 지칭되는 프로세스. 그러한 혼동에 부가하기 위해서, 이는 또한 연속적인 패킷들 내에서 상이한 소스 어드레스들을 포함할 수 있고, 그에 의해서 해커가 패킷들을 동일 클라이언트 디바이스로부터 기원하는 것으로 식별하는 것을 방지한다.

[0191] 본 발명은 또한 전화 컨퍼런스 콜의 취급에서의 특유의 발전을 포함한다. 일반적인 컨퍼런스 콜에서, 패킷은 모든 통화 참여자에게 송신된다. 본 발명에 따라, 클라이언트 디바이스 또는 다른 노드가 패킷을 묵음 처리된 참여자 또는 참여자들에게 전송하는 것을 방지함으로써, 특정 지정 참여자가 "묵음처리"될 수 있고, 즉, 통화로부터 배제될 수 있다. 대안적인 실시예에서, 데이터 패킷은 방송 모드로 그룹 통화 내의 모든 참여자에게, 그러나 상이한 암호 방법들을 이용하여, 송신된다. 일반적인 컨퍼런스 콜의 경우에, 데이터 패킷은 암호를 이용하여 모든 사용자에게 송신되고, 여기에서 모든 참여자는 해독 키의 복사본을 갖는다. 프라이빗 모드 또는 묵음 모드에서, 사용자에게 방송되는 데이터 패킷은 상이한 암호를 이용하고, 여기에서 선택된 사용자만이 해독 키를 공유한다.

[0192] SDNP 네트워크 및 프로토콜을 이용하는 통신에 본질적인 보안 메커니즘은 또한, 보안 파일 및 데이터 저장에 완벽히 적합하도록 한다. SDNP 네트워크를 통한 일반적 통신이 전형적으로 하나의 클라이언트 디바이스로부터 다른 클라이언트 디바이스로의 스크램블링된, 암호화된 데이터의 익명의 단편화된 데이터 이송을 포함하기 때문에, 사실상, 이송에서 통신을 중단하는 것 그리고 원래의 클라이언트 디바이스가 이를 검색하기를 원하는 때까지 이를 하나 이상의 버퍼 내에 무기한으로 저장하는 것에 의해서, 파일 및 데이터 저장이 실현될 수 있다. 이러한 분산된 파일 저장이 본원에서 종종 분산형 데이터 저장으로 지칭된다.

[0193] 이하에 열거된 도면에서, 일반적으로 유사한 구성요소는 동일한 도면부호가 부여된다. 그러나 주어진 도면부호가 할당되는 모든 구성요소는 반드시 동일한 도면부호를 갖는 다른 구성요소와 동일하지 않음을 인식해야 한다. 예를 들어, 지정 도면부호를 갖는 암호화 동작은 반드시 동일한 참조 번호를 갖는 다른 암호화 동작과 동일할 필요는 없다. 또한, 구성요소의 그룹, 예를 들어 단일의 도면부호에 의해 집합적으로 식별되는 네트워크에서의 서버가 반드시 필수적으로 동일할 필요는 없다.

## *도면의 간단한 설명*

[0194] 도 1은 네트워크에 걸친 통상적인 패킷 전송을 도시하는 개략도이다.

도 2a는 패킷 스크램블링 프로세스를 도시한 개략도이다.

도 2b는 패킷 언스크램블링 프로세스를 도시한 개략도이다.

도 2c는 다양한 패킷 스크램블링 알고리즘을 도시한 개략도이다.

도 2d는 고정 매개변수 패킷 스크램블링을 도시한 개략도이다.

도 2e는 은폐 숫자를 갖는 동적 스크램블링을 도시한 개략도이다.

도 3은 패킷 재-스크램블링 프로세스를 도시한 개략도이다.

도 4a는 패킷 암호화 프로세스를 도시한 개략도이다.

도 4b는 패킷 해독 프로세스를 도시한 개략도이다.

도 5는 암호화된 스크램블링 및 그 역기능의 프로세스를 도시한 개략도이다.

도 6은 재-스크램블링 및 재-암호화를 포함하는 DUSE 재-패킷팅의 프로세스를 도시한 개략도이다.

도 7a는 고정-길이 패킷 분할의 프로세스를 도시한 개략도이다.

도 7b는 고정-길이 패킷 혼합의 프로세스를 도시한 개략도이다.

도 8은 다양한 패킷-혼합 방법을 도시한 개략도이다.

도 9a는 SDNP 보안 기능 및 역기능을 요약한 표이다.

도 9b는 단일 루트 라스트 마일 통신을 위한 유입 및 유출 데이터 패킷에 실시되는 SDNP 보안 동작을 도시하는 블록도이다.

도 9c는 다중-루트 라스트 마일 통신을 위한 유입 및 유출 데이터 패킷에 실시되는 SDNP 보안 동작을 도시하는 블록도이다.

도 9d는 SDNP 클라이언트 디바이스에서의 오디오, 비디오, 텍스트, 및 파일 콘텐츠 생성, 데이터 패킷 준비, 데이터 패킷 인식, 및 콘텐츠 재생산을 도시하는 블록도이다.

도 9e는 계층적 데이터 캡슐화를 설명하기 위해서 7-계층 OSI 모델을 이용하는 SDNP 데이터 패킷의 그래프 도면이다.

도 9f는 SDNP 페이로드의 그래프 및 막대형 도면이다.

도 9g는 삼중-채널 통신을 이용하는 SDNP 게이트웨이에서의 인바운드 라스트 마일 데이터 패킷 프로세싱을 도시하는 블록도이다.

도 9h는 단일-채널 통신을 이용하는 SDNP 게이트웨이에서의 인바운드 라스트 마일 데이터 패킷 프로세싱을 도시하는 블록도이다.

도 9i는 삼중-채널 통신을 이용하는 SDNP 게이트웨이에서의 아웃바운드 라스트 마일 데이터 패킷 프로세싱을 도시하는 블록도이다.

도 10은 SDNP 클라우드의 개략도이다.

도 11은 신원 확인이 없는 미보안 라스트 마일 통신의 예를 개략적으로 도시한다.

도 12는 통화자의 신원 확인이 없는 일반적인 구형 전화 시스템(POTS)에 걸친 미보안 라스트 마일 통신을 도시한다.

도 13은 신원 확인이 있는 미보안 라스트 마일 통신의 예를 개략적으로 도시한다.

도 14는, 운영자-기반의 신원 확인이 있는, 유사한 공공 서비스 전화 네트워크(PSTN)에 걸친 미보안 라스트 마일 통신을 도시한다.

도 15는, 로그인- 또는 토큰-기반의 신원 확인이 있는, 유선 디지털 네트워크에 걸친 미보안 라스트 마일 통신을 도시한다.

도 16은, PEST- 또는 신용카드-기반의 신원 확인이 있는, 유선 아날로그 네트워크에 걸친 미보안 라스트 마일 통신을 도시한다.

도 17은 신원 확인을 지원할 수 있는 하이퍼보안 라스트 마일 통신의 예를 개략적으로 도시한다.

도 18은 WiFi 무선 네트워크를 통한 신원-확인 가능 하이퍼보안 라스트 마일 통신을 도시한다.

도 19는 셀룰러 무선 네트워크를 통한 신원-확인 가능 하이퍼보안 라스트 마일 통신을 도시한다.

도 20은 이더넷 유선 네트워크를 통한 신원-확인 가능 하이퍼보안 라스트 마일 통신을 도시한다.

도 21은 케이블 유선 네트워크를 통한 신원-확인 가능 하이퍼보안 라스트 마일 통신을 도시한다.

도 22는 조합된 케이블 유선 및 홈 WiFi 무선 네트워크를 통한 신원-확인 가능 하이퍼보안 라스트 마일 통신을 도시한다.

도 23은 신원-페어링 보안 LAN 라스트 링크에 연결된 신원-확인 가능 하이퍼보안 통신 레그를 포함하는 라스트 마일 통신의 예를 개략적으로 도시한다.

도 24는 유선에 의해서 신원-페어링 보안 디바이스에 그리고 미식별된 미보안 디바이스에 연결된 신원-확인 가능 하이퍼보안 유선 통신 레그를 포함하는 라스트 마일 통신을 도시한다.

도 25는 WiFi LAN에 의해서 가정 및 직장용 신원-페어링 WPA-보안 컴퓨팅 및 통신 디바이스에 연결된 신원-확인 가능 하이퍼보안 유선 통신 레그를 포함하는 라스트 마일 통신을 도시한다.

도 26은 WiFi LAN에 의해서 신원-페어링 WPA-보안 홈 IoT 디바이스에 연결된 신원-확인 가능 하이퍼보안 유선 통신 레그를 포함하는 라스트 마일 통신을 도시한다.

도 27은 이더넷에 의해서 또는 WiFi LAN에 의해서 사업용 신원-페어링 WPA-보안 디바이스에 연결된 신원-확인 가능 하이퍼보안 유선 통신 레그를 포함하는 라스트 마일 통신을 도시한다.

도 28은 신원-페어링 보안 유선 또는 보안 무선 LAN 라스트 링크에 연결된 신원-확인 가능 하이퍼보안 통신 레그를 포함하는 라스트 마일 통신의 예를 개략적으로 도시한다.

도 29a는 라스트 마일 통신에서 적용 가능한 이더넷 및 WiFi를 포함하는 유선 및 무선 하이퍼보안 브릿지를 개략적으로 도시한다.

도 29b는 라스트 마일 통신에서 적용 가능한 위성 및 자동차 네트워크를 이용하는 유선 및 무선 하이퍼보안 브릿지를 개략적으로 도시한다.

도 29c는 라스트 마일 통신에서 적용 가능한 케이블 및 셀룰러 네트워크를 이용하는 유선 및 무선 하이퍼보안 브릿지를 개략적으로 도시한다.

도 30은, 위성 전화(sat phone), 항공기, 기차, 선박, 및 가정용 위성 수신기(셋톱 박스)를 포함하는 다양한 디바이스에 대한 위성 업링크 및 다운링크를 통한 신원-확인 가능 하이퍼보안 무선 통신을 포함하는 라스트 마일 통신을 도시한다.

도 31a는 위성 연결성을 갖는 온보드 항공기 통신 네트워크 내의 디바이스들 사이의 라스트 링크 하이퍼보안 통신의 예이다.

도 31b는 항공기 위성 통신 및 안테나 모듈의 예이다.

도 32는 멀티 채널의 위성 연결성을 갖는 온보드 해양 크루즈 선박 통신 네트워크 내의 디바이스들 사이의 라스트 링크 하이퍼보안 통신의 예이다.

도 33은 라디오 및 위성 연결성을 갖는 온보드 기차 통신 네트워크 내의 디바이스들 사이의 라스트 마일 하이퍼보안 통신의 예이다.

도 34는 셀룰러 라스트 링크 연결성을 포함하는 자동차 텔레매틱 모듈에 대한 하이퍼보안 라스트 마일 통신을 도시한다.

도 35는 셀룰러 연결성을 갖는 자동차 통신 네트워크 내의 텔레매틱 모듈과 인-캐빈 WiFi 연결 디바이스 사이의 라스트 링크 통신의 예이다.

도 36은 셀룰러 연결성을 갖는 하이퍼보안 운반체간 통신의 예이다.

도 37은 마이크로파, 위성, 및 섬유 네트워크에 걸친 하이퍼보안 트렁크 라인 통신을 도시한다.

도 38은 하이퍼보안, 보안, 및 미보안 통신 네트워크를 위한 보안, 신원 확인, 및 통화자 익명성 특징들의 비교를 도시한다.

도 39는 고정 IP 어드레스를 갖는 단일-루트 라스트 마일 하이퍼보안 통신의 개략도이다.

도 40a는 고정 IP 어드레스를 이용한 단일-루트 라스트 마일 하이퍼보안 통신의 개략적 IP 스택 도면이다.

도 40b는 고정 IP 어드레스를 이용하는 단일-루트 라스트 마일 하이퍼보안 통신의 단순화된 도면이다.

도 41은 동적 클라이언트 IP 어드레스를 갖는 단일-루트 라스트 마일 하이퍼보안 통신의 개략도이다.

도 42a는 동적 클라이언트 IP 어드레스를 이용한 단일-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면이다.

도 42b는 동적 클라이언트 IP 어드레스를 이용한 단일-루트 라스트 마일 하이퍼보안 통신의 대안적인 IP 스택 도면이다.

도 43은 고정 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 개략도이다.

도 44a는 단일 PHY 라스트 링크를 이용한 고정 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면이다.

도 44b는 다중 PHY 라스트 링크를 이용한 고정 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면이다.

도 45는 동적 클라이언트 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 개략도이다.

도 46a는 단일 PHY 라스트 링크를 이용한 동적 클라이언트 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면이다.

도 46b는 다중 PHY 라스트 링크를 이용한 동적 클라이언트 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면이다.

도 47은 동적 클라이언트 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 대안적인 버전의 개략도이다.

도 48은 동적 클라이언트 IP 어드레스를 갖는 다중-루트 라스트 마일 하이퍼보안 통신의 대안적인 버전의 IP 스택 도면이다.

도 49는 SDNP 페이로드를 실행하는 이더넷 통신을 위한 IPv4 및 IPv6 데이터그램의 그래프 도면이다.

도 50a는 SDNP-클라우드 통신을 위해서 클라이언트에서 이용되는 IPv4 및 IPv6 라스트 링크 이더넷 패킷의 그래프 도면이다.

도 50b는 SDNP-클라우드 통신을 위해서 클라이언트에서 이용되는 IPv4 및 IPv6 게이트웨이 링크 이더넷 패킷의 그래프 도면이다.

도 50c는 클라이언트 통신을 위해서 SDNP-클라우드에서 이용되는 IPv4 및 IPv6 게이트웨이 링크 이더넷 패킷의 그래프 도면이다.

도 50d는 클라이언트 통신을 위해서 SDNP-클라우드에서 이용되는 IPv4 및 IPv6 라스트 링크 이더넷 패킷의 그래프 도면이다.

도 51a는 고정 클라이언트 어드레싱을 갖는 단일 경로 라스트 마일 통신에서 이용되는 연속적인 이더넷 데이터 패킷(축약됨)을 도시한다.

도 51b는 동적 클라이언트 어드레싱을 갖는 단일 경로 라스트 마일 통신에서 이용되는 연속적인 이더넷 데이터 패킷(축약됨)을 도시한다.

도 51c는 고정 클라이언트 어드레싱을 갖는 다중-경로 라스트 마일 통신에서 이용되는 연속적인 이더넷 데이터 패킷(축약됨)을 도시한다.

도 51d는 동적 클라이언트 어드레싱을 갖는 다중-경로 라스트 마일 통신에서 이용되는 연속적인 이더넷 데이터 패킷(축약됨)을 도시한다.

도 52a는 이더넷에 걸친 SDNP 라스트 마일 라우팅을 요약한 표이다.

도 52b는 이더넷에 걸친 단일 경로 라스트 마일 통신에 관한 위상적(topological) 설명이다.

도 52c는 이더넷에 걸친 다중-경로 라스트 마일 통신에 관한 위상적 설명이다.

도 52d는 이더넷에 걸친 다중-경로 라스트 마일 통신에 관한 부가적인 위상적 설명이다.

도 53은 SDNP 페이로드를 수반하는 WiFi 통신을 위한 IPv4 및 IPv6 데이터그램의 그래프 도면이다.

도 54a는 SDNP-클라우드 통신을 위해서 클라이언트에서 이용되는 IPv4 및 IPv6 라스트 링크 WiFi 패킷의 그래프 도면이다.

도 54b는 SDNP-클라우드 통신을 위해서 클라이언트에서 이용되는 IPv4 및 IPv6 게이트웨이 링크 WiFi 패킷의 그래프 도면이다.

도 54c는 클라이언트 통신을 위해서 SDNP-클라우드에서 이용되는 IPv4 및 IPv6 게이트웨이 링크 WiFi 패킷의 그래프 도면이다.

도 54d는 클라이언트 통신을 위해서 SDNP-클라우드에서 이용되는 IPv4 및 IPv6 라스트 링크 WiFi 패킷의 그래프 도면이다.

도 55는 SDNP 페이로드를 수반하는 4G 셀룰러 통신을 위한 IPv4 및 IPv6 데이터그램의 그래프 도면이다.

도 56a는 SDNP-클라우드 통신을 위해서 클라이언트에서 이용되는 IPv4 및 IPv6 라스트 링크 4G 셀룰러 데이터 패킷의 그래프 도면이다.

도 56b는 클라이언트 통신을 위해서 SDNP-클라우드에서 이용되는 IPv4 및 IPv6 라스트 링크 4G 셀룰러 패킷의 그래프 도면이다.

도 57a는 단일-미디어 다중-PHY 라스트 링크 통신의 그래프 도면이다.

도 57b는 혼합-미디어 다중-PHY 라스트 링크 통신의 그래프 도면이다.

도 57c는 다중-PHY 라스트 링크 통신의 대안적인 구현예의 그래프 도면이다.

도 58은 다중-PHY 이더넷을 경유하여 전달되는 IPv6 데이터그램을 이용하는 SDNP-클라우드 라스트 링크 통신에 대한 연속적인 클라이언트의 그래프 도면이다.

도 59는 다중-PHY WiFi를 경유하여 전달되는 IPv6 데이터그램을 이용하는 SDNP-클라우드 라스트 링크 통신에 대한 연속적인 클라이언트의 그래프 도면이다.

도 60은 다중-PHY 4G 셀룰러 네트워크를 경유하여 전달되는 IPv6 데이터그램을 이용하는 SDNP-클라우드 라스트 링크 통신에 대한 연속적인 클라이언트의 그래프 도면이다.

도 61은 이더넷 및 WiFi를 통한 다중-PHY 전달을 이용하는 IPv6 데이터그램을 이용하는 SDNP-클라우드 라스트 링크 통신에 대한 연속적인 클라이언트의 그래프 도면이다. 도 62는 WiFi 및 4G 셀룰러 네트워크를 통한 다중-PHY 전달을 이용하는 IPv6 데이터그램을 이용하는 SDNP-클라우드 라스트 링크 통신에 대한 연속적인 클라이언트의 그래프 도면이다. 도 63은 계층 1 내지 계층 7 기능을 도시하는 DOCSIS 케이블 모뎀 통신 네트워크의 OSI 계층 스택 구성의 개략도이다.

도 64는 SDNP 페이로드를 수반하는 케이블 시스템을 위한 DOCSIS3 기반 통신 패킷의 그래프 도면이다.

도 65a는 다양한 DOCSIS3 프로토콜을 위한 스펙트럼 할당 및 캐리어 변조 방법의 그래프 도면이다.

도 65b는 CTMS와 CM 사이의 DOCSIS3.1 통신 시퀀스의 그래프 도면이다.

도 65c는 DOCSIS3.1 업스트림 통신의 그래프 도면이다. 도 65d는 DOCSIS3.1 다운스트림 통신의 그래프 도면이다.

도 66은 라스트 마일 통신을 위한 삼중-경로 SDNP 네트워크의 개략도이다.

도 67은 삼중-채널 SDNP 라스트 마일 통신에서의 "통화 요청" 동작의 개략도이다.

도 68은 삼중-채널 SDNP 라스트 마일 통신에서의 "어드레스 요청" 동작의 개략도이다.

도 69는 삼중-채널 SDNP 라스트 마일 통신에서의 "어드레스 전달" 동작의 개략도이다.

도 70은 SDNP 명령 및 제어 패킷 합성을 도시한 흐름도이다.

도 71은 단일-경로 삼중-채널 SDNP 라스트 마일 통신에서의 "라우팅 지시" 동작의 개략도이다.

도 72는 SDNP 클라이언트로부터 SDNP 클라우드로의 단일-경로 삼중-채널 SDNP 라스트 마일 통신에서의 "SDNP 통화" 동작의 개략도이다.

도 73a는 SDNP 통화에서의 SDNP 클라이언트에 대한 SDNP 클라우드 및 라스트 마일 삼중-경로 통신의 개략도이다. 도 73b는 비-SDNP클라이언트에 대한 "콜 아웃"으로서 구현된 SDNP 클라우드 및 라스트 마일 삼중-경로 통신의 개략도이다.

도 74는 다중-경로 삼중-채널 SDNP 라스트 마일 통신에서의 "라우팅 지시" 동작의 개략도이다.

도 75a는 SDNP 클라이언트로부터 SDNP 클라우드까지의 방향의 다중-경로 삼중-채널 SDNP 라스트 마일 통신에서의 "SDNP 통화" 동작의 개략도이다.

도 75b는 SDNP 클라우드로부터 SDNP 클라이언트까지의 방향의 다중-경로 삼중-채널 SDNP 라스트 마일 통신에서의 "SDNP 통화" 동작의 개략도이다.

도 76은 단일-경로 삼중-채널 SDNP 라스트 마일 통신에서의 그룹-통화 "라우팅 지시" 동작의 개략도이다.

도 77a는 구역 U1 클라이언트로부터 다른 구역 내의 클라이언트까지의 방향의 SDNP 다중-경로 클라우드 전송 및 SDNP 라스트 마일 통신을 이용하는 "SDNP 그룹 통화"의 개략도이다.

도 77b는 구역 U7 클라이언트로부터 다른 구역 내의 클라이언트까지의 방향의 SDNP 다중-경로 클라우드 전송 및 SDNP 라스트 마일 통신을 이용하는 "SDNP 그룹 통화"의 개략도이다.

도 77c는 구역 U9 클라이언트로부터 동일 구역 상의 그리고 다른 구역 내의 다른 클라이언트까지의 방향의 SDNP 다중-경로 클라우드 전송 및 SDNP 라스트 마일 통신을 이용하는 "SDNP 그룹 통화"의 개략도이다.

도 78은 SDNP 클라이언트 및 미보안 PSTN 디바이스 모두에 대한 SDNP 다중-경로 클라우드 전송 및 라스트 마일 통신을 이용하는 "SDNP 그룹 통화"의 개략도이다.

도 79a는 SDNP 그룹 통화에서의 정규 통화 및 프라이빗 통화 동작의 막대형 도면이다.

도 79b는 SDNP 그룹 통화에서의 정규 통화 및 하이퍼-프라이빗 통화 동작의 막대형 도면이다.

도 80a는 SDNP PTT 그룹 통화에서의 정규 및 프라이빗 푸시-투-토크(push-to-talk) 동작의 막대형 도면이다.

도 80b는 SDNP PTT 그룹 통화에서의 정규 및 하이퍼-프라이빗 푸시-투-토크 동작의 막대형 도면이다.

도 81은 단편화된 데이터의 하이퍼보안 파일 저장에서의 기록-동작을 위한 데이터 전송의 개략도이다.

도 82a는 단편화된 데이터의 하이퍼보안 파일 저장에서의 기록-동작을 위한 데이터 흐름의 개략도이다.

도 82b는 단편화된 데이터의 하이퍼보안 파일 저장에서의 판독-동작을 위한 데이터 흐름의 개략도이다.

도 83은 단편화된 데이터의 하이퍼보안 파일 저장에서의 판독-동작을 위한 데이터 전송의 개략도이다.

도 84a는 파일 저장 솔루션에 연결된 SDNP 클라우드의 다양한 예를 도시한다.

도 84b는 로컬 및 클라우드 연결 저장 서버를 포함하는 분산형 하이퍼보안 파일 저장 네트워크의 개략도이다.

도 85a는 비중복(RRF = 0) 하이퍼보안 파일 저장을 위한 파일 맵핑이다.

도 85b는 RRF = 1 판독 중복 하이퍼보안 파일 저장을 위한 파일 맵핑이다.

도 85c는 RRF = 2 판독 중복 하이퍼보안 파일 저장을 위한 파일 맵핑이다.

도 86은 삼중-채널 네트워크 통신을 이용하는 분산형 하이퍼보안 파일 저장 시스템을 위한 네트워크 맵이다.

도 87a는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 기록 요청 동작을 도시한다.

도 87b는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 서버 명칭 요청 동작을 도시한다.

도 87c는 분산형 하이퍼보안 파일 저장 시스템 내의 시그널링 서버 계획 동작을 도시한다.

도 87d는 분산형 하이퍼보안 파일 저장 시스템 내의 시그널링 서버 클라이언트측 라스트 마일 및 SDNP 클라우드 기록 라우팅 지시를 도시한다.

도 87e는 분산형 하이퍼보안 파일 저장 시스템 내의 시그널링 서버 저장측 라스트 마일 및 SDNP 클라우드 기록

라우팅 지시를 도시한다.

도 88은 분산형 하이퍼보안 파일 저장 시스템 내의 파일 전달을 도시한다.

도 89a는 분산형 하이퍼보안 파일 저장 시스템 내의 링크 응답 확인 파일 저장 및 기록 동작을 도시한다.

도 89b은 분산형 하이퍼보안 파일 저장 시스템 내의 파일 저장 서버 링크 전달을 도시한다. 도 89c는 FS 링크를 포함하는 파일 저장 서버 기록 확인 데이터 패킷을 도시한다.

도 89d는 클라이언트의 SDNP 메신저 내의 파일 저장 판독 링크의 합성을 도시한다.

도 90a는 LRF = 0 비중복 FS 링크를 갖는 비중복 RRF = 0 하이퍼보안 파일 저장을 위한 파일 맵이다.

도 90b는 LRF = 1 중복 FS 링크를 갖는 비중복 RRF = 0 하이퍼보안 파일 저장을 위한 파일 맵이다.

도 90c는 LRF = 1 중복 FS 링크를 갖는 비중복 RRF = 1 하이퍼보안 파일 저장을 위한 파일 맵이다.

도 91은 파일 저장 서버 및 클라이언트 FS 링크의 수에 따른 저장 탄력성을 나타내는 그래프이다.

도 92는 SDNP-인코딩 및 SDNP-디코딩 기능의 개략도이다.

도 93a는 클라이언트측 파일 보안 및 하이퍼보안 파일 전송을 갖는 SDNP 분산형 파일 저장의 개략도이다.

도 93b는 네스트형 파일 보안 및 하이퍼보안 파일 전송을 갖는 SDNP 분산형 파일 저장의 개략도이다.

도 94는 SDNP 분산형 파일 저장 기록 동작에서의 하이퍼보안 인코딩의 단순화된 개략도이다.

도 95는 SDNP 분산형 파일 저장 판독 동작에서의 하이퍼보안 디코딩의 단순화된 개략도이다.

도 96a는 하이퍼보안 파일 판독 동작에서 AAA 동작을 설명하는 흐름도이다.

도 96b는 하이퍼보안 파일 판독 동작에서 파일 액세스 및 SDNP 전송을 설명하는 흐름도이다.

도 97a는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 판독 요청 동작을 도시한다.

도 97b는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 저장 서버 명칭 요청 동작을 도시한다.

도 97c는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 저장 서버 명칭 전달 및 시그널링 서버 계획 동작을 도시한다.

도 97d는 분산형 하이퍼보안 파일 저장 시스템 내의 시그널링 서버 저장측 라스트 마일 및 SDNP 클라우드 라우팅 판독 지시를 도시한다.

도 97e는 분산형 하이퍼보안 파일 저장 시스템 내의 시그널링 서버 클라이언트측 라스트 마일 및 SDNP 클라우드 판독 라우팅 지시를 도시한다.

도 98은 분산형 하이퍼보안 파일 저장 시스템 내의 판독 동작 중의 저장측 파일 디코딩을 도시한다.

도 99는 판독 동작 중의 분산형 하이퍼보안 파일 저장 시스템 내의 파일 데이터 전달을 도시한다.

도 100은 링크 리프레시(link refresh) 중의 분산형 하이퍼보안 파일 저장 시스템 내의 파일 데이터 전달을 도시한다.

도 101은 파일을 재분산시키기 위해서 이용되는 분산형 하이퍼보안 파일 저장 시스템 내의 파일 데이터 전달을 도시한다.

도 102는 SDNP 텍스트 메시징 내의 타임 스탬프를 도시한다.

도 103은 SDNP 등록된 통신의 흐름도이다.

도 104a는 인터넷 OTT 통신에서의 엔드-투-엔드 암호화를 도시한다.

도 104b는 하이퍼보안 통신에서의 엔드-투-엔드 암호화를 도시한다.

도 105a는, SDNP 보안 에이전트가 진출 통화의 비가시적 모니터링을 실시하는, "SDNP 통화" 동작의 개략도이다.

도 105b는, SDNP 보안 에이전트가 진입 통화의 비가시적 모니터링을 실시하는, "SDNP 통화" 동작의 개략도이다.

도 106은, SDNP 보안 에이전트가 FS 링크 라우팅의 비가시적 모니터링을 실시하는, 분산형 하이퍼보안 파일 저

장 시스템 내의 파일 저장 서버 링크 전달을 도시한다.

도 107은, SDNP 보안 에이전트가 다중-경로 라스트 마일 통신을 이용하는 진출 통화의 비가시적 모니터링을 실시하는, "SDNP 통화" 동작의 개략도이다.

도 108은 SDNP 보안 에이전트를 지정하고 인증하기 위한 단계의 흐름도이다.

도 109는 SS7 취약성에 노출된 타워 통신에 대한 휴대폰을 도시한다.

도 110은 SS7 공격을 격퇴하기 위해서 전화 번호 은폐를 이용하는 SDNP 통신을 도시한다.

도 111은 별개의 서버들에 호스팅된 SDNP 소프트스위치-기반의 클라우드들의 연결성을 도시한다.

도 112는 공유 서버들에 호스팅된 SDNP 소프트스위치-기반의 클라우드의 연결성을 도시한다.

도 113은 중첩되는 네트워크들에 호스팅된 SDNP 소프트스위치-기반의 클라우드의 연결성을 도시한다. 도 114는 글로벌 SDNP 클라우드 텔코에 액세스하는 SDNP 소프트스위치-기반의 클라우드의 연결성을 도시한다.

도 115는 네스트형 SDNP 서브네트의 예이다.

## *발명을 실시하기 위한 구체적인 내용*

[0195] 회선 교환형 전화기술의 거의 1.5 세기 동안, 오늘날의 통신 시스템 및 네트워크는 불과 10년 만에 케이블 및 광섬유를 통해 이더넷, WiFi, 4G/LTE, 및 DOCSIS3 데이터가 운반된 인터넷 프로토콜을 사용하여 패킷 교환형 통신으로 모두 이동되었다. 신뢰할 수 있는 IP 패킷 전달을 보장하기 위해 중복 경로를 사용하는 것, 즉 시스템 상호 운용성의 독보적인 레벨 및 전세계에 걸친 연결성과 함께, 인터넷이 처음 생성된 이유를 포함하여, 음성, 텍스트, 그림, 비디오 및 데이터를 제공하는 이점은 많다. 그러나 어떤 혁신이라도 신기술이 창안하는 도전의 강도는 종종 유도된 이점과 일치한다.

[0196] **기존 통신사업자의 단점**

[0197] 본 발명의 배경 기술 전체에 걸쳐 상세히 기재된 바와 같이, 오늘날의 통신은 많은 단점을 갖고 있다. 오늘날 에이티앤티(AT&T), 버라이즌(Verizon), 엔티티(NTT), 보다폰(Vodaphone) 등과 같은 세계 주요 장거리 통신 업체가 소유한 맞춤형 디지털 하드웨어를 포함하는 최고 성능의 통신 시스템은 일반적으로 우수한 음질을 제공하지만, 그러나 고가의 월사용료, 연결 요금, 장거리 요금, 복잡한 데이터 요금제, 장거리 로밍 요금, 및 다양한 서비스 요금이 포함된다. 이들 네트워크는 비공개이기 때문에, 실제 데이터 보안은 공개적으로 알려지지 않으며, 보안 위반, 해킹 및 침입은 일반적으로 공개되지 않는다. 오늘날 언론에 보도된 유선 전화 및 프라이버시 침해의 수를 감안하면, 사설 캐리어 통신 보안은, 그 사설 클라우드에서가 아니라도, 적어도 라스트 마일 연결에서 여전히 의심의 여지가 있다.

[0198] "인터넷 서비스 제공자" 또는 ISP는 글로벌 통신 체인에서 다른 링크를 형성한다. 본 발명의 배경 기술에 기재된 바와 같이, VoIP 또는 "인터넷 프로토콜을 통한 음성"을 사용하여 인터넷을 통해 전달되는 음성은 이하를 포함하는 수많은 서비스 품질 또는 QoS 문제로 고통받고 있다:

[0199] * 패킷 교환형 네트워크인 인터넷은, 적시에 IP 패킷을 제공하거나 또는 지연 시간이 적고 QoS가 높은 실시간 애플리케이션을 지원하도록 설계되지 않았다.

[0200] * IP 패킷의 라우팅은 예측할 수 없는 경로를 취하고 있고, 결과적으로, 끊임없이 변하는 지연, 높은 데이터 에러율의 폭발, 및 예기치 않은 통화 끊김을 초래한다.

[0201] * IP 패킷 라우팅은 인터넷 서비스 제공자의 재량에 따라 이루어지며, 이는 패킷이 라우팅되는 네트워크를 제어하며 또한 자체 네트워크의 로드 균형을 조정하거나 또는 그 네트워크를 지나는 일반적인 트래픽의 연결 품질의 열화를 감수하면서 그 VIP 클라이언트의 서비스를 더 좋게 하기 위해 라우팅을 조정할 수 있다.

[0202] * 인터넷 상에서 무임승차하는 라인, 카카오 톡, 비버(Viber)와 같은 오버 더 탑 또는 OTT 제공자는 인터넷 히치하이커로서 작용하며, 또한 QoS에 영향을 미치는 네트워크 또는 요인을 제어하지 못한다.

[0203] * 적당한 데이터 전송률에서도 합리적인 음성 품질의 오디오를 제공하지 못하는 무거운 오디오 코덱의 사용

[0204] * TCP 전송 프로토콜을 기반으로 하는 VoIP는 핸드세이킹 및 IP 패킷 재방송 중 유도된 지연에 의해 유발된 높은 대기 시간 및 열화된 오디오 품질로 고통받고 있다. 보조되지 않는 UDP 전송은 페이로드 무결성을 제공하지

않는다.

[0205] QoS 문제 외에도, 오늘날의 디바이스 및 네트워크의 보안은 최악이어서, 글로벌 통신의 미래 요구를 지원하기에 전적으로 허용할 수 없는 수준이다. 명칭이 보안 동적 통신 네트워크 및 프로토콜인, 배경 기술 섹션에서 상세히 설명한 바와 같이, 네트워크 보안은, 스파이웨어, 트로이 목마, 감염 및 피싱을 포함하는; 라스트 링크에서, 스파이웨어, IP 패킷 스니핑, 도청 및 사이버 해적 "모조" 휴대폰 타워의 통화 차단을 포함하는; 그리고 라스트 마일 연결성의 로컬 네트워크 또는 텔코 부분에서, 스파이웨어, IP 패킷 스니핑, 바이러스와 같은 감염, 사이버 해적 "중간자 공격"을 포함하는, 통신 디바이스 상의 대규모 사이버 공격의 어레이에 취약하다. 클라우드 자체는, 중간자 공격, 서비스 거부 공격 및 인증되지 않은 정부 감시로부터의, 바이러스와 같은 감염에 의한, 임의의 클라우드 게이트웨이에서의 보안 파괴에 의해서 무단 액세스될 수 있다. 요약하면, 오늘날의 통신 보안은 사이버 해적들이 쉽게 악용하고 사이버 범죄 및 사이버 프라이버시 침해에 유용한 다음과 같은 다양한 취약점에 의해 손상된다.

[0206] * 목적지 IP 어드레스, 목적지 포트 # 및 목적지 MAC 어드레스를 포함하여, IP 패킷의 목적지의 노출

[0207] * 소스 IP 어드레스, 소스 포트 # 및 본래 MAC 어드레스를 포함하는, IP 패킷의 소스 노출.

[0208] * 사용된 계층 4 전송 유형 및 포트 # 요청된 서비스 유형 및 IP 패킷의 페이로드에 캡슐화된 애플리케이션 데이터의 노출.

[0209] * 암호화되지 않은 파일에서, 개인 및 기밀 정보, 로그인 정보, 애플리케이션 패스워드, 재무 기록, 비디오 및 사진을 포함하여, IP 패킷의 페이로드에 캡슐화된 모든 애플리케이션 및 파일 데이터.

[0210] * 사이버 당사자가 암호화된 파일을 파괴하기 위한 반복된 기회를 가질 수 있게 하는 통신의 다이얼로그.

[0211] * FTP, 이메일 및 웹 페이지 기반 감염을 사용하여, 통신 디바이스 및 라우터 내에 스파이웨어 및 피싱 프로그램 및 트로이 목마를 포함하는, 맬웨어를 설치할 수 있는 많은 기회.

[0212] 인터넷 프로토콜을 사용하는 패킷 교환형 통신 네트워크의 기본적으로 본질적인 약점인, 키 포인트의 반복은, 임의의 적대적 당사자 또는 사이버 해적이 IP 패킷을 가로채서 IP 패킷에 포함된 데이터를 생성하는데 어떤 디바이스가 포함되었는지를 알 수 있다는 것이고, 여기서 IP 패킷이 어디서 왔는지, IP 패킷이 전송되는 곳, 데이터가 어떻게 전송되는지, 즉 UDP 또는 TCP 인지, 그리고 어떤 종류의 서비스가 요청되는지, 즉 페이로드 내에 어떤 종류의 애플리케이션 데이터가 포함되는지 등을 알 수 있다. 이와 관련하여 사이버 해적은 대화의 "문맥"을 결정할 수 있어서, 암호를 균열시키고, 암호 보안을 파괴하며, 그리고 파일, 데이터 및 페이로드 콘텐츠에 대한 무단 액세스를 얻는 기회를 향상시킨다.

[0213] ***암호화*** - 기재된 바와 같이 다양한 사이버 공격에 대해 방어하기 위해, 오늘날 네트워크 관리자, IT 전문가 및 애플리케이션은 주로 단일의 방어-암호화에 의존한다. 암호화는, 읽을 수 있는 텍스트, 실행 가능한 프로그램, 볼 수 있는 비디오 및 그림, 또는 이해하기 쉬운 오디오이든 간에, "평문(plaintext)"으로도 알려져 있는 인식 가능한 콘텐츠를, 무의미한 텍스트 문자의 스트링으로서 보이는, "암호문"으로서 알려진 대안적인 파일 유형으로 변환하는 수단이다.

[0214] 보호되지 않은 파일을 암호화된 파일로 변환하는 암호화 프로세스는 암호 변환 프로세스의 임의의 명백한 패턴을 드러내지 않고 데이터를 등가의 텍스트 요소로 변경하기 위해 암호(cypher)로 지칭되는, 논리적 또는 수학적 알고리즘을 사용하는 단계를 포함한다. 그 후, 암호화된 파일은 목적지 디바이스에 의해 수신될 때까지 통신 네트워크 또는 매체를 통해 송신된다. 파일 수신에 따라, "해독"이라는 프로세스를 사용하는 수신 디바이스는 그 후 인코딩된 메시지를 본래의 내용으로 해독한다. "암호화"로 널리 알려진 암호화 및 해독의 연구는 컴퓨터 과학 및 전기 공학과 함께, 수 이론, 집합 이론, 및 알고리즘 설계를 포함하여, 수학 요소를 혼합한다.

[0215] 간단한 "단일 키" 또는 "대칭 키" 암호화 기술에 있어서, 양 당사자에 의해 선험적으로 알려진 단일 키워드 또는 구문은 파일 암호화 및 해독 프로세스를 언로킹할 수 있다. 제2차 세계 대전에서, 예를 들어 오픈 라디오 채널 상에서 통신된 잠수함과 해상 선박은 암호화된 메시지를 사용하였다. 처음에는 암호화가 단일 키 기반이었다. 암호 패턴을 분석함으로써, 연합군 암호 학자들은 때때로 암호 핵심 단어나 패턴을 찾아낼 수 있었고, 그 후 발견 없이 암호화된 파일을 읽을 수 있었다. 암호화 방법이 더 복잡해짐에 따라, 코드를 수동으로 파괴하는 것은 더욱 어려워졌다.

[0216] 코드는 컴퓨팅의 초기 형태인 기계 기반 암호로 발전했다. 당시 코드를 파괴하는 유일한 방법은 암호 기계를 훔쳐서 파일을 암호화하는 것과 동일한 도구를 사용하여 메시지를 해독하는 것이었다. 문제는 훔치는 것이 검출되

지 않고 암호 기계를 훔치는 방법이었다. 코드 기계가 손상된 것으로 알려졌다면, 적군은 간단히 코드를 변경하고 이미 동작중인 암호 기계를 업데이트만 하면 된다. 이 원칙은 현재까지도 여전히 실천되고 있으며, 가장 효과적인 사이버 공격은 검출되지 않은 공격이다.

[0217] 컴퓨팅과 냉전 시대의 도래로 인해, 암호화는 더욱 복잡해졌지만, 그러나 암호화 코드를 해독하는데 사용된 컴퓨터의 속도 또한 향상되었다. 보안 통신 개발의 각 단계에서, 정보를 암호화하는 기술 및 노하우와 암호화 코드를 해독하는 능력이 그 속도로 거의 발전되지 않았다. 암호화의 주요한 다음 진화 단계는 오늘날에도 여전히 사용되는 1970년대의 이중 키 암호화의 혁신으로 이루어졌다. 가장 잘 알려진 이중 키 암호화 방법 중 하나는 그 개발자인 리베스트(Rivest), 샤미르(Shamir) 및 아델만(Adleman)의 이름을 딴 RSA 공개 키 암호화 시스템이다. 공표된 RSA를 알고 있음에도 불구하고, 동시대의 개발자들은 동일 원칙을 독자적으로 고안했다. RSA는 공중에게 비밀로 유지되는 2개의 큰 소수에 기반하는 2개의 암호 키를 사용한다. 하나의 알고리즘은 이들 2개의 소수를 여기에서 E-키로 언급되는 암호 키로 변환하는데 사용되고, 동일한 2개의 비밀 소수를 여기에서 D-키로도 지칭되는 비밀 암호 키로 변환하기 위해 상이한 수학적 알고리즘이 사용된다. 여기에서는 "키 공개자"로서 지칭되는 비밀의 소수를 선택한 RSA 사용자는 전형적으로 1024b 내지 4096b의 크기를 포함하는, 알고리즘 방식으로 생성된 E-키를, 파일 암호화를 원하는 사람에게 배포 또는 "공개"한다. 이 키는 암호화되지 않은 형태로 많은 당사자에게 배포될 수 있기 때문에, 상기-E 키는 "공공 키"로서 알려져 있다.

[0218] 키 공개자와 통신하기를 원하는 당사자는 특별한 키 게시자에게 송신될 임의의 파일을 암호화하기 위해, 전형적으로 상업용 소프트웨어 형태로 제공되는 공개적으로 사용 가능한 알고리즘과 함께 이 공용 전자 키를 사용한다. 암호화된 파일의 수신에 따라, 키 게시자는 그 후 파일을 해독하기 위해 그 비밀 D-키를 사용하여, 이를 평문으로 복귀시킨다. 일반적으로 이중 키 방법과 RSA 알고리즘의 고유한 특징은 특히 파일을 암호화하는데 사용된 공공 E-키가 해독에 사용될 수 없다는 점이다. 키 게시자에 의해 소유된 비밀의 D-키만이 파일 해독의 능력을 갖고 있다.

[0219] 파일 암호화 및 해독에서 이중 키, 분할 키 또는 다중 키 교환의 개념은 구체적으로 RSA 또는 임의의 하나의 알고리즘 방법으로 제한되지 않지만, 통신 방법을 단계의 시퀀스로서 방법론적으로 특정한다. 스위치 패킷 통신 네트워크에 걸친 이중-키 교환에서, 디바이스, 예를 들어, 휴대폰으로부터 보안 파일을 수신하기를 원하는 노트북은 먼저 소정 알고리즘을 이용하여 2개의 키, 즉 암호화를 위한 E-키 및 해독을 위한 D-키를 발생시킨다. 그 후, 노트북은 IP 패킷을 수반하는 공공 네트워크 통신을 사용하여 E-키를 휴대폰에 송신한다. 암호화되지 않은 형태의 IP 패킷은, 그 페이로드로서, 전송 프로토콜(TCP) 및 E-키의 암호화된 복사본뿐만 아니라, 휴대폰의 목적지 IP 어드레스 "CP" 및 상응 포트와 함께, 노트북의 MAC 어드레스, IP 소스 어드레스 "NB" 및 포트 어드레스를 포함한다.

[0220] 이어서, 합의된 암호화 알고리즘 또는 소프트웨어 패키지를 사용하여, 휴대폰은 휴대폰으로부터 노트북으로의 보안 통신에서 IP 패킷의 페이로드로서 운반되는 암호화된 파일, 즉 암호문을 생성하기 위해서, 암호화 알고리즘 및 암호화 E-키를 사용하여 평문 파일을 프로세스한다. IP 패킷의 수신 시에, 알고리즘은 비밀 해독 키 즉, D 키를 사용하여 파일을 해독한다. D-키가 그 상응 E-키와 일치하도록 만들어지기 때문에, 본질적으로 알고리즘은 암호문을 해독하여 다시 암호화되지 않은 평문으로 되돌리기 위해서 두 키에 관한 지식을 이용한다. IP 패킷의 페이로드가 암호화된 파일, 즉 암호문의 형태로 보안 되지만, IP 패킷의 나머지는 암호화되지 않고, 또한 소스 IP 어드레스 "CP" 및 포트 및 목적지 IP 어드레스 "NB" 및 관련의 포트를 포함하는 임의의 사이버 해적에 의해 스니핑 가능하며, 판독될 수 있다. 따라서 페이로드 자체가 오픈될 수 없더라도, 통신은 모니터링될 수 있다.

[0221] ***가상 사설 네트워크*** - 암호화에 의존하는 다른 보안 방법은 "가상 사설 네트워크" 또는 VPN의 보안 방법이다. VPN에 있어서, 암호화된 IP 패킷을 사용하여 네트워크에 터널 또는 보안 파이프가 형성된다. 페이로드만 암호화하기보다는, VPN에서 전체 IP 패킷이 암호화되고, 그 후 캡슐화된 패킷을 하나의 VPN 게이트웨이로부터 다른 VPN 게이트웨이로 전송하는 뮬(mule) 또는 반송파로서 동작하는 다른 암호화되지 않은 IP 패킷 내로 캡슐화된다. 본래, VPN은 이질적인 근거리 통신망을 장거리로 함께 연결하기 위해, 예를 들어 뉴욕, 로스앤젤레스 및 도쿄에서 사설 네트워크를 운영하는 회사가, 하나의 글로벌 사설 네트워크를 공유하는 것과 같이, 동일한 기능을 사용하여 다양한 LAN을 상호 연결하기를 원할 때 사용되었다.

[0222] 기본적인 VPN 개념은, 예를 들어, rf를 통해서 무선으로 그리고 유선 연결을 통해 많은 수의 디바이스를 지원하는 하나의 LAN의 일부로서 제1 서버가, VPN 터널을 가로지르는 암호화된 콘텐츠를 포함하는 "가상 사설 네트워크" 또는 VPN에 의해서, 데스크탑, 노트북, 및 다른 WiFi 기반의 스테이션에 대한 유선 연결을 가지는 제2 서버

에 연결되는, 2개의 디바이스들 사이의 암호화된 통신으로 생각될 수 있다.

[0223] 이러한 비교적 좁은 대역폭 링크에 더하여, 제1 서버는 또한 넓은 대역폭 연결을 통해서 수퍼 컴퓨터에 연결될 수 있다. 결과적인 데이터 통신은, 외부 IP 패킷 내에 임베딩된 내부 VPN 패킷을 포함하는 데이터 패킷의 시퀀스를 포함한다. 동작 시에, 소스 IP 어드레스 및 소스 포트 #를 특정하는, 서버 A로부터의 외부 IP 패킷은 목적지 IP 어드레스 및 목적지 포트 #에서 서버 B로 송신된다. 이러한 외부 IP 패킷은, 데이터 전달을 위해서 서로에 대한 암호화된 터널을 형성하기 위해서, 제1 및 제2 서버 사이에 통신을 구축한다. 외부 패킷에 의해서 수반되는 VPN 페이로드는 라스트 마일 IP 패킷을 포함하여, 말단 디바이스, 예를 들어 소스 IP 어드레스 "DT" 및 그 상응 애드혹 포트 #를 갖는데스크탑, 그리고 다른 말단 디바이스, 예를 들어 소스 IP 어드레스 "NB" 및 그 상응 애드혹 포트 #를 갖는 노트북 사이의 직접적인 통신을 제공한다. 비록 임의의 통신 세션이 개시될 수 있지만, 하나의 예에서, 파일 전달을 위한 요청은 VPN 터널을 통해서 실시된다.

[0224] 가상 사설 네트워크를 사용하여 안전하게 이런 전송을 설정하기 위해, 실제 통신이 개시되기 전에 VPN 터널이 생성되고 세션이 시작된다. 기업 애플리케이션에서, VPN 터널은 인터넷을 통해 수반되지 않고, 그 대신 그 자체의 광섬유 및 하드웨어 네트워크를 소유하는 전용 ISP 또는 캐리어에 의해 종종 수반된다. 이러한 캐리어는 종종 주어진 비용에 대해 지정 대역폭을 보장하도록, VPN 서비스를 요구하는 회사와의 연간 또는 장기 계약 계약을 체결한다. 이상적으로는, 고속 전용 링크는 VPN의 성능, QoS 또는 보안을 방해하는 중간 또는 "라스트 마일" 연결이 없이, 직접 연결된다.

[0225] 동작 시에, 통상적인 VPN은 2-단계 프로세스 - VPN을 생성하기 위한 또는 VPN에 "로그인"하기 위한, 그리고 보안 파이프 또는 터널 내에서 데이터를 전달하기 위한 제2 단계 -를 필요로 한다. 터널링의 개념은, 계층 1 내지 계층 4를 포함하고, 계층 5는 가상 VP 세션(723)을 생성하기 위해서 이용되고, 프레젠테이션 계층인 계층 6은 서버들 사이에서 VPN 게이트웨이-대-게이트웨이 파이프를 형성하는데 필요한 암호화를 촉진하기 위해서 이용되는, (VPN 연결을 수반하기 위해서 이용되는) 7-계층 통신 스택에 의해서 실행되는 외부 IP 패킷으로서 계층적인 것으로 생각될 수 있다. VPN 연결이 IP 패킷을 송신하기 위해서 인터넷 프로토콜을 이용하지만, VPN의 PHY 계층 1 및 VPN 데이터 링크 계층 2는, 인터넷에 걸친 예측될 수 없는 라우팅을 최소화하기 위해서, 전용 캐리어에 의해서 종종 지원된다. 예를 들어 통신하는데스크탑들 사이의 디바이스-대-디바이스 통신으로서 전달되는 애플리케이션 계층 7 데이터는, VPN이 존재하지 않는 경우에서와 같은 통신을 구축하기 위해서 필요한 모두 7개의 OSI 계층을 포함하는 터널링된 데이터로서 전달된다. 이러한 방식으로, VPN은 VPN 내부 패킷을 이송하기 위해서 이용되는 계층-7 내에서 동작하는 통신 프로토콜로서 생각될 수 있다.

[0226] 동작 시, 외부 IP 패킷은, 하나의 통신 스택으로부터의 다른 통신 스택으로 일단 전달되면, 패킷의 실제 메시지인, 캡슐화된 데이터를 노출시키도록 개방된다. 이러한 방식으로, 엔드-투-엔드 통신은, VPN 터널이 임의의 통신 시도 전에 형성되어야만 하고 또한 대화가 종료된 후에는 닫혀져야만 한다는 점을 제외하고는, VPN 터널을 생성하는데 사용된 세부 사항을 무시하고 이루어진다. 먼저 VPN 터널을 여는 것을 실패하면, 결과적으로 IP 패킷 스니핑, 도용, 감염 등에 취약한 IP 패킷의 암호화되지 않은 전송이 초래될 것이다. 대화가 완료된 후 VPN을 닫지 않으면, 다른 사람의 VPN 터널에서의 불법 활동을 숨길 수 있는 기회를 사이버 범죄자에게 제공할 수 있으며, 가로채는 것이 발생되는, 무고한 사람에 대해 부과되는 가능한 형사 처벌을 초래할 수 있다.

[0227] VPN이 전용 용량 및 대역폭을 갖는 사설 연결을 이용하여 서로 상호 연결하기 위한 다수의 사설 근거리 네트워크를 위한 일반적인 방식이지만, 공공 네트워크 및 인터넷을 통한 VPN의 이용은 두 당사자 통신에서 문제가 있다. VPN에서의 하나의 문제는 VPN 연결이, 패킷-바이-패킷 기반이 아니라, 사용 전에, 미리 구축되어야 한다는 것이다. 예를 들어, 패킷-교환형 네트워크에 걸쳐 연결된 VoIP 통화에서, 휴대폰이 제2 휴대폰의 의도된 통화 수신자와 접촉할 수 있기 전에, VPN 세션을 먼저 구축하여야 한다. 이를 위해서, 통화자의 휴대폰에 먼저 VPN 연결 애플리케이션이 로딩되어야 한다. 이어서, 통화자는 IP 패킷을 VPN 호스트에, 전형적으로 서비스 제공자에게 송신하여야 한다. 이러한 패킷은 임의의 이용 가능한 라스트 마일 라우팅, 예를 들어 무선 통신을 통해서 휴대폰으로부터 근처의 WiFi 기반의 기지국까지, 이어서 유선 통신에 의해서 로컬 라우터로, 이어서 유선 통신에 의해서 VPN 호스트까지 전달된다. 통화자의 휴대폰과 VPN 호스트 사이의 세션이 구축되면, 통화자의 휴대폰은 이어서, 통화자의 휴대폰으로부터 VPN 호스트까지 VPN 터널을 생성하도록, VPN 호스트에 지시하여야 한다. 터널 내의 계층 5 세션이 계층 6에 의해서 암호화될 때, VPN 터널의 이러한 레그가 촉진된다.

[0228] VPN 연결이 일단 설정되면, 통화자의 휴대폰은 임의의 VoIP 전화 앱을 통해서 통화를 임의의 다른 전화에 위치시킬 수 있다. 통화되는 전화가 동일 VPN에 연결되지 않는 경우에, 애플리케이션은 목적지 통화 전화, 즉 통화되는 사람에 가장 가까운 VPN 호스트로부터 라스트 마일에 걸친 "콜 아웃" 링크를 구축하여야 한다. VoIP 애플

리케이션이 사용될 수 없거나 사용을 위해서 인증되지 않은 경우에, 통화가 실패할 것이고 즉각적으로 종료될 것이다. 그렇지 않은 경우에, 내부 IP 패킷은 통화하는 휴대폰과 목적지 휴대폰 사이에서 애플리케이션 계층 5 세션을 구축하여, IP 테스트 패킷이 적절히 해독되고 이해될 수 있는지를 확인할 것이다.

[0229] 통화를 위치시키기 위해서, 전화의 정상 다이얼 기능으로부터가 아니라, 통화자의 전화, 즉 캐리어의 데이터 플랜을 사용하는 휴대폰 앱에서 동작되는 계층 7 애플리케이션으로부터 통화가 와야 하는데, 이는 전화 내의 전화 캐리어의 SIM 카드가 VPN 터널과 양립될 수 없기 때문이다. 통화가 개시되면, 통화자의 휴대폰은, 통신 애플리케이션에 따른 소리의 작은 단편 또는 "스닙펫(snippet)"을 나타내는 연속적인 IP 패킷을 전송한다. 이러한 패킷은 통화자의 휴대폰 내의 애플리케이션으로부터 네트워크를 통해서, 예를 들어 WiFi 링크를 통해서 근처의 WiFi 기반의 기지국으로 송신되고, 이어서 유선 연결을 통해서 라우터에, 그리고 최종적으로 유선 연결을 통해서 VPN 호스트에 송신된다. 이어서, 데이터는, 목적지 VPN 게이트웨이인, VPN 네트워크의 말단 디바이스에 대한 VPN 터널을 통해서 VPN 호스트로 보안 송신된다. 이러한 예에서, VPN 터널은 목적지 휴대폰까지 전혀 연장되지 않고, 그 대신 통화되는 디바이스에 도달하기 전에 중단된다. VPN의 목적지 게이트웨이를 넘어서, 데이터는 더 이상 암호화되지 않는데, 이는 VPN 캐리어가 더 이상 관여되지 않기 때문이다. VPN 터널을 떠나는 데이터 패킷에서, VPN 호스트는 목적지 디바이스의 라스트 마일 연결, 예를 들어 유선 연결을 경유하여 데이터를 가까운 라우터에 계속 전달하고, 이어서 로컬 휴대폰 시스템 및 타워에 대한 유선 연결에 의해서, 2G, 3G 또는 4G 전화통신을 이용하여 정상 셀룰러 전화 통화로서 통화를 전송한다. 휴대폰 앱으로부터 동일 앱을 작동시키지 않는 전화로 통화하는 프로세스는 "콜 아웃" 특징으로 지칭된다.

[0230] 전술한 예는 공공 네트워크에 걸친 VPN에 대한 연결에서의 다른 문제를 강조한다 - VPN 호스트로부터 통화되는 사람까지의 라스트 마일 링크는 VPN의 일부가 아니고, 그에 다라 보안, 성능 또는 통화 QoS를 보장하지 않는다. 구체적으로, 연결을 포함하는 통화자의 라스트 마일은 전부 스니핑에 열려 있고 사이버-공격에 노출된다. 통화가 완료되고 통화자의 휴대폰이 끊기면, VPN 링크가 종료되어야 하고, 그에 의해서 VPN 계층 5은 VPN 세션의 폐쇄를 조정하고 통화자의 휴대폰은 VPN 호스트로부터 분리된다.

[0231] 컴퓨터-대-컴퓨터 데이터 전달을 위해서 원래 생성된, 가상의 사설 네트워크의 적응은 몇몇 주요 문제를 갖는다.

[0232] * 목적지 VPN 게이트웨이로부터 목적지 휴대폰까지의 라스트 마일 통신은 보안이 되지 않고, 스니핑 및 감시 위험이 있다.

[0233] * 통화자의 휴대폰과 VPN 게이트웨이 사이의 라스트 마일 통신은, 통화자가 데이터 통신 기반의 앱을 이용하는 경우에만, 안전하다. 통화자가 전화통신 링크, 즉 다이얼 특징을 이용하여 VPN 게이트웨이에 연결하는 경우에, 통화자의 휴대폰으로부터 가장 가까운 VPN 게이트웨이로의 라스트 마일 통신은 안전하지 않고, 스니핑 및 감시 위험이 있다.

[0234] * 양 당사자가 데이터 통신을 이용하고 그들의 관련 라스트 마일 링크에 걸친 전화통신을 이용하지 않는 경우에 그리고 양 당사자가 통화를 개시하기에 앞서서 동일 VPN에 합류하는 것을 아는 경우에만 통화가 보안 엔드-투-엔드가 될 수 있다. 마지막 중요 항목은 보안 VPN 통신의 역설을 강조한다 - 통화되는 사람은, 네트워크에 합류하기 위해서, 그들이 통화되기 전에 통화되고 있다는 것을 알 필요가 있다. 통화되고 있다는 것을 그들에게 알리기 위해서, 통화가 시작되기 전에, 그들은 먼저 연결되어야 하고 VPN에 로그인 하도록 지시받아야 한다. 본질적으로, 보안 전화 통화에 연결하기 위해서, 이들은 미보안 전화 통화를 수신하여야 한다. 미보안 전화 통화는 용이하게 해킹, 스니핑, 및 감시된다. 또한, 미보안 통화의 메타데이터는 누가 통화하는지, 누가 통화되는지, 그리고 언제 통화가 발생되는지를 노출시킨다. 통화 메타데이터는 사람의 활동을 추적하는데 있어서 또는 범죄의 표적으로서 이들을 프로파일링하는데 있어서 매우 유용하다.

[0235] 보안 염려를 무시하더라고, 이하를 포함하는 다른 이유 중 임의의 이유로 인해서, VPN을 통해서 통화를 위치시키는 것 또는 서류를 보내는 것이 실패하지 않는다는 것이 보장되지 않는다:

[0236] * VPN은 실시간 애플리케이션, VoIP 또는 비디오를 지원하기에 충분히 짧은 대기 시간으로 동작하지 않을 수 있다.

[0237] * 통화자로부터 VPN 게이트웨이로 또는 VPN 게이트웨이로부터 통화 수신기로의 VPN 라스트 마일 연결은, 실시간 애플리케이션, VoIP 또는 비디오를 지원할 수 있을 정도로 충분히 짧은 대기 시간으로 동작하지 않을 수 있다.

[0238] * 통화자 또는 의도된 수신기에 가장 가까운 VPN 게이트웨이, 즉 "라스트 마일"은 매우 멀리 있을 수 있으며, 가능하게는 VPN이 없는 통화 수신기에 대한 거리보다 훨씬 더 멀어서, 연결이 과도한 대기 시간, 네트워크 불안

정성, 알려지지 않은 네트워크를 통한 제어되지 않은 라우팅, 다양한 QOS, 및 연결의 보호되지 않은 부분에서의 중간자 공격에 대한 수많은 기회에 노출되게 한다.

[0239] * VPN 게이트웨이로부터 통화 수신기로의 VPN 라스트 마일 연결은, "콜 아웃"연결 및 패킷 포워딩 또는 로컬 텔코로의 지원 링크를 지원하지 않을 수 있다.

[0240] * 지역 캐리어 또는 정부 검열관은 국가 안보 또는 규정 준수라는 이유로 알려진 VPN 게이트웨이 내외로의 통화 또는 연결을 차단할 수 있다.

[0241] * 회사 VPN을 사용할 때, VoIP 통화는 단지 회사 직원 및 지정된 허가된 사용자에게만 그리고 그로부터 제한될 수 있으며, 금융 거래 및 비디오 스트리밍이 차단될 수 있으며, 야후, 구글 등과 같은 공공 이메일 서버에 대한 사적 이메일이 차단될 수 있고, 유튜브, 채팅 프로그램 또는 트위터와 같은 많은 웹 사이트는 회사 정책에 따라 차단될 수 있다.

[0242] * 불안정한 네트워크의 경우, VPN 운영자에 의해 수동으로 리셋될 때까지, VPN이 개방되고 통화자의 디바이스에 연결된 영구적인 세션을 유지할 수 있다. 이는 후속 연결을 위한 대역폭의 손실 또는 값비싼 연결 비용을 초래할 수 있다.

[0243] ***네트워크 비교*** - "오버 더 탑" 또는 OTT 제공자에 의해 제공된 통신과 애드혹 VPN에 연결하기 위해 공공 네트워크를 사용하는 통신 시스템을 비교하면, VPN 링크 자체 이외에도, 두 통신 시스템의 대부분은 거의 동일한 구성 요소 및 연결을 갖고 있음을 용이하게 알 수 있다. 구체적으로, 휴대폰 WiFi 무선 연결, WiFi 기지국, 유선 연결 및 라우터를 포함하는 통화자의 라스트 마일이 양 구현예에서 동일한 라스트 마일 연결성을 나타낸다. 유사하게, 다른 당사자의 라스트 마일 상에서, 통화자의 휴대폰, 휴대폰 연결, 셀 기지국 및 타워, 유선 연결 및 라우터는 인터넷 및 VPN 버전 모두에 대해 동일하다. 주요한 차이점은 공공 네트워크에서 VPN 호스트들 사이의 보안 통신을 갖는 VPN 터널이, 클라우드 전체를 통해서 미보안 통신을 수반하는 서버/라우터에 의해 대체된다는 점이다. 다른 차이점은 OTT 통신에 있으며, 통화는 즉각적으로 이용될 수 있고, VPN을 이용할 때, VPN을 설정하기 위해서 그리고 통화 전에 그리고 통화 이후에 VPN 세션을 종료시키기 위해서 여분의 단계가 요구된다.

[0244] 두 예에 있어서, 라스트 마일 연결은 예측할 수 없는 통화 QOS, 패킷 스니핑에 대한 노출, 및 사이버 공격 위험을 제공한다. 서버/라우터가 서로 상이한 로케일에서 상이한 ISP에 의해서 관리되기 때문에, 서버를 기존의 다른 클라우드들로서 해석할 수 있다. 예를 들어, 구글, 야후, 아마존, 및 마이크로소프트가 소유하고 그에 의해서 운영되는 공공 개방 네트워크가, 비록 이들 모두가 인터넷에 의해서 상호 링크되지만, 상이한 클라우드들로서, 예를 들어 "아마존 클라우드"로서 간주될 수 있다.

[0245] 경쟁적인 네트워크이나 덜 대중적인 토폴로지, 피어-투-피어 네트워크 또는 PPN은 라우터 또는 ISP가 아니라 PPN에 의해 관리되는 패킷 라우팅을 갖는 많은 수의 피어로 구성된 네트워크를 포함한다. 피어-투-피어 네트워크가 수십 년 동안 하드웨어에 존재했지만, 인터넷 서비스 제공자의 제어, 비용, 및 규제를 피하는 수단으로 개념을 대중화한 것은 냅스터(Napster)였다. 음악 저작권 침해에 대한 미국 정부의 규제에 의해 소송이 제기되었을 때, 냅스터의 선구자들은 빠져나와서, 초기 OTT 캐리어 스카이프에 침입하였다. 그 당시 스카이프의 네트워크는 전통적인 OTT로부터 냅스터와 유사한 PPN으로 변환되었다.

[0246] PPN 동작에서 PPN에 대해 로그인 연결을 형성하는 모든 디바이스는 PPN에서 하나 이상의 노드가 된다. 예를 들어, 하나의 지리적 위치에서, PPN 소프트웨어가 설치된 휴대폰이 피어-투-피어 네트워크에 로그인하면, 해당 지역 내의 다른 모든 연결된 디바이스는 네트워크의 일부가 된다. 하나의 디바이스에서 다른 디바이스로 전화를 걸면 다른 디바이스에서 PPN에 연결된 다른 디바이스로 연결된다. 예를 들어, 휴대폰이 그 PPN 연결을 사용하여 다른 PPN 연결된 디바이스, 예를 들어 휴대폰으로 통화한다면, 그러한 통화는 두 당사자 사이의 PPN에 물리적으로 위치된 임의의 디바이스(들)를 통한 우회 경로를 따른다. 예를 들어, 통화자의 휴대폰으로부터 나오는 통화는 WiFi에 의해서 로컬 WiFi 기지국을 통해 근처의 데스크탑에, 그 후에 다른 사람의 노트북에, 다른 데스크탑에, 또 다른 데스크탑에, 그리고 마지막으로 로컬 휴대폰 기지국 및 타워를 통해 목적지 휴대폰에 연결된다. 이 방식으로 모든 라우팅은 PPN에 의해서 제어되었으며, 인터넷은 라우팅의 관리에 포함되지 않았다. 양 당사자가 사용하기 때문에, 네트워크에 연결하는데 사용되는 PPN 소프트웨어는 VoIP 기반 음성 통신을 위한 애플리케이션으로서 작용한다.

[0247] 하나의 휴대폰이 지구의 반대편에 있는 비-PPN 디바이스 휴대폰을 통화하려는 경우에, 특히 바다 또는 산맥을 가로질러 패킷을 송신하기 위해서, 라우팅이 일부 링크 상에 인터넷을 필수적으로 포함할 수 있다. 로컬 지리적 위치에서 라우팅의 제1 부분이 이전의 예와 유사한 방식으로 진행되어, 통화자의 휴대폰으로부터 시작하여 WiFi

기지국, 데스크탑, 노트북, 다른 데스크탑 등을 통해 라우팅된다. 이 시점에서 가장 가까운 노트북이 네트워크에 연결되어 있다면, 통화는 이를 통해 라우팅될 것이고, 그렇지 않으면 통화는 로컬 휴대폰 기지국 및 타워를 통해서 휴대폰으로 라우팅되고, 그 후에, 이를 계속 송신하기 전에, 휴대폰 기지국 및 타워로 되돌린다.

[0248] 전화가 태평양을 횡단한다면, 컴퓨터 및 휴대폰은 대양을 가로질러 트래픽을 운반할 수 없으므로, 통화는 반드시 호스팅된 클라우드의 인터넷 제3자 서버/라우터까지, 그리고 다른 클라우드 내의 제3자 서버/라우터에 대한 연결을 통해서 앞으로 라우팅된다. 예를 들어, 이러한 것이 그 목적지에 접근할 때, 통화는 인터넷을 떠나고, 먼저 데스크탑을 통해서 목적지 지리적 위치 내의 PPN에 진입하고, 그러한 데스크탑은 다시 WiFi에, 노트북에, 그리고 기지국에 연결된다. WiFi가 PPN 앱을 동작시키기 않기 때문에, WiFi에 진입하는 실제 패킷은 WiFi 서브넷 내의 태블릿 또는 휴대폰까지 이동되어야 하고, 유선 연결을 통해서 휴대폰 기지국 및 타워 상으로 송신되기 전에, WiFi로 복귀되어야 한다. 마지막으로, 통화자 휴대폰 통화는, PPN 인에이블링 디바이스가 아닌 목적지 휴대폰에 연결된다. 그에 의해서, 연결은 PPN을 위한 "콜 아웃"을 구성하는데, 이는 그러한 것이 PPN 네트워크를 빠져나오기 때문이다. 이러한 PPN 접근방식을 이용할 때, VPN과 마찬가지로, 통화를 위치시키는 것은, PPN 로그인을 완료하는 것에 의해서, 통화 디바이스를 PPN 네트워크에 먼저 등록하는 것을 포함한다. 그 후에, 통화가 PPN 앱을 이용하여 위치될 수 있다. PPN 접근법의 장점은 장거리에 대한 통화를 운반하는데 하드웨어가 거의 또는 전혀 필요 없으며, 또한 PPN에 연결되는 모든 디바이스가 그 상태, 로딩 및 대기 시간과 관련하여 PPN 운영자를 규칙적으로 업데이트하기 때문에, PPN 운영자는 지연을 최소화하기 위한 패킷의 라우팅을 결정할 수 있다는 것이다.

[0249] 이러한 접근방식의 단점은 패킷이 잠재적인 보안 위협을 나타내고 또한 통화 지연 및 통화 QoS 상에 예측할 수 없는 충격을 갖는 많은 알 수 없는 노드를 포함하는 네트워크를 통과한다는 점이다. 따라서 스카이프를 제외하고, 계층 3에서 또는 그 초과에서 동작하는 피어-투-피어 네트워크는 패킷 교환형 통신 네트워크에서 일반적으로 이용되지 않는다.

[0250] 애드혹 VPN 제공자, 인터넷 OTT 제공자, 및 PPN 피어 네트워크의 비교 요약이 아래 표에서 대비되어 있다.

표 2

[0251]

| 네트워크 | 가상의 사설 VPN | 인터넷 OTT | 피어-투-피어 PPN |
|---|---|---|---|
| 노드 | 공공/호스팅된 서버 | 공공 라우터/서버 | PPN 사용자 |
| 노드 능력 | 알려진 기반시설 | 알려진 기반시설 | 혼합됨, 알려지지 않음 |
| 클라우드 대역폭 | 보장됨 | 예측 불가능 | 예측 불가능 |
| 라스트 마일 대역폭 | 제공자 의존적 | 제공자 의존적 | PPN 의존적 |
| 대기 시간 | 관리 불가능 | 관리 불가능 | 최적의 작용 |
| 네트워크 안정성 | 관리 불가능 | 관리 불가능, 중복 | 최적의 작용 |
| 통화 설정 | 복잡한 로그인 | 요구되지 않음 | 로그인 |
| 사용자 신원 | 사용자 이름 | 전화 번호 | 사용자 이름 |
| VoIP QoS | 양호까지 가변적 | 가변적 | 가변적 |
| 클라우드 보안 | 암호화된 페이로드만 | 미암호화 | 미암호화 |
| 라스트 마일 보안 | 미암호화 | 미암호화 | 미암호화 |
| 스니핑 가능 | 패킷 헤더(클라우드)<br>전체 패킷(라스트 마일) | 전체 패킷 | 전체 패킷 |

[0252] 도시된 바와 같이, VPN 및 인터넷은 고정된 기반 시설을 구성하지만, 피어-투-피어 네트워크의 노드는 로그인한 사람과 PPN에 연결된 디바이스에 따라 달라진다. 네트워크의 고속 장거리 연결, 예를 들어 대양과 산맥을 횡단하는 네트워크로서 이 표의 맥락에 정의된 클라우드 대역폭은, VPN의 경우에만 계약 상 보장되며, 그렇지 않으면 예측할 수 없다. 라스트 마일 대역폭은 인터넷 및 VPN 제공자 모두에 따라 달라지는 로컬 제공자이지만, PPN은 전적으로누가 로그인했는지에 따라 달라진다.연속적으로 송신된 IP 패킷의 전파 지연인, 대기 시간은 OTT 및 VPN에 대해 관리할 수 없는데, 이는 제공자가 라스트 마일에서 라우팅을 제어하지는 않지만, 그 대신 로컬 텔코 또는 네트워크 제공자에 의존하는 한편, 특별한 지리적 위치에서 해당 시간에 온라인 상태인 노드들 사이에서 트래픽을 지향시키기 위해 최상의 노력을 사용하는 제한된 능력을 갖기 때문이다. 마찬가지로, 네트워크 안정성을 위해, PPN은 네트워크를 유지하기 위해 트래픽을 재라우팅할 수 있지만, 그러나 로그인한 사람에 전적으로 의존한다. 다른 한편으로, 인터넷은 본질적으로 중복되어 있으며 전달을 보장하는 것이 확실하지만, 반드시 시기적절한 것은 아니다. 애드혹 VPN 에 대한 네트워크 안정성은 VPN 호스트에 대한 연결 권한이 부여된 노드 수

에 따른다. 이들 노드가 오프라인이 되면, VPN은 무능력해진다.

[0253] 통화 설정 관점에서, 인터넷은 항상 사용 가능하며, PPN은 전화를 걸기 전에 PPN에 로그인하는 추가 단계가 필요하며, VPN은 복잡한 로그인 절차를 포함할 수 있다. 더욱이, 대부분의 사용자는 OTT가 VPN 및 PPN에 의해서 사용되는 별도의 로그인 ID보다는 사용 용이성의 주요 이점으로 전화번호의 OTT 사용을 고려한다. 나열된 모두 3개의 네트워크는 가변형 VoIP QoS로 인해 어려움을 겪고 있으며, 일반적으로 상용 전화기술 캐리어보다 훨씬 뒤떨어져 있다.

[0254] 보안상 관점에서, 3가지 옵션 모두는 판독 가능한 어드레스 및 페이로드를 갖는 패킷 스니핑에 완전히 노출된 라스트 마일에 의해 좋지 못하다. VPN은 클라우드 연결의 암호화를 제공하지만, 그러나 VPN 호스트의 IP 어드레스를 노출시킨다. 따라서 도시된 네트워크 옵션은 안전하다고 간주되지 않는다. 따라서 암호화는 다양한 애플리케이션에 의해 해킹 및 사이버 공격을 방지하도록 계층 6 프로토콜 또는 계층 7 애플리케이션 자체의 임베딩된 부분으로 사용된다.

[0255] ***암호화에 대한 파잉 신뢰*** - IP 패킷을 암호화하거나 VPN을 설정하는데 사용되는지의 여부와는 관계없이, 오늘날의 네트워크 보안은 거의 전적으로 암호화에만 의존하며 또한 최신 패킷 교환형 기반 통신 네트워크에 하나의 약점을 나타내고 있다. 예를 들어, RSA 암호화를 공격하는 방법에 대해 많은 연구가 수행되었다. 소수를 큰 크기로 제한하는 것은 무차별적인 힘 방법을 사용하여 해독 D-키 코드를 파괴할 위험을 크게 줄이는 반면에, 다항식 요소 방법은 보다 작은 소수 기반 키에 기초하여 키를 균열시키는데 있어서 성공적으로 시연되었다. "양자 컴퓨팅"의 진화는 궁극적으로 합리적인 사이버 공격 시간에 RSA 기반 및 다른 암호화 키를 파괴하는 실제적인 방법으로 이어질 것이라는 우려가 존재한다.

[0256] 이전에 존재했던 코드 파괴의 위험성을 극복하기 위해, 2001년 US NIST 에 의해 채택된 "진보된 암호화 표준"이나 AES 암호와 같은 새로운 알고리즘 및 "더 큰 키" 암호화 방법이 등장했다. 라인달(Rijndael) 암호에 기초하여, 대체-치환 네트워크(substitution-permutation network)로서 알려진 설계 원리는, 상이한 키 및 블록 크기를 사용하여 텍스트 대체 및 순열을 조합한다. 그 현재의 형태에서, 알고리즘은 128, 192 비트 및 256 비트의 가변 길이를 포함하는 키를 갖는 128 비트의 고정 블록 크기를 포함하며, 입력 파일 변환에 사용된 대응하는 반복 횟수는 10, 12, 및 14 사이클이다. 실제적 문제로서, AES 암호는 소프트웨어 또는 하드웨어에서 키의 크기와는 관계없이 효율적이고 신속하게 실행될 수 있다. 암호화 토착어에서, 256b 키를 사용하는 AES 기반 암호화는 AES256 암호화로서 지칭된다. 512b 키를 사용하는 AES512 암호화도 사용할 수 있다.

[0257] 새로운 세대가 암호 기술을 향상시켜 보다 나은 암호화 방법을 만들고 그리고 이들을 신속하게 깨뜨리는 반면에, 이익을 추구하는 사이버 범죄자는 단순히 컴퓨팅을 사용하여 암호화된 파일을 파괴하기보다는 그 표적에 자주 집중한다. 이미 기재된 바와 같이, 패킷 스니핑과 포트 심문을 사용하여, 사이버 해적은 대화, 회사 서버 또는 심지어 VPN 게이트웨이에 대한 중요한 정보를 얻을 수 있다. 사이버 프로파일링에 의해, 네트워크 자체를 공격하기보다는 회사의 CFO 또는 CEO의 개인용 컴퓨터, 노트북 및 휴대폰에 대한 사이버 공격을 시작하는 것이 더 쉬울 수도 있다. 임베딩된 링크를 열었을 때 맬웨어 및 스파이웨어를 자동으로 설치하는 이메일을 고용자에게 보내는 것은 방화벽 보안을 완전히 우회하는데, 그 이유는 이들이 필수적으로 연결하여 동작해야 하는 "내부"로부터 네트워크에 들어가기 때문이다.

[0258] 데이터가 변경 없이 즉 정적으로 네트워크를 통해 이동한다면, 암호화를 파괴할 가능성도 높아진다. 예를 들어, 도 1의 네트워크에서, 패킷(790, 792, 794, 799)의 하부 데이터는 패킷이 네트워크를 통해 이동함에 따라 변경되지 않는다. 도시된 각각의 데이터 패킷은 이것이 생성되었을 때 그 본래의 순서대로 변경되지 않은 시간 또는 페이지로 순차적으로 배열되는 일련의 데이터 또는 소리를 포함한다. 데이터 패킷의 콘텐츠가 텍스트라면, 시퀀스 1A-1B-1C-1D-1E-1F에서 암호화되지 않은 평문 파일을 읽는 것은 코뮤니케 번호 "1"에 대한 "읽기 쉬운"텍스트로 나타날 것이다. 데이터 패킷의 콘텐츠가 오디오라면, 시퀀스 1A-1B-1C-1D-1E-1F에서 암호화되지 않은 평문 파일을 변환, 즉 "재생"하는 것은 본질적으로 소프트웨어 기반 D/A 변환기인 대응의 오디오 코덱을 통해 오디오 파일 번호 "1"에 대한 소리로 나타날 것이다.

[0259] 어느 경우나, 본 발명 전체에 걸쳐, 고정된 크기 박스로 표현되는 각각의 데이터 슬롯은 규정된 수의 비트, 예를 들어 2 바이트(2B) 길이를 포함한다. 슬롯당 정확한 비트 수는, 네트워크에서의 모든 통신 노드가 각 데이터 슬롯의 크기를 아는 한 유연하다. 각 데이터 슬롯에는 오디오, 비디오 또는 텍스트 데이터가 포함되어 있으며, 도면에서 번호 뒤에 텍스트가 표기되어 있다. 예를 들어, 도시된 바와 같이, 데이터 패킷(790)의 제1 슬롯은 숫자 "1"이 지정 통신 # 1을 나타내고 텍스트 "A"가 통신 # 1의 데이터의 제1 부분을 나타내는 콘텐츠(1A)를 포함한다. 마찬가지로, 데이터 패킷(790)의 제2 슬롯은 숫자 "1"이 이것이 동일한 통신 # 1의 일부임을 나타내는 텍

스트 "1B"를 포함하고 또한 텍스트 "B"는 1A의 순차적으로 이어지는 통신 # 1 에서의 데이터의 제2 번째 부분을 나타내는 콘텐츠(1B)를 포함한다.

[0260] 예를 들어, 동일한 데이터 패킷이 가상으로 포함된 콘텐츠 "2A"를 포함한다면, 데이터는 상이한 통신에서, 특히 통신 # 1 과는 관계 없는 통신 # 2 에 대한 제1 패킷 "A"를 나타낸다. 균질한 통신을 포함하는 데이터 패킷, 예를 들어 통신 # 1에 대한 모든 데이터는 상이한 통신을 혼합하는 것보다 분석 및 판독하기가 더 쉽다. 적절한 순서로 순차적으로 배열된 데이터는 이것이 오디오, 텍스트, 그래픽, 사진, 비디오, 실행 가능한 코드 등인지의 여부와는 관계없이, 사이버 공격자가 데이터의 특성을 해석하는 것을 용이하게 한다.

[0261] 더욱이, 도시된 예에 있어서, 패킷의 소스 및 목적지 IP 어드레스가 일정하게 유지되기 때문에, 즉 들어가거나 또는 나가는 게이트웨이 서버(21A, 21F)와 동일한 형태로 네트워크를 통한 전송 중 패킷이 바뀌지 않은 상태로 존재하는 경우, 하부의 데이터가 바뀌지 않기 때문에, 해커는 데이터 패킷을 가로챌 더 많은 기회를 갖고, 또한 파일을 분석 및 개봉하거나 또는 대화를 청취할 수 있는 더 좋은 기회를 가질 수 있다. 단순한 전송 및 1차원 보안, 즉 보호를 위한 암호화에만 의존하는 것은 사이버 공격의 위험을 증가시키는데, 그 이유는 패킷 교환형 네트워크와 같은 지나치게 단순화된 인터넷의 사용에서 성공의 가능성이 더 높기 때문이다.

[0262] **실시간 네트워크 및 연결된 디바이스 보안**

[0263] 오늘날의 패킷 교환형 네트워크를 괴롭히는 과잉의 보안 취약점을 해결하면서 전화, 비디오 및 데이터 통신의 서비스 품질(QoS)을 향상시키기 위해서, IP 패킷 라우팅 제어에 대한 새롭고 혁신적인 체계적인 접근법이 요구되며, 이종 기술을 포함하는 세계적인 네트워크를 관리하는 것은 동시에 엔드-투-엔드 보안을 지원한다. 이러한 독창적인 패킷 교환형 네트워크의 목표는 이하의 기준을 포함한다.

[0264] 1. 네트워크 전체를 통해 실시간 음성, 비디오 및 데이터 트래픽 라우팅을 동적으로 관리하는 단계를 포함하는 글로벌 네트워크 또는 텔코의 보안 및 QoS를 보장한다.

[0265] 2. 통신 네트워크의 라스트 마일에서 "로컬 네트워크 또는 텔코"의 보안 및 QoS를 보장한다.

[0266] 3. 미보안 라인을 통한 보안 통신 제공을 포함하여, 통신 네트워크의 "라스트 링크"의 보안 및 QoS를 보장한다.

[0267] 4. 미인증 또는 위조된 액세스 또는 사용을 방지하기 위해, 통신 디바이스의 보안을 확인하고 사용자를 인증한다.

[0268] 5. 무단 액세스를 방지하기 위해, 디바이스 또는 온라인 네트워크 또는 클라우드 저장소에 데이터를 저장하는 보안 수단을 촉진시킨다.

[0269] 6. 재무, 개인, 의료 및 생체 인식 데이터 및 기록을 포함하는 모든 비공개 개인 정보의 보안 및 프라이버시 보호를 제공한다.

[0270] 7. 온라인 뱅킹 및 쇼핑, 신용카드 및 전자 지불(e-pay)을 포함하는 모든 금융 거래의 보안 및 개인 정보 보호를 제공한다.

[0271] 8. M2M(Machine-to-Machine), V2V(Vehicle-To-Vehicle) 및 V2X(Vehicle-to-Infrastructure) 통신을 포함하는 처리 및 정보 교환에서 보안, 프라이버시 보호 및 필요에 따라 익명성을 제공한다.

[0272] 전술한 목표 중에서, 본 개시 내용에 포함된 발명적인 사안은 항목 # 2에 기재된 제2 토픽, 즉 "통신 네트워크의 라스트 마일 내의 로컬 네트워크 또는 텔코의 보안 및 QoS"에 관한 것이다. 이러한 토픽은 실시간 통신 성능을 희생시키지 않는 보안 라스트 마일 연결성으로서 간주될 수 있다.

[0273] **용어 정의**

[0274] 문맥이 달리 요구하지 않는 한, 보안 동적 통신 네트워크 및 프로토콜의 기재에 사용된 용어는 이하의 의미를 갖는다.

[0275] 익명 데이터 패킷: 본래의 본래 또는 최종 목적지에 대한 정보가 부족한 데이터 패킷.

[0276] 클라이언트 또는 클라이언트 디바이스: 라스트 마일을 통해서 SDNP 클라우드에 연결된 디바이스, 전형적으로 휴대폰, 태블릿, 노트북, 데스크탑, 또는 IoT 디바이스.

[0277] 은폐: 스크램블링, 분할, 정크 데이터 삽입, 및 암호화와 같은 보안 동작의 임의의 순차적인 조합을 이용하여 SDNP 패킷 또는 그 일부의 콘텐츠가 인식되지 않게 하는 인코딩 프로세스. 은폐된 데이터의 회복은 반대 순서의

역기능 또는 디코딩 프로세스, 예를 들어 해독, 정크 데이터 제거, 혼합 및 언스크램블링의 실행을 필요로 한다.

[0278] 해독: 데이터 패킷을 암호문으로부터 평문으로 변환하기 위해서 사용되는 수학적 동작.

[0279] 분해 데이터 저장: 다양한 단편화된 파일을 상이한 데이터 저장 노드들에 저장하기 전에, 데이터 파일을 단편화하고 그 콘텐츠를 은폐하는 프로세스.

[0280] DMZ 서버: 선택기, 시드 생성기, 키 생성기 및 기타 공유 비밀을 저장하는데 사용되는, SDNP 네트워크 또는 인터넷으로부터 직접 액세스할 수 없는 컴퓨터 서버. DMZ는 또한 "공기 갭형(air gapped)" 서버, 즉 유선 네트워크 연결 또는 액세스를 가지지 않는 컴퓨터로 지칭될 수 있다.

[0281] 동적 암호화/해독: 데이터 패킷이 SDNP 네트워크를 횡단할 때, 동적으로 변하는 키에 의존하는 암호화 및 해독.

[0282] 동적 혼합: 혼합 데이터 패킷이 생성될 때 시간, 상태 및 구역과 같은 상태에 기초하여 시드의 함수로서 혼합 알고리즘(분할 알고리즘의 역기능)이 동적으로 변하는 혼합 프로세스.

[0283] 동적 스크램블링/언스크램블링: 데이터 패킷이 생성된 시간 또는 생성된 지역과 같은, 상태의 함수로서 동적으로 변화되는 알고리즘에 의존하는 스크램블링 및 언스크램블링.

[0284] 동적 분할: 데이터 패킷이 다중 서브-패킷으로 분할될 때 시간, 상태 및 지역과 같은 상태를 기초로 시드의 함수로서 분할 알고리즘이 동적으로 변하는 분할 프로세스.

[0285] 암호화: 데이터 패킷을 평문으로부터 암호문으로 변환하는데 사용되는 수학 동작.

[0286] 단편화된 데이터 전송: SDNP 네트워크를 통해 분할되고 혼합된 데이터의 라우팅.

[0287] 정크 데이터 삭제(또는 "역-정킹(De-junking)"): 본래의 데이터를 복원하거나 또는 데이터 패킷의 본래 길이를 복구하기 위해, 데이터 패킷으로부터의 정크 데이터의 제거.

[0288] 정크 데이터 삽입(또는 "정킹(juncking)"): 실제 데이터 콘텐츠를 난독화하기 위해 또는 데이터 패킷의 길이를 관리하기 위해, 데이터 패킷 내에 무의미한 데이터를 의도적으로 도입하는 것.

[0289] 키: 키를 생성하기 위해서 비밀 알고리즘을 사용하는 키 생성기 내에 시간과 같은 상태를 입력함으로써 생성되는 위장된 디지털 값. 키는 선택기로부터 패킷의 데이터를 암호화 또는 해독하는 알고리즘을 선택하는데 사용된다. 키는 공개 또는 비보안 라인에 걸쳐 상태에 관한 정보를 안전하게 통과시키는데 사용될 수 있다.

[0290] 키 교환 서버: 네트워크 운영자 스파이 행위의 임의의 가능성을 방지하기 위해서, 공공 암호화 키를 클라이언트에, 그리고 선택적으로 대칭 키 암호화를 사용하는 서버에, 특히 클라이언트 관리형 키 관리, 즉 엔드-투-엔드 암호화를 기초로 하는 클라이언트에 배포하기 위해서 사용되는, 종종 제3자 호스팅된 그리고 SDNP 네트워크 운영자와는 독립적인, 컴퓨터 서버.

[0291] 라스트 링크: 클라이언트의 디바이스와 이것이 통신하는 네트워크에서의 제1 디바이스, 전형적으로 라디오 타워, WiFi 라우터, 케이블 모뎀, 셋톱박스 또는 이더넷 연결 사이의 네트워크 연결. 이더넷 통신의 경우에, 라스트 링크는 케이블 모뎀 또는 광섬유 모뎀에 대한 물리적으로 "테더링된" (즉, 유선) 연결을 포함한다. (예를 들어, 카페에서) WiFi 연결을 위해서, 라스트 링크는 DSL, 케이블, 또는 섬유 네트워크에 연결된 WiFi 라우터를 포함한다. 셀룰러 네트워크에서, 라스트 링크는, 예를 들어 3G 또는 4G/LTE를 포함할 수 있는, 셀룰러 타워와 모바일 폰 사이의 라디오 링크를 포함한다.

[0292] 라스트 마일: 라스트 링크를 포함하는, SDNP 또는 다른 유형의 네트워크 또는 클라우드 내의 클라이언트와 게이트웨이 미디어 노드 사이의 네트워크 연결. 라스트 마일은 전형적으로 로컬 텔코 및 케이블 회사, 예를 들어 Comcast cable, Verizon cellular, Korean Telecom, British Telecom, 등이 소유하고 그들에 의해서 운용되는 네트워크에 걸친 통신을 포함한다.

[0293] 혼합: 인식 불가능한 콘텐츠를 갖는 하나의 더 긴 데이터 패킷(또는 일련의 더 작은 서브-패킷들)을 생성하기 위해서, 상이한 데이터 유형들을 포함할 수 있는 상이한 소스들로부터의 데이터 패킷들을 조합하는 것. 일부 경우에, 이전에 분할된 데이터 패킷들이 혼합되어 원래의 데이터 콘텐츠를 복원한다. 혼합 동작은 또한 정크 데이터 삽입 및 삭제 및 파싱을 포함할 수 있다.

[0294] 다수 PHY 또는 다중-PHY: 다수의 물리적 미디어, 예를 들어 광섬유 및 4G, 상이한 WiFi 채널들 및 주파수들, 4G

및 WiFi, 이더넷 WiFi, 등에 걸친 관련된 시퀀셜 데이터 패킷의 교번적인 전송을 포함하는 통신.

[0295] 파싱: 저장 또는 전송을 위해 데이터 패킷을 더 짧은 서브-패킷으로 파괴하는 수치 동작.

[0296] 라우터: 해당 IP 헤더 내에 특정된 목적지 어드레스로의 데이터그램의 라우팅을 지향시키는 디바이스. SDNP 네트워크 외부의 패킷 라우팅을 위해서, 이용되는 IP 어드레스는 유효 인터넷 IP 어드레스(DNS 서버에 의해서 인식되는 어드레스)를 나타낼 수 있거나, 로컬 네트워크 제공자에 의해서 운영되는 네트워크 어드레스 트랜스레이터에 의해서 할당된 NAT 어드레스를 나타낼 수 있다(예를 들어, Comcast는 Comcast 케이블/섬유 네트워크 내의 통신을 위한 자체의 내부 IP 어드레스를 할당한다).

[0297] 스크램블링: 데이터 패킷에서 데이터 세그먼트의 순서 또는 시퀀스가 그 자연적인 순서로부터 인식 불가능한 형태로 변경되는 동작.

[0298] 분할: 데이터 패킷(또는 일련의 직렬 데이터 패킷)이 다중 목적지로 라우팅되는 다중 서브-패킷으로 분할되는 동작. 분할 동작은 정크 데이터 삽입 및 삭제를 포함할 수도 있다.

[0299] 소프트스위치(SoftSwitch): 전기통신 스위치 및 라우터의 기능을 수행하는 실행 가능한 코드를 포함하는 소프트웨어.

[0300] SDNP: 본 발명에 따라 제조된 하이퍼-보안 통신 네트워크를 의미하는 "보안 동적 통신 네트워크 및 프로토콜"의 약자.

[0301] SDNP 어드레스: SDNP 클라우드를 통해서 또는 다음 목적지 디바이스의 애드혹 IP 어드레스, 즉, 단일 홉을 실행하기에 충분한 정보만을 포함하는 라스트 마일에 걸쳐 SDNP 패킷을 라우팅시키기 위해서 이용되는 어드레스.

[0302] SDNP 관리 서버: 실행 가능한 코드 및 공유 비밀을 전 세계 또는 지정 구역의 SDNP 서버에 배포하는데 사용되는 컴퓨터 서버.

[0303] SDNP 브릿지 노드: 하나의 SDNP 구역 또는 클라우드를 상이한 보안 자격 증명을 갖는 다른 구역 또는 클라우드에 연결하는 SDNP 노드.

[0304] SDNP 클라이언트 또는 클라이언트 디바이스: 일반적으로 라스트 마일을 통해 연결하는, SDNP 클라우드에 연결하기 위해서 SDNP 애플리케이션을 동작시키는 네트워크 연결된 디바이스, 전형적으로 휴대폰, 태블릿, 노트북, 데스크탑 또는 IoT 디바이스.

[0305] SDNP 클라우드: SDNP 통신 노드 동작을 수행하기 위해, 소프트스위치 실행 가능한 코드를 동작시키는 상호 연결된 SDNP 서버의 네트워크.

[0306] SDNP 게이트웨이 노드: 라스트 마일을 통해서 SDNP 클라우드를 클라이언트 디바이스에 연결하는 미디어 노드. SDNP 게이트웨이 노드는 (SDNP 클라우드의, 그리고 라스트 마일의) 적어도 2개의 구역에 대한 액세스를 요구한다.

[0307] SDNP 미디어 노드: 암호화/해독, 스크램블링/언스크램블링, 혼합/분할, 태깅(tagging) 및 SDNP 헤더 및 서브 헤드 생성을 포함하여, 시그널링 기능을 수행하는 시그널링 서버 또는 다른 컴퓨터로부터의 명령에 따라 특별한 식별 태그로 들어오는 데이터 패킷을 처리하는 소프트스위치 실행 가능한 코드. SDNP 미디어 노드는 지정 태그를 갖는 들어오는 데이터 패킷을 식별하고 새로 생성된 데이터 패킷을 그 후 목적지로 전송하는 역할을 한다.

[0308] SDNP 미디어 서버: 이중 채널 및 3중 채널 통신에서 SDNP 미디어 노드의 기능을 수행하고 또한 단일 채널 통신에서 SDNP 시그널링 노드 및 SDNP 네임 서버 노드의 동작을 수행하는 소프트스위치를 호스트하는 컴퓨터 서버.

[0309] SDNP 네임 서버: 3채널 통신에서 SDNP 네임 서버 노드의 기능을 수행하는 소프트스위치를 호스트하는 컴퓨터 서버.

[0310] SDNP 네임 서버 노드: SDNP 클라우드에 연결된 모든 SDNP 디바이스의 동적 목록을 관리하는 소프트스위치 실행 가능한 코드.

[0311] SDNP 네트워크: SDNP 클라우드뿐만 아니라, 라스트 링크 및 라스트 마일 통신을 포함하는 클라이언트로부터 클라이언트로 확장하는 전체 하이퍼 보안 통신 네트워크.

[0312] SDNP 노드: 컴퓨터 서버 또는 대안적으로 SDNP 네트워크에 연결된 하드웨어 디바이스 상에서 동작하는 소프트웨어 기반 "소프트스위치"를 포함하며, 미디어 노드, 시그널링 노드 또는 네임 서버로서 SDNP 노드로서 기능하는

SDNP 통신 노드.

[0313] SDNP 서버: SDNP 미디어 서버, SDNP 시그널링 서버 또는 SDNP 네임 서버를 포함하며 또한 SDNP 노드로서 동작하도록 적용 가능한 소프트스위치 기능을 호스트하는 컴퓨터 서버.

[0314] SDNP 시그널링 노드: 당사자 사이의 통화 또는 통신을 시작하고, 통화자 기준에 기초하여 단편화된 데이터를 전송하기 위한 다중 루트의 전부 또는 일부를 결정하여, 들어오고 나가는 데이터 패킷을 어떻게 관리할지를 SDNP 미디어에 지시하는 소프트스위치 실행 가능한 코드.

[0315] SDNP 시그널링 또는 신호 서버: 이중 채널 및 3중 채널 SDNP 통신에서 SDNP 시그널링 노드의 기능을 수행하고, 또한 이중 채널 통신에서 SDNP 네임 서버 노드의 임무를 수행하는 소프트스위치를 호스트하는 컴퓨터 서버.

[0316] SDNP 태그: 유입 데이터 패킷 또는 그 서브-패킷을 식별하기 위해서 이용되는 소스 어드레스, SDNP 집 코드, 또는 임의의 다른 코드.

[0317] 보안 동작: 패킷이 생성되는 곳의 구역 및 상태와 관련된 상태-의존적 보안 자격 증명을 이용하여 은폐를 실시하기 위해서(또는 은폐된 패킷의 콘텐츠를 복구하기 위해서) 데이터 패킷을 수정하는 프로세스

[0318] 보안 설정 또는 보안 자격 증명: 네트워크 시간과 같이 끊임없이 변화하는 입력 상태와 함께 비밀 알고리즘을 사용하여 시드 생성기 또는 키 생성기에 의해 생성되며, 따라서 공개 또는 비 보안 라인을 통해 안전하게 전송될 수 있는 시드 및 키와 같은 디지털 값.

[0319] 시드: 시간과 같은 상태를 비밀 알고리즘을 사용하여 시드를 생성하는 시드 생성기에 입력함으로써 생성되는 위장된 디지털 값. 시드는 선택기로부터 패킷 내의 데이터를 스크램블, 암호화 또는 분할하기 위한 알고리즘을 선택하는데 사용된다. 시드는 공개 또는 비 보안 라인을 통해 상태에 관한 정보를 안전하게 통과시키는데 사용될 수 있다.

[0320] 선택기: 공유 비밀의 일부이며 또한 패킷이나 패킷을 스크램블링, 언스크램블링, 암호화, 해독, 분할 또는 혼합하기 위해서 특별한 알고리즘을 선택하도록 시드 또는 키와 함께 사용되는 가능한 스크램블링, 암호화 또는 분할 알고리즘의 목록 또는 표.

[0321] 공유 비밀: 시드 생성기, 키 생성기, 구역 정보에 의해 사용되는 알고리즘 및 SDNP 네트워크 또는 인터넷을 통해 액세스할 수 없는 DMZ 서버에 로컬로 저장된 알고리즘 셔플링 프로세스뿐만 아니라, 스크램블링/언스크램블링, 암호화/해독 및 혼합/분할 알고리즘의 표 또는 선택기를 포함하는, SDNP 노드 동작에 관한 기밀 정보.

[0322] 단일 PHY: 단일 물리적 미디어를 통해서, 예를 들어 광섬유, 또는 이더넷, 또는 WiFi, 또는 셀룰러 네트워크를 통해서만, 전송되는 관련 데이터 패킷의 통신.

[0323] 상태: 시드 또는 키와 같은 보안 설정을 동적으로 생성하거나 또는 혼합, 분할, 스크램블링 및 암호화와 같은 지정한 SDNP 동작을 위한 알고리즘을 선택하는데 사용되는 위치, 구역 또는 네트워크 시간과 같은 입력.

[0324] 시간: SDNP 네트워크를 가로질러 통신을 동기화하는데 사용되는 범용 네트워크 시간

[0325] 언스크램블링: 스크램블링된 데이터 패킷의 데이터 세그먼트를 그 본래의 순서 또는 순차적으로 복원하는 프로세스. 언스크램블링은 스크램블링의 역기능이다.

[0326] 구역: 공통 보안 자격 증명 및 공유 비밀을 공유하는 지정 상호 연결된 서버의 네트워크. 라스트 마일 연결은 SDNP 클라우드에서 이들과 별도의 구역을 포함한다.

[0327] **보안 동적 통신 네트워크 및 프로토콜(SDNP) 설계**

[0328] 실시간 패킷 대기 시간을 최소화하고 안정적인 통화 연결성을 보장하며 또한 음성 통신 및 비디오 스트리밍의 최고 무결성을 전달하면서 패킷 교환형 통신의 사이버 공격 및 해킹을 방지하기 위해, 공개된 보안 동적 통신 네트워크 및 프로토콜 또는 SDNP가 다음을 포함하는 많은 지침 원칙에 따라 설계되었다.

[0329] * 실시간 통신은 최단 대기 시간 경로를 사용하여 항상 발생해야 한다.

[0330] * 데이터 패킷의 무단 검사 또는 스니핑은 패킷의 출처, 진행 위치 또는 그 내부에 있는 것에 대한 내용을 제공하지 않아야 한다.

[0331] * 데이터 패킷 페이로드는 역동적으로 재암호화해야 한다. 즉, 임의의 합리적인 시간에 해킹될 위험 없이, 상이한 암호화 알고리즘을 사용하여 해독된 후 다시 암호화되어야 한다.

[0332] * 이들이 해독된 후라도, 모든 데이터 패킷 페이로드는 다중 대화의 동적 스크램블링된 혼합과 정크 패킷 필러와 혼합된 무관한 데이터를 포함하는 이해할 수 없는 페이로드를 여전히 포함한다. 그러한 지침의 실행은 다양한 실시예에서 이하의 일부 또는 전부를 포함하는 다양한 독창적인 발명적인 방법, 기능, 특징 및 실행을 포함한다.

[0333] * SDNP는, 인터넷을 통해 액세스할 수 없는 독점적인 명령 및 제어 소프트웨어를 사용하여 실현된 소프트-스위치 기능인, 텔코, 즉 전기통신 시스템을 포함하는 하나 또는 그 이상의 전용 클라우드를 사용한다.

[0334] * 모든 인트라 클라우드 통신은 DNS 인식 IP 어드레스가 아니라 SDNP 어드레스 및 동적 포트(즉, 독점 NAT 어드레스)에 기초하는 독점적인 클라우드 내에서 전용 SDNP 패킷 라우팅을 사용하여 발생한다. SDNP 어드레스는 인터넷에서 또는 SDNP 클라우드 외부에서 사용될 수 없거나 라우팅할 수 없다.

[0335] * SDNP 네트워크는 사용 가능한 최저 대기 시간 경로를 통해 모든 실시간 통신을 지속적으로 식별하고 동적으로 라우팅한다.

[0336] * 보안 또는 실시간 통신은 클라우드 간 및 라스트 마일 통신 및 일반적으로 보이지 않는 어드레스로 단일 홉 라우팅을 사용하는 경우를 제외하고는, SDNP 클라우드 외부 또는 인터넷을 통해 라우팅되지 않는다.

[0337] * 데이터 패킷에 포함된 라우팅 데이터는, 2개의 인접한 디바이스 사이에서 단일 홉에 대한 라우팅을 식별하여, 마지막 및 다음 서버의 SDNP 또는 IP 어드레스만 식별한다.

[0338] * 통화자와 수신기의 전화번호 또는 IP 어드레스, 즉 클라이언트의 각 소스 및 목적지 어드레스가 IP 패킷 헤더에 존재하지 않으며 또한 암호화된 페이로드에 존재하지도 않는다.

[0339] * 명령 및 제어 관련 공유 비밀은 인터넷을 통해 액세스할 수 없는 보안 DMZ 서버에 설치된 시스템 소프트웨어에 존재한다.

[0340] * SDNP 패킷 통신은 3개의 독립적인 채널, 즉 SDNP 클라우드 내의 요소를 식별하는데 사용되는 "네임 서버", 콘텐츠 및 데이터 라우팅에 사용되는 "미디어 서버", 그리고 패킷 및 통화 명령 및 제어에 사용되는 "시그널링 서버"를 통해 발생할 수 있다.

[0341] * 키 및 수치 시드(필요에 따른)와 함께 라우팅 정보는, 통화 또는 코뮤니케 전에 독립적인 시그널링 채널을 통해 모든 참여 미디어 서버에 공급되며 콘텐츠는 공급되지 않는다. 상기 시그널링 서버는 미디어 서버에 네트워크를 횡단하는 패킷의 마지막 및 다음 목적지만을 공급한다.

[0342] * 미디어 패킷은 통화, 문서, 텍스트 또는 파일의 일부만을 나타내는 단편화된 데이터를 포함하며, 다른 소스 및 상이한 유형의 단편화된 데이터를 포함하는 다른 패킷과 동적으로 혼합되고 그리고 재혼합된다.

[0343] * 미디어 및 콘텐츠 관련 패킷으로부터 시그널링 서버 관련 통신을 분리시키는 것을 포함하여, 제1 및 라스트 마일 통신을 보호하기 위해, 특수 보안 방법이 사용된다.

[0344] * 패킷 전송은 시그널링 패킷, 명령 및 제어 패킷, 데이터 파일, 애플리케이션 파일, 시스템 파일, 패킷 손실에 민감하거나 또는 대기 시간이 TCP 전송을 이용하는 다른 파일과 함께, 강화된 UDP에 기초하여 음성 및 실시간 비디오 또는 스트림을 갖는 콘텐츠 유형 의존형이다.

[0345] * 특수 보안 및 인증 방법은 디바이스가 복제품이 아니라 실제 클라이언트인지를 확인하고 또한 통신하는 사람이 사기꾼이 아니라 디바이스의 진정한 소유자임을 인증하는데 사용된다.

[0346] * 낮은 대기 시간 및 높은 QoS로 보안 통신을 보장하기 위해, 기재된 "보안 동적 네트워크 및 프로토콜" 또는 SDNP는 이하를 포함하는 독창적인 "동적 메시"네트워크를 이용한다:

[0347] * 최소 대기 시간의 동적 적응형 다중 경로 및 메시형 라우팅

[0348] * 동적 패킷 스크램블링

[0349] * 패킷 분할, 혼합, 파싱 및 정크 비트 패킷 필러를 사용하는 동적 단편화.

[0350] * 네트워크 또는 클라우드 전반에 걸친 동적 인트라-노드 페이로드 암호화.

[0351] * 어드레스 위장 및 알아야 할 라우팅 정보를 갖는 동적 네트워크 프로토콜.

[0352] * 시그널링, 명령 및 제어, 및 네트워크 어드레스로부터 미디어 및 콘텐츠를 분리하는 다중 채널 통신

[0353] * 데이터 유형 지정한 특성 및 상황별 라우팅에 의한 동적 적응형 실시간 전송 프로토콜.

[0354] * 사용자 키 관리에 의한 클라이언트 암호화된 페이로드의 지원.

[0355] * 혼잡한 네트워크에서 높은 QoS를 위한 경량 오디오 코덱.

[0356] 전술한 바와 같이, SDNP 통신은 데이터 패킷을 동적으로 라우팅하기 위해 다중 경로 및 메시형 통신에 의존한다. 본 발명에 따른 SDNP 통신에서, 인터넷 OTT 및 VoIP 통신에 사용되는 대조적인 단일 루트 패킷 통신과는 달리, 데이터 패킷의 콘텐츠는 공통 소스 또는 통화자로부터의 정보를 포함하는 일관적인 패킷에 의해 직렬로 전달되지 않지만, 다중 소스 및 통화자로부터 나타나는 콘텐츠를 동적으로 혼합 및 재혼합하는 단편화된 형태로, 여기서 상기 데이터는 데이터, 콘텐츠, 음성, 비디오 및 유사한 데이터 유형의 파일의 불완전한 부분을 정크 데이터 필러로 집계한다. 데이터 단편화 및 전송의 기재된 실현의 이점은 암호화되지 않은 및 언스크램블링된 데이터 패킷이 관련 없는 데이터 및 데이터 유형의 조합을 나타내기 때문에 해석하기가 거의 불가능 하다는 점이다.

[0357] 단편화된 패킷 혼합 및 패킷 스크램블링과 패킷 스크램블링 및 동적 암호화와 조합함으로써, 이들 동적으로 암호화된, 스크램블링된, 단편화된 데이터의 하이브리드화된 패킷은 공유 비밀, 키, 수치 시드, 데이터를 생성, 패킷, 및 동적으로 재패킷하는데 사용되는 시간 및 상태 변수가 없는 임의의 당사자 또는 관찰자에게 전혀 이해할 수 없는 무의미한 패킷을 포함한다

[0358] 또한, 각 패킷의 단편화된 콘텐츠, 및 이를 생성하는데 사용된 비밀은 패킷이 새로운 단편과 그리고 수정된 시드, 키, 알고리즘 및 암호와 같은 새로운 보안 규정으로 재구성되기 전에, 불과 몇 초만 유효하다. 사이버 해적이 상태 의존형 SDNP 데이터 패킷을 파괴하고 개봉할 수 있는 제한된 주기는 SDNP 보안을 더욱 향상시켜, 1초당 10만 건의 처리 기간이 필요하며, 이를 파괴하는 시간보다 큰 12배의 도전 과제가 필요하다.

[0359] 전술한 방법의 조합은 정적 암호화로부터 얻을 수 있는 보안을 훨씬 넘어선 다차원 보안을 촉진시킨다. 따라서 기재된 보안 동적 통신 네트워크 및 프로토콜은 여기에서는 "하이퍼보안"네트워크로서 지칭된다.

[0360] ***데이터 패킷 스크램블링(Data Packet Scrambling)*** - 기재된 발명에 따라, 패킷 교환형 네트워크를 통한 보안 통신은 해킹을 방지하고 보안을 보장하기 위해 여러 요소에 의존하며, 그 중 하나는 SDNP 패킷 스크램블링을 포함한다. SDNP 패킷 스크램블링은 데이터 세그먼트를 순서 없이 재배열하여, 정보를 이해할 수 없게 하고 쓸모없게 한다. 도 2a에 도시된 바와 같이, 스크램블링 동작(924)을 통해 처리된 스크램블링되지 않은 데이터 패킷, 즉 데이터 패킷(923)은 스크램블링된 데이터 패킷(925)으로 나타난다. 스크램블링 동작은 임의의 알고리즘, 수치 방법, 또는 시퀀싱 방법을 사용할 수 있다. 알고리즘은 정적 방정식을 나타낼 수 있으며, 또는 스크램블링이 발생한 시간(920) 및 시드 생성기(921)에 의해 생성된 수치 시드(929)와 같은 "상태"에 기초한 동적 변수 또는 수치 시드를 포함할 수 있으며, 이는 스크램블링 시에 시간(920)과 같은 상태에 의존하는 알고리즘을 사용하여 시드(929)를 발생시킬 수 있다. 예를 들어, 각 날짜가 단조롭게 오름차순으로 고유의 숫자로 변환된다면, 모든 시드(929)는 고유하다. 시간(920) 및 시드(929)는 지정한 알고리즘을 선택하기 위해 사용될 수 있으며, 또는 이용가능한 스크램블링 방법의 목록으로부터, 즉 스크램블링 알고리즘(922)으로부터 선택된 지정한 스크램블링 동작(924)을 선택하거나 계산하는데 사용될 수도 있다. 데이터 흐름도에서, 여기에 기호(926)로 도시된 바와 같이, 개략적인 또는 기호적인 표현을 사용하여 이 패킷-스크램블링 동작 및 시퀀스를 도시하는 것이 편리하다.

[0361] 도 2b에 도시된 언스크램블링 동작은 스크램블링 동작(924)의 역기능, 특히 언스크램블링 동작(927)을 도시하며, 여기서 스크램블링된 데이터 패킷(925)을 생성하는데 사용된 상태 또는 시간(920) 및 대응하는 시드(929)는 언스크램블링된 데이터, 특히 언스크램블링된 데이터 패킷(923)을 되돌리는데 재사용된다. 패킷 스크램블링이 처음 발생했을 때 사용된 것과 동일한 상태 또는 시간(920)을 사용하면, 스크램블링 알고리즘 목록(922)로부터 선택된 바와 같이, 스크램블링 동작(927)에서 동일한 스크램블링 방법이 다시 이용되어야만 한다. 스크램블링 알고리즘 목록(922)은 "스크램블링"이라는 용어를 참고하며, 동일한 알고리즘 표는 "언스크램블링"을 수행하는데 필요한 역기능을 식별하고 선택하는데 사용되며, 즉 스크램블링 알고리즘 목록(922)은 데이터 패킷을 스크램블링하고 또한 데이터 패킷을 언스크램블링하는데 필요한 정보를 포함한다. 두 기능이 역순으로 수행되는 동일한 단계를 포함하기 때문에, 목록(922)은 "스크램블링/언스크램블링"알고리즘 목록(922)으로서 이름을 바꿀 수 있다. 그러나 명확함을 위해, 상기 표는 기능에 의해서만 표시되고, 반 기능으로는 표시되지 않는다.

[0362] 언스크램블링 동작(927)을 실행하기 위해 선택된 스크램블링 알고리즘이 패킷 스크램블링에 사용된 본래의 알고리즘과 일치하지 않거나, 또는 시드(929) 또는 상태 또는 시간(920)이 발생한 타임 스크램블링과 일치하지 않으면, 언스크램블링 동작은 본래의 언스크램블링된 데이터 패킷을 복구하는 것을 실패할 것이며, 그리고 상기 패

킷 데이터가 손실될 것이다. 데이터 흐름도에 있어서, 여기에 기호(928)로 도시된 바와 같이, 개략적인 또는 기호적인 표현을 사용하여 이 패킷 언스크램블링 프로세스 및 시퀀스를 설명하는 것이 편리하다.

[0363] 개시된 발명에 따라, 본래의 프로세스와 반대 순서로 단계를 반복하는 것을 의미하는 가역적인 프로세스가 각각의 데이터 세그먼트를 주어진 데이터 패킷에서 그 본래의 그리고 적절한 위치로 복귀시키는 한, 많은 알고리즘이 스크램블링 동작을 수행하는데 사용될 수 있다. 수학적으로, 허용 가능한 스크램블링 알고리즘은 가역적인 알고리즘이며, 즉 함수 F(A)는 역함수(anti-function) $F^{-1}(A)$를 갖거나 또는 대안적으로 변형이 상응하는 역함수를 가지며, 그에 따라 $F^{-1}[F(A)] = A$가 되며, 이는 함수(F)에 의해 처리된 데이터 파일, 시퀀스, 텍스트 스트링, 파일 또는 벡터(A)는 역함수($F^{-1}$)를 사용하는 후속 처리에 따라 값 또는 시퀀스에서 손상되지 않은 본래의 입력(A)을 복원한다는 것을 의미한다.

[0364] 이러한 가역기능의 예는 미러링(mirroring) 및 위상 시프트 알고리즘을 포함하는 도 2c에 도시된 정적 스크램블링 알고리즘에 의해 도시된다. 미러링 알고리즘에 있어서, 데이터 세그먼트는 미러링 프로세스의 모듈 또는 "모드(mod)"에 의해 정의된 대칭선의 둘레에서 다른 데이터 세그먼트와 거울상으로서 스와핑된다. 도시된 바와 같은 모드-2 미러링에 있어서, 본래의 입력 데이터 패킷(930)의 매 2개의 데이터 세그먼트가 교환되고, 즉 1A 및 1B는 제1 및 제2 데이터 세그먼트 사이의 중심에 있는, 제3 및 제4 데이터 세그먼트 사이의 중심에 있는 대칭선을 갖는, 또는 수학적으로 $1.5^{th}$, $3.5^{th}$, $5.5^{th}$, ..., $(1.5 + 2n)^{th}$ 위치로서 스크램블링된 출력 데이터 패킷(935)을 생성하기 위해 1C 및 1D, 1E 및 1F 등과 같이 위치가 교환된다.

[0365] 모드-3 미러링에 있어서, 3개 마다의 데이터 세그먼트의 제1 및 제3 데이터 세그먼트가 스와핑되며, 반면에 각 3쌍의 중간 패킷은 본래 위치로 유지된다. 따라서 스크램블링된 데이터 패킷 출력(936)을 생성하기 위해, 데이터 세그먼트(1A, 1C)는 스와핑되며, 반면에 1B는 3쌍의 중심에 유지되고, 데이터 세그먼트(1D, 1F)는 스와핑되고, 1E는 3쌍의 중심에 유지된다. 모드-3 미러링에 있어서, 대칭선은 $2^{th}$, $5^{th}$, $8^{th}$, ..., $(2 + 3n)^{th}$ 위치에서 중심에 있다.

[0366] 모드-4 미러링에 있어서, 입력 데이터 패킷(931)으로부터 스크램블링된 출력 데이터 패킷(937)을 생성하기 위해서, 4개 마다의 데이터 세그먼트의 제1 및 제4 데이터 세그먼트 그리고 제2 및 제3 데이터 세그먼트가 스와핑된다. 따라서 데이터 세그먼트(1A)는 1D와 스와핑되고, 데이터 세그먼트(1B)는 1C와 스와핑된다. 모드-4 미러링에 있어서, 대칭선은 모든 4쌍의 제2 및 제3 데이터 세그먼트 사이에서 중심에 있으며, 예를 들어 제2 및 제3 데이터 세그먼트 사이, 제6 및 제7 데이터 세그먼트 등으로, 또는 수학적으로 $2.5^{th}$, $6.5^{th}$, ..., $(2.5 + 4n)^{th}$ 위치에 있다. 모드-m 미러링에 있어서, 입력 데이터 패킷(932)의 제m 데이터 세그먼트는 제1, 즉 $0^{th}$ 데이터 세그먼트와 스와핑되며; $0^{th}$ 데이터 세그먼트는 $m^{th}$ 요소와 스와핑되며, 마찬가지로 $n^{th}$ 요소는 스크램블링된 출력 데이터 패킷(938)을 생성하기 위해 $(m-n)^{th}$ 데이터 세그먼트와 스와핑된다.

[0367] 도 2c에도 도시된 다른 스크램블링 방법은 모든 데이터 세그먼트가 좌측으로 또는 우측으로 1 프레임, 2 프레임, 또는 그 이상의 프레임만큼 시프트되는 프레임 시프트이다. 예를 들어, 단일 프레임 위상 시프트에서, 모든 데이터 세그먼트는 스크램블링된 출력 데이터 패킷(940)을 생성하기 위해 1 프레임만큼 시프트되며, 여기서 제1 데이터 세그먼트는 제2 위치로 시프트되고; 제2 데이터 세그먼트는 제3 프레임으로 시프트된다. 도시된 예에서 입력 데이터 패킷(930)의 최종 프레임인 프레임 1F는 데이터 세그먼트(1A)에 의해 이전에 점유된 제1 프레임으로 시프트된다.

[0368] 2-프레임 위상 시프트에서, 입력 데이터 패킷(930)의 제1 데이터 세그먼트(1A)는 2개의 프레임만큼 데이터 세그먼트(1C)에 의해 이미 점유된 위치로 시프트되고, 제4 프레임(1D)은 스크램블링된 출력 데이터 패킷(941)의 마지막 위치로 시프트되며, 최종 데이터 세그먼트(1E)의 다음은 제1 위치로 시프트되고, 최종 위치(1F)는 제2 위치로 시프트된다. 마찬가지로, 4프레임 위상 시프트에서, 입력 데이터 패킷(930)의 데이터 세그먼트는 스크램블링된 출력 데이터 패킷(942)을 생성하기 위해, 제1 프레임(1A)이 1F를 대체하는 1E, 1B, 1A를 대체하는 1C에 의해 이미 유지된 프레임을 대체하는 제1 프레임(1A)으로 네 번째 위치로 시프트된다. 최대 위상 시프트의 경우에, 제1 프레임은 마지막을 대체하고, 1B에 의해 본래 유지된 제2 프레임은 출력 데이터 패킷(943)의 제1 프레임이 되고, 제2 요소는 제1 위치로 시프트되고, 제3 위치는 두 번째 위치로 시프트된다. 하나의 프레임을 최대 위상 시프트 이상으로 위상 시프트하면 입력으로부터 바뀌지 않은 출력 데이터로 나타난다. 도시된 예는 데이터가 오른쪽으로 시프트된 위상 시프트를 포함한다. 이 알고리즘은 왼쪽으로 이동하지만 결과가 다른 위상

이동에도 적용된다.

[0369] 개시된 바와 같은 전술한 알고리즘 및 유사한 방법은 여기에서 정적 스크램블링 알고리즘으로서 지칭되는데, 그 이유는 스크램블링 동작이 단일 시간에서 발생하여 입력 데이터 세트를 고유의 출력으로 변환하기 때문이다. 더욱이, 이미 도시된 알고리즘은 스크램블링이 어떻게 일어나는지를 결정하기 위해 데이터 패킷의 값에 의존하지 않는다. 도 2d에 도시된 바와 같이, 기재된 발명에 따라, 매개변수적 스크램블링은 데이터 패킷 자체 내에 포함된 데이터로부터 유도된 값에 기초하여, 스크램블링 방법이 가능한 스크램블링 알고리즘의 표, 예를 들어, 분류 # A, 분류 # B로부터 선택된다는 것을 의미한다. 예를 들어, 데이터 세그먼트 내에 포함된 데이터의 계산에 기초하여, 각 데이터 세그먼트가 수치로 변환될 수 있다고 가정하자. 데이터 세그먼트의 수치를 결정할 수 있는 하나의 방법은 데이터 세그먼트에서 비트 데이터와 동일한 10진수 또는 16진수를 사용하는 것이다. 데이터 세그먼트가 여러 용어를 포함한다면, 데이터 세그먼트의 숫자를 합산하여 숫자를 찾아낼 수 있다. 데이터 세그먼트 데이터는 단일 숫자 또는 "매개변수"와 조합되며, 그 후 어떤 스크램블링 방법이 사용되는지를 선택하는데 사용된다.

[0370] 도시된 예에 있어서, 언스크램블링된 데이터 패킷(930)은 단계(950)에서 매개변수로 각 데이터 세그먼트에 대한 수치를 포함하는 데이터 표(951)로 변환된다. 데이터 세그먼트 1A에 도시된 바와 같이, 0 번째 프레임인 데이터 세그먼트(1A)는 23의 수치를 가지며, 제1 프레임인 데이터 세그먼트(1B)는 125라는 수치를 갖는다. 단일 데이터 패킷 값은 전체 데이터 패킷(930)에 대해 단계(952)에서 추출된다. 도시된 예에 있어서, 합계(953)는 매개변수적으로 모두 1002인 표(951)로부터의 모든 데이터 세그먼트 값의 선형 총합을 나타내며, 매개변수적으로 총합은 1002이다. 단계(954)에서 이 매개변수적 값, 즉 합계(953)는 표(955)에서 많은 중첩되지 않은 숫자 범위에 대해 합계(953)를 비교하여 어떤 종류의 정렬 루틴이 사용되어야 하는지를 결정하기 위해, 소프트웨어에서 사전 정의된 상태의 세트인 상태 표에 대해 비교된다. 이 예에 있어서, 매개변수 값(1002)은 1000 내지 1499 범위에 속하며, 이는 분류 # C를 사용해야 한다는 것을 의미한다. 일단 정렬 루틴이 선택되었다면, 매개변수 값은 더 이상 요구되지 않는다. 언스크램블링된 데이터 입력(930)은 그 후 스크램블 데이터 패킷 출력(959)을 생성하기 위해 단계(956)에서 선택된 방법에 의해 스크램블링된이다. 도시된 예에 있어서, 표(957)에 요약된 분류 # C는 각 데이터 세그먼트에 대한 상대 이동의 세트를 포함한다. 스크램블링된 데이터 패킷(959)의 제1 데이터 세그먼트인 0 번째 프레임은 1D 데이터 세그먼트를 3회 이동, 즉 3 시프트만큼 좌측으로 이동시킴으로써 결정된다. 제1 프레임은 그 본래 위치, 즉 0 개소의 이동으로부터 변하지 않은 데이터 세그먼트(1B)를 포함한다. 제2 프레임은 그 본래 위치로부터 2회 이동하여 좌측으로 시프트된 데이터 세그먼트인 1E를 포함한다. 그 본래의 위치로부터 좌측으로 시프트된 데이터 세그먼트(1F)를 포함하는 제3 프레임에 대해서도 동일하다. 스크램블링된 데이터 패킷 출력(959)의 제4 프레임은 그 본래 위치로부터 우측으로 시프트된 데이터 세그먼트(1C), 즉 +2 이동을 포함한다. 제5 프레임은 그 본래의 위치로부터 우측으로 5회, 즉 +5 시프트된 데이터 세그먼트(1A)를 포함한다.

[0371] 분류 #C에 대해 표(957)에 요약된 이러한 방식으로, 모든 데이터 세그먼트는 매개변수적으로 결정된 스크램블링된 데이터 패킷(959)을 생성하기 위해 새로운 위치로 독특하게 이동된다. 스크램블링된 데이터 패킷을 언스크램블링하기 위해, 동일한 알고리즘이 언스크램블링 동작을 수행하도록 선택되는 것을 보장하기 위해, 데이터 패킷의 매개변수 값(953)은 스크램블링 동작의 결과로서 변화될 수 없다. 예를 들어, 모든 데이터 세그먼트의 매개변수 값의 선형 합계를 사용하면 숫자의 순서와는 관계없이 동일한 수치를 생성한다.

[0372] 동적 스크램블링은 데이터 패킷이 스크램블링되었을 때의 조건을 식별할 수 있어서, 동일한 방법이 언스크램블링 동작을 수행하도록 선택될 수 있게 하는, 시스템 상태, 예를 들어 시간을 이용한다. 도 2e에 도시된 시스템에서, 상기 상태는 패키지의 송신자 또는 수신자에게 전송된 위장된 수치 시드를 생성하는데 사용되며, 그 후 표로부터 스크램블링 알고리즘을 선택하기 위해 시드를 사용한다. 대안적으로, 상태 자체는 송신자 또는 수신자에게 전송될 수 있고, 상기 상태는 스크램블링/언스크램블링 알고리즘을 선택하는데 사용되는 은폐 숫자를 생성하기 위해 송신자 또는 수신자에 위치된 은폐 숫자 생성기에 의해 사용될 수 있다. 따라서, 도 2e에서, 상태, 예를 들어 시간(920)은 은폐 숫자 생성기(960)를 사용하여 은폐 숫자(961)를 생성하고, 스크램블링 알고리즘 목록(962)으로부터 스크램블링 방법을 선택하는데 사용된다. 은폐 숫자 생성기(960)는 또한 은폐 숫자 HN(961b)를 스크램블링 동작(963)에 직접적으로 입력할 수 있고, 여기에서 HN은 스크램블링 동작 실행에서 변수로서의 역할을 할 수 있다. 그 후에, 스크램블링 동작(963)은 언스크램블링 데이터 패킷(930)을 스크램블링된 데이터 패킷(964)으로 변환한다. 도 2f에 도시된 바와 같이, 상태(920)가 은폐 숫자 생성기(960)에 직접 전달될 수 있거나, 상태(920)가 시드 생성기(921)를 통해 은폐 숫자 생성기로 전달될 수 있다.

[0373] 수치 시드 대신에 스크램블링 알고리즘을 선택하기 위해 은폐 숫자를 사용하는 이점은 데이터 스트림을 분석함으로써, 즉 스크램블링된 데이터의 반복된 세트를 대응의 수치 시드와 통계적으로 관련시킴으로써 사이버 범죄

자가 스크램블링 표를 재생성할 가능성을 제거한다는 점이다. 시드가 데이터 스트림에서 보일 수 있고 이에 따라 스파이 활동에 노출될 수도 있더라도, 은폐 숫자 생성기와 은폐 숫자(HN)는 공유된 비밀을 기초로 한다. 따라서 은폐 숫자(HN)는 데이터 스트림에 존재하지 않거나 스파이 활동 또는 스니핑에 노출되며, 네트워크를통해 전송되지는 않지만 수치 시드로부터 로컬로 생성된다는 것을 의미한다. 은폐 숫자 생성기의 이런 수학적 동작은, 수치 시드의 목적이 위장되어 있기 때문에, 해커를 좌절시키는 추가적인 보안 계층을 부여한다.

[0374] 알고리즘이 일단 선택되면, 수치 시드는 스크램블링 프로세스(963)의 알고리즘에서 입력 변수로서 사용될 수도 있다. 수치 시드의 이중 사용은 시드가 알고리즘을 직접 선택하지는 않지만 그와 함께 작용하기 때문에 혼동되는 분석이다. 스크램블링된 데이터 세그먼트의 최종 시퀀스를 결정한다. 유사한 방식으로, 동적으로 스크램블링된 데이터 패킷을 스크램블링하기 위해, 시드(929)(또는 대안적으로 상태 또는 시간(920))는 스크램블링을 초기에 수행하는 통신 노드, 디바이스 또는 소프트웨어로부터 스크램블링을 원하는 노드 또는 디바이스로 통과되어야만 한다.

[0375] 개시된 발명에 따라, 시드 생성 알고리즘(921), 은폐 숫자 생성기(960), 및 스크램블링 알고리즘의 목록(962)은 "공유된 비밀", DMZ 서버에 저장되고(후술되는 바와 같이) 데이터 패킷의 송신자 또는 수신자에게는 알려지지 않은 정보를 나타낸다. 상기 공유 비밀은 사전에 설정되며, 또한 가능하기로는 비밀이 누출되지 않는 것을 보장하기 위해 다양한 인증 절차가 사용되는 코드 설치 중에 송신될 통신 데이터 패킷과는 관련이 없다. 이하에 기재되는 바와 같이, 공유 비밀은 도난당한 비밀 중 한 세트를 알고 있으면 해커가 전체 통신 네트워크에 액세스하거나 실시간 성명을 가로채지 못하도록, "구역"으로 제한된다.

[0376] 데이터 패킷 전송 중에 스크램블링 알고리즘이 변화하는 동적 스크램블링에서 임의의 공유 비밀에 추가하여, 데이터를 스크램블링하거나 언스크램블링하기 위해 "상태"에 기초하는 시드가 요구된다. 시드가 기반이 되는 이 상태는 시드를 생성하는데 사용된 상태에 대한 모호성이 없는 한, 또한 상기 데이터 패킷을 마지막 스크램블링하는데 어떤 상태가 사용되었는지를 다음 노드에 알려주는 약간의 수단이 있는 한, 시간, 통신 노드 번호, 네트워크 ID 또는 GPS 위치와 같은 임의의 물리적 매개변수를 포함할 수 있다. 시드를 생성하기 위해 시드 생성기에 의해 사용된 알고리즘은 공유 비밀의 일부이며, 이에 따라 시드의 지식은 시드의 기반이 되는 상태를 결정하는 것을 허용하지 않는다. 시드는 데이터 패킷 자체 내에 이를 매립함으로써, 이를 다른 채널 또는 경로, 또는 그 일부 조합을 통해 송신함으로써 하나의 통신 노드로부터 다음 통신 노드로 통과될 수 있다. 예를 들어, 시드를 생성하는데 사용된 상태는, 카운터에 의해서 생성되고 데이터 패킷이 통신 노드를 횡단할 때마다 일정한 수만큼 후속적으로 증가되는 난수를 포함할 수 있으며, 각각의 카운트는 특정 스크램블링 알고리즘을 나타낸다.

[0377] 동적 스크램블링의 일 실시예에 있어서, 스크램블링의 제1 사례 중, 사용되는 스크램블링 방법을 선택하기 위해 난수가 생성된다. 이 난수는 명령 및 제어를 위해 예약되고 스크램블링에 노출되지 않는 데이터 패킷의 헤더 또는 부분에서 데이터 패킷에 매립된다. 데이터 패킷이 다음 노드에 도달하였을 때, 매립된 수는 적절한 알고리즘을 선택하여 들어오는 데이터 패킷을 언스크램블링하도록, 통신 노드에 의해 판독되며 또한 소프트웨어에 의해 사용된다. 수, 즉 "카운트"는 하나의 카운트 또는 일부 다른 미리 결정된 정수만큼 다음에 증가되며, 패킷은 이 새로운 수와 관련된 알고리즘에 따라 스크램블링되고, 또한 새로운 카운트는 이전의 수를 덮어 쓰는 데이터 패킷 출력에 저장된다. 다음 통신 노드는 상기 프로세스를 반복한다.

[0378] 스크램블링 알고리즘을 선택하기 위해 기재된 카운터 기반 방법의 다른 실시예에 있어서, 초기 스크램블링 알고리즘을 선택하기 위해 난수가 생성되며, 이 수는 지정 데이터 패킷을 "공유된 비밀"로서 전송하기 위해 사용되는 모든 통신 노드로 전달된다. 예를 들어, 0으로 시작하는 카운트는 명령 및 제어를 위해 예약되고 스크램블링에 노출되지 않는 데이터 패킷의 헤더 또는 부분의 데이터 패킷에도 매립된다. 그 후 데이터 패킷은 다음 통신 노드로 포워딩된다. 패킷이 다음 통신 노드에 도착하였을 때, 서버는 카운트의 값을 판독하고, 초기 난수에 카운트를 부가하며, 데이터 패킷을 최종 스크램블링하는데 사용되는 스크램블링 알고리즘을 식별하고, 이에 따라 패킷을 언스크램블한다. 그 후 카운트는 하나 또는 임의의 미리 결정된 정수만큼 증가되며, 카운트는 데이터 패킷의 헤더 또는 명령 및 제어를 위해 예약되고 스크램블링에 노출되지 않은 데이터 패킷의 임의의 부분에 다시 저장되어 이전 카운트를 덮어쓴다. 공유 비밀로서 기능하는 난수는 통신 데이터 패킷에서 통신되지 않는다. 데이터 패킷이 다음 통신 노드에 도달하였을 때, 서버는 데이터 패킷으로부터 추출된 수정된 카운터 값에 추가되는 난수 공유 비밀을 추가한다. 이 새로운 수는 들어오는 패킷을 스크램블링하기 위해 마지막 통신 노드에 의해 사용된 스크램블링 알고리즘을 고유하게 식별한다. 이 방법에 있어서, 데이터가 의미하는 것을 알지 못하는 사이버 해적은 데이터 패킷의 언스크램블링된 부분에서 의미 없는 카운트 숫자만을 가로챌 수 있다.

[0379] 다른 대안적인 방법에 있어서, 은폐 숫자는 패킷의 상태 및 어떤 알고리즘이 이를 스크램블링하기 위해 이용되

었는지를 통신하기 위해 사용될 수 있다. 은폐 숫자는 기밀 번호, 즉 통신 노드간에 절대 통신되지 않으며 따라서 임의의 중간 공격자 또는 사이버 해적에게 스니핑이 불가능하거나 발견될 수 없는 "은폐 숫자"를 생성하기 위해 함께 숫자 알고리즘을 일반적으로 포함하는 공유 암호와 함께 시변화 상태 또는 시드를 결합한다. 은폐 숫자는 사용된 스크램블 알고리즘을 선택하는데 사용된다. 숨은 숫자를 계산하는데 사용된 알고리즘을 알지 못하면 상태 또는 시드가 의미가 없는데, 그 이유는 공유 비밀 알고리즘이 네트워크 또는 인터넷을 통해 액세스할 수 없는 방화벽 뒤에 저장될 수 있기 때문에, 네트워크 트래픽의 모니터링의 양이 패턴을 폭로하지 않기 때문이다. 문제를 더욱 복잡하게 하기 위해, 시드의 위치는 공유된 비밀을 나타낼 수도 있다. 일 실시예에 있어서, 데이터 패킷의 언스크램블링된 부분에 의해 운반되고 데이터 스니핑, 예를 들어, 27482567822552213에 의해 관찰 가능한 번호는 숫자의 일부만 시드를 나타내는 긴 숫자를 포함한다. 예를 들어, 제3 내지 제8 숫자가 시드를 나타낸다면, 실제 시드는 전체 숫자가 아니라 굵게 표시된 숫자 27482567822552213 이며, 즉 시드는 48256 이다. 이 시드는 은폐 숫자를 생성하기 위해 공유 비밀 알고리즘과 조합되며, 상기 은폐 숫자는 네트워크 전체를 통해 동적으로 변하는 스크램블 알고리즘을 선택하는데 사용된다.

[0380] SDNP 네트워크 내의 데이터 패킷의 스크램블링의 적용이 2015년 7월 20일에 출원되고 명칭이 "Secure Dynamic Communication Network and Protocol"인 미국 출원 제14/803,869호에서 설명되어 있다. 라스트 마일 통신에서 데이터 패킷 스크램블링을 적용하는 것은 이러한 개시 내용에서 더 구체적으로 설명될 것이다.

[0381] 설명된 바와 같이, 비록 스크램블링되었더라도, 네트워크를 횡단하는 데이터는 "평문"으로 지칭될 수 있는데, 그 이유는 실제 데이터가 데이터 패킷에 존재하기 때문에, 즉, 패킷이 암호문으로 암호화되지 않았기 때문이다. 대조적으로, 암호문에서, 스크램블 여부와는 상관없이 본래 데이터를 포함하는 텍스트 스트링은 암호 키를 사용하여 일련의 무의미한 텍스트로 번역되고, 또한 해독 키 없이 그 본래의 평문 형태로 복원될 수 없다. 기재된 SDNP 기반 통신에서의 암호화의 역할은 이하의 섹션 "암호화"에서 보다 자세히 논의된다.

[0382] 네트워크를 통한 전송 중에 데이터 패킷의 순서를 변경하기 위해, 도 3에 도시된 바와 같이 패킷 "재스크램블링"이 요구된다. 패킷 재스크램블링의 프로세스는 이를 다시 스크램블링하기 전에 새로운 스크램블링 알고리즘을 가지고 스크램블링된 데이터 패킷을 그 언스크램블링된 상태로 복귀시킨다. 따라서 여기에 사용되는 바와 같이 "재스크램블링"이라는 용어는 전형적으로 상이한 스크램블링 알고리즘 또는 방법으로 데이터 패킷의 언스크램블링 및 그 후 이를 다시 스크램블링하는 것을 의미한다. 이런 접근법은 이전에 스크램블링된 패키지를 스크램블링하고 또한 본래 데이터를 복원하는데 필요한 시퀀스 트랙을 잃어버림으로써 발생할 수 있는 데이터 손상의 위험을 피한다. 도시된 바와 같이, 일단 패킷 스크램블링 동작(926)에 의해 초기에 스크램블링되었다면, 스크램블링된 데이터 패킷(1008)은 먼저 데이터를 스크램블링하는데 사용된 스크램블링 알고리즘의 역동작을 사용하는 언스크램블링 동작(928)으로 이를 언스크램블링하고, 그 후 이전의 스크램블링 동작(926)에 사용된 것 보다 상이한 스크램블링 알고리즘을 사용하는 새로운 스크램블링 동작(926)으로 데이터 패킷을 스크램블함으로써 "재스크램블"된다. 결과적인 재스크램블링된 데이터 패킷(1009)은 이전의 스크램블링된 데이터 패킷(1008)과는 상이하다. 재스크램블링 동작(1017)은 여기서 "US 재스크램블링"으로서 지칭되는 스크램블링이 뒤따르는 언스크램블링의 연속적인 적용을 포함한다. 여기서 “US”는 “언스크램블링-스크램블링(unscrambling-scraambling)”의 약어이다. 본래의 데이터 패킷(930)을 회복하기 위해, 최종 패킷 언스크램블링 동작(928)은 데이터 패킷을 마지막 재스크램블링하는데 사용된 동일한 알고리즘의 역기능을 사용할 것을 요구한다.

[0383] 개시된 발명에 따라, 데이터의 정적 및 동적 스크램블은 언스크램블링된 데이터의 해석을 의미 없게 하고, 소리를 인식할 수 없는 노이즈로 재정렬하고, 비디오를 비디오 스노우로 재정렬하고, 텍스트를 재정렬하고, 및 복구할 수 없는 코드를 스크램블한다. 자체적으로, 스크램블링은 큰 수준의 보안을 제공한다. 그러나 여기에 기재된 SDNP 방법에서, 스크램블링은 해킹, 사이버 공격, 사이버 해적, 및 중간 공격자 공격으로부터 자유로운 통신을 제공하고 보장하는데 이용되는 단지 하나의 요소일 뿐이다.

[0384] ***패킷 암호화(Packet Encryption)*** - 기재된 발명에 따라, 패킷 교환형 네트워크를 통한 보안 통신은 해킹을 방지하고 보안을 보장하기 위해 여러 요소에 의존하는데, 그 중 하나는 SDNP 암호화를 포함한다. 이미 기재된 바와 같이 그리스어로 "은폐, 은닉, 모호"라는 의미의 암호화는 통상적으로 "평문"이라고 지칭되는 일반 정보 또는 데이터를 비밀 지식 없이 읽을 수 없는 이해하기 어려운 포맷을 포함하는 "암호문"으로 변환하는 수단을 나타낸다. 현대의 통신에서, 이런 비밀 지식은 일반적으로 데이터를 암호화하고 해독하는데 사용되는 하나 또는 그 이상의 "키"를 공유하는 것을 포함한다. 상기 키는 일반적으로 알고리즘으로 생성된 의사 난수를 포함한다. 오늘날 많은 기사와 텍스트가 닐 스티븐슨(Neal Stephenson) ⓒ 1999에 의한 "암호화", 사이몬 싱(Simon Singh) ⓒ 1999에 의한 "코드 북: 고대 이집트로부터 양자 암호로의 비밀의 과학", 닐 퍼거슨(Niels Ferguson) ⓒ 2013에 의한 "실질 암호화" 및 1939년에 처음 출판된 "해독: 암호 및 그 해법에 관한 연구"와 같은 다양한 암호화 기술

의 장단점을 논의하는데 사용할 수 있다.

[0385] 암호화 또는 암호의 개념이 오래되었고 본 기술분야의 당업자에게 잘 알려져 있지만, 개시된 보안 동적 통신 네트워크 및 프로토콜에서의 암호화의 적용은 독특하며, 임의의 클라이언트의 자체 암호화와 상관없이 네트워크 아키텍처 자체에 엔드 투 엔드 암호화와 단일의 홉 노드 대 노드 동적 암호화 모두를 촉진시켰다. SDNP 통신은 충분한 시간이 주어진 기본 수칙으로 구성되며, 또한 암호화된 암호문과는 상관없이 임의의 정적 암호화된 파일 또는 메시지가 결국 파괴되어 그 정보가 도난당할 수 있다. 이런 가정이 실제로 부정확할 수 있지만, 반대의 경우, 즉 지정 암호화 방법이 실패할 때까지 기다리는 것은 허용할 수 없고 되돌릴 수 없는 결과적 손상을 초래할 수 있기 때문에, 명제를 증명하거나 반증할 필요가 없다.

[0386] 대신에, SDNP 통신은 모든 암호화된 파일이 제한된 "유효 기간"을 갖는다는 전제를 기반으로 하며, 즉 암호화된 데이터는 한정된 기간 동안만 안전하며 비밀 데이터는 동적으로 규칙적인 간격으로 다시 암호화되어야 하며, 또한 최첨단 컴퓨터로 그 암호화를 균열시키는데 요구되는 최상의 시간 추정 보다 이상적으로 훨씬 더 자주 발생한다는 것을 은유적으로 의미한다. 예를 들어, 암호학자에 의해 암호 엔진의 대향 서버 팜(server farm)이 1년 내에 주어진 암호를 깨뜨릴 수 있다고 추정된다면, SDNP 통신에서 데이터 패킷은 매초 또는 심지어 매 100 ms 간격으로 재암호화될 것이며, 최상의 기술의 능력이 이를 균열시킬 수 있는 것보다 더 짧다. 따라서 SDNP 암호화는 반드시 동적인, 즉 시변화형이며, 또한 공간적으로, 즉 패킷 교환형 네트워크 또는 지리적 위치에서 통신 노드의 위치에 따라 변한다. 따라서 여기에 사용되는 바와 같이, "재암호화" 또는 "재암호"라는 용어는 데이터 패킷을 해독하고 그 후 전형적으로 상이한 암호화 알고리즘 또는 방법으로 이를 다시 암호화하는 것을 지칭한다.

[0387] 따라서, SDNP 암호화는 암호화되지 않은 평문으로부터의 데이터를 반복적으로 자주 암호화 텍스트로 변환하여, 정보를 이해할 수 없고 쓸모 없게 만든다. SDNP의 동적 암호화 방법을 사용함으로써 주어진 패킷의 데이터 암호화가 기적적으로 파괴되었더라도, 다음 데이터 패킷은 완전히 상이한 암호화 키 또는 암호를 사용하며, 또한 그 암호화를 균열시키기 위해 완전히 새로운 노력을 요구한다. 각각 독창적으로 암호화된 데이터 패킷의 전체 콘텐츠를 제한함으로써, 허가되지 않은 액세스의 잠재적 피해가 완화되는데, 그 이유는 노출된 데이터 패킷 자체가 너무 작아서 사이버 해적단에 의해 의미 없거나 유용하지 않은 데이터 파일을 포함하기 때문이다. 더욱이, 동적인 암호화를 전술한 SDNP 스크램블링 방법과 조합함으로써, 통신 보안이 대단히 향상된다. 심지어 그 암호화되지 않은 형태에서, 가로챈 데이터 파일은 데이터 세그먼트의 의미 없고 이해할 수 없는 시퀀스로 스크램블링된 데이터, 음성 또는 비디오의 단지 작은 스니펫만 포함할 뿐이다.

[0388] 유효 기간 보안 문제를 피하기 위해서, SDNP 암호화는 동적이고 상태-의존적이다. 도 4a에 도시된 바와 같이, 암호화 동작(1020)을 통해 처리된 평문(930)을 포함하는 암호화되지 않은 데이터 패킷은, 암호문(1024 또는 1025)을 포함하는 암호화된 데이터 패킷으로 나타난다. 암호문(1024)의 경우, 평문(930)의 전체 데이터 패킷은 전부 암호화되며, 데이터 세그먼트(1A 내지 1F)를 단일의 데이터 파일로서 취급한다. 암호문(1025)의 경우에, 각 데이터 세그먼트(1A 내지 1F)는 개별적으로 그리고 명확하게 암호화되고 다른 데이터 세그먼트와 병합되지 않는다. 제1 데이터 세그먼트(1A)는 예시적인 목적으로 7 $로 시작하며 도시되지 않은 긴 텍스트 스트링 또는 숫자를 포함하는 텍스트 스트링에 의해 도시된 대응하는 제1 암호 텍스트 데이터 세그먼트로 암호화된다. 마찬가지로, 제2 평문 데이터 세그먼트(1B)는 *^로 시작하는 예시적인 목적으로 도시된 긴 텍스트 스트링을 포함하는 제2 암호 암호문 데이터 세그먼트로 암호화된다. 텍스트 7 $ 및 *^는 의미 없은 기호, 숫자 및 영숫자 텍스트 스트링의 시작을 나타내는 것을 의미하며, 평문 소스 또는 암호화될 텍스트 스트링의 길이에서 지정한 데이터에 대해 어떤 것을 제한하거나 부여하지 않는다.

[0389] 암호화 동작(1020)은 이용 가능한 임의의 알고리즘, 암호화 또는 암호 방법을 사용할 수 있다. 알고리즘이 정적 방정식을 나타낼 수 있는 반면에, 일 실시예에서 암호화 동작은 암호화가 발생할 때 시간(920)과 같은 동적 변수 또는 "상태" 및 "E 키"(1022)를 생성하기 위해 암호화 생성기(1021)를 사용하며, 이는 암호화가 수행되었던 시간(920)과 같은 상태에 의존할 수도 있다. 예를 들어, 암호화의 날짜 및 시간은 암호화 알고리즘이 발견되더라도 재생성될 수 없는 암호화 키를 생성하기 위한 수치 시드로서 사용될 수 있다. 시간(920) 또는 다른 "상태"는 사용 가능한 암호화 알고리즘의 목록인 암호화 알고리즘 목록(1023)로부터 지정 알고리즘을 선택하도록 사용될 수도 있다. 데이터 흐름도에서, 암호화 동작(1026)을 위해 도시된 심볼에 의해 도시된 바와 같이, 도식적인 또는 기호적인 표현을 사용하여 이 패킷 암호화 동작 및 시퀀스를 설명하는 것이 편리하다. 본 발명의 전반에 걸쳐, 패드록(padlock)은 또한 보안 및 암호화된 데이터를 기호로 나타낼 수도 있다. 패드록의 꼭대기에 위치한 시계면(clock face)을 갖는 패드록은 구체적으로 보안 전달 메커니즘, 예를 들어 암호화된 파일을 나타

내며, 이는 지정 간격 또는 지정 시간 내에 수신되지 않았다면, 자멸하고 영원히 손실된다.

[0390] 도 4b에 도시된 해독 동작은 암호화 동작(1020)의 역기능, 구체적으로는 해독 동작(1031)을 도시하고 있으며, 여기서 D-키 생성기(1029)에 의해 생성된 해독 키 또는 "D-키"와 함께, 상태 또는 시간(920) 및 암호문(1024)을 생성하기 위해 사용된 다른 상태는 본래의 평문 데이터 패킷(990)을 포함하는 암호화되지 않은 데이터를 생성하기 위해 암호화를 취소하기 위해, 즉 파일을 해독하기 위해 재사용된다. 패킷 암호화가 처음 발생했을 때 사용된 동일한 상태 또는 시간(920)을 사용하여, 암호화 알고리즘 목록(1023)으로부터 선택된 동일한 암호화 동작이 해독 동작(1031)에서 다시 사용될 수 있다. 암호화 알고리즘 목록(1023)이 용어 "암호화"를 지칭하더라도, 동일한 알고리즘 표가 "해독"을 수행하는데 필요한 역기능을 식별하고 선택하는데 사용되며, 즉 암호화 알고리즘 목록(1023)은 데이터 패킷을 암호화하고 해독하는데 필요한 정보를 포함한다. 두 기능이 역순으로 수행되는 동일한 단계를 포함하기 때문에, 표(1023)는 "암호화/해독" 알고리즘 표(1023)로 이름이 바뀔 수 있다. 그러나 명확함을 위해, 표는 기능에 의해서만 표시되고 반 기능으로는 라벨링되지 않는다.

[0391] 해독 동작(1031)을 실행하기 위해 선택된 암호화 알고리즘이 패킷 암호화 동작(1020)에 사용된 본래의 알고리즘의 역과 일치하지 않으면, 시간 또는 상태(920)가 암호화가 발생된 시간과 일치하지 않으면, 또는 D-키(1030)가 암호화 중 사용된 E-키(1022)에 대해 미리 정의된 숫자 관계를 갖지 못하면, 해독 동작(1031)은 본래의 암호화되지 않은 데이터(990)를 복구하지 못하며, 또한 패킷 데이터는 손실될 것이다. 데이터 흐름도에 있어서, 해독 동작(1032)을 위해 도시된 심볼로 도시된 바와 같이, 이 패킷 해독 동작 및 시퀀스를 개략적인 또는 심볼형 표현을 사용하여 도시하는 것이 편리하다.

[0392] 본 발명에서 이미 설명한 바와 같이, 암호 작성술에서 암호화 및 해독 키의 사용과, 대칭형 공개 키 암호화, RSA 암호화, 및 AES256 암호화와 같은 공통 암호화 알고리즘의 암호화의 사용에 관한 지식은 통상적인 것이며 그리고 본 기술분야의 숙련자에게 잘 알려져 있다. 그러나 기재된 SDNP 통신 시스템에서의 이러한 알려진 암호화 방법의 적용은 해킹 또는 해독에 쉽게 영향을 받지 않는데, 그 이유는 숨겨진 정보, 공유된 비밀, 및 기재된 SDNP 통신에 고유한 시간-의존 동적 변수 및 상태 때문이다.

[0393] 따라서 사이버 해적이 강력한 암호화 방법을 깨기에 충분한 컴퓨터 성능을 갖추고 있더라도, 이들은 해독 동작을 수행하는데 필요한 비공개 또는 공유 비밀로서 SDNP 네트워크에 매립된 어떤 정보가 부족하며, 암호화가 변하기 전에 몇 분의 1 초에 암호화를 균열시켜야만 한다. 또한, 기재된 SDNP 네트워크를 횡단하는 모든 데이터 패킷은 고유 키 및 동적 상태를 갖는 상이한 암호화 방법을 이용한다. 주어진 패킷 내에 포함된 누락된 정보, 동적 상태 및 제한된 정보 콘텐츠의 조합은 사이버 해적에게 대한 도전과 배제 모두에서 임의의 주어진 데이터 패킷으로부터 의미 있는 데이터 절도를 얻게 한다.

[0394] SDNP 네트워크 내의 데이터 패킷의 동적 암호화 및 해독의 적용이, 전술한 "Secure Dynamic Communication Network and Protocol"라는 명칭의 미국 출원 제14/803,869호에 설명되어 있다. 라스트 마일 통신에서의 데이터 패킷 암호문의 적용은 이러한 개시 내용에서 더 구체적으로 설명될 것이다.

[0395] 전체 문서, 비디오 스트림 또는 음성 대화를 가로채서 일관된 데이터 시퀀스를 재구성하기 위해, 사이버 공격은 연속적으로 하나가 아니라 수천 개의 연속적인 SDNP 패킷을 연속적으로 균열시키고 해독해야 한다. 일련의 SDNP 패킷의 연속적인 해킹의 벅찬 도전은 동적 암호화와 상기 데이터 패킷 스크램블링에 관한 이미 기재된 방법을 조합함으로써 더욱 악화된다. 도 5에 도시된 바와 같이, 암호화된 스크램블링된 데이터 패킷(1024)의 생성은 스크램블링되지 않은 평문 데이터 패킷(990)을 먼저 스크램블링된 평문 데이터 패킷(1008)으로 변환하고 그 후 스크램블링된 데이터 패킷의 암호문(1024)으로 변환하기 위해, 스크램블링 동작(926)과 암호화 동작(1026)의 연속적인 조합을 포함한다. 암호화된 스크램블링된 패키지를 되돌리기 위해, 스크램블링된 평문 데이터 패킷(1035)을 복원하도록 먼저 해독 동작(1032)에 의해, 그 후 다음 언스크램블링된 평문 데이터 패킷(990)을 복원하도록 언스크램블링 동작(928)에 의해 역기능이 역순으로 적용되어야만 한다.

[0396] 도시된 바와 같이, 스크램블링 및 암호화는 보안 통신을 달성 시 보완적인 기술을 나타낸다. 네트워크를 횡단하는 암호화되지 않은 스크램블링된 데이터는 "평문"으로서 지칭되는데, 그 이유는 실제 데이터가 데이터 패킷에 존재하기 때문에, 즉 패킷이 암호문으로 암호화되지 않았기 때문이다. 암호화된 데이터 패킷 또는 암호문은 암호화 키를 사용하여 무의미한 일련의 터무니없는 텍스트로 변환된 스크램블 또는 언스크램블링된 텍스트 스트링을 포함하며, 또한 대응하는 해독 키 없이 그 본래의 평문 형태로 복원될 수 없다. 사용된 알고리즘에 따라, 암호화 및 해독 키는 사전 정의된 수학적 관계에 의해 수학적으로 관련된 동일한 키 또는 구별 키를 포함할 수 있다. 따라서 스크램블링 및 암호화는 SDNP 통신을 위해 기재된 발명에 따라 보안 통신의 달성 시 보완적인 기술을 나타낸다.

[0397] 2가지 방법, 즉 스크램블링 및 암호화는 암호화된 스크램블링된 데이터 패킷으로부터 본래 데이터 패킷을 복원하는데 사용되는 시퀀스가 이를 생성하는데 사용된 역순으로 발생해야 한다는 점을 제외하고는, 조합하여 사용하는 경우라도 독립적으로 고려할 수 있다. 예를 들어, 데이터 패킷(990)이 스크램블링 동작(926)을 사용하여 먼저 스크램블링되고 나서 암호화 동작(1026)을 사용하여 암호화되면, 본래의 데이터 패킷을 복원하기 위해, 암호화된 스크램블링된 데이터 패킷(1024)은 먼저 해독 동작(1032)을 사용하여 해독되어야만 하고, 그 후 언스크램블링동작(928)을 사용하여 언스크램블링되어야 한다. 수학적으로, 스크램블링 동작(F)이 일련의 비트열 또는 텍스트 스트링을 등가의 스크램블링된 버전으로 스크램블링하고 언스크램블링 동작($F^{-1}$)이 스크램블링을 취소하면, $F^{-1}[F(A)] = A$으로 되며, 유사하게 암호화 동작(G)이 평문의 스트링을 등가 암호문으로 암호화하고, 해독 동작($G^{-1}$)이 암호화를 취소하면, $G^{-1}[G(A)] = A$으로 되며, 그 후, 조합하여 스크램블링 및 이어서 암호화 및 해독 그리고 언스크램블링의 연속적인 동작은 본래의 변수(argument)(A)인, 언스크램블링된 평문 데이터 패킷으로 복원시킨다. 따라서, $F^{-1}\{G^{-1}[G(F(A))]\} = A$으로 되는데, 이는 시퀀스가 역순으로 발생하기 때문이며, 특히 [$G^{-1}$] 암호화된 스크램블링된 패킷[G(F(A)]을 해독하는 것은 스크램블링된 평문 데이터 패킷 F(A)를 복원한다. 스크램블링된 평문 패킷 F(A)의 후속의 언스크램블링 동작[F(A)]은 본래의 데이터 패킷(A)을 복원한다.

[0398] 제공된 선형 방법이 사용되면, 시퀀스는 가역적이다. 예를 들어, 데이터 패킷이 먼저 암호화되고 나서 스크램블링된다면, 그 후 본래의 데이터 패킷을 복원하기 위해, 스크램블링된 암호문은 먼저 언스크램블링되고 해독되어야만한다. 따라서 $G^{-1}\{F^{-1}[F(G(A))]\} = A$가 된다.

[0399] 시퀀스 변경은 작용하지 않는다. 먼저 언스크램블링이 없이 이전에 암호화되고 나서 스크램블링된 데이터 패킷을 해독하면 본래의 데이터 패킷을 복구하지 않을 것이며, 즉 $F^{-1}\{G^{-1}[F(G(A))]\} \neq A$으로 된다.

[0400] 마찬가지로, 스크램블링되고 그 후 암호화된 패킷의 해독 또한 본래의 데이터 패킷을 복원하지 못할 것인데, 이는 $G^{-1}\{F^{-1}[G(F(A))]\} \neq A$ 이기 때문이다.

[0401] 요약하면, 평문 패킷이 암호화되기 전에 스크램블링된다면, 언스크램블링되기 전에 해독되어야만 하며, 평문 패킷이 스크램블링되기 전에 암호화되었다면, 해독되기 전에 언스크램블링되어야만 한다.

[0402] 본 발명에 따른 SDNP 방법의 일 실시예에 있어서, 스크램블링 및 암호화는 어느 순서로 수행될 수 있지만, 네트워크 전송 중에는 암호화 및 해독이 스크램블링보다 더 빈번하게 발생하며, 따라서 도 5에 도시된 바와 같이 역전되기보다는 언스크램블링 전에 스크램블링 및 해독이 발생한 후에만 암호화가 발생해야 한다. 편의상, 우리는 암호화 동작(1026)에 이어지는 패킷 스크램블링 동작(926)의 조합을 스크램블링된 패킷 암호화 동작(1041)으로서 정의하였으며, 또한 그 역으로, 패킷 언스크램블링 동작(928)에 이어지는 해독화 동작(1032)의 조합을 해독된 패킷 스크램블링 동작(1042)으로서 정의하였다. 이들 하이브리드된 동작은 본 발명에 따라 정적 및 동적 SDNP 통신에 사용될 수 있다.

[0403] 정적 스크램블링 암호화를 사용하는 임의의 실행에서 보안을 향상시키기 위한 하나의 수단은 각각의 데이터 패킷이 통신 네트워크에 들어가는 시간($t_1$)에서 상태, 시드 및/또는 키에서의 변경을 포함하여, 송신된 각각의 데이터 패킷이 상이한 스크램블링 및/또는 암호화 방법에 노출되는 것을 보장하는 것이다.

[0404] 그러나 패킷이 정시에 네트워크를 횡단할 때, 데이터 패킷의 암호화 또는 스크램블링 또는 두 가지 모두를 동적으로 변경하는 것이 더욱 강력한 대안이다. 필요한 데이터 처리를 촉진시켜 SDNP 통신의 완전 동적 버전을 구현하기 위해, 이것이 패킷 교환형 통신 네트워크에서 각각의 통신 노드를 통과할 때, 각각의 패킷을 "재스크램블"(즉, 언스크램블 및 스크램블) 및 재암호화(즉, 암호화 해제 및 그 후 암호화)하도록 이전의 정의된 프로세스를 조합할 필요가 있다. 여기서 사용되는 바와 같이, "재패킷" 또는 "재패킷팅"이라는 용어는 언스크램블링되기 전에 처음에 해독되거나 또는 해독되기 전에 언스크램블링되는지에 따라 때로 "재스크램블링" 및 "재암호화"의 조합을 지칭하기 위해 사용될 것이다. 어느 경우에나, 주어진 노드에서 언스크램블링 및 해독 동작은 패킷이 이전 노드를 떠날 때 스크램블링 및 암호화 동작의 반대의 순서로 수행되어야만 하며, 즉 패킷이 이전의 노드에서 스크램블링되고 그 후 암호화되었다면, 현재 노드에서 먼저 해독되어야 하고 그 후 언스크램블링되어야 한다. 전형적으로, 패킷은 현재 노드를 떠날 때 스크램블링되고 그 후 암호화될 것이다.

[0405] 통신 노드에서의 "재패킷" 동작이 도 6에 도시되어 있으며, 여기서 들어오는 암호문 데이터 패킷(1040)은 먼저 해독 동작(1032)에 의해 해독되고, 그 후 본래의 패킷의 콘텐츠를 포함하는 언스크램블링된 평문 데이터 패킷

(990)을 복구하기 위해 언스크램블링 동작(928)에 의해 언스크램블된다. 패킷 내의 임의의 정보가 검사, 파싱, 분할, 또는 재지향되어야만 한다면, 언스크램블링된 평문 파일은 이러한 동작을 수행하기에 가장 적합한 포맷이다. 그 후, 평문 데이터 패킷(990)은 새로운 스크램블링된 암호문 데이터 패킷(1043)을 생성하기 위해, 암호화 동작(1026)에 의해 수행되는 새로운 암호화가 뒤따르는 스크램블링 동작(926)을 사용하여 다시 스크램블링된이다. 들어오는 스크램블링된 암호문 데이터 패킷(1040)의 재패킷 동작이 해독, 언스크램블링, 스크램블링 및 암호화에 의해 연속적으로 발생하기 때문에, 약어 DUSE 재패킷 동작(1045)은 여기에서는 본 발명에 따라 기재된 기술을 나타내기 위해 여기에 사용된다. 동적 보안 네트워크에서, 해독 동작(1032) 및 언스크램블링 동작(928)을 수행하는데 사용되는 상태 또는 시간, 해독 키 및 임의의 시드는 바람직하게는 스크램블링 동작(926) 및 암호화 동작을 실행하는데 사용되는 상태 또는 시간, 시드 또는 암호화 키와는 상이하다.

[0406] SDNP 네트워크 내의 데이터 패킷의 재패킷의 적용이 전술한 "Secure Dynamic Communication Network and Protocol"라는 명칭의 미국 출원 제14/803,869호에서 설명되어 있다. 라스트 마일 통신에서의 데이터 패킷 재패킷의 적용은 이러한 개시 내용에서 더 구체적으로 설명될 것이다.

[0407] ***패킷 혼합 및 분할(Packet Mixing and Splitting)*** - 여기에 기재된 보안 동적 통신 네트워크 및 프로토콜의 다른 핵심 요소는 데이터 패킷을 서브-패킷으로 분할하고, 이들 서브-패킷을 다중 경로 내로 유도하고, 및 서브-패킷을 혼합 및 재결합하여 완전한 데이터 패킷을 구성하는 그 능력이다. 패킷 분할의 프로세스가 도 7a에 도시되어 있으며, 여기서 데이터 패킷(1054)은 알고리즘 파싱 동작(1052)과 그리고 비 데이터 "정크" 데이터 세그먼트를 삽입하거나 제거하는 능력을 갖는 정크 동작(1053)과 조합된 분할 동작(1051)을 사용하여 분할된다. 인간 게놈에 존재하는 정크 DNA와 유사하게, 정크 데이터 세그먼트는 정크 동작(1053)에 의해 삽입되어, 데이터 패킷의 길이를 연장하거나 제어하고, 또는 필요에 따라 제거한다. 정크 동작(1053)은 패킷을 채우기에 부적절한 양의 데이터가 있을 때 특히 중요하다. 데이터 패킷 내에 삽입된 정크 데이터 세그먼트의 존재는 사이버 해적이 실제 데이터를 노이즈로부터 구별하는 것을 어렵게 한다. 여기에 사용되는 바와 같이, "정크" 패킷 또는 데이터 세그먼트는 완전히 무의미한 데이터(비트)로 구성된 패킷 또는 데이터 세그먼트이다. 이들 정크 비트는 의미 없는 비트의 바다에서 실제 데이터를 혼동스럽게 하는 데이터 패킷의 스트림 내에 도입될 수 있다.

[0408] 파싱 동작(1052)의 목적은 각각의 구성요소를 처리하기 위해 데이터 패킷(1054)을 더 작은 데이터 패킷, 예를 들어, 데이터 서브-패킷(1055, 1056)으로 분할하는 것이다. 데이터 패킷(1054)을 더 작은 단편으로 분할하는 것은 다중 경로 전송을 지원하는 것과 같은, 즉 다중 및 상이한 경로를 통해 데이터 패킷을 전송하는 것과 같은, 그리고 상이한 암호화 방법을 사용하여 구성 서브-패킷의 고유한 암호화를 촉진시키는 것과 같은 고유한 이점을 제공한다.

[0409] 분할 동작은 임의의 알고리즘, 숫자 방법 또는 파싱 방법을 사용할 수 있다. 알고리즘은 정적 방정식을 나타내거나, 또는 들어오는 입력 데이터 패킷(1054)이 많은 서브-패킷에 의해 처음 형성되었을 때의 시간(920) 및 시드 생성기(921)에 의해 생성된 수치 시드(929)와 같은 동적 변수 또는 수치 시드 또는 "상태"를 포함할 수 있으며, 이는 또한 데이터 패킷의 생성 시 시간(920)과 같은 상태에 의존할 수 있다. 예를 들어, 각각의 날짜가 단조롭게 오름차순으로 고유한 숫자로 변환되었다면, 모든 시드(929)는 고유하다. 시간(920) 및 시드(929)는 이용가능한 방법의 목록, 즉 알고리즘(1050)으로부터 선택된 지정 알고리즘을 식별하는데 사용될 수 있다. 패킷 분할 또는 비 혼합은 지정한 패킷을 생성하기 위해 정확하게 사용된 정밀한 역 시퀀스로 실행되는 동일한 알고리즘을 사용하는, 혼합의 절차를 포함한다. 궁극적으로 사용된 모든 동작은 취소되지만, 그러나 반드시 하나의 단계에서는 아니다. 예를 들어, 스크램블링된 암호화된 데이터 패킷은 해독되지만 스크램블링된 채로 존재할 수 있다. 분할 동작(1051)에 의해 처리되면, 분할되지 않은 들어오는 데이터 패킷(1054)은 다중 데이터 패킷으로 변환되며, 예를 들어 상기 동작을 알고리즘으로 수행하기 위해 파싱 동작(1052)을 사용하여 고정된 길이의 패킷(1055, 1056)을 분할한다. 데이터 흐름도에 있어서, 분할 동작(1057)을 위해 도시된 심볼에 의해 여기에 도시되는 바와 같이, 도식적인 또는 심볼형 표현을 사용하는 파싱(1052) 및 정크 동작(1053)을 포함하는 이런 패킷 분할 동작(1051)을 설명하는 것이 편리하다.

[0410] 따라서 여기에 사용되는 바와 같이, "분할"이라는 용어는 파싱을 포함하며, 이는 패킷을 2개 또는 그 이상의 패킷 또는 서브-패킷으로의 분리를 지칭하며, 또한 이는 결과적인 "파싱된" 패킷에 정크 패킷 또는 서브-패킷의 삽입 또는 결과적인 "파싱된" 패킷 또는 서브-패킷에서 정크 패킷 또는 서브-패킷의 삭제를 포함할 수도 있다.

[0411] 도 7b에 도시된 역기능, 패킷-혼합 동작(1060)은 혼합된 패킷(1054)을 형성하기 위해 다중 패킷(1055, 1056)을 함께 조합한다. 패킷 분할과 마찬가지로, 패킷 혼합 동작은 임의의 알고리즘, 수치 방법 또는 혼합 방법을 사용할 수 있다. 상기 알고리즘은 정적 방정식을 나타낼 수 있거나, 들어오는 데이터 패킷(1055, 1056)이 혼합될 때

의 조건을 지정하기 위해 사용되는 시간(920)과 같은 동적 변수 또는 수치 시드 또는 "상태"를 포함할 수 있다. 데이터 패킷을 생성하는데 사용되는 혼합 동작은 시간(920)과 같은 상태에 의존할 수도 있는 시드 생성기(921)에 의해 생성되는 수치 시드(929)를 이용할 수 있다. 시간(920) 및 시드(929)는 사용 가능한 혼합 방법의 목록, 즉 혼합 알고리즘(1050)으로부터 선택된 지정 혼합 알고리즘을 식별하는데 사용될 수 있다. 데이터 흐름도에 있어서, 혼합 동작(1061)을 위해 도시된 심볼에 의해 여기에 도시된 바와 같이, 개략적인 또는 심볼형 표현을 사용하여 이 패킷 혼합 동작을 설명하는 것이 편리하다.

[0412] 본 발명에 따라, 패킷 혼합 및 분할은 다수의 가능한 알고리즘 중 임의를 이용할 수 있다. 도 8은 연쇄(concatenation), 인터리빙(interleaving) 또는 알고리즘 방법을 포함하는 다수의 가능한 혼합 방법 중 3개를 도시하고 있다. 연결 시, 데이터 패킷(1056)의 데이터 세그먼트 시퀀스는 데이터 패킷(1055)의 단부에 추가되어, 혼합 패킷(1054)을 생성한다. 인터리빙에 있어서, 데이터 패킷(1055, 1056)의 데이터 세그먼트는 교번적인 형태로, 즉 1A, 2A, 1B, 2B 등에 결합되어, 혼합 데이터 패킷(1065)을 형성한다. 패킷 혼합을 위해 사용되는 다른 방법은 알고리즘을 포함한다. 도시된 예에 있어서, 인터리빙된 반사 대칭을 포함하는 알고리즘은 혼합된 패킷(1066)의 전반부에서 1A, 2A, 1B, 2B, 1C, 2C의 순서로 데이터 세그먼트를 교차하고, 후반부에서 반대 순서로, 즉 2D, 1D, 2E, 1E, 2F, 1F의 순서로 교차한다.

[0413] 데이터 패킷 혼합 및 분할을 SDNP 네트워크에서 적용하는 것이 "Secure Dynamic Communication Network and Protocol"라는 명칭의 전술한 미국 출원 제14/803,869호에서 설명된다. 도 9a는, 기능 및 그 상응 역동작, 즉 역기능뿐만 아니라 상응 기능의 동적 구성요소 즉, 데이터 패킷 상에서 실행될 때의 각각의 기능의 상태 또는 시간을 포함하는 SDNP 기능적 요소를 개략적으로 도시한다. SDNP 기능은 패킷 스크램블링(926) 및 그 역기능 패킷 언스크램블링(928)을 포함하는 스크램블링 동작; 분할(1057) 및 그 역기능 혼합(1061)을 포함하는 단편화 동작, 정크 삽입(1053) 및 정크 제거(1053B)를 포함하는 기만 동작과 함께, 암호화(1026) 및 해독(1032)을 포함하는 암호화 동작을 포함한다. 이러한 모든 동작은 시간 또는 상태 변수(920)에 따라 특이적으로 발생된다.

[0414] 라스트 마일 통신에서 스크램블링, 언스크램블링, 암호화, 해독, 및 기만과 함께, 데이터 패킷 혼합 및 분할을 적용하는 것은 집합적으로 SDNP 라스트 마일 보안 동작을 포함한다. 이러한 SDNP 라스트 마일 보안 동작은 "지향적"이고, 이는 모든 진출 데이터 패킷을 위해서 그리고 그곳에서 실시되는 동작이 유입 데이터 패킷 상에서 실시되는 동작과 다르다는 것을 의미한다.

[0415] SDNP 라스트 마일 보안 동작은 또한 라스트 마일에 걸쳐 대칭적이고 가역적이며, 이는 특정 라스트 마일에 특정된 키, 시드, 공유 비밀과 같은 로컬 보안 자격 증명을 이용할 때, 클라이언트의 디바이스 내의 아웃바운드 데이터 패킷에서 실시되는 동작이, 일반적으로 역기능, 즉 수학적 역수로 실시하는 것, 또는 클라이언트의 디바이스에 의해서 원래 실행되었던 그러나 반대 시퀀스의 모든 기능적 동작에 의해서, SDNP 게이트웨이에서 원상태로 돌려진다는 것을 의미한다. 따라서, SDNP 게이트웨이는 SDNP 클라우드를 통해서 라우팅하기 위한 준비에서 원래의 콘텐츠로 복원할 수 있다. 유사하게, 라스트 마일을 위한 구역-특정 보안 자격 증명을 이용하여 클라이언트의 디바이스 내로 데이터 패킷을 유입시키기 위해서, 클라이언트 디바이스에서 실행되는 SDNP 라스트 마일 보안 동작은, 반대 시퀀스의 역기능을 실행함으로써 SDNP 게이트웨이에 의해서 실시되는 각각의 보안 동작을 원상태로 돌린다. 이러한 방식으로, 클라이언트 디바이스는 모든 유입 데이터 패킷에서 원래의 데이터를 복원할 수 있다.

[0416] SDNP 라스트 마일 보안 동작은 동적이고 국소적이며, 즉 구역 특이적이고, 데이터 패킷이 준비될 때 어떠한 매개변수가 사용되었는지 그리고 특정 라스트 마일에 특이적인 영역, 지리적 위치, 또는 로케일이 어떠한지를 결정하기 위해서, 상태 의존적 조건, 즉 위치, 시간 등을 이용한다. 국소화되는 것에 의해서, 상이한 영역들에서 그리고 상이한 라스트 마일 연결들에서 실시된 데이터 패킷 준비는 결코 동일한 코딩을 가지지 않거나 동일한 보안 자격 증명을 사용하지 않는다. 또한, 이러한 라스트 마일 보안 자격 증명은 항상 SDNP 클라우드에서 사용되는 것과 상이하다. 또한, 동적으로, 데이터 패킷을 생성하기 위해서 이용된 상태가 일정하게 변화되어, 각각의 데이터 패킷에서 실시되는 실제 보안 프로세스를 더 혼동시키고 2개의 데이터 패킷이 유사하게 만들지 않는다.

[0417] 각각의 라스트 마일 통신에 대해서 특정된 지향적인 대칭적 가역적 동적 국소화된 보안 동작의 특유의 조합적 적용에 의해서, 본 발명에서 만들어진 동적 스크램블링, 동적 단편화, 동적 기만, 및 동적 암호화의 알고리즘적 적용은, 단순한 정적 암호화 방법의 이용으로 달성될 수 없는 하이퍼보안 통신을 보장한다. 단지 수십 밀리초의 지속시간 동안 유효한 동적 방법의 포괄적인 적용은 해석을 거의 불가능하게 할 뿐만 아니라, 다른 도달 전에 데이터 패킷을 해독 또는 해석할 수 있는 시간을 해커에게 주지 않는다. 실제로, SDNP 라스트 마일 보안

동작은, 소프트웨어, 펌웨어, 하드웨어, 전용 보안 IC, 또는 그 임의의 조합을 이용하여 실행될 수 있다.

[0418] 비록 무수한 조합적 시퀀스가 가능하지만, 특히 단일-경로 라스트 마일 통신에서 이용되는 직렬 SDNP 페이로드를 위한, SDNP 라스트 마일 보안 동작의 하나의 예가 도 9b에 도시되어 있고, 즉 여기에서 클라이언트의 디바이스는 단일 SDNP 게이트웨이와 통신한다. 그러한 프로세스는 2개의 지향적 동작 시퀀스를 포함하고, 그 중 하나는 진출 데이터 패킷을 위한 것이고, 다른 하나는 진입 데이터 패킷을 위한 것이다. 도면의 상부 절반에 도시된, 진출 데이터 패킷의 경우에, "송신되는 데이터"가 먼저 패킷-스크램블링 동작(926)을 이용하여 스크램블링되고, 이어서 정크 데이터(1053A)의 삽입에 의해서 기만이 실시된다. 일부 경우에, 전체 패킷이 전체적으로 정크 데이터를 포함하여, 해커에 의한 데이터 채굴 시도를 더 혼란스럽게 할 수 있다.

[0419] 이어서, 이러한 패킷들은 파싱 동작(1052)을 이용하는 분할 동작(1057)에 의해서 다수의 단편으로 분할되고, 암호화 동작(1026)으로 별개로 송신된다. 이어서, 각각의 단편은 공통된 또는 구분된 암호화 키를 이용하여 암호화되고, 결과적인 암호문은 데이터 패킷(1199A)으로서 도시된 직렬 SDNP 페이로드로 배열된다. 이어서, 라스트 링크 및 라스트 마일 상으로의 통신을 위한 준비에서, 패킷이 IP 데이터 패킷으로, 즉 "IP 패킷 준비"로 포맷된다. 실시되는 모든 동작은 동적이고, 보안 프로세스 실행 중에 특정 시간에서 또는 특정 상태(920A)로 발생된다.

[0420] 도면의 하부 절반에 도시된 유입 데이터 패킷의 경우에, 직렬 SDNP 페이로드(1199B)를 포함하는 라스트 링크로부터의, 즉 "IP 패킷 인식"으로부터의 유입 데이터가 먼저, 실제 데이터 스트림을 복원하기 위해서 해독 동작(1032) 및 후속되는 혼합 동작(1061)에 의해서, 단편으로 또는 전체적으로 해독된다. 이어서, "수신 데이터"를 복원하기 위해서, 역정크 동작(1053B) 및 후속되는 패킷 언스크램블링 동작(928)을 이용하여, 데이터 패킷이 역정킹되고, 즉 정크 데이터가 데이터 패킷으로부터 제거된다. 유입 데이터 패킷에서 실시되는 모든 동작은, SDNP 게이트웨이가 데이터 패킷을 생성할 때 이용한, 즉 패킷의 탄생시에 특정 시간에 관한 또는 특정 상태(920B)를 갖는 정보를 포함하는, 상태(920B)를 이용하여야 한다. 이러한 상태 정보는 시그널링 서버에 의해서 상이한 통신을 통해서 송신될 수 있거나, 평문으로서 또는 대안적으로 정적 암호문으로서, 즉 SDNP 라스트 마일 보안 동작에 의해서 이미 알려진 해독 키를 갖는 암호문으로서 유입 데이터 패킷 내에서 수반될 수 있다. 그러나, 상태(920B)에 관한 상세 내용은 상태(920B) 내에 포함된 상태 정보를 필요로 하는 키를 이용하여 해독될 수 없거나, 달리 코드는 그 자체의 보안 자격 증명을 열고 사용할 수 없을 것이다.

[0421] 특히 다중-경로 라스트 마일 통신에서 이용되는 병렬 SDNP 페이로드를 위한, SDNP 라스트 마일 보안 동작의 다른 예가 도 9c에 도시되어 있고, 즉 여기에서 클라이언트의 디바이스는 다수의 SDNP 게이트웨이와 통신한다. 전술한 그 단일 경로 대응부분과 마찬가지로, 그러한 프로세스는 2개의 지향적 동작 시퀀스를 포함하고, 그 중 하나는 진출 데이터 패킷을 위한 것이고, 다른 하나는 진입 데이터 패킷을 위한 것이다. 도면의 상부 절반에 도시된, 진출 데이터 패킷의 경우에, "송신되는 데이터"가 먼저 패킷-스크램블링 동작(926)을 이용하여 스크램블링되고, 이어서 정크 데이터(1053C)의 삽입에 의해서 기만이 실시된다. 일부 경우에, 전체 패킷이 전체적으로 정크 데이터를 포함하여, 해커에 의한 데이터 탈취 시도를 더 혼란스럽게 할 수 있다.

[0422] 이어서, 이러한 패킷들은 파싱 동작(1052)을 이용하는 분할 동작(1057)에 의해서 다수의 서브-패킷으로 분할되고, 암호화 동작(1026)으로 별개로 송신된다. 이어서, 각각의 단편은 공통된 또는 구분된 암호화 키를 이용하여 암호화되고, 결과적인 암호문은 데이터 패킷(1199C, 1199D, 및 1199E)으로서 도시된 다중 SDNP 페이로드로 배열된다. 이어서, 라스트 링크 및 라스트 마일 상으로의 통신을 위한 준비에서, 패킷이 분리된 그리고 구분된 IP 데이터 패킷들, 즉 "IP 패킷 준비"로 포맷된다. 실시되는 모든 동작은 동적이고, 보안 프로세스 실행 중에 특정 시간에서 또는 특정 상태(920C)로 발생된다.

[0423] 도면의 하부 절반에 도시된 유입 데이터 패킷의 경우에, 병렬 SDNP 페이로드(1199F, 1199G, 및 1199H)를 포함하는 라스트 링크로부터의, 즉 "IP 패킷 인식"으로부터의 유입 데이터가 먼저, 실제 데이터 스트림을 복원하기 위해서 해독 동작(1032) 및 후속되는 혼합 동작(1061)에 의해서, 단편 방식으로 해독된다. 이어서, "수신 데이터"를 복원하기 위해서, 역정크 동작(1053D) 및 후속되는 패킷 언스크램블링 동작(928)을 이용하여, 데이터 패킷이 역정킹되고, 즉 정크 데이터가 데이터 패킷으로부터 제거된다. 유입 데이터 패킷에서 실시되는 모든 동작은, SDNP 게이트웨이가 데이터 패킷을 생성할 때 이용한, 즉 패킷의 탄생시에 특정 시간에 관한 또는 특정 상태(920D)를 갖는 정보를 포함하는, 상태(920D)를 이용하여야 한다. 이러한 상태 정보는 시그널링 서버에 의해서 상이한 통신을 통해서 송신될 수 있거나, 평문으로서 또는 대안적으로 정적 암호문으로서, 즉 SDNP 라스트 마일 보안 동작에 의해서 이미 알려진 해독 키를 갖는 암호문으로서 유입 데이터 패킷 내에서 수반될 수 있다.

[0424] SDNP 라스트 마일 보안 동작은 양 진입 데이터 및 진출 데이터 패킷 모두에서 동일한 알고리즘 또는 방법을 이

용할 필요가 없다. 도 9d에 예시된 바와 같이, 진출 데이터 패킷은 SDNP 라스트 마일 보안 동작(1190A)을 이용하는 한편, 진입 데이터 패킷은 SDNP 라스트 마일 보안 동작(1190B)을 이용한다. 도면의 상부 절반을 참조하면, 진출 데이터 패킷은 변환기 또는 센서로부터의 실시간 데이터 소스의 임의의 조합을 나타내는 데이터를 수반할 수 있거나, 통신 전에 만들어진 파일을 포함할 수 있다. 예를 들어, 마이크로폰(1180)에 의해서 전기 신호로 변화된 소리(1198A) 및 카메라(1181)로부터의 비디오 신호가 오디오 비디오 코덱(1182A)에 의해서 동등한 디지털 포맷으로 변환된다. 생성된 포맷은 일반적으로, 프레젠테이션 계층인, OSI 계층 6에 따라 표준 디바이스로 해석 가능한 그리고 상호 동작 가능한 png, pic, mpeg, mov 등과 같은 표준을 포함한다. 표준 오디오 비디오 포맷을 이용하는 것은 소스와 목적지 어드레스 사이에서 파일을 열기 위한 독점적 코드를 전달할 필요성을 방지한다.

[0425] 이어서, 오디오 비디오 코덱(1182A)의 디지털 출력이, 콘텐츠 혼합기(1184)를 이용하여, 가상의 키보드(1183)(터치 스크린 상에서 실현된 키패드)로부터의 텍스트 데이터와 그리고 데이터 파일(1179A)과 혼합된다. 이러한 혼합기는, 다시, 데이터 파일을 SDNP 라스트 마일 보안 동작(1190A)으로 송신하고, 정적 파일로부터 실시간 데이터 패킷을 식별하고 라벨링하도록, SDNP 헤더 정보를 IP 패킷 준비 동작(1191A)에 제공한다. 이어서, SDNP 라스트 마일 보안 동작(1190A)은 보안 데이터 패킷을 IP 패킷 준비 동작(1191A)에 전달하고, 이는 그 후에, SDNP 시그널링 서버(1603)에 의해서 수신된 라우팅 명령어에 따라, SDNP 페이로드를 IP 데이터 패킷 내로 임베딩한다. 데이터 패킷은 다중-경로 라스트 마일 통신을 위한 다수의 IP 패킷으로 분산될 수 있거나, 직렬 데이터 스트링으로 연쇄될 수 있고 단일 경로 라스트 마일 통신을 위해서 하나 이상 직렬 데이터 패킷 내로 임베딩되고 피팅될 수 있다. 이어서, 계층 1 및 계층 2 데이터를 부가하여 IP 데이터 패킷을 완성하기 위해서, 이러한 패킷이 클라이언트 PHY 동작(1192A)으로 전달된다.

[0426] 도면의 하부 절반에서 도시된 역동작에서, 클라이언트 PHY(1192B)에 의해서 수신된 라스트 링크로부터의 진입 데이터가 IP 패킷 인식 동작(1191B)으로 전달되고, 이는 진입 데이터를 유효 메시지로서 또는 미지의 그리고 가능한 악성 데이터 패킷으로서 식별한다. 유효 메시지는, 시그널링 서버(1603)에 의해서 클라이언트 디바이스에 그리고 IP 패킷 인식 동작(1191B)에 미리 통신된, SDNP 태그, 시드, 키, 및 다른 식별자를 이용하여 식별된다.

[0427] 의인화에 따라, IP 패킷 인식 동작(1191B)은 유효 진입 데이터 패킷을 예상하고 심지어 기대한다. 적절한 식별을 가지지 않는 미예측 데이터 패킷은 폐기되고 결코 열리거나 더 프로세스되지 않는다. 이러한 방식으로, 해커는 그 스스로를 위장할 수 없고, 그 신원을 SDNP 클라우드에 먼저 등록하지 않고는, 유효 데이터를 어떠한 SDNP 노드로도 송신할 수 없다.

[0428] IP 패킷 인식 동작(1191B)은 유효 데이터 패킷을 SDNP 라스트 마일 보안 동작(1190B)에 전달하고, 이는 다시 데이터 패킷의 실제 콘텐츠 - 비디오, 오디오, 텍스트, 및 데이터 파일의 직렬로 배열된 혼합을 포함하는 데이터 - 를 재구성하기 위한 모든 필요 동작을 실시한다. 데이터 패킷 생성에서 사용된 혼합 동작을 원상태로 돌리는, 예를 들어 다른 통화자의 전화에서 실시된 혼합기 동작(1184)에 의해서 생성된 직렬 데이터 파일을 분류하는 역다중화기인, 콘텐츠 역다중화(1193)가 이어서 사용되어 여러 가지 파일 유형을 분리한다. 콘텐츠 역다중화(1193)의 출력은, 메신저 창(1196) 내에 디스플레이되어 도시된 텍스트, 데이터 파일(1179A), 및 오디오 비디오 코덱(1182B)에 송신된 실시간 데이터를 포함한다. 오디오 비디오 코덱(1182B)은 디지털 프레젠테이션 계층 데이터를 라이브 비디오 이미지(1195)로 변환하거나, 스피커(1194)를 통해서 소리(1198B)로 변환한다.

[0429] 라스트 마일 데이터 전송을 위해서, 데이터는, 전술한 러시아 전통의 포개지는 인형 모델과 유사하게, 도 9e에 도시된 다중-겹침 배열로 임베딩 또는 랩핑되어야 한다. 따라서, SDNP 페이로드(438)는, 전송 헤더(436)와 함께 IP 페이로드(435)를 포함하는, 전송 페이로드(437)를 나타낸다. IP 페이로드(435)와 IP 헤더(434)의 조합은, MAC 페이로드(432)와 동등한, IP 데이터그램을 나타낸다. MAC 헤더(431) 및 맥 푸터(footer)(433) 내에서 MAC 페이로드(432)를 랩핑하는 것은 MAC "프레임"을 초래하고, 그러한 프레임은, 전기 신호, 광, 라디오파, 또는 마이크로파와 같은 물리적 미디어를 포함하는, PHY 계층 1 콘텐츠로도 알려진, 물리적 계층(490)과 동등하다.

[0430] SDNP 라우팅에서, 계층 2 내의 MAC 헤더(431)는 라스트 링크를 위한 MAC 연결을 설명하고, 즉 라스트 마일 링크 내의 클라이언트 디바이스와 제1 디바이스 사이의 연결을 설명한다. 클라이언트 디바이스 및 SDNP 게이트웨이의 소스 및 목적지 어드레스를 이용하는 것에 의해서, 계층 3 내의 헤더(434)는 라스트 마일에 걸친 라우팅의 종료점을 특정한다. 그러나, 라스트 마일이 SDNP 클라우드의 일부가 아니기 때문에, 라스트 마일에 걸쳐 데이터 패킷이 취하는 정확한 경로는 명시적으로 기술되지 않거나 제어될 수 없다. SDNP 라스트 마일 통신에서, 계층 4 내의 전송 헤더(436)는 SDNP 실시간 페이로드를 위해서 사용되고, 또한 각각의 패킷에서 사용된 애드혹 할당된 SDNP 포트 어드레스 - 포트 질의 사이버-공격 전략을 방지하기 위해서 동적으로 변화되는 어드레스 - 를 특정한다.

[0431] 라스트 마일 IP 패킷의 페이로드인, SDNP 페이로드(438)는, 구역 정보, 키, 및 시드를 포함하는 SDNP 프리앰블(1198), 및 독립적으로 암호화된 암호문의 다수의 세그먼트의 직렬 스트링인, SDNP 데이터 필드(1199A)를 포함한다. 암호문의 해독된 형태는 평문 파일(1197A, 1997B, 및 1197C)을 포함하고, 이들 각각은 그 자체의 특이적 SDNP 헤더, 및 상응하는 데이터 파일 데이터(91), 데이터(92), 및 데이터(93) 각각을 포함한다. 개별적인 서브-헤더는 적용 가능한 것으로서 태그, 집, 어드레스, 긴급성, 및 QoS 데이터를 갖는 정보를 포함한다.

[0432] SDNP 프리앰블 및 헤더의 역할은 이용되는 명령 및 제어 방법에 따라 달라진다. 3-당사자 라스트 마일 통신에서, 시그널링 서버는, 통화를 위해서, 파일을 송신하기 위해서, 또는 세션을 열기 위해서 서로 어떻게 통신하여야 하는지를, 클라이언트 디바이스 및 SDNP 게이트웨이 또는 게이트웨이들에 지시한다. 따라서, 지시는, 어떠한 미디어 데이터 패킷도 송신하기 전에, TCP 전송을 갖는 명령 및 제어 데이터 패킷을 이용하여 양 디바이스에 통신된다. 따라서, 클라이언트와 SDNP 게이트웨이 사이의 라스트 마일 통신에서 요구되는 최소 데이터는 진입 패킷을 식별하기 위해서 이용되는 태그 또는 어드레스이다. 일부 경우에, 예를 들어, 시그널링 서버가 도달될 수 없는 경우에, 대안적인 실시예에서, SDNP 데이터 패킷은 그 프리앰블 및 패킷 헤더 내에서 부가적인 데이터를 수반할 수 있다.

[0433] 도 9f에 도시된 데이터 패킷 및 첨부된 표(1177)는 SDNP 페이로드(438) 내에서 SDNP 정보를 운반하기 위해서 이용되는 하나의 예시적인 포맷을 도시한다. 데이터 패킷은 SDNP 프리앰블(1198) 및 그 상응 데이터 필드 "데이터 X 필드"를 가지는 1 내지 8개의 데이터 필드 헤더(1178X)를 포함한다. "데이터 1 필드", "데이터 2 필드" 등과 같은 각각의 데이터 필드에는 그 상응 헤더(Hdr 1, Hdr 2 등)가 선행하고, 보이스, 텍스트, 비디오, 사진, 영화, 파일 등을 포함하는 코뮤니케의 콘텐츠를 수반한다. 데이터 필드의 수는, 4b 길이 필드 #, 즉 이진수 0001 내지 이진수 1111에 의해서 결정되는 바와 같이 1 내지 8 사이에서 변경될 수 있다. SDNP 프리앰블(1198) 및 SDNP 페이로드(438)의 길이는 필드 # 제원에 의해서 영향을 받는다. 하나의 필드만이 선택되는 경우, 즉 필드 # = 0001 이진수인 경우에, SDNP 프리앰블(1198)은 L Fld 1(L Fld 2 내지 L Fld 8은 제거될 것이다)만을 포함할 것이고, SDNP 페이로드(438)는 Hdr 1 및 데이터 1 필드만을 포함할 것이다. 8개의 필드의 최대값이 선택되는 경우, 즉 필드 # = 1111 이진수인 경우, SDNP 프리앰블(1198)은 8 길이 제원(L 필드 1 내지 L 필드 8)을 포함할 것이고, SDNP 페이로드(438)는, Hdr 1, 데이터 1 필드, Hdr 2, 데이터 2 필드, ...Hdr 8, 데이터 8 필드와 같은 시퀀스로, 8개의 데이터 필드 및 헤더를 포함할 것이다. 도시된 바와 같이, SDNP 프리앰블(1198)은 필드 길이 제원(L Fld 1, L Fld 2 및 L Fld 8)을 포함한다. L Fld 2와 L Fld 8 사이의 작은 간극은 시퀀스 계속을 나타내기 위한 것을 의미하고, 데이터 내의 간극을 나타내지 않는다.

[0434] L Fld X에 의해서 특정된 각각의 데이터 필드의 길이는 0 또는 0B(없는 데이터 필드)로부터 FFFF 또는 65,535B의 최대 16진법 길이까지 변경될 수 있다. 이더넷과의 양립성과 관련된 실제적인 이유로, 임의의 하나의 필드를 위한 최대 데이터 패킷 길이는 바람직하게 1500B 또는 16진수 05DC로 제한되고, 모든 데이터 필드의 총 길이는 9000B 또는 16진수 2328의 점보 패킷 크기를 초과하지 않아야 한다. 각각의 데이터 필드의 특정된 길이가 독립적으로 변경될 수 있다. 예를 들어 L Fld 8 = 0000 16진수인 0의 필드 길이는 상응 데이터 8 필드의 제거를 초래하나, 상응 헤더(Hdr 8)를 제거하지는 않는다. 헤더는 필드 # 제원에 의해서만 제거된다.

[0435] 이러한 SDNP 프로토콜에 따라, 다양한 데이터 필드에 걸친 콘텐츠의 할당이 매우 유연하다. 단일 목적지로 지향된 데이터가 단일 데이터 필드 내에 포함될 수 있거나, 기만 목적을 위해서 다수의 데이터 필드로 분할될 수 있고 정크 데이터와 병합될 수 있다. 데이터 필드의 크기가 독립적으로 달라질 수 있다. 정크 데이터만을 포함하는 데이터 필드가 또한 포함될 수 있거나, 대안적으로 정크 데이터만을 포함하는 전체 데이터 패킷이 생성될 수 있다. 그러나, 효율적인 패킷 라우팅을 위해서, 상이한 목적지들을 표적으로 하는 데이터가 분리된 데이터 필드들로 구획되어야 하고, 각각의 데이터 필드는 그자체의 특이적 헤더를 갖는다.

[0436] SDNP 패킷 포맷은, SDNP 클라우드 또는 라스트 마일 통신에서와 같은 다수의 클라우드 및 구역들에 걸쳐지는 것을 포함하는 전체 SDNP 네트워크 전반을 통해서, 엔드-투-엔드 전송을 위해서 적용될 수 있다. 비록, SDNP 데이터 패킷의 콘텐츠가, 네트워크를 횡단할 때, 변화되지만, SDNP 패킷 포맷은 변화되지 않고 유지된다. 이러한 포맷이 최소 데이터 오버헤드를 포함하기 때문에, SDNP 데이터 패킷 포맷은 큰 페이로드를 위해서 또는 시간 임계적 실시간 통신을 위해서 동일하게 적용될 수 있다. 패킷 포맷은 양방향 데이터 플로우를 위해서, 즉 라스트 마일로부터 SDNP 게이트웨이로의 그리고 SDNP 클라우드에 걸친 데이터 플로우를 위해서, 또는 역으로, 라스트 마일에 걸친 목적지 클라이언트 디바이스로의 전송을 위해서 SDNP 게이트웨이를 빠져나오는, 클라우드로부터 발생된 데이터 패킷을 전달하기 위해서 적용될 수 있다.

[0437] 동작시에, SDNP 데이터 라우팅의 방향은 네트워크 계층 3 소스 및 도 9e의 IP 헤더(434) 내에 기술된 목적지 어

드레스에 의해서 결정된다. 미디어 노드가 그 경로 상에서 다음 미디어 노드를 전송하기 위해서 패킷을 준비하는 시간에, 각각의 패킷에 그 소스 및 목적지 어드레스가 로딩되고 삼중-채널 통신에서, 패킷의 목적지의 SDNP 또는 IP 어드레스는, 진출 패킷 준비에 앞서서 명령 및 제어(C&C) 패킷으로서, 시그널링 서버로부터 미디어 노드로 전달된다. 일반적으로, 시그널링 서버는, 송신(통화자) 및 목적지(피통화자) 디바이스 모두를 포함하는 통신 통로 내의 모든 노드에 C&C 지시를 송신할 수 있다. 단일 채널 통신만이 이용가능한 경우에, 예를 들어 긴 전파 지연을 갖는 링크에서, 시그널링 서버는 진입 패킷의 미디어 노드 또는 그러한 것으로 무엇을 할지를 미리 경고할 수 없다. 그러한 경우에, 라우팅 어드레스는 SDNP 페이로드(438) 내의 진입 데이터 패킷 내에서 수반된다. 그러한 경우에, 미디어 서버는, 라우팅 및 상태 정보뿐만 아니라 보안 자격 증명을 포함하는 진입 SDNP 패킷 내에 포함된 데이터 필드를 이용하여 진입 패킷을 어떻게 프로세스할 지에 관한 디폴트 지시를 따른다.

[0438] 페이로드(438)는 2개의 부분, 즉 프리앰블(1198)을 포함하는 판독 가능 부분, 및 "은폐 형태"의 데이터를 포함하는 비판독 가능 부분(1199a)으로 구성된다. 이러한 패킷의 콘텐츠는, 암호화, 스크램블링, 및 가능한 정크 데이터 포함과 같이, 그 콘텐츠를 감추기 위한 임의의 수의 은폐 기술을 이용할 수 있다. 은폐 방법은 유용한 콘텐츠(1197a, 1997b 및 1197c)를 추출하기 위해서 원상태로 되돌려져야 한다. 이러한 패킷은 미래의 진출 패킷의 목적지 어드레스를 포함한다. 어드레스는, 다음 패킷이 준비되고 암호화될 수 있기 전에, 단지 짧은 순간 동안 미은폐 또는 해독된 형태로 단지 존재한다.

[0439] 설명된 바와 같이, SDNP 프리앰블(1198)은 전체 패킷과 관련된 정보를 포함한다. 데이터 필드 제원 이외에, 도 9f는, SDNP 패킷이 생성되었던 SDNP 구역, 예를 들어 구역(U1), 2개의 수치 시드, 및 2개의 키를 또한 포함하는 SDNP 프리앰블(1198)을 도시한다. 이러한 키 및 시드는 스크램블링/언스크램블링, 정크 삽입/제거, 혼합/분할, 및 암호화/해독 프로세스에서 구역 특정 보안 자격 증명으로서 이용될 수 있다. 시드 및 키가 데이터 필드를 열고 판독하는데 필요한 보안 자격 증명의 전달을 위한 배타적 수단으로서 이용될 수 있거나, 미디어 패킷 내의 코뮤니케 콘텐츠의 수반에 포함되지 않는 시그널링 서버, 명령 및 제어 컴퓨터의 네트워크로부터 클라이언트의 디바이스 및 SDNP 게이트웨이로 송신된 명령 및 제어 패킷과 함께 사용될 수 있다.

[0440] 시드 및 키는 공공적으로, 즉 비-암호화 형태로 보안 전달될 수 있는데, 이는 데이터가 그 이용에 필요한 정보를 가지지 않기 때문이다 - 이들은 보안 자격 증명의 부분만을 포함한다. 보안 자격 증명의 다른 부분인, 손실 단편들이 다른 데이터 패킷 내에서 이미 송신되었을 수 있거나, 네트워크를 통해서 전달되지 않고 메시지의 일부가 아닌 알고리즘의 공유된 비밀, 참조표, 및 코드를 포함할 수 있다. 암호화 키는 대칭적 키일 수 있고, 여기에서 송신자 및 수신자 모두가 키를 보유하거나, 공공 키를 보유할 수 있으며, 그러한 경우에 송신자를 포함하는 공공이 암호화 키에 액세스할 수 있으나 수신자만이, 즉 암호화 키를 생성하는 당사자만이 해독 키를 보유한다. 또한, 모든 보안 자격 증명이 특정 보안 구역, 예를 들어 U1으로 제한되고, 동적이고, 특정 시간 내에 사용되지 않는 경우에 만료되는 특정 시간 또는 상태로 제한된다. 예를 들어 시그널링 서버가 보안 동작과 관련된 SDNP 디바이스에 독립적으로 지시하기 때문에, 시드 및 키 데이터 필드가 보안 자격 증명으로서 사용되지 않는 경우에, 이러한 필드가 암호화 키로 잘못 보이는 수치 값으로 채워져, 사이버-공격자가 유인 보안 키를 분석하는데 시간을 낭비하도록 잘못 안내할 수 있다.

[0441] 라스트 마일 통신에서, 클라이언트의 디바이스와 SDNP 게이트웨이 사이의 중간 라우터는 전송된 데이터 패킷을 프로세스, 해석 또는 열지 않는데, 이는 그들이 SDNP 네트워크의 일부가 아니고 내부에 포함된 SDNP 패킷 데이터를 질의 또는 해석할 수 있는 능력을 가지지 않기 때문이다. 그 대신, 모든 보안 동작은, SDNP 클라이언트 및 SDNP 게이트웨이인, 2개의 단부 지점에서 배타적으로 실행되는데, 이는 이러한 디바이스들 만이 SDNP 통신 노드로서 동작하기 때문이다. 각각의 단부 지점이 SDNP 프로토콜을 동적으로 실행하기 때문에, 라스트 마일 통신은 전체 라스트 마일에 걸쳐 하이퍼보안이다. 다른 통화 당사자가 또한 SDNP 소프트웨어를 작동시키는 경우에, 제2 당사자의 라스트 마일이 또한 전술한 SDNP 방법에 의해서 보안되고, 하이퍼보안 통신이 "엔드-투-엔드"로 - 하나의 통화자로부터 다른 통화자까지 - 보장된다.

[0442] 그러나, 단부 디바이스가 SDNP 클라이언트가 아닌 경우에, 통화자에 가장 근접한 라우터 즉, 라스트 링크 라우터가 SDNP 펌웨어로 인에이블링될 수 있고, 라스트 링크는, SDNP 인에이블드가 아니더라도, SDNP 인에이블드 라우터에 의해서 실시되는 특별한 기능으로부터 합리적으로 보안될 수 있다. 이러한 대안적인 라스트 링크 보안 방법은 이 개시 내용의 후속 섹션에서 더 구체적으로 설명되고 이러한 섹션에서 더 구체적으로 설명하지 않을 것이다. 설명된 방법은, 라스트 링크 통신 보안에 적용될 수 있지만, 라스트 마일의 다른 부분을 보호하기에 충분치 않다.

[0443] 다시 도 9f를 참조하면, 각각의 그리고 모든 SDNP 데이터 필드는, 연관된 데이터 필드에 특이적으로 적용 가능

하나 다른 데이터 필드를 위해서는 유용하지 않은 정보를 포함하는 SDNP 데이터 필드 헤더(1178X)에 의해서 수반된다. 구체적으로, 개시된 실시예에서, 각각의 헤더는, 어떠한 종류의 데이터가 연관 데이터 필드 내에 포함되는지, 특정 데이터 필드 및 그 목적지를 식별하기 위해서 사용되는 목적지 어드레스 필드, 하나의 구역으로부터 다른 구역으로 포워드 구역 정보를 운반하기 위해서 이용된 필드 구역뿐만 아니라, 긴급성 및 전달 정보를 설명하는 데이터 유형 필드를 포함한다. 도시된 바와 같이, 각각의 SDNP 데이터 페이로드(438)는 하나의 SDNP 프리앰블(1198), 및 하나 이상 SDNP 데이터 필드 헤더(1178X) 및 상응 데이터 x 필드를 포함하고, 여기에서 x는 페이로드의 크기 및 긴급성에 따라 5 내지 50 범위일 수 있는 분리된 페이로드의 수를 설명한다.

[0444] 시그널링 서버가 설명 정보의 대부분을 SDNP 클라이언트 및 SDNP 게이트웨이에 공급할 수 있지만, 라스트 마일 데이터 패킷에 의해서 필수적으로 수반되는 하나의 기본 성분은 데이터 패킷을 식별하는데 필요한 "어드레스 필드" 또는 태그이다. (도면에서 "Dest Addr"로 축약된) SDNP 페이로드의 목적지 어드레스로서 지칭되는 필드는 하나의 데이터 필드의 신원을 다른 신원으로부터 구별하기에 충분한 임의의 특이적 식별자를 포함할 수 있다. 그 목적은 공항에서 가방을 또는 운반자가 선적한 상자를 태그 및 추적하기 위해서 이용되는 바코드의 기능과 유사하다. 어드레스 유형은, 데이터 패킷의 식별에서 충돌을 방지할 수 있을 정도로 식별자가 특이적이기만 하다면, 예를 들어 수치 태그, SDNP 집, IPv4 또는 IPv6 어드레스, NAT 어드레스, 또는 심지어 POTS 정규 전화번호를 포함할 수 있다. 목적지 어드레스 필드의 크기는 선택된 어드레스 유형의 타입에 따라 달라진다.

[0445] 라우팅 중에 패킷 익명성을 유지하기 위해서, 실제 전화 번호 또는 IP 어드레스 대신, SDNP 집 코드와 같은 비밀 코드를 SDNP 목적지 어드레스로서 이용하는 것이 바람직할 수 있다. 동작시에, SDNP 클라이언트로부터의 데이터 패킷이 SDNP 게이트웨이에 도달할 때마다, SDNP 페이로드가 해독되고 이어서 각각의 데이터 필드 헤더가 식별 목적지 어드레스를 위해서 검사된다. 데이터 헤더가 검사될 수 있기 전에, 패킷의 생성에서 이용된 은폐 방법을 원상태로 돌리기 위해서, 데이터 패킷이 해독되거나 프로세스되어야 한다. 이중-채널 또는 삼중-채널 통신의 경우에, 도 9g에서 도시된 바와 같이, 시그널링 서버(1603)은 데이터 패킷 및 그 상응 식별 마킹 및 보안 자격 증명의 계획된 도달을 SDNP 게이트웨이에 미리 통지하였다. 따라서, SDNP 게이트웨이가 SDNP 클라이언트로부터 송신된 라스트 마일 통신을 포함하는 데이터 패킷(438A)을 수신할 때, 게이트웨이는, 암호문으로부터의 SDNP 페이로드를 평문 데이터 패킷(438B)으로 변환하기 위해서, SDNP 라스트 마일 보안 동작(1190D)을 실시한다. 보안 동작은 콘텐츠 및 프로세스를 은폐하기 위해서 진출 데이터 패킷을 수정하는 그리고 콘텐츠를 밝히기 위해서 진입 데이터 패킷을 수정하는 프로세싱을 설명한다.

[0446] 구체적으로, 진입 데이터 패킷에서 실시되는 보안 동작은, 암호화를 원상태로 돌리기 위해서 해독을 이용하는 것, 스크램블링을 원상태로 돌리기 위해서 언스크램블링하는 것, 정크 삽입을 제거하기 위해서 역정크하는 것, 및 분할을 원상태로 돌리기 위해서 혼합하는 것을 포함하여, 해당 전송 전에 실시된 은폐 동작을 원상태로 돌리는 것에 의해서, 그 콘텐츠를 복원하기 위해서 사용된다. 이러한 프로세스는, 데이터 패킷이 생성될 때의 그러한 데이터 패킷의 상태 및 구역에 따라 실시된다. 진출 데이터 패킷에서, 보안 동작은, 데이터 패킷이 생성될 때 상태 및 구역에 따라 암호화, 스크램블링, 정크 삽입, 및 패킷 분할을 실시하는 것에 의해서, 전송 전에 데이터 패킷의 콘텐츠를 은폐하는 것을 포함한다. 데이터 패킷(438A) 내의 미암호화 시드 및 키 데이터 필드는 무시될 수 있거나 선택적으로 암호문을 해독하기 위해서 시그널링 서버 정보와 함께 이용될 수 있다. 결과적인 동작은, 데이터 필드의 목적지 어드레스, 데이터 유형, 긴급성 및 전달 정보를 포함하는, 데이터 필드 1 및 Hdr 1로 표시된 그 연관된 데이터 필드 헤더(117D)를 밝힌다. 그러한 경우에, 목적지 어드레스는 라우팅 어드레스가 아니고 단지 SDNP 집이고, 즉 패킷을 식별하기 위해서 이용된 태그는 특정 대화의 일부이다.

[0447] 특정 데이터 필드가, 시그널링 서버(1603)로부터의 지시와 매칭되는, 식별된 목적지 어드레스, 예를 들어 SDNP 집 코드를 포함하는 것으로 확인되면, 데이터 필드가 추출되고, 선택적으로 혼합기(1184Z)에 의해서 다른 관련 콘텐츠와 혼합되고, 그 다음 목적지로의 전달을 위해서 SDNP 패킷 준비 동작(1191Z)에 의해서, 새로운 IP 또는 SDNP 데이터그램으로 재랩핑된다. 클라우드로 향하는 새로운 데이터 패킷은, SDNP 페이로드(435Z)인, 새로운 패킷의 목적지 및 데이터 콘텐츠를 포함하는, SDNP 헤더(434Z)를 포함한다. IP 어드레스 또는 SDNP 어드레스로서 시그널링 서버(1603)에 의해서 게이트웨이 미디어 노드에 공급된 목적지가 SDNP 클라우드 노드로서 동작하는 다른 SDNP 서버를 포함할 수 있거나, 다른 SDNP 클라이언트로의 라스트 마일 통신을 포함할 수 있다. 그러한 삼중-채널 통신의 경우에, 목적지 어드레스는 실제 어드레스가 아니고 패킷을 식별하기 위한 수단이며, 여기에서 그 다음 목적지는 SDNP 게이트웨이에 의해서 이미 알려져 있다. 패킷의 목적지가 SDNP 클라우드 라우팅을 위한 것인 경우에, 데이터 패킷은, 라스트 마일에서 사용된 U1 자격 증명이 아니라, 클라우드를 위한 Z1 보안 자격 증명에 따른 SDNP 클라우드 보안 동작(1190Z)에 의해서 프로세스된다.

[0448] 단일 채널 통신에서, 도 9h에 도시된 바와 같이, 시그널링 서버는 데이터 패킷 및 그 데이터 필드의 임박한 도

달에 앞서서 SDNP 게이트웨이를 알릴 수 없는데, 이는 (i) 로컬 네트워크에서 동작되는 시그널링 서버가 없거나, (ii) 시그널링 서버가 일시적으로 오프라인이거나, (iii) 시그널링 서버가 너무 바쁘고 패킷을 제시간에 우선적으로 라우팅시킬 수 없기 때문이다. 그러한 경우에, SDNP 클라이언트로부터의 데이터 패킷(438A)은, 암호문 데이터 패킷(438A)을 평문 데이터 패킷(438B)으로 변환하는 SDNP 라스트 마일 보안 동작(1190D)을 이용하여 데이터 패킷을 해독하기 위해서, 필요 보안 자격 증명 구역(U1), 시드 1, 시드 2, 키 1 및 키 2를 수반하여야 한다. 표준 SDNP 데이터 패킷 포맷은, 필드의 콘텐츠가 특정 미디어 노드에 의해서 요구되지 않는 경우에도, 이러한 데이터 필드를 보존한다. 예를 들어, 데이터 패킷을 생성하기 위해서 이용된 특정 은폐 프로세스가 키 2 필드를 이용하지 않는 경우에, 해당 필드 내의 데이터는 의미가 없고 목적지 노드에 의해서 이용되지 않는다. 그럼에도 불구하고, 데이터 패킷은 사용된 또는 사용되지 않는 필드를 위한 동일한 수의 바이트를 보전하고, 그에 따라 모든 SDNP 데이터 패킷은 균질한 포맷이 된다. 데이터 패킷(438A) 내의 암호문을 일단 해독하면, SDNP 게이트웨이는 데이터 패킷 데이터 1 필드 및 그 연관된 Hdr 1 필드 헤더(1178D)의 콘텐츠를 평문 데이터 패킷(438B)으로부터 추출한다. 이러한 데이터 패킷으로부터, IP 패킷 인식 프로세스(1191D)는 2가지 이유 - 첫 번째로 삼중-채널 통신에서 진입 패킷이 예상되는지를 확인하기 위한 이유, 그리고, 두 번째로 새로운 SDNP 어드레스를 생성하기 위한 이유 - 로 Hdr 1 필드 헤더(1178D)로부터의 A 유형 및 목적지 어드레스를 위한 데이터 필드들을 조합한다. 이러한 새로운 SDNP 어드레스는 D 유형, 긴급성 및 전달 필드와 조합되고, SDNP 패킷 준비 동작(1191Z)에 의해서 프로세스되어 진출 데이터 패킷 내에서 SDNP 헤더(434Z)를 생성한다. 데이터 1 필드의 콘텐츠는 또한 진입 평문 데이터 패킷(438B)으로부터 추출되고, 그 콘텐츠는 선택적으로 다른 진출 콘텐츠와 혼합되어(1184Z) 진출 SDNP 페이로드(435Z)를 생성한다. 이어서, 패킷은 포워딩을 위한 준비에서 SDNP 클라우드 보안(1190Z)에 의해서 프로세스된다. 이러한 방식으로, 진입 데이터 패킷을 식별하기 위해서 그리고 필요한 경우에 포워딩 어드레스를 제공하기 위해서, 어드레스 필드가 다수의 기능을 실시한다.

[0449] 미디어 노드가 시그널링 서버로부터 지시를 먼저 수신하지 않고 데이터 패킷을 수신한 경우에, 미디어 노드는, 진입 데이터 패킷을 어떻게 프로세스할 것인지 그리고 진출 데이터 패킷을 어떻게 준비할 지에 관한 디폴트 지시로 복귀할 것이다. 미디어 노드가 미공표 진입 패킷을 어떻게 핸들링할 지에 관한 어떠한 지시도 보유하지 않은 경우에, 데이터 패킷은 폐기될 것이다. 미디어 노드가 미식별 패킷을 어떻게 프로세스할 지에 관한 지시로 인에이블링되는 경우에, 미디어 노드는 첫 번째로, 보안 자격 증명에 따라 패킷이 유효 SDNP 패킷인지를 확인할 것이고, 그에 따라 이를 프로세스할 것이다. 그러나, 송신자가 식별될 수 없는 경우에, 예를 들어 암호화 코드, 시드, 또는 소스 어드레스가 유효하지 않은 경우에, 패킷은 위조로서 폐기될 것이다.

[0450] 도 9f를 다시 참조하면, "필드 구역"으로 표시된 패킷 필드는, 특정 필드가 생성된 구역, 즉 과거의 암호화 또는 스크램블링이 예를 들어 U1 또는 U2 구역 설정으로 실시되었는지의 여부를 설명한다. 네스트형 보안 프로토콜 또는 다른 네스트형 은폐 방법의 경우에, 언스크램블링, 해독, 또는 데이터 패킷의 은폐를 원상태로 돌리는 부가적인 정보, 예를 들어 키, 시드, 시간 또는 상태를 요구하고, 그러한 경우에 "필드 기타"로 표시된 패킷 필드가 필드-특정 정보를 운반하기 위해서 이용될 수 있다. 일반적으로, 예를 들어 암호화된 데이터 필드가 이어서 스크램블링되거나 2번째로 암호화되는, 네스트형 보안 프로토콜에서를 제외하고, 이러한 필드는 이용되지 않는다. 정확하게 데이터 패킷의 준비에 반대되는 순서로 데이터 복원을 실시하기 위해서, 네스트형 보안 방법을 이용할 때 주의를 기울여야 하고, 그렇지 않으면 콘텐츠를 영원히 잃게 될 것이다.

[0451] "데이터 유형"이라고 표시된 패킷 필드는, 사용되는 경우에, 보이스 및 라이브 비디오와 같은 시간 민감형 정보를 포함하는 데이터 패킷으로부터의 실시간 통신을 필요로 하지 않는, 문맥-특정 라우팅, 구별 데이터, 미리-기록된 비디오, 텍스트 및 컴퓨터 파일을 촉진하고, 즉 실시간 라우팅을 비-실시간 데이터로부터 구별한다. 데이터 유형은 보이스, 텍스트, 실시간 비디오, 데이터, 소프트웨어 등을 포함한다.

[0452] "긴급성" 및 "전달"이라고 표시된 패킷 필드들이 함께 이용되어, 특정 데이터 필드에서 어떻게 데이터를 최적으로 라우팅시킬지를 결정한다. 긴급성은 스네일, 보통, 우선, 및 긴급 분류를 포함한다. 전달은 일반, 중복, 특별, 및 VIP 분류를 위한 다양한 QoS 마커를 포함한다. 본 발명의 일 실시예에서, 표(1177)에 도시된 바와 같은 다양한 데이터 필드의 이진수 크기는 필요 통신 대역폭을 최소화하도록 선택된다. 예를 들어, 도시된 바와 같은 데이터 필드는 0 내지 200B 범위일 수 있고, 그에 의해서 데이터 필드마다 200B의 8개의 데이터 필드는, SDNP 패킷이 1,600B의 데이터를 운반할 수 있다는 것을 의미한다.

[0453] 도 9g 및 도 9h 모두는, 클라이언트 디바이스가 구역(U1)에서 라스트 마일을 경유하여 게이트웨이 노드로 데이터 패킷을 송신하는 경우를 도시한다. 이어서, 게이트웨이 노드는 구역(U1) 보안 자격 증명을 이용하여 라스트 마일 보안 및 이용된 은폐 방법을 원상태로 돌리기 위해서 진입 데이터 패킷을 프로세스한다. 게이트웨이 노드는 이어서 혼합 프로세스(1184Z)에서 패킷의 콘텐츠를 다른 패킷의 콘텐츠와 혼합하여, 구역(Z1)의 보안 자격

증명을 이용하여 SDNP 클라우드를 통해서 전송하기 위한 새로운 패킷(또는 패킷들)을 생성할 수 있다.

[0454] SDNP 게이트웨이가 클라우드로부터 데이터 패킷을 수신하고 데이터 패킷을, 예를 들어 클라이언트의 전화(피통화자)에 대한 SDNP 클라우드로부터, 클라이언트 디바이스로 데이터 패킷을 송신할 때, 유사한 프로세스가 이용된다. 도 9i에 도시된 바와 같이, 이중-채널 또는 삼중-채널 통신 시그널링 서버(2603)는, 클라우드로부터 오는 데이터 패킷 및 그 상응 식별 마킹 및 보안 자격 증명의 계획된 도달에 대해서 SDNP 게이트웨이에 미리 통지하였다. 따라서, SDNP 게이트웨이가 SDNP 클라우드로부터 데이터 패킷(2438A)을 수신할 때, 게이트웨이는, 암호문으로부터의 SDNP 페이로드를 평문 텍스트 데이터 패킷(2438B)으로 변환하기 위해서, SDNP 클라우드 보안 동작(2190D)을 실시한다. 데이터 패킷(2438 A) 내의 미암호화 시드 및 키 데이터 필드는 무시될 수 있거나 선택적으로 암호문을 해독하기 위해서 시그널링 서버 정보와 함께 이용될 수 있다. 데이터 필드의 사용은 패킷의 페이로드 은폐에서 이용된 알고리즘에 의존한다. 예를 들어, 암호화가 이용되지 않는 경우에, 암호화 키를 포함하는 필드가 무시된다.

[0455] 결과적인 동작은 많은 수의 데이터 필드를 추출한다. 후속 동작은 콘텐츠-분할 동작(2184Z)에서 이러한 데이터 필드를 분할하여, 인식 동작(2191D)을 이용하여 데이터 필드 1 및 Hdr 1로 표시된 그 연관 데이터 필드 헤더(2117D)를 포함하는 특정 콘텐츠를 추출한다. 헤더(Hdr 1)는 데이터 필드의 목적지 어드레스, 데이터 유형, 긴급성, 및 전달 정보를 포함한다. 이어서, 추출된 데이터 필드는 그 다음 목적지로 전달하기 위해서 SDNP 패킷 준비 동작(1191Z)에 의해서 새로운 IP 또는 SDNP 데이터그램으로 재랩핑된다. 클라우드로 향하는 새로운 데이터 패킷은, SDNP 페이로드(2435Z)인, 새로운 패킷의 목적지(사람의 전화 번호에 상응하는 IP 어드레스) 및 데이터 콘텐츠를 포함하는, SDNP 헤더(2434Z)를 포함한다. 이어서, 클라우드에서 사용된 Z1 자격 증명이 아닌, 라스트 마일을 위한 U1 보안 자격 증명에 따라, 진출 패킷이 SDNP 라스트 마일 보안 동작(2190Z)에 의해서 프로세스된다.

[0456] 시그널링 서버를 이용할 수 없다면, 즉 단일-채널 통신에서, 미디어 노드는 이전에 전달된 지시를 디폴트 지시로서 이용하여 진입 데이터 패킷을 프로세스하여야 한다. 그러한 상황에서, 진입 데이터 패킷은 (미리 결정된 공유 비밀로서 이전에 전달된 SDNP 집 코드 또는 인증 코드와 같이) 송신기가 유효 SDNP 클라이언트라는 것을 확인하는데 필요한 기준에 대하여 체크된다. 패킷이 유효한 것으로 결정되면, 패킷은 디폴트 지시에 따라 프로세스된다. 그렇지 않은 경우에, 패킷은 폐기된다.

[0457] 전술한 방법은 예시적인 것이고 데이터 패킷의 프로세싱 및 라우팅을 특정 데이터 패킷 포맷으로 제한하기 위한 것은 아니다.

[0458] **<u>통신에서의 보안 및 프라이버시</u>**

[0459] 라스트 마일 통신에서의 중요 고려사항은, 보안 통신 및 프라이빗 통신 모두를 지원할 수 있는 네트워크의 능력이다. 비록 프라이버시 및 보안이 종종 연관되지만, 이들은 동일한 것이 아니다. 통신에서 사용되는 용어와 같은 보안은 "인식 가능한 형태로 데이터를 통신하기 위한 미인증 액세스를 방지하기 위한 통제"로 간주된다. 그러나, 보안은, 개인 또는 에이전시가 통신에 액세스 또는 모니터할 수 있는 권한을 갖는 경우는 포함하지 않는다.

[0460] 프라이버시는 "다른 사람에 의해서 관찰되거나 방해받지 않는 그리고 공공의 주의로부터 자유로운 상태 또는 조건"으로서 정의된다. 프라이버시의 법적 용어는 개인의 정보에 대한 액세스를 제어할 수 있는 개인의 권리로 정의된다.

[0461] 통신에서, 개인의 보이스 통화, 비디오, 텍스트, 이메일, 개인 메시징 등에서의 개인의 프라이버시 권리는 국가에 따라 크게 다르다. 통신에 대한 법적으로 유효한 액세스를 제공하기 위한, 적용 가능한 정부 규제를 따르는 역할이 후속 섹션에서 설명된다. 그 이외에, 이상적인 네트워크 및 통신 시스템은 통신의 해킹을 방지할 수 있어야 하고, 즉 절대적으로 보안되어야 하고, 모든 통신이 알 권리가 있는 사람들로 제한되도록 보장될 수 있어야 하고, 즉 프라이빗이 되어야 한다.

[0462] 네트워크의 프라이버시 및 보안 능력을 평가할 때, 네트워크의 라스트 마일 및 그 연결된 디바이스들은 주의 깊게 고려되어야 한다. 정보 액세스 특권을 구축하기 위해서 이용되는 보안 자격 증명에 따라, 라스트 마일 및 그 연결 디바이스는 네트워크의 보안 및 프라이버시를 빈번하게 결정하고, 즉 라스트 마일은 가장 약한 링크를 나타낸다. 통신 네트워크의 4개의 가능한 조합이 고려되어야 한다:

[0463] * 보안 및 프라이빗 네트워크. 개인의 관점으로부터, 이러한 경우는, 정보의 보안 및 개인을 위한 프라이버시 모두를 보장하는, 이상적인 네트워크 성능을 나타낸다. 이러한 극단적인 것에서, 진정한 보안 프라이빗 네트워

크는 임의의 개인, 정부, 에이전시 또는 회사가 의미 있는 통신을 도난 당할 수 없다는 것 그리고 개인의 거동, 행위, 그 접촉 및 동료, 그 개인 선호 사항 및 활동 등에 관한 프라이빗 데이터를 획득할 수 없다는 것을 의미한다. 비록 프라이버시 권리 주장이 이상적인 보안 프라이빗 네트워크를 비밀 통신에서 황금 표준으로서 간주하지만, 정부, 보안 기관, 및 회사는 통신에서의 절대 자율성을 문제가 있는 것으로 보고, 개인이 절대적인 보안성 및 면책성을 가지고 범죄 활동 및 테러에 관여할 수 있게 하는 것으로 본다.

[0464] * 프라이버시가 결여된 미보안 네트워크. 보안되지 않고 프라이버시 규정(예를 들어, 오늘날 인터넷 OTT 캐리어)을 가지지 않는 네트워크는 통신 채널을 이용하는 개인, 그룹, 클럽, 회사 또는 정부에 대한 상당한 위험을 나타낸다. 사이버-해커가 통화 및 데이터에 용이하게 액세스할 수 있기 때문에, 임의의 악의의 당사자는, 그들이 선택한 임의의 목적을 위해서, 이러한 정보를 이용할 수 있다. 실제 조커 및 스패머의 경우에, 미보안 통신 채널은 혼동을 유발하도록, 네트워크가 스팸으로 넘쳐나도록, 서비스 공격을 초기에 거부하도록, 그리고 해로운 악영향을 생성하도록 명령받을 수 있다. 이데올로기 신봉자, 정책적 활동가 및 종교 컬트의 경우에, 미보안 통신을 이용하여 민감한 정보를 유출시켜 정책 변화, 정부 관리의 불신, 폭동 자극, 또는 심지어 정부 전복을 유발할 수 있다(예로서 연대적으로 맹렬한 국가간 반향을 유발한 수십만 건의 민감한 정부 문서의 위키리크스 폭로와 같은, 역사 소설 영화 "The Fifth Estate" (DreamWorks ⓒ 2013) 참조). 조직화된 범죄 및 마피아와 연관된 것과 같은 경제적으로 동기 부여된 사이버-범죄의 경우에, 공격은 금전적 범죄, 예를 들어 절도, 펀드 전환, 사기, 신원 절도, 돈세탁, 강탈, 블랙메일, 및 다른 중범죄에 초점을 맞춘다. 마약 카르텔, 갱, 및 테러리스트와 같은 두려움 및 협박과 관련된 사람들의 경우에, 공격, 납치, 살인, 폭탄테러, 또는 테러 행위와 같은 폭력적 범죄를 계획하고 실시하기 위해서, 그 경쟁자, 적, 및 표적 피해자의 위치, 이동, 및 행동을 추적하기 위해서 미보안 통신을 모니터링할 수 있다. 마지막으로, 개인의 사이버-공격의 경우에, 미보안 통신을 이용하여, 사회보장번호, 여권, 은행 정보, 신용카드 정보, 의료 기록, 및 다른 개인 비밀 정보를 포함하는 개인의 프라이빗 정보를 포함하는 데이터베이스를 불법적으로 해킹할 수 있다.

[0465] * 프라이버시가 결여된 보안 네트워크. 프라이버시가 결여된 보안 네트워크의 예는 일반적으로, 부적절한 또는 불법적인 통신이 회사의 네트워크에 걸쳐 발생되지 않도록 보장하기 위해서 IT(정보 기술) 관리자 또는 보안 부서가 모든 회사 통신을 모니터링하기 위한 권리 및 권한을 가지는, 회사 계정를 포함한다. 네트워크가 해커 및 사이버-범죄로부터 안전하더라도, 그러한 네트워크 상의 통신은 프라이빗한 것이 아니고, 회사 통신 기반시설의 미승인된 개인적 이용, 회사 간첩행위, 비밀보장 합의 위반, 지적 재산의 미승인 공개(IP 누설), 성희롱, 공정 공개 규정의 위반(등록된 FD), 내부자 거래, FCPA(해외부정지불 방지법)의 위반, 수뢰, 뇌물 수수, 사기, 재정 보고 위반, 보안성 위반, 및 기타를 포함하는 잘못된 행위를 검출하기 위해서 승인된 에이전트에 의해서 모니터링될 수 있다. 회사 통신에서, 개인의 회사 통신이 프라이빗하지 않다는 것 그리고 회사 전화 통화, 이메일, 텍스트, 개인 메시징 및 SMS, 및 다른 코뮤니케를 포함하여 모니터링될 수 있다는 것을, 입사시에 개인이 통지 받는다. 법원 선례의 경우에, 시민 또는 범죄자이든 간에, 개인 정보가 회사 정보와 혼합된 경우에도, 이들의 코뮤니케가 또한 법원에서 소환될 수 있고 증거로 제출될 수 있다. 본질적으로 회사의 피고용인이 회사 통신, 디바이스, 및 네트워크를 개인 용도를 위해서 이용하는 경우에, (대리인-클라이언트 특권의 경우를 제외하고), 모든 정보는 공정한 것이 되고 프라이빗한 것으로 간주되지 않아야 한다. 이러한 그리고 다른 이유로, 비지니스 및 개인 용도를 위해서 라인 및 카카오톡과 같은 개인 메신저를 혼합 이용하는 것이 특히 문제가 되는데, 이는 피고용인은 그들의 텍스트 채팅, 사진, 및 파일에 관한 검사를 방지할 수 있는 프라이버시 권리를 주장할 수 없기 때문이다.

[0466] * 준-프라이빗, 미보안 네트워크. 준-프라이빗 미보안 네트워크는, 데이터를 수반하는 네트워크가 해킹되나, 예를 들어 와이어 탭핑되나, 보안 제공된 특정 조건의 결여가 충족됨에도 불구하고 프라이빗한 거래가 비밀로 실시될 수 있는 것이다. 이러한 방식에서, 심지어 통화를 가로챈 해커에 의해서도 노출될 수 없는, 공유 비밀을 이용하는 다양한 수단에 의해서, 통화자(또는 통화자들)의 신원을 확인하는 것에 의해서 프라이버시가 구축된다. 프라이빗 미보안 통신의 일반적인 예는 보이스 은행 거래이다. 통화자는, 사기꾼이 답을 알기 어려울 수 있는 일련의 계속 변화되는 질문, 예를 들어 "당신이 지난 밤에 저녁을 먹고 당사의 신용카드로 지불한 것을 알고 있습니다. 어떤 도시에서 저녁 식사를 하였는지 알려 주실 수 있나요" 또는 "당신은 와인 양조장으로부터 규칙적인 청구서를 받고 있습니다. 어떤 와인 양조장입니까"에 답변하는 것에 의해서 그 신원을 확인한다. 다른 예시적인 질문은 "당신이 좋아하는 초등학교 선생님의 성을 말해주실 수 있나요?"이다. 작업을 위한 이러한 신원 확인 방법에서, 은행은 (신용카드 진술서와 같은) 비-공개 정보에 대한 액세스를 가지거나 은행 및 그 클라이언트는, 일반적으로 전자적이 아니고 직접 만나서 계정을 처음 만들 때, 공유 비밀의 세트를 구축하여야 한다. 통화자가 확인된 신원의 경우에, 클라이언트는 사이버범죄에 유리하지 않을 수 있는 특정 행동을 실시하도록 기관에 지시할 수 있다. 예를 들어, "내 저금으로부터 $10,000을 내 당좌예금계좌로 이동시키세요." 그러

나, 돈의 이체가 다른 은행으로 전달되는 경우에, 클라이언트의 프라이버시를 보장하기 위해서 보다 더 엄격한 인증이 이루어져야 한다. 어떠한 경우에도, 프라이버시는, 통신이 전자적으로 또는 청각적으로 공유 비밀을 노출시킬 수 없는 조건의 충족에 의존하고, 그렇지 않은 경우에 모든 프라이버시를 잃게되고 계정이 위험할 수 있다. 따라서, 미보안 라인 상의 그러한 인증된 통신은, 조건부 프라이버시를 의미하는 준-프라이빗으로 지칭된다. 클라이언트 만이 소유하는 은행이 발행한 디바이스인, 보안 토큰의 이용에 의해서, 미보안 네트워크를 통한 다른 예 또는 준-프라이빗 통신이 실시될 수 있다. 번호가 은행의 인증된 번호와 일치되는지를 확인하는 은행 운영자에게, 디바이스에 의해서 생성된 의사-난수를 말한다. 그러한 숫자가 8개 이상의 숫자이기 때문에, 올바른 코드를 처음에 추측할 수 있는 가능성은 아주 작다. 잘못된 토큰 숫자가 기록된 경우에, 통화가 종료되고, 계정은 동결되며, 사기 담당 부서에 조사하도록 경고된다. 임의의 그러한 경우에, 미보안 네트워크에 걸친 프라이버시를 보장하는 것의 중요성은, 계정 번호, PIN, 신용카드 정보, 등과 같은 임의의 비밀 상세 내용을 구두로 노출시키지 않고 통화할 수 있는 것에 의존하고, 즉 통신은 단지 준-프라이빗이다.

[0467] ***신원 확인 및 AAA*** - 보안 및 프라이버시의 개념은 정확하고 신뢰 가능한 신원 확인, 즉 대화하는 통화자가 누구인지에 의존한다.

[0468] "인증"이라고도 알려져 있는 신원 확인은, 데이터 및 통신의 이용을 유효하게 하는데 있어서 그리고 불법적 또는 미승인 액세스를 방지하는데 있어서 중요하다. 신뢰 가능한 신원 확인은 국가 보안, 법 집행, IP 소유, 비지니스 기업, 및 개인 권리에서 중요하다. 신원 확인의 중요성의 예가 이하를 포함한다:

[0469] * 나라의 국가 보안을 위해서, 범죄자, 스파이, 테러리스트, 마약 밀매상, 및 국가 비밀을 폭로하거나 국가 안보를 위협하는 임의의 사람을 추적하는데 있어서, 통화자 신원 확인은 중요하다. 기밀, 비밀, 또는 탑 시크릿 코뮤니케, 데이터 및 파일의 액세스, 판독, 또는 송신에 대해서 인증된 개인을 식별할 수 있는 것이 마찬가지로 중요하다.

[0470] * 법 집행을 위해서, 통화자 식별 확인은, 절도, 방화, 마약 밀매, 밀수, 매춘 및 인신 매매, 강탈, 블랙메일, 및 다른 중범죄와 같은 범죄 활동에 관련된 개인 또는 기관을 식별하는데 있어서 중요하다. 경찰, 소방관, 구급 의료대원, 공원 보안관, 항공 보안요원, TSA 및 공항 보안요원, 항만 당국, 세관, 및 해안 경비 서비스를 포함하는 인증된 법 집행 에이전트인 개인들을 식별할 수 있는 것이 마찬가지로 중요하다.

[0471] * 영화 스튜디오와 같은 IP 소유자의 경우에, 음악, 영화, 책, 비디오 등과 같은 저작권 대상의 무단 배포 및 프라이버시와 관련된 개인, 기관, 및 단체를 식별하는데 있어서 신원 식별이 중요하다. 이는 IP 및 저작권 대상의 유효하고 적법한 배포를 확인하는데 있어서 마찬가지로 중요하다.

[0472] * 비지니스 기업을 위해서, 그 피고용인의 신원 확인은, 비공개 중요 정보의 의도적 또는 우발적 누출을 추적하는데 있어서, 상업적 간첩활동과 관련된 사람을 식별하는데 있어서, 지적 재산의 불법적 공개에 관련된 개인을 식별하는데 있어서, 그리고 회사 통신의 사기적 또는 개인적 이용과 같은 다른 범죄를 저지른 사람을 식별하는데 있어서 중요하다. 이는, 회사 기밀 정보를 이용할 수 있는 사람의 신원을 확인하는데 있어서, 그리고 특히 그들이 액세스할 수 있는 데이터의 특정 유형을 인증하는데 있어서 중요하다. 예를 들어, 마켓팅 직원이 얼마나 많이 받는지를 비교하기 위해서 회사의 엔지니어링 부서가 마켓팅 부서의 개인적인 기록에 액세스할 수 없어야 한다.

[0473] * 개인의 경우에, 통화하는 사람 또는 사람들이 사기꾼이 아니라는 것을 확인함으로써 통화자의 "프라이버시"를 보장하는데 있어서 신원 확인이 중요하다.

[0474] 그에 따라, 신원 확인의 역할은 개인의 신원을 확인하기 위한, 즉 요구하는 사람인지 인증하기 위한, 그리고 그 신원을 허위진술하는 사람을 식별하고, 차단하고, 최종적으로 체포하기 위한 것이다. 인증은 삼중-A 보안 모델의 제1 "A"이거나, AAA는 "승인, 인증, 및 관리"를 나타낸다. PIN 코드, 암호, 지문, 토큰, 및 질의 응답 방법과 같은 많은 방법이 개인의 신원을 확인하기 위해서 그리고 그들이 시스템에서 계정을 가지는지를 인증하기 위해서 사용된다.

[0475] 일단 인증되면, 유효 사용자의 신원을 이용하여, 코뮤니케, 데이터, 파일, 시스템 운영 등에 대한 액세스 권리 및 특권을 결정한다. 이러한 특권 및 액세스 권리는 시스템에 의해서 허여된 바와 같은 사용자의 "인증"로서 통칭되고, 즉 인증된 사용자는 그들에게 인증된 통신, 데이터, 파일 및 시스템 특징에만 액세스할 수 있다. 그에 따라, 인증은 "특권" 또는 "액세스"와 동의어이다.

[0476] AAA에서의 제3의 "A"는 관리를 나타낸다. 관리는, 예를 들어 사용량 기반 과금 청구 관리를 위해서, 그리고 네트워크, 파일, 및 시스템 운영에 대한 미인증 액세스 시도를 모니터링 및 기록하기 위해서, 네트워크 및 파일에

대한 인증된 액세스를 기록하는 부기행위이다. 관리는 또한 인증 동작에 필요한 보안 자격 증명, PIN, 암호 등의 변화를 추적하는데 있어서 중요하다.

[0477] AAA 과정을 실시할 수 있는 네트워크의 능력은 프라이버시를 보장하는 것보다 그리고 미인증 사용자 또는 네트워크 운영자로부터의 네트워크의 부정 사용의 방지보다 최우선한다. 사용자의 신원을 보장할 수 없는 임의의 네트워크는 불법적인 목적을 위해서 부정사용될 수 있다. 미인증 사용자에 의한 네트워크 부정사용은 OTT 통신에서 불가피한 문제인데, 이는 통화자 신원을 입증하기 위한 수단이 없기 때문이다. 미식별 사용자, 즉 익명자에 의한 미인증 액세스 및 네트워크 통신은 현대의 통신에서 상당한 위험이 된다.

[0478] ***익명성(Anonymity)*** - 통신에서의 익명성 원칙은 추적 가능성이 없이 통신하기 위해서 통화자의 신원을 의도적으로 은폐하는 행위이다. 익명 통신의 거의 상징적인 예는 페이폰이다. 페이폰 통화에서, 지불은 추적될 수 없는 현금에 의해서 이루어지고, 페이폰 번호는 공공적이고, 누구나 그러한 전화를 사용할 수 있고, 이는 통화자의 신원이 알려지지 않고 통화자가 누구인지를 결정할 수 있는 특정 수단이 없다는 것을 의미한다. 전화 번호가 나열되지 않기 때문에, 개인이 번호를 소유하지 않고 (정교한 음성 인식 소프트웨어를 통하는 경우를 제외하고) 통화자의 신원을 식별할 수 있는 방법이 없다. 휴대폰과 같은 등록된 디바이스의 경우에, 디바이스의 소유자의 신원이 전화 번호를 통해서 추적될 수 있으나, 통화자의 신원은 여전히 알려지지 않고 유지될 수 있다. 예를 들어, 전화가 절도된 것일 수 있거나, 통화자의 진정한 신원을 감추기 위해서 사용량 기반 과금 SIM 카드가 이용될 수 있다. 대안적으로, 노트북, 태블릿, 또는 휴대폰이 공공 카페 내의 WiFi를 통해서 연결되어, 임의의 공공 페이폰 또는 전화 부스와 유사한 익명성을 제공할 수 있다.

[0479] 일부 OTT 캐리어는, 가입자의 신원 확인 없이, 페이폰과 같은 VoIP 전화 서비스를 운영하도록 선택되었다. 예를 들어, 온라인보고서(http://money.cnn.com/2015/11 /17/technology/isis-telegram/)에서, CNN Money는 "텔레그램이라는 앱이 지하디스트 중에 인기 있는 새로운 것이다"라고 발표했다. 연구에 따르면, 텔레그램 애플리케이션은 파리 공격을 위한 비밀스러운 계획을 세우는 ISIS 테러리스트의 도구였다. 그러한 기사에서, "텔레그램 개발자는, Isis가 파리 공격 전에 통신을 위해서 그러한 앱을 이용하였다는 것을 알고 있었다" (http://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-knew-isis-communicate-paris-pavel-durov-a6742126.html),

[0480] 텔레그램 개발자 Pavel Durov는: '프라이버시를 위한 권리는 테러리즘과 같은 나쁜 것이 발생될 것에 대한 우리의 두려움보다 중요하다'고 하였다.

[0481] 언론에서 보고된 범죄에 이용된 프라이버시 및 익명성의 다른 예는 BitTorrent - 저작권 대상을 불법적으로 다운로드하고 공유하기 위해서 종종 이용되는 애플리케이션 및 데이터 네트워크 -의 예이다. "50,000명의 BitTorrent 사용자는 불법적인 다운로드에 대한 혐의로 제소되었다"라는 제목의 CNN Money Tech의 뉴스(http://money.cnn.com/2011/06/10/technology/bittorrent_lawsuits/)에서, 사용자는, "The Hurt Locker"라는 영화 및 다른 저작물을 불법적으로 다운로드 한 것에 대해서 새로운 반-프라이버시법에 의해 고소된 것으로 보고되었다. 네트워크 운영자 BitTorrent는, 개인 활동을 위해서 그 네트워크를 이용하는 사람들에 대해서 책임이 없다는 페이폰 포지션을 취하였다. 자유 발언 옹호자는 이러한 포지션을 지지하는 한편, 법 집행부 및 정부, 국가 보안, 및 IP 권리 옹호자는 이러한 태도를 무분별하고 무책임한 것으로 혐오한다. 해당 정책과 관계없이, 통신 시스템이 통화자 확인 실시를 할 수 없는 한, 익명 통화 중단에 관한 논의는 순전히 학술적이다.

[0482] 통화자 확인 및 인증은, 지적 재산, 엔지니어링 개발, 제품 평가, 제조 노하우, 기밀 재정 보고서 및 프로젝션, 비지니스 상황, 판매 예측, 재고 및 WIP, 품질 조사, 비지니스 및 IP 계약, 고객 목록, 피고용인 기록, 및 다른 거래 비밀을 포함하는 회사 기밀 데이터에 대한 액세스를 제어하는데 있어서, 회사 및 비지니스 기업에 있어서 특히 중요하다. 회사 통신에 액세스할 때, 임의의 피고용인, 계약자, 또는 담당관에게 허여된 액세스 특권은 그 신원 확인에 따라 달라진다. 투자자 통화를 포함하는 컨퍼런스 콜에서, 통화에 누가 참여하는지를 확인하는데 있어서 그리고 알 필요가 없는 사람이 청취하지 않도록 보장하는데 있어서, 신원 확인은 중요하다.

[0483] 역설적으로, 범죄 방지 및 회사 간첩행위를 저지하기 위해서 통화자 인증이 사용되는 반면, 동일한 사용자 인증은 통화자의 프라이버시를 보장하는데 있어서 유리하게 유용한다. 통화 또는 텍스트 채팅에서의 양 당사자가 소정의 서명된 인증 과정을 통해서 그 신원을 확인하는 경우에, 사기꾼은 통화 또는 그 데이터에 액세스하지 못하고, 그에 따라 통화는 범죄 공격으로부터 보호된다.

[0484] 마지막으로, 익명 통화자를 익명 통화로부터 구별하기 위한 구분이 이루어져야 한다. 익명 통화자는, 통신하는 네트워크로부터 그 진정한 신원을 위장하는 사람이다. 그러나, 익명 통화는, 통화자가 네트워크로부터 익명성을

가질 것을 요구하지 않고, 통신 중에 통화 데이터 패킷에서 그 진정한 신원을 혼란시킬 것만을 요구한다. SDNP 네트워크 상의 등록된 계정 보유자는, 이러한 개시 내용에 따라, 네트워크가 그 신원 및 전화 번호를 알고 있는 경우에도, 익명 데이터를 이용하여, 통화를 위치시킬 수 있거나 데이터를 송신할 수 있다. 이러한 방식으로, 법-준수 시민은, 그 신원을 SDNP 네트워크 운영자에게 은폐할 필요가 없이, 익명을 통신할 수 있다. 통화자가 일반 프라이빗 통화, 엔터테인먼트, 또는 비지니스에 관련되는 경우에, 네트워크는 SDNP 명칭 서버 데이터베이스 내에 저장된 바와 같은 그 신원을 알더라도, 그들의 SDNP 통화는 프라이빗 및 보안을 유지한다.

[0485] 법적인 익명 통신을 위한 필요성의 예는, 게이머의 신원, 특히 어린이의 신원을 보호하는 것이 중요한 세계적인 게이밍을 포함한다. 익명성이 유리할 수 있는 다른 경우는, 운전을 악화시키는 다른 운전자의 개인 데이터를 식별하는 것에 의해서, 난폭 운전을 하는 운전자를 가혹한 보복으로부터 보호하기 위한 차량-대-차량(V2V) 통신이다. 대조적으로, 통화자가 통신에서 범죄 또는 다른 흉악한 행동과 관련되는 경우에, 법 공무원이 (적용 가능한 법에 따라) 그 통화 및 데이터 전송에 액세스할 수 있다. 이러한 방식으로, 법을 지키는 시민의 신원을 노출시키지 않거나 통화를 공개하지 않고도, 네트워크 운영자는 법원 명령 및 소환의 요건을 만족시킬 수 있다.

[0486] 요약하면, 개시된 SDNP 통신 방법을 이용하면, 식별 가능한 SDNP 가입자만이 익명 통화를 위치시킬 수 있다. 미식별 통화자는 SDNP 네트워크에 대한 액세스 또는 익명 통화를 위치시킬 수 있는 능력을 가지지 않는다.

[0487] ***국가 보안 및 프라이버시*** - 보안 및 프라이빗 통신의 특성은, 정부의 역할 및 법이 고려될 때 더 혼동된다. 모든 국가는 그 국경 내의 통신을 제어하기 위해서 그들의 주권을 주장한다. 그러나, 인터넷 및 동적으로 라우팅되는 패킷 교환형 데이터 네트워크의 출현으로, 네트워크 감시 및 모니터링이 많은 기술적 및 법률적 난제에 직면한다. 하나의 관심사는 트래픽을 "통한" 서버-대-서버 네트워크 - 중단 없는 국가를 통과하는 데이터 패킷 - 를 모니터링하는 것이다. 인터넷 트래픽이 동적으로 라우팅되기 때문에, 네트워크 운영은 어떠한 데이터 패킷을 그 서버의 네트워크가 운반하는지에 대해서는 관심이 없다. 물론, 모든 국가가 이러한 대용의 큰 데이터를 가로채고 디코딩할 수 있지만, 암호화로 인해서, 암호화 키를 알지 못한 액세스는 특히 실시간 모니터링에 있어서 어렵다. 그리고 통화자가 국가 내에 체류하지 않을 수 있기 때문에, 특정 국가는 통화를 위치시키기 위해서 이용되는 암호화 키를 소환하거나 요구할 수 있는 관할권이 없다. 그러한 네트워크 통과-데이터는 지구 대기를 횡단하는 라디오 파동 트래픽과 유사하다. 라디오 파동이 위를 통과하더라도, 이들을 중단시킬 실질적인 방법이 없다. 유사하게, 국가의 기반시설을 인터넷으로부터 완전히 격리시키는 것을 제외하고, 네트워크 통과-데이터 트래픽을 중단시킬 실질적인 방법이 없다.

[0488] 통신을 통제하기 위한 보다 실용적인 해결책은 라스트 마일 통신에 대한 모니터링에 집중하는 것이고, 즉 통화의 소스 및/또는 목적지가 국가의 국경 내에서 발생되는 경우에 통화 및 통화 데이터를 가로채고 모니터링하는 것이다. 이러한 접근방식은, (i) 데이터의 크기가 더 작아진다는 것, 즉 분석을 위해서 보다 관리 가능하다는 것, (ii) 라스트 마일 통신 캐리어 또는 네트워크 운영자가 그 체류 국가의 법의 적용을 받는다는 것, (iii) 라스트 마일 캐리어 또는 네트워크 운영자가 임의의 이용 가능한 암호화 키의 제공을 위해서 소환될 수 있다는 것, (iv) 라스트 마일 네트워크에 연결하기 위해서 통화자의 디바이스 자체가 전자적으로 "등록"되어야 한다는 것 그리고 그렇게 함으로써 통화자에 대한 정보를 넘긴다는 것, 그리고 (v) 임의의 네트워크 연결 디바이스의 위치가 네트워크 어드레스, GPS 데이터, 또는 라디오 신호 삼각측량을 이용하여 결정될 수 있다는 것을 포함하는, 대량의 통과-데이터 트래픽보다 우수한 몇몇 장점을 갖는다.

[0489] 네트워크 통과-데이터 규정을 강화하는 것과 관련된 법적 및 기술적 난제와 달리, 라스트 마일 통신 및 통화 종료를 통제하는 법은 전체적으로 라스트 마일 네트워크 운영자가 체류하는 국가의 권리이다. 국가의 프라이버시 법에 따라서, 이하의 조합을 포함하여, 라스트 마일 통신에서 요구하는 액세스의 레벨을 국가의 통제가 강요할 수 있다:

[0490] * 문제 원인을 기초로 하는 법원의 소환장이 없이는 어떠한 데이터 또는 통화도 모니터링할 수 있는 권리가 없는 것. 법원 명령으로, 임의의 통화 또는 데이터 통신을 비밀스럽게 모니터링할 수 있는 권리.

[0491] * 법원 명령이 없이, 모든 통화의 메타데이터를 모니터링할 수 있는 권리.

[0492] * 법원 명령이 없이, 모든 통화 및 데이터 통신을 모니터링할 수 있는 권리.

[0493] * 임의의 그리고 모든 통신을 가로채고, 모니터링하고, 필요에 따라 차단할 수 있는 권리.

[0494] 예를 들어, 미국과 같은 다양한 정부는, 법원 명령이 없이도 통화의 "메타데이터"를 모니터링할 수 있는 권리를 보유하는 포지션을 취하였다. 메타데이터는, 통화 데이터 자체에 실제로 액세스하지 않고, 누가 누구와 통화하는지, 얼마나 오래 통화하였는지, 통화 시에 통화자가 위치한 곳 등과 관련된 데이터 패킷 정보를 포함한다. 본

질적으로, 메타데이터는 IP 패킷의 데이터 헤더를 포함하나, 그 페이로드는 포함하지 않는다. 대조적으로, 통화 및 데이터 통신의 모니터링은, 헤더 데이터뿐만 아니라, 페이로드 자체에 대한 액세스를 포함한다. 페이로드가 암호화될 수 있는 그러한 경우에, 정부는, 마스터 암호화 키(존재하는 경우)를 제공할 것을 네트워크 운영자에게 주장할 수 있다. 프라이버시 옹호자에 의해서 제기되는 하나의 문제는 정부의 권력 남용이다. 구체적으로, 네트워크가 하나의 세트의 마스터 암호화 키에 의존하는 경우에, 특정 개인의 정부 감시를 가능하게 하기 위한 법원의 명령에 응답하여 이러한 키를 포기하는 것은, 비록 법원 명령은 개인 또는 그룹으로 제한되었지만, 정부가 모든 통화를 모니터링할 수 있게 한다. 이러한 문제는 "누가 경찰을 위한 경찰이 되어야 하는가?"에 대한 질문으로 종종 언급된다. 다른 고려사항은 국제 통화를 위치시키는 개인의 프라이버시 권리에 관한 것이다. 그러한 경우에, 통화자는, 정부 액세스를 위한 관련 법이 양 통화자의 위치, 즉 2개의 라스트 마일 네트워크들이 발생되는 위치에 따라 달라진다는 것을 알아야 한다. 미국으로부터 중국으로의 통화는 미국 내의 통화자에 대해서 미국법이 적용될 것이고 중국 내의 다른 통화자는 중국법이 적용될 것이다. 그러한 상황에서, 하나의 정부에 의한 통화 액세스는 다른 경우보다 클 수 있다. 따라서, 더 큰 프라이버시 권리를 갖는 국가 내의 통화자는 다른 국가의 정부에 의해서 위반되는 그들의 프라이버시를 고려할 수 있으나, 법률적 기반을 가지지 않는 국가와 통화하기 때문에 불만을 제기하지 못한다.

[0495] 이전에 개시된 보안 동적 통화 네트워크 및 프로토콜을 이용하는 통신의 경우에, SDNP 네트워크에 걸쳐 익명으로 전송된 단편화되고 스크램블링되고 동적으로 암호화된 데이터 패킷의 하이퍼보안 클라우드 통신에서 통과-데이터를 가로채는 것은 사실상 불가능하다. 따라서, 하이퍼보안 통화의 프라이버시 및 보안은 디바이스 및 라스트 마일 통신에 의해서 결정된다. 개시된 SDNP 방법을 라스트 마일 통신에 적응시킴으로써, 하이퍼보안 통신 및 큰-무결성의 프라이버시가 가능한 라스트 마일이 본원에서 개시된 바와 같이 실현될 수 있다.

[0496] 또한, 각각의 국가에 대한 라스트 마일 통신을 통제하는 지역적인 법을 수용하기 위해서 SDNP 네트워크의 보안 및 프라이버시 설정을 조정하는 메커니즘이 개시된다. 이러한 방법은, 통화 데이터를 해커 및 사이버-범죄에 노출시키지 않고, 인증된 보안 당국이 법 및 법원 처분에 따라 통신을 모니터링할 수 있게 하는 안전수단을 포함한다. 따라서, 본원에서 개시된 하이퍼보안 라스트 마일 통신에서, 사이버-공격에 취약한 "백 도어"의 이용은 활용되지 않는다.

[0497] **<u>하이퍼보안 라스트 마일 통신 방법 및 장치</u>**

[0498] 엔드-투-엔드 하이퍼보안을 보장하기 위해서, SDNP 클라우드 내의 암호화되고 스크램블링된 익명의 단편화된 데이터 패킷 라우팅을 위한 이전에 개시된 방법의 적용이 라스트 마일 내의 통신을 위해서 유사하게 구성되어야 한다. 라스트 마일 통신을 보장하는 것이 특히 문제가 되는데, 이는 데이터가, SDNP 운영자에 의해서 호스팅되지 않은 네트워크 상에서 운반될 수 있고, 패킷 라우팅이 통상적인 IP 패킷 라우팅을 포함할 수 있고, 라스트 마일 네트워크의 고유의 보안이, 가능하게는 라스트 마일 네트워크 운영자의 공모로, 사이버 범죄에 의해서 알지 못하게 손상될 수 있기 때문이다.

[0499] 본 발명에 따라, 라스트 마일 통신은 필수적으로, SDNP 클라우드 내의 데이터 패킷과 상이한 패킷 포맷을 이용하는 데이터 클라우드 네트워크 외부의 IP 데이터그램의 전송을 포함한다. 도 10에 도시된 바와 같이, (소프트-스위치 인에이블드 SDNP 노드($M_{0,0}$ 내지 $M_{0,f}$)에 의해서 개략적으로 표시된) 서버(1201)를 포함하는 SDNP 클라우드가 예시적인 데이터 패킷(1222B, 1222C, 및 1222F)에서 도시된 SDNP 데이터그램을 이용하여 VoIP, 비디오, 텍스트, 및 데이터를 전송한다. SDNP 데이터그램은 SDNP 계층 3 소스 및 목적지 어드레스를 포함하고, 인터넷 IP 어드레스는 포함하지 않는다. SDNP 어드레스는, 이들이 SDNP 명칭 서버 또는 SDNP 명칭 서버의 기능을 실시하는 다른 서버에 의해서만 인식될 수 있고, 인터넷의 DNS 명칭 서버에 의해서는 인식될 수 없다는 점에서, IP 어드레스와 상이하다.

[0500] 전술한 미국 출원 제14/803,869호에서 설명된 바와 같이, SDNP 패킷은, 네트워크를 통해서 이동될 때, 동적으로 변화되며, 공유된 비밀 및 (시간과 같은) 동적 "상태"에 따라 라우팅 어드레스가 업데이트되고 페이로드의 지속적 변화가 실시된다. 예를 들어, 노드($M_{0,0}$)에 의해서 송신된 데이터 패킷(1222B)은, 특이적 SDNP 어드레스 및 특이적인 암호화된 페이로드를 갖는, 계층 3 SDNP 데이터그램(B)을 포함한다. 다운스트림, 노드($M_{0,1}$)로부터 출력된 데이터 패킷(1222C)은 상이한 SDNP 어드레스 및 재암호화된 페이로드를 갖는 계층 3 SDNP 데이터그램(C)을 포함한다. 몇십 밀리초 후에, 동일 페이로드는, 데이터를 프로세스하고 IP 데이터그램(G)을 포함하는 데이터 패킷(1223G)을 라스트 마일을 통해서 포워딩하는 노드($M_{0,f}$)에 도달한다.

[0501] 규정된 상태에 따라 변화가 실시되기 때문에, 실시되었던 것과 반대 순서로 실행되는 일련의 역기능 동작을 실

시함으로써, 원래의 패킷 데이터가 복원될 수 있다. 예를 들어, 스크램블링, 정크 삽입(기만), 및 암호화 단계를 포함하는 SDNP 기능적 시퀀스는, 상응 역기능을 실시하기 위해서 기능을 실행을 위해 이용된 동일 상태가 실시된다면, 반대 시퀀스 해독, 정크 제거, 및 언스크램블링에 의해서 원상태로 되돌아 갈 수 있다. 패킷을 위한 상태 데이터는, 패킷의 페이로드 내에 임베딩되어 시간, 시드, 또는 키로서 수반될 수 있거나, 패킷에 미리 송신될 수 있다. SDNP 클라우드 내의 데이터 전송 및 프로세싱은 SDNP 클라우드 특정 공유 비밀 및 보안 자격 증명을 이용하여 동작된다. 공유 비밀 및 보안 자격 증명의 공통 세트를 공유하는 미디어 노드가 보안 "구역"으로 지칭될 수 있다. SDNP 클라우드 내에서 동작되는 보안 자격 증명을 위해서 사용된 구역은 SDNP 클라우드 외부의 임의의 사용자 통신에 노출될 수 없다. 따라서, 모든 라스트 마일 통신은, SDNP 클라우드와 상이한 SDNP 보안 구역을 포함하여야 한다.

[0502] 도시된 예에서, 상응 노드($M_{0,0}$ 내지 $M_{0,f}$)를 호스팅하는 서버(1201A) 및 서버(1201F)는 SDNP 게이트웨이로서 동작하고, 즉 이들은 SDNP 클라우드 외부의 디바이스뿐만 아니라 다른 클라우드내 SDNP 노드와 통신한다.

[0503] 이러한 게이트웨이로부터 클라우드 외부의 통신 디바이스로의 통신은 "라스트 마일" 통신을 나타낸다. 따라서, 게이트웨이 노드는, 이들이 연결되는, SDNP 클라우드 및 라스트 마일 네트워크 모두의 구역 보안 자격 증명을 이해하여야 하고, 패킷 라우팅 중에 트랜스레이터로서 작용한다. 의미론적으로, 라스트 마일이라는 용어는, SDNP 클라우드 외측의 통신을 의미하는 추상적인 개념이고, 1 마일의 거리를 특정적으로 지칭하지 않는다. 그 대신, 라스트 마일이라는 용어는, 클라이언트 디바이스가 SDNP 클라이언트로서 동작하는지의 여부와 관계없이, 임의의 거리의 클라이언트 디바이스와 SDNP 클라우드 사이의 임의의 통신을 포함하고, 다시 말해서 SDNP 애플리케이션 소프트웨어 또는 펌웨어를 작동하거나 그렇지 않다.

[0504] 라스트 마일이라는 용어는 또한 통화를 개시하는 클라이언트 디바이스 및 통화되는 클라이언트 디바이스 모두에 적용된다. 문헌적으로 말하면, 통화자의 데이터가, 라스트 대신, 통화의 "제1 마일"을 나타낸다 - 제1 마일과 라스트 마일 사이의 구분은 임의적이다. 구체적으로, 임의의 듀플렉스 변환에서 또는 임의의 IP 통신 "세션"에서, 통화를 수신하는 디바이스는 통화자에 대한 응답을 송신함으로써 콜 또는 세션 요청에 필수적으로 응답한다. 임의의 2-방향 통신에서, 제1 마일 연결은 그에 따라 응답 데이터 통로에서 라스트 마일로서 반드시 기능한다. 본질적으로, 통화자를 위한 제1 마일은 동시에 응답자를 위한 라스트 마일이다. 따라서, 라스트 마일이라는 정의된 용어는 본원 전체에서, 어떠한 디바이스가 통화 또는 통신 세션을 개시하였는지와 관계없이, 제1 마일 및 라스트 마일 모두를 의미하기 위해서 사용된다.

[0505] SDNP 클라이언트 이외의 임의의 디바이스에 대한 SDNP 클라우드 외부의 통신은 필수적으로 IP 데이터그램을 이용하여 이루어지고, SDNP IP 데이터그램에 의해서 이루어지지 않는다. 예를 들어, 도 10을 다시 참조하면, 데이터 패킷(1223A)은, SDNP 어드레스가 아니라, IP 어드레스를 갖는 SDNP 페이로드를 이용하여 구성된 "IP 데이터그램(A)"를 포함한다. 유사하게, IP 데이터그램(G)은 IP 어드레스를 이용하여 라우팅된 SDNP 페이로드를 포함하는 데이터 패킷(1223G)을 포함한다. IP 소스 및 목적지 어드레스는, 라우팅이 이루어지는 네트워크에 의해서 인식될 수 있는 임의의 IPv4 또는 IPv6 어드레스를 나타낸다. IP 어드레스는 인터넷의 DNS 서버에 의해서 인식될 수 있는 인터넷 어드레스를 포함할 수 있거나, 대안적으로 로컬 네트워크 서비스 제공자에 의해서 형성된 로컬 네트워크에 걸친 라우팅을 위해서 사용되는 NAT 어드레스를 포함할 수 있다.

[0506] 라스트 마일 통신에서 이용되는 하드웨어 및 펌웨어가 상당히 달라질 수 있고 전화 라인, 섬유 통신, 케이블 TV 네트워크, 3G 및 4G 무선 네트워크, 마이크로파 통신 타워, 및 위성을 포함할 수 있기 때문에, 라스트 마일 통신의 분석은, 이용된 다양한 계층 1 물리적 네트워크 및 그 상응 계층 2 데이터 링크 포맷을 위해서 고려되어야 한다. 포맷은, 예를 들어, 아날로그(POTS), 이더넷, WiFi, 3G, 4G/LTE, 및 DOCSIS3을 포함할 수 있다. 각각의 라스트 마일 구현예의 상응 보안 및 프라이버시 능력은 SDNP "콜 아웃" 통신에 관한 이하의 섹션에서 케이스별로 고려된다.

[0507] ***미보안 라인을 통한 SDNP 콜 아웃(SDNP Call Out Over Unsecured Lines)*** - 당업계의 용어로서, 분리된 (그리고 일반적으로 상이한) 네트워크에 걸쳐 전송되는 규정 네트워크를 떠나는 임의의 통화가 일반적으로 "콜 아웃"으로 지칭되고, 이는 데이터 또는 보이스가, 다른 네트워크로 전송되도록 하나의 네트워크를 떠난다는 것을 의미한다. 예를 들어, 스카이프 애플리케이션이 작동되는 클라이언트들 사이의 통신이 일반적으로 스카이프 통화로서 지칭되나, 스카이프 클라이언트로부터 정규의 또는 휴대폰 번호로 통화를 위치시키는 것은 스카이프 콜 아웃 피쳐, 또는 "스카이프 아웃" 통화로 지칭된다. 일반적으로, 정규 전화로의 콜 아웃은, 가입 비용으로서 또는 사용량 기반 과금으로서 약간의 부가 비용을 포함한다.

[0508] 본 개시 내용의 문맥에서, 미보안 라스트 마일 연결을 통한 SDNP 클라우드로부터 SDNP 클라이언트 이외의 임의

의 디바이스로의 통신은 본원에서 "SDNP 콜 아웃"이라는 정의된 용어로 지칭된다. 도 11은 미보안 라스트 마일 상으로 라우팅되는 SDNP 콜 아웃의 2개의 예를 개략적으로 나타낸다. 상부 예에서, 통신은 아날로그 신호를 이용하여 전화기 또는 페이폰(6A)과 같은 아날로그 디바이스에 대해서 이루어진다. 그러한 경우에, SDNP 게이트웨이는 디지털-대-아날로그 변환기를 포함하여야 한다. 그렇지 않은 경우에, 모뎀 또는 변환 디바이스가 게이트웨이에 부가될 수 있다. 정보는, 데이터 패킷이 아니라, 아날로그 신호(1221)에 의해서 운반된다. 아날로그 전화 신호는, 보이스 운반에 효과적이지만, 고속 데이터 통신에 적합하지 않다.

[0509] 하부의 경우에, SDNP 콜 아웃은, 디지털 네트워크를 통해서, SDNP 클라이언트로서 인에이블링되지 않은, 즉 SDNP 소프트웨어 또는 펌웨어로 인에이블링되지 않은 디지털 디바이스(예를 들어, 휴대폰(32))로 발생된다. 그러한 경우에, 데이터 패킷(1223)은, 일반적으로 인터넷 프로토콜, 즉 7-계층 OSI 모델에 따른 IP 패킷 포맷을 이용하여, 통화 또는 데이터를 운반한다. IP 데이터그램은 IP 또는 NAT 어드레스를 그 소스 및 목적지 어드레스 필드 내에서 포함하고, IP 또는 VoIP 데이터를 그 페이로드로서 포함한다. 디지털 통로는, 라스트 마일 연결에 따라 달라지는 이더넷, WiFi, 또는 4G/LTE와 같은 다양한 형태의 디지털 데이터를 포함할 수 있다.

[0510] 예시적인 개략도 중 하나에서, 라스트 마일 통신 데이터가 미보안 통신 채널 또는 네트워크를 통해서 SDNP 네트워크의 외측으로 운반되기 때문에, 통화는 보안되지 않고 해킹, 스파이, 와이어 탭핑, 및 다른 사이버 공격에 노출된다. 본원의 배경 섹션에서 설명된 바와 같이, 라스트 마일을 위한 미보안 라인 및 연결은, 연선 구리 와이어, 동축 케이블, 섬유, 이더넷, WiFi, 셀룰러, 또는 위성이든 간에, 암호화와 같은 특별한 보안 방법이 엔드-투-엔드 데이터 통로 내에 삽입되지 않는 한, 본질적으로 보안되지 않는다. 가장 보안이 뛰어난 데이터 클라우드 또는 VPN의 보안은 그에 따라 가장 약한 링크 - 이 예에서, 라스트 마일 -에 의해서 손상된다. 특히 하나의 양호하게-형성된 전기, 마이크로파, 또는 라디오 파동 연결에서, 심지어 암호화가 보안을 보장하지 못한다. 보안 결여에 더하여, 개략적인 예는 신원 확인을 위한 어떠한 메커니즘도 포함하지 않는다. 인증 불가능에서, 라스트 마일은 프라이버시를 보장하지 못한다. 그에 따라, 예시적인 개략도는 통화자 프라이버시를 결여한 미보안 라스트 마일 네트워크를 나타낸다.

[0511] 도 12는, 디지털 네트워크 서비스 제공자 NSP 호스팅된 유선 또는 섬유 링크(24)에 걸쳐 공공 스위치형 전화 네트워크 또는 PSTN 게이트웨이(1A)에 연결하는, 미보안 라스트 마일 결여 프라이버시에 대한 SDNP 콜 아웃을 실행하는 SDNP 게이트웨이(1201A)을 도시한다. 이어서, PSTN 게이트웨이(1A)는 아날로그 통신 연결(4)을 통해서 일반적인 종래 전화 시스템(POTS) 스위치(3)로 라우팅된다. 이어서, POTS 스위치(3)는 연선 구리 와이어(7)를 통해서 통상의 전화 통화를 가정 전화(6)에, 무선 전화 시스템(5)에, 또는 페이폰(6A)에 위치시킨다. 전체 라스트 마일은 프라이빗도 아니고 보안도 아니다. SDNP 데이터그램(A)을 포함하는 데이터 패킷(1222A)의 통신이 SDNP 네트워크 내의 SDNP 어드레싱 및 SDNP 페이로드를 이용하지만, 데이터가 라스트 마일 하이퍼보안에 진입하면, 이점을 상실한다. 예를 들어, NSP 네트워크 호스팅된 유선 또는 섬유 링크(24)에 의해서 운반되는 IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)은, 인터넷 DNS 서버에 의해서 인식 가능한 통상적인 IP 어드레싱을 이용하고 임의의 사이버-해적에 의해서 스니핑될 수 있는 통상적인 IP 페이로드를 포함한다. 아날로그 라인(4 및 7)은 마찬가지로 취약한데, 이는 이들이 단순한 아날로그 오디오 신호를 아날로그 통화 데이터(1221)로서 운반하기 때문이다. 비록 SDNP 게이트웨이가 미보안 비-프라이빗 콜 아웃을 지원할 수 있지만, SDNP 보안 통화를 프라이버시 지원을 결여하는 미보안 라스트 마일 네트워크에 연결하도록 잘못 전달된다.

[0512] 신원확인을 이용하여, 전술한 미보안 라스트 마일 구현예에 대한 약간의 개선이 달성될 수 있다. 도 13은 미보안의 그러나 2개의 상이한 유형의 인증을 갖는 라스트 마일 상으로 라우팅되는 SDNP 콜 아웃의 예를 개략적으로 도시한다. 상부 예는 아날로그 또는 POTS을 통한 SDNP 게이트웨이(1220A)로부터 비지니스 사무실 데스크탑 전화(9)까지의 SDNP 콜 아웃을 도시한다. 도시된 바와 같이, 운영자(1225)는 인증을 수동적으로 실시하여, 계정 보유자의 신원을 확인하고 그 계정 ID를 확인한다. 비록 인증되지만, 아날로그 소리(1221)에 의해서 운반되는 통화는 미보안이고, 비밀 또는 계정 정보가 대화에서 음성으로 노출되지 않는 경우에만 프라이빗이고, 즉 비밀이 노출되지 않은 경우에 정보는 프라이빗이나, 정보가 노출되면 통신은 더 이상 프라이빗이 아니다. 따라서, 준-프라이빗이라는 용어는 본원에서 미보안 라인을 통한 인증된 통화, 즉 조건부 프라이빗 통화를 지칭하기 위해서 사용된다.

[0513] 하부 개략도는, SDNP 게이트웨이(1220A)로부터 미보안 디지털 라스트 마일 상으로의 SDNP 콜 아웃을 도시한다. IP 데이터그램(1223)에 의해서 데스크탑 PC(36)와 같은 전자 디바이스에 전달되는 데이터는, 미보안이지만, 사이버-공격자가 액세스를 가지지 않는 토큰(1226)과 같은 전자적 ID 입증 방법을 이용하여 인증될 수 있다. 라인이 미보안이고 스니핑될 수 있기 때문에, 계정 번호 또는 비밀 데이터를 노출시키지 않도록 디지털 다이알로그

에서 주의를 기울여야 한다.

[0514] 준-프라이빗 미보안 통화의 구체적인 예가 이하의 몇몇 예에 도시되어 있다. 도 14에서, 신원확인된 미보안 라스트 마일 통신이 SDNP 네트워크와 사무실 데스크탑 전화(9), 예를 들어 프라이빗 뱅커의 전화 사이에 도시되어 있다. 계정 보유자의 통화는, 예를 들어 국제 통화를 할 경우 SDNP 네트워크 내의 하이퍼보안 통신을 이용하여 국제적으로 라우팅될 수 있고 최종적으로 SDNP 게이트웨이(1201A)를 통해서 SDNP 콜 아웃으로서 라스트 마일에 연결될 수 있다. 통화의 장거리 부분은, SDNP 페이로드를 갖는 SDNP 데이터그램(A)을 포함하는 데이터 패킷(1222A)와 같은 동적으로 변화되는 SDNP 데이터그램을 이용하여 발생된다. 이어서, 데이터 패킷(1222A)은 SDNP 게이트웨이(1201A)에 의해서 SDNP 데이터그램(A)으로부터 데이터 패킷(1223B)에 의해서 도시된 IP 데이터그램(B)으로 변환된다. SDNP 데이터그램(A)과 달리, IP 데이터그램(B)은 스니핑 가능한 IP 페이로드를 포함한다. 데이터 패킷(1223B)은 네트워크 서비스 제공자(NSP)에 운영 유선 또는 섬유 링크(24)에 의해서 공공 교환 전화 네트워크 또는 PSTN 게이트웨이(1A)로 전송된다. 다시, 이러한 게이트웨이는 아날로그 통화(1221)를 수반하는 POTS 라인(4)을 통해서 회사 스위치보드(8A)에 연결된다. 회사 스위치보드(8A)는 아날로그 프라이빗 브랜치 교환을 통해서 데스크탑 전화(9)에 또는 PBX 라인(7A)을 통해서 데스크탑 전화(9)에 그리고 또한 개인 인증 운영기(1225)에 연결된다. 통화 중에, 계정 보유자는 데스크탑 전화(9)에서, 그러나 임의의 거래 계약을 시작할 수 있기 전에, 프라이빗 뱅커와 접촉하고, 개인 인증 운영기(1225)가 통화에 합류하여 통화자의 신원을 확인하고, 그 후에 통화를 떠나며, 그에 따라 통화자의 프라이버시가 유지된다. 그러나, 통화가 보안이 아니기 때문에, 계정 번호, 암호, 또는 PIN과 같은 기밀 정보를 음성으로 유출하지 않도록, 프라이빗 뱅커 및 계정 보유자 모두가 주의를 기울여야 한다. 따라서, 통화는 준-프라이빗이고, 즉 조건부로 프라이빗이다.

[0515] 도 15에서, 신원 확인된 미보안 라스트 마일 통신이 SDNP 네트워크와 데스크탑 컴퓨터(36) 사이에 도시되어 있다. 디지털 통신 세션에서, 데스크탑 컴퓨터(36)는 몇몇 디지털 매체에 걸쳐 운반되는 IP 데이터그램(B)을 이용하여 SDNP 게이트웨이(1201A)에 대해서 통신한다. 제1 레그에서, 이더넷(106A)은 IP 데이터그램(B)을 포함하는 데이터 패킷(1223D)을 데스크탑 컴퓨터(36)로부터 이더넷 기반의 로컬 라우터(27B)로 운반한다. 이더넷 로컬 라우터는 다시 IP 데이터그램(B)을 포함하는 데이터 패킷(1223C)을 이용하여 인터넷 서비스 제공자(ISP) 유선 또는 섬유 링크(24)를 통해서 네트워크 라우터(27)에 대해서 통신한다. 네트워크 서비스 제공자 라인(NSP) 동작 유선 또는 섬유 링크(24)는 네트워크 라우터(27)와 SDNP 게이트웨이(1201A) 사이의 라스트 마일의 마지막 레그 상에서 IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)을 운반한다. IP 데이터그램이 이용되기 때문에, 라스트 마일은 미보안이다. 로그인 창(1227) 및 보안 토큰(1228)과 같은 ID 확인을 위한 디지털 방법이 통신이 준-프라이빗으로 유지되게 통신을 보장하기 위한 인증을 위해서 이용될 수 있다. 이러한 디지털 인증은 사기꾼에 의한 이용을 방지하도록 단일 사용으로 제한되어야 한다. 예를 들어, 토큰이 숫자를 생성하고 이러한 것이 액세스 획득을 위해서 이용되면, 그 조합은 그러한 사용에 더 이상 유효하지 않고, 해커가 토큰을 가로채는 경우에, 그 토큰은 쓸모가 없는데, 이는 그 것이 만료되었고 더 이상 유효하지 않기 때문이다.

[0516] 신원-확인된 미보안 라스트 마일 통신의 다른 예가 도 16에 도시되어 있고, 여기에서 SDNP 게이트웨이(1201A)는 SDNP 콜 아웃으로서 판매 지점(POS) 단말기(38) 및 가스 펌프 POS 단말기(38A)와 통신한다. 도시된 바와 같은 라스트 마일 통신은 IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)을 네트워크 라우터(27)에 운반하는 NSP 유선 또는 섬유 링크(24)를 포함하는 디지털 및 아날로그 연결의 혼합이고, 이어서 유선 또는 섬유 링크(24A)가 데이터 패킷(1223C) 내에서 IP 데이터그램(B)을 운반하고, POTS 또는 아날로그 라인(30B)은 판매 지점(POS) 단말기(38) 및 가스 펌프 POS 단말기(38A)에 연결된 아날로그 통화(1221A)로서 디지털 PCM(펄스 코드 변조) 데이터를 운반한다. 금융 거래에서의 인증은, 스마트카드 통합 회로 기반의 전자 인증을 포함할 수 있고 동적 PIN(1228)에 의한 것일 수 있는 은행 카드 데이터(1229)를 기초로 한다. 인증은 SDNP 게이트웨이(1201A)를 통해서 또는 다른 라스트 마일을 통해서 SDNP 네트워크에 연결된 금융 기관(1230)으로 확인하는 것을 포함한다.

[0517] ***하이퍼보안 라스트 마일 통신*** - 보안 동적 통신 네트워크 및 프로토콜의 기술을 적응시킴으로써, 하이퍼보안 통신이 라스트 마일을 경유하여 달성될 수 있다. 하이퍼보안을 촉진하기 위해서, 연결된 디바이스는 "SDNP 클라이언트"로서 SDNP 코드를 실행하여야 한다. SDNP 클라이언트는, 연결된 통신 디바이스 상에서 호스팅된, 동작 명령어, 공유 비밀, 및 SDNP 연결성 정보를 포함한다. SDNP 클라이언트는 동작 시스템 상에서 작동되는 소프트웨어, 마이크로제어기 또는 프로그램 가능 IC 상에서, 또는 전용 하드웨어 또는 집적 회로 내에서 작동되는 펌웨어를 포함할 수 있다. 도 17은 "SDNP 연결"을 이용한 라스트 마일을 통한 예시적인 하이퍼보안 통신을 개략적으로 나타낸다. 도시된 바와 같이, SDNP 게이트웨이(1201A)는 SDNP 클라이언트를 작동시키는 디바이스에, 이러한 예에서 데스크탑 컴퓨터(36) 상에서 동작되는 SDNP 앱(1335)에 연결된다. SDNP 클라이언트는 하드웨어이고 운영 시스템 특이적이다. 모바일 디바이스에서, 안드로이드, iOS, 및 윈도우 모바일을 이용하는 상이한 모바일 디바

이스 플랫폼을 위해서, 분리된 앱들이 요구된다. 유사하게, 구분된 OS-특이적 애플리케이션이, Windows 10, MacOS, Unix 및 Linux 등을 포함하는, 노트북, 데스크탑 PC, 및 서버를 위해서 요구된다. POS 단말기, 핫스팟, IoT 등과 같이 더 높은 레벨의 운영 시스템을 가지지 않는 디바이스 내의 SDNP 클라이언트의 하드웨어 호스팅은 코드를 실행하는 프로그래밍 가능 디바이스에 적응되어야 한다. 프로그래밍 가능 집적 회로는 종종 IC의 공급자, 예를 들어 Qualcomm, Broadcom, Intel, AMD, NVidia, Microchip 등에 특유한 칩-특이적 개발 환경에서의 프로그래밍을 종종 요구한다.

[0518] SDNP 게이트웨이(1201A) 및 SDNP 앱(1335)이 SDNP 페이로드(1222)를 이용하여 통신하기 때문에, 통화자 신원 및 통화 페이로드는 패킷 스니핑에서 이해될 수 없고, 구체적으로 SDNP 페이로드(1222)는 DNS 서버에 의해서 인식되지 않는 소스 및 목적지 SDNP 의사-어드레스를 포함하고, 페이로드는, 스크램블링되고, 단편화되고, 정크 데이터 삽입과 혼합되고, 동적으로 암호화될 수 있는 SDNP 데이터를 포함한다. SDNP 페이로드(1222)는 IP 데이터그램(1223) 내에 임베딩되고, 이는, SDNP 어드레스 대신, 라스트 마일 연결성을 위해서 이용되는 셀룰러, 케이블 또는 ISP 캐리어의 네트워크의 IP 어드레스 또는 NAT 어드레스를 이용하여 라스트 마일에 걸쳐 라우팅을 지향시킨다.

[0519] SDNP 기반의 하이퍼보안 라스트 통신의 다른 양태는, 임의의 SDNP 클라이언트가 본질적으로 인증 및 식원 확인을 할 수 있다는 것이다. 그에 따라, 프라이버시 특징은 AAA를 지원하기 위한 프라이버시를 달성할 수 있는 네트워크의 능력을 기초로 하지 않고, 클라이언트 소프트웨어 또는 펌웨어가 입증 프로세스를 촉진하도록 설계되었는지의 여부를 기초로 한다. 임의의 하이퍼보안 라스트 마일이 신원 확인 가능하기 때문에, 이하의 하이퍼보안 라스트 마일 예가 프라이빗 및 비-프라이빗 보안 통신 모두에 적용된다는 것을 이해하여야 한다. 그에 따라 준-프라이버시 특징을 갖는 미보안 라스트 마일 네트워크와 달리, 하이퍼보안 라스트 마일에 걸친 프라이빗 통신은, 네트워크가 아니라, SDNP 클라이언트에 의해서 결정되고, 클라이언트가 희망하는 모든 정도의 단일-인자 또는 다수-인자 인증 과정을 지원할 수 있다.

[0520] 하이퍼보안 통화의 구체적인 예가 이하의 몇몇 예에 도시되어 있다. 도 18에서, 하이퍼보안 라스트 마일 통신이 SDNP 네트워크와 WiFi 라스트 링크를 갖는 다양한 셀룰러 모바일 디바이스 사이에 도시되어 있다. 도시된 바와 같이, SDNP 데이터그램(A)을 포함하고 SDNP 페이로드를 포함하는 데이터 패킷(1222A)이, 라스트 마일 통신을 위한 SDNP 게이트웨이(1201A)에 의해서, SDNP 페이로드를 또한 포함하는 IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)으로 변환된다. 하이퍼보안 라스트 마일이, SDNP 클라우드 이용 대신, 상이한 공유 비밀, 수치적 시드, 암호화 키, 및 다른 구역-특이적 보안 자격 증명을 이용하기 때문에, IP 데이터그램(B) 내의 SDNP 페이로드는 SDNP 데이터그램(A) 내의 SDNP 페이로드와 상이하다. 다시 말해서, SDNP 게이트웨이(1201A)는, 하나의 보안 구역으로부터의 페이로드를 다른 것으로 변화시키는 것에 의해서, 그리고 SDNP 라우팅 정보를 DNS 서버에 의해서 인식될 수 없는 소스 및 어드레스 SDNP 어드레스로서 임베딩하는 것에 의해서, SDNP 데이터그램을 IP 데이터그램으로 변환한다.

[0521] 이러한 구역-특이적 SDNP 페이로드는 다음에 IP 데이터그램 패킷 내에서, NAT 또는 인터넷 어드레스인, 라스트 마일 네트워크 특이적 IP 어드레스를 포함하는 IP 헤더와 랩핑되고, 그에 따라 SDNP 게이트웨이(1201A)와 통신 디바이스, 즉 SDNP 클라이언트로서 작용하는 태블릿(33) 및 휴대폰(32) 사이의 패킷 라우팅을 돕는다. 라스트 마일 라우팅 내의 중간 디바이스들이 SDNP 클라이언트가 아니기 때문에, IP 데이터그램(B) 내의 SDNP 페이로드의 구성은 라스트 마일에 걸쳐 이동할 때 고정되어 유지된다. 다시 말해서, 데이터 패킷(1223B, 1223C, 및 1223D)은 동일하게 구성된 데이터그램이고, 이들 모두는 동일한 SDNP 페이로드 - 패킷이 라스트 마일을 따라서 디바이스로부터 디바이스로 호핑할 때 변화되지 않는 페이로드 - 를 갖는 SDNP 데이터그램(B)를 포함한다. 단순히 요약하면, IP 데이터그램 또는 SDNP 데이터그램이든 간에, SDNP 네트워크 노드 또는 SDNP 클라이언트 만이 레벨 3 데이터그램 내에 임베딩된 SDNP 페이로드를 재구축할 수 있다.

[0522] 도시된 바와 같이, IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)은 NSP 운영 유선 또는 섬유 링크(24)에 의해서 네트워크 라우터(27)로 운반되고, 이어서 데이터 패킷(1223C)은 또한 ISP 운영 유선 또는 섬유 링크(24A)에 의해서 WiFi 라우터(26)로 운반되는 IP 데이터그램(B)를 포함한다. 이어서, WiFi 라우터(26)는, SDNP 앱(1335A)이 동작되는 휴대폰(32) 및 태블릿(33)과 같은 모바일 디바이스로 WiFi 링크(29)에 걸친 IP 데이터그램(B)을 포함하는 데이터 패킷(1223D)을 이용하는 라스트 링크 통신을 촉진한다. 따라서, 이러한 디바이스는, 원래의 메시지 또는 소리를 재생성하기 위한, 해독, 역-정크화, 언스크램블링 및 페이로드의 콘텐츠와 다른 데이터 패킷으로부터의 데이터 단편의 혼합을 포함하는, IP 데이터그램(B)를 포함하는 데이터 패킷(1223D) 내에 포함된 데이터를 해석할 수 있는 SDNP 클라이언트로서 기능한다.

[0523] 도 19에서, 하이퍼보안 라스트 마일 통신이 SDNP 네트워크와 셀룰러 라디오 라스트 링크를 갖는 다양한 셀룰러 모바일 디바이스 사이에 도시되어 있다. 도시된 바와 같이, IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)은 NSP 운영 유선 또는 섬유 링크(24)에 의해서 네트워크 라우터(27)로 운반되고, 이어서 데이터 패킷(1223C)은 또한 셀룰러 네트워크(25)를 생성하기 위해서 모바일 네트워크 운영자(MNO) 유선 또는 섬유 링크(24B)에 의해서 셀룰러 기지국(17)으로 운반되는 IP 데이터그램(B)를 포함한다. 이어서, 셀룰러 기지국(17)은, SDNP 앱(1335A)이 동작되는 휴대폰(32) 및 태블릿(33)과 같은 모바일 디바이스로 3G, 4G/LTE(28)에 걸친 IP 데이터그램(B)을 포함하는 데이터 패킷(1223D)을 이용하는 라스트 링크 통신을 촉진한다.

[0524] 이전의 예에서와 같이, 라스트 마일 라우팅 내의 중간 디바이스들이 SDNP 클라이언트가 아니기 때문에, IP 데이터그램(B) 내의 SDNP 페이로드의 구성은 라스트 마일에 걸쳐 이동할 때 고정되어 유지된다. 다시 말해서, 데이터 패킷(1223B, 1223C, 및 1223D)은 동일하게 구성된 데이터그램이고, 이들 모두는 동일한 SDNP 페이로드 - 패킷이 라스트 마일을 따라서 디바이스로부터 디바이스로 호핑할 때 변화되지 않는 페이로드 - 를 갖는 SDNP 데이터그램(B)를 포함한다.

[0525] 도 20에서, 하이퍼보안 라스트 마일 통신이 SDNP 네트워크와 이더넷 라스트 링크를 갖는 다양한 테더링된(비-모바일) 디바이스 사이에 도시되어 있다. 도시된 바와 같이, IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)은 NSP 운영 유선 또는 섬유 링크(24)에 의해서 네트워크 라우터(27)로 운반되고, 이어서 데이터 패킷(1223C)은 또한 인터넷 서비스 제공자(ISP) 유선 또는 광섬유 링크(24A)에 의해서 이더넷 라우터(103A)로 운반되는 IP 데이터그램(B)를 포함한다. 이어서, 이더넷 라우터(103A)는, IP 데이터그램(B)를 포함하는 데이터 패킷(1223D)을 이용한, 이더넷(106A)에 걸친, SDNP 앱(1335C)가 작동되는 데스크탑 컴퓨터(36) 및 SDNP 펌웨어(1335B)가 작동되는 데스크탑 전화(37)와 같은 테더링된 디바이스와의 라스트 링크 통신을 촉진한다. 라스트 마일 내에 SDNP 네트워크 노드 또는 SDNP 클라이언트가 없을 때, 데이터 패킷(1223B, 1223C, 및 1223D)은 동일하게 구성된 데이터그램이고, 이들 모두는 동일한 SDNP 페이로드 - 패킷이 라스트 마일을 따라서 디바이스로부터 디바이스로 호핑할 때 변화되지 않는 페이로드 - 를 갖는 SDNP 데이터그램(B)를 포함한다.

[0526] 도 21에서, 하이퍼보안 라스트 마일 통신이 SDNP 네트워크와 케이블 서비스 클라이언트 사이에 도시되어 있다. 도시된 바와 같이, IP 데이터그램(B)을 포함하는 데이터 패킷(1223A)이 NSP 유선 또는 섬유 링크(24)에 의해서 케이블 CMTS(101), 즉, 케이블 운영자의 명령, 통신 및 콘텐츠 분배 센터로 운반된다. 그러한 케이블 운영자는 케이블 TV, 사용량 기반 과금, 전화 서비스, 인터넷 연결성, 비지니스 서비스, 및 기타와 같은 다양한 서비스를 제공한다. 이어서, CMTS(101) 헤드 유닛은 DOCSIS3 및 (본 개시 내용의 배경 섹션에서 설명된) 트렐리스(trellis) 포맷팅에 따라 변조된 섬유 또는 동축을 이용하여 케이블(106)을 통해서 클라이언트에 연결되어 대역폭 및 실시간 서비스를 최적화한다. 클라이언트에 투과적으로, 케이블 운영자는 데이터그램 포맷을 유지할 수 있거나 대안적으로 IP 데이터그램을 독점적 데이터그램 포맷으로 패키징할 수 있다. 본원에서 CMTS 데이터그램(C)로 지칭되는, 이러한 데이터 패킷은 케이블 특이적 NAT 어드레싱을 이용하고, 케이블(106) 상의 전달을 위해서 SDNP 페이로드를 데이터 패킷(1224C) 내에서 n 네스트형 페이로드로서 캡슐화한다.

[0527] 도시된 바와 같이, 케이블 CMTS(101)는 CMTS 데이터그램(C)를 케이블 모뎀(103)으로 라우팅시키고, 이는 다시 라스트 링크 전달을 위한 미변경 SDNP 페이로드를 갖는 IP 데이터그램(B)을 포함하는 페이로드 데이터 패킷(1223B)을 추출한다. SDNP 클라이언트 인에이블드 디바이스에 대한 라스트 링크는, SDNP 클라이언트 앱(1335C)이 작동되는 데스크탑 컴퓨터(36)에 대한 이더넷(106)에 걸친 것, 또는 SDNP 클라이언트 펌웨어(1335B)가 작동되는 무선 전화(5A)에 대한 구리 연선(7)에 걸친 것을 포함하는, 몇 개의 포맷으로 발생될 수 있다. 케이블 CMTS(101)는 또한 CMTS 데이터그램(C)을 케이블 모뎀(103)으로 라우팅시키고, 이는 다시 원래의 IP 데이터그램, 예를 들어 IP 데이터그램(B)를 추출하고, 이것 그리고 다른 비디오 콘텐츠를 케이블(106)을 통해서 케이블 TV 셋톱 박스에 송신한다. 이어서, 케이블 셋톱 박스는 IP 데이터그램(B) 및 콘텐츠를 HDMI-2(107)를 통해서, SDNP 앱(1335D)이 작동되는, UHD 인터랙티브 TV(39)로 포워딩한다. 대안적으로, SDNP 펌웨어는 케이블 TV 셋탑 박스(102)에 의해서 호스팅될 수 있다.

[0528] 도 22에서, 하이퍼보안 라스트 마일 통신이 SDNP 네트워크와 케이블 서비스 제공자를 통해서 연결된 WiFi 홈 네트워크 사이에 도시되어 있다. 도시된 바와 같이, IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)이 NSP 유선 또는 섬유 링크(24A)에 의해서 케이블 CMTS(101), 즉, 케이블 운영자의 명령, 통신 및 콘텐츠 분배 센터로 운반된다. 이어서, CMTS(101) 헤드 유닛은 동축 또는 섬유에 걸친 유선 또는 섬유 링크(24A)를 이용하여 특정 클라이언트의 케이블(WiFi) 모뎀 라우터(100B)에 연결되어 WiFi 액세스 지점(26)을 생성한다. 데이터 패킷(1224C)의 라우팅은 인터넷 어드레스를 갖는 IP 데이터그램을 포함할 수 있거나, NAT 어드레싱을 갖는 독점적 CMTS 데이터그램(C)를 포함할 수 있다. SDNP 게이트웨이(1201A)와 케이블 (WiFi) 모뎀 라우터(26) 사이의 라우팅은 하이퍼

보안 라스트 마일의 와이어라인 레그를 나타낸다.

[0529] 홈 네트워크 내의 라스트 레그는, IP 데이터그램(B)를 포함하는 데이터 패킷(1223D)에 의해서 무선으로 케이블(WiFi) 모뎀 라우터(26)를 다양한 홈 디바이스에 연결하는 WiFi 링크(29)를 포함한다. 엔드-투-엔드 하이퍼보안을 촉진하기 위해서, 디바이스는 디바이스 상에 로딩된 소프트웨어 또는 펌웨어를 이용하여 SDNP 클라이언트로서 동작되어야 한다. 예를 들어, 노트북(35) 및 데스크탑 컴퓨터(36)는 컴퓨터 앱(1335C)을 이용하여 SDNP 클라이언트로서 동작되며, 휴대폰(32) 및 태블릿(33)은 모바일 앱(1335A)을 이용하여 SDNP 클라이언트로서 동작된다. 이러한 경우에 등록기(34K)인, IoT 디바이스는, 그들의 제어 시스템에 SDNP 펌웨어(1335E)가 로딩되는 경우에, SDNP 클라이언트로서 동작할 수 있다. 그러나, 그러한 디바이스가 SDNP 클라이언트의 소프트웨어가 임베딩되지 않거나 될 수 없는 경우에, 엔드-투-엔드 보안은 다른 수단에 의해서 달성될 수 있다.

[0530] ***신원-페어링된 라스트 링크 보안(Identity-Paired Last Link Security)*** - 연결된 디바이스가 SDNP 클라이언트로서 작용할 수 없는 경우에, 하이퍼보안은 보장된 엔드-투-엔드가 될 수 없다. 그러한 경우에, SDNP 원격 게이트웨이의 이용은 하이퍼보안 통신을 확장시켜 해당 라스트 링크을 제외한 통신의 라스트 마일을 커버할 수 있다. 라스트 링크 즉, 통신 디바이스에 직접적으로 연결되는 라스트 마일의 부분은 SDNP 호스트로서 인에이블링되지 않고, 라스트 링크 보안은 라스트 링크 통신을 촉진하기 위해서 이용된 근거리 네트워크(LAN)을 통해서 보장되어야 한다. 도 23은 라스트 마일 통신에서의 SDNP 원격 게이트웨이(1350)의 이용을 개략적으로 나타낸다. SDNP 원격 게이트웨이(1350)는 원격 게이트웨이로서 기능하도록 SDNP 펌웨어(1335H)에 의해서 인에이블링된 임의의 통신 디바이스를 포함한다. 따라서, SDNP 게이트웨이(1201A)와 SDNP 원격 게이트웨이(1350) 사이의 SDNP 연결은 IP 또는 NAT 소스 및 목적지 어드레스 그리고 SDNP 페이로드(1222)를 포함하는 IP 데이터그램(1223A)을 포함한다. SDNP 페이로드(1222)는 라스트 마일 구역 특정 보안 자격 증명을 이용하는 DNS 서버 및 네스트형 SDNP 페이로드에 의해서 인식될 수 없는 SDNP 어드레스를 포함한다. 이러한 SDNP 연결은, 신원 확인 및 통화 프라이버시를 지원할 수 있는 하이퍼보안이다.

[0531] SDNP 원격 게이트웨이(1350)와 SDNP 클라이언트 이외의 임의의 연결된 디바이스(예를 들어, 데스크탑 컴퓨터(36)) 사이에서, 통신은 근거리 네트워크 또는 LAN 연결, 예를 들어 이더넷, WiFi 또는 다른 프로토콜에 의해서 실시된다. 보안은, 통신 디바이스와 SDNP 원격 게이트웨이 사이에서 페어링된 LAN 보안 프로토콜 및 디바이스에 의해서 촉진된다. 디바이스 페어링은, 2개의 통신 디바이스 사이의 인증 시퀀스가 2개의 디바이스의 신원을 구축하여 미인증 액세스를 방지하게 하는 프로세스이다.

[0532] 도 24에서, SDNP 인에이블링된 라우터(1351), 즉 SDNP 펌웨어(1335H)가 작동되는 라우터가 원격 SDNP 게이트웨이의 기능을 실시한다. 이러한 게이트웨이는 IP 데이터그램(A)을 포함하는 데이터 패킷(1223A)을 IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)으로 변환한다. SDNP 펌웨어(1335H)가 IP 데이터그램(A)에 포함된 SDNP 페이로드를 해석할 수 있지만, 연결된 디바이스들은 SDNP 클라이언트들이 아니다. 그 대신, SDNP 라우터(1351)가 SDNP 페이로드를 통상적인 IP 페이로드로 변환한다. 부가적인 보안 방법이 디바이스 내로 도입되지 않는다면, 이러한 라스트 링크는 미보안이다. 가정에서의 사용에서, 이러한 미보안 디바이스 연결은 종종 염려가 되지 않는데, 이는 라스트 링크가 가정 내에서 일어나기 때문이다. 해커가 와이어탭에 연결하기 위해서 가정에 물리적으로 침입하지 않는 한, 그러한 와이어라인 연결은 스니핑될 수 없다. 비-SDNP 디바이스에 대한 유선 가정-내 라스트 링크의 예는, 데스크탑 컴퓨터(36)에 연결된 그리고 TV(39)에 연결된 모뎀(103C) 또는 HDMI-2에 연결된 예에 의해서 도시된, 이더넷(106A)을 포함한다.

[0533] SDNP 연결 및 하이퍼보안 통신이 SDNP 라우터(1351)까지만 연장되기 때문에, 라스트 링크는 와이어라인 연결에서 보안을 달성하기 위해서 인증 및 암호화에 의존하여야 한다. 이더넷에서, 그러한 보안은 인증된 디바이스들 사이의 암호화를 이용하는 가상의 근거리 네트워크 동작 또는 VLAN과 같이, 계층 1 내지 계층 3 상에서 동작되는 iSCSI를 포함하는 임의 수의 보안 방법(http://www.computerweekly.com/ feature/iSCSI-security-Networking-and-security-options-available)을 이용할 수 있다. 대안적으로, "IP 보안" 또는 IPSec 프레임워크를 이용하는 계층 4 내지 계층 6 방법을 이용하여 보안이 달성될 수 있다. 원래 Cisco에 의해서 산업 표준으로서 데이터 저장을 위해서 개발되었고 홍보한, IPSec은 2개의 보안 모드를 제공한다. "인증 헤더" 모드에서, 수신 디바이스는 데이터의 송신자를 인증할 수 있다. 이러한 모드에서, 데이터 필드가 암호화되나, 헤더는 인식 가능한 IP 어드레스를 이용한다. 터널 모드로도 알려진, 보안 페이로드 캡슐화(ESP)에서, IP 헤더를 포함하는 전체 IP 패킷이 암호화되고 새롭게 해독된 IP 패킷 내에서 네스팅되며, 그에 따라 라우팅이 적절하게 기능할 수 있고 패킷은 그 정확한 네트워크 목적지에 도달할 수 있다.

[0534] 어느 경우에도, 보안은, 네트워크에 연결될 수 있게 하기 위해서, 인증 디바이스에 의존한다. 가정 네트워크에

서, 예를 들어 컴퓨터들, 공유된 저장 드라이브, IoT 및 다른 디바이스 연결에 연결되는 개인용 네트워크에서, 네트워크-연결된 하드웨어는 빈번하게 교환되지 않는다. 그러한 경우에, 인증은 본질적으로 네트워크 또는 라우터에 대한 액세스를 획득하는 장치의 등록 프로세스를 포함한다. 특정 사용자의 신원을 식별하는 대신, 이러한 유형의 인증은, 연결을 위해서 승인된 디바이스들을 식별하고 인식하기 위해서, 일반적으로 일부 디바이스 태그, 명칭, 또는 ID 숫자를 이용하여, 디바이스들 사이에서, 즉 디바이스-대-디바이스로 이루어진다. 네트워크 연결을 구축하는 것은, 디바이스가 먼저 서로에 대해서 도입되고 사용자에 의해서 연결이 승인될 때 설정 페이즈를 포함하고, 이어서 와이어라인 디바이스가 물리적으로 다른 것에 연결될 때마다 또는 WiFi의 경우에 2개의 디바이스가 서로의 범위 내에 오게 될 때마다, 자동화된 인증 시퀀스가 이루어진다. 신원 페어링으로서 본원에서 지칭되는 설정 페이즈는 또한 디바이스 등록, 디바이스 결합, 디바이스 페어링, 페어링, 또는 페어링 결합으로서 지칭될 수 있다. 유사한 프로세스가 디바이스와 함께 이용되어 블루투스 헤드폰을 휴대폰에 연결하거나 블루투스 휴대폰을 차량의 핸즈프리 오디오 시스템에 페어링 결합시킨다. 프로토콜은 챌린지 핸드셰이크 인증 프로토콜(challenge handshake authentication protocol) 또는 CHAP, Kerberos V5, Simple Public-Key Generic Security Services Application Programming Interface(GSSAPI), Secure Remote Password(SRP), 및 Remote Authentication Dial-In User Service(RADIUS)를 포함한다. RADIUS와 같은 일부 방법은, 파괴된 그러나 아직 다른 기술과의 조합을 위해서 이용되는, 암호화 방법에 의존한다.

[0535] 이더넷 통신이 신원-페어링된 디바이스, 예를 들어 이더넷 모뎀(103C), 구리 연선 전도체(7)를 경유하여 무선 전화(5A)에 그리고 데스크탑 전화(37)에 전달된 아날로그 전화기 신호를 포함하는 모뎀의 출력을 보호하지만, 라스트 링크는 보안이 아니다. 또한, 무선 전화(5A)의 통신 포맷은 보안이 아니고 가로챔 및 모니터링에 노출된다. 이러한 이유로, 보안 통신에서의 가정 전화의 사용은 좋지 않다.

[0536] 비디오 콘텐츠의 분배는 보안에서 다른 관심 대상이다. 예를 들어, HDTV(39)에 대한 SDNP 라우터(1351)의 통신에서, 고해상도 멀티미디어 인터페이스(HDMI), 디스플레이포트(DP), 디지털 비주얼 인터페이스(DVI), 및 덜 대중적인 기가비트 비디오 인터페이스(GVIF), 또는 통합 디지털 인터페이스(UDI)와 같은 비디오 통신 포맷이 일반적으로 HDTV 또는 디스플레이 모니터에 대한 물리적 연결을 포함한다. 원래 이러한 연결 및 그 데이터의 보안은 영화 스튜디오 및 콘텐츠 제공자의 관심이었고, 저작물의 불법 복제 및 배포를 방지하는데 초점이 맞춰졌다. 비디오 링크의 보안을 유지하기 위해서 Intel Corp.에 의해서 개발된 하나의 보안 프로토콜로서 HDCP(High-bandwidth Digital Content Protection)가 있다(https://en.wikipedia.org/wiki/High-bandwidth Digital Content Protection). 원래 그러한 시스템은 HDCP-암호화 콘텐츠가 미인증 디바이스 상에서 플레이되는 것을 방지하기 위한 것이었다. 그러한 시스템은 콘텐츠를 송신하기 전에 TV 수신기 또는 디스플레이의 인증을 체크한다. 그에 따라, DHCP는 비-라이센스가 데이터를 수신하는 것을 방지하기 위해서 인증을 사용하고, 이는 정보 도청을 방지하기 위해서 데이터를 암호화하고 손상된 디바이스의 키를 취소한다.

[0537] HDCP에 의해서, 모뎀으로부터 TV로의 콘텐츠 흐름이 인증에 의해서, 즉 식별 페어링의 이용에 의해서 보안될 수 있다. 그러나, 스마트 TV의 출현으로, 데이터 흐름은 양방향적이다. 업스트림 데이터 흐름, 즉 TV로부터 모뎀 또는 셋탑 박스로의 데이터 흐름을 촉진하기 위한 수단으로서, 개정판 1.4로부터 시작하여, HDMI는 이제 HEC 또는 HDMI 이더넷 채널로서 알려진 고속 양방향 데이터 채널을 임베딩한다. 이러한 데이터 채널은, HDMI 연결된 디바이스가 100MC/초 이더넷을 통해서 데이터를 송신 및 수신할 수 있다는 것을 의미하고, 그에 따라 이들이 IP-TV와 같은 IP-기반의 애플리케이션을 위해서 준비될 수 있게 한다. HDMI 이더넷 채널은, 별도의 이더넷 케이블을 필요로 하지 않고, 인터넷-인에이블링된 HDMI 디바이스가 HDMI 링크를 통해서 인터넷 연결을 공유할 수 있게 한다. 따라서, 보안 통신이 동일 보안 프로토콜 및 이더넷에서 이용 가능한 신원 페어링을 이용하여 HDMI에 걸쳐 촉진될 수 있다.

[0538] 도 25에서, SDNP 인에이블링된 WiFi 라우터(1352), 즉 SDNP 펌웨어(1335J)가 작동되는 WiFi 라우터의 이용이 원격 SDNP 게이트웨이의 기능을 실시한다. 이러한 게이트웨이는 IP 데이터그램(A)을 포함하는 데이터 패킷(1223A)을 IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)으로 변환한다. SDNP 펌웨어(1335J)가 IP 데이터그램(A)에 포함된 SDNP 페이로드를 해석할 수 있지만, 연결된 디바이스들은 SDNP 클라이언트들이 아니다. 그 대신, SDNP WiFi 라우터(1352)는 SDNP 페이로드를 통상적인 IP 페이로드로 변환하고, WiFi 링크(29)를 통한 통신을 촉진하기 위해서 WiFi 액세스 포인트(26)를 이용하여 연결 디바이스와 무선으로 통신한다. 부가적인 보안 방법이 디바이스 내로 도입되지 않는다면, 이러한 라스트 링크는 미보안이다. 가정이나 사무실에서의 WiFi 통신의 경우에, 보안이 염려되는데, 이는 데이터 패킷이 원거리에서 스니핑될 수 있기 때문이다. WiFi 연결된 가정 및 사무실 디바이스의 예는 데스크탑 컴퓨터(36), 노트북(35), 태블릿(33), 휴대폰(32), 스피커(34B), 프린터/스캐너(34A), 및 공유된 데이터 드라이브(34C)를 포함한다.

[0539] SDNP 게이트웨이, 즉 SDNP WiFi 라우터(1352)와, 연결된 디바이스 사이의 보안은, 이전의 WPA 및 그 미보안 선행 WPE를 대체하는, WiFi 보호 액세스(WPA-II 또는 WPA2)(IEEE 802.1 li-2004)와 같은 임의의 수의 산업 표준 프로토콜을 이용하여 달성된다. WPA2 통신은, 128-비트 키 및 1280비트 블록 크기를 갖는 AES 프로세싱을 기초로 하는 CCMP(Counter Mode Cipher Block Chaining Message Authentication Code Protocol)를 이용하여 보호된다. CCMP는 데이터 신뢰성을 제공하고, 인증을 필요로 하고, 액세스 제어를 설정한다. 인증은 설정에서 신원 페어링을 포함한다. 재-페어링은 반드시 수작업으로 실시되어야 한다. CCMP 보안은, 양호하지만, 하이퍼보안은 아니며, SDNP 클라이언트로부터 제공되는 SDNP 통신의 익명 데이터 패킷 및 동적 특성을 갖지 않는다.

[0540] 도 26에서, 가정 네트워크 내의 IoT 연결된 디바이스의 예로서, SDNP 인에이블링된 WiFi 라우터(1352), 즉 SDNP 펌웨어(1335J)가 작동되는 WiFi 라우터의 이용이 원격 SDNP 게이트웨이의 기능을 실시한다. 이러한 게이트웨이는 IP 데이터그램(A)을 포함하는 데이터 패킷(1223A)을 IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)으로 변환한다. SDNP 펌웨어(1,335 J)가 IP 데이터그램(A)에 포함된 SDNP 페이로드를 해석할 수 있지만, 연결된 IoT 디바이스들은 SDNP 클라이언트들이 아니다. 그 대신, SDNP WiFi 라우터(1352)는 SDNP 페이로드를 통상적인 IP 페이로드로 변환하고, WiFi 액세스 포인트(26)로부터의 WiFi 링크(29)를 이용하여 연결 디바이스와 무선으로 통신한다. 부가적인 보안 방법이 실시되지 않는 한, 이러한 라스트 링크는 미보안이다 - 특히 WiFi 데이터 패킷이 원거리에서 스니핑될 수 있다. 가정 내의 WiFi 연결된 IoT 디바이스의 예는 중앙 가열 및 공조(34D), 조명등(34G), 블라인드(34F), 대형 가전기기(34K), 휴대용 및 실내 HVAC(34E), 차고 도어(34L), 가정 모니터링(34J), 및 중앙 보안 시스템(34H)을 포함한다.

[0541] SDNP 게이트웨이,즉 SDNP WiFi 라우터(1352)와, 연결된 디바이스 사이의 보안은 데이터 비밀성을 촉진하는 CCMP를 이용하는 전술한 WPA2(WiFi Protected Access protocol)와 같은 임의의 수의 산업 표준을 이용하여 달성되고, 인증을 요구하고, 액세스 제어를 설정한다. WPA2는, 계층 2 프로토콜로서 구현된 디바이스 확인인, 신원 페어링을 이용하여 보안을 달성한다. 이러한 방법은 수동적인 인증 방법을 포함하는 귀찮은 것이다.

[0542] IoT 통신을 위해서 최근에 도입된 근거리 네트워크를 위해서 이용되는 대안적인 프로토콜 - AllJoyn 프레임워크로 지칭되는 근위 네트워크. 그러한 프레임워크는 디바이스를 발견하고, 세션을 생성하고, 보안 통신을 돕는다. 프레임워크는, WiFi, 이더넷, 직렬 버스 통신, 및 전력 라인 PLC를 포함하는, 수 많은 계층 2 전송 계층들을 이용하여 IoT 디바이스 연결성을 지원하도록 설계된다. 애플리케이션은, Linux, Windows, MacOS, Android, iOS, RTOS 실시간 운영 시스템, 및 오픈 소스 개발 환경 Arduino을 포함하는 수많은 플랫폼에서 동작되는 C, C++, Obj. C, 및 Java를 기초로 할 수 있다.

[0543] AllJoyn 유연 애플리케이션은 다른 것을 인증하고 암호화된 데이터를 교환하여 엔드-투-엔드 애플리케이션 레벨 보안을 가능하게 한다. 인증 및 데이터 암호화는 애플리케이션 계층 7에서 실행된다. 라우터 계층으로도 지칭되는 전송 계층 2는 애플리케이션 종료점들 사이에서 보안-관련 메시지를 전송하나 어떠한 보안 로직 자체도 실시하지 않는다. 또한 애플리케이션 계층 7에서 실시되는 "Auth Listener"라고도 알려져 있는 역통화 기능은, PIN, 암호, 또는 인증 증명서를 이용한 인증을 돕는다. 보안은 AES128 피어-투-피어 암호화를 이용하여 달성된다. WPA와 마찬가지로, AllJoyn은 명령 및 제어 시퀀스의 실행 전의 인증 프로세스에서의 신원 페어링을 이용한다. 지원되는 인증 방법은 미리-공유된 키 또는 PSK, SRP(secure remote password) 키 교환 또는 사용자 이름 및 암호를 이용한 로그인을 포함한다. 프로토콜은 또한, (i) 인증이 없는, (ii) 미리-교환된 키로 인증된, 그리고 (iii) X.509 ECDSA 증명서로 인증된, 일시적(타원형 곡선 Diffe-Hellman) 키 교환을 지원한다.

[0544] 동일한 기술이 비지니스 기업에 적용될 수 있다. 도 27에서, 가정 네트워크 내의 IoT 연결된 디바이스의 예로서, SDNP 인에이블링된 WiFi 및 이더넷 라우터(1352Z), 즉 SDNP 펌웨어(1335J)가 작동되는 이더넷 및 WiFi 라우터의 이용이 원격 SDNP 게이트웨이의 기능을 실시한다. 이러한 게이트웨이는 IP 데이터그램(A)을 포함하는 데이터 패킷(1223A)을 IP 데이터그램(B)를 포함하는 데이터 패킷(1223B)으로 변환한다. SDNP 펌웨어(1335 J)가 IP 데이터그램(A)에 포함된 SDNP 페이로드를 해석할 수 있지만, 연결된 IoT 디바이스들은 SDNP 클라이언트들이 아니다. 그 대신, SDNP 및 이더넷 WiFi 라우터(1352)는 SDNP 페이로드를 통상적인 IP 페이로드로 변환하고, WiFi 링크(29) 및 이더넷(106A) 모두를 이용하여 연결 디바이스와 통신한다.

[0545] 부가적인 보안 방법이 실시되지 않는 한, 이러한 라스트 링크는 미보안이다 - 특히 원거리에서 스니핑될 수 있는 WiFi 데이터 패킷. WiFi 연결된 IoT 비지니스 디바이스의 예는 중앙 가열 및 공조(34D), 조명등(34G), 감시 시스템(34J), 보안 시스템(34H), POS 단말기(38), 및 태블릿(33)과 같은 WiFi 핫스팟 연결된 디바이스를 포함한다. 비지니스 기업 와이어라인 연결된 디바이스는 비지니스의 특성에 따라 달라진다. 뱅킹에서, 디바이스는 이더넷 연결된 ATM 기계(38D)를 포함한다. 가스 충전소에서, 디바이스는 예를 들어 이더넷 연결된 가스 펌프(38

A)를 포함한다.

[0546] 요약하면, 라스트 링크는 SDNP 원격 게이트웨이와 통신하는 비-SDNP 클라이언트로 보안될 수 있다. 이러한 방식으로, 라스트 마일의 대부분은 하이퍼보안인 한편, 라스트 링크는 신원 페어링된 암호화된 보안을 이용한다.

[0547] ***SDNP 브릿지 통신(SDNP Bridge Communication)*** - 전술한 바와 같이, SDNP 클라우드 외부의 라스트 마일 데이터 전송은, 인터넷 소스 및 목적지 어드레스를 이용하는, 또는 대안적으로 네트워크 운영자의 NAT 어드레스를 이용하는 IP 데이터그램, 즉 데이터 패킷을 필수적으로 활용한다. 예를 들어 사무실 건물 내에서 운영되는 또는 서버에서 SDNP 소프트-스위치를 호스팅하자 하는 로컬 네트워크 서비스 제공자와 협력하는 프라이빗 네트워크의 경우에, 라스트 마일의 부분 상에서 하이퍼보안 통신을 달성하기 위해서 SDNP 데이터그램을 이용할 수 있다.

[0548] 전술한 바와 같이, 하이퍼보안 통신은 SDNP 소프트-스위치 소프트웨어 또는 펌웨어를 호스팅하기 위해서 그리고, SDNP 클라우드 내의 IP 데이터그램이 아닌, SDNP 데이터그램 및 익명 어드레스를 이용하여 통신하기 위해서 서버에 의존하고, 이러한 SDNP 소프트-스위치 인에이블드 서버는, SDNP 노드 표기($M_{0,1}$, $M_{1,0}$, $M_{1,1}$ 등)에 의해서 표시된 바와 같이, SDNP 노드로 지칭된다. 전술한 미국 출원 제14/803,869호는 또한 SDNP 브릿지 - IP 데이터그램을 다른 SDNP 클라우드에 라우팅하는 SDNP 게이트웨이 - 에 의해서 연결된 다수의 독립적인 SDNP 클라우드들 사이의 통신을 또한 개시한다.

[0549] SDNP 브릿지의 개념은 라스트 마일 통신의 부분을 위해서 유사하게 구성될 수 있다. 라스트 마일 내에서 SDNP 서브-네트워크 또는 미니-클라우드를 생성하기 위해서, 둘 이상의 서버가 SDNP 브릿지 소프트웨어 또는 펌웨어에 의해서 인에이블링되어야 한다. 단부 디바이스에서 즉, 통화 디바이스에서 동작되는 SDNP 클라이언트 소프트웨어 또는 펌웨어와 달리, SDNP 브릿지 동작은, 최종 연결로서 동작되지 않고, 데이터를 라우팅하기 위해서 이용된다. 따라서, 둘 이상의 인접 SDNP 브릿지들은 단독형 SDNP 브릿지 네트워크, SDNP 미니-클라우드 또는 SDNP 애드혹 네트워크로서 동작할 수 있다. SDNP 브릿지 기능은, 전술한 바와 같이, WiFi 라우터의 브릿지 모드 동작에 관한 계층 2 설명과 유사한 계층 3 구성을 나타낸다. SDNP-브릿지 또는 SDNP 브릿지 네트워크에서, 통신은 SDNP 데이터그램을 이용하여 이루어진다. SDNP-브릿지 또는 SDNP 브릿지 네트워크 외부로부터의 SDNP-브릿지에 대한 통신은 SDNP 페이로드를 갖는 IP 데이터그램을 이용한다.

[0550] 라스트 마일 통신 내의 SDNP 브릿지의 동작이 도 28에 도시된 개략도에서 예시되어 있고, 도 28은 SDNP 게이트웨이(1201A)를 갖는 SDNP 네트워크, SDNP 펌웨어(1335H 및 1335J)가 각각 작동되는 SDNP 브릿지 라우터(1350 및 1352Z)를 포함하는 SDNP 브릿지, 및 SDNP 클라이언트가 아닌, 여기에서 노트북(35)으로 도시된, 연결된 클라이언트 디바이스를 포함한다. 도시된 바와 같이, SDNP 게이트웨이(1201A)와 SDNP-브릿지(1350) 사이의 통신은 IP 어드레스 및 SDNP 페이로드를 갖는 IP 데이터그램(1223A)을 이용하는 보안 연결을 포함한다. SDNP 페이로드(1222A)는 다시, 구역 특정 보안 자격 증명을 이용하여 인코딩된 SDNP 라우팅 정보 및 보안 SDNP 페이로드를 포함한다. 그에 의해서, 비록 IP 어드레스 라우팅이 이용되지만, 하이퍼보안은 SDNP 페이로드를 이용하여 달성된다.

[0551] SDNP-브릿지 연결 내에서, 즉 SDNP 브릿지 라우터(1350)와 WiFi-인에이블드 SDNP 브릿지 라우터(1352Z) 사이에서, 하이퍼보안 통신이 SDNP 데이터그램(1222B)을 이용하여 발생된다. SDNP 라우팅 정보는 SDNP 페이로드(1222A) 내에 포함된 SDNP 어드레싱으로부터 추출된다. 그와 함께, SDNP-브릿지 및 SDNP 연결은, 신원 및 계정 입증을 지원할 수 있고 프라이버시를 지원할 수 있는, 라스트 마일 통신의 하이퍼보안 와이어라인 레그를 포함한다.

[0552] SDNP-브릿지 라우터(1352Z)으로부터 비-SDNP 클라이언트 디바이스 즉, 노트북(35)으로의 연결은, 근거리 네트워크, 즉 WiFi 또는 이더넷에 걸친 IP 어드레스 및 IP 페이로드를 갖는 IP 데이터그램(1223B)를 이용한다. 이러한 라스트 링크의 보안은, 하이퍼보안이 아님에도 불구하고, iSCSI, IPSec, WPA, AllJoyn, 및 기타와 같은 전술한 이더넷 및 WiFi 보안 프로토콜 중 임의의 것에 의해서 보안된다.

[0553] SDNP 브릿지의 구현은 임의의 수의 물리적 미디어에 의해서 수반되는 임의의 2개의 SDNP 인에이블드 디바이스 사이에서 발생될 수 있고, 이는 SDNP 브릿징이 계층 1 PHY 및 계층 2 전송 층 실현으로부터 불가지론적으로 동작되는 계층 3 프로토콜이라는 것을 의미한다. 예를 들어, 도 29a에 도시된 최상단 개략도에서, SDNP 펌웨어(1335H)가 각각 작동되는 2개의 SDNP 브릿지 이더넷 라우터(1351A)는 SDNP 데이터그램(1222)을 이용하여 이더넷(와이어라인) 브릿지에 걸쳐 통신한다. 중심 개략도에서, 각각이 이더넷 및 WiFi 통신할 수 있고 SDNP 펌웨어(1335J)가 작동하는, 2개의 SDNP-브릿지 라우터(1352Z)가 SDNP 데이터그램(1222)을 이용하여 WiFi(무선) 브릿지에 걸쳐 통신한다. 가장 하단의 개략도에서, SDNP 펌웨어(1335H)가 작동되는 SDNP-브릿지 이더넷 라우터

(1351A)는, 이더넷 및 WiFi 통신 작동 SDNP 펌웨어(1335J)가 가능한, SDNP-브릿지 라우터(1352Z)을 갖는 SDNP 데이터그램(1222)을 이용하여 이더넷(와이어라인) 브릿지에 걸쳐 통신한다. 이러한 방식으로, 둘 이상의 SDNP 인에이블드 라우터를 포함하는 SDNP 브릿지는, 비록 라스트 마일 내의 SDNP 클라우드 외부에서 동작되지만, 건물 전체를 통해서 또는 프라이빗 네트워크에 걸쳐 SDNP 데이터그램을 라우팅 또는 분포시킬 수 있다.

[0554] SDNP-브릿지는 케이블 TV 시스템과 같은 독점적 하드웨어를 이용하는 시스템까지 확장될 수 있다. 예를 들어, 도 29b에 도시된 최상단 도면에서, 2개의 케이블 CMTS "헤드" 서버가 수정되어, SDNP 펌웨어 또는 소프트웨어(1335L)를 작동시키고 그에 따라 케이블 CMTS SDNP 브릿지(101)로서 동작하고 SDNP 데이터그램(1222)을 이용하여 케이블 또는 섬유(와이어라인) 브릿지에 걸쳐 통신한다. SDNP-브릿지는 CMTS 헤드로부터 가입자의 집으로 연장될 수 있다. 중심 개략도에 도시된 바와 같이, SDNP 펌웨어 또는 소프트웨어(1335L)가 작동되는 케이블 CMTS SDNP 브릿지(101)는 케이블(동축) 브릿지에 걸친 SDNP 데이터그램(1222)을 이용하여 SDNP 펌웨어(1335M)가 작동되는 케이블 TV 셋탑 박스 또는 케이블 모뎀(102)에 대해서 통신한다. 이러한 방식으로, SDNP 브릿지는 하이퍼보안 통신을 가정 또는 사무실 내로 확장한다.

[0555] 개시된 SDNP-브릿지 방법은 또한 라디오 네트워크에 걸쳐 데이터를 전송하기 위해서 이용될 수 있다. 도 29b의 최하단 개략도에서, SDNP 펌웨어 또는 소프트웨어(1335N)가 작동되는 2개의 셀룰러 기지국 및 라디오 타워가 셀룰러 기지국 SDNP 브릿지(17X 및 17Y)로서 기능하여, SDNP 데이터그램(1222)을 이용하는 셀룰러 브릿지(25X 및 25Y)를 포함하는 셀룰러 네트워크에 걸쳐 무선으로 통신한다. 도 29c의 상부 개략도에서, SDNP 펌웨어 또는 소프트웨어(1335O)가 작동되는 지상 마이크로파 기지국이 지면-대-위성 링크 SDNP 브릿지(92C)로서 기능하여, SDNP 데이터그램(1222)을 이용하는 마이크로파 위성 브릿지로서 SDNP 펌웨어 또는 소프트웨어(1335P)가 작동되는 궤도 위성에, 즉 위성 SDNP 브릿지(93)에 대해서 통신한다. 이어서, 위성은 다시 가입자 또는 다른 위성과 통신한다.

[0556] SDNP 브릿지 통신은, 피어-투-피어 애드혹 통신 네트워크로서 자동차를 이용하는 자동 애플리케이션에 적응될 수 있다. 도 29c의 하부 개략도에서, SDNP 펌웨어(1335F)가 작동되는 차(1390A) 내부의 텔레매틱스 모듈이, SDNP 데이터그램(1222)을 이용하여, 자동차 라디오 브릿지를 통해서, 또한 SDNP 펌웨어(1335F)가 또한 작동되는 부근의 차량(1390B)과 통신한다. SDNP 펌웨어로 인에이블링된 각각의 차량은 동적 텔레매틱스 SDNP 브릿지 네트워크 내에서 다른 통신 노드를 형성한다. 이러한 통신은 특정 차량 또는 운전자에게 송신되는 정보를 나타내지 못하나, 그 대신 셀 타워가 지역적으로 존재하지 않는 곳에서도, 고속도로를 따라 정보를 전달할 수 있는 통신 네트워크를 형성한다.

[0557] SDNP 브릿지 네트워크의 개념은 특히 넓은 지역에 걸친 그리고 차량, 트럭, 비상 운반체, 기차, 항공기, 보트 및 대양 선박을 포함하는 운송 및 선박업에서의 통신에 있어서 특히 유리하다. 특히, 통신을 위한 광범위한 커버리지를 달성하기 위해서, 위성 네트워크가 요구된다. 시스템은 전형적으로 위성 브릿지 또는 백홀(backhaul)로 지칭되는 위성 운영자와의 네트워크 연결성, 및 위성 분배로도 알려진 그 클라이언트 및 가입자에 대한 위성 링크를 포함한다. 도 30은 SDNP 하이퍼보안 통신을 위해서 구성된 다양한 위성 연결을 개략적으로 나타낸다. 도시된 SDNP 게이트웨이(1201A)가 , SDNP 데이터그램(A) 및 SDNP 페이로드를 포함하는 데이터 패킷(1222A)을 수반하는 와이어라인 연결(94A)을 이용하는 SDNP 펌웨어 또는 소프트웨어(1335O)가 작동되는 지상 위성 안테나 접시(92C)와 통신하고, 이는 다시 동일 SDNP 데이터그램(A)을 데이터 패킷(1223B)으로서 위성 브릿지(95A)를 통해 SDNP 펌웨어 또는 소프트웨어(1335P)가 동작되는 위성(93)에 중계한다.

[0558] 하이퍼보안 통신 데이터 패킷을 SDNP 인에이블드 위성(93)으로부터 다양한 클라이언트에 분배하는 것은, SDNP 페이로드를 포함하는 데이터 패킷(1222C) 및 SDNP 데이터 패킷-A를 포함한다. 위성 통신은 양방향적이고, 위성(93)으로부터 지상 클라이언트로의 다운링크는, 업링크 연결보다, 더 강한 신호 강도 및 더 빠른 데이터 전송률을 가능하게 한다. 다시 말해서, 위성은 클라이언트의 응답보다 더 빠른 데이터 전송률로 그리고 더 강한 신호 세기로 지구의 클라이언트에 전송할 수 있다. 가입자에 대한 위성(93) 링크의 예는 SDNP 펌웨어(1335T)가 작동되는 접시 인터넷 가입자(92G)에 대한, SDNP 펌웨어(1335S)가 작동되는 위성 전화(92F)에 대한, SDNP 펌웨어(1335G)가 작동되는 고속 철도(1360C) 상단에 위치된 위성 안테나 어레이(92H)에 대한, SDNP 펌웨어(1335R)가 작동되는 대양 선박(1360B) 상단에 위치된 위성 안테나 어레이(92E)에 대한, 그리고 SDNP 펌웨어(1335Q)가 작동되는 항공기(1360A) 상단에 위치된 위성 안테나 어레이(92H)에 대한, 위성 링크(95B)를 포함한다.

[0559] 선박, 항공기, 및 기차와 같은 대형 운반체의 경우에, 각각의 시스템은 이러한 하이퍼보안 위성 통신 링크를 그 자체의 내부 통신 시스템 또는 근거리 네트워크에 연결한다. 예를 들어 도 31a는 상업용 항공기를 도시하고, 여기에서 항공기(1360A)의 동체 상단에 장착된 SDNP 펌웨어(1335X)가 작동하는 위성 안테나 모듈(92D)이 SDNP 소

프트웨어(1335Z)가 작동하는 통신 중앙 서버(1361)에 연결된다. 통신 중앙 서버(1361)는, 선택적으로 SDNP 펌웨어(1335L)가 동작되는, 기구(1367), 데이터 기록기 및 블랙 박스(1368), 미디어 저장 모듈(1363), 및 WiFi 라우터 모듈(1362)을 포함하는 다양한 시스템에 링크된다. WiFi 라우터 모듈(1362)가 항공기 전체를 통해서 위치된 WiFi 안테나(1361)의 어레이에 연결되어 WiFi 핫스팟 통신을 지원한다. 라디오 기반의 비행 제어를 제외한 모든 통신은 예를 들어 도 31b에 도시된 안테나 모듈(92D)을 이용하여 공통 위성 통신 링크를 통해서 발생된다. 안테나 모듈은 위성 전송 안테나(1360A), 위성 수신 안테나(1368A), 안테나 제어 유닛(1369), 및 40W 전압 조절기(1370)를 포함한다. 위성 수신 안테나(1368A)는 위성 전송 안테나(1360A)보다 작은데, 이는 위성 방송 파워 및 신호 강도가 안테나의 방송 강도 및 업링크 능력보다 크기 때문이다.

[0560] 해상 위성 선박 통신은, 고고도 및 근접 지구 궤도 위성을 포함하는 위성 통신의 다수의 대역을 이용한다. 예를 들어 도 32는 Ku 대역 위성 안테나(1383A) 및 저-지구-궤도 위성 안테나(1383B 및 1383C)를 포함하는 다수 대역 통신의 이용을 도시한다. 고고도 위성은 업링크 능력을 제공하지 않거나 제한되나, 지구정지궤도를 포함한 높은 고도로부터 넓은 지역을 커버할 수 있다. 그 높은 고도로 인해서, 각각의 위성의 지역 커버리지는 지도(1384)에서 도시된 바와 같이 상당하다. 지도(1385)에서 도시된 바와 같이, 낮은 지구 궤도 위성은 더 작은 지역을 커버하고, 더 많은 위성을 필요로 하며, 그에 따라 방송 지역을 커버하기 위해서 더 많은 비용이 든다. 선박의 경로에 따라, 낮은 지구 궤도 위성에 대한 액세스가 위성의 궤도 위치에 따라 간헐적일 수 있다.

[0561] Ku 대역 위성 안테나(1383A)가 TV 및 영화 콘텐츠의 분배를 위해서 일차적으로 사용되기 때문에, SDNP 보안은 일반적으로 요구되지 않는다. 추적 및 위치결정은 안테나 제어(1383)에 의해서 실시된다. 위성 안테나(1383A)로부터의 다중-채널 데이터는, 신호를 TV 수신기 및 튜너(1382)로 라우팅되는 고정 비디오 방송 데이터 및 디지털 비디오 방송 DVB 데이터로 분리하는 L-대역 멀티스위치(1381) 내로 공급된다. 비디오 콘텐츠는 중앙 통신 서버(1380) 내로 공급된다. 그러나, 보안 통신이 요구되는 경우에, Ku 대역 위성 안테나(1383A)는 SDNP 소프트웨어를 실행하도록 구성될 수 있다.

[0562] 상응하는 SDNP 펌웨어(1335U 및 1335V)가 동작되는 저-지구-궤도 위성 안테나(1383B 및 1383C)로부터의 데이터는 정보를 위성 안테나로부터, SDNP 소프트웨어(1335Z)가 동작되는 중앙 통신 서버(1380)로 정보를 중계한다. 땅의 범위 내에서, 통신 시스템은 또한, SDNP 펌웨어(1335N)가 동작되는 셀룰러 기지국(17)에 의해서 호스팅되는 4G/LTE 셀룰러 네트워크(25)를 이용하여 통신할 수 있다. 서버(1380)를 통한 통신은, SDNP 펌웨어(1335L)가 동작되는 SDNP WiFi 라우터(1362)를 이용하여 선박 전체를 통해서 분배된다. WiFi 액세스 포인트(26)의 WiFi 핫스팟 통신은 WiFi 안테나(1361)를 이용하여 선박 전체를 통해서 분배된다. SDNP 앱(1335)이 작동되는 휴대폰(32)과 같은 SDNP 클라이언트에 대한 통신은 엔드-투-엔드 하이퍼보안 통신을 돕는다. SDNP 클라이언트로서 인에이블링되지 않은 디바이스는, WAP, AllJoyn, 또는 다른 보안 프로토콜을 이용한 신원 페어링에 의존하여야 한다.

[0563] 도 33은 고속 열차에 적용된 다중-대역 통신의 적용예를 도시한다. 도시된 바와 같이, SDNP 게이트웨이(1201A)에 연결된 SDNP 소프트웨어(1335Z)가 동작되는 기차 데이터 중심 서버(1380)는, 위성 마이크로파(95B), 400MHz 라디오(1372), 및 60GHz 마이크로파(1373)를 포함하는 다중 PHY 연결을 통해서 고속 열차(1360C)에 대해서 통신한다. SDNP 통신 중에, SDNP 데이터 센터(1380)는 SDNP 펌웨어(1335D)가 동작되는 위성 안테나(92C)를 통해서 SDNP 펌웨어(1335P)가 동작되는 위성(93)에 데이터를 중계한다. 위성은 SDNP 소프트웨어(1335Y)가 동작되는 서버(1361)에 연결된 기차 안테나 어레이(1383V)와 통신한다. 대안적인 통신은 기차 궤도를 따라서 일정 간격으로 배치된 400MHz 안테나(1381) 또는 60GHz 안테나(1382)를 통해서 SDNP 데이터 중심(1380)으로부터 발생된다. 이러한 위성은 또한 SDNP 소프트웨어(1335Y)가 동작되는 기차 통신 SDNP 서버(1361)에 연결된 안테나 어레이(1383B)와 통신한다. 이어서, SDNP 서버(1361)에 의해서 수신된 통신이 WiFi 브릿지(1335Z)에 의해서 기차 전체를 통해서 그리고 WiFi 핫스팟으로서 클라이언트에 분배된다.

[0564] 자동차 및 전문적인 트럭업에서의 통신 기능은 이하를 포함하여 다면적이다:

[0565] * 음성 통신

[0566] * 네비게이션, 지도, 도로 정보, 경고

[0567] * 엔터테인먼트, 핫스팟 서비스, 인포테인먼트

[0568] * 무선 지불, 톨(toll)

[0569] * 긴급 서비스, 도로옆 지원

[0570] * 충돌 회피

[0571] * 운항 스케줄링(전문적, 함께 타기)

[0572] 자율 차량 즉, 자가-운전 차량을 위한 부가적인 기능이 또한 요구된다. "텔레매틱스" 모듈로 지칭되는 CDMA(2.5G) 제어형 중앙 유닛과 같은 종래의 셀룰러 네트워크를 주로 기초로 하는, 기존 자동차 시스템은 해킹, 사이버-공격, 및 프라이버시 공격에 매우 취약한 것으로 확인되었다. 이러한 취약성을 제거하기 위해서, 전체 네트워크가 상당한 지출이 없이 보안되어야 하고, 즉 새로운 네트워크를 설치하는 것은 재정적으로 선택사항이 될 수 없다. 그 대신, 계층 3 내지 계층 7에서 전개된 보안 방법과 같은 보안 기반시설이 하드웨어 네트워크 위에 배치되어야 한다. 이러한 전략은 본원에서 개시된 SDNP 라스트 마일 구현예와 양립될 수 있다.

[0573] 도 34는 운반체와 SDNP 클라우드 사이의 예시적인 하이퍼보안 라스트 마일 연결을 도시한다. 이전의 라스트 마일 연결에서와 같이, 라스트 마일에 걸쳐 패킷을 전송하는 것과 관련된 특별한 데이터 캐리어가 위치에 따라 크게 달라질 수 있다. 따라서, 관련 데이터 캐리어와 관계없이 하이퍼보안 통신을 제시하기 위한 예가 도시되어 있다. 도시된 바와 같이, SDNP 게이트웨이(1201A)가 네트워크 서비스 제공자(NSP) 관리 유선 또는 섬유 링크(24)를 통해서 네트워크 라우터(67A)에 연결되어, SDNP 데이터그램(A)을 포함하는 데이터 패킷(1222A)을 SDNP 페이로드를 포함하는 IP 데이터그램(B)을 포함하는 데이터 패킷(1223A)으로 변환한다. 이어서, 네트워크 라우터(67A)가, 모바일 네트워크 운영자(MNO)가 소유한 또는 그에 의해서 운영되는 유선 또는 섬유 링크(24A)를 통해서 IP 데이터그램(B)을 데이터 패킷(1223B)으로서 셀룰러 기지국(17)으로 라우팅시킨다. 이어서, IP 데이터 패킷(B)은, 셀룰러 네트워크(25)를 통해서, SDNP 페이로드를 포함하는 SDNP 데이터그램(B)을 포함하는 데이터 패킷(1223C)으로서, 셀룰러 링크(28)를 이용하는, 즉 영역 내의 모바일 네트워크 운영자에 따라 2.5G, 3G, 3.5G, 또는 4G/LTE를 이용하는, 자동차(1390A) 내의 텔레매틱스 모듈에 대해서 무선으로 통신한다. 이어서, 텔레매틱스 모듈 내에서 동작되는 SDNP 펌웨어(1335F)는 진입 데이터 패킷(1223C) 내에 임베딩된 SDNP 페이로드를 해석하여, 하이퍼보안 통신 링크를 완성한다. 따라서, 자동차 셀룰러 라스트 링크는 하이퍼보안 라스트 마일 통신의 일부로서 기능한다.

[0574] 도 35에 도시된 바와 같이, 이어서 자동차(1390A) 내의 텔레매틱스 모듈은 인포테인먼트 인터페이스(1377)에 의해서 제어되는 다양한 기능을 위해서 보안 정보를 이용한다. 내부 WiFi 핫스팟(1362D)은 또한 IP 데이터그램(B) 및 IP 데이터그램(C)를 각각 포함하는 데이터 패킷(1223B 및 1223C)을 분배한다. IP 데이터그램(B)은, SDNP 앱(1335)가 동작되는 휴대폰(32B)과 같은 임의이 SDNP 클라이언트에 대한 엔드-투-엔드 하이퍼보안 통신을 돕는 SDNP 페이로드를 포함한다. 통상적인 IP 페이로드만을 이용하는 IP 데이터그램(C)는 덜 보안적이나, 작업 디바이스는 휴대폰(32A) 및 태블릿(33A)과 같은 SDNP 클라이언트로서 동작하지 않는다. 신원 페어링은 WPA, AllJoyn 또는 다른 프로토콜을 이용하는 비-SDNP 디바이스를 위한 라스트 링크 보안을 개선하기 위해서 이용될 수 있다.

[0575] 자동차 통신에서의 다른 중요한 기능은, V2V 통신으로도 지칭되는 차량-대-차량 통신의 기능이다. V2V 통신의 목적은 주로 충돌 방지를 위한 것이다. 그러나, 본원의 개시된 SDNP 방법에 따라, V2V 통신은 또한 하이퍼보안 애드혹 피어-투-피어 네트워크로서 기능할 수 있다. 그러한 차량간 SDNP 통신이 도 36에 도시되어 있고, 여기에서 SDNP 펌웨어(1335F)가 동작되는 자동차(1390A, 1390B, 및 1390C)가 서로 그리고 SDNP 게이트웨이(1201A)에 연결된 셀룰러 기지국(17)과 피어-투-피어 네트워크를 형성한다. 차량들 사이의 통신은 IP 데이터그램 또는 SDNP 데이터그램을 이용하여 실시될 수 있다.

[0576] SNP 클라이언트 또는 게이트웨이가 비-SDNP 디바이스와 통신하는 경우에, 통신은 IP 데이터그램을 이용하여 발생된다. 예를 들어, SDNP 게이트웨이(1201A)는 SDNP 페이로드를 갖는 SDNP 데이터그램(A)을 SDNP 페이로드가 임베딩된 IP 데이터그램(B)을 포함하는 데이터 패킷(1223A)으로 변환한다. 도시된 바와 같이, 셀룰러 기지국(17)은 임베딩된 SDNP 페이로드를 갖는 IP 데이터그램(B)을 포함하는 데이터 패킷(1223B)을 이용하여 2.5G 또는 3G 셀룰러 링크(28A)에 걸쳐 자동차(1390A)에 대해서 통신하나, 임베딩된 SDNP 페이로드를 갖는 IP 데이터그램(B)을 또한 포함하는 데이터 패킷(1223C)을 이용하여 3.5G 또는 4G/LTE 셀룰러 링크(28B)에 걸쳐 자동차(1390C)에 대해서 통신할 수 있다. 이러한 방식으로, SDNP 페이로드는 데이터 패킷을 운반하기 위해서 이용되는 네트워크와 독립적으로 분배된다.

[0577] SDNP 펌웨어(1335F)로 인에이블링된 자동차가 또한 애드혹 피어-투-피어 SDNP 브릿지 또는 브릿지 네트워크를 형성할 수 있다. 예를 들어, 자동차(1390A)는, IP 데이터그램 대신, SDNP 데이터그램(C)을 포함하는 데이터 패킷(1222B)을 이용하여 V2V 라디오 링크(1391A)에 걸쳐 자동차(1390B)와 통신한다. 유사하게, 자동차(1390B)는 SDNP 데이터그램(D)을 포함하는 데이터 패킷(1222C)을 이용하여 V2V 라디오 링크(1391B)에 걸쳐 자동차(1390C)와 통신하고, IP 데이터그램에는 의존하지 않는다. 이용되는 데이터그램의 유형과 관계없이, 임베딩된 콘텐츠는

SDNP 페이로드를 이용하여 하이퍼보안을 유지한다.

[0578] SDNP 애드혹 V2V 네트워크의 다른 특징은, 터널링 기능을 실시할 수 있는, 즉 개재되는 차량이 통과 데이터를 모니터링 또는 해석할 수 없게, 하나의 차량으로부터 다른 차량으로 데이터를 전달할 수 있는 그 능력이다. 자동차(1390C)가 다른 경로와 같이 범위를 벗어나는 것으로 인해서 셀룰러 링크(28B)가 실패한 경우에, 셀룰러 기지국(17)은, 도시된 예에서 셀룰러 링크(28A), V2V 라디오 링크(1391A), 및 마지막으로 V2V 라디오 링크(1391B)를 통해서, 동일 통화자에 도달하기 위해서 SDNP 브릿지 네트워크를 이용할 수 있다. 데이터 전송 중에, 데이터 패킷(1223B, 1222B 및 1222C)은 IP 데이터그램(B)로부터 SDNP 데이터그램(C)로 그리고 최종적으로 SDNP 데이터그램(D)로 변화된다. 자동차(1390C)를 위해서 의도된 SDNP 페이로드가 목적지 자동차를 위해서 특유적으로 생성되기 때문에, 자동차(1390B) 및 그 탑승자는, 비록 애드혹 네트워크를 통한 데이터 패킷(1222B)에 의존하지만, SDNP 데이터그램(C)의 콘텐츠를 해킹 또는 모니터링할 수 없다.

[0579] 통상적인 라스트 마일 통신 이외에, 동일 SDNP 브릿지 기술을 이용하여, 장거리에 걸친 하이퍼보안 즉, 디지털 트렁크 통신으로 대량의 데이터를 송신할 수 있다. 3개의 그러한 예, 즉 마이크로파 트렁크(98), 섬유 트렁크(90), 및 위성 트렁크(95A 및 95B)가 도 37에 도시되어 있다. 이러한 기능이 SDNP 클라우드의 일부로서 간주될 수 있지만, 단일 데이터 경로는 라스트 마일 통신의 경로와 유사하고, 그에 따라 하이퍼보안을 보장하기 위해서 유사한 방법을 이용한다. 예를 들어, SDNP 소프트웨어(1335Z)가 동작되는 서버(21A 및 21B)는, SDNP 데이터그램을 포함하는 데이터 패킷(1222)을 이용하여 SDNP 펌웨어(1335W)가 동작되는 마이크로파 타워(96A 및 96B)를 경유하여 마이크로파 트렁크(98)를 통해 통신할 수 있거나, 대안적으로 서버(21A 및 21B)는 SDNP 데이터그램을 포함하는 데이터 패킷(1222)을 또한 이용하는 섬유 트렁크(98)를 통해서 직접적으로 통신할 수 있다. 글로벌 통신에서, 예를 들어 태평양 횡단 데이터 링크에서, 서버(21A 및 21B)는, 둘 모두에서 SDNP 펌웨어(1335U)가 동작되는 지구 기반의 위성 안테나(92A 및 92B)를 이용하여, 마이크로파 위성 트렁크(95A 및 95B)에 의해 SDNP 펌웨어(1335V)가 동작되는 위성(93)과 통신할 수 있다. 섬유 및 마이크로파 타워 예에서와 같이, 위성 트렁크 통신은 SDNP 데이터그램을 포함하는 데이터 패킷(1222)을 이용한다.

[0580] 결론적으로, 라스트 마일 통신에서 제공되는 보안 및 프라이버시 특징은 2개의 통신 디바이스에 따라 달라진다. 도 38은, 하단으로부터 상단까지의 순서로, 증가되는 보안 및 프라이버시를 나타내는 4개의 상이한 조합들을 대조한다. 각각의 경우에, 3개의 인자 즉, (i) 보안, 즉 코뮤니케에 대한 미인증 액세스를 방지할 수 있는 능력, (ii) ID 확인, 사용자를 인증할 수 있는 그리고 그 신원을 기초로 액세스 및 특권을 조정할 수 있는 능력, (iii) 익명성, 즉 통화자의 신원을 감시로부터 은폐할 수 있는 능력이 고려된다.

[0581] 하단 예에서, SDNP 게이트웨이(1395)는, 스니핑 가능 IP 어드레스 및 IP 페이로드를 갖는 IP 데이터그램을 포함하는 데이터 패킷(1223C)을 이용하는 어떠한 보안 규정도 없는 비-SDNP 클라이언트와 개방 통신한다. 따라서, 라스트 마일 연결은 보안되지 않고 프라이빗도 아니다. 하단에서부터 2번째 예에서, SDNP 게이트웨이(1395)는 장치 승인 및 신원 페어링의 특징을 제공하는 비-SDNP 클라이언트와 통신한다. 통신은, 스니핑 가능 IP 어드레스를 갖는 IP 데이터그램을 포함하는 데이터 패킷(1223B)에 의해서, 그러나 신원-페어링된 디바이스 만이 해독을 실시할 수 있는 암호문을 포함하는 암호화된 페이로드를 이용하여 실시된다. 통신이 프라이빗 또는 익명도 아니지만, 이는, 적어도 제한된 지속시간 동안, 향상된 보안을 제공한다.

[0582] 상단 다음의 예는, SDNP 게이트웨이(1395)가 임의의 브릿지 또는 라우터(1397)를 통해서 통신을 라우팅하고, 데이터 패킷(1223A)이 IP 데이터그램 내에서 SDNP 페이로드를 포함하기만 한다면, 하이퍼보안을 여전히 달성한다는 것을 보여준다. 달성되는 보안의 레벨은 단부 장치에 의해서만 달라지고, 라우터에 의해서는 달라지지 않는다. 상단 예에서, SDNP 어드레싱을 갖는 SDNP 데이터그램을 포함하는 데이터 패킷(1222)을 이용하는, 즉 인터넷 DNS 명칭 서버에 의해서 인식될 수 없는 소스 및 목적지 어드레스를 이용하여, 그리고 SDNP 보안 페이로드를 이용하여 SDNP 게이트웨이(1395)와 SDNP 클라이언트(1396) 사이에서 통신하는 것은 하이퍼보안이고, 우수한 보안성, 완전한 프라이버시 제공, 및 익명적인 패킷 라우팅을 제공한다.

[0583] ***하이퍼보안 라스트 마일 패킷 라우팅*** - 이용되는 계층 1 물리적 하드웨어 및 계층 2 데이터 링크 알고리즘 및 방법과 관계없이, SDNP 클라이언트 또는 SDNP-브릿지 및 SDNP 게이트웨이 사이의 패킷의 라우팅은 라스트 마일에 걸쳐 데이터 패킷을 운반 및 라우팅하기 위해서 IP 데이터그램에 의존한다. SDNP 시그널링 서버에 의해서 지향되는 SDNP 클라우드 내의 데이터 라우팅과 달리, SDNP 클라우드 또는 그 시그널링 서버는 라스트 마일을 횡단하는 IP 데이터그램을 제어하지 않는다. 따라서, 라스트 마일 전파 지연에서의 일부 가변성이 예상된다. 다행스럽게도, 라스트 마일 통신의 거리 및 가능한 경로의 수가 제한되기 때문에, 이러한 불확실성은, 글로벌 통신의 전체 엔드-투-엔드 전파 지연에 비해서 작다. 라스트 마일 변동성으로 인한 전체 전파 지연의 변동은 총 지연의

10% 미만인 것으로 추정된다.

[0584] 도 39는 고정 IP 어드레스를 이용하는 SDNP 클라이언트(1400)와 SDNP 게이트웨이(1401) 사이의 단일 경로 라스트 마일 통신을 도시한다. IP 데이터그램(1405)은 $M_{0,0}$(SDNP 게이트웨이)의 IP 목적지 어드레스, 및 SDNP 클라이언트인, 데이터 패킷의 소스($C_{1,1}$)의 IP 어드레스를 포함한다. 라스트 링크 통신은 라우터(1402A)에 대한 단일 경로(1404)를 통해서 발생된다. 데이터는 임의의 수의 라우터(R), 예를 들어 라우터(1402B)를 통해서 SDNP 게이트웨이($M_{0,0}$)로 라우팅된다.

[0585] 라스트 마일 네트워크 연결의 대안적인 도면은, PHY, 데이터 링크, 및 OSI 계층, 1, 2 및 3으로서의 네트워크 연결을 나타내는 IP 스택으로서의 각각의 통신 디바이스를 도시한다. 예를 들어, 도 40a는 고정 IP 어드레스를 이용한 단일-루트 라스트 마일 하이퍼보안 통신의 개략적 IP 스택 도면이다. 따라서, SDNP 클라이언트($C_{1,1}$)를 포함하는 클라이언트 디바이스는, 라우터(1402A 및 1402B)를 통해서 SDNP 게이트웨이($M_{0,0}$)를 포함하는 SDNP 게이트웨이(1401)를 갖는 단일 경로 라스트 마일 연결(1409)을 구축하고, 여기에서 라우터(1402A)는 WiFi 라우터를 포함하고 라우터(1402B)는 이더넷 라우터이다. 클라이언트 디바이스(1400)는 라스트 링크(1404)를 통해서 라우터(1402A)에 연결되고, 여기에서 클라이언트 IP 스택(1411)의 PHY 계층 1 물리적 연결 및 상응 데이터 링크 계층 2는 라우터 IP 스택(1412A) 내의 상응 계층 1 및 계층 2에 연결된다.

[0586] 다시, 라우터(1402A)는 이더넷을 이용하여 라우터(1402B)에 연결되고, 여기에서 WiFi 라우터의 IP 스택(1412A)의 PHY 계층 1 물리적 연결 및 상응 데이터 링크 계층 2는 이더넷 라우터 IP 스택(1402B) 내의 상응 계층 1 및 계층 2에 연결된다. 마지막으로, 라우터(1402B)는 이더넷을 이용하여 SDNP 게이트웨이 서버(1401)에 연결되고, 여기에서 이더넷 라우터의 IP 스택(1412B)의 PHY 계층 1 물리적 연결 및 상응 데이터 링크 계층 2는 게이트웨이의 IP 스택(1412B) 내의 상응 계층 1 및 계층 2에 연결된다. 동작 시에, 라우터는 방해 없이 데이터를 운반하고, 그에 따라 네트워크 계층 3 IP 데이터그램은 하나의 IP 스택으로부터 다른 스택으로, 구체적으로 IP 스택(1411) 내의 계층 3으로부터 IP 스택(1412A, 1412B)으로 그리고 최종적으로 IP 스택(1422)까지 투과적으로 흐른다. 이러한 방식으로, 데이터가 다수의 디바이스를 통해서 물리적으로 통과할 때에도, 네트워크는 IP 데이터그램을 단일 경로 데이터로서 가상의 라스트 마일 연결(1409)에 걸쳐 운반한다.

[0587] 다시 말해서, 계층 3 네트워크 데이터는 IP 데이터그램을 운반하기 위해서 이용된 물리적 연결과 독립적으로 라스트 마일을 통해서 흐르고, 즉 계층 3 라스트 마일 통신은 데이터 전달을 위해서 이용되는 기본적인 계층 1 및 계층 2 구현예에 대해서 불가지론적으로 동작된다. 도 40b에 도시된 바와 같이 개략도로부터 중간 노드를 제거함으로써, 이러한 원리는 단순화된 형태로 표시될 수 있고, 여기에서 통신 IP 스택(1411 및 1422)을 포함하는 클라이언트 디바이스(1400) 및 SDNP 게이트웨이 서버(1401)가 상응하는 컴퓨팅 및 데이터 저장 기능(1410 및 1421)으로 그리고 그로부터 데이터를 전송한다. IP 데이터그램(1405)은, 데이터 패킷 전달 프로세스에서 사용된 라우터의 수 또는 미디어와 관계없이, 라스트 마일 연결(1409)에 걸쳐 흐른다. 그에 따라, 라스트 마일은 "데이터 구성"으로서 간주될 수 있고, 즉 IP 데이터그램을 디바이스들 사이에서 운송하는 임의의 그리고 모든 물리적 수단을 의미하는 것으로 추상적 개념으로 간주될 수 있다. 그러나, 라스트 링크는 그 이상의 물리적 의미를 갖는데, 이는 통화자의 연결된 디바이스가, 구축될 수 없는 통신 링크의 업스트림 라우터에 대해 연결될 수 있어야 하기 때문이다. 예를 들어, 통화자가 WiFi 연결만을 갖는 태블릿 컴퓨터를 갖고 WiFi를 갖춘 카페에 앉아 있는, 그러나 통화자가 WiFi 네트워크에 대한 WPA 암호를 갖지 않은 경우에, 라스트 링크는 형성될 수 없고, 통화자는 라스트 마일에, SDNP 클라우드에 연결할 수 없고, 또는 통화를 위치시킬 수 없다.

[0588] 라스트 마일 통신의 다른 고려사항은, IP 데이터그램(1405)의 페이로드가, 전송 계층 4 데이터, 세션 계층 5 데이터, 프레젠테이션 계층 6 데이터, 및 애플리케이션 계층 7 데이터를 포함하는, 상부 OSI 계층을 위한 모든 정보를 포함한다는 것이다. UDP 또는 TCP 전송 프로토콜을 선택하는데 필요한 계층 4 데이터 이외에, IP 데이터그램의 페이로드 내의 남은 데이터는 공개된 SDNP 통신에 대해서 특정되고, 스스로가 SDNP 소프트웨어 또는 펌웨어를 동작시키지 않는 한, 라스트 마일을 따라 동작되는 라우터에 의해서 해석될 수 없다. 따라서, 비록 라스트 마일 네트워크 자체가 상이한 디바이스들, 캐리어들, 및 네트워크 운영자들의 혼합을 포함할 수 있지만, 단부 디바이스만이, 즉 통화자 또는 SDNP 클라이언트 및 SDNP 게이트웨이만이 라스트 마일 통신을 해석할 수 있다.

[0589] 비록 SDNP 페이로드가, 스크램블링, 단편화, 정크 데이터 삽입 및 삭제, 포맷팅에 의존하는 상태, 및 동적 암호화를 포함하는 수 많은 비밀에 의해서 보안되지만, 라스트 마일 네트워크를 통과하는 IP 데이터그램의 IP 어드레스는 필수적으로 클라이언트 디바이스(1400) 및 SDNP 게이트웨이 서버(1401)의 소스 및 목적지 어드레스를 노출시킨다. 라스트 마일에 걸친 익명성의 정도를 제공하기 위해서, 어드레스 기만이 유리하고, 즉 IP 데이터그램

내의 소스 및 목적지 어드레스를 동적으로 변화시켜 사이버-공격자를 엉뚱한 곳으로 유도한다. IP 기만은, 본원에서 "동적 클라이언트 어드레싱"으로 지칭되는, 통화자의 연결 디바이스의 IP 어드레스를 동적으로 변경함으로써, 또는 다수의 SDNP 게이트웨이와 통신함으로써, 즉 다중-경로 라스트 마일 통신에 의해서 달성된다.

[0590] 설명된 IP 어드레스 기만의 제1 방법은 순차적인 데이터 패킷의 소스 어드레스를 동적으로 변경하는 것을 포함한다. 도 41에 도시된 바와 같이, 성공적으로 전송된 IP 데이터그램(A, B, 및 C)은 3개의 상이한 소스 어드레스를 포함한다. 구체적으로, IP 데이터그램(A)(1405A)는 IP 소스 어드레스($C_{1,1}$)를 포함하고, IP 데이터그램(B)(1405B)은 IP 소스 어드레스($C_{1,2}$)를 포함하며, IP 데이터그램(C)(1405C)은 IP 소스 어드레스($C_{1,3}$)를 포함한다. 그에 따라, 비록 라우터(1402A)에 진입하는 패킷 모두가 SDNP 클라이언트(1400)으로부터 나오지만, 클라이언트 소스 어드레스($C_{1,n}$)가 동적으로 변화되어, 진정한 IP 어드레스를 혼동시키고 하나 초과의 통신 디바이스가 있는 것으로 보이게 한다. 커레이드(charade)를 완성하기 위해서, 통신 디바이스의 MAC 어드레스가 또한 동적 소스 어드레스와 함께 상응하게 변화되어야 한다.

[0591] 이러한 방법이 도 42a에서 IP 스택을 이용하여 도시되며, 여기에서 디바이스(1400, 1402A, 1402B, 1401)는 WiFi 및 이더넷을 이용하여 상응하는 IP 스택(1411N, 1412A, 1412B, 및 1422)을 통해서 통신하나, SDNP 클라이언트의 네트워크 계층 3 신원은 다수 IP 어드레스($C_{1,1}$, $C_{1,2}$, 및 $C_{1,3}$)를 포함한다. 결과적으로, 도 42b에 도시된 라스트 링크의 개략도에서 도시된 바와 같이, 라우터(1402A)에 진입하는 순차적인 데이터 패킷은, 하나가 아니라, 3개의 상이한 클라이언트 디바이스로부터 송신되는 것으로 보인다. 공유된 PHY 층은 WiFi 표준 주파수를 포함하고, 디바이스들을 연결하는 데이터 링크 계층은 802.11ac 또는 802.11n과 같은 규정된 표준을 따른다.

[0592] 네트워크 연결(1408)을 따라 라우터 디바이스(1402)에 송신된 IP 데이터그램(1405N)은 고정 목적지 IP 어드레스 IP $M_{0,0}$ 및 IP $C_{1,n}$ 으로서 수학적 표시로 표현된 순차적 소스 어드레스 IP $C_{1,1}$, IP $C_{1,2}$, IP $C_{1,3}$, 등을 포함하고, 여기에서 n = 1, 2, 3, ...으로서 각각의 순차적인 패킷을 특유하게 식별한다. 각각의 순차적인 IP 패킷은 또한 상응하는 페이로드(SDNP 1, SDNP 2, SDNP 3, 및 기타)를 포함한다. 비록 본 설명이 수학적 약어 표기 IP $C_{1,n}$을 이용하여 각각의 IP 어드레스를 인용하고 있지만, IP 어드레스가 IPv4 또는 IPv6의 국제 표준에 따라 만들어진 실제 IP 어드레스를 포함하고 임의의 보전된 IP 어드레스를 배제한다는 것을 이해하여야 한다는 것에 주목하여야 한다.

[0593] 보안성을 향상시키기 위한 다른 선택사항은 라스트 마일에서 다중경로 패킷 전송을 이용하는 것이다. SDNP 클라우드 내의 데이터 전송과 유사한 방식으로, 다중경로 라스트 마일 통신에서, 오디오 및 순차적 데이터가 파싱되고 단편화되며, 이어서 분리된 패킷들로 분할되고 상이한 SDNP 게이트웨이들로 어드레스된다. 고정 IP 어드레스를 이용하는 다중경로 데이터 전송의 예가 도 43에 도시되어 있고, 여기에서 SDNP 클라이언트(1400)는 다중 게이트웨이(1401A, 1401B, 및 1401C)와 통신한다. 도시된 바와 같이, 제1 데이터 패킷(1405A)은 IP 소스 어드레스($C_{1,1}$) 및 목적지 어드레스($M_{0,0}$)을 갖는 페이로드 SDNP(1)을 포함한다. 이어서, 데이터 패킷(1405A)은 라스트 링크(1404A)를 경유하여 라우터(1402A 및 1402B)를 통해 SDNP 게이트웨이(1401A)로 라우팅된다. 유사한 방식으로, 제2 데이터 패킷(1405B)은 IP 소스 어드레스($C_{1,1}$) 및 목적지 어드레스($M_{0,1}$)을 갖는 페이로드 SDNP(2)를 포함한다. 이어서, 데이터 패킷(1405B)은 라스트 링크(1404B)를 경유하여 라우터(1402C)를 통해 SDNP 게이트웨이(1401B)로 라우팅된다. 제3 데이터 패킷(1405C)은 IP 소스 어드레스($C_{1,1}$) 및 목적지 어드레스($M_{0,3}$)를 갖는 페이로드 SDNP(3)를 포함한다. 이어서, 데이터 패킷(1405C)은 라스트 링크(1404C)를 경유하여 라우터(1402D 및 1402E)를 통해 SDNP 게이트웨이(1401C)로 라우팅된다.

[0594] 도시된 클라이언트 디바이스(1400)과 3개의 게이트웨이(1401A, 1401B 또는 1401C) 중 하나 사이의 통로에서, IP 데이터그램은 다수의 라스트 링크(1404A, 1404B, 및 1404C)를 통해서 다수의 라우터(1402A, 1402B, 및 1402C)로 라우팅된다. 이러한 라우터는 (i) WiFi 또는 이더넷과 같은 동일한 물리적 미디어를 이용하는 완전히 독립적인 라우터, (ii) 공통 하드웨어 디바이스 내의 다수의 라우터 채널, 예를 들어 DOCSIS3 케이블 모뎀 내의 다수의 트렐리스 채널 또는 (iii) 통신을 위한 상이한 물리적 미디어, 예를 들어 WiFi를 통해 라우팅된 하나의 물리적 미디어, 3G를 통한 다른 물리적 미디어, 등을 포함할 수 있다.

[0595] 예를 들어, 도 44a는, 고정 IP 어드레스를 이용한 공통 PHY 라스트 링크(1404)를 통한 전술한 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택 도면을 도시한다. 동작에서, SDNP 클라이언트($C_{1,1}$)는, 공통 PHY, 데이터 링크, 및 네트워크 계층을 이용하여, 단일 디바이스 연결로서 라우터(1401A, 1402B, 및 1402C)와 통신한다. 어드레스

기만은 고정 클라이언트 어드레스 IP $C_{1,1}$를 포함하는, 그러나 변화되는 SDNP 게이트웨이 어드레스 IP $M_{0,0}$, IP $M_{0,1}$, 및 IP $M_{0,3}$를 갖는, 연속적인 IP 데이터그램들을 이용하여 실시된다. 패킷의 잘못된 지향은 알고리즘적으로 또는 무작위적으로 발생될 수 있다. 예를 들어, 클라이언트 디바이스(1400)으로부터 송신된 데이터그램 중 10번째 마다의 데이터그램이 SDNP 서버(1401C)로 지향되는 경우에, 클라이언트 디바이스(1400)으로부터의 10번째 진출 데이터그램은 목적지 어드레스 IP $M_{0,3}$ 및 소스 IP 어드레스 IP $C_{1,1}$을 포함할 것이다. SDNP 게이트웨이 서버(1401C)로부터의 응답은 반대 통로에서, 즉 소스 IP 어드레스 IP $M_{0,3}$ 및 목적지 어드레스 IP $C_{1,1}$을 갖는 통로에서, 클라이언트 디바이스(1400)으로 복귀된다.

[0596] 도시된 바와 같이, 클라이언트 디바이스(1400)와 라우터(1402A, 1402D, 및 1402C) 사이의 PHY 및 데이터 링크는 단일 미디어, 예를 들어 WiFi를 포함한다. 비록 라스트 링크 연결이 3개로 분할되는 단일 라인으로 표시되었지만, 물리적 연결이 팽행 와이어들을 생성하기 위해서 이용되는 전기적 Y 연결이 아니라 점-대-점으로 모두 만들어진다는 것을 이해하여야 한다. 그 대신, 도면은, 연결이 연결의 효과를 나타내고, 즉 클라이언트 IP 스택(1411)의 PHY 계층이 하나의 PHY 연결을 3개로 연장시키고, 즉 IP 스택(1412A, 1412C, 및 1412D)의 PHY 층에 연결되는 것을 의미한다. 기능적으로, 이러한 라스트 링크는 3개의 입력 확장기에 대한 단일 입력으로서 동작하고, 여기에서, 라우터 기능이 하나의 공통 전자 장치에 포함되든지 또는 구분되고 분리된 라우터들 내로 나누어지는지의 여부와 관계없이, 하나의 클라이언트는 3개의 라우터 기능에 연결된다. 도시된 바와 같이, 라스트 링크(1404)가 단일 유형의 통신 미디어 - 케이블, 섬유, WiFi, 이더넷, 또는 셀룰러 - 를 구성한다는 것을 주목하여야 한다.

[0597] 그러나, 라스트 마일의 나머지 부분이, 반드시 라스트 링크와 동일하지는 않은, 임의의 미디어를 포함할 수 있다. 대안적인 라스트 링크는 독립적인 라우터들에 연결되는 다수의 상이한 PHY 계층들을 포함한다. 그러한 구현예인, 다수의 PHY 라스트 링크에 걸쳐 고정 IP 어드레스를 이용하는 다중-경로 라스트 마일 하이퍼보안 통신을 실행하는 IP 스택이 도 44b에 도시되어 있다. 구체적으로, 클라이언트 디바이스(1400)는, 고정 클라이언트 어드레스 IP $C_{1,1}$을 갖는 공통 네트워크 계층 3 인터페이스를 이용하여, 그러나 IP 스택(1411A, 1411B, 및 1411C)에 의해서 표시된 분리되고 구분된 계층 1 및 계층 2 인터페이스를 이용하여 동작된다. 동작 시에, IP 스택(1411A)은, 라우터(1402B)를 횡단하는 소스 어드레스 IP $C_{1,1}$ 및 목적지 어드레스 IP $M_{0,0}$을 포함하는 IP 데이터그램을 지향시키는 라스트 링크(1404A)에 걸쳐 라우터(1402A)에 연결된다. 유사하게, IP 스택(1404B)은, 소스 어드레스 IP $C_{1,1}$ 및 목적지 어드레스 IP $M_{0,1}$을 포함하는 IP 데이터그램을 지향시키는 라스트 링크(1404B)에 걸쳐 라우터(1402C)에 연결된다. IP 스택(1411C)은, 라우터(1402E)를 횡단하는 소스 어드레스 IP $C_{1,1}$ 및 목적지 어드레스 IP $M_{0,3}$을 포함하는 IP 데이터그램을 지향시키는 라스트 링크(1404C)에 걸쳐 라우터(1402D)에 연결된다.

[0598] 동적 소스 어드레싱 및 다중경로 데이터 전송의 조합이 도 45에 도시되어 있고, 여기에서 SDNP 클라이언트(1400)는 동적 소스 어드레스를 이용하여 다중 게이트웨이(1401A, 1401B, 및 1401C)와 통신한다. 이러한 방법에서, 제1 데이터 패킷(1405A)은 동적 IP 소스 어드레스($C_{1,1}$) 및 목적지 어드레스($M_{0,0}$)을 갖는 페이로드 SDNP(1)을 포함한다. 이어서, 데이터 패킷(1405A)은 라스트 링크(1404A)를 경유하여 라우터(1402A 및 1402B)를 통해 SDNP 게이트웨이(1401A)로 라우팅된다. 유사한 방식으로, 제2 데이터 패킷(1405B)은 동적 IP 소스 어드레스($C_{1,2}$) 및 목적지 어드레스($M_{0,1}$)을 갖는 페이로드 SDNP(2)를 포함한다. 이어서, 데이터 패킷(1405B)은 라스트 링크(1404B)를 경유하여 라우터(1402C)를 통해 SDNP 게이트웨이(1401B)로 라우팅된다. 제3 데이터 패킷(1405C)은 동적 IP 소스 어드레스($C_{1,3}$) 및 목적지 어드레스($M_{0,3}$)를 갖는 페이로드 SDNP(3)를 포함한다. 이어서, 데이터 패킷(1405C)은 라스트 링크(1404C)를 경유하여 라우터(1402D 및 1402E)를 통해 SDNP 게이트웨이(1401C)로 라우팅된다.

[0599] 따라서, 각각의 연속적인 데이터 패킷은 변화되는 SDNP 페이로드를 포함하고, 동적으로 변화되는 소스 어드레스를 이용하고, 상이한 라스트 링크를 통해서 특이적 SDNP 게이트웨이에 라우팅된다. 트렐리스 인코딩을 갖는 DOCSIS3 케이블 모뎀과 같은 다수의 IP 입력을 갖는 단일 라우터인, 다수의 라스트 링크, 즉 라스트 링크(1404A, 1404B, 및 1404C)를 통해서, 또는 다수 형태의 미디어를 통해서, 예를 들어 다수의 WiFi의 대역을 통해서, 데이터를 전송하기 위해서, 라디오 및 WiFi의 조합 또는 와이어라인과 무선 통신의 다른 조합이 이용된다. 일 예에서, 도 46a는 단일 PHY 라스트 링크(1404)를 통한 동적 클라이언트 IP 어드레스를 이용한 다중-루트 라스트 마일 하이퍼보안 통신의 IP 스택을 도시한다. 클라이언트 디바이스(1400)는, IP 스택(1411A)에서 도시된 계층 1 및 계층 2 통신을 포함하는 공유형 물리적 인터페이스를 도시한다. 네트워크 계층 3에서, IP 스택

(1411A)은 SDNP 게이트웨이 $M_{0,0}$으로 지향된 클라이언트 어드레스($C_{1,1}$)를 생성하고, IP 스택(1411B)은 SDNP 게이트웨이 $M_{0,1}$으로 지향된 클라이언트 어드레스($C_{1,2}$)를 생성하고, IP 스택(1411C)은 SDNP 게이트웨이 $M_{0,3}$으로 지향된 클라이언트 어드레스($C_{1,3}$)를 생성한다.

[0600] 도 46b의 IP 스택 도면에 도시된 바와 같이, 동일한 다중-경로 접근방식이 동적 클라이언트 어드레싱 및 다수의 PHY 라스트 계층과 조합될 수 있다. 도시된 바와 같이, 클라이언트 디바이스(1400)는, 상응 IP 어드레스 IP $C_{1,1}$, IP $C_{1,2}$, 및 IP $C_{1,3}$ 을 갖는 IP 데이터그램을 상응 라스트 링크(1404A, 1404B, 및 1404C)를 통해서 IP 어드레스 IP $M_{0,0}$, IP $M_{0,1}$, 및 IP $M_{0,3}$를 갖는 SDNP 게이트웨이에 전송하는 3개의 IP 스택(1411A, 1411B, 및 1411C)를 포함한다.

[0601] 많은 경우에, 라스트 링크는 단일 경로를 포함하고, 여기에서 제1 라우터를 넘어서 다중경로 데이터 전송이 이용된다. 도 47에서, SDNP 클라이언트(1400)는 라스트 링크(1404)를 통해서 단일 라우터(1402A)와 통신한다. 라우터(1402A)를 넘어서, 데이터 패킷은 동적 소스 어드레스를 이용하여 다수의 게이트웨이(1401A, 1401B, 및 1401C)로 지향된다. 이러한 구현예에서, 제1 데이터 패킷(1405A)은 동적 IP 소스 어드레스($C_{1,1}$) 및 목적지 어드레스($M_{0,0}$)을 갖는 페이로드 SDNP(1)을 포함한다. 데이터 패킷(1405A)은 라스트 링크(1404)를 경유하여 그리고 라우터(1402A 및 1402B)를 통해 SDNP 게이트웨이(1401A)로 라우팅된다.

[0602] 유사한 방식으로, 제2 데이터 패킷(1405B)은 동적 IP 어드레스($C_{1,2}$) 및 목적지 어드레스($M_{0,1}$)을 갖는 페이로드 SDNP(2)를 포함한다. 데이터 패킷(1405B)은 라스트 링크(1404)를 경유하여 그리고 라우터(1402A 및 1402C)를 통해 SDNP 게이트웨이(1401B)로 라우팅된다. 제3 데이터 패킷(1405C)은 동적 IP 소스 어드레스($C_{1,3}$) 및 목적지 어드레스($M_{0,3}$)를 갖는 페이로드 SDNP(3)를 포함한다. 데이터 패킷(1405C)은 라스트 링크(1401)를 경유하여 그리고 라우터(1402A, 1402D 및 1402E)를 통해 SDNP 게이트웨이(1401C)로 연속해서 라우팅된다. 따라서, 각각의 연속적인 데이터 패킷은 변화되는 SDNP 페이로드를 포함하고, 동적으로 변화되는 소스 어드레스를 이용하고, 공통 라스트 링크를 통해서 특이적 SDNP 게이트웨이에 라우팅된다.

[0603] 이러한 라스트 마일 연결은 도 48에서 IP 스택을 이용하여 도시되고, 여기에서 라우터(1402A)만을 갖는 라스트 링크(1404)를 갖는 SDNP 클라이언트 디바이스(1400) 내의 IP 스택(1411)은, 네트워크 계층(3)에서 데이터 패킷을, 3개의 상이한 네트워크 어드레스들, 구체적으로 IP $C_{1,1}$, IP $C_{1,2}$, IP $C_{1,3}$을 포함하는 스택(1412A)에 송신한다. 따라서, 실제로 단일 클라이언트를 포함하지만, 클라이언트 디바이스(1400)는 라우터(1402A)에게 3개의 분리된 클라이언트로서 보인다. IP 데이터그램이 라우터(1402A)에 도달하면, IP 데이터그램은 분할되고 상이한 목적지 게이트웨이로의 상이한 경로들을 취한다. 소스 어드레스 IP $C_{1,1}$를 갖는 패킷은, 예를 들어, 라우터(1402B)를 통해서 목적지 IP $M_{0,0}$로 라우팅될 수 있고, 소스 어드레스 IP $C_{1,2}$를 갖는 패킷은 라우터(1402C)를 통해서 목적지 IP $M_{0,1}$로 라우팅될 수 있고, 그리고 소스 어드레스 IP $C_{1,3}$를 갖는 패킷은 라우터(1402D 및 1402E)를 통해서 목적지 IP $M_{0,3}$으로 라우팅될 수 있다. 주어진 동적 클라이언트 어드레스($C_{1,n}$)를 갖는 데이터 패킷을 특정 SDNP 게이트웨이로 지향시키기 위한 라우팅 테이블은 미리-고정되지 않고 동적으로 달라질 수 있다. IP 어드레스는 패킷별 기반으로 할당될 수 있고, 분명하게 관련 없는 데이터 패킷들이 2개의 통화자들 사이의 단일의 단편화된 통신의 부분 모두라는 사실을 더 혼란스럽게 한다.

[0604] ***라스트 마일 라우팅의 물리적 실현*** - 라스트 마일의 물리적 실현은, 이더넷, WiFi, 셀룰러, 또는 DOCSIS3 인에이블드 케이블 또는 섬유 링크를 포함하는, 다양한 미디어를 통한 통신을 포함할 수 있다. 사용되는 미디어와 관계없이, 라스트 마일에 걸친 데이터 패킷의 라우팅은 이하의 3개의 변수에 의해서 주로 제어된다:

[0605] * 통신 디바이스의 미디어 액세스 제어(MAC) 어드레스,

[0606] * IP 데이터그램의 소스 IP 어드레스,

[0607] * IP 데이터그램의 목적지 IP 어드레스.

[0608] 따라서, MAC 어드레스는 라스트 마일 통신에서 각각의 홉, 즉 계층 1 및 계층 2를 정보를 실시하기 위해서 이용되는 물리적 미디어를 제어하는 한편, IP 어드레스는 클라이언트 디바이스 및 SDNP 게이트웨이 즉, 라스트 마일의 2개의 단부에 위치되는 디바이스를 식별한다. 비록, 하이퍼보안 통신에서 사용된 페이로드가 보안 동적 통신 네트워크 및 프로토콜에 따라 규정된 프로토콜을 따르지만, 라스트 마일 내의 중간 디바이스, 즉 클라이언트 디

바이스와 게이트웨이 사이의 패킷의 경로 상의 라우터 및 다른 디바이스는 일반적으로 SDNP 기능을 실행하도록 인에이블링되지 않는데, 이는 그러한 디바이스 내에 SDNP 실행 가능 코드가 없기 때문이다. 그에 따라, SDNP 페이로드는 라스트 마일 하이퍼보안 데이터 패킷의 라우팅과 관련이 없다.

[0609] 하나의 예는 라스트 마일 통신을 위한 이더넷의 이용이다. SDNP 라스트 마일 통신을 위해서 도 9e에서 전술한 이더넷 데이터 패킷의 적응에서, 도 49는 SDNP 페이로드를 수반하는 이더넷 통신을 위한 IPv4 및 IPv6 데이터그램의 도식적 도면이다. 도시된 바와 같이, 계층 1 이더넷 패킷(188)은 데이터 프레임 헤더, 즉 프리앰블(180), SFD(start frame delimiter)(181), 및 계층 2 이더넷 패킷(189)을 포함한다. 이더넷 패킷(189)은 목적지 및 소스 MAC 어드레스(182 및 183), VLAN 구현을 위한 선택적인 802.1Q 태그(184), 이용되는 데이터 링크의 유형을 특정하기 위해서 이용되는 이더넷 필드(185)(이더넷 II 또는 IEEE802.3에 따른 길이 제원), 그리고 전체 데이터 링크 패킷의 32-비트 CRC 체크섬을 포함하는 프레임 체크(186)를 포함한다. 이더넷 패킷(189)은 또한, IP 데이터그램의 SDNP 콘텐츠(1430)를 캡슐화하기 위해서 이용되는 가변 길이 MAC 페이로드(187)를 포함한다.

[0610] 구체적으로, MAC 페이로드(187)는, 전송-헤더(436) 및 SDNP 페이로드(1430)를 포함하는 IP 헤더(434) 및 IP 페이로드(435)를 포함한다.

[0611] IP 헤더(434)는, 이진법 4를 포함하는 프로토콜 필드(447) 또는 이진법 6을 포함하는 프로토콜 필드(448)에 의해서 결정되는 바와 같은 IPv4 또는 IPv6을 IP 데이터그램이 따르는지의 여부에 따라서 달라진다. 프리앰블(440 및 444) 모두는, 이용되는 계층 4 전송 방법, 예를 들어 TCP, UDP 또는 유지 기능 ICMP 및 IGMP을 결정하기 위해서 이용되는 전송 헤더 플래그(470)를 포함한다. 구체적으로, 보안 동적 통신 네트워크 및 프로토콜에 따라, TCP 운송이 소프트웨어 및 데이터 파일을 위해서 이용되는 한편, UDP는 VoIP 및 비디오와 같은 실시간 데이터를 위해서 이용된다. 전송 헤더(436)의 길이 및 포맷은 전송 헤더(470)에 따라 달라진다. IP 헤더(434)는 IPv4 소스 및 목적지 어드레스(441 및 442) 또는 IPv6 소스 및 목적지 어드레스(445 및 446)를 포함한다.

[0612] 이더넷 패킷의 라스트 마일 라우팅은, IP 또는 MAC 어드레스가 언급하는 디바이스의 예시적인 명칭, 예를 들어 MAC $C_{1,1}$ 또는 IP $M_{0,0}$에 의해서 표시되는, IP 어드레스 및 MAC 어드레스 모두에 따라 달라진다. 이더넷 포맷된 인터넷 프로토콜에 따라 만들어진 수치적 어드레스를 나타내는 상징적인 명칭이, 간결함을 위해서, 수치적 어드레스 대신 사용된다. IP 어드레스 IP $C_{1,1}$이 상이한 포맷들을 따라고 IPv4 및 IPv6 명칭에 대해서 상이한 바이트의 수를 이용한다는 것을 주목하여야 한다. 또한, MAC 어드레스를 위한 포맷은 이용되는 계층 2 데이터 링크 프로토콜에 따라 달라진다. 따라서, 셀룰러 라디오를 위한 MAC 어드레스 MAC $C_{1,1}$는 WiFi 또는 이더넷을 이용하여 통신하는 동일한 디바이스에 대한 MAC 어드레스와 동일하지 않다. MAC 어드레스는 IP 어드레스와 관계가 없으며, 즉 동일 클라이언트를 위한 IP 어드레스 및 MAC 어드레스는 관계가 없다.

[0613] 이더넷 패킷의 순차적인 라스트 마일 라우팅이 도 50a 내지 도 50d의 예에서 도시되어 있다. 각각의 도면은 2개의 이더넷 패킷 - IPv4 데이터그램을 포함하는 상단의 이더넷 패킷 및 IPv6 데이터그램을 포함하는 하부의 이더넷 패킷 - 을 포함한다. IPv4 및 IPv6이 필드 길이가 다른 상이한 포맷들을 이용하기 때문에, 도시된 2개의 이더넷 패킷은, 동일한 페이로드를 수반할 때에도, 일반적으로 동일한 길이가 아니다. 통신 시퀀스의 제1 단계에서, SDNP 페이로드(A)는 라스트 링크(1404)를 통해서 SDNP 클라이언트(1400)로부터 라우터(1402A)로 그리고 이어서 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)로 이동된다. SDNP 게이트웨이로부터 클라이언트로의 응답은, 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)로부터 라우터(1402A)로 그리고 이어서 라스트 링크(1404)를 통해서 클라이언트(1400)로 이동되는 SDNP 페이로드(G)를 포함한다. SDNP 클라이언트(1400)는 수치적 MAC 및 IP 어드레스 MAC $C_{1,1}$ 및 IP $C_{1,1}$를 가지고, 라우터(1402A)는 수치적 MAC 어드레스 MAC R를 가지며, SDNP 게이트웨이는 수치적 MAC 및 IP 어드레스 MAC $M_{0,0}$ 및 IP $M_{0,0}$를 갖는다. 라우터(1402A)의 IP 어드레스는 데이터 패킷에서 사용되지 않는다.

[0614] SDNP 데이터그램 패킷 라우팅이 SDNP 네트워크에 의해서 완전히 제어되는 SDNP 클라우드에서와 달리, IP 데이터그램을 이용하는 라스트 마일 통신에서, SDNP 페이로드는 해석될 수 없거나 라우팅에 영향을 미칠 수 없고, 이는 라스트 마일에 걸쳐 운반되는 각각의 통신이 고정 소스 및 목적지 IP 어드레스를 포함한다는 것을 의미한다. 이더넷 패킷을 지향시키기 위해서 이용되는 물리적 미디어 또는 채널은 라스트 마일 내의 각각의 통신 노드를 연결하는 MAC 어드레스에 의해서 통제된다. 예를 들어, 도 50a는, 소스 MAC 어드레스 MAC $C_{1,1}$, 목적지 MAC 어드레스 MAC R, 소스 IP 어드레스 IP $C_{1,1}$, 목적지 어드레스 IP $M_{0,0}$ 및 SDNP 페이로드를 포함하는 라우터(1402A)로 라우팅하는 단일 PHY를 위해서 이용되는 IPv4 및 IPv6 라스트 링크 이더넷 패킷을 도시한다. 도 50b는 게이트웨

이 링크(1414)에 걸쳐 SDNP 페이로드(A)를 운반하는 상응 이더넷 패킷을 도시한다. 설명된 바와 같이, 소스 및 목적지 IP 어드레스는 IP $C_{1,1}$ 및 IP $M_{0,0}$에서 변화되지 않고 유지되는 반면, MAC 소스 및 목적지 어드레스는 그 원래의 값으로부터 MAC R 및 MAC $M_{0,0}$로 변화된다.

[0615] SDNP 게이트웨이(1401)로부터 클라이언트(1400)로의 응답 통신에서, SDNP 페이로드(G)는 응답 시퀀스에서 동일 네트워크를 횡단하고, 즉 소스 및 목적지 어드레스가 스왑된다. 도 50c에 도시된 바와 같이, 소스 및 목적지 IP 어드레스는 IP $M_{0,0}$ 및 IP $C_{1,1}$을 각각 포함하는 한편, MAC 어드레스는 소스 어드레스 MAC $M_{0,0}$ 및 목적지 MAC R을 포함한다. 도 50d에 도시된 라스트 링크 통신에서, 맥 어드레스는 소스 어드레스 MAC R 및 목적지 MAC $C_{1,1}$로 변화되는 반면, 소스 및 목적지 IP 어드레스는 IP $M_{0,0}$ 및 IP $C_{1,1}$로 변화되지 않는다.

[0616] SDNP 클라이언트로부터 라스트 마일 통신을 나타내기 위한 하나의 편리한 수단은, 소스 및 목적지 MAC 어드레스, 소스 및 목적지 IP 어드레스, 및 SDNP 페이로드를 포함하는 데이터 필드를 포함하는 "축약형" 데이터 패킷을 이용하는 것이다. 축약 형태는, 라스트 마일을 가로질러 SDNP 게이트웨이로 전달되는 연속적인 데이터 패킷 및 그 응답을 구성하는, 임의의 통신 "세션"에서 데이터 흐름을 설명하기 편리하다. 예를 들어, SDNP 클라이언트로부터 SDNP 게이트웨이로 송신된 (축약 형태로 도시된) 연속적인 이더넷 패킷이 도 51a의 상단 부분에 도시되어 있다. 각각의 행은 SDNP 페이로드(A, B 및 C)를 포함하는 연속적인 데이터 패킷을 나타낸다 가장 좌측의 열은 라스트 링크 내의 데이터 패킷을 도시하는 한편, 우측 열은 게이트웨이 링크에 걸쳐 동일 페이로드를 운반하는 데이터 패킷을 도시한다. 도시된 바와 같이, 모든 패킷은 소스 IP 어드레스로서 IP $C_{1,1}$를 그리고 목적지 IP 어드레스로서 IP $M_{0,0}$를 특정한다. IP 어드레스의 하나의 쌍 만이 이용되기 때문에, 라스트 마일은 본원에서 SDNP 단일 경로 라스트 마일 통신으로 지칭된다. 또한, 연속적인 데이터 패킷을 운반하기 위해서 SDNP 클라이언트(1400)에 의해서 이용되는 소스 IP 어드레스가 변화되지 않기 때문에, 라스트 링크는 "고정 클라이언트 어드레싱"을 이용한다.

[0617] 이웃에 대한 각각의 통신 노드들 사이의 계층 2 상호 연결을 돕기 위해서, 라스트 마일의 상이한 세그먼트들 내의 MAC 어드레스들이 필수적으로 변화된다. 도시된 바와 같이, 클라이언트로부터 라우터로 라스트 링크를 가로질러 이동하는 모든 연속적인 패킷은 소스 및 목적지 MAC 어드레스 MAC $C_{1,1}$ 및 MAC R을 이용한다. 단일 MAC 어드레스가 연속적인 데이터 패킷 내의 클라이언트를 위해서 이용되기 때문에, 라스트 링크는 단일 물리적 미디어, 즉 단일 PHY 라스트 링크를 포함한다. 게이트웨이 링크에 걸친 운반은 소스 및 목적지 MAC 어드레스 MAC R 및 MAC $M_{0,0}$을 각각 이용한다.

[0618] 그에 따라, 도시된 데이터 패킷이 SDNP 페이로드를 포함하지만, 라스트 마일에 걸친 라우팅은 필수적으로 스니핑 가능 MAC 및 IP 어드레스 - 미인증 청취자에 의한 모니터링에 의해서 해석될 수 있는 어드레스 - 를 이용한다. 동일한 소스 및 목적지 IP 어드레스를 갖는 패킷을 추적하는 것에 의해서, 미인증 청취자는, 데이터 패킷이 동일 대화 또는 세션의 일부일 가능성 있다는 것, 그리고 비록 이들이 SDNP 페이로드를 개방할 수 없지만, 이들이 여전히 통화 시간, 파일 크기, 데이터 전송률 등과 같은 메타데이터를 수집하여 통화자의 프로파일을 만들 수 있다는 것을 추정할 수 있다. 또한, MAC 및 IP 어드레스를 따르는 것에 의해서, 비유적으로 흔적 추적과 마찬가지로, 해커는 단부 디바이스, 즉 클라이언트 디바이스에 대한 통화의 시작점을 잠재적으로 추적할 수 있고, 그 후에 개인적으로 통화자를 식별할 수 있다.

[0619] 본원에서 개시된 바와 같이, 클라이언트 디바이스 추적을 방지하기 위한, 관련 통화 패킷을 더 혼동스럽게 하기 위한, 그리고 메타데이터의 수집을 방지하기 위한 더 우수한 방식은 라스트 마일 및 라스트 링크 통신에서 MAC 및 IP 어드레스를 동적으로 변화시키는 것이다. 이러한 본 발명의 기만 방법은:

[0620] * 본원에서 "다중-PHY 라스트 링크" 통신으로 지칭되는, 라스트 링크 MAC 어드레스를 동적으로 변화시키는 것에 의한 변화되는 통신 매체에 걸친 데이터 패킷 송신,

[0621] * "동적 클라이언트 어드레싱"으로 지칭된, 클라이언트 디바이스의 IP 어드레스의 신원을 동적으로 변화시키는 것에 의해서 통화자를 은폐하는 것,

[0622] * 본원에서 "다중-경로 라스트 마일" 통신으로 지칭되는, 상이한 SDNP 게이트웨이 IP 어드레스로의 그리고 그로부터의 통신의 IP 어드레스를 동적으로 변화시키는 것에 의해서, 라스트 마일에 걸쳐 연속적인 데이터 패킷의 통신 통로를 변화시키는 것.

[0623] 다중-PHY, 동적 클라이언트 어드레싱, 및 다중-경로 라스트 마일 통신의 조합은 라스트 마일 및 라스트 링크 통

신의 추적 및 탐지를 극히 어렵게 만드는데, 이는 SDNP 통화자 및 SDNP 게이트웨이만이, 어떠한 패킷이 동일 통화 또는 세션의 일부인지를 알기 때문이다. 이러한 방법들이 분리되어 또는 조합되어 이용될 수 있다.

[0624] 예를 들어, 도 51a의 하부 절반은, 고정 클라이언트 어드레싱을 갖는 단일 경로 라스트 마일 통신에서의 다중-PHY 라스트 링크 통신의 이용을 도시한다. 도시된 바와 같이, 각각의 행은 SDNP 클라이언트로부터 SDNP 게이트웨이로의 통신에서 사용되는 데이터 패킷의 쌍을 포함한다 - 좌측은 라스트 링크 데이터 패킷을 나타내고, 우측은 게이트웨이 링크 데이터 패키지를 나타낸다. 3개의 행은 3개의 연속적인 메시지를 나타내고, 상단 행은 제1 데이터 세트 "SDNP 페이로드(A)"를 포함하고, 중간 행은 SDNP 페이로드(B)를 포함하고, 하단 행은 SDNP 페이로드(C)를 포함하는 제3의 연속적인 데이터 패킷을 설명한다. 고정 클라이언트 어드레싱을 갖는 단일 경로 라스트 마일 통신에서, 모든 연속적 데이터 패킷이 고정 클라이언트 어드레스 IP $C_{1,1}$ 및 고정 목적지 어드레스 IP $M_{0,0}$을 이용한다.

[0625] 다중-PHY 라스트 링크 통신을 이용하기 위해서, 즉 다수의 물리적 미디어에 걸쳐 라스트 링크 내의 데이터를 라우팅시키기 위해서, SDNP 클라이언트의 MAC 어드레스는 순차적 데이터 패킷들 내에서 동적으로 변화되어야 한다. 각각의 MAC 어드레스는 특정 PHY 층, 예를 들어 이더넷 100BASE-T 및 1000BASE-T 연결에 상응한다. 3개의 물리적 미디어의 경우에, 클라이언트의 MAC 어드레스는 MAC $C_{1,1}$로부터 MAC $C_{1,2}$로, 이어서 MAC $C_{1,3}$으로 동적으로 연속적으로 변화되는 패킷이다. 2개의 미디어만이 이용될 수 있는 경우에, MAC 어드레스는, 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 $C_{1,1}$, ...과 같이, 무작위적인 패턴으로 변경되어 패턴 인식을 방지할 수 있다. 소스 MAC 어드레스가 변경되는 동안, 라스트 링크를 위한 MAC 목적지는 일정하게, 즉 MAC R로서 유지될 수 있다. 라스트 링크의 다중-PHY 통로의 전부가 동일 라우터 내에서 종료되기 때문에, 라스트 마일의 나머지를 통한 데이터 통로는 단일 경로 통신으로서 고정되어 유지된다. 다시 말해서, 라스트 링크가 다중-PHY 연결을 이용하지만, 라스트 마일은 단일 게이트웨이를 통해서 SDNP 클라우드에 진입하고, 라스트 마일은 단일-경로 통신을 포함한다.

[0626] 비록 다중-PHY 접근방식이 소정 정도의 기만을 제공하지만, 특정 통화로부터 데이터 패킷을 스니핑하는 패킷이 여전히 식별될 수 있는데, 이는 그들이 공통 클라이언트 IP 어드레스를 공유하기 때문이다. 이러한 검출 방법은, 동적 클라이언트 어드레싱 - 클라이언트가, 송신하는 각각의 패킷을 갖는 그 IP 어드레스를 변화시키는 동작 - 을 이용하여 방지된다. 예로서, 도 51b는 단일 경로 라스트 마일 통신에서의 클라이언트 동적 IP 어드레싱의 이용을 도시한다. 데이터 패킷의 상단 세트는 단일 PHY 라스트 링크 연결을 나타내는 한편, 데이터 패킷의 하부의 세트는 다중-PHY 구현예를 설명한다. SDNP 단일 경로 라스트 마일 통신에서, SDNP 게이트웨이의 목적지 IP 어드레스(442)는, 단일 PHY 또는 다중-PHY 방법이 이용되는지의 여부와 관계없이, 모든 데이터 패킷 내에서 수치 값 IP $M_{0,0}$으로 고정되어 유지된다.

[0627] 도시된 바와 같이, SDNP 페이로드(A)를 수반하는 동적 클라이언트 어드레싱 데이터 패킷은 IP $C_{1,1}$를 포함하는 동적으로 선택된 소스 IP 어드레스(441)를 이용하는 한편, SDNP 페이로드(B)를 수반하는 데이터 패킷은 IP $C_{1,3}$ 등을 포함하는 동적으로 선택된 소스 IP 어드레스를 이용하고, SDNP 페이로드(C)를 수반하는 데이터 패킷은 IP $C_{1,3}$를 포함하는 동적으로 선택된 소스 IP 어드레스를 이용한다. 동적으로 선택된 어드레스의 수는, 특히 IPv6에서, 거의 제한이 없다. 또한, 어드레스가 재활용되기 전에 소정 시간, 예를 들어 1초가 경과하기만 한다면, IP 어드레스가 재사용될 수 있다. 단일-PHY 라스트 링크를 갖는 동적 클라이언트 어드레스의 경우에, 비록 IP 소스 어드레스가 변화되지만, 이러한 예에서 MAC $C_{1,1}$에서, 소스 MAC 어드레스(183)의 값은 일정하게 유지된다. 다중-PHY 라스트 링크를 갖는 동적 클라이언트 어드레스의 경우에, 소스 MAC 어드레스(183)의 값이 연속적으로 변경되어, MAC $C_{1,1}$으로부터 MAC $C_{1,2}$으로 그리고 이어서 MAC $C_{1,3}$으로 변화된다. 클라이언트의 변화되는 MAC 어드레스와 그 동적 IP 어드레스 사이에는 특별한 수치적 상응성이 존재하지 않는다.

[0628] 비록 동적 클라이언트 어드레싱이 상이한 사용자들로부터 송신된 메시지를 포함하는 것으로 보이지만, 데이터 패킷은 단일 경로에 걸쳐 (다중-PHY 구현예에서의 라스트 링크 이외의) 라스트 마일의 대부분을 여전히 횡단한다. 라스트 마일 통신의 패킹 스니핑을 더 혼동시키기 위한 더 진보된 방법은 "다중-경로" 통신을 이용하는 것이다. 다중-경로 통신에서, 클라이언트를 SDNP 클라우드에 연결하기 위해서, 하나 초과의 SDNP 게이트웨이 IP 어드레스가 이용된다. SDNP 네트워크 라우팅이 시그널링 서버에 의해서 규정되고 각각의 패킷에서 식별 SDNP 태그를 이용하기 때문에, 데이터가 단일 게이트웨이를 통해서 또는 다수의 게이트웨이를 통해서 SDNP 클라우드에 진입하는지와 관계없이, SDNP 클라우드는 패킷을 목적지로 라우팅시킬 수 있다. 도 51c는 고정 클라이언트 어드

레싱을 갖는 다중-경로 라스트 마일 통신의 이용을 도시한다. 라스트 링크 내에서 도시된 모든 데이터 패킷에서, 클라이언트의 소스 IP 어드레스(441)는 수치 값 IP $C_{1,1}$로 고정적으로 유지되는 반면, SDNP 페이로드(A, B 및 C)를 포함하는 연속적인 데이터 패킷은 목적지 IP 어드레스(442)를 IP $M_{0,0}$로부터 IP $M_{0,1}$로 그리고 IP $M_{0,3}$로 동적으로 변경한다. SDNP 게이트웨이의 IP 어드레스는 무작위적으로 선택되지 않고, SDNP 시그널링 서버에 의해서 "선택"되어, 통화자에 일시적으로 근접한 게이트웨이, 즉 SDNP 클라이언트와 특정 SDNP 게이트웨이 사이의 최소 통계적 전파 지연을 갖는 게이트웨이를 나타낸다. 이러한 예에서, 동적 목적지 어드레스는 PHY 연결과 관계없이 변화된다. 예를 들어, 데이터 패킷의 상단 세트는 수치 값 MAC $C_{1,1}$을 갖는 라스트 링크를 위한 클라이언트 소스 MAC 어드레스(183)을 갖는 단일 PHY 라스트 링크 연결을 도시하는 한편, 데이터 패킷의 하부 세트는 상이한 미디어, 예를 들어 MAC $C_{1,1}$, MAC $C_{1,2}$, 및 MAC $C_{1,3}$에 걸쳐 MAC 소스 어드레스를 변경하는 다중-PHY 구현예를 설명한다. 변화되는 클라이언트의 MAC 어드레스와 SDNP 게이트웨이의 목적지 IP 어드레스 사이에는 상응 패턴 또는 수치적 관계가 존재하지 않는다.

[0629] 가장 효과적인 정도의 기만은 동적 클라이언트 어드레싱을 다중-경로 라스트 마일 통신과 조합하는 것이다. 이러한 보안 특징들의 신규 조합이, (도면의 상단 절반 내에 도시된) 단일-PHY 라스트 링크 구현예에 대해서 그리고 하부 절반에 도시된 다중-PHY 라스트 링크 버전에 대해서 도 51d에 도시되어 있다. 하부 절반에 도시된 이러한 완전히 동적인 버전에서, 소스 IP 어드레스(441)는 동적으로 그리고 무작위적으로 IP $C_{1,1}$로부터 IP $C_{1,2}$로 그리고 IP $C_{1,3}$로 변화되는 한편, 독립적으로 SDNP 게이트웨이의 목적지 IP 어드레스(442)는 IP $M_{0,0}$로부터, IP $M_{0,1}$로 그리고 IP $M_{0,3}$로 변화된다. 동적 클라이언트 어드레스가 관련없는 방식으로 변화되는 동안 전파 지연을 최소화하도록, SDNP 게이트웨이 어드레스가 SDNP 시그널링 서버에 의해서 선택된다. 전술한 예에서와 같이, 데이터 패킷의 상단 세트는 수치 값 MAC $C_{1,1}$을 갖는 라스트 링크를 위한 클라이언트 소스 MAC 어드레스(183)을 갖는 단일 PHY 라스트 링크 연결을 도시하는 한편, 데이터 패킷의 하부 세트는 상이한 미디어, 예를 들어 MAC $C_{1,1}$, MAC $C_{1,2}$, 및 MAC $C_{1,3}$에 걸쳐 MAC 소스 어드레스를 변경하는 다중-PHY 구현예를 설명한다. 변화되는 클라이언트의 MAC 어드레스와 변화되는 클라이언트 또는 SDNP 게이트웨이의 IP 어드레스 사이에는 상응 패턴 또는 수치적 관계가 존재하지 않는다. 그러나, 다중-경로 라스트 마일 통신에서, 다중-PHY 라스트 링크는, 모든 데이터를 단일 라우터(R) 내로 집중시키는 대신, 3개의 구분된 라우터($R_1$, $R_2$, 및 $R_3$)에 유리하게 연결될 수 있다.

[0630] 전술한 바와 같은 라스트 마일 기만은, 고정 클라이언트 어드레스 및 단일-PHY 라스트 링크를 갖는 단일 경로 라스트 마일을 포함하는 (행 # 10으로서 표의 하단에 도시된) 최소 보안 구현예로부터 상단 행 #1에 위치되는 동적 소스 어드레싱 및 다중-경로 라스트 마일 통신을 갖는 다중-PHY 라스트 링크에 의해서 제공되는 더 우수한 기만까지의 범위의, 도 52a의 표에서 요약된 바와 같은 10개의 상이한 경우를 나타낸다. 중간 조합들은 보안의 순서로 등급화된 것이다. ($C_{1,n}$), ($M_{0,n}$) 및 $R_n$의 표기는 SDNP 클라이언트, SDNP 게이트웨이, 및 라스트 링크 라우터를 위한 동적으로 변화되는 어드레스를 지칭한다. 동적 어드레스들은 교정되지 않는다. 행 7 내지 10은, 단일 게이트웨이 ($M_{0,0}$)를 이용하는, 단일 경로 라스트 마일 통신을 설명하는 한편, 행 1 내지 6은, 다수 게이트웨이를 갖는 다중-경로 라스트 마일 통신을 설명한다. 음영처리된 행 1 및 4를 제외하고, 라스트 링크 통신은 MAC 어드레스(R)를 갖는 단일 라우터에 연결된다. 대조적으로, 다중-경로 통신에서, 음영처리된 행 1 및 4는 동적 MAC 어드레스($R_n$)를 갖는 다중 라우터에 대한 다중-PHY 라스트 링크 통신을 설명한다.

[0631] 단일-경로 라스트 마일 통신의 동작이 4개의 조합 - 단일-PHY 라스트 링크를 갖는 고정 클라이언트 어드레싱, 다중-PHY 라스트 링크를 갖는 고정-클라이언트 어드레싱, 단일-PHY 라스트 링크를 갖는 동적 클라이언트 어드레싱, 다중-PHY 라스트 링크를 갖는 동적-클라이언트 어드레싱 - 으로 도 52b에 지형적으로 도시되어 있다. 각각의 상자는, 이용된 데이터 통로를 보여주는 3개의 연속적인 데이터 패킷 통신을 도시한다. 실선은 데이터 패킷 흐름을 나타내는 한편, 점선은 이용되지 않은 가능한 통로를 도시한다. 음영처리된 원은 라스트 마일 통신에서 이용된 통신 노드를 나타내는 한편, 빈 원은 미사용 통신 노드를 나타낸다. 도시된 바와 같이, 모든 예는 라우터(R)와 SDNP 게이트웨이 ($M_{0,0}$) 사이에서 단일 연결을 통한 라스트 마일 데이터 라우팅을 종료한다.

[0632] 상부 좌측 모서리에 도시된 단일-PHY 라스트 링크에 걸친 고정 클라이언트 어드레싱의 경우에, 각각의 연속적인 패킷은 변화되지 않는 IP 어드레스를 이용하여 전체 라스트 마일에 걸쳐 동일 통로를 취한다. 하부 좌측 모서리에 도시된 다중-PHY 라스트 링크에 걸친 고정 클라이언트 어드레싱의 경우에, 각각의 연속적인 패킷은 동적으로 변화되는 MAC 어드레스에 의해서 규정된 바와 같은 라스트 링크에 걸쳐 상이한 통로를 취한다. 라스트 마일의

나머지는 변화되지 않는 IP 어드레스에 의해서 특정되는 바와 같은 단일 경로를 포함한다. 단일 경로 운송에도 불구하고, 라스트 링크의 변화되는 물리적 미디어가 통화자 추적을 더 어렵게 만든다. 상부 우측 모서리에 도시된 단일-PHY 라스트 링크에 걸친 동적 클라이언트 어드레싱의 경우에, 각각의 연속적인 패킷은 라스트 링크를 위한 변화되지 않는 목적지 IP 어드레스 및 일정한 클라이언트 MAC 어드레스를 이용하여 전체 라스트 마일에 걸쳐 동일 통로를 취한다. 그 대신, 기만은, 동적 소스 IP 어드레스의 변화에 의해서 클라이언트의 신원을 변화시키는 것에 의해서 달성된다. 하부 우측 모서리에 도시된, 동적 클라이언트 어드레싱 및 다중-PHY 라스트 링크를 갖는 단일 경로 통신의 경우에, 모든 패킷이 단일 SDNP 게이트웨이로 라우팅되지만, 클라이언트의 MAC 어드레스 및 소스 IP 어드레스가 동적으로 그리고 무작위적으로 변화된다.

[0633] 동적 클라이언트 어드레싱은, 클라이언트 디바이스가 하나 이상의 일시적 애드혹 IP 어드레스를 이용하게 하는 프로세스이다. 프로세스는 2개의 스테이지를 포함한다. 제1 스테이지에서, 디바이스가 네트워크 상으로 처음 로그할 때, 이는 가장 가까운 라우터에 접촉하는 것에 의해서 그 존재를 로컬 서브넷에 등록한다. 이어서, 라우터는 그 연결을 동일 서브넷 상의 가장 가까운 DHCP 서버로 재지향시킨다. 동적 호스트 구성 프로토콜(DHCP)의 두문자어인, DHCP는 IP 어드레스를 동적으로 할당하기 위해서 이용되는 네트워크 관리 프로토콜이다. 등록 프로세스에서, 클라이언트 디바이스는 하나 이상 IP 어드레스를 다운로드하고 그 어드레스를 그 통신 데이터 등록부에 저장한다. 할당된 IP 어드레스가 로컬 DHCP 서버에 의해서 갱신되는 그러한 시간까지, 새로운 세션을 시작하는 것 또는 새로운 어드레스를 요청하는 것에 의해서, 클라이언트 디바이스가 통신할 때마다 이는 이러한 IP 어드레스를 이용한다. 어드레스가 특정 서브넷 내에서 동적으로 생성되기 때문에, 클라이언트 디바이스의 IP 어드레스는 인터넷 어드레스가 아니다.

[0634] 제2 스테이지에서, 클라이언트 디바이스가 통화 또는 로그를 SDNP 네트워크에 위치시킬 때, 디바이스는 SDNP 서버의 고정 IP 어드레스를 기초로 SDNP 시그널링 서버와 자동적으로 접촉한다. SDNP 서버는, 진입 메시지를 받으면, 애드혹 IP 어드레스 또는 어드레스들을 SDNP 명칭 서버에 업로드한다. 이어서, SDNP 명칭 서버는 SDNP 어드레스를 일시적 IP 어드레스의 각각을 위한 의사-코드로서 할당한다. 동작 시에, 라우팅 직전에, 패킷의 SDNP 소스 어드레스가 그 로컬 애드혹 IP 어드레스에 의해서 대체된다. SDNP 동적 어드레싱의 경우에, 소스 어드레스가 변화되는 패킷을 반복적으로 송신함으로써, 클라이언트 디바이스의 신원이 감춰진다. 이러한 방식으로, 동적 기만은 클라이언트 디바이스의 진정한 신원을 감춘다.

[0635] SDNP 게이트웨이이 도달하면, 진출 패킷을 위한 소스 어드레스는 클라이언트 IP 어드레스를 폐기하고 그 대신 게이트웨이 서버의 SDNP 어드레스를 대체한다. 이어서, 각각의 진출 SDNP 패킷은 전송 직전에 디바이스의 로컬 IP 어드레스를 그 로컬 애드혹 IP 어드레스와 교환한다. 소스 및 목적지 IP 어드레스가 일정하고 응답을 위해서 요구되는 인터넷 패킷 전송과 달리, SDNP 송신에서, 각각의 홉은 새로운 IP 어드레스를 사용한다. 그에 따라, SDNP 메시지가 최종적으로 그 목적지에 도달될 때, 클라이언트 디바이스의 소스 어드레스는 데이터 패킷에 포함되지 않는다. 그 대신, 시그널링 서버는 응답을 위한 복귀 통로와 관련하여 목적지 디바이스에 통지한다.

[0636] "다중-경로" 라스트 마일 통신의 동작이, 고정 및 동적 클라이언트 어드레싱뿐만 아니라 단일-PHY 및 다중-PHY 라스트 링크의 4개의 조합으로, 도 52c에서 지형적으로 도시되어 있다. 각각의 다중-경로 통신에서, 목적지 IP 어드레스 즉, SDNP 게이트웨이는 계속적으로 변화되고, 이는 라스트 마일 경로가 SDNP 클라우드에 대한 상이한 입력들에 연결된다는 것을 의미한다. 좌측 열에서, 클라이언트 어드레스는 고정적으로 유지되고, 이는 통화자의 신원이 변화지 않는다는 것을 의미한다. 상부 좌측 모서리 예는 라스트 링크를 위해서 단일-PHY 연결을 이용하고, 이는 클라이언트를 위한 MAC 어드레스가 또한 고정적으로 유지된다는 것을 의미한다. 비록 통신이 상이한 목적지 게이트웨이에 대해서 발생되지만, 변화 없는 라스트 링크 물리적 미디어 및 변화 없는 클라이언트 IP 어드레스는 라스트 마일이 쉽게 통화 추적되게 한다. 이러한 취약성은, 데이터 패킷을 전송하기 위해서 이용되는 라스트 링크 미디어를 변화시키는 것에 의해서 또는 통화자의 IP 어드레스의 진정한 신원을 위장함으로써 치유될 수 있다.

[0637] 하부 좌측 모서리 예는 라스트 링크를 위해서 다중-PHY 연결을 이용하고, 이는 클라이언트를 위한 MAC 어드레스가 동적으로 변화된다는 것을 의미한다. 그러한 접근방식은, 클라이언트의 신원이 고정 IP 어드레스를 유지한다는 사실을 보상한다. 엔드-투-엔드 다중-경로 라스트 마일 통신의 일부로서, 각각의 특이적 라스트 링크는 구분된 SDNP 게이트웨이들에 대한 연속적인 패킷의 여정에서 분리된 라우터들에 연결된다. 따라서, 제1 패킷은, 최종적으로 IP 어드레스 IP $M_{0,0}$를 갖는 SDNP 게이트웨이로 라우팅되기 전에, 고정 어드레스 IP $C_{1,1}$를 갖는 클라이언트로부터 MAC 어드레스 MAC $R_1$을 갖는 라우터까지 특이적 PHY 미디어를 통해서 라우팅된다. 제2 패킷에서, 최종적으로 IP 어드레스 IP $M_{0,1}$를 갖는 SDNP 게이트웨이로 라우팅되기 전에, 동일한 클라이언트 어드레스 IP $C_{1,1}$

가 특이적 PHY 미디어를 거쳐 미디어 어드레스 MAC $R_2$를 갖는 다른 라우터로 라우팅된다. 유사하게, 또한 고정 클라이언트 IP 어드레스 $C_{1,1}$을 갖는 제3 패킷은 특이적 PHY 미디어를 경유하여 미디어 어드레스 MAC $R_3$을 갖는 라우터로 라우팅되고, 여기에서 이는 후속하여 SDNP 게이트웨이 $M_{0,3}$으로 라우팅된다. 단일 소스 IP 어드레스를 갖는 클라이언트를 이용함에도 불구하고, 전체적인 분리된 궤적들에서 라스트 마일 패킷을 전달하기 위해서, 다중 라우터의 이용은 기회에 따라 다수의 PHY 라스트 링크를 이용한다.

[0638] 상부 우측 모서리에 도시된 다른 실시예에서, 단지 하나의 MAC 어드레스 및 PHY 연결이 사용되지만, 클라이언트의 신원은 동적으로 변화된다. 도시된 클라이언트의 IP 어드레스는 IP $C_{1,1}$로부터 IP $C_{1,2}$로 그리고 IP $C_{1,3}$로 동적으로 변화되는 반면, 물리적 미디어는 소스 미디어 어드레스 MAC $C_{1,1}$ 및 목적지 어드레스 MAC R로 일정하게 유지된다. 이어서, 데이터가, SDNP 시그널링 서버에 의해서 결정된 바와 같은 무작위 순서로 게이트웨이 $M_{0,0}$, $M_{0,1}$ 및 $M_{0,3}$로 계속 라우팅된다.

[0639] 라스트 마일 기만, 즉 다중-PHY 라스트 링크 및 동적 클라이언트 어드레싱을 이용하는 다중 경로 통신의 3가지 방법 모두를 조합하는 것에 의해서, 더 우수한 보안이 달성된다. 이러한 경우가 도 52c의 하부 우측 모서리에 도시되어 있고, 여기에서 다중-PHY 라스트 링크 및 다중 라우터를 이용하여 송신된 데이터 패킷은 동적 IP 어드레스를 갖는 클라이언트로부터 다수의 경로를 경유하여 다수 SDNP 게이트웨이에 전달된다. 도시된 바와 같이, 동적 소스 네트워크 어드레스 IP $C_{1,1}$를 갖는 클라이언트로부터의 제1 패킷이, 다수의 경로를 경유하여, 소스 및 목적지 미디어 어드레스 MAC $C_{1,1}$ 및 MAC $R_1$에 의해서 규정된 다중-PHY 라스트 링크를 이용하여 목적지 IP $M_{0,0}$에 송신된다. 동적으로 선택된 소스 네트워크 어드레스 IP $C_{1,2}$를 갖는 클라이언트로부터의 제2 데이터 패킷이, 다수의 경로를 경유하여, 소스 및 목적지 미디어 어드레스 MAC $C_{1,2}$ 및 MAC $R_2$에 의해서 규정된 다중-PHY 라스트 링크를 이용하여 목적지 IP $M_{0,1}$에 송신된다. 마지막으로, 동적으로 선택된 소스 네트워크 어드레스 IP $C_{1,3}$를 갖는 클라이언트로부터의 제3 데이터 패킷이, 다수의 경로를 경유하여, 소스 및 목적지 미디어 어드레스 MAC $C_{1,3}$ 및 MAC $R_3$에 의해서 규정된 다중-PHY 라스트 링크를 이용하여 목적지 IP $M_{0,3}$에 송신된다. 이러한 방식으로, 클라이언트 IP 어드레스, SDNP 게이트웨이 IP 어드레스, 클라이언트의 MAC 어드레스 및 라우터의 MAC 모두의 조합이 무작위 방식으로 동적으로 변화되어, 통화 추적 및 메타데이터의 수집을 거의 불가능하게 만든다.

[0640] 동적 IP 어드레싱, 다중 PHY 전송 및 다수 게이트웨이에 대한 다중-경로 전송에 의한 클라이언트 디바이스 IP 어드레스의 은폐 및 라스트 마일 라우팅의 혼동은 클라이언트 디바이스에 의해서 또는 시그널링 서버에 의해서 결정될 수 있다. 잘못 인도하는 프로세스는 난수 생성 또는 다른 의사-무작위 알고리즘을 이용하여 달성될 수 있다. 중요 원리는 라우팅 및 전송 변화가 예측될 수 없다는 것이다.

[0641] 다수 경로에 걸친 이더넷 패킷의 라스트 마일 데이터 전송의 2개의 약간 덜 강력한 버전이 도 52d에 도시되어 있고, 여기에서 좌측 도면은 고정 클라이언트 어드레싱 및 다중-PHY 라스트 링크 연결성을 이용하는 반면, 우측 그림은, 또한 다중-PHY 라스트 링크 연결성과 함께, 동적 클라이언트 어드레싱을 나타낸다. 이러한 구현예와 이전의 도 52c에 도시된 다중-PHY 버전 사이의 차이는, 이러한 버전이, 다중 라우터에 걸친 확산 데이터 전송 대신, 단일 라우터(R)를 이용한다는 것이다. 간략히, 라스트 링크 연결성을 위해서 단일 라우터를 이용하는 다중-경로 전송에서, 클라이언트로부터의 순차적 데이터가 다중 물리적 미디어, 즉 다중-PHY 라스트 링크에 걸쳐 확산되고, 이어서 단일 라우터(R)에 의해서 재-수집되고 다수의 게이트웨이 링크 및 이러한 공통 라우터로부터 구분된 목적지 IP 어드레스에 의해서 규정된 다수의 SDNP 게이트웨이까지 임의의 다른 라스트 마일(미도시)의 병렬 섹션들을 포함하는 라스트 마일의 나머지에 걸쳐 송신된다.

[0642] 이더넷에 대한 부속물로서, WiFi 무선 통신이 또한 SDNP 클라이언트와 SDNP 게이트웨이 사이의 라스트 마일 통신을 위해서 이용될 수 있다. WiFi 통신은, 라디오 링크를 위한 2개, 유선 네트워크 연결을 위한 하나 또는 2개인, 3개 또는 4개의 MAC 어드레스를 갖는 데이터 패킷을 요구하고, 구체적으로 이더넷 데이터 패킷을 이용한다. 도 53은 SDNP 라스트 마일 및 라스트 링크 통신을 위해서 구성된 동일 WiFi 패킷 포맷을 도시한다. 라스트 링크 통신에 적용될 수 있는 액세스 포인트로서, 단지 3개의 6B-길이 MAC 어드레스가 요구되고, 구체적으로 수신 라디오 기지국 또는 "수신기"를 위한 MAC 어드레스 1 필드(235), 송신 라디오 기지국 또는 "엑스미터"를 위한 MAC 어드레스 2 필드(236), 및 WiFi 라우터 즉, 이더넷 또는 "넷"에 대한 유선 네트워크 연결의 MAC 어드레스를 포함하는 MAC 어드레스 3 필드(237)이 요구된다. 동작 시에, 수신기 및 엑스미터 데이터 필드 내로 로딩된 MAC 어드레스의 수치 값은, (i) 라디오에서 수신되고 이더넷으로 포워딩되는 데이터 패킷인지 또는 (ii) 라디오 통신

으로 변환되는 이더넷 상의 진입 데이터인지를 결정하기 위한, DS로의/DS로부터의 지향성 설정에 따라 달라진다. MAC 어드레스 4 데이터 필드(239)는 선택적이고, WiFi 디바이스가 "무선 분배 모드"에서 라디오 브릿지로서 이용될 때에만 이용된다. 그러한 모드가, 예를 들어 사막에서, 셀룰러 또는 마이크로파 네트워크에 대한 대안으로서, 장거리에 걸친 라스트 마일 통신에서 이용될 수 있는 반면, 일반적으로 SDNP 라스트 마일에서의 WiFi 통신의 이용은 일반적으로 SDNP 클라이언트에 대한 라스트 링크 연결에 초점이 맞춰진다. 따라서, 이하의 설명은, 본원에서의 SDNP 기술이 무선 분배 모드 라우팅에서 동일하게 적용될 수 있다는 이해를 가지고, WiFi 라우터에 대한 액세스 포인트 모드에 초점을 맞출 것이다.

[0643] 이더넷 데이터 패킷과 유사하게, 프리앰블(230) 및 시작 프레임 딜리미터(SFD)(232)는 데이터 및 디바이스를 동기화하기 위한 계층 1 데이터를 포함한다. 물리적 계층 수렴 과정(PLCP)(232)은 계층 1 및 계층 2 정보(관련 패킷 길이, 데이터 전송률, 헤더에서의 에러 체크, 등)의 혼합을 포함한다. IEEE 802.11 표준에 따라, 나머지 데이터 필드는, SDNP 페이로드 전달에서 이용되는 유형인, 관리, 제어, 보존, 또는 "데이터"와 같은 WiFi 버전 패킷 유형을 특정하는 프레임 제어(233)를 포함하는 계층 2 데이터 링크 정보를 포함한다.

[0644] 지속시간 및 ID(234)는, WiFi 디바이스가 전력 절약 모드에 있지 않는 경우에, NAV 지속시간을 포함하고, 이러한 경우에 필드는 스테이션 ID를 포함한다. NAV 또는 네트워크 할당 벡터는 무선 통신 시스템에서 전력 절약을 위해서 사용되는 가상의 캐리어-감지 메커니즘이다. NAV 지속시간은, 균일한 비율로 0으로 차감 계수하는 카운터로서 간주될 수 있고, 이때, 이는, 라디오가 아이들링인지 또는 여전히 통신하는지를 결정하기 위해서 미디어를 감지한다. 아이들 모드에서, 카운터는 NAV 지속시간을 반복적으로 카운트하여, 임의의 라디오 통신 활동 요구 관심이 검출되었는지의 여부를 결정하기 위해서 체크한다. 순차적 제어 또는 "시퀀스" 필드(238)는 계층 2 패킷 프레임을 규정하는 패킷 시퀀스 및 단편 번호를 설명한다. 프레임 체크(240)는 전체 데이터 패킷의 32-비트 CRC 체크섬, 즉 에러 체크 데이터 링크 추적기를 포함한다.

[0645] WiFi 페이로드(241)은 WiFi 페이로드를 운반하기 위해서 이용되는 0B 내지 2,312B 길이의 데이터 필드이다. SDNP 라스트 마일 통신에서, 이러한 필드는, IP 헤더(434), 운송-헤더(436) 및 SDNP 페이로드(435)를 포함하는, 라스트 마일 통신에서 이용되는 IP 데이터그램을 포함한다.

[0646] IP 헤더(434)는, 이진법 4를 포함하는 프로토콜 필드(447) 또는 이진법 6을 포함하는 프로토콜 필드(448)에 의해서 결정되는 바와 같은 IPv4 또는 IPv6 프로토콜을 IP 데이터그램이 따르는지의 여부에 따라서 달라진다. 프리앰블(440 및 444) 모두는, 이용되는 계층 4 전송 방법, 예를 들어 TCP, UDP 또는 유지 기능 ICMP 및 IGMP을 결정하기 위해서 이용되는 전송 헤더 플래그(470)를 포함한다. 구체적으로, 보안 동적 통신 네트워크 및 프로토콜에 따라, TCP 운송이 소프트웨어 및 데이터 파일을 위해서 이용되는 한편, UDP는 VoIP 및 비디오와 같은 실시간 데이터를 위해서 이용된다. 전송 헤더(436)의 길이 및 포맷은 전송 헤더 플래그(470)에 따라 달라진다. IP 헤더(434)는 IPv4 소스 및 목적지 어드레스(441 및 442) 또는 IPv6 소스 및 목적지 어드레스(445 및 446)를 포함한다.

[0647] 이더넷 데이터 패킷과 유사하게, WiFi 패킷의 라스트 마일 라우팅은, IP 또는 MAC 어드레스가 언급하는 디바이스의 명칭에 의해서 상징적으로 표시되는, IP 어드레스 및 MAC 어드레스 모두에 따라 달라진다. WiFi 패킷의 순차적인 라스트 마일 라우팅이 도 54a 내지 도 54d의 예에서 도시되어 있다. 각각의 도면은 2개의 WiFi 패킷 - IPv4 데이터그램을 포함하는 상단의 WiFi 패킷 및 IPv4 데이터그램을 포함하는 하부의 WiFi 패킷 - 을 포함한다. IPv4 및 IPv6이 필드 길이가 다른 상이한 포맷들을 이용하기 때문에, 도시된 WiFi 패킷은, 동일한 페이로드를 수반할 때에도, 일반적으로 동일한 길이가 아니다.

[0648] 통신 시퀀스의 제1 단계에서, SDNP 페이로드(A)는 WiFi 라디오 미디어로서 라스트 링크(1404)를 통해서 SDNP 클라이언트(1400)로부터 WiFi 기지국/라우터(1402W)로, 그리고 와이어라인에 의해서 BS 링크(1415)를 경유하여 라우터(1402X) 상으로 이동된다. 이어서, 라우터(1402X)는 데이터 패킷을 게이트웨이 링크(1414)를 거쳐 SDNP 게이트웨이(1401)로 전달한다. SDNP 게이트웨이로부터 클라이언트로의 응답은, 와이어라인에 의해서 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)로부터 라우터(1402X)로, BL 링크(1415)를 가로질러 WiFi 라우터(1402W)로, 그리고 통신 미디어로서 WiFi 라디오를 이용하여 라스트 링크(1404)를 가로질러 클라이언트(1400)로 이동되는 SDNP 페이로드(G)를 포함한다. SDNP 클라이언트는 수치적 MAC 및 IP 어드레스 MAC $C_{1,1}$ 및 IP $C_{1,1}$를 가지고, WiFi 라우터(1402W)는 수치적 MAC 어드레스 MAC W를 가지며, 라우터(1402A)는 수치 MAC 어드레스 MAC R을 가지고, SDNP 게이트웨이는 수치적 MAC 및 IP 어드레스 MAC $M_{0,0}$ 및 IP $M_{0,0}$를 갖는다. WiFi 라우터(1402W) 및 와이어라인 라우터(1402X)의 IP 어드레스는 도시된 라스트 마일 통신에서 요구되지 않는다.

[0649] SDNP 데이터그램 패킷 라우팅이 SDNP 네트워크에 의해서 완전히 제어되는 SDNP 클라우드에서와 대조적으로, IP 데이터그램을 이용하는 라스트 마일 통신에서, SDNP 페이로드는 해석될 수 없거나 라우팅에 양향을 미칠 수 없고, 이는 라스트 마일에 걸쳐 운반되는 각각의 통신이 고정 소스 및 목적지 IP 어드레스를 포함한다는 것을 의미한다. 라디오 통신에서 WiFi 패킷을 지향시키기 위해서 그리고 와이어라인 통신에서 이더넷 패킷을 지향시키기 위해서 이용되는 물리적 미디어 또는 채널은 라스트 마일 내의 각각의 통신 노드를 연결하는 MAC 어드레스에 의해서 통제된다.

[0650] 예를 들어, 도 54a는, 엑스미터 MAC 어드레스 MAC $C_{1,1}$ 및 수신기 MAC 어드레스 MAC W를 포함하는, 라스트 링크(1404)를 통해서 WiFi 라우터(1402W)에 라우팅하는 단일-PHY 라디오를 위해서 이용되는 IPv4 및 IPv6 라스트 링크 WiFi 패킷을 도시한다. WiFi 라우터(1402W)는 또한 "넷" MAC 목적지 어드레스 MAC R을 갖는 이더넷 라우터(1402X)에 라우팅하는 BS 링크 와이어라인(1415)을 제공한다. 계층 3 네트워크 라우팅은 단부 디바이스만을, 즉 IP 어드레스 IP $C_{1,1}$를 갖는 SDNP 클라이언트(1400) 및 목적지 어드레스 IP $M_{0,0}$을 갖는 SDNP 게이트웨이(1401)만을 포함한다. 이더넷 데이터 패킷과 달리, WiFi 패킷은 3개의 어드레스 - 엑스미터 또는 소스-라디오 MAC 어드레스 MAC $C_{1,1}$ 수신기 또는 라디오-목적지 MAC 어드레스 MAC W, 및 이더넷 "넷" 어드레스 MAC R - 를 포함한다. 이러한 데이터 전송의 방향으로, 와이어라인 라우터(1402X)는 WiFi 라우터 디바이스의 네트워크 목적지로서 작용한다. 따라서, WiFi 데이터 패킷은 2개의 미디어, 즉 WiFi 라디오 라스트 링크(1404), 및 이더넷 와이어라인 BS 링크(1415)를 특정한다. 도 54b는 게이트웨이 링크(1414)에 걸쳐 SDNP 페이로드를 운송하는 상응 이더넷 패킷을 도시한다. 설명된 바와 같이, 소스 및 목적지 IP 어드레스는 IP $C_{1,1}$ 및 IP $M_{0,0}$로서 변화되지 않고 유지되는 반면, MAC 소스 및 목적지 어드레스는 그 원래의 값으로부터 MAC R 및 MAC $M_{0,0}$로 변화된다.

[0651] 응답 통신은 목적지 및 소스 IP 어드레스를 스왑하는 것, 및 그에 따라 MAC 어드레스를 조정하는 것을 포함한다. 도 54c는, 게이트웨이 링크(1414)를 통한 SDNP 게이트웨이(1401)로부터 와이어라인 기반의 라우터(1402X)로의 데이터 운송을 위한 IPv4 및 IPv6 이더넷 패킷을 도시한다. 계층 3 데이터그램 정보를 위해서, IP 소스 어드레스(441)는 SDNP 게이트웨이(1401)의 네트워크 어드레스 즉, IP $M_{0,0}$를 포함하고, IP 목적지 어드레스는, 클라이언트의 어드레스인, 값 IP $C_{1,1}$을 포함한다. 게이트웨이 링크 이더넷 팩을 위한 MAC 어드레스는, 소스 어드레스(183)를 위한 MAC $M_{0,0}$ 및 목적지 MAC 어드레스(182)를 위한 MAC R 이다.

[0652] 도 54d는 와이어 라인 BS 링크(1415) 및 WiFi 라디오 기반의 라스트 링크(1404)를 위한 IPv4 및 IPv6 WiFi 패킷을 도시한다. 네트워크 계층 3 라우팅은 SDNP 게이트웨이(1401) 어드레스 IP $M_{0,0}$ 및 SDNP 클라이언트 어드레스 IP $C_{1,1}$를 소스 및 목적지 어드레스(445 및 446)로서 포함한다. "넷"으로 표시된 MAC 어드레스 필드(237)의 기능은 라디오 모드에 따라 변화된다. 여기에서 도시된 전송 모드에서, 이러한 필드는 라디오의 진입 데이터의 와이어라인 소스의 이더넷 MAC 어드레스 즉, 데이터 패킷을 WiFi 액세스 포인트에 송신하는 라우터(1402X)의 수치 값 MAC R을 포함한다.

[0653] 도 54a에서 앞서 도시된 수신기 모드에서, 이러한 필드는 라디오 패킷으로서 수신되고 이더넷 패킷으로 변환된 데이터의 이더넷 목적지를 규정한다. 도시된 예에서, "넷" 필드(237)는, 전송 모드 및 수신 모드 모두를 위한, 라우터(1402X)의 동일 MAC 어드레스, 즉 MAC R을 포함하고, 이는 WiFi 액세스 포인트가 라스트 마일 연결성을 위해서 단일 이더넷 라우터를 이용한다는 것을 의미한다.

[0654] 선택적으로, 라스트 마일에 걸친 다중경로 통신에서, 수신 모드에서, WiFi 액세스 포인트에 의해서 수신된 데이터 패킷을 라우팅하기 위해서 이용된 와이어라인 라우터는, 전송 모드에서, WiFi 액세스 포인트에 의해서 전송되는 데이터 패킷을 라우팅하기 위해서 이용되는 것과 다를 수 있다. 예를 들어, 수신기 모드 내의 라디오 패킷을 위한 네트워크 MAC 어드레스(237)는 수치적 MAC 어드레스 MAC $R_1$을 가질 수 있는 한편, 전송 모드에서, 데이터는 상이한 라우터 연결 MAC $R_2$으로 변화될 수 있고, 이는 BS 링크가 지향적으로 달라지는 다중-PHY 구현예를 선택적으로 포함할 수 있다는 것을 의미한다. 전송 모드에서, WiFi 라우터(1402W)로부터 SDNP 클라이언트(1400)로 라우팅하는 단일-PHY 라디오(1404) 라스트 링크를 위해서 이용된 라스트 링크 WiFi 패킷은, 수치 값 MAC W을 갖는 엑스미터 MAC 어드레스(236) 및 수치 값 MAC $C_{1,1}$을 포함하는 수신기 MAC 어드레스(235)를 포함한다. 이러한 데이터 전송의 방향으로, 와이어라인 라우터(1402A)는 WiFi 라우터 디바이스에 의해서 전송되는 데이터의 소스로서 작용한다. 따라서, WiFi 데이터 패킷은 2개의 미디어, 즉 WiFi 라디오 라스트 링크(1404), 및 이더넷 와이어라인 BS 링크(1415)를 특정한다.

[0655] 셀룰러 네트워크는 SDNP 라스트 마일 통신을 위해서 구성될 수 있는 무선 통신의 다른 형태를 나타낸다. 셀룰러 네트워크는 진입 이더넷 패킷을 라디오-특정 미디어 액세스 제어(MAC) 패킷으로 재-구획한다. 데이터는 시분할(TDMA)에 의해서, 코드분할(CDMA)에 의해서, 또는 다수 서브-채널 주파수에 걸친 콘텐츠의 확산(OFDM)에 의해서 전송되고 수신될 수 있다. OFDM 또는 직교 주파수 분할 다중화를 기초로 하는 4G/LTE 통신의 경우에, 계층 2 데이터 패킷은 계층 2 내의 모든 임베딩된 서비스 데이터 유닛 또는 SDU의 3개의 상이한 레벨에 걸쳐 스택킹되고; 구체적으로 가장 낮은 레벨은 MAC 헤더(303) 및 PHY 계층 1 데이터를 포함하는 20개의 타임 슬롯(300)에 걸쳐 펼쳐진 패딩(305)과 함께 단일 프레임 MAC SDU(304)을 포함하는 PHY PDU(299)를 포함한다. MAC SDU(304)는 다시 라디오 링크 제어 또는 RLC SDU(308)를 포함한다.

[0656] 라디오 링크 제어(RLC)는 3G (UMTS) 및 4G/LTE (OFDM) 기반의 전화통신에서 이용되는 계층 2 프로토콜이다. 라디오 링크 제어의 기능은 3개의 모드 즉, 기지 모드(acknowledged mode), 미기지 모드, 및 투과 모드 중 하나에서 상부 계층 요청에 반응하는 것뿐만 아니라, 에러 검출, 에러 교정, 복제 검출, 및 특정된 포맷에 따른 데이터의 패킷화를 제공하는 것이다. 데이터의 패킷화는 RLC 데이터 PDU의 재기록 및 재-세그먼트화와 함께 RLC SDU의 연쇄화, 세그먼트화, 및 재조립을 포함한다. 예를 들어, 라디오 오버헤드 기능을 실시하기 위한 시간 할당 후에, 단일 프레임 RLC SDU(308)는, 페이로드를 운반하기 위해서 이용할 수 있는 지속시간 및 데이터 파일 크기에서, 불가피하게 제한된다. 그에 따라, 단일 프레임 RLC SDU(308)는 세그먼트로 분할되어야 하고 상이한 RLC 계층 2 포맷 - 다중-프레임 RLC SDU(319) - 으로 맵핑되어야 한다.

[0657] 도 55에 도시된 바와 같이, 단일-프레임 RLC SDU(308)를 다중-프레임 RLC SDU(319)의 다양한 K, K+1, K+2 세그먼트(313, 314, 315) 등으로 맵핑하는 것은 일-대-일 기반으로 발생되지 않는다. 예를 들어 도시된 바와 같이, 단일-프레임 RLC SDU(308)의 맵핑은 K+2 세그먼트(315)의 중간에서 종료된다. 남은 K+1 세그먼트의 미전송 부분은, 그 대신, 새로운 단일-프레임 RLC SDU(312) 내에서, 그러나 라디오 클록 동기화에 필요한 패딩 시간(310)을 허용한 후에 그리고 RLC 헤더(311) 프로세싱 후에만, 전송된다. 이러한 방법에서, K+2 슬롯 내에 캡슐화된 데이터의 전송이 정확하게 재개되며, 여기에서 이는 데이터 흐름이 결코 중단된 적이 없었던 것과 같이 남겨진다. 선택적으로, 4G는, DVD 챕터의 중간에서의 DVD 인코딩된 영화의 재생을 멈추는 것, 일부 다른 기능을 실시하기 위해서 소정 순간의 대기하는 것, 그리고 이어서 멈춰진 곳에서 정확하게 재생을 재개하는 것과 유사하다. 따라서, 어떠한 데이터 콘텐츠도 잃지 않고 셀룰러 시스템의 RF 데이터 전달률이 최대화되고, (PDU 헤더와 같은) 패킷 오버헤드 이외의 라디오 대역폭이 낭비되지 않고, 클록 동기화 패딩 시간(310)으로부터 초래되는 데이터-전송률 저하가 최소화 된다.

[0658] 다중-프레임 RLC SDU(319)은 각각의 K 세그먼트와 일-대-일 상응성으로 PDCP PDU(320)를 캡슐화한다. 예를 들어, K번째 세그먼트(313)는 PDCP 헤더(321A) 및 데이터(323)를 포함하는 IP 페이로드를 운반하고, (K+1)번째 세그먼트(314)는 PDCP 헤더(321B) 및 데이터(324)를 포함하는 IP 페이로드를 운반하며, (K+2)번째 세그먼트(315)는 PDCP 헤더(321C) 및 데이터(325)를 포함하는 IP 페이로드를 운반하고, 기타 등등도 마찬가지 이다. PDCP라는 용어는 3G 및 4G/LTE 통신 프로토콜에서 특정된 바와 같이 패킷 데이터 수렴 프로토콜의 두문자어이고, 압축, 암호화, 무결성 보장뿐만 아니라 사용자 및 제어 데이터 전달과 같은 기능을 실시한다. PDCP 헤더는 전송되는 데이터, 예를 들어 사용자 데이터, 제어 데이터 등의 유형에 따라 달라진다.

[0659] 4G 데이터 패킷 내의 데이터 전송이 연속적으로 연쇄된 데이터의 스트림을 운반하기 때문에, 페이로드 크기는 이더넷 및 WiFi 데이터 패킷에 있을 때와 같이 규정된 길이 블록으로 양자화되지 않는다. 그 대신, 상응하는 계층 2 데이터 세그먼트(313, 314, 315,...)에 의해서 운반되는 데이터 필드(323, 324, 325...)는, 도시된 바와 같이, 전송-헤더(436) 및 SDNP 페이로드(1430)를 포함하는 IP 헤더(434) 및 IP 페이로드(435)를 포함하여, 임의의 크기 페이로드를 증분적으로 지원할 수 있다. 또한, OFDM-기반의 통신에서, 각각의 타임 슬롯은 데이터를 다수의 주파수 서브캐리어 상에서 동시에 운반하고, 이는, 총 데이터 처리량은, TDMA에서와 같이, 단일 채널에 걸친 지속시간에 의해서 단순히 결정되지 않는다는 것을 의미한다. 그러나, 편의상, IP 데이터그램 크기를 이더넷 또는 WiFi 표준의 크기에 맞춰 유지하는 것이 종종 편리하다.

[0660] 도시된 바와 같이, IP 헤더(434)는, 이진법 4를 포함하는 프로토콜 필드(447) 또는 이진법 6을 포함하는 프로토콜 필드(448)에 의해서 결정되는 바와 같은 IPv4 또는 IPv6을 IP 데이터그램이 따르는지의 여부에 따라서 달라진다. 프리앰블(440 및 444) 모두는, 이용되는 계층 4 전송 방법, 예를 들어 TCP, UDP 또는 유지 기능 ICMP 및 IGMP을 결정하기 위해서 이용되는 전송 헤더 플래그(470)를 포함한다. 구체적으로, 보안 동적 통신 네트워크 및 프로토콜에 따라, TCP 운송이 소프트웨어 및 데이터 파일을 위해서 이용되는 한편, UDP는 VoIP 및 비디오와 같은 실시간 데이터를 위해서 이용된다. 전송 헤더(436)의 길이 및 포맷은 전송 헤더 비트(470)에 따라 달라진다. IP 헤더(434)는 IPv4 소스 및 목적지 어드레스(441 및 442) 또는 IPv6 소스 및 목적지 어드레스(445 및 446)를

포함한다.

[0661] IPv6 데이터그램을 이용하는 4G 통신의 예로서, 도 56a는 셀 타워 및 기지국(1402Q)에 라우팅되는 셀룰러 라디오(1404) 라스트 링크를 도시한다. 구체적으로, MAC 소스 필드(300A)에서, RLC PDU는, 클라이언트의 디바이스인, MAC $C_{1,1}$와 같은 셀룰러 소스 미디어 어드레스를 규정한다. 마찬가지로, MAC 목적지 필드(300B)는 셀 타워 및 기지국을 설명하는 MAC BS로서 셀룰러 수신기 미디어 어드레스를 특정한다. 계층 3 네트워크 라우팅은 라스트 마일 단부 디바이스만을, 즉 소스 데이터 필드에 도시된, IP 어드레스 IP $C_{1,1}$를 갖는 SDNP 클라이언트(1400) 및 목적지 어드레스 IP $M_{0,0}$을 갖는 SDNP 게이트웨이(1401)만을 포함한다. 전술한 바와 같이, 데이터 필드(323, 324, 및 325)는 IPv6 데이터그램 데이터 페이로드의 특정 섹션에 반드시 상응할 필요가 없고, 데이터 필드(323)는 IP 소스 어드레스(445), IP 목적지 어드레스(446), 및 운송 헤더(436)를 포함하는 SDNP 페이로드(A)(435)의 부분을 포함한다. 데이터 필드(324 및 325)는 SDNP 페이로드(435)의 전송되지 않은 남은 부분을 운반한다.

[0662] 도 56b는 셀 타워 및 기지국(1402Q)로부터 모바일 클라이언트 디바이스(1400)까지 셀룰러 라스트 링크(1404)를 통한 응답 메시지 SDNP 페이로드(G)를 위한 데이터 패킷을 도시하고, 그에 의해서 이전 데이터 패킷으로부터의 소스 및 목적지 어드레스가 스왑되었고, 즉 셀룰러 소스 미디어 어드레스(300A)에 미디어 어드레스 MAC BS가 로딩되고, 셀룰러 목적지 미디어 어드레스(300B)는 클라이언트의 MAC 어드레스인 MAC $C_{1,1}$로 설정되고, IPv6 데이터그램 내의 IP 소스 필드(445)는 IP $M_{0,0}$으로 설정되며, IP 목적지 필드(445)는 IP $C_{1,1}$로 설정된다. BS 링크(1415)에 걸친 네트워크 라우터(1402X)와 셀룰러 타워 및 기지국(1402Q) 사이의 라우팅은 이전의 예와 일치되는 이더넷 데이터 패킷을 이용한다.

[0663] 라스트 링크를 통한 다중-PHY 통신은 여러 조합으로 이용된 전술한 미디어 중 임의의 것을 포함할 수 있다. 다중-PHY 구현예는, 동일한 또는 상이한 데이터 전송률로 데이터를 운반하고 USB, 이더넷 10BASE-T, 100BASE-T, 1000BASE-T, 또는 DOCSIS3와 같은 공통된 또는 구분된 계층 2 프로토콜을 이용하는 다수의 와이어라인 연결을 포함할 수 있다. 와이어라인 물리적 미디어는, 성능 레벨이 저하되더라도, 이더넷 또는 USB 적합 네트워크 케이블, 동축 케이블, 광섬유, 또는 심지어 DSL을 위한 연선 구리 연결을 포함할 수 있다.

[0664] 무선 다중-PHY 통신은 WiFi, 셀룰러, 위성, 또는 라디오 주파수 및 마이크로파 대역에서 작동되는 독점적 라디오 포맷의 조합을 포함할 수 있다. 무선 라스트 링크 통신은 또한 블루투스 또는 일본의 PHS와 같은 마이크로-셀룰러 네트워크와 같은 단범위 기술을 포함할 수 있다. 무선 프로토콜은, 예를 들어, 아날로그, TDMA, GSM, CDMA, UMTS, 및 OFDM, WiFi 프로토콜 예를 들어 802.11a, 802.11b, 802.11g, 802.11n, 및 802.11ac뿐만 아니라, 위성 통신 또는 일반적인 라디오 링크를 위한 독점적 포맷을 포함하는, 2G, 2.5G, 3G, 및 4G/LTE를 위한 셀룰러 포맷을 포함할 수 있다. 계층 2 프로토콜이 계층 1 물리적 미디어에 따라 변화되기 때문에, 본 개시 내용의 문맥에서 사용된 바와 같은 다중-PHY 통신이라는 용어는, OSI 물리적 및 데이터 링크 계층 즉, 계층 1 및 계층 2 모두의 조합을 의미할 것이고, 계층 1 물리적 미디어만을 의미하는 것으로 청구범위를 제한하는 것으로 해석되지 않아야 한다.

[0665] 이더넷, WiFi, 및 셀룰러 구현예를 포함하는, 공통 계층 2 프로토콜을 이용하는 다중-PHY 통신의 예가 도 57a에 도시되어 있다. 다중-PHY 이더넷의 최상단 예에서, 라우터(27)는, 100BASE-T 및 1000BASE-T가 각각 작동되는 유선 또는 섬유 링크(24A 및 24B)를 포함하는 2개의 이더넷 케이블을 이용하여 데스크탑 컴퓨터(36)에 통신한다. 라스트 마일에 걸친 하이퍼보안 통신을 돕기 위해서, SDNP 소프트웨어(1335C)가 작동되는 데스크탑(36)이 도시되어 있다.

[0666] 다중-PHY WiFi의 중앙 예에서, WiFi 라우터(100)는 WiFi 링크(29A 및 29B)로 도시된 2개의 WiFi 채널을 통해서 노트북(35)에 통신하고, 전자는 2.4GHz 초과의 801.11n 프로토콜로 작동되고 후자는 802.11ac를 이용하여 5GHz 채널에 걸쳐 통신한다. 다중-PHY 모드로 동작하기 위해서, 노트북(35)은, 노트북 내의 다중-대역 안테나(26B)를 이용하여 다수 주파수로 신호를 동시에 송신 및 수신할 수 있어야 한다. 유사하게, WiFi 라우터는 다수-대역 안테나(26)를 이용하여 다수 주파수에서 동시에 신호를 송신 및 수신할 수 있어야 한다. 라스트 마일에 걸친 하이퍼보안 통신을 돕기 위해서, SDNP 소프트웨어(1335C)가 작동되는 노트북(35)이 도시되어 있다.

[0667] 다중-PHY 셀룰러 통신을 도시하는 하부 예에서, 셀룰러 기지국(17)은, 상응 주파수 1.8GHz 및 900MHz를 가지는 셀룰러 링크(28A 및 28B)를 포함하는 2개의 상이한 라디오 채널을 이용하여, 다중-대역 셀룰러 타워(18A)를 통해서 태블릿(39)에 동시에 통신한다. 도시된 예에서, 셀룰러 링크는 4G/LTE 네트워크를 포함한다. 도시된 바와 같이, 태블릿(39)은 내부 다중-대역 안테나(18B)를 이용하여 다수의 주파수에서 신호를 동시에 송신 및 수신할

수 있어야 한다. 라스트 마일에 걸친 하이퍼보안 통신을 돕기 위해서, SDNP 앱(1335A)이 작동되는 태블릿(39)이 도시되어 있다.

[0668] 공통 계층 2 프로토콜을 이용하는 그러한 다중-PHY 통신은 사이버 공격을 혼란시키는데, 이는 해커가, 자체의 보안을 각각 포함할 수 있는 2개의 상이한 계층 2 데이터 링크에 대한 물리적 액세스를 획득하여야 하기 때문이다. 또한, 클라이언트에서 SDNP 소프웨어(1335C), SDNP 앱(1335A), 또는 SDNP 펌웨어(1335B)(미도시)가 작동되는 경우에, 다중-PHY 연결에 걸친 SDNP 페이로드의 라우팅은, 실시간 해킹을 위한 실시간 SDNP 패킷 가로채기 및 해석을 매우 어렵게 만드는 특이적 동적 보안 자격 증명을 이용한다.

[0669] 혼합된 계층 1 미디어 및 계층 2 프로토콜을 이용하는 다중-PHY 통신의 예가 도 57b에 도시되어 있다. 이러한 예에서, 라스트 링크 데이터는 셀룰러, WiFi, 및 위성 시스템의 조합을 이용하여 실행된다. 혼합된 미디어 다중-PHY 통신의 상단 예에서, WiFi 라우터(100)는, 100BASE-T 이더넷 유선 또는 섬유 링크(24B) 및 5GHz에서 작동되는 802.11ac WiFi 링크(29B)의 조합을 이용하여, 데스크탑 컴퓨터(36)와 통신한다. 라스트 마일에 걸친 하이퍼보안 통신을 보장하기 위해서, SDNP 소프트웨어(1335C)가 작동되는 데스크탑(36)이 도시되어 있다. 그러한 예는, 와이어라인 및 무선 통신의 조합을 나타내고, 여기에서 무선 패킷 스니핑은 와이어라인 데이터를 가로채거나 관찰할 수 없다. 이러한 혼합된 이더넷 + WiFi 다중-PHY 라스트 링크 분배 방법은, 액세스 제약된 서버실 내에 록킹된 프라이빗 서버에 통신하는 건물 또는 캠퍼스 내의 보안 데스크탑 컴퓨터를 포함하는 회사 사무실 네트워크를 전개하는데 있어서 특히 매우 적합하다.

[0670] 도 57b에 도시된 혼합된-중간 다중-PHY 통신의 중간 도면에서, 내부 다중-대역 안테나(18C)를 갖는 휴대폰(32)은 2개의 상이한 무선 기술을 이용하여 통신한다. 하나의 PHY 연결인 WiFi 링크(29C)는, 예를 들어 5GHz에서의 802.11n 프로토콜을 이용하여 WiFi 라우터(100) 및 안테나(26)에 통신한다. 제2 PHY 연결인, 셀룰러 링크(28C)는, 셀룰러 타워(25) 및 기지국(17)에 대한 라스트 링크 연결성을 촉진하기 위해서, 4G/LTE 프로토콜로 작동되는 1.8GHz 캐리어를 이용한다. 셀 셀룰러 타워(25) 및 WiFi 안테나(26)가 관련 없는 시스템들 상에서 운영되기 때문에, 이러한 다중-PHY 접근 방식은 라스트 링크 내의 다수의 물리적 미디어에 의해서 수반되는 데이터 패킷들 사이의 모든 관계를 완전히 불분명하게 한다. 라스트 마일에 걸친 하이퍼보안 통신을 보장하기 위해서, SDNP 앱(1335A)이 작동되는 휴대폰(32)이 도시되어 있다.

[0671] 셀룰러 및 위성을 조합한 다중-PHY 라스트 링크 통신을 달성하기 위한 유사한 방법이 도 57b의 하단 도면에 도시되어 있고, 여기에서 SDNP 앱(1335A)이 작동되는 위성/휴대폰(32Z)은 2개의 장거리 라디오 네트워크에 걸쳐 통신한다 - 18GHz에서의 셀 셀룰러 타워(25) 및 기지국(17)에 대한 셀룰러 링크(28D), 및 예를 들어 1.9GHz에서 통신 위성(92)에 대한 위성 링크(95W). 위성(92)은 다시, 클라이언트 통신과 반드시 동일한 주파수일 필요가 없이, 광대역폭 링크(95X)를 통해서 지상 위성 안테나 및 기지국(92B)과 통신한다.

[0672] 도 57c는, 공통 프로토콜을 공유하는 그러나 주파수 분할을 이용하여 다수의 동시적인 통신 채널이 가능한 다른 다양한 다중-PHY 통신-다수 물리적 미디어를 도시한다. 그러한 시스템은, 심각한 로딩 효과가 없는 동작을 위해서 큰 대역폭 미디어를 필요로 하고, 즉 더 많은 사용자가 미디어의 대역폭 및 처리량 용량을 차지할 때 성능이 감소된다. 단지 3개의 그러한 미디어가 그렇게 큰 대역폭, 즉 (i) 동축 케이블을 이용하는 DOCSIS3 케이블 시스템, (ii) 광섬유를 이용하는 DOCSIS3 케이블 시스템, 및 (iii) 낮은 지구 궤도의 다중-GHz 위성 통신 시스템을 용이하게 이용할 수 있다. 구체적으로, 다중-PHY 케이블 시스템의 최상단 도면은, DOCSIS3 프로토콜이 작동되는 동축(coax) 또는 섬유(105)를 경유한 다수의 대역을 이용하여 케이블 CMTS(101)와 통신하는 SDNP 펌웨어(1335M)가 작동되는 셋탑 박스 또는 케이블 모뎀(102B)을 도시한다.

[0673] 하단 도면은 다중-PHY 위성 네트워크를 나타내고, 여기에서 SDNP 앱(1335A)이 작동되는 위성 인에이블드 휴대폰(32Z)가, 독점적 통신 프로토콜로 포맷된 다수의 캐리어 대역(95Z)을 이용하여 통신 위성(92)과 통신한다. 위성(92)과 지상 위성 안테나 및 기지국(92B) 사이의 통신은 수천개의 통화를 혼합하는 트렁크 라인 프로토콜(95X)을 이용하여, 클라이언트 링크(95Z) 내의 다수의 대역에 걸친 다중-PHY 통신의 이용이 클라이언트를 위한 하이퍼보안 통신을 보장하면서, 해커가 특정 통화를 식별하고 해석하는 것을 어렵게 만든다.

[0674] 다중-PHY 라스트 링크 라우팅에서 이용되는 데이터 패킷의 다른 예가 도 58에 도시되어 있고, 여기에서 SDNP 클라이언트(1400)는, 예를 들어 프로토콜 100BASE-T 및 1000BASE-T가 각각 동작되는 이더넷 유선 또는 섬유 링크(24A 및 24B)를 포함하는 2개의 분리된 PHY 연결을 통해서 라우터(1402A)와 통신한다. 라우터(1402A)는 다시 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)와 연결된다. 양 이더넷 패킷들은 소스 IP 어드레스(445), 즉 클라이언트 디바이스를 IP $C_{1,1}$로서 그리고 SDNP 게이트웨이의 목적지 IP 어드레스(446)를 IP $M_{0,0}$으로 규정한다. 유선 또는 섬유 링크(24A)에 의해서 실현된 PHY에 걸쳐 라우팅된 이더넷 패킷(A)은, MAC R을 포함하는 MAC

목적지 어드레스(182) 및 MAC $C_{1,1}$를 포함하는 MAC 소스 어드레스(183)를 포함한다. 유선 또는 섬유 링크(24B)에 의해서 실현된 PHY에 걸쳐 라우팅된 이더넷 패킷(B)은, MAC R을 포함하는 MAC 목적지 어드레스(182) 및 대안적인 PHY 연결을 형성하는 MAC $C_{1,2}$를 포함하는 다른 MAC 소스 어드레스(183)를 포함한다.

[0675] MAC $C_{1,1}$로부터 MAC $C_{1,2}$로의 소스 미디어 어드레스의 변화는 2.6GHz 100BASE-T 연결로부터 1000BASE-T 연결로 이더넷 통신을 재지향시킨다. 동작 시에, SDNP 클라이언트 디바이스(1400)로부터의 데이터 패킷이 단편화되고 이어서, SDNP 알고리즘 및 공유 비밀에 따라, SDNP 페이로드(A) 및 SDNP 페이로드(B)로 할당된다. 다중-PHY 라스트 링크에 걸친 단편화된 데이터 운송은 유선 또는 섬유 링크(24A)에 걸친 이더넷 패킷(A)에 의해서 수반되는 SDNP 페이로드(A) 및 유선 또는 섬유 링크(24B) 상의 이더넷 패킷(B)에 의해서 수반되는 SDNP 페이로드(B)로 이루어진다.

[0676] 다중-PHY 라스트 링크 라우팅에서 이용되는 데이터 패킷의 다른 예가 도 59에 도시되어 있고, 여기에서 SDNP 클라이언트(1400)는, 예를 들어 각각 2.4GHz의 802.11n 및 5GHz의 802.11ac의 프로토콜을 이용하여 WiFi 링크(29A 및 29B)를 포함하는 2개의 분리된 PHY 연결을 통해서 WiFi 라우터(1402W)와 통신한다. 라우터(1402W)는 다시 BS 링크(1415)를 통해서 라우터(1402X)에 연결되고, 라우터(1402X)는 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)에 연결된다. 양 WiFi 패킷들은 소스 IP 어드레스(445), 즉 클라이언트 디바이스를 IP $C_{1,1}$로서 그리고 SDNP 게이트웨이의 목적지 IP 어드레스(446)를 IP $M_{0,0}$으로 규정한다. WiFi 링크(29A)에 의해서 실현된 PHY에 걸쳐 라우팅된 WiFi 패킷(A)은, MAC $C_{1,1}$를 포함하는 엑스미터 MAC 라디오 소스 어드레스(236), MAC W를 포함하는 MAC 라디오 수신기 목적지 어드레스(235), 및 MAC R을 포함하는 MAC 네트워크 목적지(237)를 포함한다. WiFi 링크(29B)에 의해서 실현된 PHY에 걸쳐 라우팅된 WiFi 패킷(B)은, MAC $C_{1,2}$를 포함하는 엑스미터 MAC 라디오 소스 어드레스(236), MAC W를 포함하는 MAC 라디오 수신기 목적지 어드레스(235), 및 MAC R을 포함하는 MAC 네트워크 목적지(237)를 포함한다.

[0677] MAC $C_{1,1}$로부터 MAC $C_{1,2}$로의 소스 미디어 어드레스의 변화는 2.6GHz WiFi 라디오로부터 5GHz 송수신기로 전송을 재지향시킨다. 동작 시에, SDNP 클라이언트 디바이스(1400)로부터의 데이터 패킷이 단편화되고 이어서, SDNP 알고리즘 및 공유 비밀에 따라, SDNP 페이로드(A) 및 SDNP 페이로드(B)로 할당된다. 다중-PHY 라스트 링크에 걸친 단편화된 데이터 운송은 WiFi 링크(29A)에 걸친 WiFi 패킷(A)에 의해서 수반되는 SDNP 페이로드(A) 및 WiFi 링크(29B) 상의 WiFi 패킷(B)에 의해서 수반되는 SDNP 페이로드(B)로 이루어진다.

[0678] 다중-PHY 라스트 링크 라우팅에서 이용되는 데이터 패킷의 또 다른 예가 도 60에 도시되어 있고, 여기에서 SDNP 클라이언트(1400)는, 예를 들어 각각 1.8GHz에서의 4G/LTE 및 900MHz에서의 4G/LTE 프로토콜을 이용하여 셀룰러 링크(28A 및 28B)를 포함하는 2개의 분리된 PHY 연결을 통해서 셀 타워(1402Q)와 통신한다. 라우터(1402Q)는 다시 BS 링크(1415)를 통해서 라우터(1402X)에 연결되고, 라우터(1402X)는 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)에 연결된다. 양 셀룰러 라디오 패킷들은 소스 IP 어드레스(445), 즉 클라이언트 디바이스를 IP $C_{1,1}$로서 그리고 SDNP 게이트웨이의 목적지 IP 어드레스(446)를 IP $M_{0,0}$으로 규정한다. 셀룰러 링크(28A)에 의해서 실현된 PHY에 걸쳐 라우팅된 셀룰러 패킷(A)은, MAC $C_{1,1}$을 포함하는 엑스미터 MAC 라디오 소스 어드레스(300A) 및 MAC BS를 포함하는 MAC 셀 타워 목적지(300B)를 포함한다. 셀룰러 링크(28B)에 의해서 실현된 PHY에 걸쳐 라우팅된 셀룰러 패킷(B)은, MAC $C_{1,2}$을 포함하는 엑스미터 MAC 라디오 소스 어드레스(300A) 및 MAC BS를 포함하는 MAC 셀 타워 목적지(300B)를 포함한다.

[0679] MAC $C_{1,1}$로부터 MAC $C_{1,2}$로의 소스 미디어 어드레스의 변화는 1.8GHz 4G/LTE 셀룰러 라디오로부터 900MHz로 전송을 재지향시킨다. 동작 시에, SDNP 클라이언트 디바이스(1400)로부터의 데이터 패킷이 단편화되고 이어서, SDNP 알고리즘 및 공유 비밀에 따라, SDNP 페이로드(A) 및 SDNP 페이로드(B)로 할당된다. 다중-PHY 라스트 링크에 걸친 단편화된 데이터 운송은 WiFi 링크(28A)에 걸친 셀룰러 패킷(A)에 의해서 수반되는 SDNP 페이로드(A) 및 WiFi 링크(28B) 상의 셀룰러 패킷(B)에 의해서 수반되는 SDNP 페이로드(B)로 이루어진다.

[0680] 전술한 바와 같이, 다중-PHY 통신은 또한 상이한 미디어를 포함할 수 있다. 그러한 경우에, 각각의 연결을 위한 데이터 패킷은 상응 물리적 미디어를 위한 계층 2 프로토콜에 따라 포맷되어야 한다. 예를 들어, 도 61은 이더넷 및 WiFi를 포함하는 하이브리드 라스트 링크 통신을 도시하고, 여기에서 SDNP 클라이언트(1400)는, 예를 들어 100BASE-T 및 5GHz에서의 802.11ac 각각을 이용하여 이더넷 유선 또는 섬유 링크(24A) 및 WiFi 링크(29B)를 포함하는 2개의 분리된 PHY 연결을 통해서 WiFi 라우터(1402W)와 통신한다. 라우터(1402W)는 다시 BS 링크

(1415)를 통해서 라우터(1402X)에 연결되고, 라우터(1402X)는 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)에 연결된다. 양 WiFi 패킷들은 소스 IP 어드레스(445), 즉 클라이언트 디바이스를 IP $C_{1,1}$로서 그리고 SDNP 게이트웨이의 목적지 IP 어드레스(446)를 IP $M_{0,0}$로 규정한다. 유선 또는 섬유 링크(24A)에 의해서 실현된 PHY에 걸쳐 라우팅된 이더넷(A)는, MAC $C_{1,1}$를 포함하는 MAC 소스 어드레스(183) 및 MAC W를 포함하는 MAC 목적지 어드레스(182)를 포함한다. WiFi 링크(29B)에 의해서 실현된 PHY에 걸쳐 라우팅된 WiFi 패킷(B)은, MAC $C_{1,2}$를 포함하는 엑스미터 MAC 라디오 소스 어드레스(236), MAC W를 포함하는 MAC 라디오 수신기 목적지 어드레스(235), 및 MAC R을 포함하는 MAC 네트워크 목적지(237)를 포함한다.

[0681] MAC $C_{1,1}$로부터 MAC $C_{1,2}$로의 소스 미디어 어드레스의 변화는 이더넷으로부터 WiFi로 전송을 재지향시킨다. 동작 시에, SDNP 클라이언트 디바이스(1400)로부터의 데이터 패킷이 단편화되고 이어서, SDNP 알고리즘 및 공유 비밀에 따라, SDNP 페이로드(A) 및 SDNP 페이로드(B)로 할당된다. 다중-PHY 라스트 링크에 걸친 단편화된 데이터 운송은 유선 또는 섬유 링크(24A)에 걸친 이너넷 패킷(A)에 의해서 수반되는 SDNP 페이로드(A) 및 WiFi 링크(29B) 상의 WiFi 패킷(B)에 의해서 수반되는 SDNP 페이로드(B)로 이루어진다.

[0682] 도 62는 WiFi 및 셀룰러 통신을 포함하는 하이브리드 라스트 링크 통신을 도시하고, 여기에서 SDNP 클라이언트(1400)는 2개의 상이한 무선 기지국에 대한 2개의 분리된 PHY 연결에 걸쳐, 구체적으로 2.4GHz에서 802.11n 동작되는 WiFi 라우터(1402W)에 대한 WiFi 링크(29A), 및 900MHz 캐리어 주파수에 걸쳐 4G/LTE 동작되는 셀룰러 기지국(1402Q)에 대한 셀룰러 링크(28B)에 걸쳐 통신한다. 라우터(1402W 및 1402Q)는 다시 BS 링크(1415A 및 1415B) 각각을 통해서 라우터(1402X)에 연결되고, 라우터(1402X)는 게이트웨이 링크(1414)를 통해서 SDNP 게이트웨이(1401)에 연결된다. 양 WiFi 및 4G 셀룰러 패킷들은 소스 IP 어드레스(445), 즉 클라이언트 디바이스를 IP $C_{1,1}$로서 그리고 SDNP 게이트웨이의 목적지 IP 어드레스(446)를 IP $M_{0,0}$로 규정한다. WiFi 링크(29A)를 포함하는 연결을 통한 PHY 계층에서 라우팅된 WiFi 패킷(A)은, MAC $C_{1,1}$를 포함하는 엑스미터 MAC 라디오 소스 어드레스(236), MAC W를 포함하는 MAC 라디오 수신기 목적지 어드레스(235), 및 MAC R을 포함하는 MAC 네트워크 목적지(237)를 포함한다. WiFi 링크(29B)에 의해서 실현된 PHY 계층 연결로서 라우팅된 셀룰러(B)는, MAC $C_{1,2}$을 포함하는 MAC 소스 어드레스(300B) 및 MAC BS를 포함하는 MAC 목적지(300B)를 포함한다.

[0683] MAC $C_{1,1}$로부터 MAC $C_{1,2}$로의 소스 미디어 어드레스의 변화는 WiFi LAN으로부터 셀룰러 네트워크로 전송을 재지향시킨다. 동작 시에, SDNP 클라이언트 디바이스(1400)로부터의 데이터 패킷이 단편화되고 이어서, SDNP 알고리즘 및 공유 비밀에 따라, SDNP 페이로드(A) 및 SDNP 페이로드(B)로 할당된다. 다중-PHY 라스트 링크에 걸친 단편화된 데이터 운송은 WiFi 링크(29A)에 걸친 WiFi 패킷(A)에 의해서 수반되는 SDNP 페이로드(A) 및 셀룰러 링크(28B) 상의 셀룰러 패킷(B)에 의해서 수반되는 SDNP 페이로드(B)로 이루어진다.

[0684] 다중-PHY 통신의 다른 형태는, 상이한 주파수들의 많은 채널들을 지원할 수 있고 상이한 데이터 패킷들을 위해서 구분된 프로토콜을 이용하는 물리적 매체를 포함한다. 그러한 구현예는, SDNP 소프트웨어를 실행하는 DOCSIS3-기반의 케이블 분배 시스템을 이용하여 촉진될 수 있다. SDNP 인에이블드 DOCSIS3 케이블 분배 시스템을 위한 OSI 통신 스택이 도 63에 도시되어 있고, 이는 계층 1 PHY 연결성, 계층 2 데이터 링크, 및 케이블 모뎀 말단 디바이스 CMTS(101)뿐만 아니라 케이블-연결된 디바이스의 예, 예를 들어 케이블 모뎀 CM(103) 또는 셋탑 박스(STB)(102) 모두를 위한 중첩 계층 3 네트워크를 포함한다. 구체적으로, 케이블 모뎀 말단 시스템 디바이스 CMTS(101) 및 그 연관된 스택(378)은 클라우드 서버(22) 및 인터넷(20)에 또는 대안적으로 비디오 헤드엔드, IPTV 시스템, 또는 VoIP 시스템(미도시)에 연결된 계층 1 PHY 네트워크 인터페이스(361)를 포함한다. 네트워크 인터페이스(361) 및 데이터 링크 층(366)의 조합은 CMTS(101)의 디바이스 인터페이스 통신 스택(378) 내에 포함된다. 데이터 링크 계층 2에서, 데이터는, 포워딩 기능(370)을 통해서 네트워크 인터페이스 통신 스택으로부터 케이블 네트워크 인터페이스 통신 스택으로, 구체적으로 링크 레벨 제어(LLC)(369) 내로 전달된다. 링크 레벨 제어 802.2 LLC(369)는 IEEE 제원 802.2에 따라 규정된 하드웨어-독립형 프로토콜을 포함한다. 이어서, 패킷 데이터가 링크 보안(368)에 의해서 수정되어, 초보적인 패킷 보안을 제공하고, 사용량 기반 과금 유니캐스트 방송과 같은 콘텐츠의 미승인 시청을 주로 방지한다.

[0685] 이어서, 계층 1 PHY 케이블 인터페이스(362)는, 동축 케이블(104) 또는 광섬유(91)를 포함하는 분배 네트워크(102)를 통해서, 데이터 프레임을 케이블 모뎀(CM)(103) 또는 셋탑 박스(STB)(102) 내의 상응 계층 1 PHY 케이블 인터페이스(363)에 송신한다. 케이블 인터페이스(363)는 케이블 모뎀(CM)(103) 또는 셋탑 박스(STB)(102)의 OSI 통신 스택(379)으로서 도시된 케이블 네트워크 인터페이스의 PHY 층을 나타낸다. 데이터 패킷을 수신하면,

케이블 MAC 인터페이스(371)는 이어서 케이블 MAC 어드레스를 해석하고, 그 페이로드를 해독을 위해서 링크 보안(372)에 전달하고, 최종적으로 해석을 위해서 하드웨어 독립적 링크 계층 제어 802.2 LLC(373)에 전달한다. 이어서, CM 또는 STB 케이블 네트워크 통신 스택에 대한 입력 데이터가 투과 브릿징(374)을 통해서 CM 또는 STB 디바이스 인터페이스 통신 스택에, 구체적으로 IEEE 802.2에 대한 제원에 따라 디바이스 독립적 링크 층 제어 802.2 LLC(375)에 전달된다. 이어서, 패킷의 MAC 어드레스를 업데이트하기 위해서, 패킷이 HSD & IPTV MAC 블록(376) 또는 WiFi 802.11 MAC 블록(377)에 전달된다. WiFi 통신의 경우에, 데이터 패킷은 이어서 WiFi 안테나(26) 상의 전송을 위해서 802.11 MAC 블록(377)으로부터 WiFi PHY 계층 1 라디오 인터페이스(365)로 전달된다. 와이어라인 연결의 경우에, 데이터 패킷은 이어서 TV(39) 또는 데스크탑(36)에 대한 연결을 위해서 HSD & IPTV MAC 블록(376)으로부터 이더넷 또는 HDMI 인터페이스 블록(364)에 전달된다.

[0686] 설명한 바와 같은 PHY 및 데이터 링크 계층은 CMTS으로부터 임의 수의 케이블 모뎀(CM)까지의 연결을 구축한다. CMTS 통신 스택(378) 내에서 그리고 CM 통신 스택(379) 내에서, 데이터 패킷은, 케이블 네트워크에 의해서 또는 인터넷의 DNS 명칭 서버에 의해서 인식되는 IP 어드레스를 이용하여, OSI 계층 3 계층(360A 및 360B) 내에서 각각 IP 데이터그램 IPv4, IPv6 또는 ICMPv6으로서 준비된다. 라스트 마일 통신에서, SDNP 소스 및 목적지 IP 어드레스를 갖는 IPv4 또는 IPv6 데이터 패킷을 이용하는 SDNP 데이터그램은 일반적으로 사용되지 않는데, 이는 SDNP 소프트웨어 또는 펌웨어에 의해서 인에이블링되지 않은 연결된 디바이스가 SDNP 데이터그램 라우팅 어드레스를 해석할 수 있는 능력을 가지지 않기 때문이다.

[0687] 케이블 모뎀 네트워크 내의 전송 계층 4 동작이 장치에 의해서 변경된다. CMTS(101)의 경우에, OSI 통신 스택(378)의 계층 4 전송 층(1420)은 UDP를 독점적으로 이용하는데, 이는 그 동작이 실시간 통신, 예를 들어 비디오 데이터의 스트리밍을 필요로 하기 때문이다. 이러한 측면으로부터, 케이블 통신(102)은, 인터넷의 경우보다, SDNP 실시간 네트워크에 보다 가깝다. 케이블 모뎀이 클라이언트, 즉 단부 통신 디바이스로서 인터넷 및 케이블 네트워크 모두와 정보 처리 상호 운용성을 가지기 때문에, CM(103) 또는 STB(102)의 OSI 통신 스택(379) 내의 계층 4 전송 계층(1420B)은 실시간 동작을 위해서 UDP를 이용하고 인터넷 데이터를 위해서 TCP를 이용한다. 그러한 이용은 인터넷을 통한 VoIP을 이용하는 OTT 캐리어에서 문제가 되는데, 이는 케이블 네트워크가 IP 데이터그램을 데이터로서 해석하여, TCP 및 전송 프로토콜을 자동적으로 이용하고 실시간 통신 QoS, 대기시간, 및 전파 지연을 저하시킬 것이기 때문이다. 이러한 문제는 SDNP 인에이블드 케이블 모뎀에서 발생되지 않는다 - CM 또는 STB가 운영 SDNP 펌웨어 또는 소프트웨어인 경우에, SDNP 소프트웨어는, 맥락과 관련하여, (소프트웨어 및 파일을 위해서) TCP의 사용이 보장되는 때 그리고, 실시간 데이터를 위해서, 그렇지 않은 때를 결정한다.

[0688] 애플리케이션 계층, 즉 OSI 계층 5 내지 계층 7은 CMTS(101) 내의 계층 전송 동작(1420A) 상단에 그리고 CM(103) 또는 STB(102) 내의 운반 계층(1420B)의 상단에 놓인다. CMTS(101)에서, 이러한 애플리케이션은 전형적으로, IP 네트워크 상에서 정보 연결된 디바이스들을 수집하고 구성하기 위한 인터넷-표준 프로토콜인 SNMP(1431A)와 같은 통신 과제를 포함한다. 다른 기능은 DHCPv4(1432A) 및 DHCPv6(1433A)을 포함한다. 동적 호스트 구성 프로토콜의 두문자어인 DHCP는, 동적으로 생성된(비고정) IP 어드레스, 디폴트 게이트웨이 및 서브넷 마스크를 포함하는 필요 라우팅 정보를 IP 호스트에 자동적으로 공급하기 위한, 클라이언트 및 서버 모두를 위한 프로토콜이다. 비록 인터넷 생성 특이적, 즉 IPv4 또는 IPv6를 위한 동적 IP 어드레스 생성의 기능이, NAT 게이트웨이 또는 SNMP와 유사하게, 일반적이고 CMTS(101) 및 CM(103) 또는 STB(102) 모두를 위한 DOCSIS3 케이블 시스템에 동일하게 적용 가능하다.

[0689] 본원에서 개시된 보안 동적 통신 네트워크 및 프로토콜 애플리케이션 층 구현예는, CMTS(101) 운영 시스템의 상단에서 동작되는 SDNP 펌웨어(1430A)로서 실현될 때, 이하를 포함하는 임의 수의 특이적 과제를 실시한다:

[0690] * SDNP 페이로드를 개방하고 판독하도록 CM(103)이 인에이블링되어야 하는, 즉 CM(103)이 SDNP 클라이언트 이어야 하는 경우로서, SDNP 페이로드(1430)를 해석하지 않는 통과로서의 동작.

[0691] * 라스트 마일 원격 SDNP 게이트웨이로서 동작하는 것, 즉 CM(103)에 포워딩하기 위해서 SDNP 페이로드의 콘텐츠를 해석하고 콘텐츠를 DOCSIS3 특정 메시지(링크 보안 포함)로 변환하는 것. 그러한 경우에, CM(103)은 SDNP 클라이언트 소프트웨어 또는 펌웨어가 작동될 필요는 없다.

[0692] * 라스트 마일 SDNP 브릿지로서 동작하는 것, IP 데이터그램을 SDNP 데이터그램으로 변환하는 것, 그리고 SDNP 데이터그램을 CM(103)에 통신하는 것. 그러한 경우에, CM(103)은 SDNP 클라이언트 소프트웨어 또는 펌웨어를 작동시켜 SDNP-브릿지에 연결하여야 하고, 즉 애드혹 SDNP "플로팅" 네트워크를 형성한다.

[0693] 도시된 바와 같이, CM(103) 및 STB(102)를 위한 OSI 통신 스택(379)은, 전술한 통신 관련 앱 SNMP(1431B),

DHCPv4(1432B), 및 DHCPv6(1433B)을 포함하는 OSI 계층 5 내지 계층 7로서 분류되는 수많은 애플리케이션을 포함한다. 다른 기능, 유틸리티 TFTP(1434B) 또는 "작은 파일 전달 프로토콜"이 주로 DOCSIS3에서 소프트웨어를 케이블 네트워크를 통해서 CMTS로부터 케이블 모뎀 및 셋탑 박스로 다운로드하고 소프트웨어 업데이트를 하기 위한 수단으로 이용된다. 케이블 네트워크에서, HTTP(1435B) 또는 하이퍼텍스트 전달 프로토콜은 주로 스마트 TV에서 유용한 동적 메뉴를 페인팅하기 위한 것이다. (짧게 "Otr"(1436B)로 표기된) 다른 애플리케이션은 게이밍 앱, 진단, IPTV 앱, 비디오 기록 기능, 및 기타를 포함한다. CM(103) 또는 STB(102)에서 작동되는 SDNP 펌웨어(1430B)는, CMTS(101)이 SDNP 소프트웨어를 작동시키는지의 여부와 관계없이, 사용자 및 라스트 링크에 대한 하이퍼보안 보안 라스트 마일 통신 전부를 확장시킨다.

[0694] 도 64는 SDNP 페이로드(1430)를 전달하도록 구성된 DOCSIS3 데이터 패킷의 구성을 도시한다. 도시된 바와 같이 PHY 계층 1은, 프리앰블(391), 가변 길이 페이로드 또는 코드워드(392) 및 가드타임(393)을 포함하는 데이터 링크 계층 2 MAC 데이터를 포함하는, 가변적인 길이 및 지속시간의 물리적 미디어 디바이스 프레임(390)을 포함한다. 프리앰블(391)은, 통신 방향에 따라, 업스트림 프리앰블 또는 다운스트림 프리앰블을 포함한다. 업스트림 프리앰블의 경우에, 프리앰블(391)은 물리적 미디어 디바이스 PMD 헤더(398), MAC 헤더(399A) 및 데이터 PDU(400A)를 포함한다. 다운스트림 프리앰블의 경우에, 프리앰블(391)은 MPEG 헤더(401), MAC 헤더(399B) 및 데이터 PDU(400B)를 포함한다. 업스트림 프리앰블 내의 데이터 PDU(400A) 및 다운스트림 프리앰블 내의 데이터 PDU(400B)는 MAC 목적지 어드레스(DA)(403B) 및 MAC 소스 어드레스(SA)(403A)를 포함한다. 가변 길이 페이로드(392)의 콘텐츠는 짧은 코드워드(394) 또는 긴 코드워드(397)를 포함할 수 있다.

[0695] 짧은 코드워드(394)는 데이터(A)를 포함하는 페이로드(395A) 및 FEC A를 포함하는 에러 교정(396A)을 포함한다. 긴 코드워드(397)의 경우에, 페이로드는 데이터(A), 데이터(B), 및 데이터(C)를 각각 수반하는 다수의 페이로드 블록(395A, 395B, 및 395C)으로 분할되고, 각각의 페이로드는 상응 데이터(FEC A, FEC B, 및 FEC C)를 포함하는 자체의 에러 체킹 블록(396A, 396B, 및 396C)을 포함한다. 에러 체킹 후에, DOCSIS3로부터 전달된 데이터는, 긴 코드워드의 경우에 데이터 블록(395A, 395B 및 395C)을 그리고 짧은 코드워드의 경우에 데이터 블록(395A)만을 포함한다. 데이터(A), 데이터(B), 및 데이터(C)의 조합은, IP 소스 어드레스(445), IP 목적지 어드레스(446), 그리고 SDNP 페이로드(1430) 및 계층 4 데이터를 포함하는 운송 헤더(436)를 포함하는 데이터 필드(435)를 포함하는 인접 IP 데이터그램, 이러한 예에서, IPv6 데이터그램으로 병합된다. 이러한 방식에서, DOCSIS3은 패킷-전환 데이터 프로토콜을 이용하여 케이블 네트워크를 통해서 데이터를 탄력적으로 전달한다.

[0696] 도 65a에 도시된 바와 같이, 데이터 패킷은 하이브리드 케이블-섬유 네트워크에 걸친 다수의 채널 내에서, 즉 상이한 주파수들로 운반된다. DOCSIS 3.0에서, 데이터 채널은 아날로그 TV 신호(1440)(삼각형), QAM 데이터(1441), 및 "디플렉서" 제어 채널(1443)을 포함하는 5 MHz 내지 1,002 MHz범위이다. DOCSIS 3.1의 위상 1에서, 주파수 범위는 1,218MHz까지 확장되고, 주로 QAM에 할당된 기존 채널을 초과하는 주파수 대역에서, DOCSIS3.1 데이터 채널(1442)이 부가되어 OFDM 변조를 돕는다.

[0697] OFDM은 QAM 변조 방법에 바람직한데, 이는 채널들이 더 타이트하게 이격될 수 있기 때문이다. 변조 체계를 비교하면, QAM 주파수 분배(1445A)는 OFDM 주파수 분배(1445B)보다 스펙트럼 콘텐츠가 더 넓은 테일을 나타낸다. 구체적으로, $f_0$ 내지 $f_{-50}$의, 스펙트럼 사이드밴드 폭, 즉 캐리어 연부로부터 신호가 -50dB만큼 드롭되는 주파수까지의 폭은 QAM 주파수 분배(1445A)에서 4.3 정규화 주파수 유닛 폭이나, OFDM 주파수 분배(1445B)의 경우에 단지 0.4 정규화 주파수 유닛 폭이다. 스펙트럼 폭이 더 좁기 때문에, 더 많은 통신 채널들이 동일 스펙트럼 내로 팩킹되어 네트워크의 전체 대역폭 및 최대의 총 데이터 전송률을 증가시킬 수 있다. DOCSIS 3.1의 위상 2 전개에서, 주파수 범위는 1,794MHz로 확장된다.

[0698] QAM 데이터(1441)을 위해서 원래 할당된 대역 중 많은 대역이 OFDM 데이터(1442)를 위해서 명시적으로 할당된 새로운 채널로 대체된다.

[0699] DOCSIS-인에이블드 케이블 네트워크에서, 하나의 CMTS 유닛은 이용 가능 채널을 관리하는 많은 CM을 지원한다. 비록 CMTS가 다운스트림 통신 및 필요에 따른 동적인 채널 선택을 할당할 수 있지만, 업스트림 통신은, 다수의 CM이 데이터를 동시에 보내기 위한 시도를 하는 경우를 돕기 위해서 경쟁 관리를 필요로 한다. 따라서, 각각의 모뎀은 데이터를 송신하기 전에 CMTS으로부터 업링크 채널을 요청하여야 한다. 이러한 프로세스가 도 65b에 도시되어 있고, 이는 SDNP 앱(1335L)이 작동되는 CMTS(101)와 SDNP 펌웨어(1335M)가 작동되는 CM(103) 사이의 통신 동작의 시퀀스를 포함한다. 다중-PHY 통신에서의 IP 데이터그램의 라우팅은 IP 어드레스 "IP CMTS" 및 "IP CM1" 그리고 다수 MAC 어드레스, 예를 들어 CM(103)을 위한 "MAC CM1" 및 CMTS(101)을 위한 "MAC CMTS1", "MAC CMTS2", "MAC CMTS3", 및 "MAC CMTS4"를 이용한다. 주파수 대 시간의 그래프를 보여주는 최상단 도면에서,

CM(103)은 지정된 채널 상에서의 RQST(1445A) 전송 요청을 송신한다.

[0700] 응답이 없으면, 제2 RQST(1445B)가 송신되어, MAP 데이터 패킷(1446) 형태의 상이한 채널 상의 CMTS(101)로부터의 응답을 초래한다. MAP 데이터 패킷(1446)의 콘텐츠는, 전송할 때 그리고 그 업스트림 통신을 위해서 이용할 수 있는 채널을 CM(103)에 지시한다. MAP 데이터 패킷(1446)을 수신한 후에, CM(103)은 업링크 데이터 패킷(1447A 및 1447B) 내의 2개의 채널에 걸쳐 펼쳐진 그 업스트림 데이터를 동시에 송신한다. 중심 도면에 도시된 2개의 채널에 걸쳐 동시에 송신된 데이터의 분할은 채널 본딩으로 지칭된다. 채널 본딩은, CMTS 및 CM 사이의 통신 대역폭 및 데이터 전송률을 증가시킬 수 있는 수단이다. 이는 또한 이용 가능하지 않은 대역폭이 사용되지 않도록 보장하는 동적 방법이다. 하단 도면에서, CMTS(101)는 4개의 채널, 즉 1448A, 1448B, 1448C, 및 1448D을 채널 본딩하는 것 그리고 동시에 그러나 지속시간이 상이하게 데이터를 송신하는 것에 의해서 응답한다.

[0701] 하이브리드 섬유-케이블 네트워크에 걸친 업스트림 및 다운스트림 통신 모두에서, 대역폭은, "미니슬롯"으로 지칭되는 작은 타임 세그먼트로 분할된, 다수의 채널들 사이에서 동적으로 할당된다. 도 65c는 CM(103)으로부터 CMTS(101)로의 업스트림 통신을 도시한다. 그러한 업스트림 통신은 일반적으로 전송하기 위한 메시지 또는 요청을 포함한다. 이러한 예에서, 데이터는 총 5개의 타임 미니슬롯을 포함하는 주파수($f_1$ 및 $f_2$)에 걸쳐 송신된다. 도시된 바와 같이, 미니슬롯 1, 2, 및 3은 간격(K, (K+1), 및 (K+2)) 동안 주파수($f_1$)에서 송신되는 한편, 미니슬롯 4 및 5는 간격(K 및 (K+1)) 중에 주파수($f_2$)에서 송신되나, 간격(K+2) 중에는 송신되지 않는다. 단순화된 형태로 도시된 업스트림 데이터 패킷(1450A)은 라스트 마일 통신의 IP 소스 어드레스 "IP CM1" 및 IP 목적지 어드레스 즉, 서버(1201A)에 의해서 호스팅된 SDNP 네트워크의 게이트웨이 노드인, "IP $M_{0,0}$"을 특정한다.

[0702] 라스트 링크 통신에서, 업스트림 데이터 패킷(1450A)은 "MAC CM1"을 케이블 모뎀의 소스 MAC 어드레스로서 특정하고, PHY 미디어, 이러한 경우에 MAC 목적지 "MAC CMTS1"로서 주파수($f_1$)의 채널을 특정한다. SDNP 페이로드(A)를 포함하는 데이터 패킷(1450A)은, 비록 단일 데이터 패킷 및 페이로드를 함께 운반하지만, 총 3개의 미니슬롯, 즉 미니슬롯 1, 2 및 3을 점유한다. 대조적으로, 미니슬롯-4 및 미니슬롯-5 각각은 단일 데이터 패킷, 즉 SDNP 페이로드(B) 및 SDNP 페이로드(C)를 갖는 1450B 및 1450C만을 각각 포함한다. 데이터 패킷(1450A)과 마찬가지로 양 패킷(1450B 및 1450C)은 SDNP 클라우드의 목적지 IP 어드레스, 구체적으로 SDNP 게이트웨이 노드 $M_{0,0}$를 특정한다.

[0703] 그러나, MAC 목적지 어드레스에서, 동일 MAC 어드레스 및 물리적 미디어를 제1 패킷으로 특정하는 대신, 양 패킷(1450B 및 1450C)은 "MAC CMTS2"의 MAC 목적지 어드레스를 규정한다. 이러한 어드레스를 이용하여, 데이터 패킷(1450B 및 1450C)이 데이터 패킷(1450A)과 상이한 주파수 - 이러한 경우에, 주파수($f_1$)가 아닌, 주파수($f_2$) - 에 수반되어야 한다. 주파수의 실제 값은 CMTS(101)에 의해서 동적으로 맵핑되고 구체적으로 식별되지 않는다. 그에 의해서, DOCSIS3 인에이블드 시스템은 다중-PHY 해결책을 나타내고, 그에 의해서 단일 CMTS 유닛은 다수의 주파수에 걸쳐 그리고 256 QAM 또는 OFDM과 같은 다수의 프로토콜을 이용하여 케이블 모뎀 또는 셋탑 박스에 동시에 통신할 수 있다.

[0704] DOCSIS3 시스템에서의 일반적인 경우와 같이 어떠한 데이터 패킷이 공통 캐리어 채널 또는 주파수를 이용할지를 CM 및 CMTS가 결정할 수 있게 하는 대신, 라스트 마일 통신을 위한 개시된 보안 동적 통신 네트워크 및 프로토콜에 따라, SDNP 클라이언트 CM(103)은 상이한 MAC 목적지 어드레스를 특정하여 다수 주파수 및 채널에 걸친 통신을 강제하고, 즉 다중-PHY 동작을 강제한다. CM(103) 데이터 패킷(1450A 및 1450B/C)이 상이한 목적지 MAC 어드레스 즉, MAC CMTS1 및 MAC CMTS2를 각각 규정하기 때문에, 데이터 패킷은 라스트 링크에 걸쳐 다중-PHY 동작을 자동적으로 실행한다. 대안적으로, 예를 들어 명령 및 제어 요청을 이용하여 특이적 채널 할당을 요청하는 다른 수단을 CMTS이 촉진하는 경우에, 다중-PHY 통신을 실행하기 위한 MAC 어드레스의 이용이 다른 수단에 의해서 대체될 수 있다.

[0705] 도 65d는 CMTS(101)로부터 CM(103)으로의 다운스트림 데이터를 도시하여, 다중-PHY 다운스트림 통신에서 큰 데이터 전송률을 달성하기 위한 본딩의 이용을 보여준다. 도시된 바와 같이, 모든 데이터 패킷은 "IP CMTS"의 IP 어드레스, "IP CM1"의 목적지 IP 어드레스, 그리고 "MAC CM1"의 MAC 목적지 어드레스를 특정한다. 다중-PHY 통신은 CMTS(101)의 MAC 소스 어드레스의 제원에 의해서 제어된다. 도시된 바와 같이, SDNP 페이로드(G)를 포함하는 데이터 패킷(1450G)은 미니슬롯 15 및 16 내에서 데이터를 수반하는 주파수($f_6$)에서의 통신에 상응하는 MAC 소스 어드레스 "MAC CMTS6"을 특정한다. 데이터 패킷(1450H)은 SDNP 페이로드(H)를 포함하고, 미니슬롯 17 및 20 내에서 데이터를 수반하는 주파수($f_7$)에서의 통신에 상응하는 MAC 소스 어드레스 "MAC CMTS7"을 특정한다.

SDNP 페이로드(I)를 포함하는 데이터 패킷(1450I)은, 미니슬롯 21, 22 및 23 내에서 데이터를 수반하는 주파수($f_8$)에서의 통신에 상응하는 MAC 소스 어드레스 "MAC CMTS8"을 특정한다. 마지막으로, SDNP 페이로드(J)를 포함하는 데이터 패킷(1450J)은 미니슬롯 넘버 24 및 25 내에서 데이터를 수반하는 주파수($f_9$)에서의 통신에 상응하는 MAC 소스 어드레스 "MAC CMTS9"를 특정한다. 이러한 방식으로, 관련된 그리고 관련되지 않은 데이터 패킷은, 동시적인 업스트림 데이터와의 채널 경쟁 또는 데이터 충돌이 없이, 다중-PHY 방법을 이용하여 CMTS(101)로부터 CM(103)으로 동시에 송신될 수 있다.

[0706] ***하이퍼보안 통화 라우팅(HyperSecure Call Routing)*** - 개시된 보안 동적 통신 네트워크 및 프로토콜에 따라 만들어진 하이퍼보안 통화 라우팅은 이하의 명령 및 제어를 위한 3개의 방법 중 하나를 이용하여 실시될 수 있다.

[0707] * 삼중-채널 통신으로서, 통화 또는 코뮤니케의 라우팅이 3개의 서버 세트 즉, 오디오, 비디오 또는 데이터 파일을 운반하기 위한 SDNP 미디어 서버; 통화의 라우팅을 선택하기 위한 SDNP 시그널링 서버, 및 그 상응 SDNP 어드레스에 대한 전화 번호의 동적 맵핑을 저장하기 위한 SDNP 네임 서버를 이용하여 제어되고,

[0708] * 이중-채널 통신으로서, 통화 또는 코뮤니케의 라우팅 제어는 2개의 서버 세트 즉, 오디오, 비디오 또는 데이터 파일을 운반하기 위한 SDNP 미디어 서버; 및 통화를 라우팅하기 위한, 그리고 그 상응 SDNP 어드레스에 대한 전화 번호를 맵핑하는 SDNP 명칭 서버의 기능을 실시하기 위한 SDNP 시그널링 서버를 이용하고,

[0709] * 단일-채널 통신으로서, 데이터 운반, 경로 계획 및 SDNP 어드레스 맵 모두가 단일 서버 세트로 실행된다.

[0710] 일반적으로, 삼중-채널 통신은 사이버-공격에 대한 더 큰 면역을 제공하는데, 이는 하나의 서버 세트가 통화에 관한 모든 정보를 포함하지 않기 때문이다. 그러나, 모든 경우에, SDNP 네트워크는 임의의 주어진 서버 내에 포함되는 정보를 제한하기 위해서 분배 프로세싱을 이용한다. 또한, 단일-, 이중- 또는 삼중-채널 통신에서의 데이터 운반 중에, SDNP 미디어 서버는 제4 유형의 서버 - DMZ 서버 - 에 연결된다. DMZ 서버는, 스크램블링, 분할, 혼합, 정크 데이터 삽입 및 제거, 그리고 암호화를 포함하는, SDNP 데이터 페이로드를 프로세싱하는데 필요한 SDNP 공유 비밀을 수용하기 위해서 이용된다. 동작 시에, 미디어 서버에 의해서 수신된 진입 데이터 패킷이 DMZ 서버로 전달되고, 그 곳에서 데이터 패킷이 수정되고 미디어 서버로 다시 전달된다. 미디어 서버는, 데이터 패킷이 어떻게 수정되었는지 또는 데이터를 프로세스하기 위해서 어떠한 로직 또는 알고리즘이 이용되었는지를 알지 못한다. DMZ 서버에 저장된 실행 가능 코드 및 표가 암호화되어 코드의 분석을 방지한다. 또한, DMZ 서버는 네트워크 또는 인터넷에 연결되지 않고 오프라인으로 동작된다.

[0711] 이하의 그림은 삼중-채널 SDNP 통신 및 네트워크에 걸친 통화의 개시 또는 파일의 송신에서 이용되는 시퀀스의 하나의 예시적인 구현예를 도시한다. 이중-채널 통신의 동작은 삼중-채널 통신에 대한 사소한 수정으로서 간주될 수 있고, 여기에서 SDNP 명칭 서버 기능이 시그널링 서버에 병합된다. 단일-채널 통신은 모두 3개의 동작을 SDNP 통신 노드로서 동작하는 다기능 서버의 네트워크 내로 통합하는 것을 포함한다.

[0712] 비록 SDNP 클라우드 내의 단편화된 데이터 전송이 일반적으로 동적으로 메시된 라우팅을 이용하여 실시되지만, 라스트 마일 통신은, 구체적으로 연속적인 데이터 패킷들이 (i) 단일 SDNP 게이트웨이로 즉, 단일-경로 라스트 마일 통신으로서 라우팅되거나, 대안적으로 (ii) 다수 SDNP 게이트웨이로, 즉 다중-경로 라스트 마일 통신으로서 라우팅되는, 더 적은 라우팅 선택사항을 제공한다. 다른 라스트 마일 라우팅 선택은 동적 소스 어드레싱 및 다중-PHY 라스트 링크 연결성을 포함한다. 이러한 전달 선택사항은 시그널링 서버 내에서 생성된 IP 데이터 패킷 내에서 특정된다. 이러한 SDNP 데이터 패킷이 그 소스 및 목적지 IP 및 MAC 어드레스를 특정한다는 사실에도 불구하고, 특정 데이터 패킷이 라스트 마일 내에서 취하는 정확한 통로는 알려지지 않는다. 그 대신, 중간 통로가 라우터, 로컬 네트워크 운영자가 소유한 디바이스, 모바일 네트워크 운영자, 및 라스트 마일을 서비스하는 네트워크 서비스 제공자의 동작에 의해서 결정되고, SDNP 시그널링 서버에 의해서 결정되지 않는다. 그에 따라, 라스트 마일 통신은, 2개의 단부들이 고정되나 특이적으로 성형된 통로의 미로가 그들을 연결하는, 점프 로프와 유사하다.

[0713] 간결하게 반복하면, 단일-경로, 다중-경로, 및 메시형-경로 통신이라는 용어는 미디어 패킷의 통로, 즉 통화자들 사이의 통로 "콘텐츠" 횡단을 지칭하는 한편, 삼중-채널, 이중-채널, 및 단일-채널 통신이라는 용어는 SDNP 노드의 네트워크에 걸친 전송을 통제하기 위해서 이용되는 명령 및 제어 시스템을 지칭한다. 전술한 내용으로부터, 이하의 도면의 세트는, 개시된 보안 동적 통신 네트워크 및 프로토콜에 따라 통화를 하거나 또는 코뮤니케를 개시하는데 이용되는 단계의 시퀀스, 즉 "프로세스"를 도시한다.

[0714] 도 66은, SDNP 클라이언트(1600), IP 라우터(1602A, 1602B, 및 1602C) 시그널링 서버(1603A), SDNP 명칭 서버

(1604A), 및 SDNP 게이트웨이(1601)를 포함하는 삼중-채널 통신을 위한 단일-경로 라스트 마일 네트워크의 개략도이다. 이러한 컴퓨터 서버는, SDNP 클라이언트 $C_{1,1}$, 라우터(R), SDNP 시그널링 서버 노드(S), SDNP 명칭 서버 노드(NS), 및 SDNP 게이트웨이 노드 $M_{0,0}$ 를 포함하는 도시된 바와 같은 네트워크 노드 명칭 및 IP 어드레스를 갖는 네트워크 통신을 돕기 위해서 이용되는 SDNP 통신 노드를 호스팅한다. 네트워크 연결(1610)은 클라이언트 $C_{1,1}$,와 그 가장 가까운 라우터(1602A) 사이의 라스트 링크를 촉진하고; 네트워크 연결(1611)은 SDNP 게이트웨이 $M_{0,0}$ 과 그 가장 가까운 라우터(1602B) 사이의 게이트웨이 링크를 촉진하고; 네트워크 연결(1612)은 SDNP 시그널링 서버(1603A)와 그 가장 가까운 라우터(1602C) 사이의 게이트웨이 링크를 촉진하고; 네트워크 연결(1616)은 지형적으로 인접한 라우터(1602A 및 1602C)에 상호 연결된다. 라우터의 IP 어드레스가 IP 데이터그램에서 소스 또는 목적지 어드레스로서 사용되지 않기 때문에, "R"이라는 용어는 계층 3 상의 모든 라우터에서 공유된다. 계층 1 및 계층 2의 설명의 경우에, 각각의 라우터는 특이적 신원을 가지나, 이러한 양태는 IP 네트워크 계층 3 통화 라우팅의 설명과 관련되지 않는다. SDNP 시그널링 서버(1603A)(노드 S)는 네트워크 연결(1613)을 통해서 SDNP 명칭 서버(1604A)(노드 NS)에 그리고 많은 수의 네트워크 연결(1614)을 통해서 SDNP 클라우드 노드 $M_{0,n}$에 연결된다. 시그널링 서버(1603A)는 또한 네트워크 연결(1615)을 통해서 다른 시그널링 서버(미도시)에 연결된다.

[0715] SDNP 네트워크를 이용하여, 통화를 위치시키는 것, 즉 "세션"을 구축하는 것은 통화를 하는 SDNP 클라이언트, 즉 "통화자"로부터 개시된 이하의 단계의 시퀀스를 포함한다:

[0716] 1. SDNP 통화(또는 콜 아웃) 요청

[0717] 2. SDNP 어드레스 요청

[0718] 3. SDNP 어드레스 전달

[0719] 4. SDNP 라우팅 지시

[0720] 5. SDNP 통화(또는 콜 아웃) 시작

[0721] 제1 단계, "통화 요청"은 도 67에서 도식적으로 도시되어 있고, 여기에서 통화자, 어드레스 "IP $C_{1,1}$,"를 갖는 클라이언트(1600)가 IP 데이터그램(1620)을 갖는 통로(1610, 1616, 및 1612)에 걸쳐 어드레스 "IP S"에서 시그널링 서버(1603A)와 접촉한다. 데이터그램의 명령 및 제어 페이로드(621)는 데이터 정확도를 보장하기 위해서 TCP를 이용하는 계층 4 데이터 전송을 포함하고, 전달, 긴급성, 보안 자격 증명, 및 통화되는 당사자인 "피통화자"의 접촉 정보를 포함하는 많은 수의 요청된 통화 매개변수를 특정한다. 다른 SDNP 클라이언트로의 통화, 즉 "SDNP 통화"의 경우에, 이러한 접촉 정보는, 클라이언트의 SDNP 전화 디렉토리 내에 존재하는 데이터인, 통화되는 클라이언트의 신용 인증(CID)을 포함한다. SDNP 클라이언트가 아닌 당사자에 대한 통화인, "콜 아웃"의 경우에, 접촉 정보는 전화 번호를 포함한다. SDNP 클라이언트의 CID가 본질적으로 익명적이고 SDNP 명칭 서버에만 알려지는 반면, 전화 번호는 은폐되지 않는다. 통화되는 당사자의 프라이버시를 보호하기 위해서, C&C 페이로드 내의 전화 번호가 암호화된다. 대안적으로, 전체 C&C 페이로드(1621)가 암호화될 수 있다. C&C 페이로드(1621)가 암호문의 형태일 수 있는 반면, IP 데이터그램(1620)의 IP 어드레스는 암호화될 수 없고, 암호화되는 경우에 라우터(1602A 및 1602C)는 데이터그램을 라우팅할 수 없다.

[0722] 제2 단계인, "SDNP 어드레스 요청"은 도 68에 도시되어 있고, 여기에서 어드레스 "IP S"를 갖는 SDNP 시그널링 서버는 IP 데이터그램(1622)을 갖는 통로(1613)를 통해서 어드레스 "IP NS"에서 SDNP 명칭 서버와 접촉한다. 데이터그램의 명령 및 제어 페이로드는 계층 4 데이터 전송을 TCP로서 규정하고, 통화되는 당사자의 CID 또는 암호화된 전화 번호를 포함한다. SDNP 통화의 경우에, 명칭 서버(1604A)는 CID를 통화되는 클라이언트의 SDNP 어드레스로 변환한다. 콜 아웃의 경우에, 명칭 서버(1604A)는 통화되는 당사자의 전화 번호를 해독하고 피통화자의 위치에 가장 가까운 SDNP 게이트웨이의 SDNP 어드레스로 변환한다. 도 69에 도시된 바와 같이, 명칭 서버(1604A)는 이어서 어드레스 "IP S"에서 IP 데이터그램(1623) 내의 클라이언트의 SDNP 어드레스 또는 게이트웨이를 소스 어드레스 "IP NS"로부터 시그널링 서버(1603A)로 전달한다.

[0723] 이어서, 시그널링 서버(1603A)는 통화자 및 피통화자의 SDNP 어드레스를 이용하여 그들 사이에서 통화를, 피통화자가 SDNP 클라이언트인 경우에, 하이퍼보안 연결로서 또는 피통화자가 SDNP 클라이언트가 아닌 경우에 가장 가까운 SDNP 게이트웨이에 라우팅한다. 라우팅 지시를 준비하고 이들을 통화자의 연결을 완성하는데 필요한 모든 미디어 노드에 분배하기 위해서 이용되는 프로세스가 도 70에 도시되어 있다. 도시된 바와 같이, C&C 페이로

드(1621A)의 전달 및 긴급성 필드에 포함된 통화자의 전달 요청은, 계정 정보에 대해서 일단 입증되면, 동작(1650)에 의해서 도시된 바와 같이, 데이터그램의 전달 방법을 선택하기 위해서 이용된다. 일반, VIP, 보장형, 또는 특별한 전달을 포함하는 전달 방법은 패킷 또는 서브-패킷(패킷이 분할되거나 단편화된 경우)의 라우팅에 영향을 미친다. VIP 전달에서, 예를 들어, 가장 빠른 경로가 데이터 전송을 위해서 이용되는 한편, 다른 클라이언트에 의한 동일 경로의 로딩은 최소화된다. 보장형 전달에서, 복제 데이터 패킷 단편들이 네트워크를 거쳐, 즉 중복성을 이용하여, 송신되어, 가장 빠른 패킷을 적시에 전달하는 것을 보장하고 늦은 도달은 무시한다. 이어서, C&C 페이로드(1623A)로부터의 SDNP 어드레스 데이터와 조합된, 동작(1651)이 통화자로부터 피통화자의 SDNP 어드레스까지 또는 피통화자가 SDNP 클라이언트가 아닌 경우에 가장 가까운 게이트웨이까지 최적의 경로를 맵핑한다. C&C 페이로드(1621A) 내에 포함된 긴급성 요청 데이터을 이용하여, 순서대로 전파 지연 감소 - 스네일 전달(서두를 필요 없음), 일반 전달, 우선 전달, 및 긴급 전달을 포함하는, 패키지 긴급 동작(1652)을 선택한다.

[0724] 이어서, 긴급성 요청 정보가 동작(1653)에 의한 서브-패킷 라우팅을 위한 라우팅 및 구역을 선택하기 위해서 이용된다. 이러한 매개변수는, 임의의 적용 가능한 보안 자격 증명(1621B)과 함께, 조합되어 동작(1660)을 통해서 라우팅 명령 및 제어 패킷을 합성한다. 이러한 C&C 데이터 패킷은, TCP 특정된 계층 4 전송을 이용하여, 라스트 마일의 참여 통신 노드로 전달되나, 실시간 데이터 전달에서 이용될 때 그 계층 4 전송 프로토콜로서 UDP를 이용하는 라우팅 정보를 포함한다. 예를 들어, 구역(U1) 보안 자격 증명에 따라 만들어진 라스트 마일 라우팅은, 클라이언트 노드 $C_{1,1}$로부터 SDNP 게이트웨이 노드 $M_{0,0}$까지 데이터를 라우팅하기 위해서 이용되는 C&C 페이로드(1626)를 포함하는 IP 데이터그램(1625)으로서 생성된다. IP 데이터그램(1625)은 TCP 데이터 전송을 이용하여 SDNP 클라이언트에 전달되나, "라스트 마일 라우팅 U1"으로 지칭되는 C&C 페이로드(1626)는 실시간으로 패킷을 라우팅시키기 위해서 이용되는 데이터를 포함하여, 그 계층 4 전송 메커니즘으로서 UDP의 이용을 필요로 한다. SDNP C&C 패킷 합성 동작(1660)은 또한 TCP 데이터 패킷으로서 SDNP 클라우드 내의 노드에 전달되는 많은 다른 C&C 메시지를 생성한다. 클라우드 지시 데이터 패킷의 하나의 예는, SDNP $M_{0,0}$으로부터 SDNP $M_{0,1}$까지 데이터를 라우팅하기 위해서 이용되는 C&C 페이로드(1628A)를 포함하는 IP 데이터그램(1627A)이다. 도 71에 도시된 바와 같이, 이러한 SDNP 라우팅 지시 패킷은 직렬 연결(1612, 1616, 및 1610)에 걸쳐 클라이언트 노드 $C_{1,1}$을 포함하는 미디어 노드에, 그리고 연결(1614)에 걸쳐 SDNP 게이트웨이 노드 $M_{0,0}$ 및 SDNP 클라우드 내의 다른 노드에 분배된다.

[0725] 통화의 시작이 도 72에 도시되어 있고, 여기에서 SDNP 데이터, 예를 들어 소리, 비디오, 텍스트 등을 포함하는 미디어 SDNP 데이터그램(1630)이, C&C 데이터 패킷(1626)을 포함하는 IP 헤더 상에 첨부되고, IP $C_{1,1}$로부터 IP $M_{0,0}$까지 SDNP 클라이언트(1600)로부터 라스트 링크 네트워크 연결(1601)을 통해서 라우터(1602A 및 1602B)로 그리고 최종적으로 게이트웨이 링크(1611)를 가로질러 SDNP 게이트웨이(1601)까지 라우팅된다. 식별 태그, 보안 구역, 프리앰블, 및 SDNP 데이터 필드는 미디어 SDNP 데이터그램(1630) 내에 포함된 SDNP 미디어 패킷의 페이로드를 함께 구성한다.

[0726] SDNP 앱(1335A)가 작동되는 휴대폰(32)을 포함하는 전술한 SDNP 통화의, 즉 SDNP 게이트웨이 $M_{0,0}$으로부터 SDNP 클라이언트 $C_{7,1}$까지의 하이퍼보안 통화의 라우팅이 도 73a의 단순화된 네트워크 도면으로 도시되어 있다. 미디어 SDNP 페이로드(A) 및 헤더(1628A)를 포함하는 SDNP 데이터그램(1631A)이 SDNP 어드레스 $M_{0,0}$ 및 $M_{0,1}$을 갖는 미디어 노드들 사이에서 라우팅된다. SDNP 게이트웨이(1601)가 2개의 어드레스 - 라스트 마일 통신을 위한 IP 어드레스 "IP $M_{0,0}$", 및 SDNP 클라우드 내의 통신을 위한 SDNP 어드레스 "SDNP $M_{0,0}$" - 를 갖는다는 것을 주목해야 한다. 각각의 SDNP 데이터그램의 콘텐츠는 패킷이 SDNP 클라우드를 횡단할 때 변화되고, 그에 따라 SDNP 미디어 페이로드(A, B, 및 C) 내에 포함된 콘텐츠 - 소리, 비디오 및 텍스트가 구분되게 상이하고, 20개의 상이한 대화 또는 코뮤니케로부터의 콘텐츠를 포함할 수 있다. SDNP 클라우드 내의 데이터 라우팅 및 패킷 보안의 메커니즘이 "Secure Dynamic Communication Network and Protocol"라는 명칭의 미국 출원 제14/803,869호에서 개시되어 있고, 이는, SDNP 클라우드를 통해서 익명으로 이동되는 데이터 패킷의 콘텐츠 및 암호화가 어떻게 동적으로 그리고 연속적으로 변화되고, 단지 클라이언트의 디바이스 내에서 수렴되는지를 설명한다.

[0727] 따라서, 미디어 SDNP 페이로드(B) 및 헤더(1628B)를 포함하는 SDNP 데이터그램(1631B)이 IP 어드레스 IP $M_{0,4}$ 및 $M_{0,f}$을 갖는 미디어 노드들 사이에서 라우팅된다. SDNP 게이트웨이(1601B)를 통해서 SDNP 클라우드를 빠져나가는 데이터가 SDNP 데이터그램으로부터 IP 데이터그램(1632)으로 변환된다. 헤더(1628C) 및 SDNP 미디어 페이로드

(C)를 갖는 IP 데이터그램(1632)은, 라스트 마일을 포함하는 구역인, 구역(U2)을 위한 보안 자격 증명을 이용한다. 이어서, IP 데이터그램(1632)이 유선 또는 섬유 링크(24)를 경유하여 라스트 마일을 통해 네트워크 라우터(27)까지 라우팅되고, 그 후에 셀룰러 네트워크(25) 및 셀룰러 링크(28)를 통해서 휴대폰(32)까지 라우팅된다. 휴대폰(32)이 SDNP 클라이언트이기 때문에, 라스트 마일을 통한 통신은 하이퍼보안을 유지한다. 이러한 단순화된 예에서, 라스트 마일 상으로 클라우드를 빠져나가는 모든 데이터 패킷은 단일 SDNP 게이트웨이(1601B)로부터 라우팅된다. 실제로, 하나 초과의 SDNP 게이트웨이가 라스트 마일 데이터 라우팅에서 이용될 수 있다.

[0728] **"콜 아웃"을 위한 라스트 마일 통신이 도 73b에 도시되어 있다. 비록 SDNP** 클라우드를 통한 라우팅이, SDNP 클라이언트에 대한 통화에서와 같이, 동일한 SDNP 데이터그램(1631A 및 1631B)을 이용하지만, SDNP 게이트웨이(1601B)는 SDNP 소프트웨어를 작동하는 마지막 서버이다. 그에 따라, 콜 아웃에서의 라스트 마일 통신은 비-SDNP 페이로드를 갖는 IP 데이터그램을 이용하고, 즉 IP 데이터그램(1635)이, IP 어드레스 IP $C_{7,9}$에서 게이트웨이 IP $M_{0,0}$으로부터 PSTN까지 라우팅되어 VoIP 형태의 소리를 운반한다. 이어서, PSTN은 전화 # 및 소리 패킷(1636) 내의 아날로그 소리를 이용하여 VoIP 통화 포맷을 통상적인 전화 번호로 변환한다. 그러한 경우에, 라스트 마일은 하이퍼보안 통신을 구성하지 않는다.

[0729] 도 74에 도시된 다중경로 라스트 마일 통신에서, SDNP 시그널링 서버(1603A)에 의해서 분배된 명령 및 제어 데이터 패킷은 데이터 링크(1612 및 1610)를 통해서 클라이언트(1600)에 송신된 C&C 데이터 패킷(1625X), 데이터 링크(1614X)를 통해서 SDNP 게이트웨이(1601X)에 송신된 C&C 데이터 패킷(1627X), 및 데이터 링크(1614Y)를 통해서 SDNP 게이트웨이(1601Y)에 송신된 C&C 데이터 패킷(1627Y)을 포함한다. 다른 C&C 데이터 패킷(미도시)은 데이터 링크(1614X)를 통해서 미디어 노드를 호스팅하는 다른 서버로 송신된다. 어드레스 "IP S"로부터, 라스트 마일 라우팅(U1)을 포함하는 C&C 페이로드를 포함하는 어드레스 "IP $C_{1,1}$"으로 C&C 데이터 패킷(1625X)이 송신된다. 라스트 마일 라우팅(U1)은 2개의 상이한 라우팅 지시 - 태그 1 및 프리앰블 1을 가지고 "IP $C_{1,1}$"로부터 "IP $M_{0,0}$"로의 라우팅 지시, 및 태그 2 및 프리앰블 2를 가지는 "IP $C_{1,1}$"로부터 "IP $M_{0,1}$"로의 다른 라우팅 지시를 포함한다. 예로서 도시된, SDNP 클라우드 내의 통신 노드에 송신된 C&C 데이터 패킷은, 지시 SDNP 클라우드 라우팅 1을 포함하는 "IP S"로부터 "IP $M_{0,0}$"로 송신된 것, 및 SDNP 클라우드 라우팅 2를 포함하는 "IP $M_{0,1}$"으로 송신된 것을 포함한다.

[0730] ***SDNP 그룹 통화(SDNP Group Call)*** - 도 75a에 도시된, SDNP 클라이언트(1600)로부터 다수의 SDNP 게이트웨이로의 라스트 마일 미디어 패킷 라우팅은, 각각의 헤더(1626X 및 1626Y) 그리고 SDNP 미디어 페이로드 SDNP 데이터(X) 및 SDNP 데이터(Y)를 포함하는 2개의 데이터 패킷(1630X 및 1630Y)를 포함한다. 태그 1 및 프리앰블 1을 갖는 데이터 헤더(1626X)는 어드레스 "IP $C_{1,1}$"로부터 "IP $M_{0,0}$"으로 라우팅되는 한편, 태그 2 및 프리앰블 2를 갖는 데이터 헤더(1626Y)는 어드레스 "IP $C_{1,1}$"로부터 "IP $M_{0,1}$"로 라우팅된다.

[0731] 도 75b에 도시된 바와 같이, 다중-경로 통신을 이용하여 SDNP 클라우드로부터 클라이언트로 역방향으로 흐르는 데이터는 헤더(1626U), 태그 8, 프리앰블 8, SDNP 데이터(U), 소스 어드레스 SDNP 게이트웨이 어드레스 $M_{0,0}$ 및 목적지 어드레스 "IP $C_{0,0}$"을 포함하는 데이터 패킷(1630U)을 포함한다. 동시에, 데이터는 또한 헤더(1626V), 태그 9, 프리앰블 9, SDNP 데이터(V), 소스 어드레스 SDNP 게이트웨이 어드레스 $M_{0,1}$, 및 목적지 어드레스 "IP $C_{0,0}$"을 포함하는 데이터 패킷(1630V)을 포함한다. 이어서, SDNP 클라이언트(1600)에서 작동되는 SDNP 애플리케이션 프로그램이 진입 데이터 패킷 SDNP 데이터(U), SDNP 데이터(V), 및 다른 것을 조합하여 메시지 텍스트 또는 보이스(소리)를 재생성한다.

[0732] 라우팅 지시의 C&C 데이터 패킷 전달이 확장되어 3-방향 또는 그룹 통화, 그룹 메시징, 및 다른 다수-클라이언트 통신을 개시할 수 있다. 그러한 그룹 코뮤니케 또는 "컨퍼런스 콜"에서, 클라이언트 메시지가 다수의 수신자에게 동시에 송신된다. 이러한 그룹 기능은 통화자에 의해서 시작되고, 그룹 통화를 위한 통화자의 요청은 먼저 접촉하고자 하는 클라이언트의 그룹을 규정하고, 이어서 시그널링 서버에 의해서, 특정 그룹 통화와 연관된 데이터 패킷의 라우팅을 어떻게 핸들링할 지를, 요구된 미디어 노드에 지시한다. 그룹 통화 라우팅 지시의 예가 도 76에 도시되어 있고, 여기에서 시그널링 서버(1603P)는 라우팅 지시를 데이터 링크(1614A)를 거쳐 SDNP 클라이언트(1600A)로 그리고 데이터 링크(1614Z)를 거쳐 SDNP 클라우드 내의 많은 미디어 서버(1600Z)로 통신한다.

[0733] 따라서, 라스트 마일 라우팅(U1)을 포함하는 TCP 데이터 패킷(1627A)은 어드레스 "IP S1"에서의 시그널링 서버(1603P)로부터 어드레스 "IP $C_{1,1}$"에서의 SDNP 클라이언트로 전달되어, 통화자와의 그룹 통화를 "설정"한다. 예

시적인 TCP 데이터 패킷(1627Z)에 의해서 제공되는 C&C 데이터 패킷은 데이터 링크(1614Z)를 통해서 시그널링 서버 어드레스 "IP S1"로부터 다양한 목적지 어드레스 "IP $M_{0,y}$"로 구역(Z1)을 위한 SDNP 클라우드 전체를 통해서 동시에 분배되고, 여기서 y는 정수 변수를 나타낸다. 집합적으로, SDNP 클라우드 라우팅 지시는 통화자의 게이트웨이로부터 SDNP 클라우드 전체를 통해서 통화되는 SDNP 클라이언트에 가장 가까이 위치된 둘 이상의 다른 SDNP 게이트웨이로 라우팅되는 패킷을 구축한다.

[0734] 예로서 도시된 바와 같이, 다른 SDNP 클라이언트는 상이한 지리적 영역 내에 위치될 수 있고, 분리된 보안 구역, 예를 들어 구역(U7 및 U9) 내에 있을 수 있다. 일부 경우에, 이러한 클라이언트는 시그널링 서버(1603P)로부터 충분히 멀 수 있고, 그에 따라 다른 시그널링 서버(1603Q)가 이러한 SDNP 클라이언트를 위한 패킷 라우팅을 계획하는데 이용될 수 있다. 시그널링 서버(1603Q)는 구역(U9) 내의 라우팅 지시를 데이터 링크(1614M)를 통해서 SDNP 클라이언트(1600M)으로 그리고 데이터 링크(1614L)를 통해서 SDNP 클라이언트(1600L)로 통신한다. C&C 데이터 패킷(1625M)은, 예를 들어, "IP S4"에 위치되는 시그널링 서버로부터 어드레스 "$C_{9,1}$"에 위치되는 SDNP 클라이언트(1600M)까지 라스트 마일 라우팅 지시(U9)를 통신한다. 다른 C&C 데이터 패킷(미도시)이 유사하게 어드레스 "IP $C_{9,4}$"에 위치되는 SDNP 클라이언트에 송신된다. 라스트 마일 라우팅(U7)을 위한 지시를 포함하는 데이터 패킷(1627H)은 데이터 링크(1614H)를 통해서 "IP S4"에 위치되는 시그널링 서버(1603Q)로부터 어드레스 "IP $C_{7,1}$"에 위치되는 클라이언트(1600H)로 송신된다.

[0735] 노드(S1 및 S4)에 위치되는 시그널링 서버(1603P 및 1603Q)는 또한 데이터 링크(1613z)를 통해서 C&C 데이터 패킷으로서 정보를 교환한다. 이러한 정보는 라우팅의 어느 부분이 시그널링 서버(1603P)에 의해서 실시될 것인지 그리고 어느 부분이 시그널링 서버(1603Q)에 의해서 실시될 것인지를 구성하여, 본질적으로 라우팅 과제를 다수의 시그널링 서버에 걸쳐 분할하는 데 사용된다. 도시된 예에서, 시그널링 서버 노드(S1)는 구역(U1)을 위한 그리고 SDNP 클라우드를 위한 라스트 마일 라우팅을 관리하는 한편, 시그널링 서버 노드(S4)는 구역(U7 및 U9) 내의 라스트 마일 통신을 관리한다.

[0736] 통화 또는 코뮤니케 중의 데이터 라우팅이 도 77a에 도시되어 있고, 여기에서 데이터 패킷(1630A) 내의 SDNP 데이터 1에 의해서 수반되는 보이스가 헤더(1626A)에 의해서 IP 어드레스 "IP $C_{1,1}$"를 갖는 통화자로부터 가장 가까운 SDNP 게이트웨이 미디어 노드 $M_{0,0}$으로 라우팅된다. 데이터 패킷은 SDNP 클라우드 전송을 위해서 재-패킷화되고 게이트웨이 미디어 노드 $M_{0,4}$ 및 $M_{0,8}$로 송신된다. SDNP 클라우드에서 취해지는 통로 패킷 라우팅은 컨퍼런스 콜 참여자 중 어느 누구에게도 알려지지 않으며, 어떠한 중앙 제어도 없고 네트워크 조건에 따라 동적으로 변화된다. 이러한 예에서, SDNP 클라우드 내의 모든 SDNP 데이터 패킷은 익명 어드레싱 및 동적 암호화를 갖는 단편화된 메시형 데이터 전송을 이용할 뿐만 아니라, 동적 스크램블링, 혼합, 분리, 정크 데이터 삽입 및 제거를 이용한다. 도시된 예에서, 클라우드 전송은 SDNP 게이트웨이 노드 $M_{0,0}$에서의 진입 통신을 다른 게이트웨이로, 이 경우에 SDNP 게이트웨이 노드 $M_{0,4}$ 및 $M_{0,8}$ 로 지향시킨다.

[0737] 통화자의 음성을 수반하는 데이터 패킷(1630H) 즉, SDNP 데이터 1은 게이트웨이 노드 $M_{0,4}$를 빠져나가고, 헤더(1626H)를 이용하여, 구역(U7) 보안 자격 증명을 이용하여 "IP $M_{0,4}$ "에서의 미디어 노드로부터 "IP $C_{7,1}$"에서의 클라이언트(1600H)까지 라우팅된다. 헤더(1626H)는, 도 76에서 설명된 바와 같이, 미디어 데이터 패킷을 준비하기 전에, C&C 데이터 패킷(1627A) 내의 클라이언트(1600A)에 공급되었다. 이러한 방식으로, 실시간 데이터를 수반하는 모든 미디어 패킷이, 데이터 전송을 위해서 콘텐츠가 준비될 때, 지연 없이 준비될 수 있다. 실시간 네트워크에서, 큰 QoS는 동적 데이터의 적시의 라우팅에 의존한다. 그렇지 않은 경우에, 허용될 수 없는 긴 전파 지연이 초래될 수 있다.

[0738] SDNP 클라우드를 통해서 일단 라우팅되면, SDNP 데이터 1 페이로드가, 게이트웨이 미디어 노드 $M_{0,8}$로부터 클라이언트 IP 어드레스 "IP $C_{9,1}$" 및 "IP $C_{9,4}$"까지, 구역(U9) 컨퍼런스 콜 참여자에게, 즉 SDNP-클라이언트(1600M 및 1600L)에 전달된다. 이러한 라스트 마일 데이터 패킷(1630M 및 1630L)은, 동일 대화와 연관된 콘텐츠를 인식하기 위해서 사용되는 식별 패킷 태그들, 태그 8, 및 태그 9, SDNP 임베딩된 지시를 운반하기 위해서 이용되는 프리앰블 9 정보, 키, 시드 등, 그리고 UDP로서 계층 4 전송을 규정하기 위해서 사용되는 "L4" 데이터 필드를 특정하는 헤더(1626M 및 1626L)를 포함한다. 비록 정확성 보장을 위해서 시그널링 서버에 의해서 전달된 데이터 라우팅 지시가 TCP 전송 프로토콜을 이용하지만, 미디어 패킷 콘텐츠는 실시간 데이터를 나타내고, 그에 따라 TCP 대신에 UDP 계층 4 프로토콜을 유리하게 이용한다.

[0739] 도 77b는, 구역(U7) 클라이언트(1600H)로부터의 콘텐츠가 발생되는 동일 대화 - 즉 클라이언트 $C_{7,1}$가 말하기를 시작하는 때를 도시한다. 이러한 데이터를 클라이언트 $C_{1,1}$로부터의 보이스 콘텐츠와 대비하기 위해서, 페이로드가 모든 데이터 패킷 내에서 "SDNP 데이터 5"로서 식별된다. 특이적인 페이로드 이외에, 이전 개략도로부터의 유일한 변화는, 데이터 패킷(1630H 및 1630A)을 위한 라스트 마일 소스 및 목적지 IP 어드레스가 스왑된다는 것이다. 구체적으로, 구역(U7) SDNP 사용자를 위해서, 데이터 패킷(1630H)을 위한 소스 IP 어드레스가 IP $C_{7,1}$로 변화되고, 그 목적지는 SDNP 게이트웨이 어드레스 IP $M_{0,4}$가 된다. 구역(U1)에서, 데이터 패킷(1630A)을 위한 피통화자 목적지 IP 어드레스가 IP $C_{1,1}$로 변화되고, 그 소스 어드레스는 SDNP 게이트웨이 어드레스 IP $M_{0,0}$이 된다. 몇몇 컨퍼런스 콜 참여자가 동시에 말할 수 있다는 것 그리고 클라이언트 노드 $C_{7,1}$을 포함하는 다른 통화 참여자에게 송신된 SDNP 클라이언트 노드 $C_{1,1}$로부터의 데이터 패킷이 클라이언트 노드 $C_{1,1}$에 응답하는 클라이언트 노드 $C_{7,1}$에 대해서 동시에 발생될 수 있다는 것을 이해하여야 한다.

[0740] 라스트 마일 통신의 네트워크 레벨 3에서, 반대 방향 트래픽의 데이터 충돌은 발생되지 않는다. 그러나, 물리적 및 데이터 링크 계층 1 및 2에서, 라스트 마일 통신은, 동일 통신 링크를 위한 경쟁을 방지하기 위한 시분할을 포함할 수 있다. 그러나, 이러한 조정이 신속하게 발생되고, 그에 따라 통신은, 보이스 패킷 내에서 지연이 없이, 완전히 동시적인 방식인 것으로 보이기 쉽다. 도 77a 및 도 77b 모두에서, 구역(U9) 클라이언트에 대해서 도시된 데이터 흐름의 방향은 변화되지 않고 유지되고, 즉 데이터는 클라우드로부터 클라이언트로 흐른다는 것을 주목해야 한다. 그러나, 도 77c에서, 구역(U9) 클라이언트 노드 $C_{9,1}$가 말하기 시작한다. 이러한 경우에, 클라이언트 노드 $C_{9,4}$, $C_{1,1}$, 및 $C7_{,1}$ 모두가 보이스의 수신자, 즉 SDNP 보이스 데이터 6가 된다.

[0741] 도 78에 도시된 대안적인 실시예에서, 그룹 통화가 SDNP 클라이언트에 대한 SDNP 통화의 그리고 정규 전화 번호에 대한 "콜 아웃" 통화의 혼합을 포함할 수 있다. 도 77a에 도시된 통화 또는 코뮤니케와 유사하게, 데이터 패킷(1630A) 내의 SDNP 데이터 1에 의해서 수반되는 보이스가 헤더(1626A)에 의해서 IP 어드레스 "IP $C_{1,1}$"를 갖는 통화자로부터 미디어 노드 $M_{0,0}$을 포함하는 가장 가까운 SDNP 게이트웨이로 라우팅된다. 데이터 패킷은 SDNP 클라우드 전송을 위해서 재-패킷화되고 게이트웨이 미디어 노드 $M_{0,4}$ 및 $M_{0,8}$로 송신된다.

[0742] 도시된 예에서, 클라우드 전송은 SDNP 게이트웨이 노드 $M_{0,0}$에서의 진입 통신을 다른 게이트웨이로, 이 경우에 SDNP 게이트웨이 노드 $M_{0,4}$ 및 $M_{0,8}$ 로 지향시킨다. 통화자의 음성을 수반하는 데이터 패킷(1630H) 즉, SDNP 데이터 1은 게이트웨이 노드 $M_{0,4}$를 빠져 나가고, 헤더(1626H)를 이용하여, 구역(U7) 보안 자격 증명을 이용하여 "IP $M_{0,4}$ "에서의 미디어 노드로부터 "IP $C_{7,1}$"에서의 클라이언트(1600H)까지 라우팅된다. SDNP 데이터 1 페이로드가 또한 게이트웨이 미디어 노드 $M_{0,8}$을 통해서 컨퍼런스 콜 참여자에게 전달된다. 이러한 SDNP 게이트웨이로부터의 라스트 마일 통신은 2개의 상이한 유형의 연결, 구체적으로 SDNP-클라이언트(1600M)에 대한 하이퍼보안 연결 및 VoIP 또는 패킷 프로토콜을 이용하지 않는 통상적인 전화 시스템을 포함하는 PSTN 1에 대한 미보안 "콜 아웃" 연결을 포함한다. 어드레스 "IP $C_{9,1}$"에서 구역(U9) SDNP 클라이언트에 전달되는 라스트 마일 데이터 패킷(1630M)은, 동일 대화와 연관된 콘텐츠를 인식하기 위해서 사용되는 식별 패킷 식별자 태그 9, SDNP 임베딩된 지시를 운반하기 위해서 이용되는 프리앰블 9 정보, 키, 시드 등, 그리고 UDP로서 계층 4 전송을 규정하기 위해서 사용되는 "L4" 데이터 필드를 특정하는 헤더(1626M)를 포함한다.

[0743] 게이트웨이 노드 $M_{0,8}$ 은 또한 어드레스 IP $C_{7,9}$에서 IP 패킷(1635)을 PSTN 1에 송신한다. SDNP 데이터 1을 포함하는 페이로드를 운반하는 대신, 이러한 경우에, IP 페이로드는, 패킷 스니핑으로 가로챌 수 있는 것인, VoIP 소리 패키지로 변환되었다. 이어서, 전화 스위치 시스템인 PSTN 1이 이러한 미보안 IP 패킷을, 전화(37)와 PSTN 1 사이의 연속적인 아날로그 회로 연결이 뒤따르는 통화되는 전화 번호를 포함하는 POTS 데이터(1636)에 의해서 도시된 전화(37)에 대한 아날로그 POTS 전화 연결로 변환한다. 이러한 그리고 임의의 다른 콜 아웃 연결이 하이퍼보안이 아니기 때문에, 콜 아웃 라스트 링크에 의해서 운반되는 콘텐츠는 해킹, 와이어탭, 및 다른 감시 기술의 위험이 있다. 클라이언트의 액세스 특권을 규정하는 일부 계층적 구조가 구현되지 않으면, 전체 통화의 보안은 가장 약한 링크에 의해서 손상될 수 있고, 이는 그룹 통화 상의 모든 사람이 모든 것을 들을 수 있다는 것을 의미한다.

[0744] 이러한 포인트가 도 79a에 도시된 표에 예시되어 있고, 여기에서 그룹 통화는, 전화 번호 "Ph #1" 및 "Ph #2"에

서의 콜 아웃 참여자와 함께, SDNP 네트워크 클라이언트 노드 $C_{1,1}$, $C_{7,1}$, $C_{9,1}$, 및 $C_{9,4}$ 상의 하이퍼보안 참여자를 포함한다. 도시된 바와 같이, SDNP 클라이언트 $C_{1,1}$는 그룹 호스트이고, SDNP 클라이언트 $C_{7,1}$, $C_{9,1}$은 참여자이고, 이는 이들이 청취하고 말한다는 것을 의미하고, SDNP 클라이언트 $C_{9,4}$는 "청취자이고, 이는 이들이 통화를 청취하지만 말할 수 없거나 참여자가 청취할 수 있다는 것을 의미한다. 콜 아웃 전화 번호 "Ph #1"에서의 참여자는 또한 청취 및 말하기가 가능한 참여자인 한편, "Ph #2"에서의 참여자는 단지 콜 아웃 "청취자"로 인증되었고, 그룹 통화에서 말을 할 수 없다. 그룹 호스트는, 통화를 설정할 때, 이러한 듣기 말하기 특권, 즉 사용자 인증을 규정한다.

[0745] 표를 다시 참조하면, 정규 통화로 명명된 열에서, 그룹 통화 상의 모든 사람 즉, 호스트에 의해서 승인된 통화자는 통화를 청취할 수 있다는 것을 주목해야 한다. 통화를 해킹하고자 하나 호스트에 의해서 승인받지 못한 통화자는 통화에 연결 또는 침입할 수단 또는 심지어 통화가 발생되는지를 결정할 능력을 가지지 못한다. 동일 방법이 그룹 채팅에 적용될 수 있고, 여기에서 참여자는 메시지를 읽고 쓸 수 있지만, 관찰만 가능한 구성원은 코멘트를 읽을 수만 있고 그들의 텍스트를 채팅에 끼워 넣을 수 없다.

[0746] 이러한 개시 내용에 따라 만들어진 네트워크 액세스를 제어하기 위한 인증 및 신원 확인을 이용할 때, SDNP 시스템은, 통상적인 그룹 채팅 및 그룹 통화에서 이용될 수 없는, 프라이버시 특징을 제공한다. 이러한 특징은, 텍스트 작성 또는 말하기 전에, 프라이빗 모드를 선택함으로써, 예를 들어 잠금 심볼 또는 다른 프라이버시 아이콘을 클릭하는 것에 의해서 생성된다. 그러한 경우에, 통신은, 인증된 SDNP 클라이언트에게만 송신되고, 인증을 통해서 신원이 아직 확인되지 않은 SDNP 클라이언트에게는 송신되지 않으며 미보안 디바이스 상의 임의의 콜 아웃 청취자 또는 참여자에게는 송신되지 않는다. 이러한 포인트가 전술한 표에 명시되어 있으며, 여기에서, "미인증 SDNP 클라이언트"라고 표시된 열 아래의 프라이빗 통화에서, 모든 그룹 통화 클라이언트는 그들의 마이크로폰 및 스피커 모두가 묵음화된 반면, "인증된 SDNP 클라이언트"라고 표시된 열에서, 모든 SDNP 클라이언트는 청취할 수 있고, 참여자 $C_{1,1}$, $C_{7,1}$, 및 $C_{9,1}$는 또한 말할 수 있으나, 모든 콜 아웃 디바이스는 그들의 마이크로폰 및 스피커가 무음화되었고, 이는 프라이빗 모드에서 인증된 SDNP 클라이언트만이 듣고 말할 수 있다는 것을 의미한다. 이러한 방식으로, 확실한 신원의 SDNP 클라이언트들의 혼합, 및 알지 못하는 당사자와의 콜 아웃 연결을 갖는 그룹 통화는 통화의 공공 부분에서 상호 참여할 수 있으나, 비밀 정보를 콜 아웃 디바이스에 노출시키지 않는다. 말하기 또는 텍스트 작성 전에 임의의 SDNP 참여자의 프라이빗 아이콘을 클릭하는 것에 의해서, "콜 아웃" 통화자가 프라이빗 토론으로부터 간단히 제거될 수 있다. 프라이빗 토론의 종료 시에, 프라이빗 버튼이 해제되고 그들이 재 연결된다. 콜 아웃 통화자가 연결되지 않은, 즉 본질적으로 "통화 대기"에 배치된 시간 동안, SDNP 시스템은 대기 음악을 재생할 수 있거나, 조용히 있거나, (파도 소리 또는 빗소리와 같은) 백색 소음을 재생할 수 있다.

[0747] 그룹 채팅에서의 텍스트 메시지가 또한 동일한 방식으로 관리될 수 있다. 정규 그룹 채팅에서, 모든 텍스트 메시지가 SDNP 클라이언트 디바이스 상의 SDNP 앱에 송신되고, SMS 텍스트 메시지에 의해서 모든 콜 아웃 채팅 구성원에게 송신된다. 텍스트 메시지는 참여자에 의해서만 송신될 수 있다. "청취자" 또는 "일기 전용" 채팅 구성원으로부터 송신된 텍스트 메시지는 무시되고 채팅 그룹으로 포워딩되지 않을 것이다. 메시지를 보내기 전에 참여자가 잠금 또는 프라이버시 아이콘을 클릭한 경우에, 그 메시지는 SDNP 클라이언트에게만 송신될 것이고 모든 콜 아웃 클라이언트에게 전송되지는 않는다. 프라이빗 메시지를 수신하는 SDNP 클라이언트에서, 이들이 그 신원을 인증하였다면, 메시지는 판독을 위해서 보여질 수 있을 것이다. 이들이 그 신원 인증을 하지 않은 경우에, 관찰자가 그 신원 확인을 위한 인증을 실시할 때까지, 메시지는 은폐되고, 덮여지고, 감춰지고, 또는 아이콘, 예를 들어 자물쇠로 표시될 것이다.

[0748] SDNP 네트워크 시스템 인증에 의해서 규제되는 프라이버시 특권과 신원 확인을 조합함으로써, 디바이스의 해킹은, 그룹 채팅 및 그룹 통화에서도, 프라이빗 텍스트를 열거나 프라이빗 통화를 청취하기에 불충분하다. 이러한 특징은 디바이스 보안 매개변수 - 지역적으로 해킹될 수 있는 정보 - 에만 의존하는 것에 의해서는 보장될 수 없다. 시스템 매개변수는 속이기가 훨씬 더 어려운데, 이는 가짜 보안 및 신원 자격 증명이 시스템 로그와 일치되지 않을 것이고 무효 SDNP 클라이언트로서 거절될 것이기 때문이다.

[0749] 부가적인 정도의 프라이버시가 또한 그룹 통화 및 그룹 채팅의 실행에 부가될 수 있다. 도 79b에 도시된 표에 설명된 하이퍼보안 라스트 마일의 이러한 특이적 실시예가 본원에서 하이퍼-프라이빗 통화 또는 하이퍼-프라이빗 채팅으로 지칭된다. 하이퍼-프라이버시는 이하의 4개의 기준에 대한 통화자 또는 메시지 확인을 필요로 한다:

[0750] * 그룹 통화 상의 코뮤니케의 모든 수신자는 SDNP 클라이언트이어야 하고, 콜 아웃 디바이스는 아니어야 한다.

[0751] * 통화 또는 텍스트는, 통화, 텍스트, 화상 등이든 간에, 선험적으로 하이퍼-프라이빗 코뮤니케로서 선택되어야 한다.

[0752] * 그룹 통화 또는 채팅 상의 코뮤니케의 수신자는 그 신원 보장을 위해서 인증된 연결을 가져야 한다.

[0753] * 임의의 하이퍼-프라이빗 코뮤니케의 수신자는 "프라이빗" 참여자 또는 프라이빗 청취자로서 미리 선택되어야 한다.

[0754] 비록 처음 3개의 기준은 본질적으로 전술한 그룹 통화에서의 프라이빗 당사자의 예에서의 기준과 동일하고, 제4 기준인, 하이퍼-프라이빗 통화 또는 텍스트를 수신할 수 있는 자격이 있는 임의의 통화자가 "프라이빗" SDNP 클라이언트로서 미리 규정된 클라이언트의 목록이 로딩되어야 한다는 요건이 특이적이고 민감한 정보에 대한 액세스를 더 제한한다. 예를 들어, 막대 형태로 도시된 바와 같이, SDNP 참여자 클라이언트 $C_{1,1}$ 및 $C_{7,1}$, 그리고 SDNP 청취자 클라이언트 $C_{9,4}$는 모두 그룹 통화에서 "프라이빗" 당사자로서 지정된다. 대조적으로, SDNP 클라이언트 $C_{9,1}$는 참여자로서만 지정되나, 프라이빗 참여자로서는 지정되지 않는다. 정의에 의해서, 통화 참여자 또는 청취자는 프라이빗 당사자로서 등록될 수 없다.

[0755] 이전의 예에서와 같이, 정규 통화 중에 모든 참여자, 즉 SDNP 클라이언트 $C_{1,1}$, $C_{7,1}$, 및 $C_{9,1}$ 그리고 콜 아웃 참여자 Ph #1는 모든 대화를 들을 수 있고 모든 텍스트 메시지를 읽을 수 있을 뿐만 아니라, 언제든지 말하고 텍스트를 쓸 수 있는 반면 클라이언트 $C_{9,3}$ 및 Ph #2를 포함하는 "청취자"는 모든 대화를 듣고 텍스트를 볼 수 있지만, 그룹 통화 또는 채팅에서 말하거나 메시지를 송신할 수 없다. 그러나, 하이퍼-프라이빗 통화에서, 하이퍼-프라이빗 코뮤니케를 지정하기 위한 스위치 또는 아이콘을 선택하는 것은, 그룹 통화 또는 채팅 상의 모든 미인증 당사자를 자동적으로 차단할 뿐만 아니라, 이는 "프라이빗" 당사자 이외의 모든 당사자를 디스에이블링시킨다. 이는 또한 모든 콜 아웃 연결 및 모든 미인증 사용자를 디스에이블링시킨다. 따라서, 동작에서, 임의의 프라이빗 참여자가 프라이버시 아이콘을 선택할 때, (프라이빗 그룹 호스트를 포함하는) 프라이빗 참여자만이 그룹에 대해서 보고, 읽고, 말하고, 텍스트 작성을 할 수 있다. 모든 다른 당사자의 마이크로폰 및 스피커가 묵음화되고, 마찬가지로 그룹에 대한 텍스트 또는 첨부물을 수신 또는 송신할 수 없다. 구체적으로, 하이퍼-프라이빗 모드에서, 일단 인증되면, 클라이언트 $C_{1,1}$ 및 $C_{7,1}$모두가 듣고 말할 수 있을 뿐만 아니라 텍스트를 읽고 송신할 수 있는 반면, 프라이빗 클라이언트 $C_{9,4}$는 대화를 듣거나 그룹 텍스트를 판독할 수만 있다.

[0756] 전술한 라스트 마일 라우팅 제어 능력으로, 그룹 통화 및 그룹 채팅이 임의의 수의 방식으로 관리될 수 있다. 예를 들어, 그룹 통화 호스트는, 통화 또는 그룹에 참여할 수 있는 사람, 말하거나 텍스트를 작성할 수 있는 사람, 및 듣기 및 읽기만을 할 수 있는 사람을 결정할 수 있다. 표준 프라이빗 통화에서, 프라이빗 모드의 선택은 모든 SDNP 클라이언트를 인에이블링시키고, 일단 인증되면, 표준 비-프라이빗 그룹 통신 중에 그들이 가지는 것과 동일한 특권으로 코뮤니케에 결합시킨다. 하이퍼-프라이빗 모드에서, 프라이빗 참여자 및 프라이빗 청취자로서 규정된 SDNP 클라이언트 만이 하이퍼-프라이빗 모드 동작 중에 통신할 수 있다.

[0757] 하이퍼-프라이빗 코뮤니케의 일부에 대해서 자격을 가진 사람 즉, 프라이빗 참여자 또는 청취자로서 식별된 사람 그리고 그렇지 못한 사람의 선택이 몇 가지 방식으로 구성될 수 있다. 애드혹 하이퍼-프라이빗 그룹 통신에서, 그룹 호스트는 누가 프라이빗 통화자인지 그리고 누가 아닌지를 결정한다. SDNP "시스템 규정된" 하이퍼-프라이빗 그룹 통신에서, SDNP 네트워크 운영자는 누가 프라이빗 통화자이고 누가 아닌지를 미리 결정한다. 규칙-기반 하이퍼-프라이빗 그룹 통신에서, SDNP 네트워크는 누가 프라이빗 통화자가 될 자격이 있고 누가 아닌지를 결정하기 위한 규칙을 규정한다. 이러한 규칙이 회사 고용 목록을 기초로 할 수 있고, 예를 들어 부사장 이상만이 하이퍼-프라이빗 통화에 참여할 수 있다. 정부 및 보안 기관에서, 기준은 국가 보안 허가, 여권 번호, 경찰 뱃지 번호, 등에 의해서 설정될 수 있다. 본원에서 규정된 SDNP-인에이블드 라스트 마일 통신 방법은 이러한 예시적인 시나리오 중 임의의 것을 지원할 수 있거나, 개체군을 2개의 그룹으로 양분하기 위한 임의의 다른 기준을 이용할 수 있고, 그에 의해서 하이퍼-프라이빗 코뮤니케 액세스를 가지는 그룹과 그렇지 않은 그룹을 구성한다.

[0758] 그러한 개념이 하나 초과의 그룹으로 확장될 수 있으나, 계층적 액세스 기준이 일반적으로, 전화 통신보다, 운항관리기-기반의 전문적 통신 시스템에 보다 잘 적용될 수 있다. 그에 따라, 전문적 통신을 위한 SDNP 방법의 적용을 본원에서 더 설명하지 않을 것이다.

[0759] 그룹 통화를 위한 하나의 해결과제는 모든 사람이 동시에 말하고자 하는 경우의 문제이다. 중첩 발언은 혼란스럽고, 듣기 어렵고, 또한 원치 않는 잡음을 초래할 수 있다. 이러한 문제는, 워키-토키 또는 CB 라디오를 모방한 기능인, 푸시-투-토크 특징을 이용함으로써 해결될 수 있다. 푸시-투-토크 또는 PTT 동작에서, 한번에 한명의 참여자만이 말할 수 있다. 참여자가 말하고자 할 때, 스위치를 누르는 것은 네트워크 마이크로폰 상의 모든 다른 사람을 묵음화하여, 그룹 통화 내의 모든 다른 당사자가 듣기 전용 모드가 되게 한다. 도 80a의 표에 기재된 바와 같이, 정규 PTT 대화에서, 호스트가 PTT 버튼을 누를 때, 호스트 PTT로 표시된 열에 도시된 바와 같이, 이들은 그룹 통화보다 우선권을 가지고, 다른 통화자가 그들의 말하기 버튼을 눌렀을 때에도, 모든 다른 통화자보다 우선한다. 콜 아웃 전화 연결을 포함한, 모든 다른 통화자의 마이크로폰이 자동적으로 묵음화되고, 단지 청취자가 된다. 호스트가 그의 PPT 버튼을 누르지 않는 경우에, "다른 PTT"로 표시된 열에서 도시된 바와 같이, PTT 능력은 실행 순서대로 임의의 다른 SDNP 참여자에게 넘겨진다. 청취자로 지정된 SDNP 노드 및 콜 아웃 디바이스, 예를 들어 $C_{9,4}$ 및 Ph #1는, 전체 그룹 통화 중에, PTT 대화를 들을 수 있으나, 그들의 마이크로폰은 묵음화된다.

[0760] 네트워크에 대해서 신원이 인증된 통화자를 식별하기 위해서 SDNP 라스트 마일 능력의 이용할 때, PTT 특징이 프라이빗 푸시-투-토크 기능까지 확장될 수 있다. 프라이버시 특징 또는 아이콘이 선택될 때마다, 모든 미인증 당사자가 그룹 통화로부터 제거되고, 그들의 스피커 및 마이크로폰이 묵음화된다. 규정에 의한 콜 아웃 연결은 인증될 수 없고, 그에 따라 또한 묵음화된다. 묵음화는 양방향적이고, 배제된 당사자가 대화를 청취하는 것을 방지하나, 또한 배제된 참여자의 마이크로폰을 또한 분리한다. 인증된 당사자의 경우에, 동작이 정규 PTT와 동일하게 진행되고, 여기에서 호스트는 말하는데 우선권을 가지며, 그렇지 않은 경우에 임의의 인증된 참여자가 실행 순서대로 PTT 토크 특징을 가질 수 있다.

[0761] 도 80b의 표는, 하이퍼-프라이빗 그룹 통화가 PTT 기능으로 확장될 수 있다는 것을 도시한다. 정규 동작에서, PTT 기능성은 전술한 경우와 동일하다. 그러나, 하이퍼-프라이빗 모드에서, 프라이빗 참여자 또는 프라이빗 청취자로서 이전에 지정된 인증된 당사자만이 하이퍼-프라이빗 대화에 참여할 수 있다. 예를 들어, 하이퍼-프라이빗 모드에서, SDNP 클라이언트 $C_{9,1}$ 및 $C_{9,5}$는 말하기 또는 듣기로부터 차단되는데, 이는 그들이 프라이빗 참여자 또는 청취자로서 이전에 나열되지 않았기 때문이다. 유사하게, 디바이스에 연결된 모든 콜 아웃은 하이퍼-프라이빗 모드 동작 중에 묵음화된다. 이러한 방식으로, PTT 그룹 통화 내의 여러 당사자에 대한 액세스가 명확하게 제어될 수 있다. 묵음화는 일부 참여자(예를 들어, 콜 아웃 청취자)를 대화의 소리를 운반하는 데이터 패킷을 수신하는 것으로부터 배제하는 한편, 묵음처리되지 않은 참여자에 대한 데이터 패킷은 계속 공급하는 프로세스이다. 이러한 개시된 방법에서, 데이터 패킷은 일반 대화에서 모든 참여자에게 그리고 클라이언트의 사용자에 의해서 묵음화가 활성화될 때 목록의 서브세트에만 개별적으로 송신된다.

[0762] 대안적인 실시예에서, 데이터 패킷은 방송 모드로 그룹 통화 내의 모든 참여자에게, 그러나 상이한 암호 방법들을 이용하여, 송신된다. 일반적인 컨퍼런스 콜의 경우에, 데이터 패킷은 암호를 이용하여 모든 사용자에게 송신되고, 여기에서 모든 참여자는 해독 키의 복사본을 갖는다. 프라이빗 모드 또는 묵음 모드에서, 사용자에게 방송되는 데이터 패킷은 상이한 암호를 이용하고, 여기에서 선택된 사용자만이 해독 키를 공유한다. 키를 갖는 사람은 통화에 참여할 수 있고 없는 사람은 배제된다. 방송 패킷을 이용하는 것의 장점은, 별도의 패킷 요구를 송신하는 것보다, 라스트 마일 통신에서 더 좁은 대역폭을 요구한다는 것이다. 또 다른 실시예에서, 단일 패킷이 게이트웨이로 송신되고, 시그널링 서버는 일반 통화 모드에서 모든 참여자에게 분배하기 위한 그리고 프라이빗 또는 묵음 모드에서 통화자를 선택하기 위한 패킷을 복제한다.

[0763] ***하이퍼보안 파일 저장*** - 비록 보안 동적 통신 네트워크 및 프로토콜이 전화 통신 및 실시간 데이터 전송을 위한 하이퍼보안 통신 시스템으로서 발명되고 개발되었지만, SDNP 네트워크 및 프로토콜 고유의 보안 메커니즘은 하이퍼보안 파일 및 데이터 저장에 완벽하게 적합하다. 그 가장 단순한 설명에서, 하이퍼보안 통화가 하나의 통화자로부터 다른 통화자에게, 즉 하나의 SDNP 클라이언트로부터 다른 SDNP 클라이언트로의 엔드-투-엔드 통신에서, 스크램블링된 암호화된 데이터의 익명의 단편화된 데이터 전송을 포함하는 경우에, 하이퍼보안 파일 및 데이터 저장은, 중간에 중단되고 리콜될 때까지 무기한으로 버퍼 내에 저장되는 통신으로서 생각될 수 있다. 하이퍼보안 분배된 파일 저장을 위한 다른 명칭은 분해 데이터 저장이다.

[0764] 저장이 패킷 전달의 중간에 중단되는 통신이라는 이러한 단순화된 설명은, 처음 생각보다 기술적으로 더 정확하다. 전술한 미국 출원 제14/803,869호에서, 다른 패킷 도달까지 데이터 패킷을 일시적으로 버퍼링하는 것이 명확하게 개시되었고 동작적으로 설명되었다. SDNP 클라우드의 노드 내의 버퍼링이, 몇달이 아니라, 밀리초 규모로 발생되지만, SDNP 시스템은, 원래의 콘텐츠를 복원하기 위해서 복원되는 정보를 잃지 않고, 데이터를 대기

또는 유지할 수 있는 능력을 갖는다. 물론, 그러한 단순화된 구현예는, 디렉토리, 메뉴, 파일 재활용, 보안 자격 증명을 새롭게 하는 것, 및 다른 그러한 특징과 같은 장기간의 파일 관리에 필요한 특정 특징을 가지지 않는다.

[0765] 클라이언트로부터 단편화된 데이터 저장 네트워크로의 데이터 전송의 예가 도 81에 도시되어 있다. 도시된 바와 같이, IP 어드레스 IP $C_{1,1}$를 갖는 SDNP 클라이언트(1700A)가 일련의 데이터 패킷을 SDNP 클라우드를 통해서, 상응 IP 어드레스 IP $F_{7,1}$, IP $F_{9,1}$, 및 IP $F_{9,4}$를 갖는 SDNP 파일 저장 서버(1700H, 1700M 및 1700L)에 전송한다. 동작에서, 클라이언트 노드 $C_{1,1}$는 상응 헤더(1726X)를 갖는 일련의 데이터 패킷(1730X)을 어드레스 IP $C_{1,1}$로부터 SDNP 게이트웨이 $M_{0,0}$로 송신한다. 데이터 패킷(1730X)은 상응 헤더(1726H, 1726L 및 1726M)를 갖는 데이터 패킷(1730H, 1730L 및 1730M)에 의해서 예시된다. 정확도 보장을 위해서, 계층 4 전송은 UDP 대신 TCP를 이용한다. 패킷은 라우팅을 위해서 패킷을 식별하기 위해서 이용되는 SDNP 집 또는 다른 ID 표시된 태그 X, 데이터 패킷(1730H, 1730L 및 1730M)의 경우에, 태그 1, 태그 2, 태그 3을 포함한다. 각각의 패킷의 페이로드 부분은, 예를 들어 3개 부분 단편화 파일 SDNP 파일 1, SDNP 파일 2, 및 SDNP 파일 3 내에서 특이적 데이터를 운반한다. 라스트 마일 내의 보안 자격 증명은 상응 프리앰블 1을 갖는 구역(U1) 정보를 이용한다.

[0766] 데이터 패킷이 SDNP 클라우드에 진입하면, 데이터 패킷들은 그 신원 및 시그널링 서버(미도시)의 지시에 따라 상이한 목적지들로 라우팅된다. 헤더(1626H) 및 SDNP 파일 1을 운반하는 태그 1을 갖는 데이터 패킷(1730H)이 SDNP 게이트웨이 노드 $M_{0,4}$로 라우팅된다. 이어서, SDNP 게이트웨이 노드 $M_{0,4}$는 구역(U7)을 위한 보안 자격 증명을 이용하여 패킷(1730H)을 파일 저장 노드 $F_{7,1}$로 라우팅시킨다. 한편, SDNP 파일 2을 운반하는 태그 2로서 그 ID를 갖는 패킷(1730L)이 SDNP 게이트웨이 노드 $M_{0,8}$로 독립적으로 라우팅된다. 이어서, SDNP 게이트웨이 노드 $M_{0,8}$는 구역(U9)을 위한 보안 자격 증명을 이용하여 패킷(1730L)을 파일 저장 노드 $F_{9,4}$로 라우팅시킨다.

[0767] 거의 동시에, SDNP 파일 3을 운반하는 태그 3으로서 그 ID를 갖는 패킷(1730M)이 또한 독립적으로 SDNP 게이트웨이 노드 $M_{0,8}$으로 라우팅되고, 태그 2의ID를 갖는 데이터 패킷(1730L)과 동일한 메시형 라우팅 통로를 반드시 이용할 필요는 없다. 이어서, SDNP 게이트웨이 노드 $M_{0,8}$는 또한 구역(U9)을 위한 보안 자격 증명을 이용하여 태그 3을 갖는 패킷(1730M)을 파일 저장 노드 $F_{9,1}$로 라우팅시킨다.

[0768] 이러한 방식으로, SDNP 파일 1은 구역(U7)을 위한 보안 자격 증명을 이용하여 파일 저장 노드 $F_{7,1}$에 전달되는 한편, SDNP 파일 2 및 SDNP 파일 3은 구역(U9)을 위한 보안 자격 증명 모두를 이용하여 파일 저장 노드 $F_{9,4}$ $F_{9,1}$에 각각 전달된다. 비록 파일이 클라이언트 노드 $C_{1,1}$에 의해서 소유되지만, 클라이언트는 파일의 콘텐츠를 인코딩하고 보호하기 위해서 이용된 보안 자격 증명에 대한 액세스를 가지지 않는다. 하나의 파일 저장 노드가 모든 데이터를 포함하지 않기 때문에, 그리고 데이터를 소유하는 클라이언트가 데이터 저장을 위해서 사용되는 보안 자격 증명에 대한 액세스를 가지지 않기 때문에, 해커는 파일의 콘텐츠를 훔치기 어려운데, 이는 (i) 이들이 합치되지 않고 사용될 수 없는 조각으로 단편화되고, (ii) 모든 파일이 데이터의 스크램블링 및 암호화를 위해서 상이한 보안 자격 증명을 이용하고, (iii) 이들이 상이한 위치들에 그리고 상이한 라스트 마일 네트워크 상에 저장되고, (iv) 다양한 저장된 데이터가 동일 SDNP 소스 파일로부터 나온다는 것을 알 수 없기 때문이다. 파일 저장 서버를 포함하는 구역이 또한, 파일 소유자가 위치되는 구역 즉, SDNP 클라우드의 대향 측면들 상의 구역으로부터 구별하기 위해서 "저장측" 구역으로 지칭된다. 이러한 정의에 의해서, 구역(U1)은, 또한 "파일 소유자" 구역으로 지칭되는, SDNP 클라이언트 구역인 반면, 구역(U7 및 U9)는 "저장측" 구역이다.

[0769] SDNP 네트워크 통신 프로토콜을 파일 저장에 적용하는 것이, SDNP 클라이언트 및 파일 소유자가 그 데이터를 하이퍼보안 파일 저장 서버에 저장하는, 즉 기록하는 일반적인 단계인, "기록 동작"을 도시하는 도 82a의 흐름도로 더 도시되어 있다. 도시된 바와 같이, SDNP 클라이언트(1700A)는, 도시된 예에서 파싱된 파일(1706A, 1706B, 및 1706C)을 포함하는 3-부분 파일인, 다수-부분 파일 또는 문서를 생성하기 위해서, SDNP 분할 동작(1057) 및 파싱 기능(1052)을 이용하여, 파싱되지 않은 파일(1705)을 분할한다. 선택적으로, 파일의 콘텐츠가 분할 전에 스크램블링될 수 있다. 이어서, 이러한 3개 파일은 관련 없는 데이터 또는 코뮤니케로서 SDNP 네트워크를 가로질러 전송된다. SDNP 네트워크에 걸친 최종 목적지로의 라우팅에 포함되는 단계는, 하이퍼보안 라스트 마일 통신에 대해서 본원에서 개시된 그리고 SDNP 클라우드에서의 메시형 라우팅에 대해서 전술한 동일 방법을 이용한다. 구체적으로, 라스트 마일 하이퍼보안 전송(1707)은 구역(U1)에 따른 보안 자격 증명을 이용한다. SDNP 클라우드 내의 하이퍼보안 메시형 전송(1708)은 구역(Z1) 보안 자격 증명을 이용한다. 비록 이러한 하이퍼보안 데이

터 전송 동작이 큰 블록으로 표시되어 있지만, 패킷 전송은 실제로, 마스터 키가 없고, 중앙 제어가 없고, 패킷 콘텐츠에 대한 액세스가 없는 분산형 시스템을 이용하여, 이러한 개시 내용에서 설명된 라우터, 서버, 및 소프트-스위치의 네트워크에 걸쳐서 발생된다.

[0770] 구역(U1) 라스트 마일 라우팅이 제한된 수의 라우팅 선택을 포함하는 기반 시설에 걸쳐 데이터 패킷을 송신하는 것을 포함할 수 있지만, 다중-PHY 라스트 링크 라우팅, 다수 SDNP 게이트웨이로의 순차적인 패킷의 라우팅, 및 동적 소스 어드레싱의 이용 즉, 클라이언트의 IP 어드레스의 명칭의 변경을 포함하는, 하이퍼보안 라스트 마일 통신에 대해서 설명된 방법이 하이퍼보안 파일 저장 동작에 동일하게 적용될 수 있다. 데이터 패킷이 SDNP 클라우드에 도달하면, 그 전송은 동적으로 스크램블링된 암호화된 데이터를 갖는 익명 메시형 라우팅을 이용하여, 파일 콘텐츠 또는 심지어 통신과 연관된 메타데이터의 모니터링을 방지한다. 최종적으로, 모든 3개의 데이터 패킷이, 상이한 보안 구역들 내에 위치되는 상응 SDNP 노드 명칭 $F_{7,1}$, $F_{9,1}$, 및 $F_{9,4}$를 갖는 상이한 SDNP 파일 저장 서버(1700H, 1700M, 및 1700L)에 도달한다. 네트워크 운송 후에, 파싱된 파일 1이 구역(U7) 파일 보안 동작(1709A)에 따라 프로세스되고 SDNP 파일 저장 노드 $F_{7,1}$에 저장된다. 파싱된 파일 2 및 3이 구역(U9) 파일 보안 동작(1709B 및 1709C)에 따라 프로세스되고 SDNP 파일 저장 노드 $F_{9,1}$ 및 $F_{9,4}$에 저장된다. 이러한 방식으로, 하나의 파일이 모든 데이터를 포함하지 않고, 단일 보안 자격 증명이 원래의 것을 재생성하기 위해서 모든 성분 파일을 언록킹하지 않는다.

[0771] 도 82b에 도시된 하이퍼보안 저장된 파일의 "판독 동작"에서, 파일 저장 서버와 SDNP 클라이언트, 즉 파일 소유자 사이의 데이터 전달의 시퀀스가 반전된다. 하이퍼보안 파일의 판독은, 파일을 원래 저장하였던 프로세스를 반대 순서로 원상태로 돌리는 것을 포함하고, 그러한 프로세스는 (i) 각각의 저장 서버 내의 파싱된 파일을 식별하는 것, (ii) 각각의 파싱된 파일로부터 로컬 저장 보안 규정을 제거하는 것, (iii) SDNP 클라우드 및 하이퍼보안 라스트 마일을 가로질러, 각각의 복원된 파싱된 파일을 SDNP 클라이언트로 다시 전송하는 것, (iv) 파싱된 파일을 다양한 관련 코뮤니케로부터 수집하는 것, 및 (v) 원래의 파일을 복원하기 위해서 클라이언트의 로컬 보안 자격 증명을 이용하여, 파싱된 파일을 병합(분할-해제)하는 것 및, 적용 가능한 경우에, 스크램블링하는 것을 포함한다.

[0772] 설명된 하이퍼보안 파일 "판독 동작"을 더 설명하면, 파싱된 파일 1을 복원하기 위해서, 파일 저장 노드 $F_{7,1}$ 내에 저장된 파일 저장 서버(1700H)의 관련 콘텐츠가 구역(U7) 파일 보안 동작(1709A)을 이용하여 프로세스된다. 파싱된 파일 2 또는 3과 독립적으로, 파싱된 파일 1은, 구역(Z1) 보안 자격 증명을 이용하는 하이퍼보안 전송 동작(1708)에 의해서, 그리고 이어서 구역(U1) 라스트 마일 하이퍼보안 전송 동작(1707)에 의해서, 단순화된 형태로 도시된 예시적인 클라우드를 이용하여 SDNP 클라이언트 노드 $C_{1,1}$로 다시 통신된다. 동시에, 파싱된 파일 2을 복원하기 위해서, 파일 저장 노드 $F_{9,1}$ 내에 저장된 파일 저장 서버(1700M)의 관련 콘텐츠가 구역(U9) 파일 보안 동작(1709B)을 이용하여 프로세스된다. 파싱된 파일 1 또는 3과 독립적으로, 파싱된 파일 2는, 구역(Z1) 보안 자격 증명을 이용하는 하이퍼보안 전송 동작(1708)에 의해서, 그리고 이어서 구역(U1) 라스트 마일 하이퍼보안 전송 동작(1707)에 의해서, 단순화된 형태로 도시된 SDNP 클라우드를 이용하여 SDNP 클라이언트 노드 $C_{1,1}$로 다시 통신된다. 한편, 파싱된 파일 3을 복원하기 위해서, 파일 저장 노드 $F_{9,4}$ 내에 저장된 파일 저장 서버(1700L)의 관련 콘텐츠가 구역(U9) 파일 보안 동작(1709C)을 이용하여 프로세스된다. 파싱된 파일 1 또는 2과 독립적으로, 파싱된 파일 3은, 구역(Z1) 보안 자격 증명을 이용하는 하이퍼보안 전송 동작(1708)에 의해서, 그리고 이어서 구역(U1) 라스트 마일 하이퍼보안 전송 동작(1707)에 의해서, 단순화된 형태로 도시된 SDNP 클라우드를 이용하여 SDNP 클라이언트 노드 $C_{1,1}$로 다시 통신된다.

[0773] 판독 동작 중에 3개의 구성요소 파싱된 파일의 독립적인 패킷 라우팅이 도 83에 예시되어 있고, 여기에서 서버 노드(1700H)는 SDNP 파일 1을 운반하고 ID "태그 7"을 가지는 데이터 패킷(1731H)을, TCP 전송을 이용하여, 파일 저장 어드레스 IP $F_{7,1}$로부터, 어드레스 IP $M_{0,4}$에서 SDNP 게이트웨이 서버로 송신한다. 패킷(1731H)은 프리앰블 7 및 삼중-채널 통신에서 시그널링 서버에 의해서 전달된 명령 및 제어 패킷에서 이전에 제공되었던 다른 정보를 포함하는 헤더(1727H)를 포함한다.

[0774] 한편, 서버 노드(1700L)는, TCP 전송을 이용하여, SDNP 파일 2를 운반하고 ID "태그 9"를 가지는 데이터 패킷(1731L)을 파일 저장 어드레스 IP $F_{9,4}$로부터 어드레스 IP $M_{0,8}$에서 SDNP 게이트웨이 서버까지 송신한다. 패킷(1731L)은 프리앰블 9 및 삼중-채널 통신에서 시그널링 서버에 의해서 전달된 명령 및 제어 패킷에서 이전에 제공되었던 다른 정보를 포함하는 헤더(1727L)를 포함한다. 독립적으로 그리고 동시에, 서버 노드(1700M)는, TCP

전송을 이용하여, SDNP 파일 3를 운반하고 ID "태그 8"를 가지는 데이터 패킷(1731M)을 파일 저장 어드레스 IP $F_{9,1}$로부터 어드레스 IP $M_{0,8}$에서 SDNP 게이트웨이 서버까지 또한 송신한다.

[0775] 패킷(1731M)은 프리앰블 9 및 삼중-채널 통신에서 시그널링 서버에 의해서 전달된 명령 및 제어 패킷을 이용하여 이전에 제공되었던 다른 정보를 포함하는 헤더(1727M)를 포함한다. 3개의 데이터 패킷(1731H, 1731L, 및 1731M)은, 그들이 최종적으로 SDNP 클라우드 서버(1701U)에 의해서 호스팅되는 SDNP 게이트웨이 $M_{0,0}$로부터 나올 때까지 구역(Z1) 보안 자격 증명을 이용하여 SDNP 클라우드를 횡단하고, SDNP 클라우드 서버(1701U)에서 데이터 패킷은 상응하는 구역 헤더(1727X) 및 구역(U1) 보안 자격 증명을 이용하여 연속적인 데이터 패킷(1731X)에 의해서 어드레스 IP $C_{1,1}$에서 클라이언트 디바이스(1700A)로 순차적으로 송신된다.

[0776] 다시 도 82b를 참조하면, 3개의 파싱된 파일 1, 2, 및 3 즉, (1706A, 1706B 및 1706C)이 독립적인 라우팅을 이용하여 SDNP 클라이언트 디바이스(1700A)에 전달된 후에, 이들은 혼합 동작(1061)을 이용하여 하나의 미파싱 파일(1795)로 병합되고, 적용 가능한 경우에, 구역(U1) 보안 자격 증명에 따라 언스크램블링 동작(미도시)이 후속하여 실시된다.

[0777] 저장된 데이터 보안을 위해서 추가적인 파일 서버 동작을 부가하지 않고, 보안 동작(1709A, 1709B 및 1709C)은 SDNP 클라우드와 상응 저장-서버(1700H, 1700M, 및 1700L) 사이의 라스트 마일 하이퍼보안 통신을 실제로 포함한다. SDNP 통신 프로토콜을 이용한 계층 3 네트워크 연결성의 부산물로서, SDNP 파일 저장이 본질적으로 하이퍼보안이고, 정크 데이터 삽입 및 정크 파일과 같은 데이터 기만 방법의 이용을 포함하여, 분산형의 비휘발성 데이터 드라이버에 걸쳐 저장된 스크램블링, 단편화, 암호화된 데이터를 포함한다. 전술한 데이터 보안 방법 이외에, 본원에서 개시된 바와 같은 하이퍼보안 저장은 어떠한 의미 있는 메타데이터도 없고, 파일 소유자까지의 추적 가능성도 없고, 파일을 전달하는 라우팅도 없고, 또는 원래의 소스 파일로부터의 손실 성분을 유지하는 임의의 다른 파일 저장 서버의 신원도 없는, 익명 파일 명칭을 이용한다.

[0778] 저장 서버의 물리적 실현 즉, 그 계층 1 PHY 구현 및 계층2 전송인, SDNP 네트워크 상에서의 상호운용에도 불구하고, 프로토콜은, 저장 기능성, 액세스 시간, 또는 글로벌 액세스 가능성에 영향을 미치지 않고 매우 상당히 변경될 수 있다. 도 84a는, 예로서, 라우터(27)를 통해서 SDNP 파일 저장 서버(1740A)에 연결된 SDNP 게이트웨이(1701B)를 보여주는 최상단 도면을 포함하는 SDNP 파일 저장 서버의 물리적 실현을 도시한다. 더 뛰어난 네트워크 성능 및 공격에 대한 추가적인 복원력을 위해서, 중간 도면은 개입 라우터가 없는 광섬유(91)를 이용하여 SDNP 게이트웨이(1701B) 및 SDNP 파일 저장 서버(1740A) 사이의 직접적인 연결을 보여준다. 하한의 예에서 도시된 바와 같이, 파일 저장 서버는 서버 제어기(1740B) 및 저장 드라이브(1740C 및 1740D)를 갖는 대형 메모리 어레이를 포함할 수 있다. 드라이브는 하드 디스크 드라이브 또는 플래시 드라이브 기반의 비휘발성 메모리를 포함하는 임의의 미디어를 포함할 수 있다. 액세스를 더 제한하기 위해서, SDNP 게이트웨이 및 SDNP 파일 저장 서버는 그들을 연결하는 섬유 링크로만 동일한 위치 및 설비 내에 물리적으로 위치될 수 있다. 이들은 심지어 공통 공간을 공유할 수 있고, 예를 들어 아치형 천장 내에 물리적으로 록킹될 수 있고, 액세스 제어가 엄격하게 관리되고 설비에 진입하는 모든 사람을 감시 모니터링할 수 있다.

[0779] 도 84b는, 단편화된 데이터 파일의 일부 부분이 파일 소유자의 사이트에 국소적으로 저장될 수 있다는 것을 더 도시한다. 도시된 바와 같이, 파일 소우자의 데스크탑(36)은, (i) 서버(1701A) 상의 SDNP 게이트웨이 노드 $M_{0,0}$에 연결된 WiFi 라우터(1352)에 걸쳐 액세스되는 로컬 파일 저장 서버(1740A), (ii) SDNP 게이트웨이 노드 $M_{0,4}$에 연결된 파일 저장 서버(1740B), 및 (iii) SDNP 게이트웨이 노드 $M_{0,8}$ 에 연결된 파일 저장 서버(1740C)를 포함하는 몇 개의 디바이스에 걸쳐 분산 파일을 저장할 수 있다. 분산된 드라이브(1740A, 1740B, 및 1740C)에 걸쳐 저장될 때 데이터가 단편화되기 때문에, 비록 로컬 파일 서버(1740A) 및 파일 소유자 데스크탑(36)이 동일 WiFi(1352)를 공유하더라도, 노트북(35), 태블릿(33), 및 휴대폰(29)을 포함하는 다른 디바이스는 저장된 파일에 대한 액세스를 가지지 못한다.

[0780] 비-중복 하이퍼보안 파일 맵핑으로 지칭되는, 파일의 각각의 파싱된 부분을 분리된 파일 저장 서버에 특이적으로 저장하는 프로세스가 도 85a에 도시되어 있다. 도시된 바와 같이, SDNP 클라이언트 노드 $C_{1,1}$를 포함하는 클라이언트 디바이스(1700A)는, 저장 노드 $F_{7,1}$, $F_{9,1}$, 및 $F_{9,4}$를 각각 갖는 파싱된 파일 1, 2, 및 3 사이의 일-대-일 파일 맵핑에 상응하여, 파일 저장 서버(1700H)에만 파싱된 파일(1706A)을, 파일 저장 서버(1700M)에만 파싱된 파일(1706B)을, 그리고 파일 저장 서버(1700L)에만 파싱된 파일(1706C)을 저장한다. 파일의 전달은 하이퍼보안 라스트 마일 통신을 이용하여, 데이터의 전달뿐만 아니라 그 저장을 보안한다. 비-중복 파일 맵핑의 하나의

단점은, 파일 저장 서버 중 어느 하나의 손실이, 일시적으로 또는 영구적으로, 파일 액세스 및 복원을 위험하게 한다는 것이다. 본원의 맥락에서, "복원성" 및 "복원적"이라는 용어는 저장된 데이터에 대한 보장된 그리고 적시의 액세스를 정의하기 위해서, 즉 상당한 지속시간 동안 저장된 데이터가 손실되지 않거나 그 액세스가 손상되지 않는다는 것에 대한 확신을 정의하기 위해서 사용된다. 이러한 토큰에 의해서, 도시된 비-중복 하이퍼보안 파일 맵핑은 좋지 못한 복원력을 나타내는데, 이는 단일 지점의 실패가 파일 액세스를 방해하기 때문이다. 좋지 못한 복원성은 중복적 시스템에 의해서 극복될 수 있고, 여기에서 동일 데이터가 하나 초과의 파일 저장 서버 내에 저장된다.

[0781] 데이터 저장 시스템의 복원성을 설명하거나 평가하는 다른 측정기준은, 일차 데이터 저장이 이용될 수 없는 경우에 데이터 액세스를 제공하는 백업 시스템의 수를 정의하는 용어인, 판독 중복성 인자(RRF)로서 본원에서 정의된 측정기준이다. 도시된 예에서, 각각의 특이적 데이터 조각의 하나의 위치가 있다. 이는 0의 판독 중복성 인자, 또는 수학적으로 RRF = 0을 초래하고, 이는, 파일이 파일 소유자에 의해서 판독될 수 없기 때문에, 단일 포인트 연결 또는 파일 서버 실패가 일시적 또는 영구적 데이터 손실을 초래할 수 있다는 것을 의미한다.

[0782] RRF = 1의 판독 중복성 인자를 갖는 대안적인 파일 맵핑이 도 85b에 도시되어 있다. 이러한 예에서, 파싱된 파일 1이 파일 저장 서버 노드 $F_{9,4}$ 및 $F_{7,1}$에 저장되고, 파싱된 파일 2는 파일 저장 서버 노드 $F_{9,1}$ 및 $F_{7,1}$에 저장되고, 파싱된 파일 3은 파일 저장 서버 노드 $F_{9,4}$ 및 $F_{9,1}$에 저장된다. 그러한 구현예에서, 파일 저장 서버 노드 $F_{9,1}$가 손상되거나 이용될 수 없는 경우에, 파싱된 파일 3은 파일 저장 서버 노드 $F_{9,4}$로부터 여전히 액세스될 수 있고, 파싱된 파일 2는 파일 저장 서버 노드 $F_{7,1}$로부터 여전히 액세스될 수 있다. 따라서, 임의의 하나의 저장 노드의 실패는 하이퍼보안 파일에 대한 판독 액세스를 방해하지 않을 것이다. 도 85c는 RRF = 2인 하이퍼보안 파일 맵핑을 도시한다. 파일 맵핑은 파일 저장 서버(1700L, 1700M, 및 1700H)를 유지하나, 파일 저장 서버 노드 $F_{8,2}$, $F_{4,4}$, 및 $F_{6,8}$를 각각 실현하기 위해서 제2 세트의 파일 저장 서버(1700J, 1700E, 및 1700F)를 부가한다. 따라서, 파일 저장 서버(1700J)는 파일 저장 서버(1700L)를 위한 백업으로서 작용하고, 파일 저장 서버(1700E)는 파일 저장 서버(1700M)를 위한 백업으로서 작용하고, 파일 저장 서버(1700F)는 파일 저장 서버(1700H)를 위한 백업으로서 작용한다. 비록 도시된 예가 3개의 섹션으로 파싱된 파일을 포함하지만, 희망하는 경우에 문서가 더 많은 수의 섹션으로 파싱될 수 있다는 것이 이해될 것이다. 하이퍼보안 저장을 보장하기 위해서, 원래의 파일이 2 미만의 섹션으로 그리고 이상적으로는 3 미만의 섹션으로 파싱되지 않아야 한다.

[0783] 하이퍼보안 파일 저장을 이용하여 중복 파일을 저장 및 판독하게 하는 프로세스를 설명하기 위해서, 저장 프로세스를 촉진하기 위해서 이용되는 SDNP 네트워크 위에 놓인 코뮤니케 및 파일 전달 기능의 거래적 시퀀스를 설명하는 것이 유리하다. 도 86에 도시된 네트워크는, 예를 들어, 클라이언트 노드 $C_{1,1}$를 구현하는 클라이언트 디바이스(1700A), 라우터(1702G), SDNP 노드 S를 구현하는 시그널링 서버(1715), SDNP 노드 NS를 구현하는 명칭 서버(1714), SDNP 클라우드 노드 $M_{0,0}$, $M_{0,4}$ 및 $M_{0,8}$을 구현하는 클라우드 서버(1701U), 그리고 SDNP 파일 저장 노드 $F_{7,1}$, $F_{9,4}$, 및 $F_{9,1}$를 각각 실현하는 SDNP 파일 저장 서버(1700H, 1700L, 및 1700M)를 포함한다.

[0784] 도 87a에서, 어드레스 "IP $C_{1,1}$"에서 클라이언트 디바이스(1700A)는, C&C 페이로드(1711A)를 포함하고, 다시 파일 크기에 관한 설명 및 요청된 보안 및 중복의 레벨을 포함하는 데이터 패킷(1710A)에 의해서, 어드레스 "IP S"에서 시그널링 서버(1715)에 대한 파일 기록 요청을 한다. 도 87b에서, 시그널링 서버(1715)는 데이터 패킷(1710B)을 명칭 서버(1714)에 송신하여 파일 저장 서버 노드 $F_{7,1}$, $F_{9,4}$, 및 $F_{9,1}$의 IP 또는 SDNP 어드레스를 요청한다. 이용하기 위한 파일 어드레스 서버 노드의 선택은 저장 노드의 목록으로부터 무작위로 선택될 수 있거나, 지형적으로 클라이언트 근처에서 이용 가능한 하나의 노드를 기초로 또는 재난이 없는 영역 내의 노드를 기초로 선택된다. 선택은 또한 노드의 미사용 메모리 용량, 파일 저장 노드까지의 전파 시간, 노드의 업타임 신뢰성 등급, 또는 다른 그러한 고려사항과 같은 성능 매개변수를 기초로 할 수 있다. 도 87c에서, 명칭 서버(1714)는, 파일 저장 서버 노드 $F_{7,1}$, $F_{9,4}$, 및 $F_{9,1}$의 IP 또는 SDNP 어드레스를 포함하는 데이터 패킷(1710C)을 시그널링 서버(1715)에 송신한다. 이어서, 시그널링 서버(1715)는 파일 저장 서버(1700H, 1700L 및 1700M)에 대한 파싱된 파일의 라스트 마일 및 메시형 클라우드 전달을 계산한다.

[0785] 도 87d에서, 시그널링 서버(1715)는 데이터 패킷(1710D)을 클라이언트 디바이스(1700A)에 송신하고, 패킷은 라우터(1702G)를 통해서 어드레스 "IP S"로부터 "IP $C_{1,1}$"로 라우팅된다. 데이터 패킷(1711D)은, 클라이언트 구역인, 구역(U1) 내의 임박한 파일 전달을 위한 라스트 마일 라우팅, 구체적으로 (간결함을 위해서 "태그 X"로 표

시된) 각각의 패킷의 태그 1, 태그 2 및 태그 3 식별을 갖는 어드레스 "IP $C_{1,1}$"로부터 "IP $M_{0,0}$"에서의 SDNP 게이트웨이까지의 다수의 패킷의 라우팅을 포함하는 C&C 페이로드(1711D)를 포함한다. 동시에, 시그널링 서버(1715)는 데이터 패킷(1710E)을 SDNP 게이트웨이(1701U)에 또한 송신하고, 패킷은 어드레스 "IP S"로부터 "IP $M_{0,0}$"으로 라우팅된다. 이러한 패킷은 ID 태그 X를 갖는 패킷을 위한 구역(Z1) 보안 자격 증명을 이용한, 이러한 경우에 SDNP 게이트웨이 어드레스 "SDNP $M_{0,0}$"로부터, 예를 들어 어드레스"SDNP $M_{0,5}$"(미도시)에서, 클라우드 내의 다음 노드까지의, SDNP 클라우드 라우팅을 보여주는 C&C 페이로드(1711E)를 포함한다. 보안 동적 통신 네트워크 및 프로토콜에 따라, 메시형의 익명의 단편화 전송을 이용한 SDNP 클라우드 전체를 통한 데이터 패킷의 라우팅은 실시간 네트워크의 현재의 조건을 기초로 동적으로 선택된다. 구체적으로, 임의의 SDNP 게이트웨이에 도달하는 실시간 데이터 패킷의 SDNP 클라우드 내의 라우팅은 SDNP 클라우드 내의 노드-대-노드 전파 지연에 그리고 시그널링 서버에 의해서 할당된 각각의 실시간 데이터 패킷의 긴급성에 따라 달라진다.

[0786] 도 87e에서, 시그널링 서버(1715)는 C&C 데이터 패킷을 저장측에 위치된 라스트 마일 노드에, 즉 구역(U7 및 U9)에 송신한다. 도시된 바와 같이, 데이터 패킷(1710F)은 SDNP 게이트웨이 $M_{0,4}$로 송신되고, 패킷은 어드레스 "IP S"로부터 "IP $M_{0,4}$--"로 라우팅되고, 패킷은, 태그 1을 갖는 데이터 패킷이 게이트웨이 노드 $M_{0,4}$ 에 의해서 예상되어야 한다는 것, 그리고 수신될 때, 라스트 마일 어드레스 "IP $F_{7,1}$" 상으로 포워딩되어야 한다는 것을 통신하는 C&C 페이로드(1711F)를 포함한다. 제2 데이터 패킷(1710G)이 시그널링 서버(1715)로부터 어드레스"IP $F_{7,1}$"에 위치되는 저장 서버(1700H)로 포워딩된다. 구역(U7) 내의 저장을 위한 C&C 페이로드는 소스 어드레스 "IP $M_{0,4}$"로부터의 ID 태그 1을 갖는 진입 패킷을 규정하나, 노드의 기능이 저장이고 통신이 아니기 때문에, 목적지 필드는 빈 상태로 유지되고, 즉 무효 값으로 채워진다. 명령 및 제어 데이터 패킷이 네트워크로 분배되면, 파일 전달이 발생될 수 있다.

[0787] 도 88은 파일 하이퍼보안 저장 중의 단편화된 데이터 전송을 도시하고, 여기에서 클라이언트 디바이스(1700A)는 TCP 데이터 전송을 이용하여 SDNP 데이터 파일 1, 2, 및 3을 운반하는 일련의 데이터 패킷(1712X)을 어드레스 "IP $C_{1,1}$"으로부터 어드레스 "IP $M_{0,0}$"에 위치하는 SDNP 게이트웨이로 송신한다. 각각의 데이터 패킷은 특이적 식별자 ID 즉, 태그 1, 태그 2, 및 태그 3을 갖는다. 이어서, 이러한 파일은 SDNP 클라우드를 통해서 다른 게이트웨이로, 즉 SDNP 게이트웨이 노드 $M_{0,4}$ 및 $M_{0,8}$로 전송된다. 게이트웨이 노드 $M_{0,4}$에 도달한 SDNP 데이터 1을 포함하는 패킷이 구역(U7) 보안 자격 증명을 갖는 TCP를 이용하여 어드레스 "IP $M_{0,4}$"로부터 "IP $F_{7,1}$"까지 데이터 패킷(1712A) 내에서 전송되는 한편, 게이트웨이 노드 $M_{0,8}$에 도달한 데이터 2 및 데이터 3 패킷은 데이터 패킷(1712B 및 1712C) 내의 구역(U9) 보안 자격 증명과 함께 어드레스 "IP $M_{0,8}$"로부터 어드레스 "IP $F_{9,4}$" 및 "IP $F_{9,1}$"로 각각 전송된다. 드라이브의 데이터 스캐닝을 방지하기 위해서, 저장은 또한 파일 서버 내의 로컬 암호화를 포함한다. 이러한 암호화 프로세스는 로컬적이고, SDNP 보안 규정과 관련되지 않는다. 데이터 패킷의 콘텐츠 SDNP 데이터 1, SDNP 데이터 2, 및 SDNP 3은 저장되는 실제 단편화된 파일을 포함한다.

[0788] 각각의 데이터 패킷 내의 프리앰블, 예를 들어 데이터 패킷(1712A) 내의 프리앰블 1은 또한 대칭적 키 암호화 동작의 일부로서 클라이언트에 의해서 공급된 암호화 키를 포함할 수 있다. 대칭적 키 암호화를 이용하여, SDNP 클라이언트 노드 $C_{1,1}$는, 암호화를 위한 것이고 해독을 위한 그 보완체인, 분할 키를 생성한다. 이어서, 대칭적 암호화 키가, 이러한 예에서 데이터 패킷(1712A)에 의해서 전달된 파일 저장 서버 노드 $F_{7,1}$에 공급된다. 장래에, 클라이언트가 저장된 파일의 콘텐츠의 판독 또는 액세스를 요청할 때마다, 파일 저장 서버 노드 $F_{7,1}$는, 파일을 클라이언트로 다시 송신하기 전에, 이러한 암호화 키를 이용하여 요청된 파일을 암호화한다. 클라이언트만이 연관된 해독 키를 가지기 때문에, 클라이언트만이 판독 파일을 열 수 있다. 이러한 방법이 여분의 계층의 보호를 제공하지만, 단일 클라이언트만이 판독 동작으로서 파일에 액세스할 수 있고, 원래의 클라이언트 디바이스가 도난당하거나, 손상되거나, 분실된 경우에 중복적 액세스를 돕기 위해서 필요한 다수의 클라이언트 파일 "소유자"의 이용을 방지한다는 단점을 갖는다.

[0789] 대략적으로 데이터 전달 및 파일 저장 프로세스의 시간에, 시그널링 서버(1715)는 또한 "링크 응답" 메시지 라우팅과 관련하여 지시를 파일 저장 서버(1700H, 1700L 및 1700M)에 송신한다. 링크 응답은, 기록 동작이 성공적이었고 각각의 파싱된 파일의 저장이 완료되었다는 것을 클라이언트에게 확인시키는, 데이터 패킷 및 C&C 페이로드이다. 이러한 메시지는, 전달된 파싱된 파일의 저장과 관련된 각각의 파일 저장 서버와 독립적으로, 클라이언트 파일-소유자에게 송신된다. 파일 서버는, 서로 모르는 것과 독립적으로, 그 기록-확인 응답을 클라이언트

에 송신하고, 기록-통신 응답은, 기록 동작의 시점에서의 동작 상태와 다른 특이적 상태를 포함하는 독립적인 보안 자격 증명을 이용하여 전송된다. 이러한 링크 응답 메시지의 라우팅은, 파일을 전달하기 위해서 이용되었던 것과 동일한 라우팅 통로의 역방향을 반드시 이용할 필요는 없다. 그러한 응답은 파일의 소유자를 찾기 위한 역추적으로서 사이버-공격자에 의해서 이용될 가능성이 있다.

[0790] 그 대신, 링크 응답은, 저장된 파일이 동일 파일의 일부이고 동일한 단편화된 기록-동작의 일부로서 저장되었다는 것을 클라이언트에게 식별시키기 위해서 패킷 ID를 이용한다.

[0791] 동작 시에, 시그널링 서버는 링크 응답 메시지를 위한 라우팅을 파일 저장 서버에, 클라이언트 파일-소유자에게, 그리고 링크-응답 메시지 라우팅에 관련된 모든 중간 SDNP 노드에 송신한다. 시그널링 서버(1715)는 명령 및 제어 페이로드를 포함하는 데이터 패킷을 이용하여, 도 89a의 예에 의해서 도시된 바와 같이, 링크 응답 메시지 라우팅을 조정하고, 예를 들어 파일 저장 서버(1700H)는 어드레스 IP $F_{7,1}$로부터 어드레스 IP $M_{0,4}$로의"링크 1 응답" 라우팅을 위한 헤더 데이터를 포함하는 C&C 페이로드(1722G)를 포함하는 데이터 패킷(1721G)을 수신한다. SDNP 게이트웨이 노드 $M_{0,4}$는, 어드레스 "SDNP $M_{0,4}$"로부터, 이러한 경우에 어드레스 "SDNP $M_{0,14}$"에 있는, SDNP 클라우드(미도시) 내의 다른 노드로의 태그 1 데이터 패킷의 라우팅을 설명하는 C&C 페이로드(1722F)를 포함하는 데이터 패킷(1712F)을 수신한다. 유사하게, 시그널링 서버(1715)는 어드레스 "IP $F_{9,1}$"로부터 "IP $M_{0,8}$"까지의 "링크 3 응답" 태그 3 패킷 라스트 마일 라우팅 지시를 포함하는 데이터 패킷(1721M)을 파일 저장 서버(1700M)에 송신한다. 파일 데이터 패킷 및 그 상응 링크 응답 메시지를 위한 저장측 라스트 마일 라우팅이 동일하거나 유사할 수 있는 반면, SDNP 클라우드를 통한 응답 메시지의 라우팅은, SDNP 클라우드의 동적 특성으로 인해서, 상이할 가능성이 가장 크다.

[0792] 참여하는 파일 저장 서버 노드들로부터의 링크 응답 메시지의 실제 라우팅이 도 89b에 도시되어 있다. 도시된 바와 같이, 파일 저장 서버(1700H)는, 태그 1에 의해서 식별되고 페이로드 "FS 링크 1"을 운반하는 데이터 패킷(1720A)으로 응답한다. 패킷은, 구역(U7) 보안 자격 증명을 이용하여, 어드레스 "IP $F_{7,1}$"로부터 "IP $M_{0,4}$"에 위치되는 SDNP 게이트웨이까지 라우팅된다. SDNP 게이트웨이로부터, 태그 1 데이터 패킷은 SDNP 클라우드를 통해서 어드레스 "SDNP $M_{0,0}$"에 위치되는 클라이언트측 게이트웨이까지 라우팅되고, 여기에서 어드레스는 라스트 마일 데이터 패킷(1720X)으로 변환되고, 구역(U1) 보안 자격 증명을 이용하고 태그 1 데이터, 즉 프리앰블 1 및 FS 링크 1을 운반하는 TCP 전송을 이용하여, 어드레스 "IP $M_{0,0}$"으로부터 어드레스 "IP $C_{1,1}$"까지 라우팅된다.

[0793] 유사한 방식으로, 파일 저장 서버(1700L)는, 태그 2에 의해서 식별되고 페이로드 "FS 링크 2"을 운반하는 데이터 패킷(1720B)으로 응답한다. 패킷은, 구역(U9) 보안 자격 증명을 이용하여, 어드레스 "IP $F_{9,4}$"로부터 "IP $M_{0,8}$"에 위치되는 SDNP 게이트웨이까지 라우팅된다. SDNP 게이트웨이로부터, 태그 2 식별된 데이터 패킷은 SDNP 클라우드(라우팅 미도시)를 통해서 어드레스 "SDNP $M_{0,0}$"에 위치되는 클라이언트측 게이트웨이까지 라우팅되고, 여기에서 어드레스는 라스트 마일 데이터 패킷(1720X)으로 변환되고, 구역(U1) 보안 자격 증명을 이용하고 태그 2 데이터, 즉 프리앰블 2 및 FS 링크 2를 운반하는 TCP 전송을 이용하여, 어드레스 "IP $M_{0,0}$"으로부터 어드레스 "IP $C_{1,1}$"까지 라우팅된다.

[0794] 태그 3에 의해서 식별되고 페이로드 "FS 링크 3"을 운반하는 파싱된 파일의 제3 조각이 데이터 패킷(1720C)을 통해서 파일 저장 서버(1700M)로부터 송신된다. 이러한 태그 3 패킷은, 구역(U9) 보안 자격 증명을 이용하여, 어드레스 "IP $F_{9,1}$"로부터 "IP $M_{0,8}$"에 위치되는 SDNP 게이트웨이까지 라우팅된다. SDNP 게이트웨이로부터, 태그 3 식별된 데이터 패킷은 SDNP 클라우드를 통해서 어드레스 "SDNP $M_{0,0}$"에 위치되는 클라이언트측 게이트웨이까지 라우팅되고, 여기에서 어드레스는 라스트 마일 데이터 패킷(1720X)으로 변환되고, 구역(U1) 보안 자격 증명을 이용하고 태그 3 데이터, 즉 프리앰블 3 및 FS 링크 3을 운반하는 TCP 전송을 이용하여, 어드레스 "IP $M_{0,0}$"으로부터 어드레스 "IP $C_{1,1}$"까지 라우팅된다.

[0795] 도 89c는 파일 저장 서버(1700H)로부터 클라이언트 및 파일 소유자에게 다시 라우팅된 FS 링크 데이터 패킷(1720A)의 콘텐츠의 예를 도시한다. 도시된 바와 같이, 데이터 패킷은, 보안 구역(U7)에서 생성된 ID 태그 1을 갖는 패킷 내의 TCP를 이용하는 어드레스 "IP $F_{7,1}$"로부터 어드레스 "IP $M_{0,4}$"에 위치되는 SDNP 게이트웨이까지의 라스트 마일 라우팅을 포함한다. 응답 프리앰블(1719A)은 데이터 페이로드(1741A)에 관한 설명을 포함하고, 또

한 클라이언트에 전달되는 FS 링크 데이터 패킷(1720A)의 보안을 실행 또는 향상시키기 위해서 사용되는 선택적인 보안 자격 증명을 포함한다. 그러나, 삼중-채널 통신에서, 응답 프리앰블(1719A) 내에 포함된 응답 보안 자격 증명은 일반적으로 요구되지 않고, 추후에 하이퍼보안 저장 파일에 액세스하고 열기 위해서 클라이언트에 의해서 이용되는 것과 관련되지 않는다. 그 대신, 클라이언트로부터 파일 저장 노드 $F_{7,1}$에 저장된 파일로의 링크를 생성하는데 필요한 액세스 자격 증명은 이하를 포함하는 데이터 필드(1741A) 내에 포함된다:

[0796] * 단편화된 파일의 일부가 저장된 파일 저장 서버를 식별하는데 필요한 특이적 네트워크 태그, SDNP 어드레스, 또는 의사-어드레스.

[0797] * "저장측" 보안 구역(클라이언트의 구역이 아니다) 내의 파일을 인코딩하기 위해서 이용되는 보안 자격 증명을 규정하는 구역에 관한 설명.

[0798] * 저장에 앞서서 파일의 인코딩 중에 필요한 수치 시드 또는 시간 또는 상태(920)를 포함할 수 있는 시드 1.

[0799] * 저장 동작의 일부로서 파일 인코딩을 실행하기 위해서 이용되는 수치 시드(929)를 포함할 수 있는 시드 2.

[0800] * 구역(U7) "저장측" 암호를 해독하기 위한 해독 키(1030)을 포함하는 키 1. 이러한 키는 파일 저장 서버의 일부로서 동작하는 DMZ 서버 내에서 유지되는 공유된 비밀과 함께 사용될 수 있거나, 수치 시드와 같은 다른 보안 자격 증명과 함께만 동작될 수 있는 부분적인 해독 키를 나타낼 수 있다.

[0801] * 클라이언트에 송신된 그리고 대칭적 키 암호화를 이용하여 클라이언트로부터 파일 저장 서버로 보안 지시를 송신하기 위해서 이용되는 암호화 키(1022)를 포함하는 키 2.

[0802] * 어떻게 저장하는지를 노출시키지 않고 클라이언트가 저장 파일을 식별하는 것을 돕기 위해서 이용되는 파일 명칭 또는 다른 정보.

[0803] 전술한 데이터 패킷은 설명 목적을 위해서 사용된 것이고, 데이터 패킷의 콘텐츠를 예에서 도시된 바와 같은 정확한 요소 또는 포맷으로 제한하는 것으로서 이해되지 않아야 한다. SDNP 클라이언트 노드 $C_{1,1}$에 의해서 수신된 FS 링크(1720X)는, 단편화된 파일 저장에 참여하는 파일 저장 서버로부터 일단 수신되면, 클라이언트의 디바이스를 위한 파일 링크를 생성하도록 프로세스된다. 도 89d에 도시된 바와 같이, 이러한 동작은 혼합 동작(1753)을 이용하여 FS 링크(1741A, 1741B, 및 1741C)를 조합하고, 그에 따라 FS 링크 총 "파일 저장 판독 링크"(1754)를 생성한다. 파일 저장 링크(1754)는, 하이퍼보안 파일의 용이한 단일-누름버튼 리콜을 위해서 클라이언트의 하이퍼보안 텍스트 메신저 또는 파일 관리 시스템 상에 놓인다. 하이퍼보안 동작은 사용자가 볼 수 없다. 파일 소유자는, 파일이 실제로 단편화되고, 인코딩되고, 및 분산형 파일 저장 시스템에 걸쳐 저장되었다는 사실을 염려할 필요가 없다. 파일 리콜은 파일이 국소적으로 체류하는 것으로 보인다. 그에 따라, FS 링크는 분산형 파일 저장 시스템에 걸쳐 저장된 임의의 파일에 액세스하기 위한 키 요소이다.

[0804] FS 링크 통신의 단순화된 도면이 도 90a에 도시되어 있고, 여기에서 3개의 파일 저장 서버가 그 각각의 FS 링크를 클라이언트 노드 $C_{1,1}$ 및 상응 클라이언트 디바이스(1700A)에 송신하고, 구체적으로 파일 저장 서버(1700H)는 FS 링크 1을 송신하고, 파일 저장 서버(1700M)는 FS 링크 2를 송신하고, 파일 저장 서버(1700L)는 FS 링크 3을 송신한다. 클라이언트 디바잇스(1700A) 내에서, 클라이언트 노드 $C_{1,1}$, 내의 SDNP 앱 소프트웨어가 3개의 진입 FS 링크 1, 2, 및 3을 조합하여, 저장된 파일에 대한 링크를 형성한다. 이러한 조합된 링크는 파일 저장 확인으로서 SDNP 메신저 내에서 나타난다. 비-중복 파일 관리에서, FS 링크 정보가 클라이언트 디바이스로만 송신된다. 사용자 파일 관리를 위해서, 파일 링크는, 파일 저장이 요청되었을 때 또는 확인 메시지를 수신할 때 명명될 수 있다.

[0805] 파일 저장 링크가 직접적으로 파일 저장 서버로부터 그리고 시그널링 서버를 통하지 않고 클라이언트에 송신되기 때문에, 링크를 갖는 클라이언트만이 파일에 대한 액세스를 갖는다. 이러한 FS 링크는 단편화된 파일을 리콜 및 판독하는데 필요하다. FS 링크가 없으면, 저장된 파일 및 그 콘텐츠는 영원히 망실될 것이고, 불가역적으로 회복할 수 없게 된다. FS 링크가 손실될 수 있는 이러한 위험을 줄이기 위해서, 대안적인 접근방식은 FS 링크를 2개의 클라이언트 디바이스 - 클라이언트 디바이스 및 보조 디바이스 - 에 송신한다. 보조 디바이스는, 클라이언트에 의해서 소유된 제2 디바이스 또는, 비지니스의 경우에, 회사가 소유한 제2 디바이스일 수 있다. 대안적으로, 제2 디바이스는 그 자체의 로그인 보안 및 사용자 신원 확인을 갖는 다른 서버를 포함할 수 있다.

[0806] 본 발명에 따라 만들어진 단편화된 분산되어 저장된 파일에 대한 중복 링크 액세스가 판독 중복, 즉 RRF ≥ 1 및 비-중복 파일 저장 시스템 모두에 적용될 수 있다. 판독 중복성을 가지지 않는(RRF = 0) 하이퍼보안 분산형

메모리 시스템 내의 중복 링크의 이용이 도 90b에 도시되어 있다. 그러한 시스템에서, 파싱된 파일(1706A, 1706B, 및 1706C)과 상응하는 파일-저장 서버(1700H, 1700M, 및 1700L) 사이의 파일 맵핑이 비-중복적이다. 도시된 바와 같이, FS 링크 1, 2, 및 3은 2개의 클라이언트 디바이스, 즉 SDNP 클라이언트 노드 $C_{1,1}$를 호스팅하는 클라이언트 디바이스(1700A) 및 백업 클라이언트 노드 $C_{2,1}$를 호스팅하는 보조 클라이언트 디바이스(1700B)에 송신된다. FS 링크 중 하나가 임의의 이유로 손실되거나 이용불가능하게 되는 경우에, 백업 클라이언트 상의 FS 링크를 이용하여 파일을 복원할 수 있다. 이와 관련하여, SDNP 분산형 저장 시스템은, 단일 링크 중복의, 즉 RRF = 0 및 LRF = 1의 비-중복 판독 구현예를 설명한다.

[0807] 판독 및 링크 중복성 모두를 포함하는 하이퍼보안 메모리의 예가 도 90c에 도시되어 있고, 여기에서 파싱된 파일 1, 2 및 3이 2개의 파일 저장 서버에 각각 맵핑되고, 그에 따라 판독 중복성 인자 RRF = 1을 실현하고, 2개의 클라이언트에 송신된 각각의 FS 링크로 링크 중복성 인자 LRF = 1를 달성한다. 판독 및 링크 관련 실패 모두에 대한 저장 시스템의 면역성은, 시스템이 전체적인 저장 중복성 인자 SRF = 1을 갖는 진정한 중복 하이퍼보안 파일 관리 시스템으로서 간주될 수 있다는 것을 의미한다. 본원에서, 저장 중복성 인자(SRF)를 RRF 및 LRF 중 가장 작은 것과 동일한 중복성 인자로서 정의한다. 예를 들어, RRF = 0 및 LRF = 1인 경우에, SRF = 0이다. 그 대신 RRF = 3 및 LRF = 2인 경우에, 전체적인 저장 중복성이 SRF = 2이다. 전체 시스템 SRF = 3을 구현하기 위해서, 각각의 파싱된 파일이 (도 85c에서 앞서 도시한 바와 같이) 4개의 분리된 파일 저장 서버 내에 저장되어야 하고, FS 링크는 4개의 분리된 클라이언트에 송신되어야 한다.

[0808] 따라서, 전체 저장 중복성 인자(SRF)는 분산형 저장 시스템의 실패로부터의 복원의 직접적인 수단이다. 이러한 원리는 도 91의 그래프에서 요약되어 있고, 여기에서 가로 좌표는 파일 저장 시스템에서 사용된 파일 저장 서버의 #를 설명하고, 세로 좌표는 별도의 클라이언트들에 송신된 FS 링크의 수를 설명한다. 도시된 바와 같이, 단일 파일 저장 서버는 중복성을 가지지 않고, 즉 RRF = 0이다. 파일 저장 디바이스의 수의 증가가 판독 중복성을 개선하나, 링크 중복성에 영향을 미치지 않는다. 역으로, 링크를 단일 클라이언트에 송신하는 것은, 이용 가능한 파일 저장 서버의 수와 관계없이, 링크 중복성을 제공하지 않고, 즉 LRF = 0이다. 두 경우 모두, 즉 하나의 저장 서버 또는 하나의 클라이언트 링크에서, 전체 저장 중복성 인자(SRF) = 0이고, 이는, L 형상 영역에 의해서 도식적으로 도시된 바와 같이, 파일 저장 시스템이 복원성을 가지지 않는다는 것을 의미한다.

[0809] 도시된 바와 같이, 이전에 도시된 바와 같이, 3개의 파일 저장 서버 상에 3 부분 파싱 파일을 저장하는 것은 판독 중복성 인자(RRF) = 1을 초래한다. 적어도 2개의 클라이언트가 FS 링크를 수신하는 경우에, LRF ≥ 1의 링크 중복성이 달성된다. LRF = 1 또는 RRF = 1의 조합은 L-형상의 영역(1724B)을 생성하고, 여기에서 SRF = 1이고, 즉 어느 정도의 시스템 복원성을 제공한다. 6개의 서버가 이용되는 경우에도, FS 링크가 2개의 클라이언트에만 송신된다면, 시스템은 여전히 제한된 정도의 복원성만을, 즉 SRF = 1을 여전히 나타낸다는 것을 주목해야 한다.

[0810] FS 링크를 3개의 클라이언트에 송신하고 데이터를 6개의 저장 서버에서 중복으로 저장함으로써, 영역(1724C)은 SRF = 2가 매우 강력한 정도의 저장 복원성을 제공하는 조건을 규정한다. 영역(1724D)은 추가적인 복원성 향상을 도시하고, 여기에서 SRF = 3은 키를 수신하는 6개의 파일 저장 서버 및 4개의 클라이언트를 이용한다. 그에 따라, 가장 하단의 행 및 가장 좌측의 열은 가장 낮은 저장 복원성을 가지고, 상부 우측 모서리는 최고의 저장 복원성을 갖는다.

[0811] 이러한 개시 내용에 따라 만들어진 하이퍼보안 분산형 파일 저장은, SDNP 통신으로부터의 수 많은 본 발명에 따른 요소를 구성하는 것, 즉 재-활용하는 것에 의해서, 긴 기간동안 지속 가능한 보안을 달성한다. 이러한 본 발명에 따른 요소는 이하를 포함한다:

[0812] * 파일을 파싱하고 그 단편화된 콘텐츠를 파일 저장 서버에 연결된 많은 수의 관련없는 네트워크에 걸쳐 분산하는 것,

[0813] * 마스터 키가 없는 SDNP 동적 스크램블링되고 암호화된 익명의 단편화된 데이터 송신을 포함하는 엔드-투-엔드 하이퍼보안 통신을 이용하여 클라이언트와 파일 저장 서버 사이에서 파일을 전송하는 것,

[0814] * 저장 서버가, 저장된 데이터를 초기에 단편화 및 인코딩 하기 위해서 이용된 클라이언트 보안 자격 증명에 대한 액세스를 가지지 않는, 즉 파일 저장 서버가 파일을 디코딩, 액세스 또는 판독하는데 필요한 "클라이언트측" 라스트 마일 보안 자격 증명을 가지지 않는 방식으로, 단편화된 파일을 파일 저장 서버 내에 저장하는 것,

[0815] * 클라이언트(파일 소유자)가, 보안 링크를 통하는 것을 제외하고, 저장된 데이터를 디코딩하는데 필요한 보안 자격 증명을 가지지 않는, 즉 "클라이언트측" 라스트 마일이, 파일을 로컬적으로 인코딩하기 위해서 이용되는

"저장측" 라스트 마일 보안 자격 증명을 가지지 않는 방식으로, 저장 서버 내의 단편화된 파일을 선택적으로 인코딩하는 것,

[0816] * 파일을 위치시키고 열기 위해서 필요한 파일 저장 링크의 수를 제한하는 것, 그리고 임의의 중복 또는 백업 디바이스와 함께 파일 소유자의 클라이언트 디바이스에 대한 그러한 링크에 대한 사용자 액세스를 제한하는 것,

[0817] * 파일 링크를 실행하고 판독 또는 삭제 동작을 실시하기 위해서, 클라이언트 다중 인증 및 신원 확인을 요구하는 것,

[0818] * 익명 데이터 패킷 라우팅 및 익명 파일 명칭을 이용하는 것으로서, 그에 의해서 데이터 리콜을 위한 파일 링크의 이용이, 하이퍼보안 파일 저장의 위치 및 인코딩에 관한 정보를 노출시키지 않고, 파일 링크를 제외하고, 라우팅 정보가 SDNP 네트워크 또는 하이퍼보안 파일 저장 시스템에 저장되지 않는 것,

[0819] * 공개되지 않은 파일 서버 위치를 이용하여, 그리고 파일 저장 링크를 통하는 것을 제외하고, 클라이언트, SDNP 네트워크, 또는 다른 저장 서버에게 알려지지 않은 익명의 신원을 이용하여, 단편화된 파일을 많은 수의 저장 서버에 걸쳐 분산시키는 것,

[0820] * 삼중-채널 통신을 이용하는 것으로서, 분산형 저장을 위한 파일 라우팅을 계획하기 위해서 이용된 SDNP 시그널링 서버가 단편화된 파일의 콘텐츠 또는 파일을 인코딩하기 위해서 이용된 보안 자격 증명에 대한 액세스를 가지지 않고, 파일 콘텐츠를 전송하기 위해서 이용된 SDNP 미디어 노드가, 클라이언트 또는 파일 저장 서버의 신원 또는 어드레스를 가지지 않는 단일 홉 SDNP 데이터 패킷을 이용하는 것,

[0821] * 규칙적인 간격으로 그리고 반복된 파일 액세스 후에 동적 파일 재명명 및 데이터 재배치를 이용하는 것, 파일 재기록 동작의 시에 보안 자격 증명의 인코딩을 재생하는 것, 그리고

[0822] * 파일 분석을 방지하기 위해서 파일 저장 서버 디렉토리를 로컬적으로 암호화하는 것.

[0823] 전술한 것을 이용하면, 임의의 인식 가능한 파일 신원의 결여; (가능하게는 글로벌 스케일로) 네트워크에 걸쳐 분산된 단편화된 파일의 이용; 및 구역-특정형 보안 자격 증명의 이용은, 파일 저장 링크에 대한 액세스가 없이 하이퍼보안 저장된 파일에 대한 액세스 및 그 재구성을 생각할 수 없게 한다. 제한된 수의 그리고 SDNP 통신 시스템을 통해서만 분산된 그러한 FS 링크는 신원 확인에 의해서 더 보안된다.

[0824] 하이퍼보안 파일 저장을 위한 전술한 특징의 실행이, 도 9a에서 앞서 도시한 기능적 심볼을 이용하는 하이퍼보안 통신에서와 같은 방식으로, 개략적으로 제공될 수 있다. 간결함을 위해서, 도 92의 상부 도면에 도시된 바와 같이, 상태 또는 시간(926C)을 이용한 스크램블링(926), 정크 데이터 삽입(1053), 파싱(1052) 및 분할(1057) 및 암호화(1026)의 임의의 조합이 SDNP 인코딩 기능(1750)으로서 제공될 수 있다. 유사하게, 디코딩 기능(1751)은 상태 또는 시간(926B)을 이용한 해독(1032), 혼합(1061), 정크 데이터 제거(1053B) 및 언스크램블링(928)을 포함한다.

[0825] 전술한 보안 기능의 이용에서, 도 93a의 상단 도면은 클라이언트측 인코딩을 갖는 분산형 파일 저장의 프로세스를 도시한다. 도시된 바와 같이, 파일(1705)이 파싱되고(1052) 분할되어(1057), SDNP 클라이언트 $C_{1,1}$을 실현하기 위해서 이용된 클라이언트 디바이스(1700A) 내에서 파싱된 파일(1706)을 생성한다. 이어서, 결과적인 단편화된 파일이, 본원에서 개시된 방법에 따라 실시되는 라스트 마일 통신을 위한 SDNP 인코딩 동작(1750B)에 의해서 구역(U1) 보안 자격 증명을 이용하여 인코딩된다. 이어서, 직렬 또는 다중-경로 라스트 마일 통신에서 전달되는 파일 단편은 SDNP 게이트웨이 $M_{0,0}$에 의해서 수신되고, 파싱된 파일(1706)을 복원하는 구역(U1) 보안 자격 증명에 따라 SDNP 디코딩 동작(1751C)을 이용하여 디코딩된다. 이어서, 파싱된 파일(1706)은 SDNP 클라우드 구역(Z1) 보안 자격 증명에 따라 SDNP 인코딩 동작(1750C)에 의해서 재-인코딩된다. 메시형 전송 중에, SDNP 클라우드(미도시) 내의 일련의 구역(Z1) 디코딩 및 인코딩 동작 후에, 최종 데이터 패킷은, 예를 들어, 게이트웨이 $M_{0,8}$를 포함하는 각각의 SDNP 게이트웨이에 도달하고, 여기에서 SDNP 디코딩 동작(1751D)은 파싱된 파일(1706)을 복원하고, 구역(U9) 보안 자격 증명에 따라 SDNP 인코딩 동작(1750D)을 이용하여 이를 재-인코딩한다. 도시된 예에서, 이어서, 파싱된 파일(1706)이 2개의 파일로 단편화(분할)되고, 파싱된 파일(1706)의 단편화된 파일 2 및 3이 이어서 SDNP 디코딩 기능(1751E)을 이용하여 복원되고 파일 저장 서버(1740B 및 1740C) 내에 각각 저장된다. 이러한 방법에서, 파일 저장 서버 내에 저장된 데이터 파일이 단편화되나, (로컬 드라이브 암호화를 제외하고) 단편화되지 않은 경우에, 파일은 드라이브 데이터의 사이버 공격에 의해서 액세스될 수 있다. 따라서, 보안은 파일 단편화 및 분산된 저장에 의해서 달성된다.

[0826] 전체 클라이언트측 인코딩을 갖는 분산된 파일 저장의 프로세스를 도시하는, 도 93a의 하부 도면에 도시된 프로세스를 이용함으로써, 큰 정도의 파일 보안이 달성된다. 도시된 바와 같이, 파일(1705)이 SDNP 인코딩 동작(1750A)에 의해서 프로세스되어, SDNP 클라이언트 $C_{1,1}$을 실현하기 위해서 이용되는 클라이언트 디바이스(1700A) 내에서 스크램블링된, 암호화된, 파싱된 파일(1706)을 생성한다. 동작(1750A)은 또한 파일(1706)을 3개의 단편화된 파일 1, 2 및 3으로 분할하는 것을 포함한다. 이어서, 단편화된 파일 1, 2, 및 3이, 본원에서 개시된 방법에 따라 실시되는 라스트 마일 통신을 위한 SDNP 인코딩 동작(1750B)에 의해서 구역(U1) 보안 자격 증명을 이용하여 인코딩된다. 이어서, 직렬 또는 다중-경로 라스트 마일 통신에서 전달되는 파일 단편은 SDNP 게이트웨이 $M_{0,0}$에 의해서 수신되고, 스크램블링된, 암호화된, 파싱된 파일(1706)을 복원하는 구역(U1) 보안 자격 증명에 따라 SDNP 디코딩 동작(1751C)을 이용하여 디코딩된다. 이어서, 파싱된 파일(1706)은 SDNP 클라우드 구역(Z1) 보안 자격 증명에 따라 SDNP 인코딩 동작(1750C)에 의해서 재-인코딩된다.

[0827] 메시형 전송 중에, SDNP 클라우드(미도시) 내의 일련의 구역(Z1) 디코딩 및 인코딩 동작 후에, 최종 데이터 패킷은, 예를 들어, 게이트웨이 $M_{0,8}$를 포함하는 각각의 SDNP 게이트웨이에 도달하고, 여기에서 SDNP 디코딩 동작(1751D)은 스크램블링된, 암호화된, 파싱된 파일(1706)을 복원하고, 구역(U9) 보안 자격 증명에 따라 SDNP 인코딩 동작(1750D)을 이용하여 이를 재-인코딩한다. 스크램블링된, 암호화된, 파싱된 파일(1706)의 단편화된 파일 2 및 3이 이어서 SDNP 디코딩 기능(1751E)을 이용하여 복원되고, 파일 저장 서버(1740B 및 1740C) 내에 각각 저장된다. 그에 따라, 파일은 단편화되고 분산된 저장에 의해서뿐만 아니라, 클라이언트의 보안 구역에만 알려진 스크램블링, 정크 데이터, 및 암호화의 소정 조합에 의해서 보안된다. 유사한 방식으로, 파일 1은 SDNP 클라우드를 통해서 게이트웨이 $M_{0,4}$로 전송되고, 여기에서 그 파일은 도 88의 패킷(1712A)에 대해서 도시된 바와 같이 구역(U7) 내의 파일 저장(1700H) 내에 저장된다.

[0828] 설명된 양 예에서, 도 93b의 도면에 도시된 최종 SDNP 디코딩 동작(1751E)을 제거함으로써, 더 큰 정도의 보안성이 달성될 수 있다. 이러한 방식으로, 파일 저장 서버에 저장된 파일은 구역(U9) 보안 자격 증명을 이용하는 SDNP 인코딩 동작(1750D)에 의해서 인코딩되어 유지된다. 상부 도면에서, 파일은 클라이언트에 의해서 단편화되나, 구역(U9)을 위한 저장측 보안 자격 증명에 따라 인코딩된다. 하부 도면에서, 파일은 클라이언트측 보안 자격 증명(U1)에 따라 인코딩되고, 이어서 구역(U9)을 위한 저장측 보안 자격 증명에 따라 2번째로 인코딩된다. 그러한 파일의 이중 인코딩은, 단편화되고 분산된 파일 저장에 의해서 보안되는 것 외에도, 네스트형 하이퍼보안 저장을 나타내는데, 이는 구역(U9) 보안 자격 증명에 의해서 인코딩된 파일이 U1 보안 자격 증명에 의해서 인코딩된 파일을 포함하기 때문이다. 개시된 바와 같은 네스트형 보안의 장점은, 클라이언트 및 저장 서버 어느 것도 저장 파일을 열기 위한 필요 정보를 갖지 않는다는 것이다.

[0829] 하이퍼보안 분해된 파일 저장을 구현하는 예시적인 방법의 요지가 도 94에 도시되어 있다. 도시된 예에서, 하이퍼보안 통신 및 SDNP 클라우드 라우팅을 위해서 이용된 인코딩 및 디코딩이 제거되어 파일 인코딩의 넷 효과만을 나타낸다. 상부 좌측 모서리는 클라이언트 구역 단편화의 경우를 나타내고, 여기에서 문서는 구역(U1) 보안 자격 증명에 따라 단편화되나, 네트워크의 저장측에 의해서 부여된 어떠한 부가적인 보안 규정도 가지지 않는다. 하부 좌측 모서리는 클라이언트 구역 인코딩의 경우를 나타내고, 여기에서 문서는 동작(1750B)에 의해서 인코딩되고, 즉 구역(U1) 보안 자격 증명에 따라 스크램블링되고, 정크화되고, 단편화되고, 암호화되나, 네트워크의 저장측에 어떠한 보안 규정도 도입하지 않는다.

[0830] 상부 우측 모서리는 클라이언트 구역 U1 단편화의 경우를 나타내나, 여기에서 SDNP 인코딩의 추가적인 단계 즉, 스크램블링, 정크 삽입, 단편화, 및 암호화가 구역(U9)에 따라 저장측에 도입된다. 하부 우측 모서리는 완전 네스트형 하이퍼보안 파일 저장의 예를 나타내고, 여기에서 파일은 구역(U1) 클라이언트측 보안 자격 증명을 갖는 SDNP 인코딩 동작(1750B)에 따라 인코딩되고 단편화되며, 이어서 파일은 저장측 라스트 마일의 구역(U9) 보안 자격 증명에 따라 2번째로 인코딩된다.

[0831] 파일의 리콜 및 판독을 위해서, 데이터 리콜은, 도 95에 도시된 바와 같이, 인코딩의 정확한 역순으로 실행되는 역-기능을 포함하는 보안 동작을 이용하여야 한다. 상부 좌측 경우에서, 클라이언트 구역 단편화된 데이터를 리콜하기 위해서, 상이한 파일 저장 서버들로부터 리콜된 파싱된 파일(1706)이 병합 동작(1061)을 이용하여 재조합되어 원래의 파일(1705)을 복원한다. 클라이언트 구역 인코딩된 데이터를 리콜하는 하부 좌측 경우에, 혼합, 해독, 언스크램블링을 포함하는 분할 동작(1750B)의 정확한 역-기능인, SDNP 디코딩 동작(1751H)을 이용하여 원래의 파일(1705)에 액세스하도록, 상이한 파일 저장 서버들로부터 리콜된 파싱된 파일(1706)이 회복된다. 저장 구역 인코딩된, 클라이언트 구역 단편화된 파일에 관한 상부 우측 경우에, 역 동작은, 구역(U9) 보안 동작의 영

향을 원상태로 돌려 파싱된 파일(1706)을 복원하기 위해서 SDNP 디코딩 동작(1751F)을 첫 번째로 실시하는 것, 그리고 이어지는 구역(Z1) 보안 자격 증명에 따라 만들어진 파일 분할 동작(1057)의 효과를 취소하기 위해서 파일 병합 동작(1061)을 포함한다.

[0832] 완전-네스트형 하이퍼보안 파일을 판독하기 위한 하부 우측 예에서, 상이한 파일 저장 서버들에 저장된 데이터가 구역(U9) 보안 자격 증명을 이용하여 SDNP 디코딩 동작(1751D)에 의해서 디코딩되어, 구역(Z1) 보신에 따라 여전히 스크램블링되고, 정크화되고, 파싱되고, 암호화된 다수 부분 파일인, 파일(1706)을 재구성한다. 이어서, 구역(Z1) 특정 SDNP 디코딩 동작(1751H)은, 원래의 파일(1705)을 리콜하기 위해서 혼합, 해독, 언스크램블링을 포함하는 동작인, 인코더(1750B)의 순차적인 역-기능을 실시한다. 파일을 복원하기 위해서 순차적인 역-기능을 실행하는 동작은 이를 생성하기 위해서 사용된 시퀀스의 반대 순서로 이루어져야 한다. 예를 들어, 인코딩이 분할, 이어서 스크램블링, 및 이어서, 암호화를 포함하는 경우에, 반대 또는 역-기능 즉, 디코딩은, 해독, 이어서 언스크램블링, 그리고 이어서 혼합의 동작 시퀀스를 포함하여야 한다. 그러나, 인코딩이 패킷의 스크램블링, 이어서 암호화, 그리고 이어서 분할을 순차적으로 포함하는 경우에, 반대 또는 역-기능 즉, 디코딩은 데이터 패킷의 혼합, 이어서 해독, 및 최종적으로 언스크램블링의 시퀀스를 포함하여야 한다.

[0833] 파일 리콜 또는 "파일 판독 동작"을 실시하기 위해서, 클라이언트는, 시스템의 하이퍼보안 파일 저장 시스템에 저장된 파일을 리콜하고 판독하는데 필요한 단계를 개시하기 위해서 "파일 저장 판독 링크"를 클릭하는 것에 의해서 합쳐진 파일 링크를 실시한다. 판독 프로세스는 도 96a에 도시된 바와 같은 이하의 단계를 포함한다:

[0834] * 파일 소유자 및 클라이언트(1700A) 또는 인증된 사용자가, SDNP 인에이블드 하이퍼보안 메신저(1196), 파일 관리자, 또는 다른 SDNP 인에이블드 인터페이스와 같은 SDNP 애플리케이션 내의 "파일 저장 판독 링크"를 클릭한다.

[0835] * 다이알로그 인터페이스(1765) 또는 선택적으로 명령 라인 지시를 이용하여, 클라이언트(1700A)는, 파일 판독, 파일 편집(기록 특권으로 파일의 복사본을 만든다), 파일 제거(삭제), 링크 리프레시(보안 자격 증명 재발행), 또는 파일의 재분배(파일 단편들을 상이한 파일 저장 서버들로 이동시키고 새로운 파일 저장 판독 링크를 파일 소유자 클라이언트 또는 클라이언트들에 발행)를 포함하는, 그 파일 요청(1761)을 특정한다.

[0836] * "클라이언트 입증" 동작(1762)에서, SDNP 시그널링 서버(1715)는 파일을 요청하는 클라이언트 또는 클라이언트들의 신원을 확인한다(인증). 다이알로그 박스(1767)를 이용하여, 클라이언트는 PIN, 또는 선택적으로 디바이스 또는 보안 토큰을 검출하는 제2 인자를 이용하여 그 신원을 확인시켜야 한다. 대안적으로, SMS 텍스트가, 동일 클라이언트에 의해서 소유된 다른 디바이스에 송신될 수 있다. 다수의 클라이언트에 의한 액세스 승인을 요구하는 파일에서, 모든 사용자의 신원이 반드시 입증되어야 한다(다중-인증).

[0837] * "특권 입증" 동작(1763)에서, 시그널링 서버(1715)는, 요청 클라이언트(1700A)가 판독 또는 판독/삭제 특권(인증)을 가지고 요청 파일에 액세스하도록 인증되었다는 것을 확인한다. 사용자가 여전히 파일을 다운로드 또는 판독하기를 원하는지의 여부를 확인하기 전에, 결과가 다이알 박스(1768) 내에 디스플레이된다. 신원이 확인되지 않는 경우에, 요청자는 다시 시도하도록 지시받을 수 있다. 특정된 수의 실패 시도 후에, 파일 관리자(1700Z)(있는 경우)는 실패 시도를 인식할 것이고, 계정을 록킹할 것이다. 다이알로그 박스는 문제를 사용자에게 알려 그들이 파일 관리자와 접촉하게 할 수 있거나, 대안적으로, 해킹이 의심되는 경우에, 박스가 빈칸이 되거나 심지어 사용자를 SDNP 애플리케이션으로부터 완전히 방출한다.

[0838] * 문서 요청 관리 동작(1764)에서, SDNP 시그널링 서버(1715)는 파일 액세스 요청 및 요청의 특성(관리)과 관련하여 파일 저장 관리자(1700Z)에게 알린다. 이러한 관리 단계는 (i) 전부 생략될 수 있고, (ii) 파일 저장 관리자의 계정으로 파일 액세스 요청을 로그할 수 있고, (iii) 시도된 파일 액세스를 즉각적으로 알리는 메시지를 파일 저장 관리자에게 송신할 수 있고, 또는 (iv) 파일을 요청하는 클라이언트에게 액세스 허용되기 전에 다이알로그 박스(1769)를 통해서 파일 저장 관리자의 승인을 요구할 수 있다.

[0839] 이러한 인증, 입증, 및 관리(AAA) 단계 후에, 승인 시에, 클라이언트는, 예시된 목적을 위해서 판독 요청으로서 사용되는 것으로 여기에 도시된, 도 96b에 도시된 흐름도에서 도시된 단계를 이용하여 파일에 대한 액세스를 요청한다. 이러한 단계는 이하를 포함한다:

[0840] * 판독 요청 동작(1770)에서, 요청하는 클라이언트(1700A)는 파일 판독 요청을 SDNP 시그널링 서버(1715)에 송신한다.

[0841] * 저장 서버 명칭 요청 동작(1771)에서, SDNP 시그널링 서버(1715)는 파일 저장 서버 명칭 요청을 SDNP 명칭 서버(1714)에 송신하여 관련 파일 저장 서버, 예를 들어 파일 저장 서버(1700M)의 현재 SDNP 어드레스를

요청한다. SDNP 방법에 따라, SDNP 클라이언트(파일 서버 포함)를 위한 SDNP 어드레스는, 장기간의 클라이언트 추적 가능성을 방지하기 위해서, 적어도 매일 한차례 변화된다.

[0842] * 저장 명칭 전달 동작(1772)에서, SDNP 명칭 서버(1714)는 요청된 파일 명칭 "FS 어드레스"를 SDNP 시그널링 서버(1715)에 전달하고, 그에 의해서 SDNP 시그널링 서버는 파일 리콜 라우팅을 맵핑한다.

[0843] * 라우팅 지시 동작(1773)에서, SDNP 시그널링 서버는 파일 라우팅 지시를 클라이언트(1700A)에, 서버(1700U)와 같은 SDNP 클라우드 내의 노드에, 그리고 상태 또는 시간(920), 수치 시드(923), 해독 키(1030), 및 (대칭적 키 암호화된 통신에서 사용된) 선택적인 암호화 키(1022)를 포함하는 구역(U9) 보안 자격 증명을 갖는 파일 저장 서버(1700M)와 같은 구역 특정 보안 자격 증명을 갖는 파일 저장 서버에 송신한다.

[0844] * 로컬 파일 복원 동작(1774)에서, 파일의 생성에 특정된 상태 또는 시간 정보를 포함하는 적용 가능한 보안 자격 증명을 이용할 때, 모든 저장측 라스트 마일 내의 DMZ 서버는 파싱된 파일을 디코딩하고 복원하며, 운반을 위한 준비에서 데이터를 하나 이상 데이터 패킷 내로 배열한다.

[0845] * 파일 전달 동작(1775)에서, 각각의 파싱된 파일은 SDNP 시그널링 서버의 라우팅 지시에 따라 SDNP 네트워크에 걸쳐 독립적인 전달을 이용하여 요청 클라이언트에 전달되고, 예를 들어 여기에서 파일 저장 서버(1700M)는 파일을 클라이언트(1700A)에 송신한다.

[0846] * 진입되는 파싱된 데이터 파일은 클라이언트 구역 보안 자격 증명에 따라 더 디코딩되고, 파싱된 파일이 병합되어 관찰 또는 전달을 위해서 준비된 원래의 미파싱 파일을 재생성한다.

[0847] 그러한 단계는 이하의 도면의 시퀀스로 표시된다. 도 97a에서, 어드레스 "IP $C_{1,1}$"에서의 클라이언트 디바이스는, TCP 전송, 파일 관련된 헤더 정보, 및 둘 이상의 FS 링크을 특정하는 C&C 페이로드(1811A)를 포함하는, 데이터 패킷(1810a)을 이용하여 어드레스 "IP S"에서 시그널링 서버(1715)에 대한 파일 판독 요청을 만든다. FS 링크는, 라우팅을 위해서 SDNP 어드레스 또는 IP 어드레스로 변환되어야 하는 태그 또는 의사 어드레스를 이용하여 익명으로 저장된 파일 단편의 위치를 설명한다. 그러나, 시그널링 서버(1715)는 이렇게 명명된 사용자 ID에 대한 현재의 SDNP 어드레스를 알지 못하고, SDNP 명칭 서버(1714)로부터 현재의 정보를 요청하여야 한다. 도 97b에서, 시그널링 서버(1715)는 데이터 패킷(1,810B)을 명칭 서버(1714)에 송신하여 파일 저장 서버 노드 $F_{7,1}$, $F_{9,4}$, 및 $F_{9,1}$의 IP 또는 SDNP 어드레스를 요청한다. 도 97c에서, 명칭 서버(1714)는, 파일 저장 서버 노드 $F_{7,1}$, $F_{9,4}$, 및 $F_{9,1}$의 IP 또는 SDNP 어드레스를 포함하는 데이터 패킷(1810C)을 시그널링 서버(1715)에 송신한다. 이어서, 시그널링 서버(1715)는 파일 저장 서버에 대한 파싱된 파일의 라스트 마일 및 메시형 클라우드 전달을 계산한다.

[0848] 도 97d에서, 시그널링 서버(1715)는 C&C 데이터 패킷을 저장측에 위치된 라스트 마일 노드에, 즉 구역(U7 및 U9)에 송신한다. 도시된 바와 같이, 데이터 패킷(1810G)이 어드레스(S)에서 시그널링 서버(1715)로부터 어드레스 "IP $F_{7,1}$"에서 파일 저장 서버(1700H)에 포워딩되어, "파일 1 판독 지시"(1811G)를 포함하는 C&C 페이로드를 운반한다. 이러한 패킷은, U7 보안 자격 증명을 이용하여, ID 태그 1을 갖는 파일을 그 어드레스 "IP $F_{7,1}$"로부터 어드레스 "IP $M_{0,4}$"에서 SDNP 게이트웨이로 송신하도록 파일 저장 서버에 지시한다.

[0849] 동시에, 데이터 패킷(1810F)은 SDNP 게이트웨이 $M_{0,4}$로 송신되고, 패킷은 어드레스 "IP S"로부터 "IP $M_{0,4}$--"로 라우팅되고, 패킷은, 태그 1을 갖는 데이터 패킷이 게이트웨이 노드 $M_{0,4}$ 에 의해서 예상되어야 한다는 것, 그리고 수신될 때, SDNP 클라우드에서 Z1 보안 자격 증명을 이용하여, 예를 들어 어드레스 "SDNP $M_{0,31}$"로 포워딩되어야 한다는 것을 통신하는 C&C 페이로드(1811F)를 포함한다.

[0850] "파일 3 판독 지시"를 포함하는 C&C 페이로드(1811I)를 포함하는, 제2 데이터 패킷(1810I)이 어드레스 "IP S"에서 SDNP 시그널링 서버(1715)로부터 어드레스 "IP $F_{9,1}$"에서 파일 저장 서버(1700M)로 송신된다. 이러한 지시는, 구역(U90) 보안 자격 증명을 이용하여, ID 태그 3을 갖는 파일을 어드레스 IP $M_{0,8}$에서 SDNP 게이트웨이에 송신하도록, 파일 저장 서버(1700M)에 명령한다. 다른 C&C 패킷(미도시)이, 마찬가지로, 노드 $F_{9,4}$ 및 $M_{0,8}$뿐만 아니라 SDNP 클라우드 내의 노드와 같은 노드를 다른 파일 저장 서버 및 게이트웨이로 송신한다.

[0851] 도 97e에서, 시그널링 서버(1715)는 데이터 패킷(1810D)을 클라이언트 디바이스(1700A)에 송신하고, 패킷은 라우터(1702G)를 통해서 어드레스 "IP S"로부터 "IP $C_{1,1}$"로 라우팅된다. 데이터 패킷(1810D)은, 구역(U1) 보안 자

격 증명을 이용하여 어드레스 "IP $M_{0,0}$"에서 SDNP 게이트웨이(1701U)로부터 태그 1, 태그 2 등을 갖는 다수의 진입 데이터 패킷의 예측을 클라이언트에게 알려주는 C&C 페이로드(1811D)를 포함한다. 동시에, 시그널링 서버(1715)는 또한 데이터 패킷(1810E)을 SDNP 게이트웨이(1701U)에 송신하고, 패킷은 어드레스 "IP S"로부터 "IP $M_{0,0}$"으로 라우팅된다. 이러한 패킷은 SDNP 클라우드 내로부터 전송된 태그 1, 태그 2, 및 태그 3으로서 식별된 진입 데이터 패킷을 위해서 적용될 수 있는 구역(U1) 내의 라스트 마일 라우팅을 위한 C&C 페이로드(1811E)를 포함한다.

[0852] 명령 및 제어 데이터 패킷이 네트워크로 분배되면, 파일 전달이 발생될 수 있다. 전달의 제1 단계가 도 98에 도시되어 있고, 여기에서 FS 링크 3을 포함하는 데이터 패킷(1741R)이, 예시적인 상태(920), 수치 시드(929), 해독 키(1030), 및 암호화 키(1022)를 포함하는 정보를 SDNP 디코딩 동작(1751R)에 제공한다. SDNP 디코딩 동작(1751R) 대신, 이러한 정보가 DMZ 서버(1762)에 의해서 프로세스되어, 파싱된 파일이 마지막으로 인코딩되었을 때의 상태인, 상태(920)에서 모두가 실시되는, 패킷 해독(1032R), 혼합(1061R), 역-정킹(1053R), 및 언스크램블링(928R)과 같은 공유 비밀을 포함하는 기능을 실행한다. 암호화 키(1022)가 파일 디코딩을 위해서 구체적으로 필요하지 않으나, 파싱된 파일을 클라이언트 및 파일 소유자에게 다시 전송하기 위해서 대칭적 키 암호화에서 이용될 수 있음을 주목해야 한다.

[0853] 파일 라우팅 및 데이터 전송이 도 99에서 도시되어 있고, 이는 U7 보안 자격 증명을 이용하여 어드레스 "IP $F_{7,1}$"로부터 "IP $M_{0,4}$"까지 파일 1을 운반하는 TCP 데이터 패킷(1720A), U9 보안 자격 증명을 이용하여 어드레스 "IP $F_{9,4}$"로부터 "IP $M_{0,8}$"까지 파일 2를 운반하는 TCP 데이터 패킷(1720B), 및 U9 보안 자격 증명을 이용하여 어드레스 "IP $F_{9,1}$"로부터 "IP $M_{0,8}$"까지 파일 3을 운반하는 TCP 데이터 패킷(1720C)를 포함한다. SDNP 클라우드(미도시)를 통한 전송 후에, 일련의 데이터 패킷(1720X)이 어드레스 "IP $M_{0,0}$"에서 SDNP 게이트웨이로부터 클라이언트 어드레스 "IP $C_{1,1}$"까지 전달된다.

[0854] 판독 동작에서, 데이터는 그 "판독 전용" 형태로 SDNP 앱 내로 로딩된다. 파일이 SDNP 애플리케이션 내에서 샌드박스되어(sandboxed) 유지되는 한, 파일은 SDNP 애플리케이션 및 네트워크의 특징에 의해서 보호되고, 디바이스의 운영 시스템의 로그인 과정 및 약한 보안 규정에 의존하지 않는다. 프라이빗 문서에 대한 판독 전용 액세스의 필요성은 비지니스에서 일반적이다. 회사의 재정, 법률, 제조, 엔지니어링 및 품질 부서에 의해서 생성된 파일은, 흔히 판독-전용 콘텐츠를 나타내는 것의 예를 도시한다. 많은 경우에, 이러한 회사 프라이빗 파일은 그 방출에 앞서서 검토를 위해 회사 임원에게 포워딩되어야, 즉 전자적으로 분배되어야 한다.

[0855] 해당 담당자에 대한 회사의 그리고 개인의 책임에 대한 심각한 경제적 그리고 심지어 법률적 결과를 수반하는, 통신된 정보의 우연한 또는 조기 공개가 치명적일 수 있다. 예를 들어, 공공 회사의 공개되지 않은 재정 보고서는 그 공개까지 엄격한 비밀이다. 미국에서, 규정 FD 또는 "공정 공개"는, 정보가 특혜 없이 동시에 모두에게 공공적으로 이용될 수 있어야 한다는 것을 의미한다. 만약 임의의 외부 당사자가 그 공공 공개 전에 해당 정보에 액세스한다면, 이는 규정 FD의 위반이 된다. 문서의 비밀을 유지 및 보장하기 위한 의무를 회사가 소홀히 하였기 때문에 규정 FD 위반이 발생된 것으로 법원이 결정하는 경우에, 심지어 선택적인 공개로부터 초래된 내부자 거래가 없더라도, 회사는 그 위반에 대해서 유죄가 될 수 있고 그 담당자는 개인적으로 책임을 질 수 있다.

[0856] SDNP 앱에서, 하나의 계정 신원으로부터 다른 계정 신원으로의 데이터 전달을 방지하기 위해서, 검색 파일이 분류되고(샌드박스화되고), 예를 들어 파일은 비지니스와 개인 계정 사이에서 스왑될 수 없다. 판독자의 인증 특권에 따라, 사용자는 SDNP 애플리케이션의 외부로 그리고 디바이스 메모리 내의 인코딩되지 않은 저장부 내로 검색 파일을 다운로드할 수 있거나 할 수 없다.

[0857] SDNP 인에이블드 애플리케이션 외부의 파일 다운로드는 파일 및 그것이 포함하는 데이터의 보안을 손상시킨다. SDNP 애플리케이션 내에 있는 데이터에 대해서, 액세스가 제어되고, 사용자의 행위가 제한되며, 디바이스 및 SDNP 네트워크 모두는 사용자 신원을 입증하여야 한다. 그러한 다중-계층 다중 인증은, 전화를 열기 위해서 필요한 단순한 4-숫자 핀의 파괴보다 극복하기가 훨씬 더 어렵다. 대조적으로, 파일이 컴퓨터, 태블릿, 또는 휴대폰으로 일단 다운로드되면, 미인증 액세스를 방지하는 것, 누가 액세스 하였는지를 결정하는 것, 또는 누가 파일을 복사하였는지를 결정하는 것이 거의 불가능하다.

[0858] 따라서, SDNP 통신을 이용하여, 파일 소유자는 민감한 문서 및 파일을 록킹, 즉 분류할 수 있고, 그에 따라 다른 사람들은 이들을 판독할 수 있으나 이들을 그 전화기로 다운로드할 수 없다. 부가적인 단계를 이용하여 LCD 디스플레이 화면의 스크린 샷 또는 촬영을 방지할 수 있다. 보안 및 프라이버시가 요구되지 않는 다른 경우에,

SDNP 앱으로부터 전화기의 메모리로의 검색 파일의 전달이 가능하고 제한 없이 사용될 수 있다.

[0859] 편집 동작에서, 파일의 편집 가능한 형태가 디바이스 내로 다운로드될 수 있고 파일의 편집에 필요한 애플리케이션 프로그램에 전달된다. 파일 요청 및 데이터 교환을 실행하기 위해서, - SDNP 네트워크의 데이터 전달의 측면에서 - 클라이언트의 SDNP 애플리케이션의 동작 이외에, 파일 판독 요청과 파일 편집 요청 사이의 SDNP 네트워크 동작의 기본적인 차이는 없고, 그러한 동작들은 기능적으로 동등하다. 그에 따라 판독 동작과 편집 동작 사이의 차이는 애플리케이션 특정 파일을 포함하는 계층 5 내지 계층 7의 실행에서 주로 존재하는 것으로 간주될 수 있다.

[0860] 검색된 파일을 편집하기 위해서, 애플리케이션은 (i) 디바이스의 운영 시스템 고유의, 그러나 SDNP 애플리케이션의 외부에서 동작되는, 디바이스 임베딩된 애플리케이션(예를 들어, Simpletext)일 수 있거나, (ii) 디바이스의 운영 시스템 상에서, 그러나 SDNP 애플리케이션의 외부에서 작동하는 제3자 애플리케이션, 예를 들어 Microsoft Word, Adobe Acrobat, 등일 수 있거나, 또는 (iii) SDNP 애플리케이션 내부에서 동작되고 디바이스 또는 그 운영 시스템에 의해서 직접적으로 액세스될 수 없는 보안 애플리케이션일 수 있다. 예를 들어, 회사 보도 자료가 SDNP 애플리케이션 샌드박스 내에서 편집될 수 있으나, 전화기의 메모리 내로 다운로드될 수 없다. 비지니스 보안을 유지하기 위한 부가된 규정으로서, 비지니스가 소유한, 즉, SDNP 비지니스 계정 칸 내에 샌드박스화된 임의 파일은, 비록 개인 및 비지니스 프로파일이 동일 SDNP 애플리케이션 내에서 작동되지만, 사용자의 개인 SDNP 계정으로 전달될 수 없다.

[0861] 편집 후에, SDNP 파일 저장 서버 상에서의 편집된 파일의 저장은, 파일 소유자가 구체적으로 요청하지 않는 한, 기존 파일에 겹쳐쓰기되지 않는다.

[0862] 그 대신, 제2 버전이 제1 버전에 더하여 저장되고, 이전 버전의 삭제는 사용자가 삭제 동작을 실행할 것을 요구한다. 하이퍼보안 파일 저장이 신원 확인을 항상 요구하기 때문에, 편집된 파일을 저장하는 프로세스는 전용 하이퍼보안 네트워크 통신을 가지지 않는 파일 저장부로부터 입수될 수 없는 특이적 시스템 특징을 포함할 수 있다. 하나의 그러한 특이적 특징은 파일에 사인하고 일자를 기입하기 위해서(또는 아시아에서 스탬핑/초핑하고 그리고 일자를 기입하기 위해서) 이용된 사인 입증 기능이다. 서명 기능은 문서 홀더에 그리고 원래의 문서 생성기에 송신된 등록된 영수증을 포함할 수 있다.

[0863] 본 발명에 따라 만들어진 하이퍼보안 데이터 저장에서, 삭제 동작은 모든 기존의 파싱된 파일에 무작위 숫자를 겹쳐 쓰는 것 그리고 선택적으로 1시간 후에 이를 다시 실시하여, 작지만 검출될 수도 있는 저장된 비트의 전하 또는 자기장의 아날로그 변동을 더 불분명하게 하는 것을 포함한다. 파일 기록은 또한 데이터 드라이브의 파일 기록을 혼동스럽게 하도록 겹쳐쓰기된다. 데이터 및 파일 기록을 삭제한 후에, 클라이언트의 데이터 링크가 SDNP 시스템의 메시지 자가-파괴 특징을 이용하여 클라이언트 디바이스 내에서 파괴되고, FS 링크의 임의의 나머지가 SDNP 시스템으로부터 퍼지된다. 그러나, 파일 시스템 관리자가 제3자 소프트웨어로 그 사용자 기반의 활동성을 추적한 경우에, 파일 자체에 액세스하지 않았더라도, 관리자는 파일의 소유자, 그 생성 일자, 파일에 누가 그리고 언제 액세스하였는지, 그리고 삭제된 때를 포함하는 파일의 이력에 관한 메타데이터를 여전히 보유할 수 있다.

[0864] SDNP 네트워크 및 하이퍼보안 라스트 마일 기능은 또한, 개인 계정 프로파일을 위한 것이 아니라 회사 계정을 위한 다른 특징 및 동작 과정을 지원할 수 있다. 전술한 바와 같이, 개인 계정에서의 삭제 동작은 정크 데이터를 파일에 재기록하는 것, 파일의 존재에 관한 드라이브의 색인 기록의 퍼지, 그리고 메시지 자가-파괴를 이용하여 파일의 이전의 단편화된 저장 위치에 대한 모든 FS 링크의 파괴를 포함한다. 그러나, 회사 계정에서, 파일 저장 관리자는, 파일을 영구적으로 파괴하기 위해서는, 예를 들어 도 96a의 다이알로그 박스(1769)과 유사하나 파일 소유자가 아니라 관리자에게 송신되는 승인 프로세스를 이용한, 사전 승인을 필요로 할 수 있다.

[0865] 회사의 파일 관리자가 파일 삭제를 허용하지 않도록 선택한 경우에, 이하를 포함하는 몇 가지 시나리오가 발생될 수 있다: (i) 파일이 삭제되지 않을 것이고 파일 판독 링크가 그들의 SDNP 애플리케이션 또는 SDNP 통신기 메시지 이력에서 유지된다는 것을 파일 소유자가 통지 받거나, (ii) 파일 소유자는 파일이 삭제되지 않을 것임을 통지 받고, 예를 들어 이는 "보관 목적"을 위해서 보전될 것이나, 그 개인 파일 판독 링크는, SDNP 시스템의 메시지 자가 파괴 규정을 이용하여, 그들의 SDNP 애플리케이션으로부터 제거될 것이며, 이는 소유자가 파일을 삭제하려고 한 경우에 파일 저장 관리자만이 이를 리콜할 수 있다는 것을 의미하고, 또는 (iii) 파일 소유자의 개인 파일 판독 링크는 SDNP 시스템의 메시지 자가 파괴 규정을 이용하여 그들의 SDNP 애플리케이션으로부터 제거될 것이나, 파일이 회사에 의해서 유지되고 있다는 것을 이들은 통지 받지 않는다.

[0866] 개시된 익명적 단편화되고 분산된 파일 저장 시스템의 동작에 고유한 라스트 마일 하이퍼보안으로 인해서, "파일 저장 판독 링크"가 없이는, 심지어 파일 저장 관리자에 의해서도, 저장된 파일이 검색 가능하지 않다. 관리자가 파일에 대한 액세스를 획득하기 위해서, 이들은, 파일이 저장되고 편집될 때마다, 상응 파일 저장 판독 링크에 있어야 한다. 이러한 모니터링의 레벨이 회사 계정을 위해서 가능하지만, 모든 파일에 대한 모든 변화를 추적할 때 생성되는 많은 양의 데이터는 항상 모든 파일 관리 시스템을 압도할 것이다. 개시된 바와 같은 개시된 SDNP 시스템에서 가능한 지능형 필터는 시도된 파일 삭제만을 추적한다. 이러한 접근방식에서, 관리자는 파일의 생성은 모니터링하지 않고, 파일을 삭제하려는 시도만을 추적한다. 파일 소유자가 파일을 삭제하려고 시도할 때마다, 그때만, 상응 파일 저장 판독 링크가 승인 또는 저장을 위해서 관리자의 데이터베이스 또는 콘솔에 전달된다.

[0867] 모니터링이 필요한 특정 피고용인 및 계약자를 식별함으로써, 데이터베이스 크기가 더 최소화될 수 있다. 예를 들어, 회사가 회계 감사 또는 특허 소송에 관여된 경우에, 일반적으로 당사자들은 어떠한 관련 데이터도 삭제하지 않도록 또는 임의의 파일을 삭제하지 않도록 통지받는다. 개시된 SDNP 파일 저장 시스템에 의해서 인에이블링된 파일 관리 특징을 이용하여, 조사에 관련된 직원의 임의의 파일 삭제 시도가 시도된 삭제를 로그하는 것에 의해서 추적될 수 있고, 경우에 따라 "해당 시간에" 파일 저장 링크의 복사본이 파일 저장 관리자에게 또는 독립적인 조사자에게 송신될 수 있다. 그러한 방법은 유리한데, 이는 그 방법이 모니터링되는 데이터의 양을 제한하고, 이는 당연하게 잘못된 것을 덮으려고 하는 의심스러운 활동을 관리자에게 경고한다. 클라이언트 및 파일 소유자의 디바이스 자체의 파괴에 의한 파일 저장 명칭 링크의 우발적 또는 악의적인 손실을 방지하기 위해서, 앞서 개시된 바와 같은 중복 파일 저장 링크의 이용이 필수적이다. 회사의 경우에, 백업 복사본이 보안된 사무실 내에 위치된 컴퓨터 상에서 또는 중앙 집중된 회사 서버에서 유지될 수 있다.

[0868] 극도의 보안의 경우에, 예를 들어 국가 안보의 경우에, 파일의 삭제는 이하를 포함하는 다수 단계의 방법을 포함할 수 있다: (i) 파일을 무작위 데이터로 겹쳐 쓰는 것, (ii) 저장 드라이브의 모든 다른 파일을 일부 다른 저장 디바이스 상으로 복사하는 것, (iii) 드라이브의 벌크 삭제를 실시하는 것, (iv) 드라이브를 재포맷하는 것, (v) 드라이브의 저장 필드를 무작위 숫자로 겹쳐쓰기 하는 것, 그리고 선택적으로 (vi) 필요한 경우에 보전된 파일을 역으로 복사하는 것. 통상적인 파일의 데이터 겹쳐쓰기와 달리, 벌크 삭제 프로세스는 읽기-쓰기 저장 미디어 자체에 영향을 미쳐 그 전기적, 자기적, 또는 광학적 특성을 분자 레벨에서 자연스럽게 무작위화한다. 자기 드라이브의 벌크 삭제는 큰 전자석을 이용할 수 있고, 플래시의 벌크 삭제는 IC를 고온까지 가열하는 것 그리고 가능하게는 이들을 높은 동작 전압의 이온화 복사선에 노출시킬 수 있다. 자기적-광학적 드라이브는 큰 자기장을 이용하여 벌크 삭제될 수 있다. 재-기록 가능 광학 드라이브는, 디스크 포맷 트랙을 가로질러 스캐닝되는 밝은 스캐닝 레이저를 이용하여 벌크 삭제될 수 있다. 어떠한 경우에도, 벌크 삭제는, 심지어 저장 매체가 손상되어 다시 사용할 수 없게 되는 위험을 감수하면서도, 삭제 후에 저장 미디어가 완전히 데이터를 잃게 되는 극단적인 경우를 나타낸다.

[0869] 하이퍼보안 분산형 파일 저장 시스템에서의 다른 중요 인자는 파일 데이터 및 링크 액세스의 무결성을 유지하는 것이다. 링크의 우발적 손실 방지를 보장하기 위해서, 때때로, 파일 저장 판독 링크를 재구축 즉, 재확인하고 보안 자격 증명을 재발행하는 것이 유리하다. 본원에서 "리프레시 링크" 명령으로 지칭되는 이러한 프로세스는 수동적으로 또는 자동적으로 클라이언트로부터 개시될 수 있고, 또한 약간의 미리 규정된 간격 후에 파일 저장 서버로부터 개시될 수 있다. 클라이언트로부터 개시된 요청의 경우에, SDNP 시그널링 서버가 명령 및 제어 패킷을 상응 서버에 통신한다. 링크 리프레시가 도 100에 도시된 바와 같이 개시되면, 파일은, 구역(U9) 보안 자격 증명을 이용하여 이전에 생성되었던 시간($t_1$) 시간에서의 "올드" 상태인, 상태(320X)에서 SDNP 디코딩 동작(1751F)에 의해서 판독 및 디코딩된다. 이어서, 파일은 시간($t_2$)에서의 새로운 상태(920Y)를 이용하여 SDNP 인코딩 동작(1750D)에 의해서 재-인코딩되고 저장 드라이브에 저장된다. 이어서, 리프레시된 저장 링크, 예를 들어 FS 링크 3이 SDNP 네트워크를 통해서, 클라이언트 디바이스(1700A)인, 파일 소유자에게 다시 송신된다. 결과적인 파일은 시간($t_2$)에서 구역(U9) 보안 자격 증명으로 업데이트된 인코딩된 데이터를 포함한다. 그러나, 원래의 파일을 생성하고 파싱하는데 이용된 구역(U1)에서의 클라이언트의 보안 자격 증명은 업데이트되지 않는다. 파일을 판독하기 위해서, 판독 동작은 시간($t_2$)에 상응하는 상태에서 구역(U9) 보안 자격 증명을 이용하여 파일을 먼저 디코딩하여야 하고, 이어서, 클라이언트 노드 $C_{1,1}$로의 전송 후에, 파일이 최초로 만들어졌던 시간과 연관된 구역(Z1) 보안 자격 증명을 이용하여 파일을 디코딩한다.

[0870] 향상된 보안을 위한 다른 규정으로서, 재분산 파일 동작이, 선택된 파일 저장 링크를 위한 모든 파싱된 파일을 새로운 또는 다른 파일 저장 서버로 이동시킨다. 그러한 동작은 파싱된 파일을 완전히 새로운 서버로 송신할 수

있거나, 대안적으로 파일이 기존 저장 노드들 사이에서 재분산될 수 있다. 각각의 경우에, 보안 자격 증명이 업데이트되고, 새로운 파일 FS 링크이 발행되고 파일에 대한 액세스를 가지는 클라이언트 또는 클라이언트들로 송신된다. 이러한 동작은 예로서 도 101에서 도시되어 있고, 여기에서 구역(U7) 내의 파일 저장 SDNP 노드 $F_{7,1}$의 콘텐츠가, 파일이 생성되었던 시간($t_1$)에서의 상태인, 상태(920X)를 이용하여 SDNP 디코딩 동작(1751H)에 의해서 디코딩된다. 이어서, 파일은 SDNP 네트워크(미도시)를 통해서 파일 저장 SDNP 노드 $F_{9,4}$로 전송되고, 여기에서 파일은 시간($t_2$)에 상응하는 상태(920Y)로서 구역(U9) 보안 자격 증명을 이용하여 SDNP 인코딩 동작(1750L)에 의해서 인코딩된다. 이어서, 파일이 저장되고, 업데이트된 FS 링크 2가 파일 액세스를 갖는 파일 소유자 및 다른 클라이언트에게 송신된다.

[0871] 전술한 파일 전달과 동시에, 구역(U9) 내의 파일 저장 SDNP 노드 $F_{9,4}$의 콘텐츠가, 파일이 생성되었던 시간($t_1$)에서의 상태인, 상태(920X)를 이용하여 SDNP 디코딩 동작(1751L)에 의해서 디코딩된다. 이어서, 파일은 SDNP 네트워크(미도시)를 통해서 파일 저장 SDNP 노드 $F_{9,1}$로 전송되고, 여기에서 파일은 시간($t_2$)에 상응하는 상태(920Y)로서 구역(U9) 보안 자격 증명을 이용하여 SDNP 인코딩 동작(1750M)에 의해서 인코딩된다. 이어서, 파일이 저장되고, 업데이트된 FS 링크 3가 파일 액세스를 갖는 파일 소유자 및 다른 클라이언트에게 송신된다. 유사한 방식으로, 구역(U9) 내의 파일 저장 SDNP 노드 $F_{9,1}$의 콘텐츠가, 파일이 생성되었던 시간($t_1$)에서의 상태인, 상태(920X)를 이용하여 SDNP 디코딩 동작(1751M)에 의해서 디코딩된다. 이어서, 파일은 SDNP 네트워크(미도시)를 통해서 파일 저장 SDNP 노드 $F_{7,1}$로 전송되고, 여기에서 파일은 시간($t_2$)에 상응하는 상태(920Y)로서 구역(U7) 보안 자격 증명을 이용하여 SDNP 인코딩 동작(1750H)에 의해서 인코딩된다. 이어서, 파일이 저장되고, 업데이트된 FS 링크 1가 파일 액세스를 갖는 파일 소유자 및 다른 클라이언트에게 송신된다. 이러한 방식으로, 3개의 파일 모두가 재배치되고 새로운 보안 자격 증명이 발행되며, 인증된 액세스를 가지는 클라이언트에는 업데이트된 FS 링크 1, 2, 및 3을 기초로 새로운 파일 저장 판독 링크가 발행된다.

[0872] 하이퍼보안 파일 저장 시스템에 의해서 실시되는 다른 필수적인 유지보수 기능은 임의의 라이브 링크를 갖지 않는 파일 즉, "좀비 파일"을 체크하기 위해서 이용되는 동작이다. 이러한 동작은, 클라이언트 또는 파일 소유자 대신 파일 저장 서버가 개시한다는 것을 제외하고, 리프레시 링크 동작과 유사하다. 동작 시에, 각각의 파일 저장 서버는, 파일이 마지막으로 액세스된 이후의 시간을 추적한다. 파일에서의 마지막 동작이 활동 없이 특정된 간격, 예를 들어 1달을 초과하는 경우에, 파일 저장 서버는 클라이언트 또는 클라이언트들에 접촉하여 링크가 여전히 활성적인지의 여부를 확인한다. 파일 저장 서버는 FS 링크를 클라이언트에 송신하기 위해서 이용된 것과 동일한 방법을 이용하여 클라이언트에 접촉할 수 있다. 파일이 저장되는 시간에, 파일 저장 서버는 클라이언트의 SDNP 집 또는 의사-어드레스를 보유한다.

[0873] 특정 간격 동안 활동이 없는 경우에, 파일 저장 서버는 링크가 활성적으로 유지된다는 것을 재확인하기 위한 요청으로 SDNP 시그널링 서버와 접촉한다. 이어서, SDNP 시그널링 서버는 파일 저장 서버에 참여하는 각각에 대한 FS 링크 입증 요청의 전달 경로를 계획한다. 이어서, 각각의 파일 저장 서버는 그 요청을 SDNP 네트워크를 통해서 클라이언트에 송신한다. 모든 참여 SDNP 클라이언트 노드는, 파일 링크가 디바이스 내에 여전히 존재한다는 확인으로 응답한다. 파일 링크가 확인되는 경우에, 해당 시간에서 클라이언트는 링크 리프레시를 실시하는 것에 대한 선택 사항을 갖는다. 그러나, 디바이스 응답이 없는 경우에, 즉 활성적 파일 판독 링크가 유지되지 않은 경우에, 파일 저장 서버는, 파일 링크가 중단되었거나 손실되었다는 것을 관리자에게 통지하고, 1 내지 3달과 같은 소정 간격 후에, 요구되지 않은 좀비 파일을 영구적으로 또는 회복 불가능하게 삭제한다.

[0874] ***등록된 통신*** - 본 발명에 따라 만들어진 SDNP 통신의 다른 특징은, "등록된 통신"을 전달 또는 저장할 수 있는 네트워크의 능력이다. 등록된 통신은, 법적 유효성을 구축하기 위해서 통신을 e-사인 및 e-촙(chop)할 수 있는 능력을 포함하여, 사인된 시간-스탬핑된 메시지로서의 코뮤니케의 하이퍼보안 전달 또는 파일의 하이퍼보안 저장을 포함한다. 등록된 통신은 또한, 사인된 또는 초핑된 시간-스탬핑된 응답을 이용하여 문서 또는 파일의 수령을 확인하는 "증명된 메시지" 핸드쉐이킹 방법(handshaking method)을 송신할 수 있는 능력을 포함한다. 모든 등록된 통신은, 클라이언트 디바이스 내의 SDNP 애플리케이션에 의해서 개시되지만, 라스트 마일 통신을 통해서 즉, SDNP 네트워크의 라스트 마일에 걸친 통신을 통해서 증명된다. 스탬프 확인을 무단으로 변경하고자 하는 클라이언트에 의한 임의의 시도는 메시지와 스탬프 확인의 네트워크 기록 즉 수령 통지서 사이의 불일치를 초래할 것이다.

[0875] SDNP 통신에서의 "상태"의 이용에 의해서, 즉 코뮤니케에서 그리고 파일 저장에서 메시지 특정 보안 자격 증명을 구축하기 위해서 시간 및 다른 특이적 변수들이 이용되는 경우에, 시간 스탬핑은 SDNP 통신의 고유

특징이다. 이러한 포인트가 도 102에 도시된 SDNP 통신기 애플리케이션 창(1800)에 예시되어 있고, 여기에서 송신되고 수신된 각각의 텍스트 메시지가, 메시지가 송신된 때, 메시지가 수신된 때, 그리고 메시지가 판독된 때를 나타내는 시간 스탬프(1801A 및 1801B)의 상응 세트를 갖는다. SDNP 시그널링 서버에 의해서 구축된 글로벌 시간 기준을 포함하는 시간 정보가 라스트 마일 네트워크를 통해서 클라이언트에 전달된다. 이어서, SDNP 클라이언트 앱은 시간 스탬프를 정보 디스플레이 내로 통합한다.

[0876] 등록된 통신에서, 코뮤니케는 프로세스의 일부로서 공식 스탬프를 생성한다. 등록된 통신 프로세스의 하나의 예가 도 103에 도시되어 있고, 여기에서 하이퍼보안 메시지가 실행되어 다이알로그 박스(1803)를 포함하는 선택적 파일 첨부 단계(1802)로 시작되고, 그러한 다이알로그 박스에서 메시지 또는 파일을 송신하는 클라이언트 즉, 송신자는 파일을 메시지에 첨부할 지의 여부를 선택하고 그렇게 하는 경우에 디렉토리 브라우저를 이용하여 파일을 찾는다. 명령 다이알로그(1804)를 다음에 이용하여, 정규의 또는 등록된 전달을 이용할 지의 여부를 선택한 다이알로그 박스(1805)에 따라 등록된 메시지를 송신한다. 이어서, 메시지는 본 발명에 따라 만들어진 하이퍼보안 통신을 이용하여 송신된다.

[0877] "메시지 수용된" 단계(1806)에서, 수신 당사자는, 메시지에 액세스하기 위해서 그리고 진입 메시지 및 파일의 수용을 확인하는 인증된 영수증을 송신하기 위해서 그들의 신원을 확인하는데 필요한 일련의 단계를 완료한다. 이러한 프로세스는 수령 인증 동작(1807)으로 시작하고, 여기에서 수신 클라이언트는 그들의 신원을 확인하도록 요청받는다. 그들의 신원 인증이 없는 경우에, 수령 당사자는 메시지에 액세스할 수 없을 것이고, 메시지는 파괴될 것이고 송신자는 인증 단계 실패를 통지받을 것이다. 이러한 방식으로, 송신자는, 수신 당사자가 도난된 그들의 디바이스를 가졌을 수 있을 가능성을 경고 받을 수 있다. 신원이 확인되면, 수신 당사자는, 그들이 진입 메시지 및 부착물을 수용하기 원하는지 또는 거부하는지의 여부와 관련하여, 수령 인증 동작(1808)에서 질문을 받는다. 메시지가 거부되는 경우에, 송신자는 통지받는다.

[0878] 수신 당사자가 '예'를 선택함으로써 메시지를 수용하는 경우에, 이들은, 전자 사인(e-사인)을 선택하는 것 및/또는 스탬프/촙(e-촙)을 선택하는 것에 의해서, 메시지를 수용하기 위해서 사인하기 위한 수령 관리 단계(1809)를 완료하여야 한다. 송신자는 요구되는 선택사항을 특정할 수 있다. 일부 국가에서, 법적 구속력을 위해서, 촙 및 사인 모두가 요구된다. 후속 다이알로그 박스(미도시)는, 사인 또는 촙을 디바이스의 파일 디렉토리 내에 위치시킬 것을 사용자에게 지시한다. 대안적으로, 오디오/비디오 기록이 확인으로서 이용될 수 있다. 수령자는 기록 중에 읽어야 하는 것에 관한 지시를 받는다. 메시지가 사인되면, 메시지가 수령자에게 보여질 수 있고, 첨부된 파일은 송신자의 요건에 따라 보여질 수 있거나 다운로드될 수 있다.

[0879] 문서를 수용할 때, 메시지 수신자를 식별하는 사인된 시간-스탬핑된 메시지 영수증(1811), 수신된 임베딩된 텍스트 및 부착된 파일명, 메시지가 수신된 일자 및 시간, 그리고 e-사인, e-촙 중 어느 하나, 오디오 기록, 오디오-비디오 기록, 또는 그 일부 조합을 포함하는 사인이 알림 동작(1810)에서 송신자에 송신된다. 보관 영수증 선택사항(1812)에서, 송신자는 사인된 시간 스탬핑된 메시지 영수증(1811)의 복사본을, 송신자가 메시지를 리콜하는데 필요한 파일 판독 링크(1813)을 수신하는 시스템의 하이퍼보안 파일 저장 시스템에 저장할 수 있는 기회를 갖는다. 대안적으로, 메시지 영수증(1811)은 송신자의 디바이스 내로의 다운로드를 위해서 이용될 수 있다.

[0880] ***암호화 기반의 보안 관련 문제*** - 정부 안보 기관은, 현대 상회의 기업 범죄, IP 절도, 사이버 범죄, 해킹, 범죄 조직, 마약 카르텔, 마피아, 야쿠자, 지하디스트, 및 테러리스트에서, 통화자에게 추적할 수 없는 익명 통신 즉, 데이터 보안 및 통화자의 신원 은폐를 위해서 암호화를 이용하는 시스템을 제공하는 임의의 통신 시스템(은유적으로, 페이폰)이, 네트워크 운영자, 애플리케이션 개발자, 및 디바이스 제조자에게 무분별하고 무책임한 비지니스 실무를 제공한다고 주장하고 있다.

[0881] 불행하게도, 보안을 달성하기 위해서 암호화에 의존하는 통신은 범죄자 및 법-준수 시민을 유사하게 보호한다는 것이 사실이다. 전술한 바와 같이, 본 대상은, 텔레그램이라고 지칭되는 전화 애플리케이션 프로그램을 이용한, ISIS 테러리스트의 범죄 활동 및 그들의 파리 및 벨기에에서의 공격에 관한 많은 새로운 이야기에 초점을 맞췄다. 이러한 앱은, 단부-사용자 기반의 암호화로도 알려져 있는, 엔드-투-엔드 암호화를 이용하는 보안 통신을 돕는다. 해독 키가 2명의 통신 당자사들에 의해서만 유지되고 개입 네트워크 또는 그 운영자에 의해서는 유지되지 않기 때문에, 엔드-투-엔드 암호화는 보안 당국에게 특히 문제가 된다. 텔레그램에 대처하는 보안 당국은, 큰-키 엔드-투-엔드 암호화가, 테러리스트들이 개방된 통신을 이용하여 비밀리에 활동할 수 있게 하는 국가적 그리고 심지어 국제적 보안 위험을 제공한다고 주장한다. 텔레그램에 우호적인 주장은 무엇보다도 개인 프라이버시를 지지한다.

[0882] 연방 판사가, FBI에 유리하게, 총격자가 소유한 것으로 주장된 잠금된 전화기를 "여는 것"을 보조하도록 Apple

에 명령하였을 때, 14명을 살해하고 22명을 부상입힌 2015년 12월 2일자 캘리포니아 샌 버너디노의 총격 사건과 관련한 프라이버시 논쟁이 다시 발생하였다. 2016년 2월 17일에, 워싱턴 포스트 기사의 제목은 "Apple은 샌버너디노 공격과 연계된 iPhone 크랙에 대한 FBI의 요구를 거부하기로 단언하였다"였다. Apple 및 그 CEO는 법원 명령을 따르지 않은 것에 대한 몇 가지 이유를 언급하였다. 기사는 온라인 상에서 확인될 수 있다 (https://www.washingtonpost.com/ world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-l le5-9823-02b905009f99_story.html). 가장 주목할 것으로, Apple은, Apple이 해독 키를 가지지 않는 방식으로 엔지니어링되었기 때문에, 공무원이 영장을 가지고 있을 때에도, 법 집행을 위해서 새로운 iPhone을 언록킹할 수 없다고 확고부동하게 주장하였다 - 본질적으로 엔드-투-엔드 암호화의 해결과제의 또 다른 예에 관한 공포가 일어나고 있다. Apple은, 전화기의 사용자 - 또는 암호를 알고 있는 누군가 - 만이 전화기를 언록킹할 수 있다고 주장하였다. 정부는, 암호화 피쳐를 언록킹할 필요가 없고, 단지 10번의 성공하지 못한 로그인 시도 후에 전화기의 메모리를 지워버리는 특징을 디스에이블링시키는 것만이 필요하다고 주장하였다. 온라인 진술에서, Apple의 CEO인 Tim Cook은 그러한 단계가 iPhone 보안을 위험하게 약화시킬 수 있다고 반박하였다. 그는 다음과 같이 말하였다: "일단 생성되면", "그러한 기술은 임의의 수의 디바이스에서 다시 계속 사용될 수 있다. 물리적 세계에서, 이는 - 음식점 및 은행으로부터 점포 및 가정까지 - 수억개의 록을 개방할 수 있는 마스터 키와 동일할 것이다. 합리적인 사람은 그러한 것을 용인할 수 없을 것이다." 그는 계속하여, "이러한 명령에 반대하는 것은 결코 경솔한 것이 아니다. 우리는, 도를 넘어선 미국 정부의 요청에 대해 목소리를 높여야 한다고 생각합니다."

[0883] 미국 사법부가 그 권한을 넘어섰다는 Apple의 마지막 포인트는 기술적 위치가 아니라 법률적 논쟁이고, 헌법론자들과 개인정보 보호자들의 감정을 반영하는 사람들은, 확실한 이유가 없이 정부가 통신을 모니터링할 수 있는 또는 개인의 프라이버시를 침범할 수 있는 법률적 권한을 가지지 않는다는 것을 주장한다. 특히 샌 버너디노의 경우에 확실한 이유의 기준을 명확하게 충족시키지만, 논쟁되고 있는, 모든 통신 디바이스를 열 수 있는 범용 백도어를 생성한다는 생각은 당국에 의한 권한 남용을 초래한다. 그들의 2016년 2월 23일자 기사에서, The Atlantic 지는 "Apple이 옳고: FBI는 많은 전화기의 침투를 원한다"로 동의하였다. 같은 날, Guardian은 "FBI가 수십대의 iPhone에 액세스하고자 한다고, Apple이 주장한다"고 보고하였다.

[0884] 이상하게, 미국 의회도 동일한 프라이버시-관련 포지션을 취하였다. "의회는, FBI가 iPhone을 언록킹하도록 애플을 압박하는 것은 '헛고생이다'라고 발표하였다"라는 제목의 Guardian의 3월 1일자 후속 기사에서, 미국 입법자들은 미국 사법부에서 프라이버시를 침해 및 침범하고 있다고 비난하였다. Microsoft의 법률 자문인 Brad Smith는 샌프란시스코의 RSA 컨퍼런스에서, "지옥으로의 통로는 백도어에서 시작한다"고 말하였다. Smith는 "이러한 중요한 사건에서 Apple을 지지하기 위한" 집회에서 제시된 컴퓨터 보안 산업에 이의를 제기하였다.

[0885] 그러한 불길 속에서, NSA 내부 고발자인 Edward Snowden을 포함하는 많은 보안 전문가는, 전화기의 언록킹은 FBI가 주장하는 것만큼 어렵지 않다는 견지를 공표하였다. Great Democracy 컨퍼런스를 위한 Moscow로부터 Common Cause Blueprint로의 비디오 링크를 통한 토론(3월 8 및 9일)에서, Snowden은 다음과 같이 말했다: "FBI가 말하길, Apple은 전화기를 언록킹하기 위한 '독점적 기술적 수단'을 갖고 있다. 점잖게 말해도, 이는 헛소리이다." 사건이 법정에 오기 전에, FBI는, 록킹된 iPhone을 뚫을 수 있는 방법을 이미 발견하였다고 보고하였다. 2016년 3월 29일에, Fortune Magazine 기사는, "FBI는 iPhone를 어떻게 뚫었는지를 Apple에 말하지 않았다'라고 보고하였다.

[0886] Apple-FBI 사건의 법률적 및 지정학적인 결과는 큰 영향을 가져왔다. FBI의 선례에 따라, 다른 국가들은 - 세계를 여행하는 미국 시민이 운반하는 전화기를 포함하여 - 그들의 네트워크에 연결된 모든 통신 디바이스에 대한 백도어를 주장할 것으로 예상된다. 또한, 이제, iPhone이 성공적으로 해킹되었고, 범죄자는 새로운 형태의 사이버범죄 및 신원 절도를 저지르기 위한 이러한 방법을 언젠가는 발견하거나 재-발명할 것이다. 범죄자에게 당하지 않기 위해서, 정부는 감시 및 스파이 활동을 확장하기 위해서 동일한 방법을 이용하려고 할 수 있고, 심지어 같은 정부 내의 여러 부서들이 이러한 방법을 이용하여 서로의 활동에 대해서 스파이 활동을 할 수 있다. 관련 이야기로서, 여러 정부들이 엔드-투-엔드 통신에서 이용되는 암호화의 레벨을 제한하는 것을 고려한다.

[0887] 집합적으로, 이러한 이벤트는, 공공 도메인에서 현재 이용 가능한 기존 보안 방법들의 뻔한 조합은, 적어도 범죄자 및 테러리스트를 돕지 않고서는, 보안 및 프라이버시 모두를 보장하지 않는다는 깨달음을 분명하게 뒷받침한다. 문제는, 네트워크 보안 및 엔드-투-엔드 보안 모두 그리고 그 연관 통화자 프라이버시를 달성하기 위해서 암호화에만 의존하는 것으로부터 기원한다. 암호화 키의 비트 크기를 증가시키는 것에 의해서 텍스트, 보이스, 또는 파일의 보안을 높이는 것은 임의의 코뮤니케가 더 안전하고 크랙하기 더 어렵게 한다. 향상된 보안은, 보안 및 프라이버시 유지에 있어서, 그리고 신원 절도에 대한 대항에 있어서, 비지니스 및 법-준수 시민을 보호한

다. 불행하게도, 동일한 향상된 보안은, 차별 없이, 범죄자 및 테러리스트를 검출로부터 보호하여, 이들이 벌을 받지 않고 그리고 노출되지 않고 활동할 수 있게 한다.

[0888] 이러한 포인트가 도 104a에 도시되어 있고, 여기에서 통화자(1825A)는, 많은 사이버-공격을 받는 인터넷(1821), 즉 큰 취약성의 "공격 표면"을 갖는 네트워크와 같은 미보안 네트워크를 통해서, 피통화자(1825Q)에 통신한다. 공격 표면을 줄이기 위해서, 암호화(1026) 및 해독(1032)을 이용하여, 네트워크(1821)보다 작은 공격 표면을 갖는 암호화된 파이프 또는 터널(1820)을 형성한다. 문제는, 얼마나 큰 암호화 키를 이용하여야 하는지를 결정하는 것이다. 표(1824)에 도시된 바와 같이, 암호화 키가 클수록, 더 많은 조합이 존재하고 암호를 크랙하기가 더 어렵다. 암호화는 2가지 목적 즉, (i) 중간자 공격을 방지하기 위한 네트워크 보안을 제공하기 위한, 그리고 (ii) 엔드-투-엔드 보안을 통해서 통화자 프라이버시를 보장하기 위한 목적을 위해서 사용된다. 라인(1823)에 의해서 도시된 바와 같이, 임의의 네트워크 보안의 개선은 동등한 엔드-투-엔드 보안의 개선을 초래한다. 높은 네트워크 보안이 악의적 외부 공격을 방지하는데 있어서 유리하지만, 과다한 엔드-투-엔드 암호화는 양날의 검이다. 큰 키 크기, 예를 들어 AES256 또는 AES512가 이용되는 경우에, 시스템은 "최고 비밀" 네트워크 성능을 전달하고, 당연히 통화자를 위해서 동일한 등급의 보안을 제공한다. 그러나, 통화자가 의심되는 범죄자 또는 테러리스트인 경우에, 네트워크 운영자 또는 정부는 통화자의 활동을 검출 또는 모니터링할 수 없다.

[0889] 키 크기 상충성은 복잡하다. 암호화 키가 너무 작은 경우에, 범죄자는 네트워크 및 그 사용자를 표적으로서 공격할 수 있다. 암호화 키가 너무 크다면, 범죄자는 그들의 불법적 활동을 감추기 위해서 그리고 진행되는 사기와 부정행위를 검출하기 위한 조사자의 노력을 무력화시키기 위해서, 네트워크를 이용할 수 있다. 회사 환경에서, 회사의 보안 정책은 엔드-투-엔드 암호화 전체를 거부할 수 있는데, 이는 그러한 것이 피고용인의 활동을 모니터링하는 것 또는 회사 조사 및 IP 소송을 따르는 것을 방지하기 때문이다.

[0890] 심지어 어떠한 크기의 키가 파괴 가능하고 보안이 어떠한지를 결정하는 것도 어렵고, 기술의 발전에 따라 달라진다. 다시 표(1824)를 참조하면, 무차별 대입 공격에서 분석되어야 하는 가능한 조합의 수는 암호의 키 크기의 기능에 따라 계산된다. 16-비트 키는 65k개의 조합만을 가지는데 반해서, 56-비트 키는 $10^{16}$개의 조합을 가지고, 128-비트 키는 $10^{38}$개 초과의 조합을 갖는다. 256-비트 키는 128-비트 키보다 39 자릿수가 더 큰 조합을 갖는다. 패턴 인식의 이용을 무시하면, 무차별 대입 공격은 코드를 해킹하기 위해서 모든 조합을 시도한다. EETimes의 "무차별 대입 공격에 대해서 AES를 어떻게 보안하는가?"라는 제목의 기사(http://www.eetimes.com/document.asp?doc_id=1279619)에서, 저자는, 무차별 대입 공격을 실시하기 위해서 10.5 페타플롭이 가능한 약 2012 슈퍼컴퓨터에서 필요로 하는 시간을 추정하였다. 페타플롭은 초당 천조 또는 $10^{15}$의 플로팅 포인트 동작, 또는 천 테라플롭이다. 따라서, 56-비트 키는 399 초만을 필요로 하고, 128-비트 키는 $1.02 \times 10^{18}$ 년을 필요로 하며, 192-비트 키는 $1.872 \times 10^{37}$ 년을 필요로 하고, 256-비트 키는 $3.31 \times 10^{56}$ 년을 필요로 한다.

[0891] 무차별 대입 공격을 극복하는데 필요한 시간 또한 변화된다. 기사가 작성된 이후에, 세계의 가장 빠른 컴퓨터는 이미 속도가 3배가 되었다. "수퍼 컴퓨터: 오바마가 세계에서 가장 빠른 컴퓨터를 주문하였다"라는 제목의 2015년 7월 30일자 BBC 뉴스 기사에서 보고된 바에 따르면, 조사자는, 차세대 수퍼 컴퓨터의 목표 속력이 기록 보유 컴퓨터보다 20배 더 빠르다는 것, 즉 초당 엑소플롭, 또는 백만-백만 플로팅 포인트 동작이 가능한 기계라는 것을 보고하였다. 이는, 암호를 크랙하는데 필요한 시간이 매년 계속적으로 짧아진다는 것을 의미한다. 암호를 크랙킹하기 위한 다른 새로운 접근방식은, 비트코인 채굴과 동일한 방법인, 대량 병렬 프로세싱을 이용하는 것이다. 하나의 수퍼 컴퓨터를 가지는 대신, 수천개 또는 백만개의 병렬 컴퓨터를 이용하는 것은, 비례적으로 시간을 줄이면서 동시에 공격을 진행할 수 있게 한다. 오늘날의 가장 빠른 마이크로프로세서는 이미 1.1 테라플롭을 돌파하였고, 그에 따라 함께 동작되는 3천개의 최상급 마이크로프로세서는 오늘날 세계에서 가장 빠른 컴퓨터와 동일하다. 백만개의 마이크로프로세서만이 엑소플롭 컴퓨터의 실현을 위해서 요구된다. 전용 ASIC가 보안을 더 붕괴할 수 있는 한편, 양자 연산은 많은 자릿수만큼 연산 능력을 변화시킬 것이다.

[0892] 결과적으로, 큰 키 엔드-투-엔드 암호화는 통신에서 프라이버시 및 보안을 달성하기 위한 좋은 해결책이 아니다. 본원에서 개시된 바와 같은 SDNP 네트워크 및 하이퍼보안 라스트 마일 통신에 의해서 가능해진 대안적인 접근방식은 엔드-투-엔드 암호화를 네트워크 보안으로부터 분리한다. 도 104b에 도시된 바와 같이, 각각 통화자 및 피통화자를 나타내는 SDNP 클라이언트(1700A 및 1700Q) 사이의 통신은 SDNP 네트워크(1831)에 의해서 실행된다. 네트워크의 작은 공격 표면은, 제어를 위해서 삼중-채널 통신을 이용하여 라우팅된, 동적 스크램블링, 단편화, 정크 삽입, 및 홉-바이-홉 암호화를 이용하는 익명성 다중-경로 및 메시형 데이터 전송에 의해서 실현된다. 비록 라스트 마일 통신 및 SDNP 클라우드 내의 모든 홉이 동적으로 변화되는 보안 자격 증명

을 포함하지만, 프로세스는, SDNP 인코딩 동작(1832) 및 SDNP 디코딩 동작(1833)에 의해서 단순화된 형태로 제공된다.

[0893] 표(1834)에 의해서 설명되고 라인 세그먼트(1830)에 의해서 도시된 바와 같이, 이러한 방법은, 여러 조합에서, 암호화에만 의존하지 않고, 비밀 또는 최고 비밀 암호화 표준과 동등한 보안을 달성한다. 라인 세그먼트(1830)이 편평(flat)하기 때문에, 이는 y-축에 도시된 엔드-투-엔드 암호화와 x-축에 도시된 네트워크 보안 사이에 상호 의존성이 없다는 것을 의미한다. 그 대신 네트워크 보안 레벨은, 다양한 SDNP 보안 방법의 적용에 의해서, 케이스 A로부터 케이스 D까지 조정될 수 있다. 이러한 보안 동작은, 통화자 및 피통화자가, SDNP 네트워크(1831) 및 그 여러 보안 구역을 통해서 데이터 패킷을 전송하기 위해서 이용되는 보안 자격 증명을 알지 못하는 방식으로, SDNP 소프트웨어에 의해서 실시된다. 특히, 대화하는 클라이언트들은 임의의 암호화 라스트 마일 네트워크의 키 교환에 알고(knowingly) 참여하지 않는다. 분산형 네트워크로서, SDNP 클라우드 내의 암호화의 이용은 라스트 마일 보안에 관련되지 않고, 그러한 시스템을 위한 마스터키는 존재하지 않는다. 따라서, SDNP 네트워크(1831) 보안은, 암호화된 파이프 또는 터널(1820)을 생성하기 위해서 암호화(1026) 및 해독(1032)에 의해서 실시되는 엔드-투-엔드 암호화에 의존하지 않는다.

[0894] SDNP 네트워크(1831)에 의해서 이용되는 암호화는 엔드-투-엔드 암호화된 터널(1820)과 동일한 크기의 키를 이용할 필요가 없다. 그래프에 도시된 바와 같이, 엔드-투-엔드 암호화의 상업적 및 회사 보안 애플리케이션은, SDNP 클라우드 내의 단일-홉 동적 암호화가 AES256를 이용하는 경우에도, 점선(1835)에 의해서 도시된 (AES128와 같은) 128b 키 암호화를 이용할 수 있다. 사실상, 엔드-투-엔드 암호화는, 네트워크 보안을 손상시키지 않고, RSA 또는 다른 암호를 이용할 수 있다. SDNP 네트워크(1831)는, 엔드-투-엔드 암호화 터널(1820)이 아닌 경우에도, FIPS 140-2 군사 등급 보안을 따르는 AES 암호화에 의해서 여전히 보호된다. 설명된 바와 같이, SDNP 네트워크(1831)는 모든 외부 사이버-공격 및 중간자 공격에 대해서 보호한다. 엔드-투-엔드 암호화된 터널(1820)은 통화자를 네트워크 운영자의 개입 및 다른 "내부" 해커 작업으로부터 보호한다. 이와 관련하여, 이러한 개시 내용에서 엔드-투-엔드 암호화는, 데이터 패킷 전송 보안을 달성하기 위해서가 아니라, 주로 통화자 프라이버시를 보장하기 위해서 이용된다.

[0895] 네트워크의 보안을 위험하게 하지 않으면서 엔드-투-엔드 암호화의 강도를 증가 또는 감소시킬 수 있거나 심지어 제거할 수 있기 때문에, 그러한 방법은 넓은 범위의 적용예를 위해서 구성될 수 있다. 예를 들어, 점선(1835)에 의해서 도시된 128b 키 암호화가 작은 회사나 개인적 용도에서 너무 엄격한 경우에, 개인의 프라이버시를 포기하지 않으면서 비트의 수를 감소시킬 수 있다. 군사용 또는 정부 적용예에서, 암호화 키 길이는 필요에 따라 192b, 256b 또는 심지어 512b까지 증가될 수 있다. 이와 관련하여, 개시된 SDNP 시스템은 오늘날 암호화 기반의 통화에서의 부족함을 극복하여, 임의의 대안적인 애플리케이션, 디바이스, 또는 네트워크에 의해서 이용될 수 없는 특징을 제공한다.

[0896] ***보안 관리*** - SDNP 통신의 다른 키 특징은 보안 관리에 대한 특이적 접근방식이다. 보안 관리는 이하를 포함하는 수많은 상황에서 요구된다:

[0897] * HR 정책 또는 피고용인 조사에 따라 실시되는 피고용인 통신의 모니터링,

[0898] * 회계 감사, 법회계학, 또는 회계 보고 지원에서의 피고용인 통신의 모니터링 및 기록,

[0899] * 합병 및 인수 거래의 일부로서의 회사간 통신의 문서화,

[0900] * IP 또는 회사 소송의 일부로서의 회사간 통신의 문서화,

[0901] * 소환장 및 형사 조사에 따른 코뮤니케 및 문서의 요구를 따르는 것,

[0902] * 계정 정보, 통화, 메시지 모니터링에 대한 법적 명령, 그리고 국가 안보와 관련된 파일 액세스를 따르는 것.

[0903] 적절한 인증으로, SDNP 네트워크 관리자는, 통신 모니터링 및 데이터 감시를 위해서 지정된 "SDNP 보안 에이전트"에 대한 SDNP 네트워크 트래픽의 액세스를 촉진할 수 있다. SDNP 보안 에이전트를 구축하고 인에이블링시키는 프로세스는, 모니터링 활동에 앞서 필수적으로 실시되는 다중-계층 승인 및 인증 프로세스를 포함한다. 남용을 방지하기 위해서, 어떠한 개인도, 심지어 SDNP 네트워크 관리자도 독립적으로 모니터링을 시작할 수 없다. 마스터 네트워크 키를 가지지 않고, DMZ 서버 내에서 오프라인으로 동작하는 구역-특정 보안 자격 증명을 이용하여 실행되는 동적 SDNP 인코딩 및 디코딩을 이용하는, 중앙 제어를 가지지 않는 분산형 네트워크로서의 SDNP 통신의 동적 특성으로 인해서, 사후에 데이터를 복원하거나 대화를 리콜하는 메커니즘은 존재하지 않는다. 데이터는, 전형적으로 100 밀리초 미만인, 짧은 지속시간 동안만 SDNP 네트워크 내에 머무른다. 분산형 시스템으로

서, SDNP 네트워크가 본질적으로 중앙 제어를 가지지 않도록 설계되고, 그러한 중앙 제어가 없이는 심지어 이전 통화의 메타데이터도 이용할 수 없다. 따라서, SDNP 네트워크는 선험적 보안 모니터링만을 지원하고, 이는, 지정된 SDNP 보안 에이전트에 의한 모니터링이 코뮤니케를 가로채기 전에 구축되어야 한다는 것을 의미한다.

[0904] 또한, SDNP 클라우드 내의 단편화된 메시형 통신의 동적 특성으로 인해서, 클라우드 내의 SDNP 노드는 완전한 대화의 데이터 패킷을 운반하지 않고, 즉 SDNP 게이트웨이를 넘어서 운반하지 않는다. 대부분의 노드는 데이터의 5% 이하를 그리고 전형적으로 라우팅 변화전의 시간에 10 ms동안만 운반한다. SDNP 통신에 따라, 동적 라우팅은 상이한 미디어 서버를 통해서 통신을 계속적으로 재지향시킨다. 따라서, 클라우드 액세스는 코뮤니케의 복원 또는 모니터링을 위해서 유효하지 않다. SDNP 클라우드의 데이터 패킷이 캡쳐될 수는 있지만, 이들은, 관련 없는 소리, 데이터, 대화, 및 정크 데이터의 쓸모 없는 혼합을 포함한다. 그 대신, 지정 SDNP 보안 에이전트에 의한 모니터링은 라스트 마일 내에서만 생산적으로 발생될 수 있고, 여기에서, 관련된 데이터 패킷의 완전한 세트는 필수적으로 클라이언트 디바이스 내에서 또는 바람직하게 SDNP 게이트웨이 내에서 횡단한다.

[0905] 보안 모니터링에서의 데이터 패킷 라우팅의 예가 도 105a에 개략적으로 도시되어 있고, 여기에서 SDNP 보안 에이전트(1840)는 SDNP 클라이언트 디바이스(1600A)와 SDNP 클라이언트 디바이스(1600H) 사이의 대화를 모니터링한다. SDNP 클라이언트 디바이스(1600A)로부터 라스트 마일 라우터(1602G)를 통해서 SDNP 게이트웨이(1701U)까지 그리고 SDNP 클라우드를 통해서 송신된 데이터 패킷을 이용하여 대화가 이루어지는 한편, 클라이언트 디바이스(1600A)로부터 송신된 데이터 패킷은 SDNP 게이트웨이(1700U)에 의해서 폐쇄되고 지정 SDNP 보안 에이전트(1840)으로 안전하게 라우팅된다. 구체적으로, UDP 전송 중에, 라스트 마일 데이터 패킷(1630A)은 SDNP 데이터 1을 어드레스 "IP $C_{1,1}$"에서의 SDNP 클라이언트로부터 어드레스 "IP $M_{0,0}$"에서의 SDNP 게이트웨이까지 운반되어, 어드레스 "IP $M_{0,4}$"에서의 SDNP 게이트웨이로부터 나오고 U7 라스트 마일을 통해서 SDNP 클라이언트 어드레스 "IP $C_{7,1}$"로 전달된다. 인증된 모니터링 중에, 복제된 SDNP 데이터 1이 SDNP 어드레스 "IP SA"에서 SDNP 보안 에이전트(1840)에 안전하게 전달된다. 복제된 모니터링 데이터 패킷(1841)은, 중복되는 데이터 복제물들을 통화자들이 볼 수 있다는 것을 제외하고, SDNP 그룹-통화와 동일한 방식으로 동작한다. 그에 따라, 통화자는 그들이 모니터링되고 있다는 것을 알지 못한다.

[0906] 보안 모니터링은 수신 통화에서도 작용한다. 도 105b에서, SDNP 데이터 7이 어드레스 "IP $C_{7,1}$"를 갖는 클라이언트 디바이스(1600H)으로부터 어드레스 "IP $M_{0,4}$"에서의 SDNP 게이트웨이까지 송신된다. SDNP 클라우드 전송 후에, 데이터는 어드레스 "IP $M_{0,0}$"에서의 SDNP 게이트웨이로부터 2개의 목적지로 전달된다. 어드레스 "IP $C_{1,1}$"에서의 클라이언트(1600A)인, 제1 목적지는 SDNP 데이터 7을 포함하는 응답 데이터 패킷(1640A)을 수신한다. SDNP 보안 에이전트(1840)인 제2 목적지는, 데이터 패킷(1842)을 통해서, 복제된 데이터 "SDNP 데이터 7"을 포함하는 동일한 페이로드를 수신한다. 데이터 패킷(1842)의 전달은 통화자들에게 보일 수 없고, 그에 따라 그들은 그들이 모니터링된다는 것을 알지 못한다.

[0907] 동일한 방법이 단편화된 분산형 파일 저장의 모니터링에 적용될 수 있다. 그러나, 단편화 데이터 파일을 캡쳐하는 대신, 보안 에이전트는 관련된 FS 링크의 복사본을 수신하기만 하면된다. 그러한 예가 도 106에 도시되어 있고, 여기에서 SDNP 파일 저장 디바이스(1700H)는 FS 링크 1을 포함하는 데이터 패킷(1740H)을 어드레스 "IP $F_{1,1}$"로부터 게이트웨이 어드레스 "IP $M_{0,4}$"로 송신하고, 이는 SDNP 클라우드를 통해서 라우팅된 후에 데이터 패킷(1740A)에 의해서 클라이언트(1600A)에 포워딩된다. 복제된 페이로드 "FS 링크 1"은 또한, 게이트웨이 어드레스 "IP $M_{0,0}$"으로부터 송신된 데이터 패킷(1843)에 의해서 어드레스 "IP SA"에서의 SDNP 보안 에이전트(1840)에 전달된다. 실시간 통신의 경우에서와 같이, 클라이언트(1600A)인 파일 소유자는 SDNP 보안 에이전트에 의해서 모니터링된다는 것을 알지 못한다.

[0908] 동일한 모니터링 메커니즘이 다중-경로 라스트 마일 통신을 위해서 작용하고, 여기에서 데이터 패킷은 하나 초과의 SDNP 게이트웨이를 통해서 SDNP 클라우드에 진입 및 진출한다. 이러한 경우가 도 107에 도시되어 있고, 여기에서 클라이언트 디바이스(1600A)로부터의 라스트 마일 통신은 페이로드 SDNP 데이터 1을 포함하는 분할 데이터 패킷(1630A), 및 SDNP 게이트웨이(1701U 및 1701V) 각각을 통해서 클라우드에 진입하는 페이로드 SDNP 데이터 2를 운반하는 데이터 패킷(1630B)을 포함한다. SDNP 클라우드 라우팅 후에, 데이터 패킷들이 재조합되고, 조합된 데이터 SDNP 데이터 3을 포함하는 페이로드를 갖는 단일 데이터 패킷(1630L)으로서 클라우드로부터 나오는 것으로 도시되어 있다. 동작 시에, 클라이언트 노드 $C_{1,1}$으로부터의 진입 SDNP 데이터 1 및 SDNP 데이터 2의 복제물을 생성하도록 그리고 이들을 어드레스 "IP SA"에서 SDNP 보안 에이전트(1840)으로 지향시키도록, 시그널링

서버가 어드레스 "IP $M_{0,0}$" 및 "IP $M_{0,11}$"을 갖는 SDNP 게이트웨이에 지시한다. 복제된 데이터는, 보안 에이전트가 그 자체의 특이적 보안 구역 내에서, 즉 임의의 다른 디바이스에서 이용될 수 없는 자격 증명을 이용하는 구역(SA) 내에서 동작된다는 것을 제외하고, 모든 SDNP 데이터 전송에 이용된 동일한 하이퍼보안 방법을 이용하여 데이터 패킷(1841A 및 1841B) 내에서 송신된다. 따라서, 지정된 보안 에이전트가 특정 대화를 모니터링한 기록이나 증거는 존재하지 않는다.

[0909] SDNP 모니터링 활동이 은밀하고 본질적으로 검출될 수 없는 비노출 컨퍼런스 콜과 동등하기 때문에, 네트워크 모니터링의 이용을 승인하고 확인하기 위해서 그리고 모니터링을 실행하도록 인증된 SDNP 보안 에이전트를 지정 및 확인하기 위해서, SDNP 시스템이 독립적인 체크를 이용하는 것이 중요하다. SDNP 보안 에이전트는, 네트워크 관리자를 제외하고, 임의의 SDNP 클라이언트일 수 있다. 시스템 부패에 대한 보호로서, 임의의 SDNP 네트워크 운영자 또는 SDNP 관리자는 SDNP 보안 에이전트로서 활동할 수 없고, 즉 네트워크를 관리하는 사람은, 심지어 그들이 위협 받거나 블랙메일을 받았을 때에도, 그 스스로를 위해서 그 능력을 파괴할 수 없다.

[0910] SDNP 보안 에이전트는 개인, 정부 기관, 정부 지정 대표자, 또는 법무관을 구성할 수 있다. 지정되는 보안 에이전트의 특별한 필수 자격은 적용 가능한 지역적 법률에 따라 회사 또는 나라에 의해서 달라진다. SDNP 보안 에이전트의 모니터링 하드웨어는 기록, 데이터 저장, 및 정교한 해독 능력을 갖는 통신 디바이스 및 컴퓨터 서버를 포함할 수 있다. SDNP 네트워크로부터 지정 SDNP 보안 에이전트로 송신된 모든 통신은 클라이언트의 코뮤니케 자체와 동일한 하이퍼보안 통신으로 전송되고, 그에 따라 보안 모니터링은, 인증된 보안 에이전트에 의해서 실시되는 모니터링을 제외하고, 통화의 비밀성 또는 통화자의 프라이버시를 손상시키지 않는다.

[0911] 또한, 인증된 SDNP 에이전트의 모니터링 및 허용된 능력의 구현은 어떠한 수단으로도 네트워크 무결성 및 보안을 손상시키지 않는다. 동작 세부사항 또는 DMZ 공유된 비밀이 네트워크 운영자에게 또는 임의의 보안 에이전트에게 노출되지 않고 - SDNP 시스템의 동작은, 인간 운영자의 개입이나 관여가 없이, 자동적으로 그리고 자율적으로 이루어지는 한편, DMZ 서버는 온라인 엑세스를 통해서 이용될 수 없는 구역 특정 자격 증명을 이용하여 보안을 제공한다. 그에 따라, 보안 모니터링은 시스템의 보안을 저하시키지 않고, 또는 SDNP 네트워크를 사이버 공격에 취약하게 만들지 않는다.

[0912] 데이터 페이로드는 통화자에 의해서 생성된 것과 동일한 형태로 SDNP 보안 에이전트에 전달된다. SDNP 보안 에이전트에 대한 전달의 일부로서, 전달되는 데이터 패킷 내에 네트워크 보안 규정이 존재하지 않도록, 모든 네트워크 SDNP 인코딩이 디코딩된다. 그러나, 클라이언트가 엔드-투-엔드 암호를 이용하는 경우에, 클라이언트가 엔드-투-엔드 해독 키를 네트워크와 미리 공유하기로 또는 SDNP 네트워크에 의해서 액세스될 수 있는 독립적인 키 서버 유틸리티를 이용하기로 합의하지 않은 경우에, SDNP 보안 에이전트는 클라이언트의 엔드-투-엔드 암호를 파괴하여야 할 것이다. 반복하면, 그러한 엔드-투-엔드 암호화 및 해독 키는 프라이버시 목적을 위해서 SDNP 방법에 일차로 포함되고, SDNP 동적 인코딩 기능에서 이용되는 모든 암호화에 관련되지 않는다.

[0913] 모니터링 남용 위험을 최소화하기 위해서, 클라이언트 또는 클라이언트의 그룹 모니터링을 위해, 지정된 SDNP 보안 에이전트를 구축하고 인증하기 위해서 이용되는 SDNP 관리가 다수 단계 프로세스이다. SDNP 시스템이 모니터링을 실시하기 위한 규정을 포함하지만, 이러한 특징의 합법적인 적용은 네트워크 운영자, 네트워크 관리자, 및 인증 에이전시 또는 에이전트의 책임이다. 이러한 당사자들은, 함께, 모니터링이 합법적으로 그리고 모니터링이 실시되는 국가의 법률에 따라 실시되도록 보장하는 것에 대해서 개인적으로 책임을 진다.

[0914] 모니터링 필요성은 임의의 수의 상황으로부터 발생될 수 있다. 회사에서, 성희롱과 관련된 내부 고발자 불만 또는 클레임이 HR 조사를 촉발할 수 있거나 법회계학을 초래할 수 있다. 소송 문제(잠재적으로 개그 오더(gag order)를 포함)와 연관된 법원 소환장이 또한 모니터링을 요구할 수 있다. 회사 문제에서, 회사 SDNP 네트워크를 이용하는 통신은 일반적으로 회사 코뮤니케로 제한되고, 프라이빗 및 개인적 통신을 커버하지 않는다. 대부분의 국가에서, 범죄 의도가 의심되지 않는 한, 프라이빗 통신은 보호된다. 국가 보안 또는 법 집행 행위의 경우에, 통화자의 공공 및 프라이빗 SDNP 계정 모두가 모니터링될 수 있다. 그러한 경우에, 회사를 위한 회사 SDNP 네트워크 운영자는 회사 통신에 대해서 모니터링 프로세스를 실시할 것인 반면, 독립적인 원격통신 SDNP 네트워크 운영자는 통화자의 프라이빗 통신의 모니터링을 실행하기 위한 위치에 있는 유일한 제공자일 것이다. 일부 국가에서, 정부는 프라이빗 시민의 모니터링을 시작하기 위해서 법원-승인 소환장을 제시하여야 하는 반면, 다른 국가에서 정부는 사실 기반으로 임의의 그리고 모든 프라이빗 통신을 모니터링할 수 있는 권한을 주장할 수 있다. 국제 통신의 경우에, 어떠한 법률이 적용될 수 있는지 그리고 통화 모니터링을 가능하게 하기 위한 네트워크의 위치가 어디에 있어야 하는지를 결정하는 것이 더 어렵다.

[0915] 모니터링을 가능하게 하기 위해서 이용되는 AAA 프로세스의 하나의 예가 도 108에 도시되어 있다. 클라이언트의

모니터링을 승인하기 위한 프로세스는, 바람직하게 자율적으로 그리고 네트워크 운영자 또는 네트워크 관리와 독립적으로 동작하는, 모니터링 동작을 설정하기 위해서 이용되는 네트워크 관리자(1850), 클라이언트 모니터링을 담당하는 보안 에이전트(1840), 및 모니터링 프로세스를 승인하기 위해서 이용되는 3개의 인증 에이전트(1851A 1851B, 및 1851C)를 포함한다. 프로세스는, 조사 또는 법원 명령에 응답하여 모니터 요청(1862)을 하고자 하는 네트워크 관리자(1850)로 시작된다. 명령 다이알로그 박스(1862)를 이용하여, 관리자는, 모니터링이 요청되는 개인의 전화 번호를 식별한다. 요청이 사람의 그룹을 모니터링하기 위한 것인 경우에, 이들은 모든 당사자를 나열한 파일의 시스템 내로 하나씩 입력될 수 있고, 그들의 연관된 전화번호가 시스템 내로 업로드될 수 있다.

[0916] 인증 단계(1863)에서, 네트워크 관리자(1850)는 예시적인 다이알로그 박스(1864)를 이용하여 모니터링 기능을 실시하기 위해서 권장된 후보 보안 에이전트(1840)를 식별한다. 회사의 경우에, 개인이 HR 감독관, 법률 자문, 감사 위원회의 구성원, 및 독립적인 회계 회사 대표, 또는 독립적인 조사관일 수 있다. 합법적인 경우에, 보안 에이전트는 법무관, 지방 검사, FBI 에이전트 또는, 예를 들어 정부 부정행위의 경우에, 특별 기소 위원회 조사 패널과 같은, 다른 정식 임명된 조사 위원회 구성원일 수 있다. 이어서, 시스템은, 보안 에이전트가 SDNP 계정을 가지고 있다는 것 그리고 이들이 회사 또는 네트워크 운영자에 의해서 특정된 규칙을 준수한다는 것을 보장하기 위해서 SDNP 명칭 서버(1714)로 체크한다. 국가 안보와 관련된 일부 경우에, 제안된 보안 에이전트 자격증명 및 범죄 기록에 대한 후속 조사가, 그 승인 전에, 실시될 수 있다.

[0917] 보안 에이전트가 승인되면, 인증 단계(1865)에서 모니터링을 위한 요청이 인증 에이전트(1851A, 1851B, 및 1851C)로 포워딩되고, 인증 에이전트는 대상에 관한 설명의 명칭, 모니터링을 실시하기 위한 과제를 갖는 보안 에이전트의 이름 또는 위치, 모니터링 조사의 예상 지속시간, 및 조사의 이유를 포함하는, 다이알로그 박스(1866) 내에 존재하는 정보를 리뷰한다. 각각의 인증 에이전트는 요청을 수락 또는 거부할 수 있다. 이어서, 네트워크 운영자 또는 회사의 규칙은, 모니터링 동작이 인증 에이전트의 만장일치 승인을 기초로 승인되는지 또는 단순히 과반으로 승인되는지를 결정한다. 인증 에이전트의 신원은, 회사의 경우에서와 같이, 알려질 수 있거나, 범죄의 경우에, 그들의 신원은 익명으로 유지되어 SDNP 네트워크의 익명의 통신 특징에 의해서 보호될 수 있다.

[0918] 모니터링이 승인되면, 관리 단계(1867)에서, 클라이언트의 데이터베이스(1868)가 명칭 서버(1714)에서 업데이트되어 모니터링되는 SDNP 클라이언트를 태그하고, 보안 에이전트로서 인증된 SDNP 클라이언트, 이러한 예에서 음영처리된 데이터의 행을 식별한다. 이러한 데이터베이스 내의 SDNP 어드레스는, 모니터링되는 클라이언트와 지정된 보안 에이전트 사이의 동일 관계를 유지하기 위해서, SDNP 어드레스들이 섞일 때, 매일 함께 업데이트된다. 조사 일자가 만료되면, 모니터링 링크가 자동적으로 분리된다. 관리 단계(1869)에서, SDNP 보안 에이전트(1840)가 링크에 송신되어, 이들이 모니터링되는 식별된 클라이언트의 모든 진행 통신을 수신할 수 있게 한다. 그들의 이러한 정보의 이용은 SDNP 네트워크 동작의 문제가 아니다. 보안 에이전트에 의한 개인의 프라이빗 정보에 관한 미인증 유출은, 보안 에이전트가 완전히 책임을 지는 범죄를 구성할 수 있다.

[0919] 이러한 본 발명의 모니터링 방법을 통해서, SDNP 네트워크는 그에 의해서 부정행위 및 잠재적인 테러리스트 활동에 관한 범죄 조사를 지원할 수 있는 한편, 법을 지키는 시민을 위한 보안 통신 미디어를 유지한다. SDNP 네트워크는, 죄가 없는 시민의 프라이버시를 위험하게 하지 않고 또는 SDNP 글로벌 통신 네트워크의 보안을 손상시키지 않고, 합법적 법원 명령에 따라 권한을 가진 자에게 프라이빗 클라이언트 통신을 안전하게 전달할 수 있다. 법원 명령 전달에서 백도어 또는 마스터 키가 이용되지 않았기 때문에, SDNP 네트워크에 걸친 추후의 통신은 익명으로 그리고 하이퍼보안으로 유지된다. 이러한 방식으로, 보안 동적 통신 네트워크 및 프로토콜 그리고 그 하이퍼보안 라스트 마일 통신은 임의의 다른 수단에 의해서 이용될 수 없는 보안 특징을 제공할 수 있고, OTT 및 실질적으로 모든 메신저 및 통신기 앱에 의해서 이용되는 엔드-투-엔드 암호화에 과다하게 의존하는 것에 의해서 발생되는 범죄 및 테러를 돕는 것을 완전히 방지할 수 있다.

[0920] ***SS7 취약성 극복*** - 만약 Apple-FBI 논쟁이 통신 및 보안 산업에서 큰 문제가 되지 않았다면, 60 Minutes 에피소드(http://www.cbsnews.com/news/60-minutes-hacking-your-phone/)가, 통상적인 무선 전화통신을 위한 신호 제어 채널인, 시그널링 시스템 7 또는 SS7의 심각한 보안 취약성을 폭로하였다. 그러한 쇼에서 명확히 드러난 바와 같이, SS7 취약성은 잠재적으로 모든 스마트폰 및 연결된 디바이스를 패킷 스니핑 및 사이버 공격에 노출시키고, 그에 따라 개인의 전화 번호를 단순히 아는 것에 의한, 무선 대화의 도청, 그리고 SMS 텍스트, 첨부된 파일, 및 사진의 관찰을 가능하게 한다.

[0921] 시그널링 시스템 7은 세계적인 모든 형태의 디지털 전화 통화에서 이용되는 1975년에 개발된 전화 통화 시그널링 프로토콜이다. 이는, 통화의 라우팅을 핸들링하기 위해서, PHY 계층 1, 데이터 링크 계층 2, 및 네트워크 계

층 3에서 동작되는 메시지 전달 부분 또는 "MTP" 동작을 포함한다. 엔드-투-엔드 라우팅은, 전송 계층 4에서 동작되는 시그널링 연결 제어 부분 또는 "SCCP" 동작을 이용하여 관리된다. 프로토콜은 또한 청구, 로밍, 및 통화 인증과 관련된 많은 수의 애플리케이션 계층 7 기능을 포함한다. SS7 프로토콜은, 불가피하게 필요함에도 불구하고, 공격에 극도로 취약하고 통상적인 전화통화의 보안에 상당한 위험을 제공한다.

[0922] 2016년 4월(https://en.wikipedia.org/wiki/Signalling_System_No._7)에, 미국 의회 감독위원회는 "이러한 취약성을 갖는 애플리케이션은, 개별 표적을 모니터링하는 범죄자부터, 미국 기업에 대한 경제적 스파이 활동을 하는 외국 기업체, 미국 정부 관리를 모니터링하는 국가에 이르기까지 제한이 없는 것으로 생각된다. ...취약성은 개인의 프라이버시뿐만 아니라 미국의 혁신, 경쟁력 및 국가 안보에도 심각한 영향을 미친다. 텍스트 메시지를 이용하는 다중 인증과 같은 - 디지털 보안에서의 많은 혁신이 쓸모 없게될 수 있다"고 보고하였다.

[0923] SS7 사이버 공격은 본질적으로, SS7 정보의 특정 포맷팅을 가이드로서 이용함으로써 콘텐츠 및 메타데이터 모두를 가로채는, 패킷 스니핑의 분류로부터 초래된다. SS7 프로토콜은 본질적으로, 패킷 정보를 해석할 수 있게 하는 정보 템플레이트(information template)를 제공한다. 도 109에 도시된 바와 같이, 문제는, 가입자 및 그들의 계정에 관한 다양한 유형의 개인 정보를 포함하는, SIM 카드 또는 "가입자 신원 모듈"로 시작된다. 도시된 바와 같이, 네트워크 제공자에 의해서 일반적으로 발행되는 캐리어 SIM 카드(1880)는, 상응 라디오 링크(28A, 28B, 및 28C)를 갖는 안테나(25A, 25B, 및 25C)에 의해서 도시된 셀룰러 네트워크에 대해서 전화기(32)를 식별하기 위해서 이용된다. 각각의 SIM 카드는, SIM 카드를 국제적으로 식별하기 위해서 이용되는 18개 또는 19개의 숫자를 갖는 ICCID 또는 "집적 회로 카드 ID"인, 특이적 식별자를 포함한다. 국제 모바일 가입자 신원 또는 IMSI는 개별적인 운영자 네트워크, 즉 SIM 카드가 작동하는 가정 네트워크를 식별한다. 로컬 네트워크 제공자는 IMSI 번호를 이용하여 SIM 카드와 통신하여 통화를 구축한다.

[0924] SIM 카드는 또한, SIM 카드가 발행된 국가를 식별하기 위한 3개-숫자인, "모바일 국가 코드" 또는 MCC를 포함한다. 국제 휴대폰 통화를 모바일 폰으로부터 위치시킬 때, MCC는 다이얼링 시퀀스의 일부로서 요구된다. MCC의 예는 미국을 위한 310 내지 316, 영국을 위한 234 내지 235, 중국을 위한 460, 프랑스를 위한 208, 러시아를 위한 250, 독일을 위한 262, 캐나다를 위한 302, 브라질을 위한 724를 포함한다. MCC는 "모바일 네트워크 코드" 또는 MNC와 함께 이용되어, SIM 카드를 발행한 네트워크 제공자를 식별한다. 코드의 전체 목록이 온라인 https://en.wikipedia.org/ wiki/Mobile_country_code에 나열되어 있다. SIM 카드는 또한 15개-숫자 "모바일 스테이션 국제 가입자 디렉토리 번호" 또는 MSISDN을 포함하여, SIM이 동작되는 네트워크의 유형 및 가입자를 특이적으로 규정한다. SFM 카드는 또한 사용자 전화 번호 및 SMS 텍스트 디렉토리를 유지하고, SMS 텍스트 디렉토리는 진입 및 진출 통화의 기록 및 시간 및 일자 정보와 함께 송신된 텍스트를 포함한다. 최근 몇년 간, 캐리어는, 모바일 지불을 촉진하기 위해서 신용 카드 자격 증명을 저장하기 위한 소위 보안 요소를 갖는 특별한 SIM 카드를 이용하기 시작하였다.

[0925] MCC, MNC 및 MSISDN 코드가 연결 프로세스의 일부로서 전송되기 때문에, 임의의 SIM 카드 및 가입자의 연관된 전화 번호의 본국 및 캐리어는 SS7 침입 및 패킷 스니핑에 의해서 용이하게 식별될 수 있다. 전송된 데이터(1881)는 전화 디렉토리, 온라인 정보, 또는 소셜 미디어를 통해서, 즉 프로파일링을 통해서 통화자의 신원을 추적하기 위해서 용이하게 이용될 수 있다. 식별되고 상호 관련되면, 전화 번호 및 SIM은, 가입자가 세계적으로 어디에서 이동하는지와 관계없이, 가입자의 활동을 모니터링하기 위해서 이용될 수 있다. 암호화는 기본 통화 정보 또는 메타데이터를 은폐하지 않는다. 엔드-투-엔드 암호에서도, 데이터 패킷은 동일한 대화로부터 오는 것으로 용이하게 식별될 수 있고, 캡쳐될 수 있고, 후속 해독 시도를 위해서 저장될 수 있다.

[0926] 메타데이터 및 콘텐츠 이외에, 통화자의 위치가 또한 SS7 취약성에 의해서 손상된다. 임의의 셀룰러 네트워크에서, 전화는 메시지를, 특정 통화에서 이용 가능한지를 식별하는 로컬 셀 타워에 송신한다. 이러한 등록 패킷은 규칙적인 간격으로 송신된다. 이러한 패킷을 모니터링하는 것은, 전화가 통화 중이 아닌 경우에도 그리고 GPS가 꺼져 있는 경우에도, 특정 SIM 카드를 갖는 전화의 위치가 위치결정될 수 있게 한다. 그러한 방식으로, 가입자의 위치 및 이동이, 그들을 모르고도, 축적될 수 있다.

[0927] SS7 고유의 취약성에도 불구하고, 보안 동적 통신 네트워크 및 프로토콜에 따라 만들어진 하이퍼보안 라스트 마일 통신은, 라스트 링크 내의 의미 있는 통화 데이터를 가림으로써, SS7 공격을 막는다. 특히, 하이퍼보안 라스트 마일 통신은, 이하를 포함하는, 통상적인 전화통화 또는 OTT 인터넷 통신보다 우수한 상당한 보안성을 제공한다:

[0928] * 하이퍼보안 라스트 마일 통신은, 당사자가 SDNP 클라이언트가 아닌 경우에도, 통화하는 또는 메시지를 받는 당사자의 전화 번호 또는 IP 어드레스를 노출시키지 않는다.

[0929] * 하이퍼보안 라스트 마일 통신은, 순차적 데이터 패킷이 동일 통화의 일부인지 또는 상이한 목적지들을 갖는 관련 없는 데이터 패킷을 나타내는지를 식별하지 않는다.

[0930] * 데이터 패킷의 통화 특정성을 은폐함으로써, 하이퍼보안 라스트 마일 통신은 통화 시간에 관한 메타데이터를 감춘다.

[0931] * 하이퍼보안 라스트 마일 통신은 페이로드를 동적으로 인코딩하여, 패킷 콘텐츠에 대한 미인증 액세스를 방지하고 보이스, 비디오, 및 텍스트 통신뿐만 아니라 사진, 파일 및 다른 콘텐츠의 프라이버시를 보호한다.

[0932] 따라서, 설명된 바와 같이, 개시된 보안 동적 통신 네트워크 및 프로토콜을 이용하는 통신 및 하이퍼보안 라스트 마일 통신은 SS7 취약성에 의해서 영향을 받지 않는다. SDNP 통신이 그 자체의 프로토콜을 이용하여 발생되고 인코딩된 페이로드에 의해서 운반되기 때문에, 2G, 3G, 및 4G/LTE 전화통화와 같은 개방된 미암호화 채널을 통해서 운반되는 패킷에서도, 통화 데이터 또는 콘텐츠가 SDNP 데이터 패킷으로부터 추출될 수 없다. 그에 따라, 패킷 스니핑은, SDNP 코딩 및 단편화된 데이터 전송에 대한 사이버-공격의 개시에 있어서 효과가 없다.

[0933] ***SDNP 은폐*** - 전술한 내용에서, SDNP 통신 상에서 가지는 유일한 영향의 SS7 취약성은 통화자의 위치 노출이다. 캐리어의 SIM 내의 전화 번호가 각각의 사용자의 신원과 연계되기 때문에,휴대폰이 켜질 때마다 이는, 전화 통화가 발생되지 않는 때에도, 가장 가까운 휴대폰 타워와 필수적으로 통신한다. 이어서, 이러한 셀 타워 정보를 이용하여 사용자의 위치를 삼각 측량할 수 있고, GPS가 꺼졌을 때에도, 가입자의 이동을 추적할 수 있다. 그러한 미인증 추적이 SS7에 의존하기 때문에, 통상적인 캐리어의 SIM 카드를 이용하는 디바이스는, 그러한 디바이스가 SDNP 클라이언트로서 동작하더라도, 위치 추적에 취약하다.

[0934] 단순화된 네트워크 개략도인 도 110에 도시된 바와 같이, 본원에서 "SDNP 은폐"라고 지칭되는 라스트 마일 하이퍼보안 통신의 향상은 가입자 추적을 전적으로 방지한다. 이러한 특징을 구현하기 위해서, 일반 캐리어 SIM 카드(1880)가 SDNP SIM 카드(1882)로 대체된다. SDNP SIM 카드는, 가입자가 아니라, SDNP 네트워크 운영자에게 등록되고, 그에 따라 개인적인 가입자 정보가 SDNP SIM 카드(1882)에 포함되지 않는다. SDNP SIM 카드(1882)는, 네트워크 액세스를 가지나 어떠한 개인 정보도 가지지 않는다는 점에서, 선불형 SIM 카드와 유사하다. 그 대신, 계정 보유자의 개인 정보 전부는 SDNP 네트워크 명칭 서버 내에 안전하게 포함되고, 해커가 액세스할 수 없거나 사이버-공격에 취약하지 않다.

[0935] 동작 시에, SDNP 은폐는, SDNP 네트워크 운영자에게만 알려진, SIM 카드(1882)를 이용하는 것에 의해서, 소유자의 진정한 신원을 감춘다. 따라서, 휴대폰(32)과 셀 타워(25B) 사이의 PHY 계층 1 및 데이터 링크 계층 2 연결(28B)을 구축하기 위해서 SIM 카드에 포함된 전화 번호가 이용되나, 그러나 라우팅은 제공하지 않는다. 그 대신, 라스트 마일 라우팅을 위한 데이터 패킷 소스 및 목적지 어드레스가, SDNP 시그널링 서버(1603A)로부터의 지시에 따라, SDNP 앱(1335A) 및 SDNP 게이트웨이(1601A)에 의해서 관리된다.

[0936] SDNP 게이트웨이(1601A)를 통해서 라우팅되면, SDNP 앱으로부터의 통화는 SIM 카드 번호와 상이한 번호를 갖는 것으로 보인다. 물리적 SIM 카드 번호로부터 SDNP 전화 번호로의 이러한 변환은 SDNP 명칭 서버(1604A)에 의해서 실시되고, 그러한 동안에 변환 표(1885)에 따라 통화 라우팅은 SDNP 전화 번호를 SIM 전화 번호로 변경하고, 그에 의해서 임의의 사용자에 대한 물리적 SIM 카드 번호를 은폐한다. SDNP 은폐를 이용하면, 전화 소유자의 진정한 신원이 완전히 은폐된다. SDNP 클라이언트에게 통화를 하기 위해서, 외부 통화자는, 심지어 그들 자체가 SDNP 클라이언트가 아닌 경우에도, SDNP #로 통화를 할 수 있다. SDNP 네트워크는, SIM 카드 전화 번호를 결코 노출시키지 않고, 통화를 SDNP 클라이언트에 자동적으로 라우팅시킨다. 유사하게, SDNP 클라이언트는 콜 아웃을 비-SDNP 피통화자에 위치시키고, 통화 수신자는, SIM 카드 번호로부터가 아니라, SDNP #로부터 수신 통화를 확인한다. 이러한 방식으로, SDNP는, SDNP 시스템이 실시간 네트워크이고 인터넷은 그렇지 않다는 것을 제외하고, 인터넷 통신에서의 NAT 게이트웨이의 기능과 유사한 전화통화 기능을 실시한다.

[0937] 전화기(32)의 진정한 사용자 신원이 통화(28B)에 의해서 결코 노출되지 않기 때문에, 전화기의 위치를 삼각측량하는 것은 효과가 없는데, 이는 그 사용자 및 모든 통신이 익명으로 유지되기 때문이다. 따라서, 미식별 휴대폰의 위치를 추적하는 것이 해커에게 유리하지 않고, SS7 취약성을 회피한다. SDNP 클라이언트가 국제적으로 이동하는 경우에, 이동자는 로컬 선불 SIM 카드를 구매할 수 있고 이를 그 SDNP 번호에 링크시킬 수 있다. SDNP 가입자는 그 SDNP 전화 번호에 위치된 통화를 여전히 수신할 것이나, 라스트 링크는 로컬 SIM 카드를 이용하여 이루어질 것이고, 그에 따라 로밍 과금을 방지한다. 이러한 방식으로, 단일 SDNP 전화 번호가, 장거리 비용이 없이, 국제전화 번호로서 기능한다.

[0938] ***SDNP 서브넷*** - 그 특이적 소프트스위치 소프트웨어-기반의 통신 노드를 이용하며, SDNP 통신 클라우드가, 프라

이빗 또는 공공 호스팅된, 상호 연결된 컴퓨터의 임의의 네트워크에 걸쳐 원격으로 전개될 수 있다. 서버 네트워크의 예는 개인적으로 소유된 공공적으로 임대된 네트워크, 예를 들어 Microsoft, Google, 및 Amazon에 의해서 호스팅된 네트워크를 포함한다. 도 111은 2개의 분리된 서버 네트워크에 걸쳐 전개된 2개의 SDNP 클라우드를 도시한다. 도시된 바와 같이, 서버(1901A, 1901B, 1901C, 및 1901D)를 포함하는 SDNP 클라우드는 SDNP 통신 노드 $M_{0,0}$, $M_{0,4}$, $M_{0,7}$, 및 $M_{0,8}$를 각각 호스팅한다. 서버(1902A, 1902B, 및 1902C)를 포함하는 제2 SDNP 클라우드가 SDNP 노드 $M_{10,0}$, $M_{10,1}$, 및 $M_{10,2}$를 각각 호스팅한다. 이들이, 구역(Z0) 및 구역(Z10) 각각의, 분리된 보안 자격 증명을 이용하기 때문에, 2개의 SDNP 클라우드는 완전히 구분되고 정보를 직접적으로 공유할 수 없다. 그러나, SDNP 앱(1335)d1 작동되는 휴대폰(32)으로서 도시된 단일 SDNP 클라이언트는, 비록 이들이 다른 컴퓨터 서버 임대 제공자에 의해서 호스팅되지만, 양 클라우드에 적절한 인증 액세스를 갖는다. 예에 의해서 도시된 바와 같이, SDNP 클라이언트 $C_{1,1}$는 라우터(1910)를 통한 하이퍼보안 라스트 마일 통신을 이용하여 구역(Z0) 클라우드 내의 SDNP 게이트웨이 노드 $M_{0,7}$에 액세스할 수 있고, 대화 또는 데이터 패킷의 혼합 위험이 없이, 동일 라우터(1910)를 통한 하이퍼보안 라스트 마일 통신을 이용하여 구역(Z10) 클라우드 내의 SDNP 게이트웨이 노드 $M_{10,0}$에 액세스할 수 있다.

[0939] 2개의 독립적인 클라우드에 대한 액세스는 공통 통신기 애플리케이션(UI/UX 1920)을 통해서 이루어진다. 각각의 클라우드에 대한 액세스는 분리된 다이알로그 샌드박스(1921A 및 1921B) 내에서 구획된다. 비록 정보가 개인 계정 샌드박스(1921A)로부터 전화기 내로 다운로드될 수 있지만, 비지니스 계정 샌드박스(1921B)로부터의 데이터 방출은 비지니스 및 회사의 보안 관리에 따라 달라진다.

[0940] 디바이스의 SDNP 클라우드에 대한 연결은 디바이스 내로의, 소프트웨어 또는 펌웨어로서의, SDNP 앱의 설치를 요구한다. 설치는 (i) 애플리케이션을 다운로드하는 것 (ii) SDNP 네트워크 생성된 인증 코드로 디바이스 신원을 확인하는 것, (iii) 개인 식별 자격 증명을 구축하는 것, (iv) 특정 SDNP 클라우드 결합을 위한 승인을 수신하는 것을 포함한다. 일단 활성화되면, SDNP 애플리케이션은 독립적인 SDNP 클라우드에 대한 하이퍼보안 라스트 마일 연결을 생성한다. 많은 경우에, 비지니스 계정에 대한 신원 유효성 및 사용자 인증은 개인 계정 액세스에서 요구되는 것보다 더 정교하고, 다중 인증 방법을 수반할 수 있다.

[0941] SDNP 통신이 소프트웨어-기반이기 때문에, 각각의 통신 클라우드를 위한 구분된 그리고 분리된 보안 자격 증명에서, 동일 서버에 의해서 호스팅될 때에도, 임의의 설치된 SDNP 통신 네트워크들 사이에 상호작용이 존재하지 않는다. 각각의 맞춤형 SDNP 클라우드를 특이적으로 형성하는 구역 특정 보안 자격 증명에서, 2개의 SDNP 클라우드가 유사하지 않고 그에 따라 데이터를 직접적으로 공유할 수 없다. 유리하게, 데이터 누출 위험이 없이, 다수의 SDNP 클라우드들이 동일 서버 또는 서버 네트워크 내에 공존할 수 있다. 클라우드 소유자의 요건에 따라 규정된 바에 따라, 비지니스 네트워크에 대한 액세스가 제어된다. 따라서, 2개의 상이한 전화들이 2개의 분리된 네트워크에 연결될 것이 요구되는 경우와 같이, 동일 보안으로 동작되는, 공통 호스트 서버를 공유할 때, 2개의 계정 및 통신 클라우드의 혼합이 금지된다. 구역 특정 SDNP 클라우드 또는 "서브넷"의 자율성이 도 112에 더 도시되어 있고, 여기에서 서버(1901A, 1901B, 1901C, 및 1901D)는 2개의 클라우드 - 구역-Z0 SDNP 통신 노드 $M_{0,0}$, $M_{0,4}$, $M_{0,7}$, $M_{0,8}$을 각각 포함하는 하나의 클라우드, 및 구역-Z7 SDNP 통신 노드 $M_{7,0}$, $M_{7,4}$, $M_{7,7}$, $M_{7,8}$을 포함하는 제2 클라우드를 동시에 호스팅한다. 동일 서버 내에서 동작됨에도 불구하고, SDNP 구축된 프로토콜을 이용하는 하이퍼보안 통신은 어떠한 직접적인 데이터 교환도 방지한다. 그에 따라, 액세스는, 직접적인 클라우드-간 데이터 교환을 통해서가 아니라, 라스트 마일 통신에 의해서 관리된다.

[0942] SDNP 통신은 개인적으로 임대된 공공적으로 이용 가능한 서버로 제한되지 않고, 또한 상이한 유형들의 회사 또는 정부 에이전시들에 맞춰 구성될 수 있다. 사실상, 민간 기업은 종종, 특히 비지니스 크리티컬 애플리케이션에서, 그 자체의 네트워크를 호스팅하는 것이 바람직하다. 프라이빗 네트워크의 예는 FedEx, Walmart, IBM 등을 포함한다. 비밀성을 위해서, 연구 기관, 대학, 및 의료 센터에 의해서 이용되는 네트워크가 또한 빈번하게 자가-호스팅된다. 프라이빗 서버 네트워크는 또한, SalesForce.com, Box.com, Dropbox, eTrade, SAP, 등과 같은 글로벌 비지니스 클라우드 애플리케이션; eBay, Amazon.com, Priceline.com, e-Insurance와 같은 전자거래 플랫폼 및 비교-쇼핑 네트워크; YouTube, Amazon Prime, Netflix, Hulu, Comcast Xfinity와 같은 미디어 스트리밍 서비스; 그리고 Facebook, Twitter, 및 Snapchat과 같은 소셜 미디어를 호스팅하기 위해서 이용된다.

[0943] 대기업에서, IT 부서는 모기업 및 그 자회사를 위해서 분리된 네트워크들을 운용하는 것을 선택할 수 있다. 그러나, 많은 사설 호스팅되는 비지니스에서, 기반시설 비용이 네트워크 설계에서 중요 인자로 간주된다. 2개의 완전히 상이한 하드웨어 기반의 시스템을 지원하는 대신, SDNP 시스템은, 분리되고 공유된 서버 자원의 조합을

이용하여 그 네트워크를 전개할 수 있는 능력을 회사에 제공한다. 도 113에 도시된 바와 같이, 2개의 법인체, 예를 들어 모기업 및 그 자회사는 분리된 그리고 공유된 서버들 모두를 포함하는 서버 네트워크를 함께-호스팅한다. 특히, 서버(1903, 1904B, 1904C, 및 1904D)는 모기업체를 위해서 구역 Z7 통신 노드 $M_{7,0}$, $M_{7,4}$, $M_{7,7}$, 및 $M_{7,8}$ 각각을 호스팅하는 한편, 서버(1901A, 1901B, 1901C, 및 1903)은 회사의 지역적 자회사를 위해서 상응 구역(Z0) 통신 노드 $M_{0,0}$, $M_{0,4}$, $M_{0,7}$, 및 $M_{0,8}$을 호스팅한다. 도시된 바와 같이, 예를 들어, 서버(1903)는 2개의 SDNP 통신 노드 즉, 모기업체를 위한 노드 $M_{7,0}$ 및 자회사를 위한 노드 $M_{0,8}$를 호스팅한다. 그 구분된 보안 자격 증명으로 인해서, 비록 서버(1903) 및 다른 서버(미도시)가 양 법인체에 의해서 공유되지만, 데이터는 모기업 SDNP 클라우드와 자회사 SDNP 클라우드 사이에서 직접적으로 공유되지 않는다. 일반적으로 피고용인이 그 고용자의 클라우드에만 액세스하도록 제한되지만, 회사 관리자의 경우에, 양 클라우드에 대한 액세스가 요구될 수 있다. SDNP 통신기 앱(UI/UX 1920)에 의해서 도시된 것과 같은 적절한 인증된 사용자는 다양한 법인체를 위한 분리된 다이알로그 샌드박스(1921C 및 1921D)를 포함한다. 이러한 방식으로, 하나의 휴대폰 또는 태블릿이, 사용자가 다수의 전화기를 수반하는 경우와 같이, 데이터의 조합 위험이 없이, 상이한 법인체들의 다수의 SDNP 클라우드들에 액세스할 수 있다.

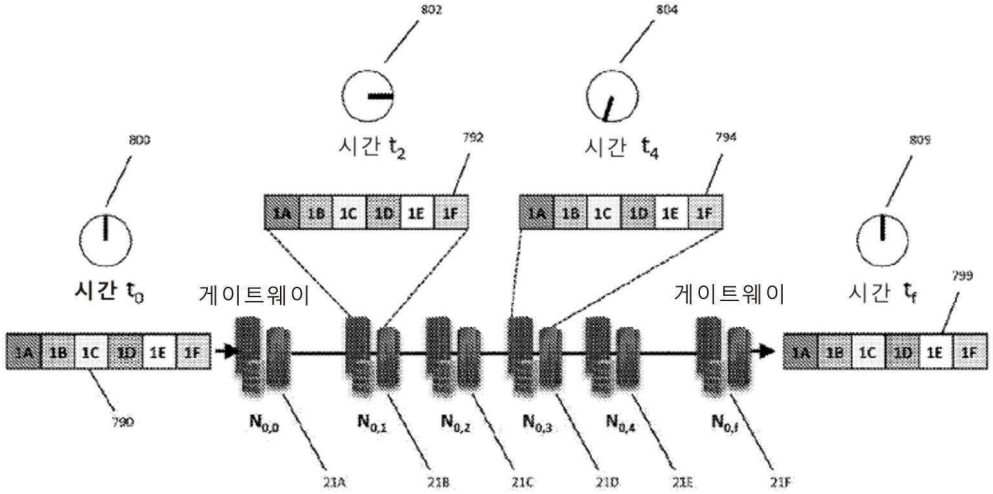
[0944] 다수의 SDNP 클라우드에 대한 액세스를 가능하게 하거나 금지하기 위해서 라스트 마일 하이퍼보안 보안 자격 증명을 이용하는 SDNP 앱의 다중-프로파일 특징은 단일 SDNP 앱으로부터의 제한이 없는 계정 프로파일의 수를 지원한다. 도 114에서, 예를 들어, SDNP 클라이언트 $C_{1,1}$은, SDNP 노드 $M_{99,1}$ 내지 $M_{99,5}$ 각각을 호스팅하는 서버(1909A 내지 1909E)를 포함하는 구역(Z99) 글로벌 SDNP 텔코에 걸쳐, 장거리 비용이 없이, 국제통화를 할 수 있고, 다른 클라우드, 예를 들어 SDNP 노드 $M_{9,0}$, $M_{9,4}$, 및 $M_{9,8}$을 호스팅하는 서버(1905A, 1905B, 및 1905C)를 포함하는 구역 Z9 회사 클라우드에 대한 액세스를 획득할 수 있고, 또한 SDNP 노드 $M_{0,0}$, $M_{0,4}$, 및 $M_{0,8}$ 각각을 호스팅하는 서버(1901A, 1901B, 및 1901C)를 통해서 구역 Z0 클라우드의 가입자에게 통화할 수 있다. 임의의 주어진 클라우드에 대한 액세스 특권은 라스트 마일 통신을 통해서 SDNP 게이트웨이까지 강제되고, 인증된 사용자를 관리하기 위해서 이용되는 시스템의 SDNP 시그널링 서버 및 SDNP 명칭 서버에 의해서 관리된다.

[0945] SDNP 통신은, 정부 및 보안을 위해서 요구되는 높은 보안 및 제한된 액세스 네트워크에서 동일하게 적용될 수 있다. 예를 들어, 미국에서, 보안 제한된 통신은, 의회 및 사법 서버 네트워크와 함께, 지방 및 주 법 집행, FBI, 미국 방위군, 미국 국가 안보국, 미군(별개로 또는 통합적으로), 미국 국무부를 포함하는 다양한 부서에 의해서 요구된다. 유사하게, 다른 국가는 다양한 정부 기관을 위해서 분리된 네트워크들을 호스팅한다.

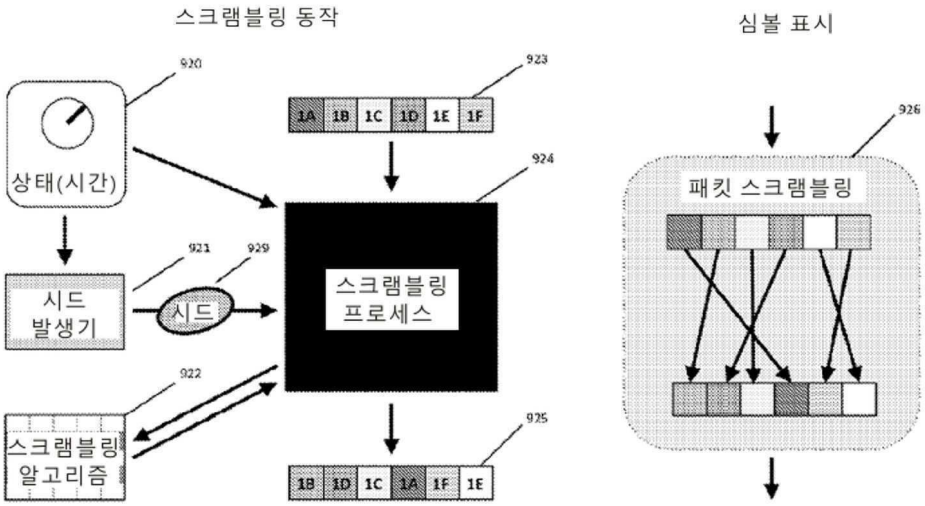
[0946] "알 필요가 있는 것"을 기초로 하는 특정 클라우드에 대한 액세스를 지원하기 위해서, 네스트형 서브넷 아키텍처가 SDNP 통신 방법 및 기술을 이용하여 구현될 수 있다. 예를 들어, 도 115에서, 네스트형 SDNP 클라우드 구조는, SDNP 통신 노드 $M_{0,0}$, $M_{0,4}$, $M_{0,5}$, 및 $M_{0,9}$ 각각을 호스팅하는 임대된 컴퓨터 서버(1907A 내지 1907D)를 포함하는 보안 클라우드를 포함한다. 이러한 외부 네트워크 "쉘" 내에서의 통신은 구역 Z0 보안 자격 증명을 포함하고, SDNP 통신기(1920)에서 디스플레이된 바와 같이 "비밀" 레벨 다이알로그 샌드박스(1912E) 내에서 디스플레이된다. 네스트형 클라우드는 또한, 정부-호스팅된 서버(1906A, 1906B 및 1906C) 상응 SDNP 서버 노드 $M_{8,0}$, $M_{8,2}$, 및 $M_{8,4}$를 포함하는 구역 Z8 보안 자격 증명을 갖는 향상된 보안의 내부 코어를 포함한다. 클라이언트 $C_{1,1}$가 구역 Z8 코어에 대한 액세스를 획득하기 위해서, 이들은 "최고 비밀" 보안 등급을 가져야 하고, 강화된 통신 샌드박스(1921F)를 통해서 통신하여야 한다. 이러한 기술의 하나의 예시적인 정부 적용예는 미국 국무부에서이고, 여기에서 구역 Z8 내의 최고 비밀 통신은 대사 및 국무장관에 의한 액세스로 제한되는 반면, 세계에 걸쳐진 다른 미국 대사관 직원은 구역 Z0 보안 자격 증명을 이용한 하이퍼보안 "비밀" 통신으로 제한된다.

도면

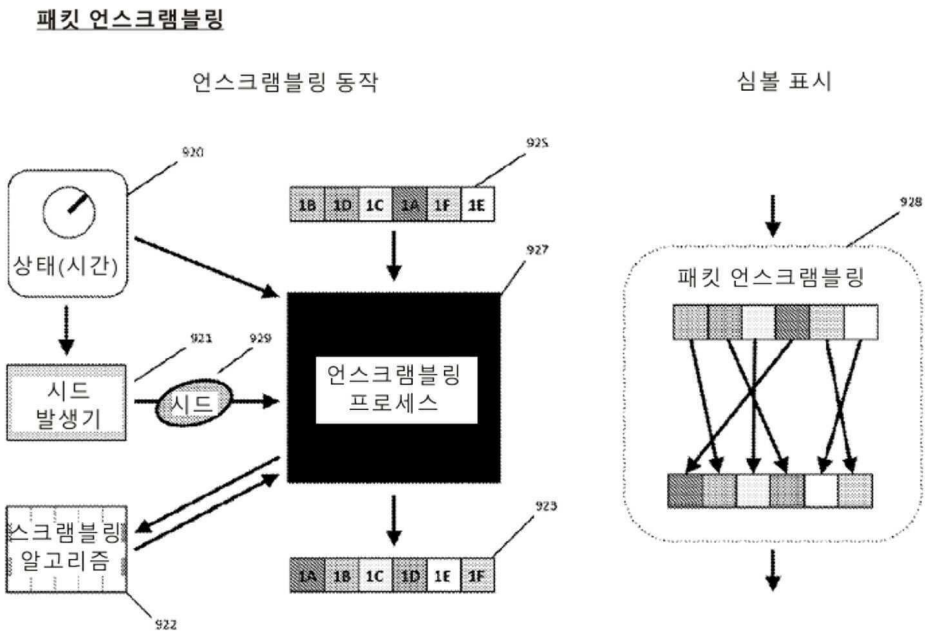
도면1


802
804
시간 $t_2$
시간 $t_4$
800
792
794
809
799
시간 $t_0$
게이트웨이
게이트웨이
시간 $t_f$
1A 1B 1C 1D 1E 1F
790
$N_{0,0}$
$N_{0,1}$
$N_{0,2}$
$N_{0,3}$
$N_{0,4}$
$N_{0,f}$
21A
21B
21C
21D
21E
21F

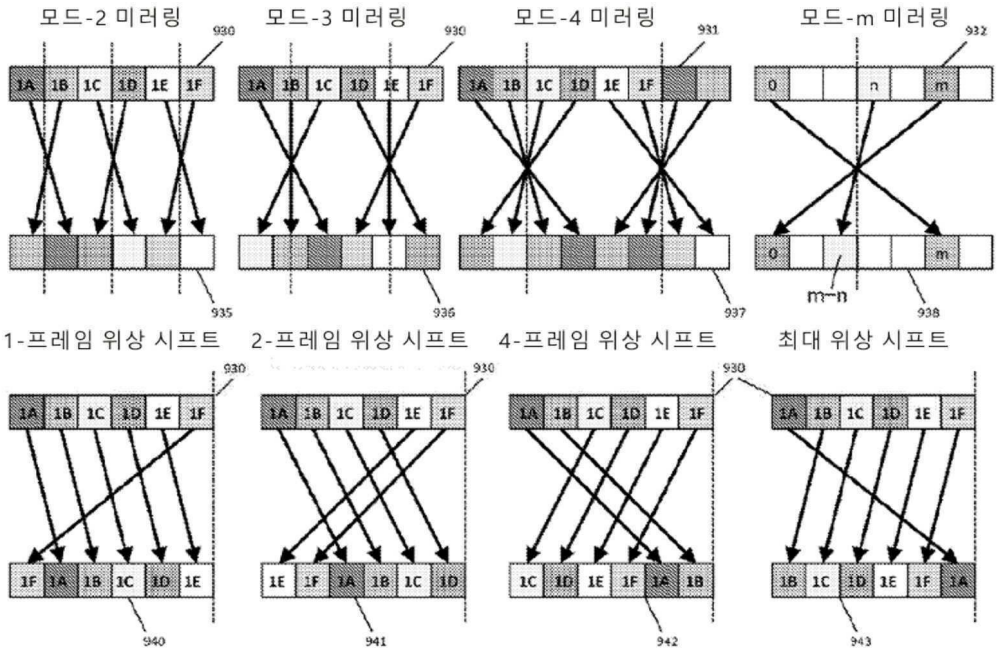
도면2a


스크램블링 동작
심볼 표시
920
923
924
926
상태(시간)
1A 1B 1C 1D 1E 1F
패킷 스크램블링
921
929
시드 발생기
시드
스크램블링 프로세스
922
925
스크램블링 알고리즘
1B 1D 1C 1A 1F 1E

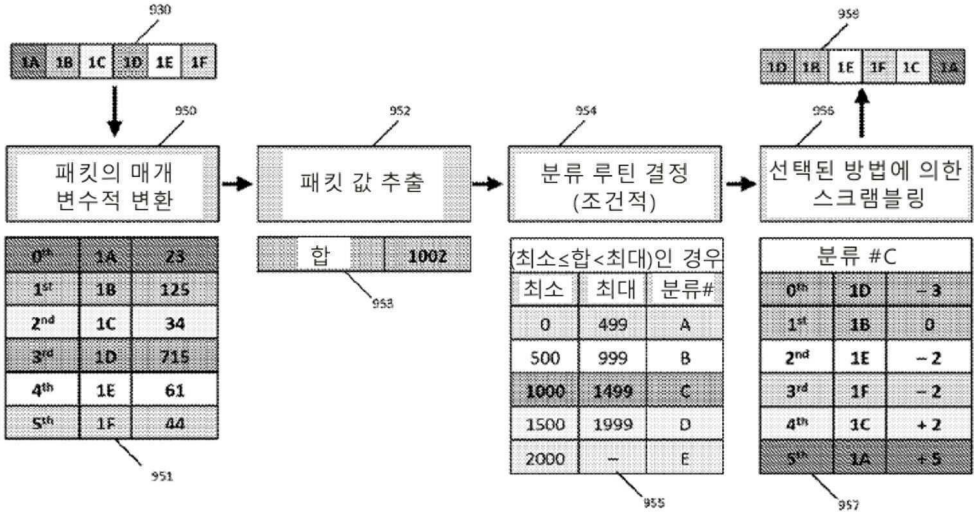
도면2b


패킷 언스크램블링
언스크램블링 동작
심볼 표시
920
925
상태(시간)
1B 1D 1C 1A 1F 1E
927
921
929
시드 발생기
시드
언스크램블링 프로세스
923
스크램블링 알고리즘
922
928
패킷 언스크램블링

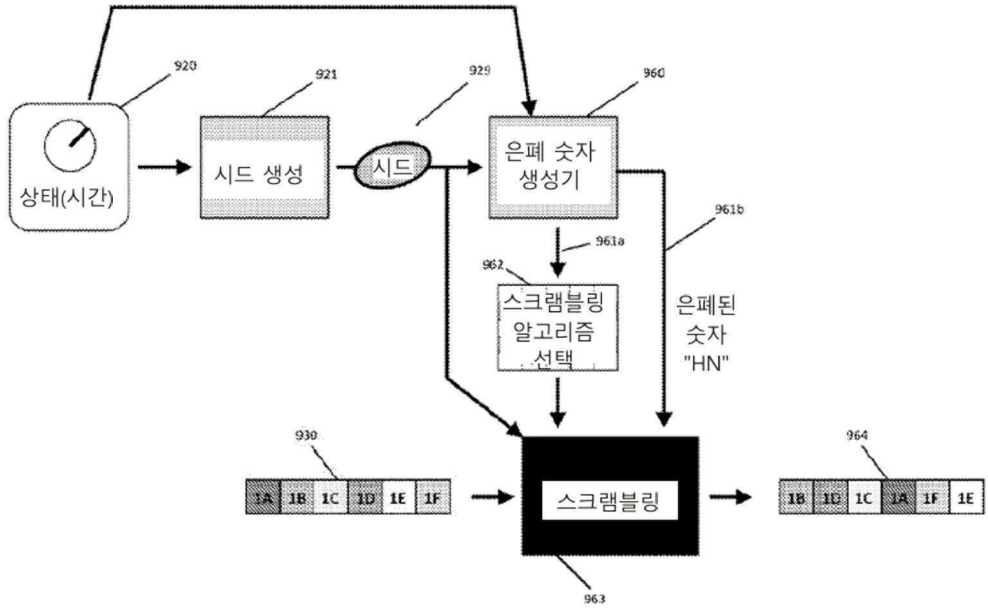
도면2c


모드-2 미러링
모드-3 미러링
모드-4 미러링
모드-m 미러링
930
931
932
1A 1B 1C 1D 1E 1F
0 n m
0 m
m-n
935
936
937
938
1-프레임 위상 시프트
2-프레임 위상 시프트
4-프레임 위상 시프트
최대 위상 시프트
940
941
942
943

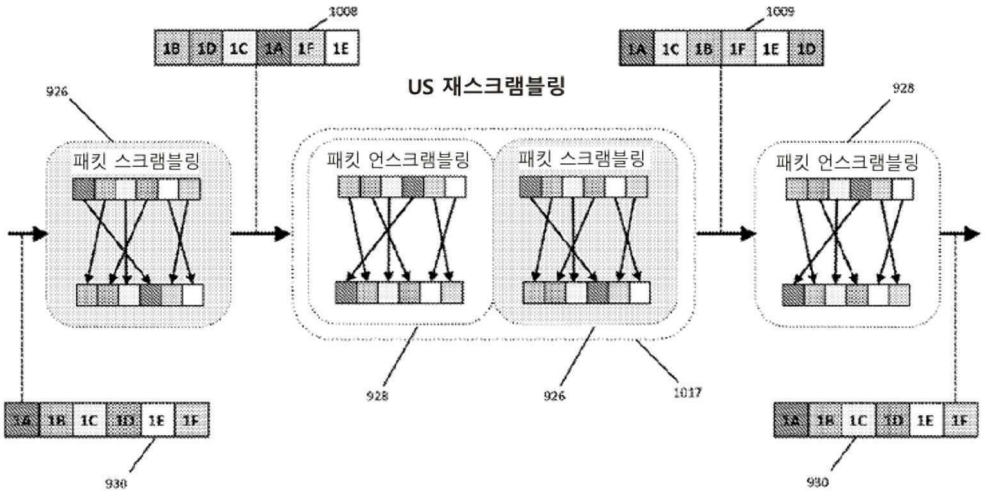
도면2d


930
1A 1B 1C 1D 1E 1F
950
패킷의 매개 변수적 변환
952
패킷 값 추출
954
분류 루틴 결정 (조건적)
956
선택된 방법에 의한 스크램블링
959
1D 1B 1E 1F 1C 1A
0th 1A 23
1st 1B 125
2nd 1C 34
3rd 1D 715
4th 1E 61
5th 1F 44
951
합 1002
953
(최소≤합<최대)인 경우
최소 최대 분류#
0 499 A
500 999 B
1000 1499 C
1500 1999 D
2000 ~ E
955
분류 #C
0th 1D -3
1st 1B 0
2nd 1E -2
3rd 1F -2
4th 1C +2
5th 1A +5
957

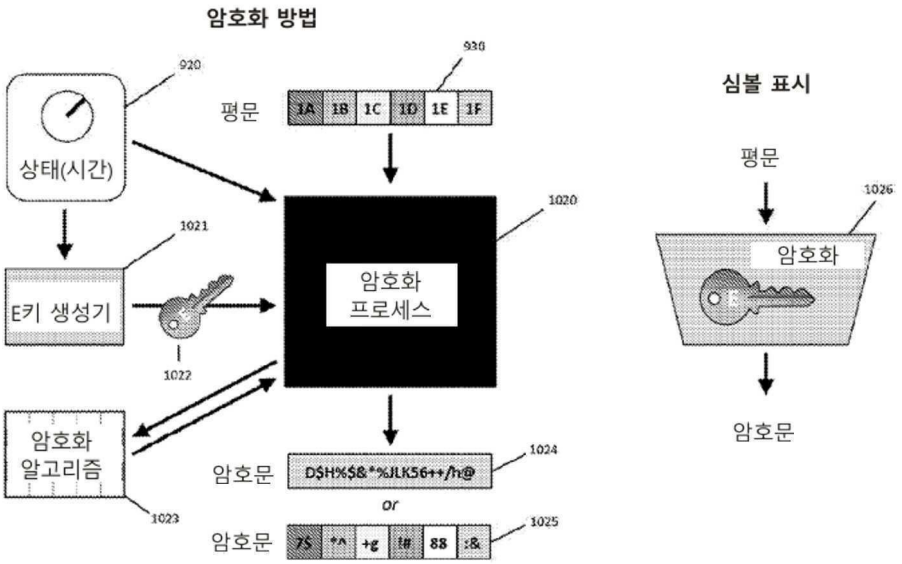
도면2e


920
상태(시간)
921
시드 생성
929
시드
960
은폐 숫자 생성기
961b
961a
962
스크램블링 알고리즘 선택
은폐된 숫자 "HN"
930
1A 1B 1C 1D 1E 1F
963
스크램블링
964
1B 1D 1C 1A 1F 1E

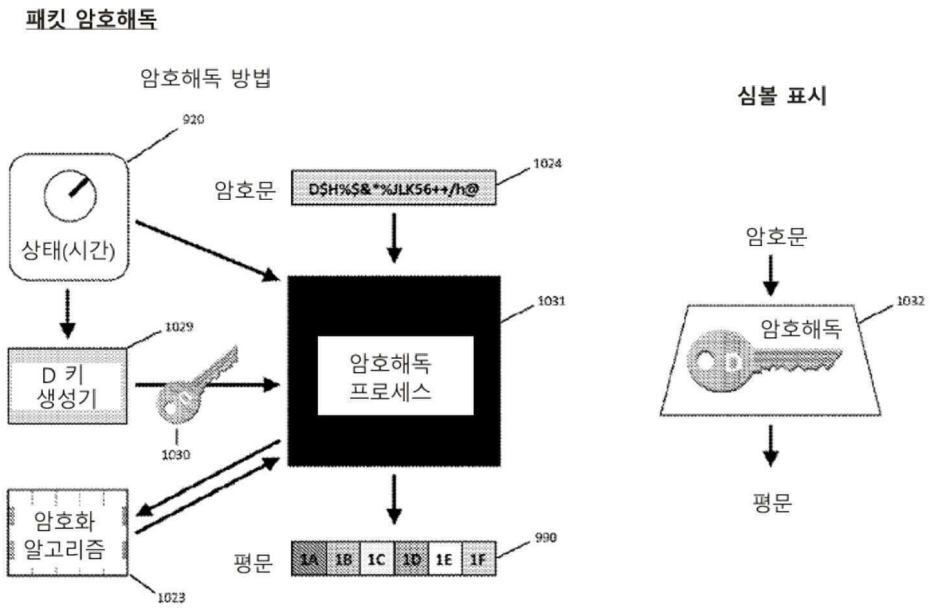
도면3


US 재스크램블링
패킷 스크램블링
패킷 언스크램블링
패킷 스크램블링
패킷 언스크램블링
926
928
1008
1009
1017
930

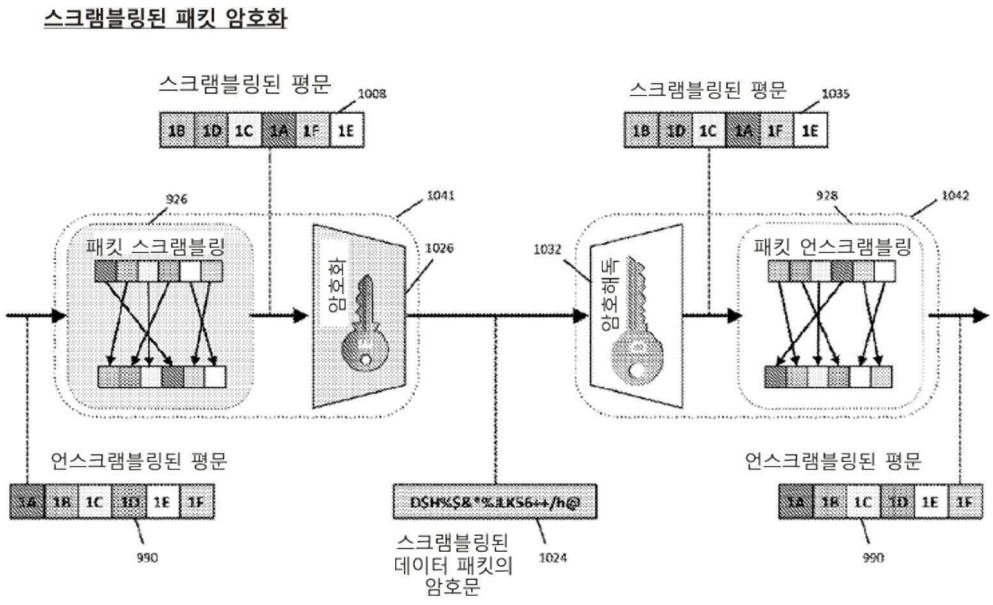
도면4a


암호화 방법
상태(시간)
평문
암호화
프로세스
E키 생성기
암호화
알고리즘
암호문
D$H%$&*%JLK56++/h@
or
920
930
1020
1021
1022
1023
1024
1025
심볼 표시
평문
암호화
암호문
1026

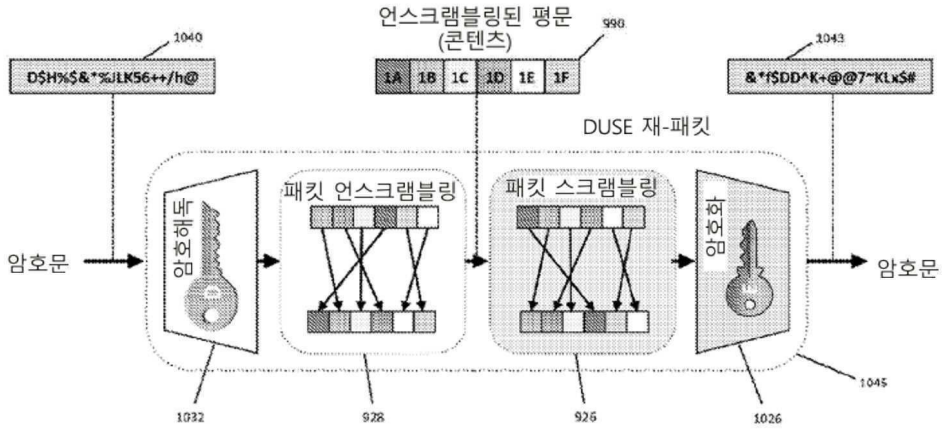
도면4b


패킷 암호해독
암호해독 방법
920
상태(시간)
암호문
D$H%$&*%JLK56++/h@
1024
1031
암호해독
프로세스
1029
D 키
생성기
1030
암호화
알고리즘
1023
평문
1A 1B 1C 1D 1E 1F
990
심볼 표시
암호문
1032
암호해독
평문

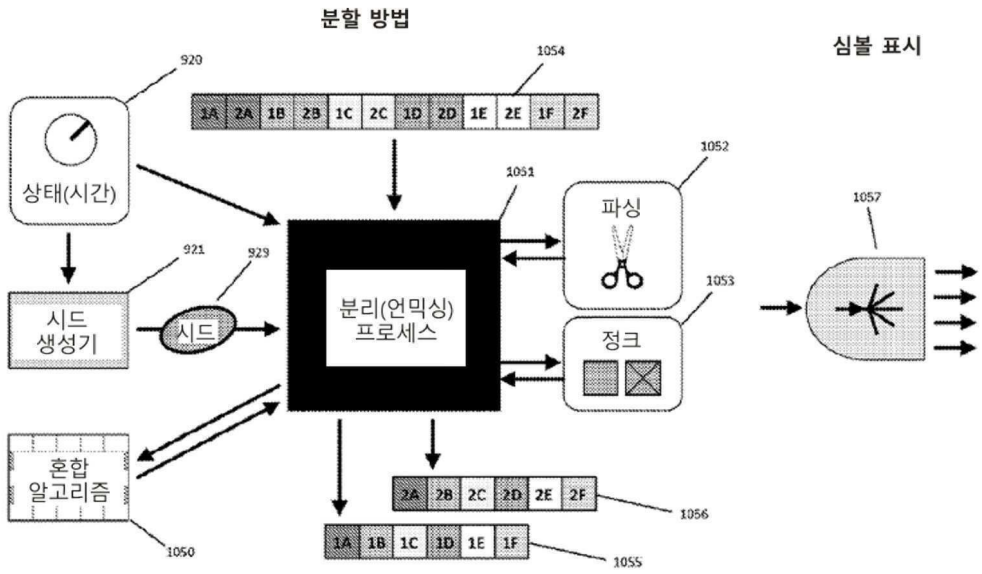
도면5


스크램블링된 패킷 암호화
스크램블링된 평문
1008
1B 1D 1C 1A 1F 1E
926
패킷 스크램블링
1041
암호화
1026
스크램블링된 평문
1035
1B 1D 1C 1A 1F 1E
928
1042
패킷 언스크램블링
1032
암호해독
언스크램블링된 평문
1A 1B 1C 1D 1E 1F
990
D$H%$&*%JLK56++/h@
1024
스크램블링된
데이터 패킷의
암호문
언스크램블링된 평문
1A 1B 1C 1D 1E 1F
990

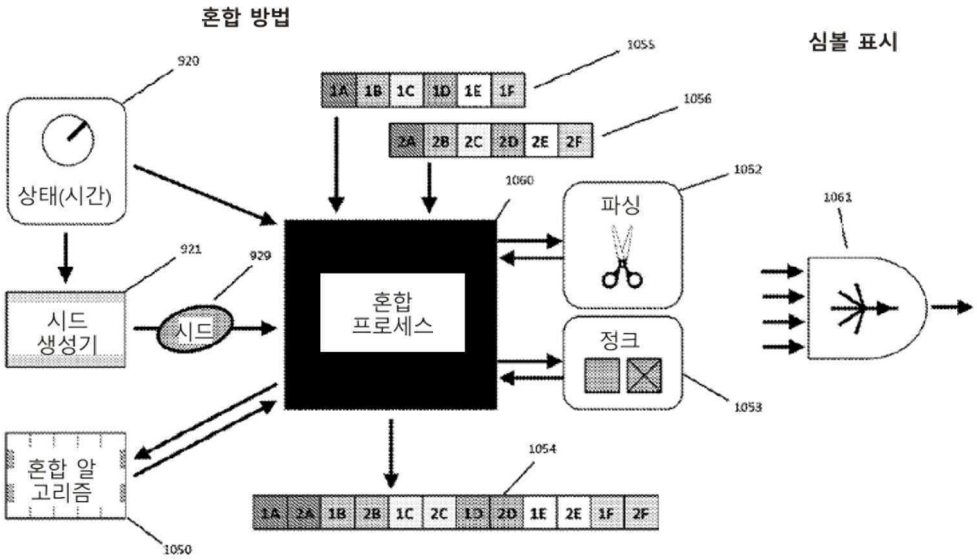
도면6


언스크램블링된 평문
(콘텐츠)
998
1040
D$H%$&*%JLK56++/h@
1043
&*fSDD^K+@@7~KLxS#
1A 1B 1C 1D 1E 1F
DUSE 재-패킷
암호문
복호화
패킷 언스크램블링
패킷 스크램블링
암호화
암호문
1045
1032
928
926
1026

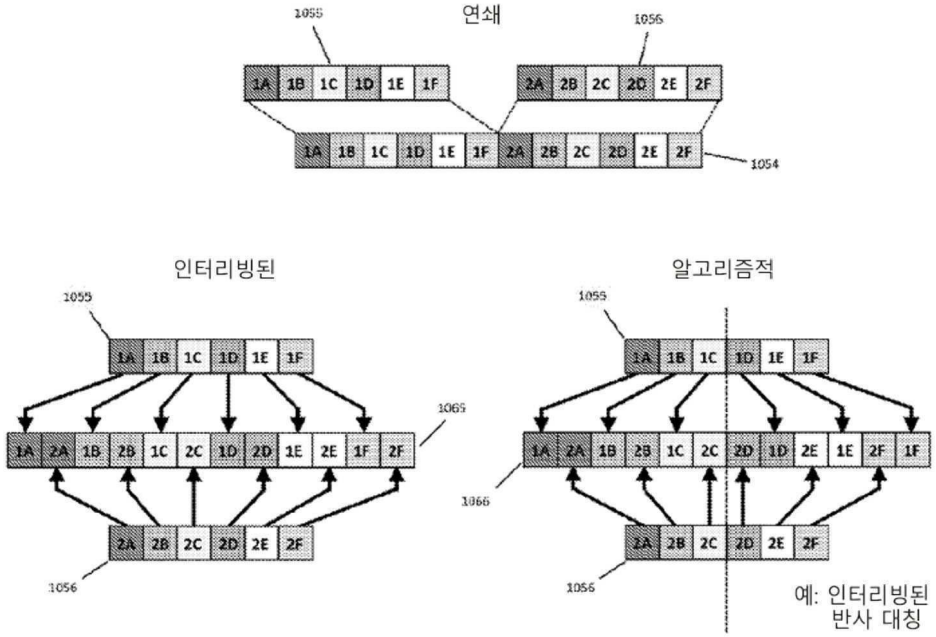
도면7a


분할 방법
심볼 표시
920
1054
1A 2A 1B 2B 1C 2C 1D 2D 1E 2E 1F 2F
상태(시간)
1051
1052
파싱
1057
921
929
시드 생성기
시드
분리(언믹싱) 프로세스
1053
정크
혼합 알고리즘
2A 2B 2C 2D 2E 2F
1056
1A 1B 1C 1D 1E 1F
1050
1055

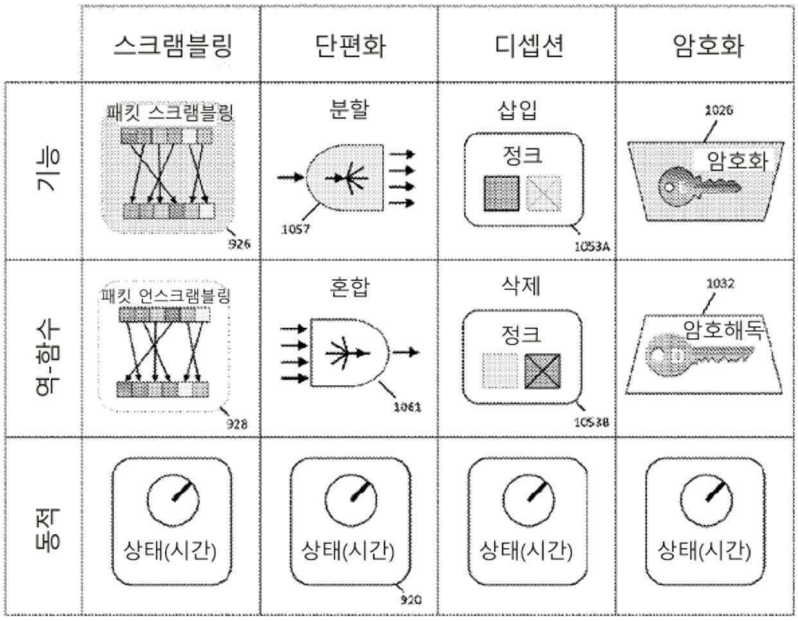
도면7b


혼합 방법
심볼 표시
920
상태(시간)
921
시드 생성기
929
시드
혼합 알고리즘
1050
혼합 프로세스
1060
1055
1A 1B 1C 1D 1E 1F
1056
2A 2B 2C 2D 2E 2F
1052
파싱
정크
1053
1061
1054
1A 2A 1B 2B 1C 2C 1D 2D 1E 2E 1F 2F

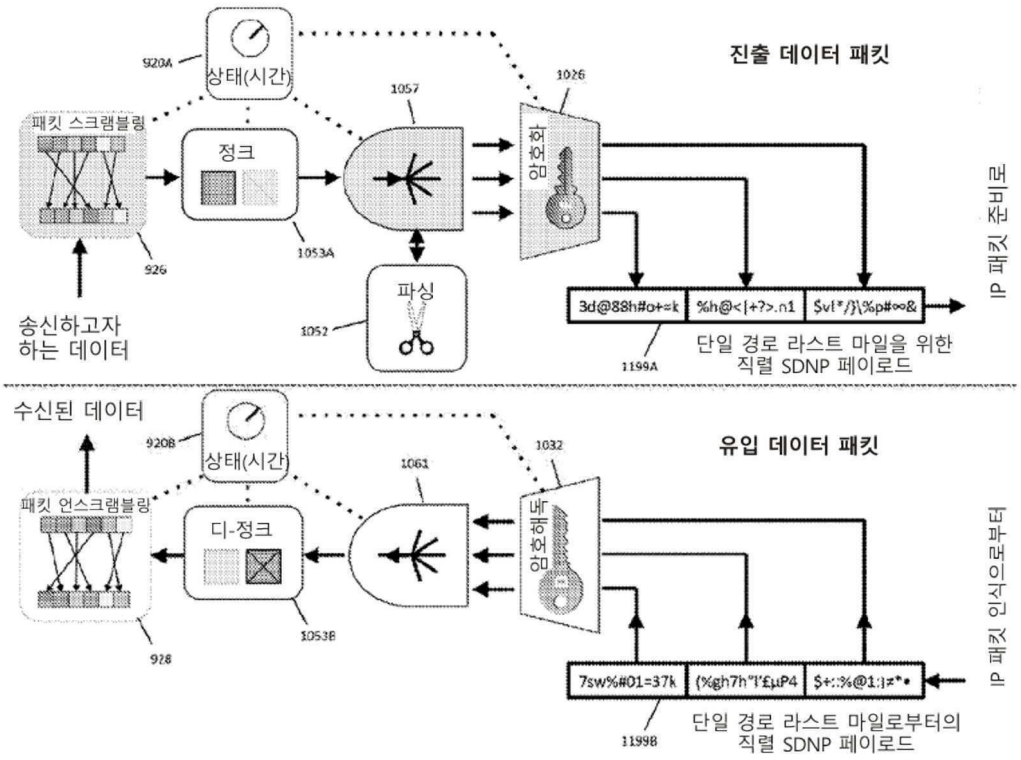
도면8


연쇄
1055
1A 1B 1C 1D 1E 1F
1056
2A 2B 2C 2D 2E 2F
1A 1B 1C 1D 1E 1F 2A 2B 2C 2D 2E 2F
1054
인터리빙된
1055
1A 1B 1C 1D 1E 1F
1A 2A 1B 2B 1C 2C 1D 2D 1E 2E 1F 2F
1065
2A 2B 2C 2D 2E 2F
1056
알고리즘적
1055
1A 1B 1C 1D 1E 1F
1A 2A 1B 2B 1C 2C 2D 1D 2E 1E 2F 1F
1066
2A 2B 2C 2D 2E 2F
1056
예: 인터리빙된
반사 대칭

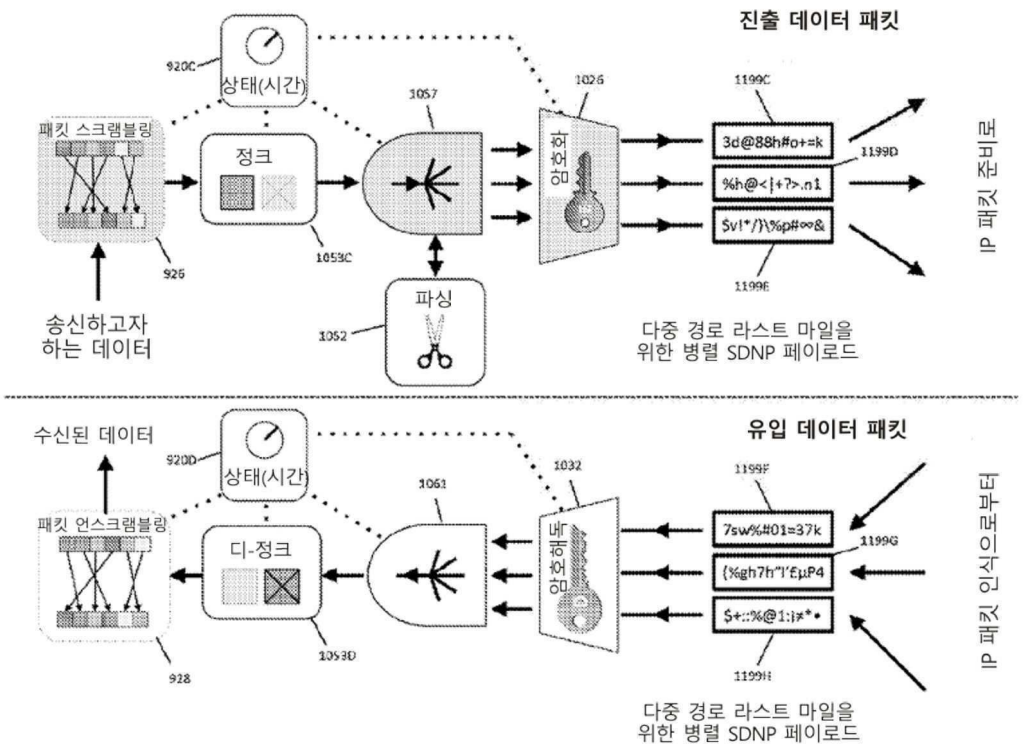
도면9a


스크램블링
단편화
디셉션
암호화
기능
역-함수
동적
패킷 스크램블링
분할
삽입
정크
암호화
패킷 언스크램블링
혼합
삭제
정크
암호해독
상태(시간)
상태(시간)
상태(시간)
상태(시간)

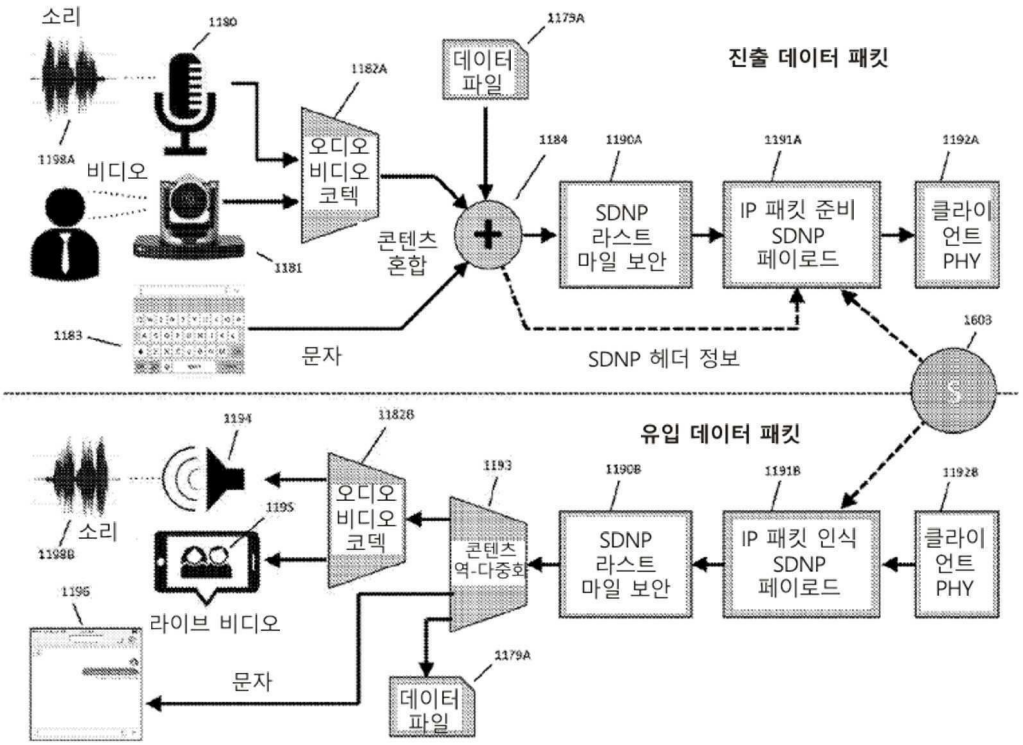
도면9b


진출 데이터 패킷
상태(시간)
패킷 스크램블링
정크
암호화
파싱
송신하고자
하는 데이터
3d@88h#o+=k
%h@<|+?>.n1
$v!*/}\%p#∞&
단일 경로 라스트 마일을 위한
직렬 SDNP 페이로드
IP 패킷 준비로
수신된 데이터
상태(시간)
패킷 언스크램블링
디-정크
암호해독
7sw%#01=37k
(%gh7h"l'£µP4
$+:;%@1:]≠*•
단일 경로 라스트 마일로부터의
직렬 SDNP 페이로드
유입 데이터 패킷
IP 패킷 인식으로부터

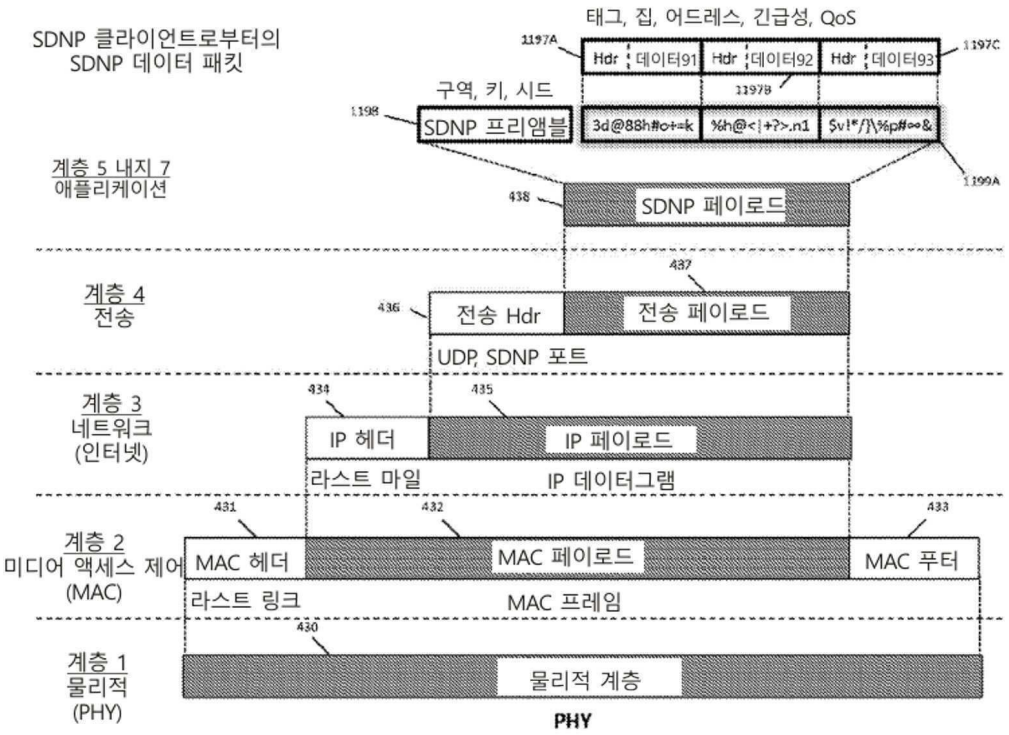
도면9c


진출 데이터 패킷
920C
상태(시간)
패킷 스크램블링
정크
1057
1026
암호화
1199C
3d@88h#o+=k
1199D
%h@<|+?>.n1
$v!*/}\%p#∞&
1199E
IP 패킷 준비로
926
1053C
송신하고자
하는 데이터
파싱
1052
다중 경로 라스트 마일을
위한 병렬 SDNP 페이로드
수신된 데이터
유입 데이터 패킷
920D
상태(시간)
패킷 언스크램블링
디-정크
1061
1032
암호해독
1199F
7sw%#01=37k
1199G
{%gh7h"l'£µP4
$+::%@1:i*•
1199H
IP 패킷 인식으로부터
928
1053D
다중 경로 라스트 마일을
위한 병렬 SDNP 페이로드

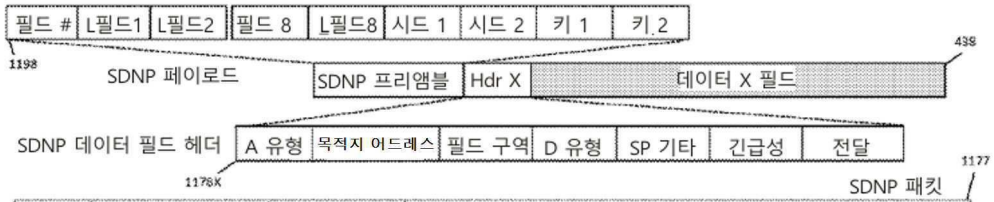
도면9d


소리
1180
1198A
비디오
1181
1182A
오디오
비디오
코텍
콘텐츠
혼합
1183
문자
1175A
데이터
파일
진출 데이터 패킷
1184
1190A
SDNP
라스트
마일 보안
1191A
IP 패킷 준비
SDNP
페이로드
1192A
클라이
언트
PHY
1603
SDNP 헤더 정보
유입 데이터 패킷
1194
1182B
오디오
비디오
코덱
1195
소리
1198B
라이브 비디오
1196
문자
1193
콘텐츠
역-다중화
1190B
SDNP
라스트
마일 보안
1191B
IP 패킷 인식
SDNP
페이로드
1192B
클라이
언트
PHY
1179A
데이터
파일

도면9e

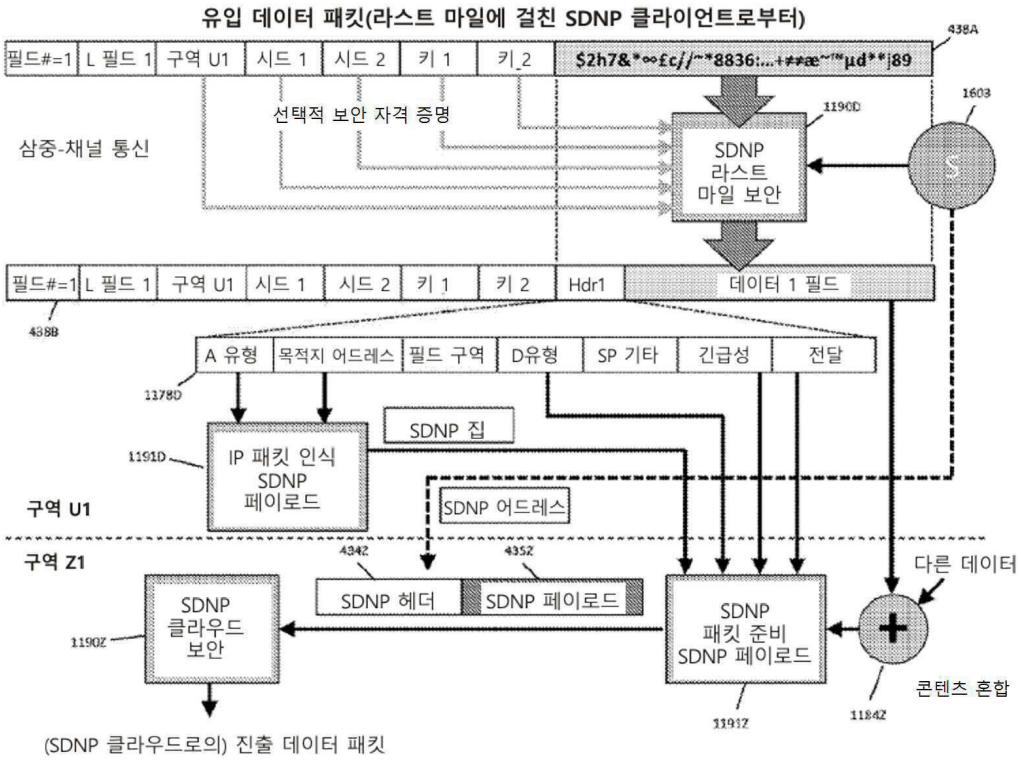



도면9f

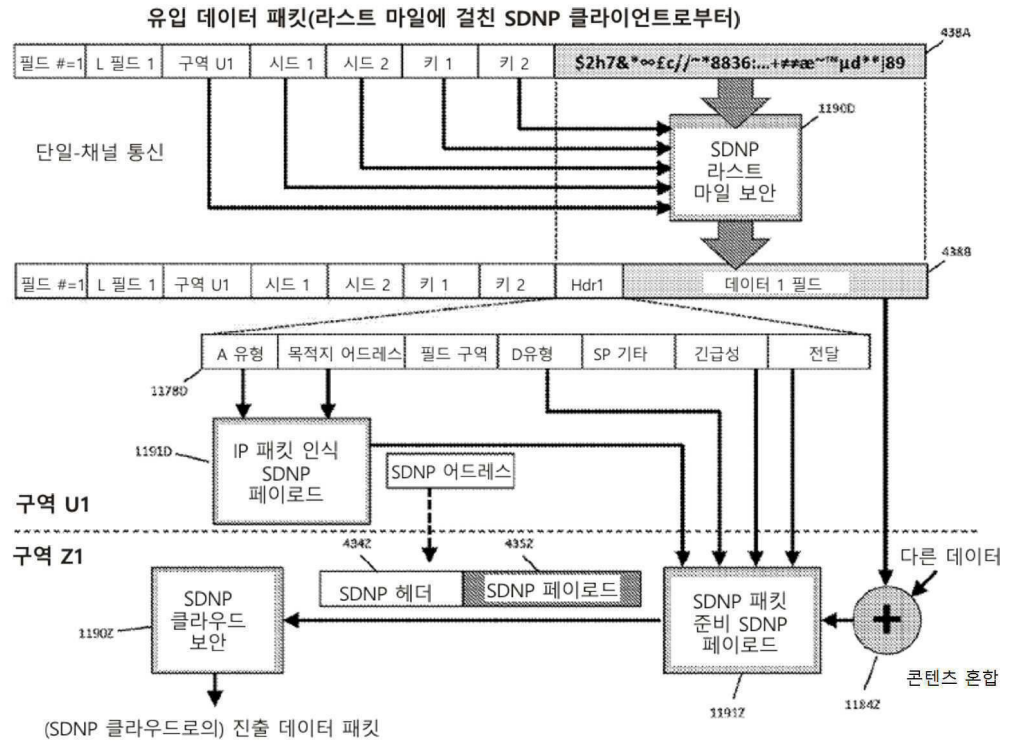



| 계층 | 패킷 필드 | 크기 | 함수 |
|---|---|---|---|
| 3 | 필드# | 4b | 필드의 번호 |
| 3 | L 필드 1, 2, X | 4B | 데이터 필드 1, 2, ..., 8의 길이 |
| 3 | 구역 | 12b | 현재 SDNP 구역(4096개 구역 중 하나) |
| 5 | 시드 1, 2 | 8B, 8B | (스크램블링, 혼합 등을 위한) 2개의 32 비트 시드 |
| 6 | 키 1, 2 | 64B, 64B | (암호화를 위한) 2개의 512 비트 키 |
| 3 | A(어드레스) 유형 | 2b | 목적지 어드레스의 유형(태그, SDNP 집, IPv6, NAT, POTS #) |
| 3 | 목적지 어드레스 | 18 내지 12B | 태그, IP 어드레스, SDNP 어드레스, NAT 어드레스, SDNP 집, 전화 # |
| 3 | 필드 구역 | 12b | SDNP 구역 수반-정방향(4096개 구역 중 하나)ㅁ |
| 4 | D(데이터) 유형 | 2b | 데이터의 유형(보이스, 문자, 비디오, 데이터, 소프트웨어...) |
| 6 | 필드 기타 | 8B | 필드 확장, 필드 언스크램블링 정보, 등 |
| 4 | 긴급성 | 2b | 서브-패킷의 긴급성(스네일, 정상, 우선, 긴급) |
| 4 | 전달 | 2b | QoS 마커(정상, 중복, 특별, VIP...) |
| 5 내지 7 | 패킷 X 내의 데이터 | 0 내지 200B | 0 내지 200B/서브-패킷 당 200B까지의 데이터, 8 서브-패킷 최대 |

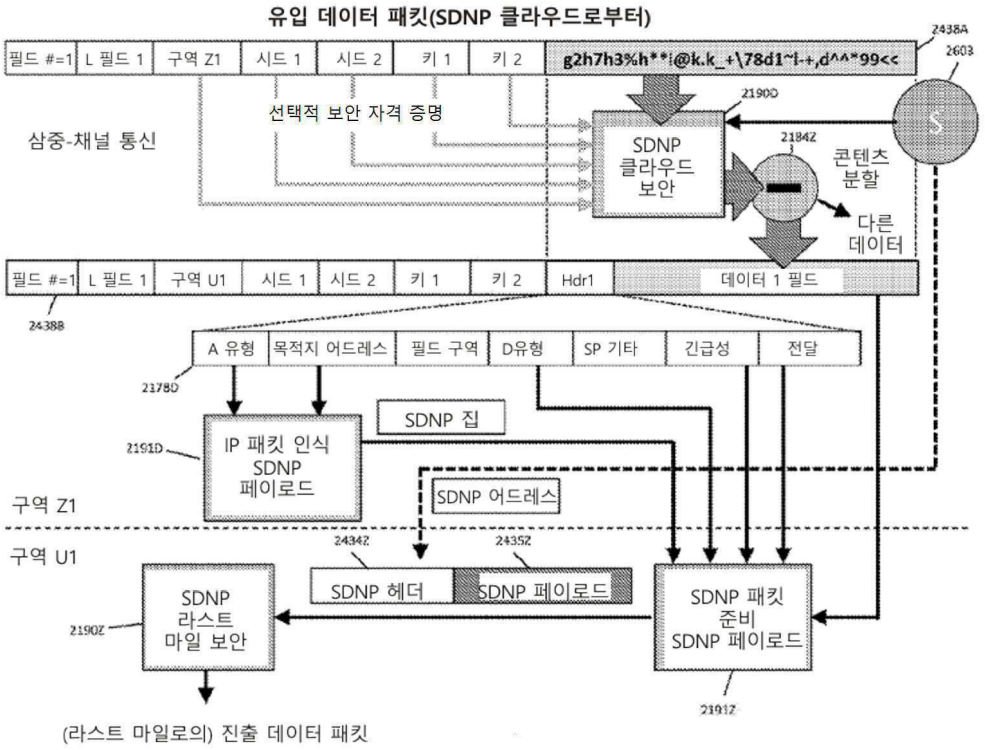
도면9g


유입 데이터 패킷(라스트 마일에 걸친 SDNP 클라이언트로부터)
필드#=1
L 필드 1
구역 U1
시드 1
시드 2
키 1
키 2
$2h7&*∞£c//~*8836:...+≠æ~™µd**|89
438A
선택적 보안 자격 증명
삼중-채널 통신
1190D
SDNP 라스트 마일 보안
1603
Hdr1
데이터 1 필드
438B
A 유형
목적지 어드레스
필드 구역
D유형
SP 기타
긴급성
전달
1178D
SDNP 집
1191D
IP 패킷 인식 SDNP 페이로드
SDNP 어드레스
구역 U1
구역 Z1
4342
4352
SDNP 헤더
SDNP 페이로드
다른 데이터
SDNP 클라우드 보안
1190Z
SDNP 패킷 준비 SDNP 페이로드
1191Z
1184Z
콘텐츠 혼합
(SDNP 클라우드로의) 진출 데이터 패킷

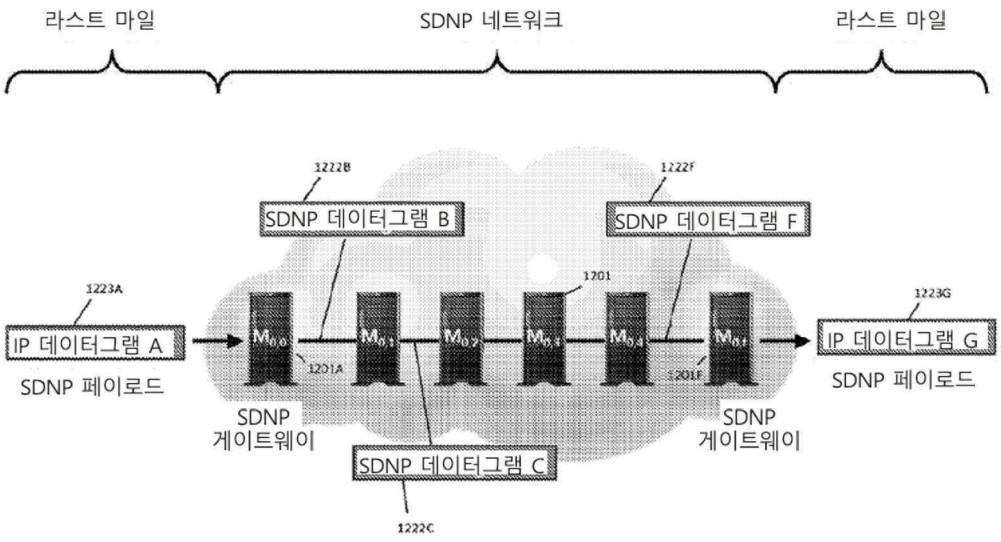
도면9h


유입 데이터 패킷(라스트 마일에 걸친 SDNP 클라이언트로부터)
필드 #=1
L 필드 1
구역 U1
시드 1
시드 2
키 1
키 2
$2h7&*∞£c//~*8836:...+≠æ~™µd**|89
438A
단일-채널 통신
1190D
SDNP 라스트 마일 보안
Hdr1
데이터 1 필드
438B
A 유형
목적지 어드레스
필드 구역
D유형
SP 기타
긴급성
전달
1178D
1191D
IP 패킷 인식 SDNP 페이로드
SDNP 어드레스
구역 U1
구역 Z1
4342
4352
SDNP 헤더
SDNP 페이로드
다른 데이터
SDNP 클라우드 보안
1190Z
SDNP 패킷 준비 SDNP 페이로드
1191Z
1184Z
콘텐츠 혼합
(SDNP 클라우드로의) 진출 데이터 패킷

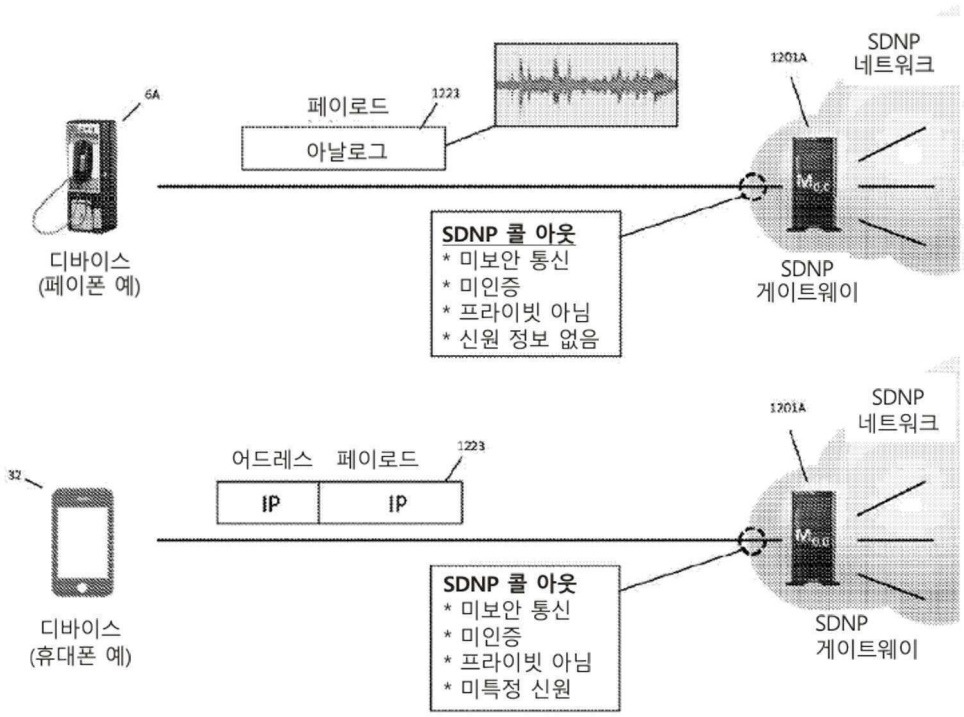
도면9i


유입 데이터 패킷(SDNP 클라우드로부터)
필드 #=1
L 필드 1
구역 Z1
시드 1
시드 2
키 1
키 2
g2h7h3%h**i@k.k_+\78d1~l-+,d^^*99<<
2438A
2603
선택적 보안 자격 증명
삼중-채널 통신
2190D
SDNP
클라우드
보안
21842
콘텐츠
분할
다른
데이터
필드 #=1
L 필드 1
구역 U1
시드 1
시드 2
키 1
키 2
Hdr1
데이터 1 필드
24388
A 유형
목적지 어드레스
필드 구역
D유형
SP 기타
긴급성
전달
2378D
SDNP 집
2191D
IP 패킷 인식
SDNP
페이로드
SDNP 어드레스
구역 Z1
구역 U1
24342
24352
SDNP 헤더
SDNP 페이로드
SDNP
라스트
마일 보안
2190Z
SDNP 패킷
준비
SDNP 페이로드
2191Z
(라스트 마일로의) 진출 데이터 패킷

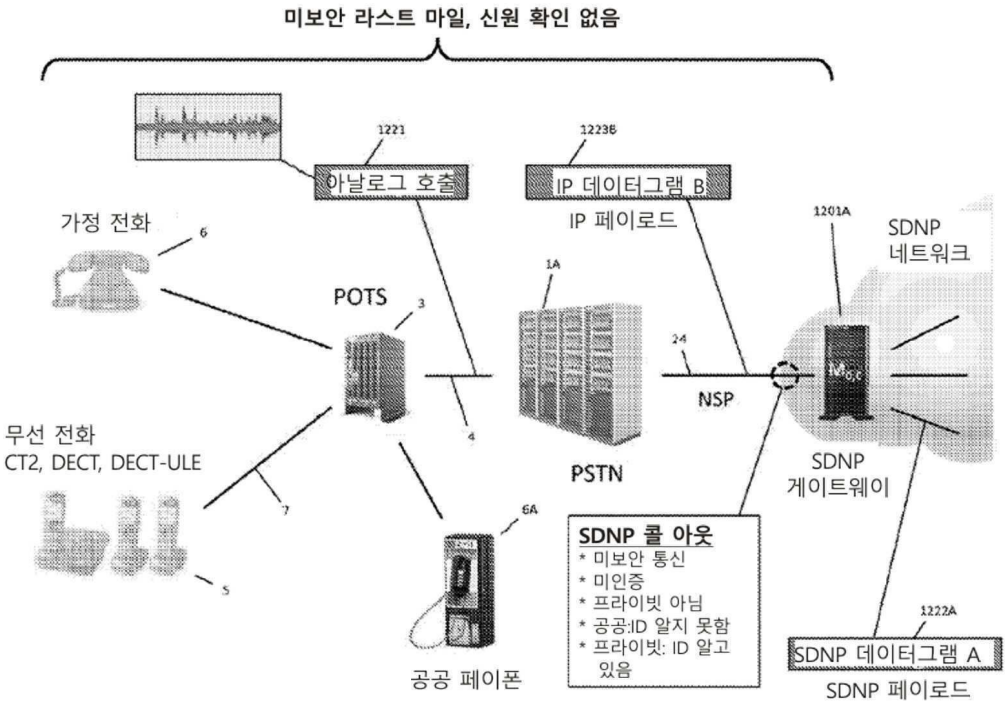
도면10


라스트 마일
SDNP 네트워크
라스트 마일
12228
SDNP 데이터그램 B
1222F
SDNP 데이터그램 F
1223A
IP 데이터그램 A
SDNP 페이로드
1201
1201A
1201F
1223G
IP 데이터그램 G
SDNP 페이로드
SDNP
게이트웨이
SDNP
게이트웨이
SDNP 데이터그램 C
1222C

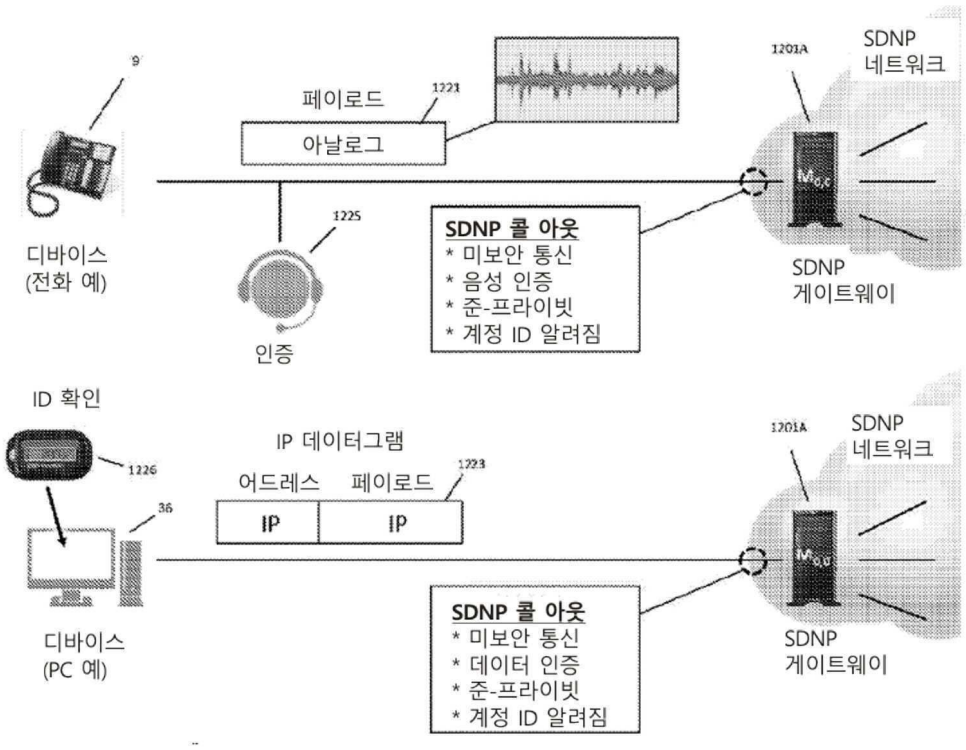
도면11


6A
디바이스
(페이폰 예)
페이로드
1223
아날로그
1201A
SDNP
네트워크
SDNP 콜 아웃
* 미보안 통신
* 미인증
* 프라이빗 아님
* 신원 정보 없음
SDNP
게이트웨이
32
디바이스
(휴대폰 예)
어드레스
페이로드
1223
IP
IP
1201A
SDNP
네트워크
SDNP 콜 아웃
* 미보안 통신
* 미인증
* 프라이빗 아님
* 미특정 신원
SDNP
게이트웨이

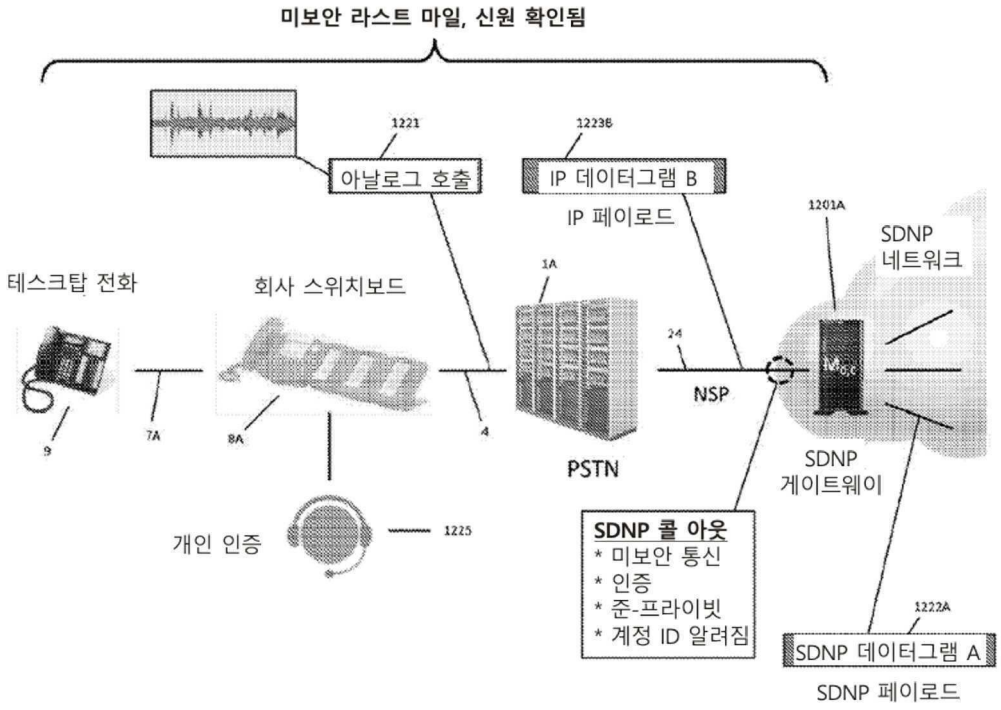
도면12


미보안 라스트 마일, 신원 확인 없음
1221
아날로그 호출
1223B
IP 데이터그램 B
IP 페이로드
가정 전화
6
POTS
3
1A
24
NSP
1201A
SDNP
네트워크
무선 전화
CT2, DECT, DECT-ULE
7
5
4
PSTN
SDNP
게이트웨이
6A
공공 페이폰
SDNP 콜 아웃
* 미보안 통신
* 미인증
* 프라이빗 아님
* 공공:ID 알지 못함
* 프라이빗: ID 알고
있음
1222A
SDNP 데이터그램 A
SDNP 페이로드

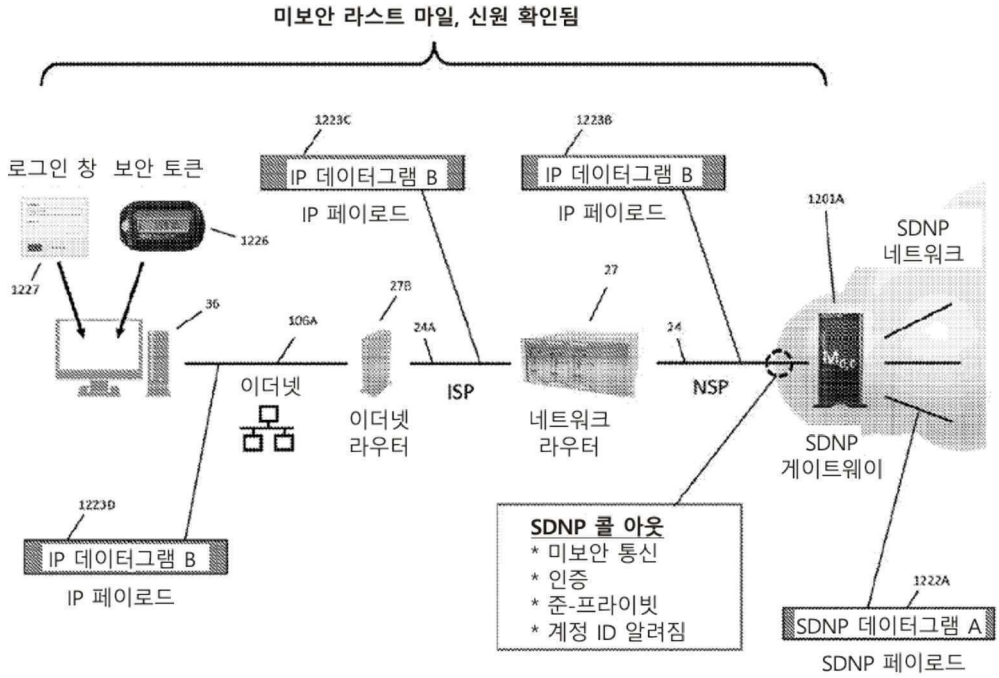
도면13


9
디바이스
(전화 예)
페이로드
1221
아날로그
1225
인증
SDNP 콜 아웃
* 미보안 통신
* 음성 인증
* 준-프라이빗
* 계정 ID 알려짐
1201A
SDNP
네트워크
SDNP
게이트웨이
ID 확인
1226
36
디바이스
(PC 예)
IP 데이터그램
어드레스
페이로드
1223
IP
IP
SDNP 콜 아웃
* 미보안 통신
* 데이터 인증
* 준-프라이빗
* 계정 ID 알려짐
1201A
SDNP
네트워크
SDNP
게이트웨이

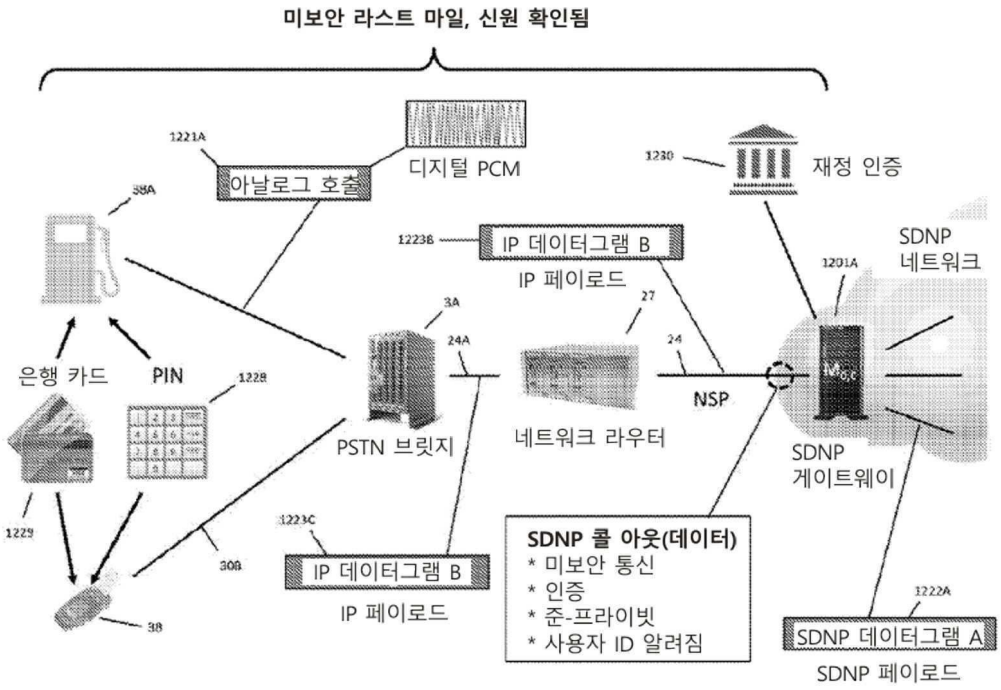
도면14


미보안 라스트 마일, 신원 확인됨
1221
아날로그 호출
1223B
IP 데이터그램 B
IP 페이로드
1201A
SDNP
네트워크
테스크탑 전화
회사 스위치보드
1A
24
NSP
9
7A
8A
4
PSTN
SDNP
게이트웨이
개인 인증
1225
SDNP 콜 아웃
* 미보안 통신
* 인증
* 준-프라이빗
* 계정 ID 알려짐
1222A
SDNP 데이터그램 A
SDNP 페이로드

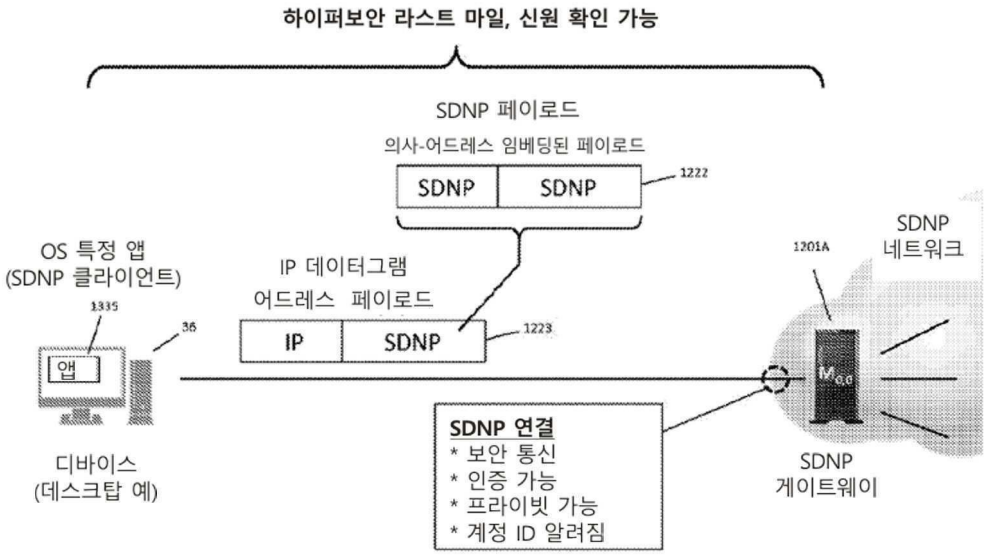
도면15


미보안 라스트 마일, 신원 확인됨
로그인 창 보안 토큰
1223C
IP 데이터그램 B
IP 페이로드
1223B
IP 데이터그램 B
IP 페이로드
1201A
SDNP
네트워크
1226
1227
36
106A
이더넷
27B
24A
ISP
27
네트워크
라우터
24
NSP
SDNP
게이트웨이
1223D
IP 데이터그램 B
IP 페이로드
SDNP 콜 아웃
* 미보안 통신
* 인증
* 준-프라이빗
* 계정 ID 알려짐
1222A
SDNP 데이터그램 A
SDNP 페이로드

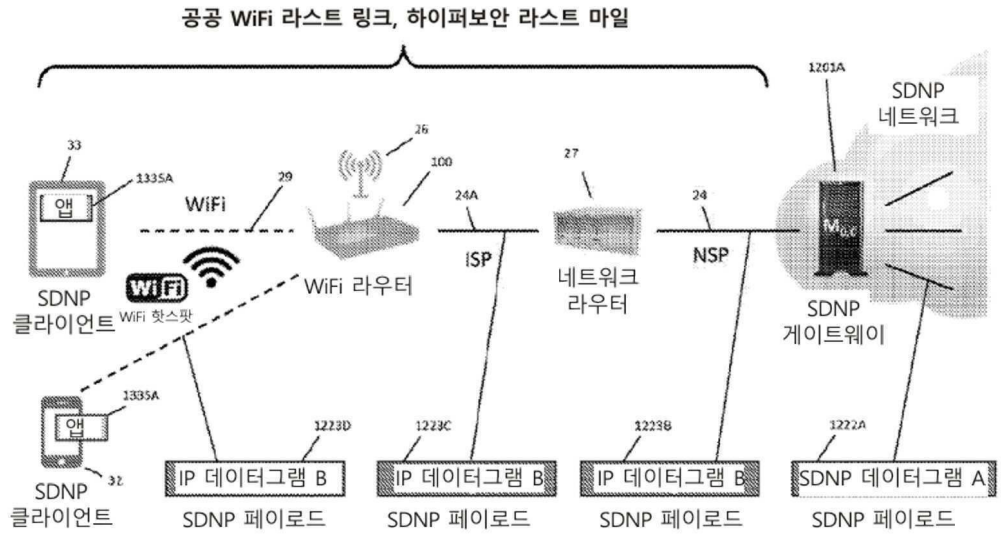
도면16


미보안 라스트 마일, 신원 확인됨
1221A
아날로그 호출
디지털 PCM
1230
재정 인증
38A
1223B
IP 데이터그램 B
IP 페이로드
1201A
SDNP
네트워크
3A
24A
27
24
NSP
은행 카드
PIN
1228
PSTN 브릿지
네트워크 라우터
SDNP
게이트웨이
1229
30B
38
1223C
IP 데이터그램 B
IP 페이로드
SDNP 콜 아웃(데이터)
* 미보안 통신
* 인증
* 준-프라이빗
* 사용자 ID 알려짐
1222A
SDNP 데이터그램 A
SDNP 페이로드

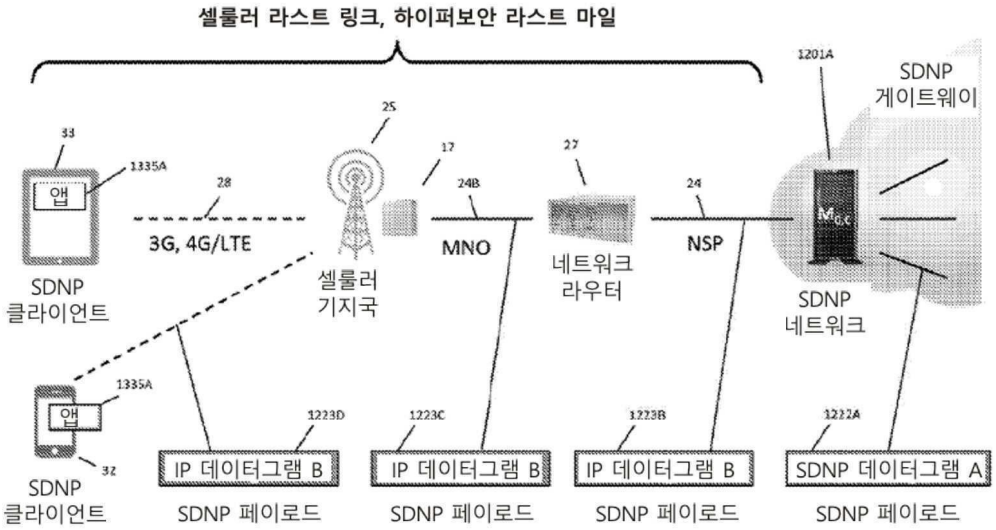
도면17


하이퍼보안 라스트 마일, 신원 확인 가능
SDNP 페이로드
의사-어드레스 임베딩된 페이로드
SDNP
SDNP
1222
OS 특정 앱
(SDNP 클라이언트)
IP 데이터그램
어드레스 페이로드
IP
SDNP
1223
1335
36
앱
디바이스
(데스크탑 예)
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
1201A
SDNP
네트워크
SDNP
게이트웨이

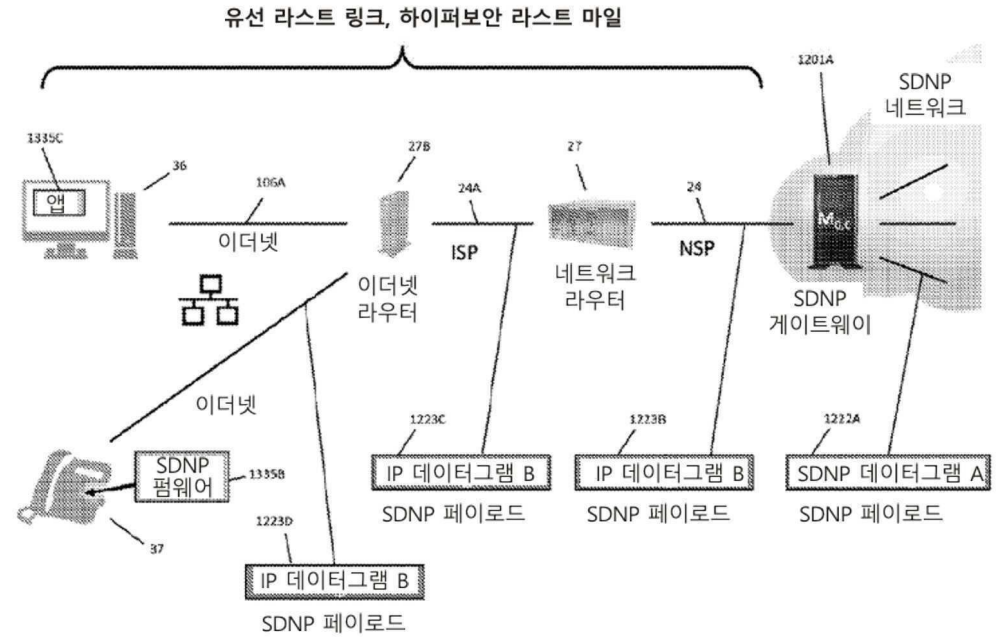
도면18


공공 WiFi 라스트 링크, 하이퍼보안 라스트 마일
1201A
SDNP
네트워크
33
1335A
앱
SDNP
클라이언트
WiFi
29
WiFi 핫스팟
26
100
WiFi 라우터
24A
ISP
27
네트워크
라우터
24
NSP
SDNP
게이트웨이
1335A
앱
32
SDNP
클라이언트
1223D
IP 데이터그램 B
SDNP 페이로드
1223C
IP 데이터그램 B
SDNP 페이로드
1223B
IP 데이터그램 B
SDNP 페이로드
1222A
SDNP 데이터그램 A
SDNP 페이로드

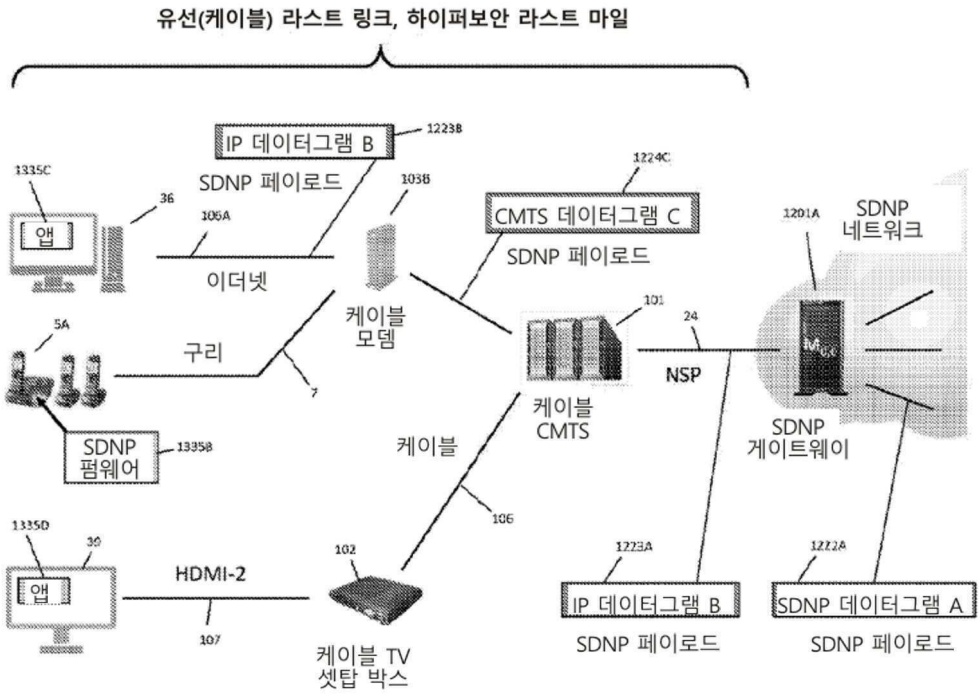
도면19


셀룰러 라스트 링크, 하이퍼보안 라스트 마일
33
1335A
앱
SDNP
클라이언트
28
3G, 4G/LTE
25
셀룰러
기지국
17
24B
MNO
27
네트워크
라우터
24
NSP
1201A
SDNP
게이트웨이
SDNP
네트워크
1335A
앱
32
SDNP
클라이언트
1223D
IP 데이터그램 B
SDNP 페이로드
1223C
IP 데이터그램 B
SDNP 페이로드
1223B
IP 데이터그램 B
SDNP 페이로드
1222A
SDNP 데이터그램 A
SDNP 페이로드

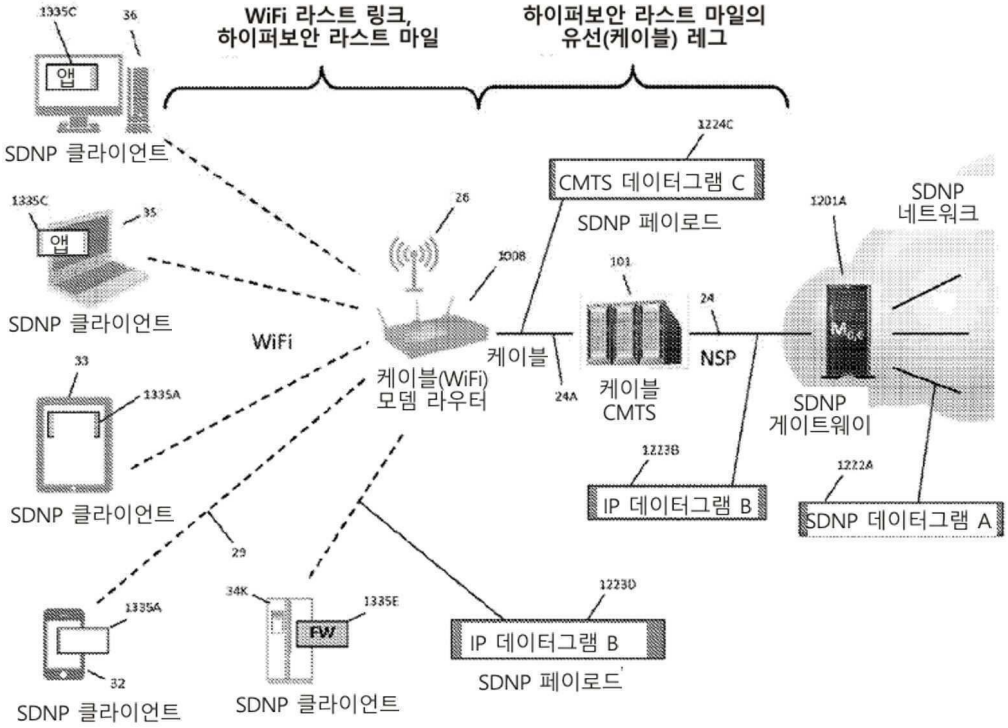
도면20


유선 라스트 링크, 하이퍼보안 라스트 마일
1335C
앱
36
106A
이더넷
27B
24A
ISP
27
네트워크
라우터
24
NSP
1201A
SDNP
네트워크
SDNP
게이트웨이
이더넷
라우터
이더넷
SDNP
펌웨어
1335B
37
1223D
IP 데이터그램 B
SDNP 페이로드
1223C
IP 데이터그램 B
SDNP 페이로드
1223B
IP 데이터그램 B
SDNP 페이로드
1222A
SDNP 데이터그램 A
SDNP 페이로드

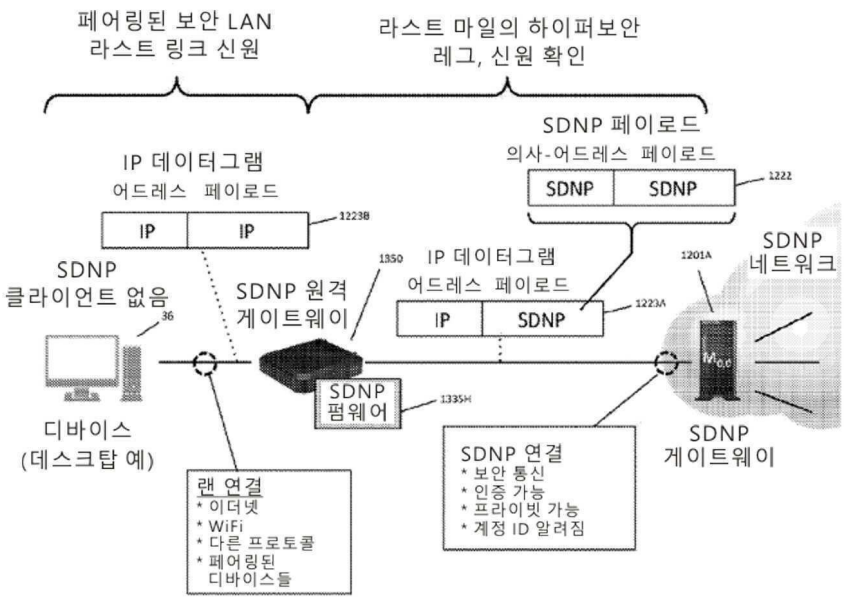
도면21


유선(케이블) 라스트 링크, 하이퍼보안 라스트 마일
IP 데이터그램 B
1223B
SDNP 페이로드
1335C
앱
36
106A
이더넷
1038
케이블
모뎀
CMTS 데이터그램 C
1224C
SDNP 페이로드
1201A
SDNP
네트워크
5A
구리
7
SDNP
펌웨어
1335B
케이블
106
101
24
NSP
케이블
CMTS
SDNP
게이트웨이
1335D
30
앱
HDMI-2
107
102
케이블 TV
셋탑 박스
1223A
IP 데이터그램 B
SDNP 페이로드
1222A
SDNP 데이터그램 A
SDNP 페이로드

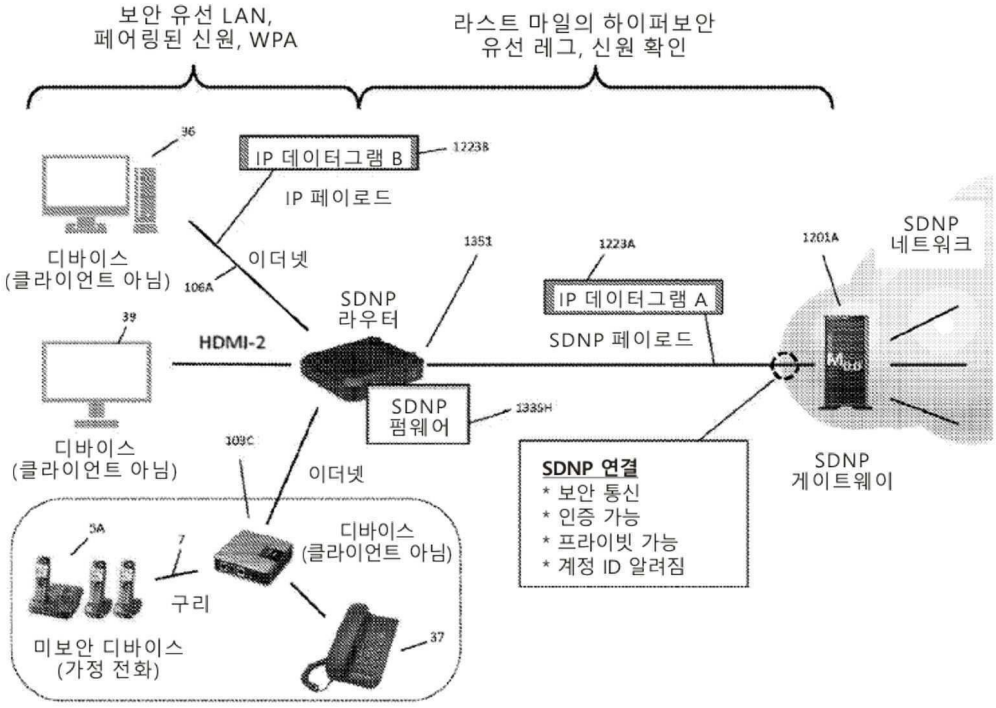
도면22


WiFi 라스트 링크,
하이퍼보안 라스트 마일
하이퍼보안 라스트 마일의
유선(케이블) 레그
1335C
36
앱
SDNP 클라이언트
1224C
CMTS 데이터그램 C
SDNP 페이로드
1201A
SDNP
네트워크
1335C
35
앱
SDNP 클라이언트
26
1008
WiFi
케이블(WiFi)
모뎀 라우터
케이블
24A
101
24
NSP
케이블
CMTS
SDNP
게이트웨이
33
1335A
SDNP 클라이언트
1223B
IP 데이터그램 B
1222A
SDNP 데이터그램 A
29
1335A
32
SDNP 클라이언트
34K
1335E
FW
SDNP 클라이언트
1223D
IP 데이터그램 B
SDNP 페이로드

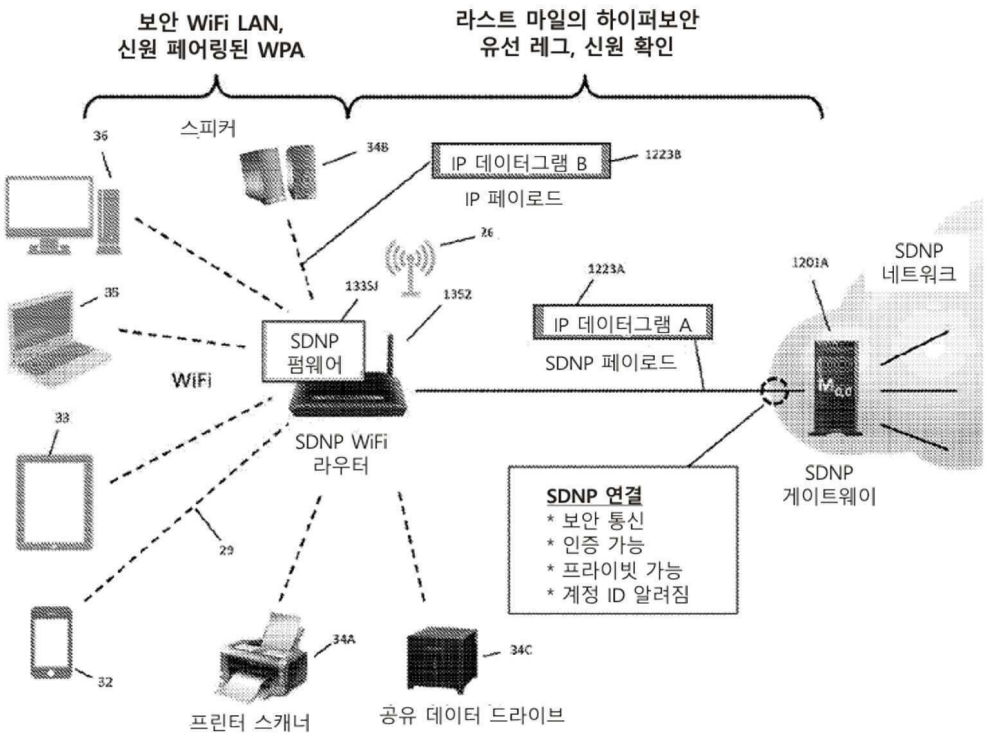
도면23


페어링된 보안 LAN
라스트 링크 신원
라스트 마일의 하이퍼보안
레그, 신원 확인
SDNP 페이로드
의사-어드레스 페이로드
SDNP
SDNP
1222
IP 데이터그램
어드레스 페이로드
IP
IP
1223B
SDNP
클라이언트 없음
36
SDNP 원격
게이트웨이
1350
IP 데이터그램
어드레스 페이로드
IP
SDNP
1223A
1201A
SDNP
네트워크
SDNP
펌웨어
1335H
디바이스
(데스크탑 예)
랜 연결
* 이더넷
* WiFi
* 다른 프로토콜
* 페어링된
디바이스들
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
SDNP
게이트웨이

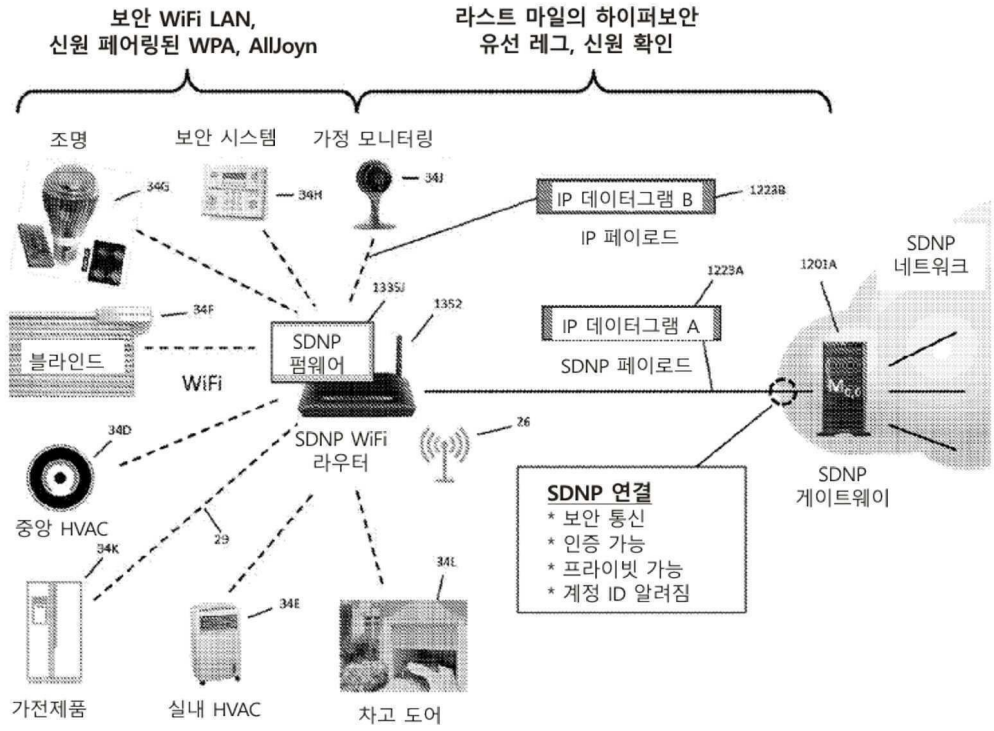
도면24


보안 유선 LAN,
페어링된 신원, WPA
라스트 마일의 하이퍼보안
유선 레그, 신원 확인
36
IP 데이터그램 B
1223B
IP 페이로드
디바이스
(클라이언트 아님)
이더넷
106A
1351
1223A
SDNP
라우터
IP 데이터그램 A
SDNP 페이로드
1201A
SDNP
네트워크
39
HDMI-2
SDNP
펌웨어
1335H
디바이스
(클라이언트 아님)
109C
이더넷
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
SDNP
게이트웨이
5A
7
구리
디바이스
(클라이언트 아님)
미보안 디바이스
(가정 전화)
37

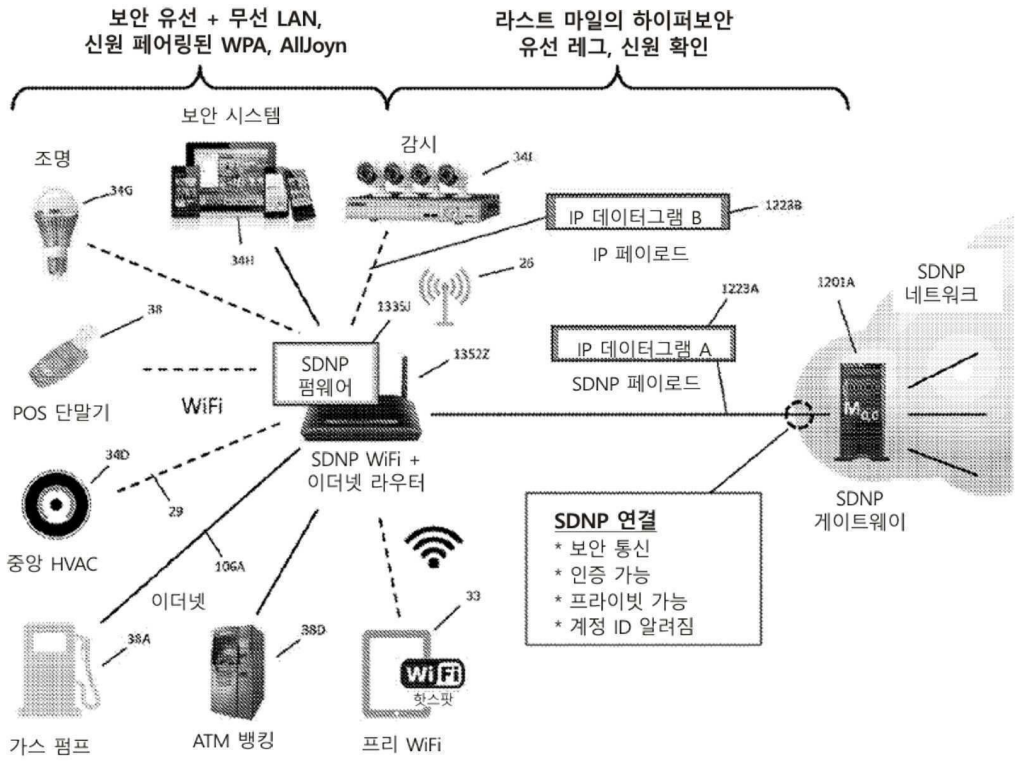
도면25


보안 WiFi LAN,
신원 페어링된 WPA
라스트 마일의 하이퍼보안
유선 레그, 신원 확인
스피커
36
34B
IP 데이터그램 B
1223B
IP 페이로드
26
1335J
1352
35
SDNP
펌웨어
WiFi
1223A
IP 데이터그램 A
SDNP 페이로드
1201A
SDNP
네트워크
33
SDNP WiFi
라우터
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
SDNP
게이트웨이
29
32
34A
34C
프린터 스캐너
공유 데이터 드라이브

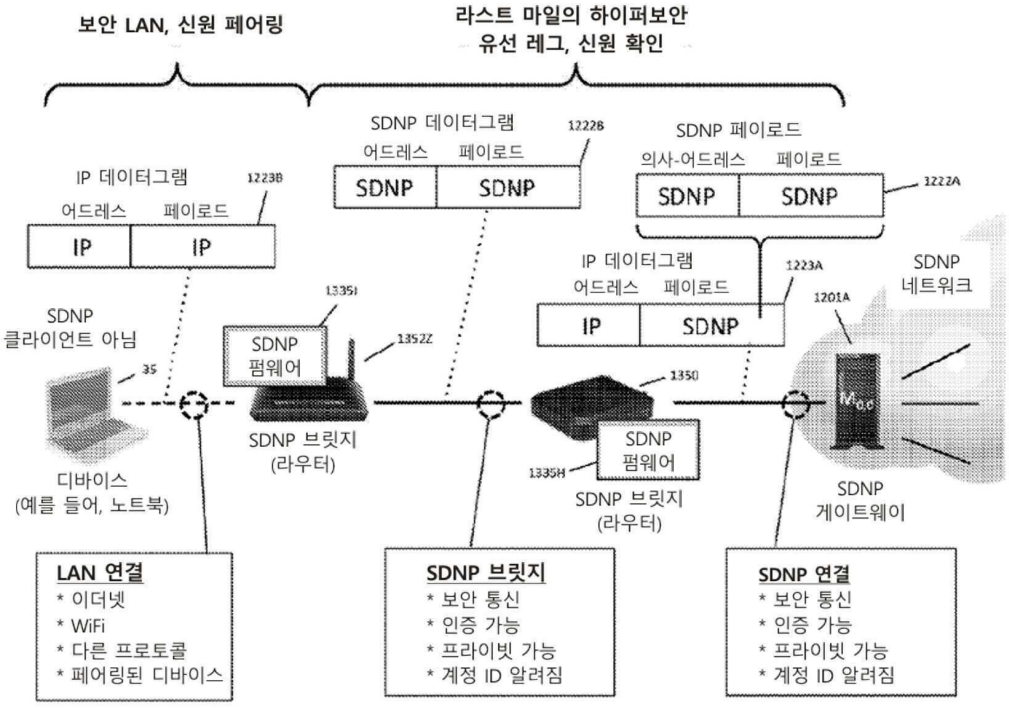
도면26


보안 WiFi LAN,
신원 페어링된 WPA, AllJoyn
라스트 마일의 하이퍼보안
유선 레그, 신원 확인
조명
보안 시스템
가정 모니터링
34G
34H
34J
IP 데이터그램 B
1223B
IP 페이로드
1223A
1201A
SDNP
네트워크
1335J
1352
34F
블라인드
WiFi
SDNP
펌웨어
IP 데이터그램 A
SDNP 페이로드
34D
26
SDNP WiFi
라우터
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
SDNP
게이트웨이
중앙 HVAC
29
34K
34E
34L
가전제품
실내 HVAC
차고 도어

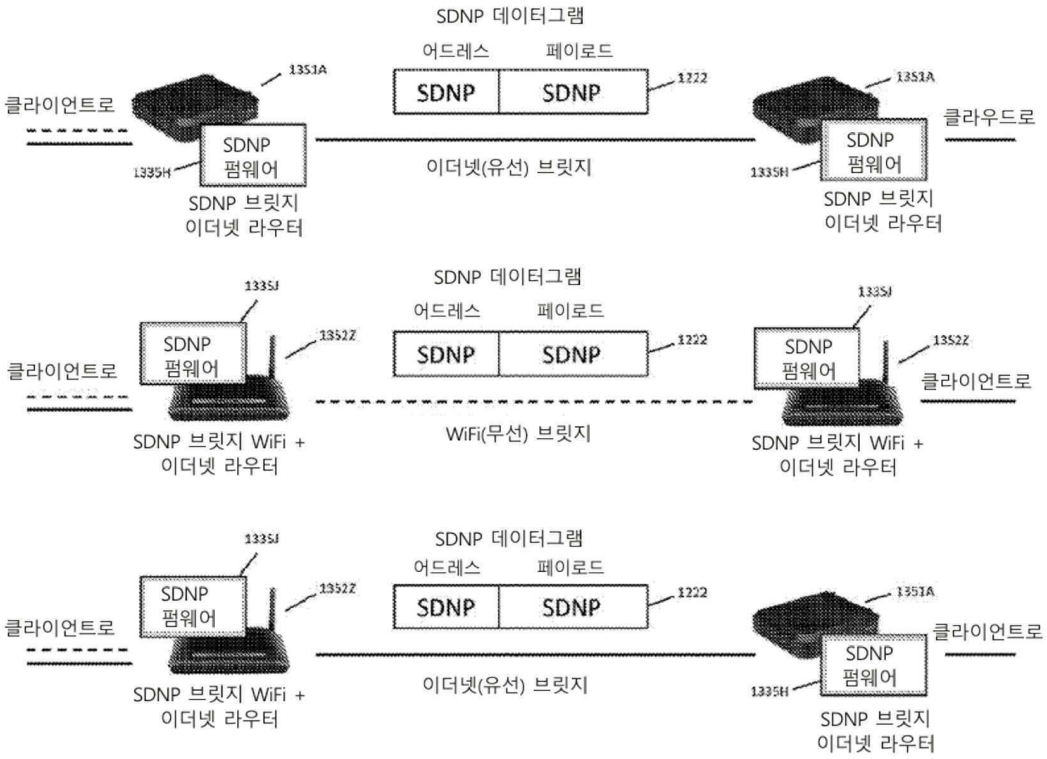
도면27


보안 유선 + 무선 LAN,
신원 페어링된 WPA, AllJoyn
라스트 마일의 하이퍼보안
유선 레그, 신원 확인
보안 시스템
조명
감시
IP 데이터그램 B
IP 페이로드
SDNP
네트워크
SDNP
펌웨어
WiFi
POS 단말기
IP 데이터그램 A
SDNP 페이로드
SDNP WiFi +
이더넷 라우터
SDNP
게이트웨이
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
중앙 HVAC
이더넷
가스 펌프
ATM 뱅킹
프리 WiFi
WiFi
핫스팟

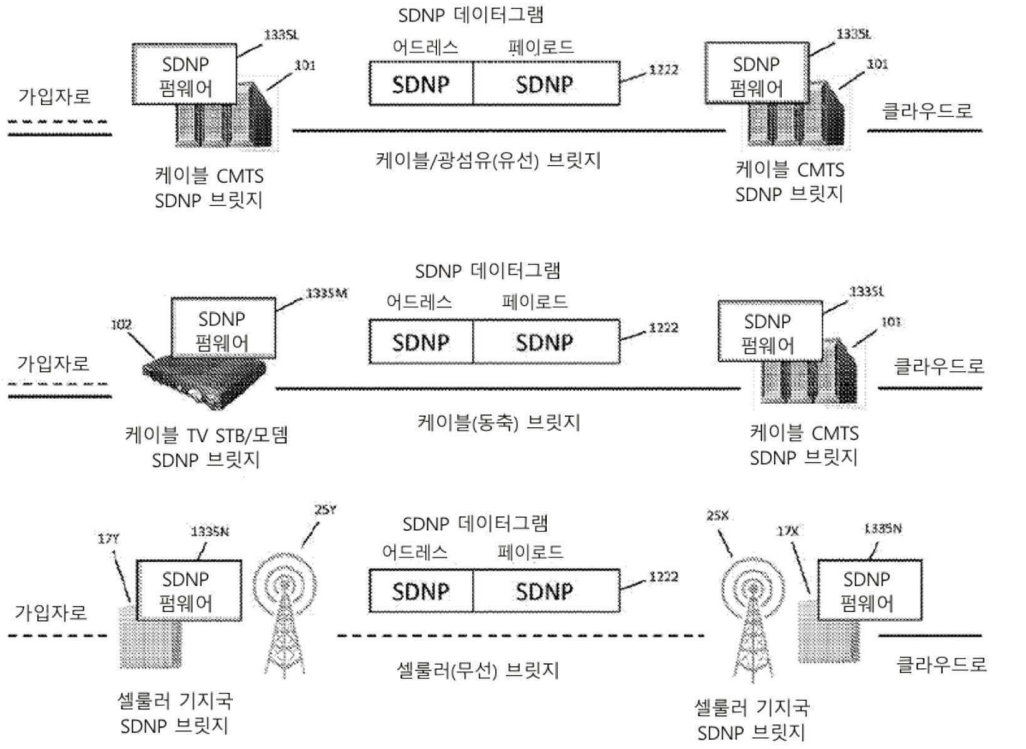
도면28


보안 LAN, 신원 페어링
라스트 마일의 하이퍼보안
유선 레그, 신원 확인
SDNP 데이터그램
어드레스 페이로드
SDNP SDNP
SDNP 페이로드
의사-어드레스 페이로드
SDNP SDNP
IP 데이터그램
어드레스 페이로드
IP IP
IP 데이터그램
어드레스 페이로드
IP SDNP
SDNP
네트워크
SDNP
클라이언트 아님
SDNP
펌웨어
SDNP 브릿지
(라우터)
SDNP
펌웨어
SDNP 브릿지
(라우터)
SDNP
게이트웨이
디바이스
(예를 들어, 노트북)
LAN 연결
* 이더넷
* WiFi
* 다른 프로토콜
* 페어링된 디바이스
SDNP 브릿지
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐
SDNP 연결
* 보안 통신
* 인증 가능
* 프라이빗 가능
* 계정 ID 알려짐

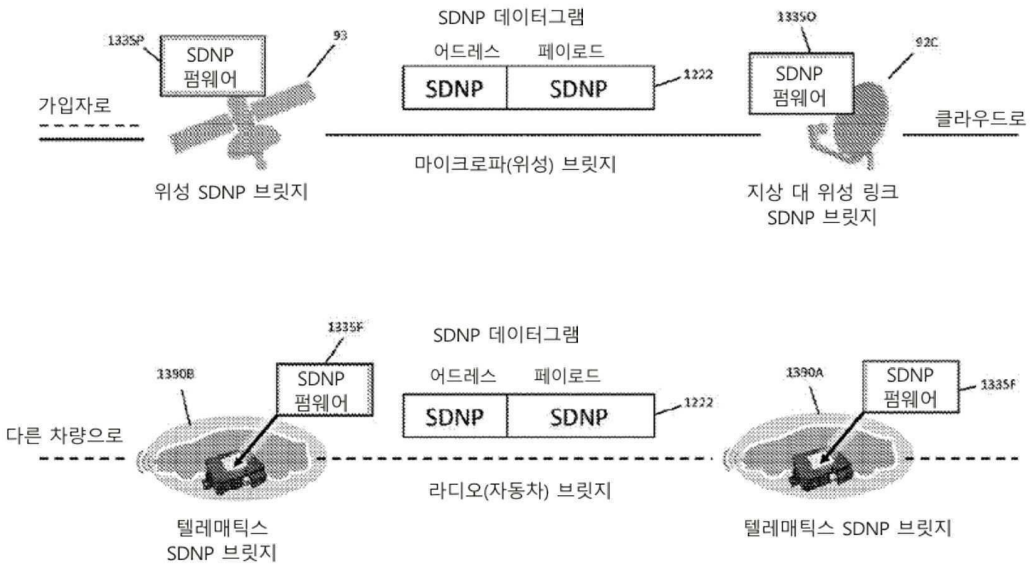
도면29a


SDNP 데이터그램
어드레스
페이로드
SDNP
SDNP
1222
클라이언트로
SDNP
펌웨어
1335H
1351A
SDNP 브릿지
이더넷 라우터
이더넷(유선) 브릿지
클라우드로
1335J
1352Z
SDNP 브릿지 WiFi +
이더넷 라우터
WiFi(무선) 브릿지

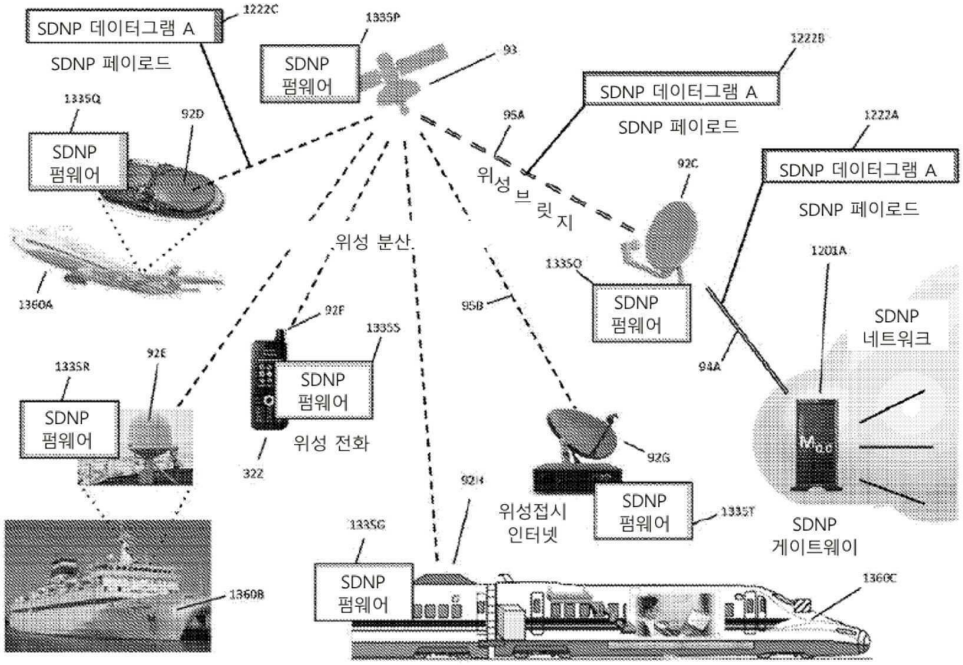
도면29b


SDNP 데이터그램
어드레스
페이로드
SDNP
SDNP
1222
가입자로
SDNP
펌웨어
1335L
101
케이블 CMTS
SDNP 브릿지
케이블/광섬유(유선) 브릿지
클라우드로
1335M
102
케이블 TV STB/모뎀
SDNP 브릿지
케이블(동축) 브릿지
1335N
17Y
25Y
셀룰러 기지국
SDNP 브릿지
셀룰러(무선) 브릿지
25X
17X

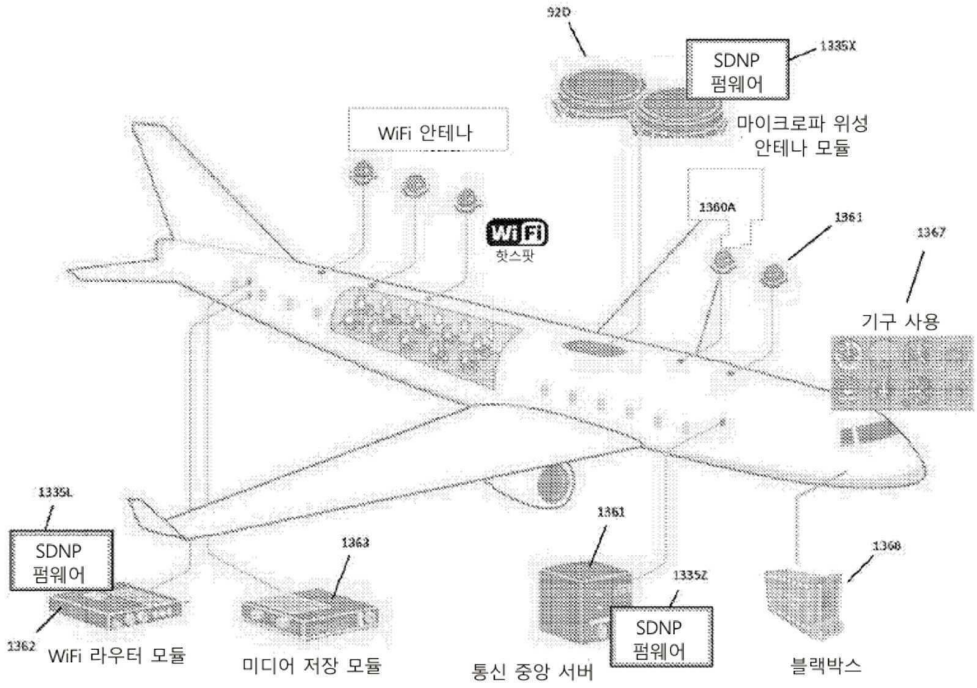
도면29c


SDNP 데이터그램
어드레스
페이로드
SDNP
SDNP
1222
SDNP
펌웨어
1335P
93
가입자로
위성 SDNP 브릿지
마이크로파(위성) 브릿지
1335O
92C
SDNP
펌웨어
클라우드로
지상 대 위성 링크
SDNP 브릿지
SDNP 데이터그램
어드레스
페이로드
SDNP
SDNP
1222
SDNP
펌웨어
1335F
1390B
다른 차량으로
텔레매틱스
SDNP 브릿지
라디오(자동차) 브릿지
1390A
SDNP
펌웨어
1335F
텔레매틱스 SDNP 브릿지

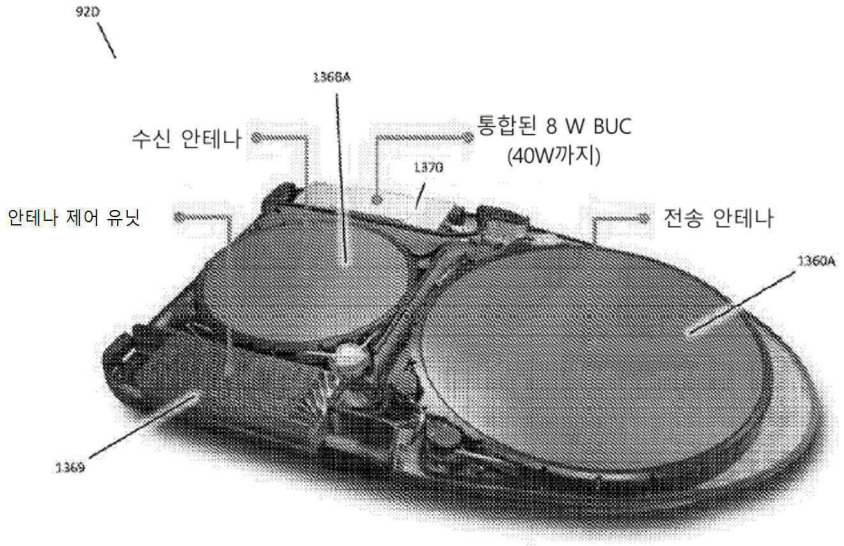
도면30


SDNP 데이터그램 A
1222C
SDNP 페이로드
SDNP
펌웨어
1335P
93
1335Q
92D
SDNP
펌웨어
1360A
위성 분산
95A
위성 브릿지
SDNP 데이터그램 A
1222B
SDNP 페이로드
92C
1335O
SDNP
펌웨어
95B
SDNP 데이터그램 A
1222A
SDNP 페이로드
1201A
SDNP
네트워크
94A
92F
1335S
SDNP
펌웨어
위성 전화
322
1335R
92E
SDNP
펌웨어
1360B
92G
위성접시
인터넷
92H
SDNP
펌웨어
1335T
SDNP
게이트웨이
1335G
SDNP
펌웨어
1360C

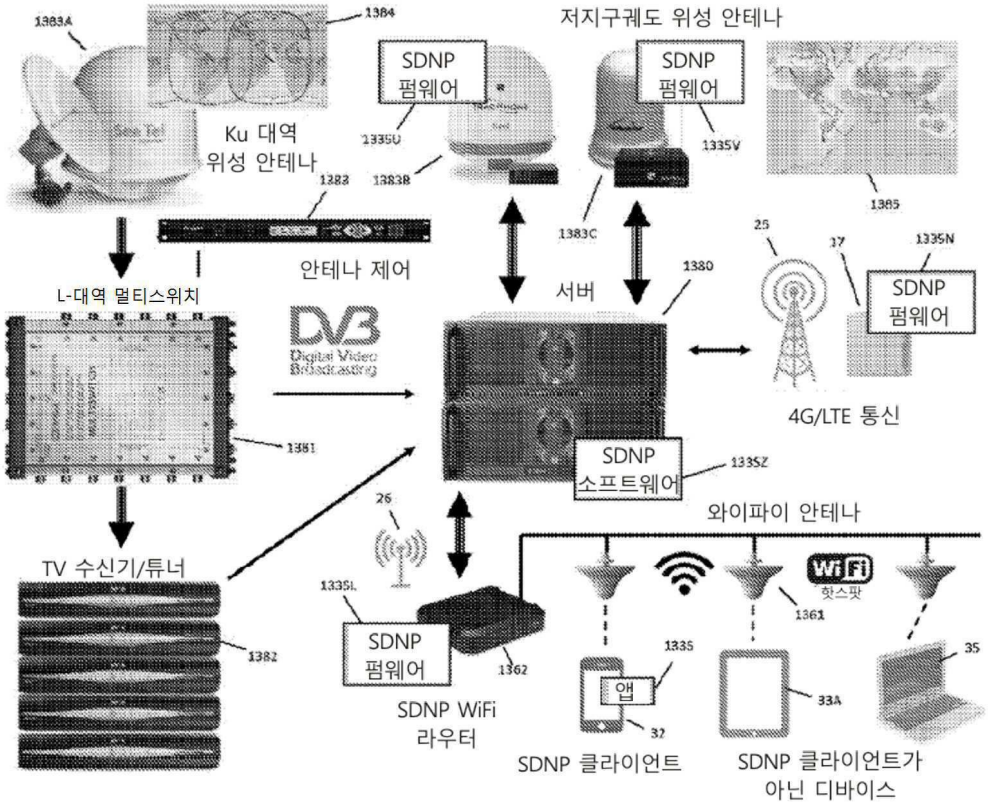
도면31a


92D
1335X
SDNP
펌웨어
WiFi 안테나
마이크로파 위성
안테나 모듈
1360A
1361
1367
WiFi
핫스팟
기구 사용
1335L
SDNP
펌웨어
1363
1361
1368
1335Z
SDNP
펌웨어
1362
WiFi 라우터 모듈
미디어 저장 모듈
통신 중앙 서버
블랙박스

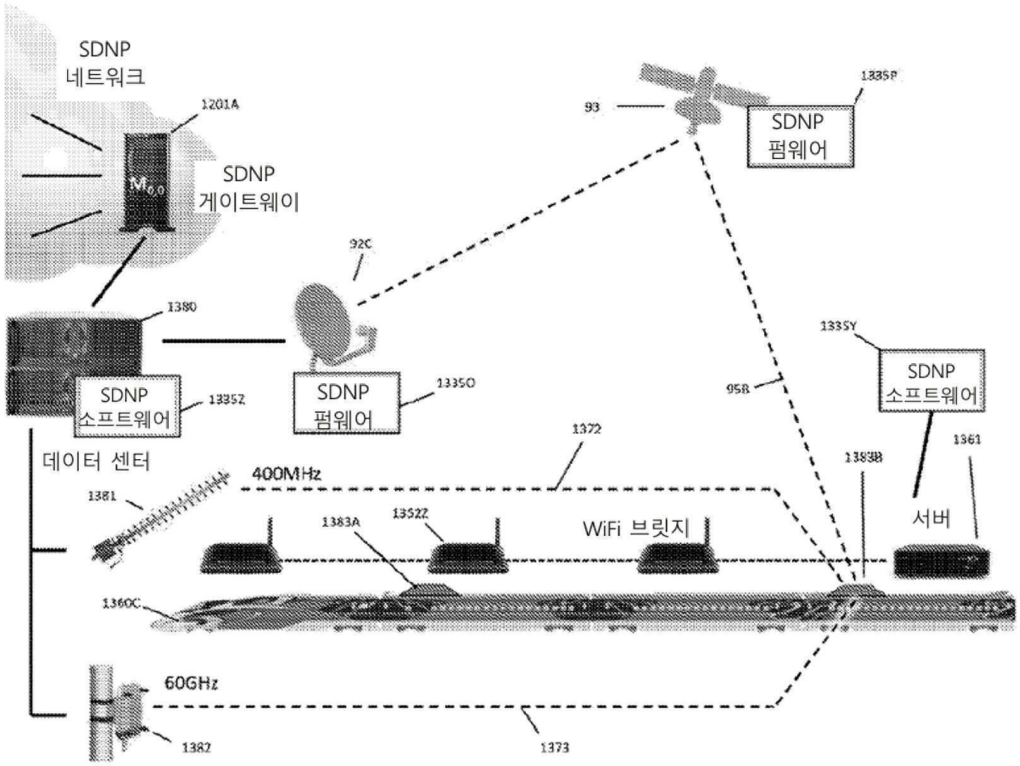
도면31b


92D
1368A
수신 안테나
통합된 8 W BUC
(40W까지)
1370
안테나 제어 유닛
전송 안테나
1360A
1369

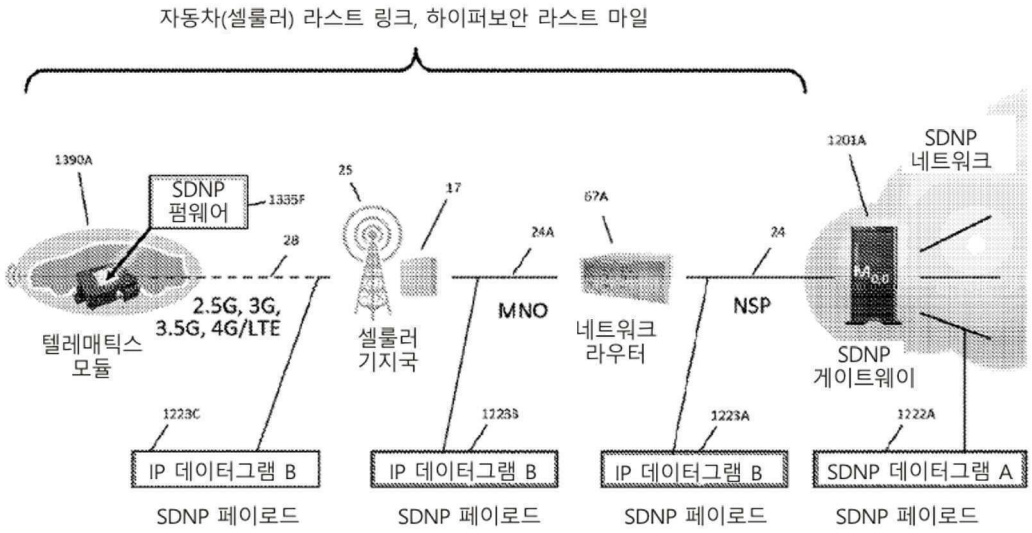
도면32


저지구궤도 위성 안테나
SDNP 펌웨어
SDNP 펌웨어
Ku 대역 위성 안테나
안테나 제어
L-대역 멀티스위치
서버
SDNP 펌웨어
4G/LTE 통신
SDNP 소프트웨어
와이파이 안테나
TV 수신기/튜너
SDNP 펌웨어
SDNP WiFi 라우터
앱
SDNP 클라이언트
SDNP 클라이언트가 아닌 디바이스
WiFi
핫스팟

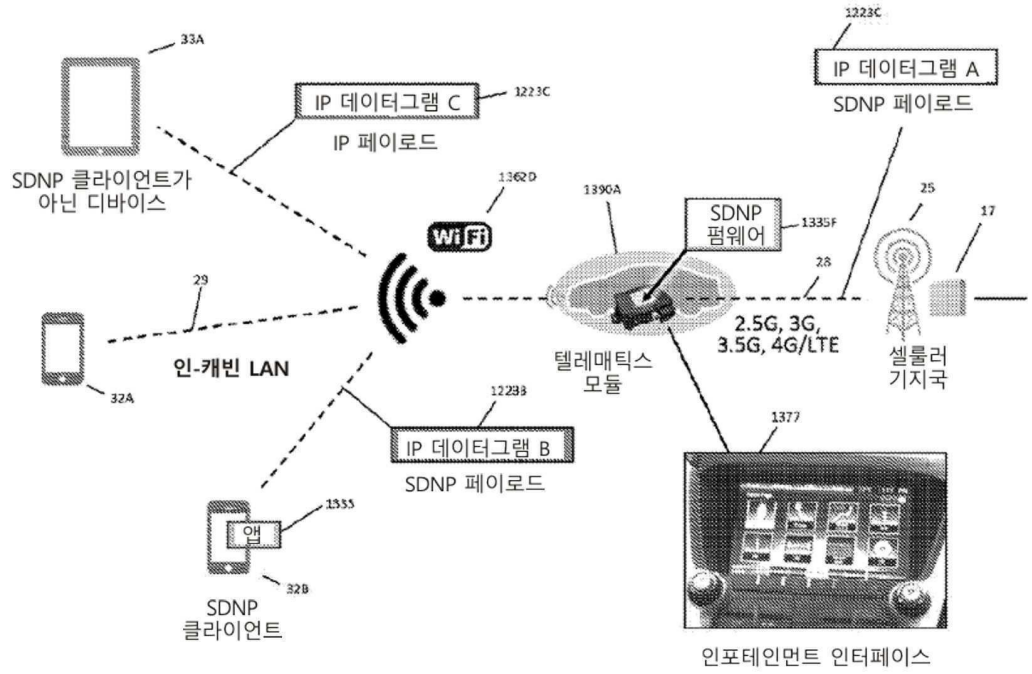
도면33


SDNP 네트워크
SDNP 게이트웨이
SDNP 펌웨어
SDNP 소프트웨어
SDNP 펌웨어
SDNP 소프트웨어
데이터 센터
400MHz
WiFi 브릿지
서버
60GHz

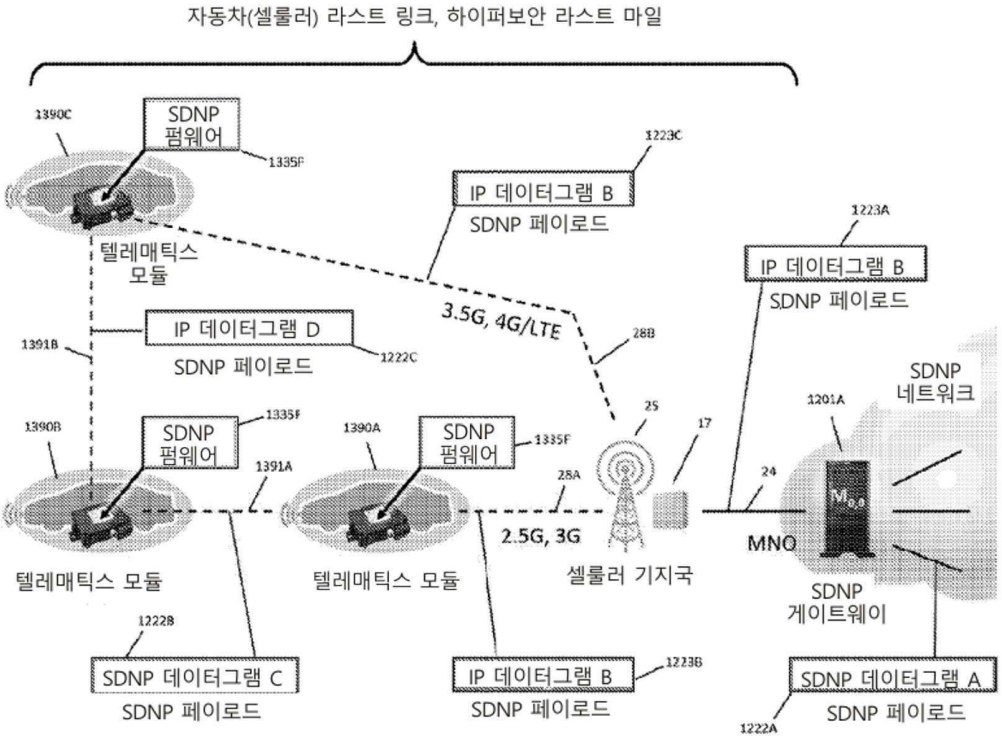
도면34


자동차(셀룰러) 라스트 링크, 하이퍼보안 라스트 마일
1390A
SDNP
펌웨어
1335F
28
2.5G, 3G,
3.5G, 4G/LTE
텔레매틱스
모듈
25
17
셀룰러
기지국
24A
MNO
67A
네트워크
라우터
24
NSP
1201A
SDNP
네트워크
SDNP
게이트웨이
1223C
IP 데이터그램 B
SDNP 페이로드
1223B
IP 데이터그램 B
SDNP 페이로드
1223A
IP 데이터그램 B
SDNP 페이로드
1222A
SDNP 데이터그램 A
SDNP 페이로드

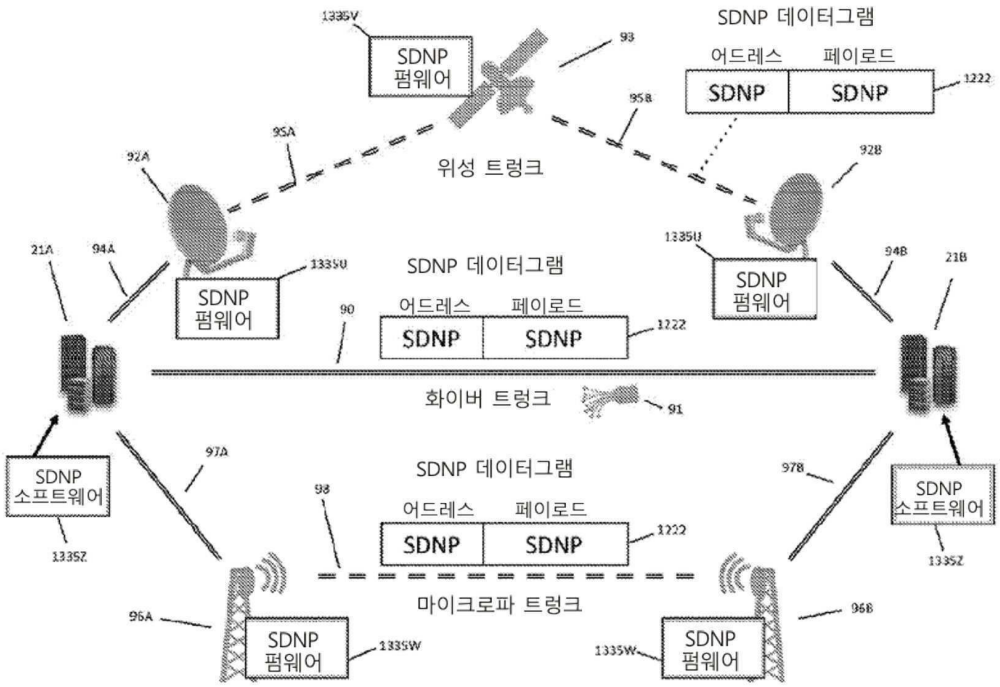
도면35


33A
SDNP 클라이언트가
아닌 디바이스
IP 데이터그램 C
1223C
IP 페이로드
1362D
WiFi
29
인-캐빈 LAN
32A
1390A
SDNP
펌웨어
1335F
28
2.5G, 3G,
3.5G, 4G/LTE
텔레매틱스
모듈
25
17
셀룰러
기지국
1223C
IP 데이터그램 A
SDNP 페이로드
1223B
IP 데이터그램 B
SDNP 페이로드
1377
인포테인먼트 인터페이스
1333
앱
32B
SDNP
클라이언트

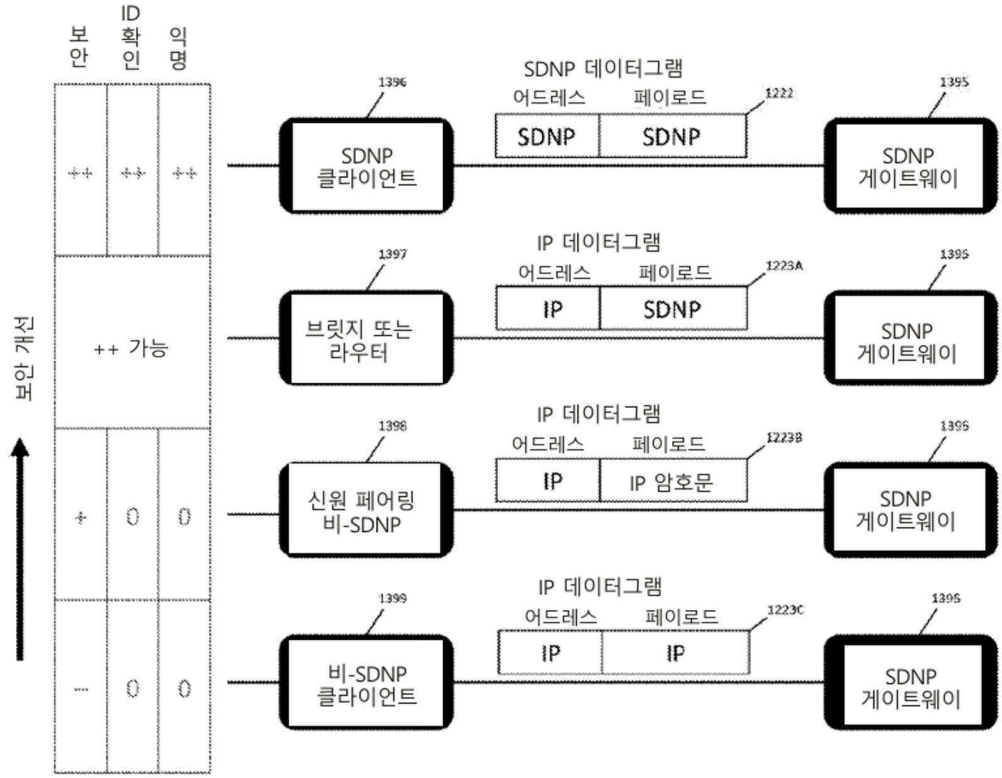
도면36


자동차(셀룰러) 라스트 링크, 하이퍼보안 라스트 마일
SDNP 펌웨어
텔레매틱스 모듈
IP 데이터그램 B
SDNP 페이로드
IP 데이터그램 D
SDNP 페이로드
3.5G, 4G/LTE
2.5G, 3G
셀룰러 기지국
MNO
SDNP 네트워크
SDNP 게이트웨이
SDNP 데이터그램 C
SDNP 데이터그램 A

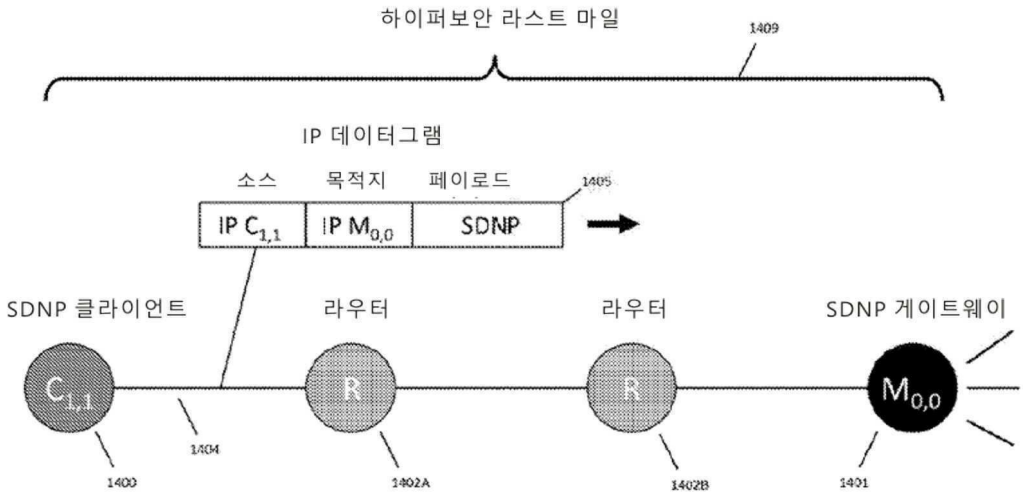
도면37


SDNP 펌웨어
SDNP 데이터그램
어드레스
페이로드
SDNP
위성 트렁크
화이버 트렁크
마이크로파 트렁크
SDNP 소프트웨어

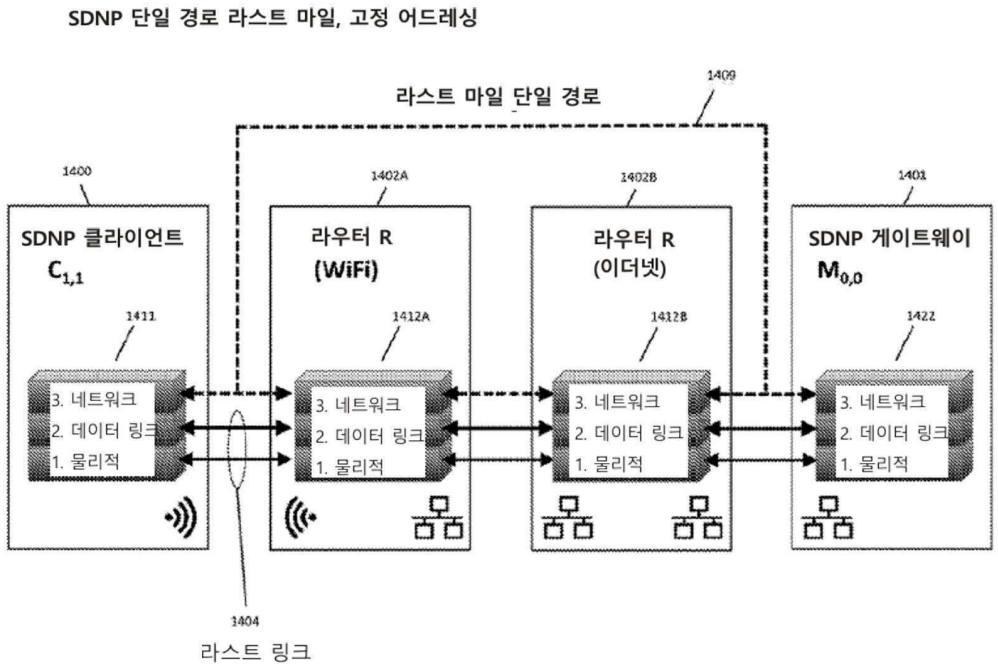
도면38


ID
보안
확인
익명
보안 개선
++
++
++
++ 가능
+
0
0
-
0
0
SDNP 데이터그램
어드레스
페이로드
SDNP
SDNP
1222
1396
SDNP 클라이언트
1395
SDNP 게이트웨이
IP 데이터그램
어드레스
페이로드
IP
SDNP
1223A
1397
브릿지 또는 라우터
1395
SDNP 게이트웨이
IP 데이터그램
어드레스
페이로드
IP
IP 암호문
1223B
1398
신원 페어링 비-SDNP
1395
SDNP 게이트웨이
IP 데이터그램
어드레스
페이로드
IP
IP
1223C
1399
비-SDNP 클라이언트
1395
SDNP 게이트웨이

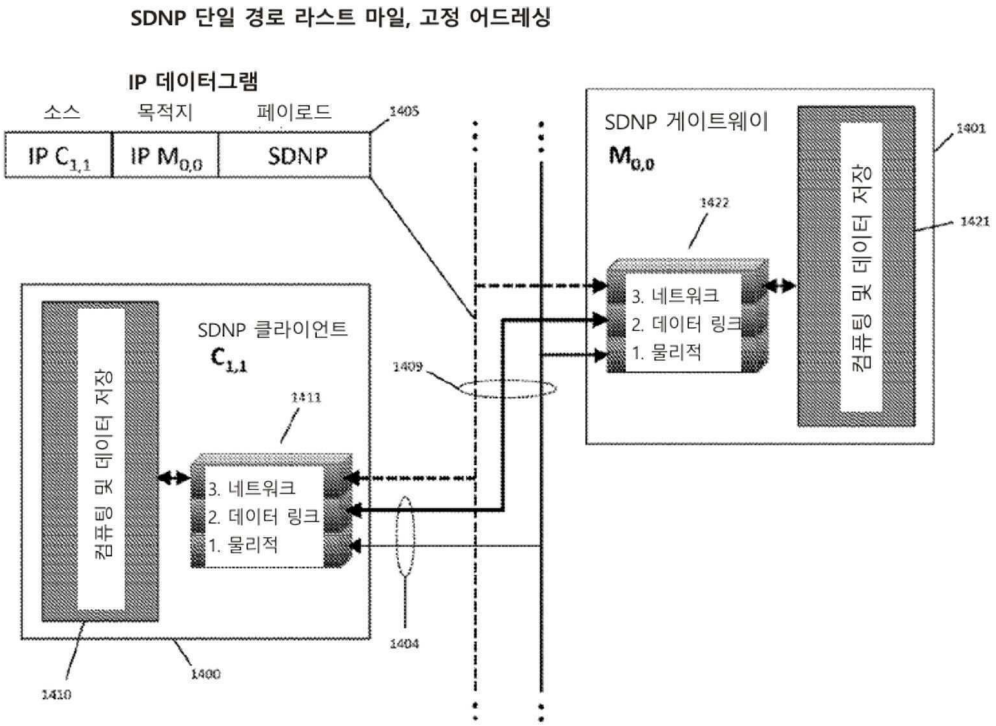
도면39


하이퍼보안 라스트 마일
1409
IP 데이터그램
소스
목적지
페이로드
1405
IP $C_{1,1}$
IP $M_{0,0}$
SDNP
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
$C_{1,1}$
R
R
$M_{0,0}$
1400
1404
1402A
1402B
1401

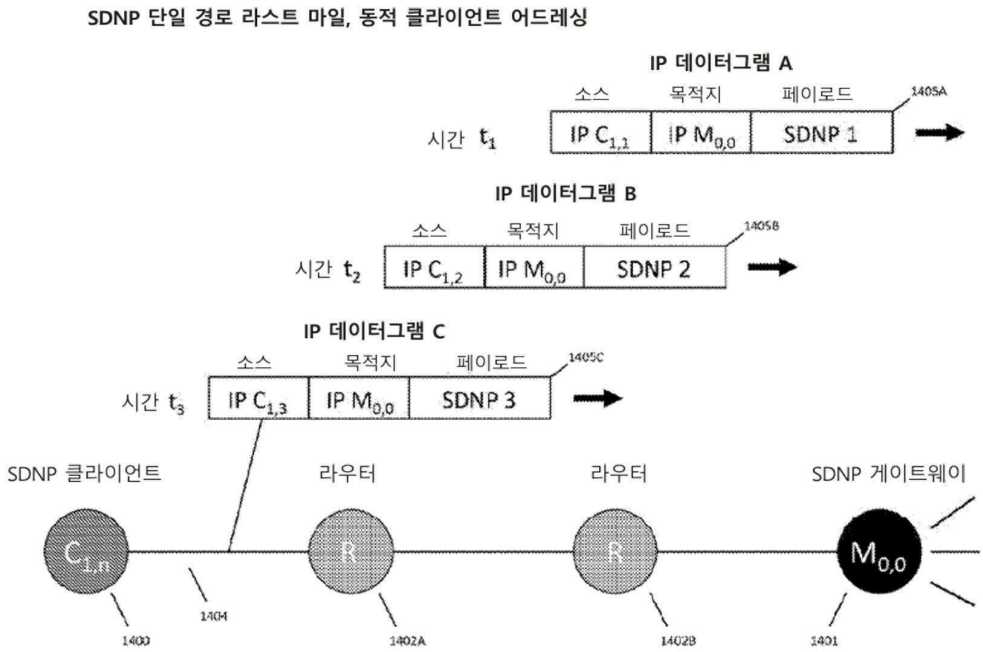
도면40a


SDNP 단일 경로 라스트 마일, 고정 어드레싱
라스트 마일 단일 경로
1409
1400
SDNP 클라이언트
C1,1
1402A
라우터 R
(WiFi)
1402B
라우터 R
(이더넷)
1401
SDNP 게이트웨이
M0,0
1411
1412A
1412B
1422
3. 네트워크
2. 데이터 링크
1. 물리적
1404
라스트 링크

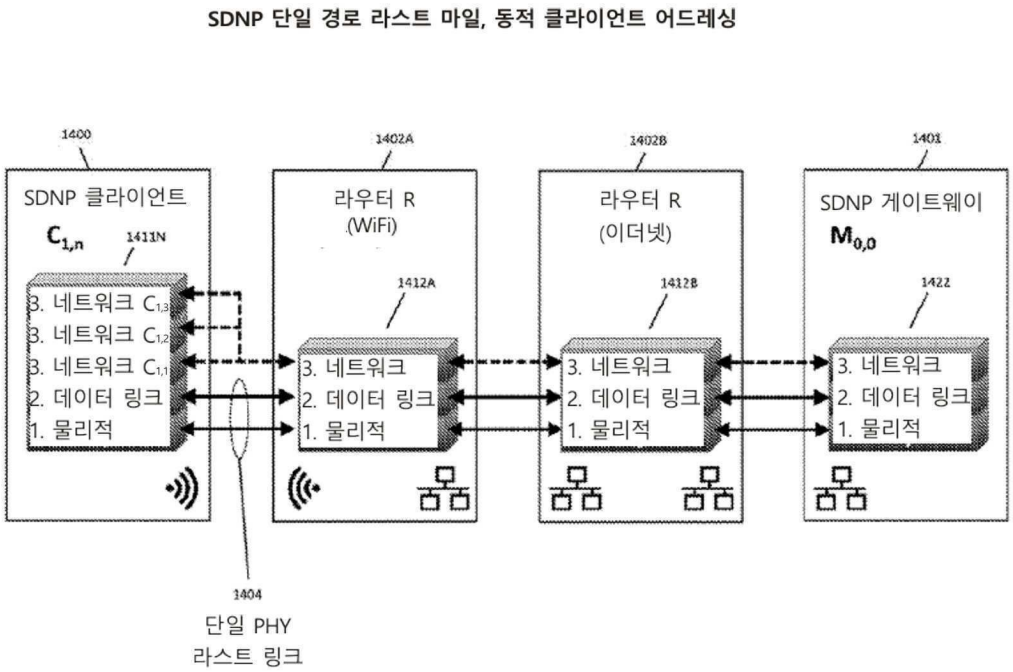
도면40b


SDNP 단일 경로 라스트 마일, 고정 어드레싱
IP 데이터그램
소스
목적지
페이로드
1405
IP C1,1
IP M0,0
SDNP
SDNP 게이트웨이
M0,0
1401
1422
1421
3. 네트워크
2. 데이터 링크
1. 물리적
컴퓨팅 및 데이터 저장
SDNP 클라이언트
C1,1
1409
1411
1404
1400
1410

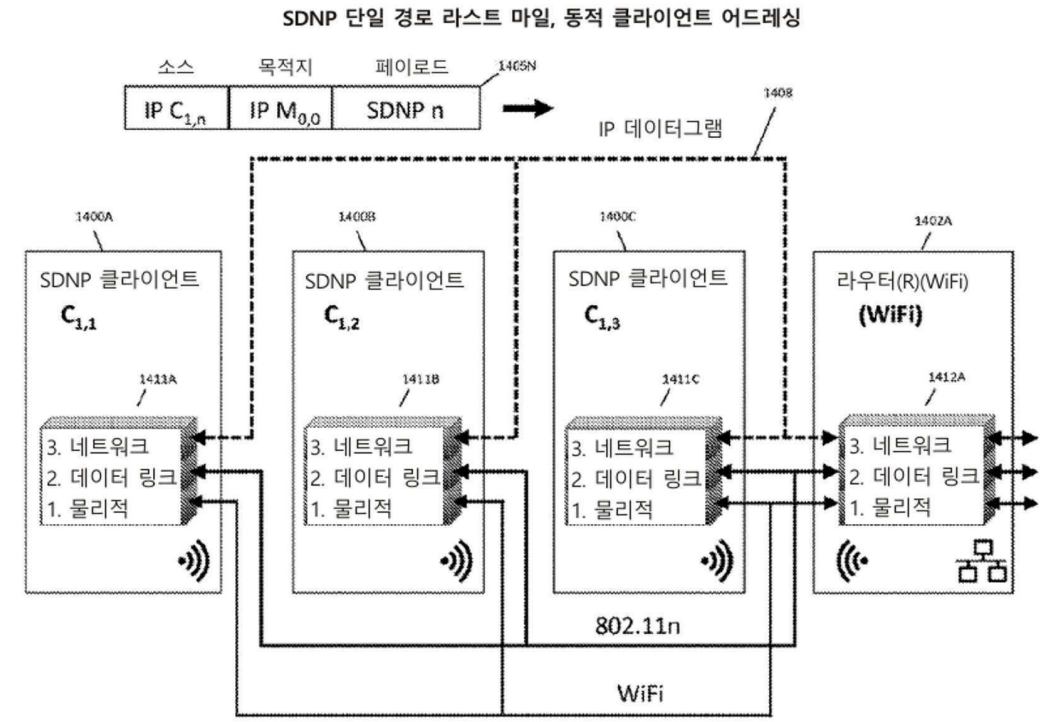
도면41


SDNP 단일 경로 라스트 마일, 동적 클라이언트 어드레싱
IP 데이터그램 A
소스
목적지
페이로드
1405A
시간 $t_1$
IP $C_{1,1}$
IP $M_{0,0}$
SDNP 1
IP 데이터그램 B
소스
목적지
페이로드
1405B
시간 $t_2$
IP $C_{1,2}$
IP $M_{0,0}$
SDNP 2
IP 데이터그램 C
소스
목적지
페이로드
1405C
시간 $t_3$
IP $C_{1,3}$
IP $M_{0,0}$
SDNP 3
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
$C_{1,n}$
R
R
$M_{0,0}$
1400
1404
1402A
1402B
1401

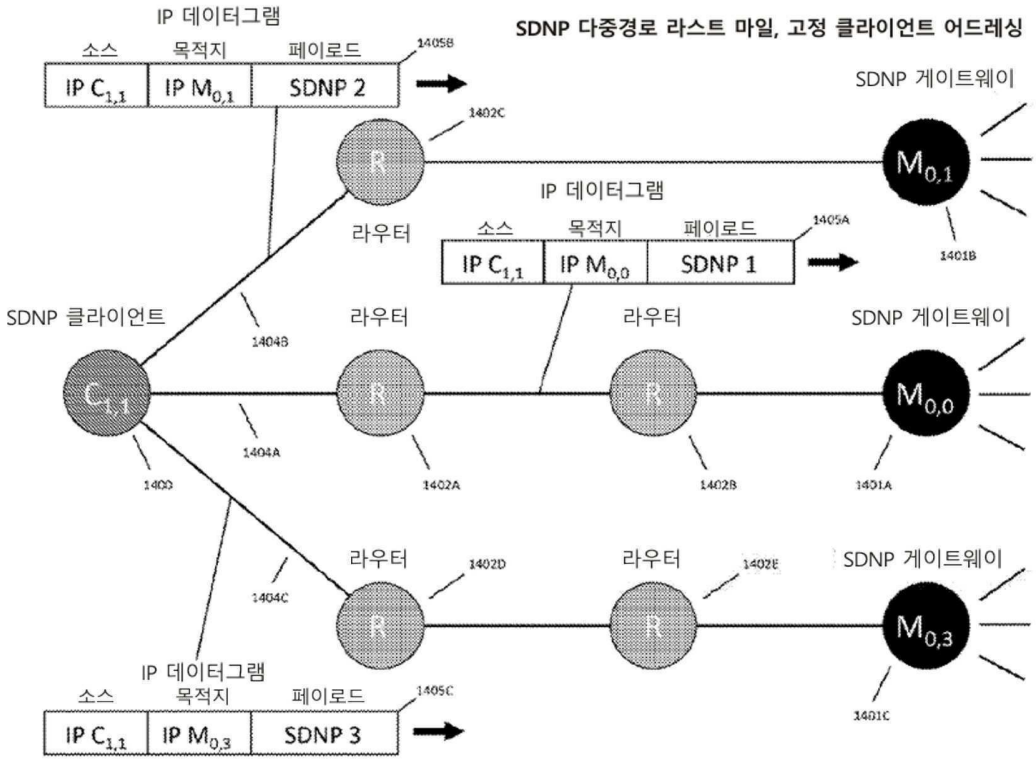
도면42a


SDNP 단일 경로 라스트 마일, 동적 클라이언트 어드레싱
1400
SDNP 클라이언트
$C_{1,n}$
1411N
3. 네트워크 $C_{1,3}$
3. 네트워크 $C_{1,2}$
3. 네트워크 $C_{1,1}$
2. 데이터 링크
1. 물리적
1402A
라우터 R
(WiFi)
1412A
3. 네트워크
2. 데이터 링크
1. 물리적
1402B
라우터 R
(이더넷)
1412B
3. 네트워크
2. 데이터 링크
1. 물리적
1401
SDNP 게이트웨이
$M_{0,0}$
1422
3. 네트워크
2. 데이터 링크
1. 물리적
1404
단일 PHY
라스트 링크

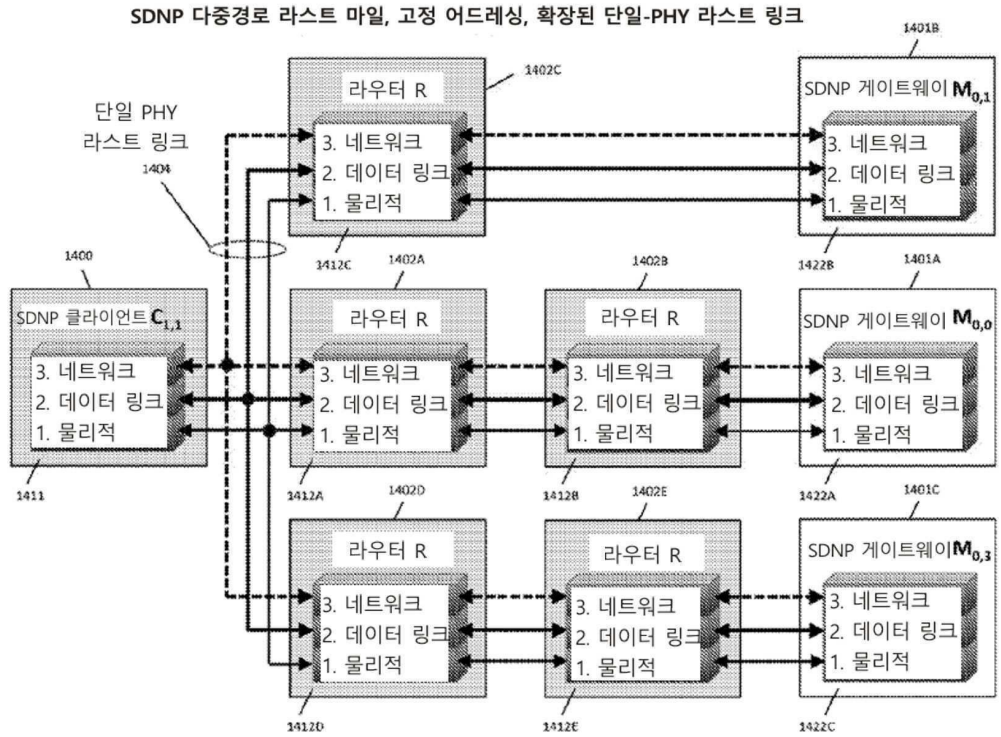
도면42b


SDNP 단일 경로 라스트 마일, 동적 클라이언트 어드레싱
소스
목적지
페이로드
1405N
IP $C_{1,n}$
IP $M_{0,0}$
SDNP n
IP 데이터그램
1408
1400A
1400B
1400C
1402A
SDNP 클라이언트
$C_{1,1}$
SDNP 클라이언트
$C_{1,2}$
SDNP 클라이언트
$C_{1,3}$
라우터(R)(WiFi)
(WiFi)
1413A
1411B
1411C
1412A
3. 네트워크
2. 데이터 링크
1. 물리적
802.11n
WiFi

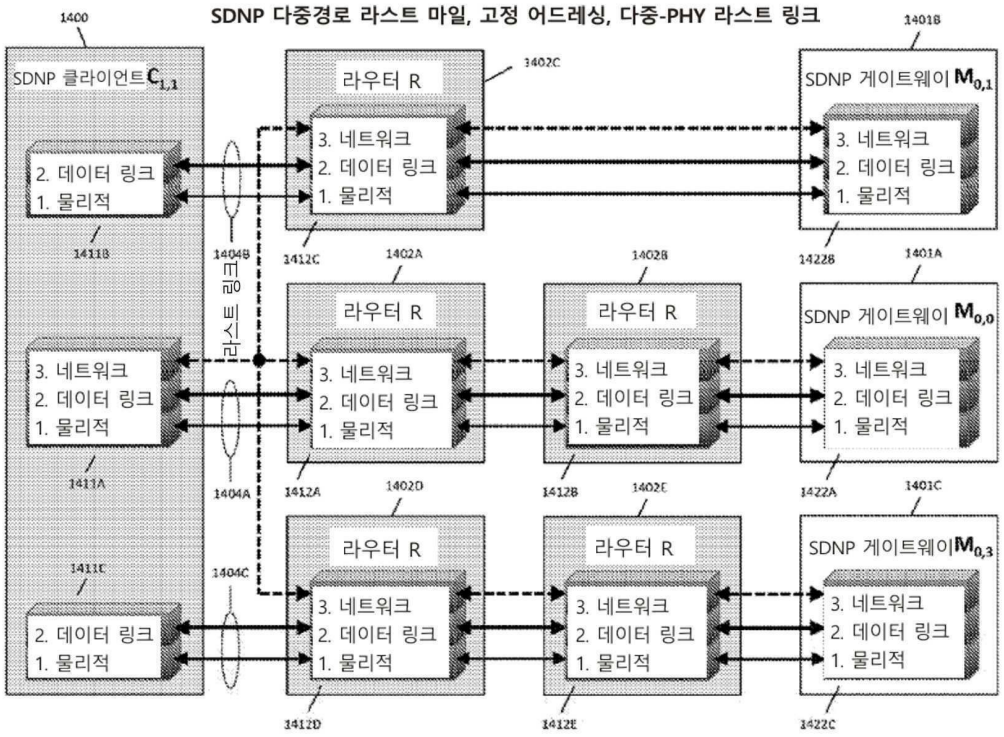
도면43


IP 데이터그램
소스
목적지
페이로드
1405B
IP $C_{1,1}$
IP $M_{0,1}$
SDNP 2
SDNP 게이트웨이
1402C
R
$M_{0,1}$
IP 데이터그램
라우터
소스
목적지
페이로드
1405A
IP $C_{1,1}$
IP $M_{0,0}$
SDNP 1
1401B
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
$C_{1,1}$
R
R
$M_{0,0}$
1404B
1404A
1400
1402A
1402B
1401A
라우터
1402D
라우터
1402E
SDNP 게이트웨이
1404C
R
R
$M_{0,3}$
IP 데이터그램
소스
목적지
페이로드
1405C
IP $C_{1,1}$
IP $M_{0,3}$
SDNP 3
1401C

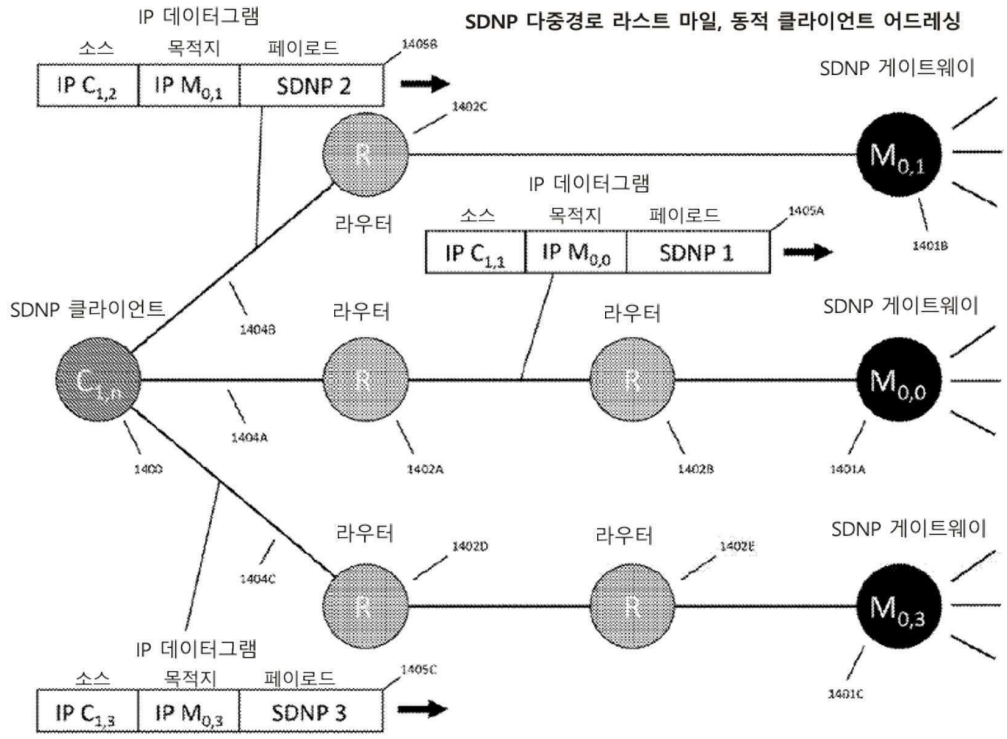
도면44a


SDNP 다중경로 라스트 마일, 고정 어드레싱, 확장된 단일-PHY 라스트 링크
단일 PHY
라스트 링크
1404
1400
SDNP 클라이언트 $C_{1,1}$
3. 네트워크
2. 데이터 링크
1. 물리적
1411
라우터 R
1402C
1412C
1402A
1412A
1402B
1412B
1402D
1412D
1402E
1412E
SDNP 게이트웨이 $M_{0,1}$
1401B
1422B
SDNP 게이트웨이 $M_{0,0}$
1401A
1422A
SDNP 게이트웨이 $M_{0,3}$
1401C
1422C

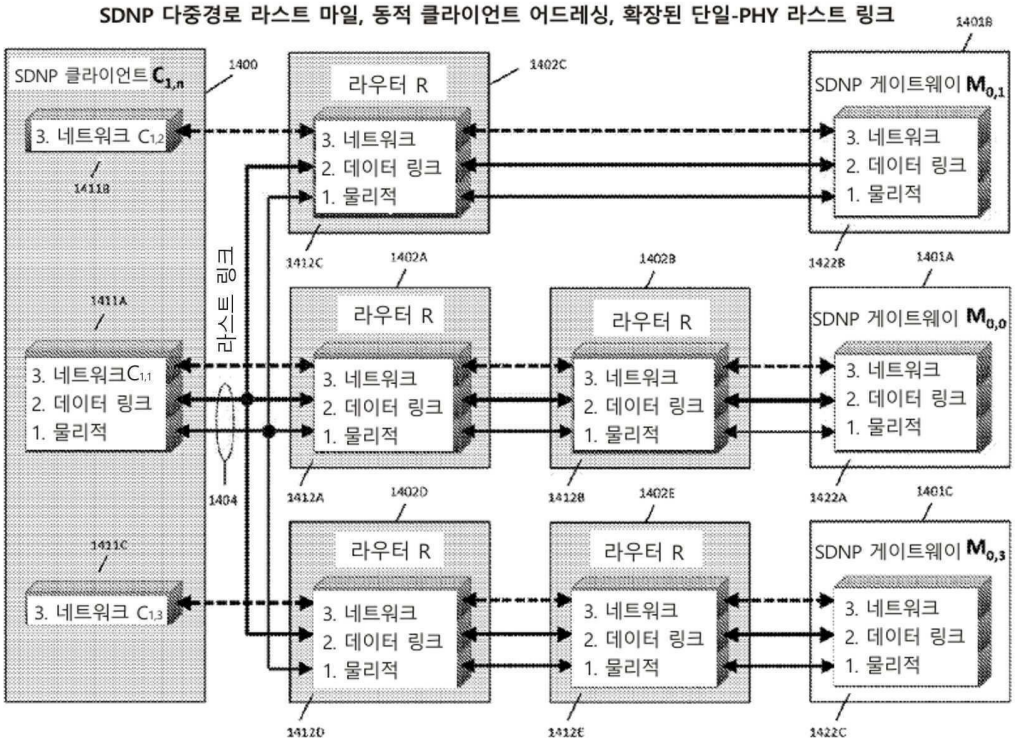
도면44b


SDNP 다중경로 라스트 마일, 고정 어드레싱, 다중-PHY 라스트 링크
1400
SDNP 클라이언트 $C_{1,1}$
2. 데이터 링크
1. 물리적
1411B
3. 네트워크
1411A
1411C
1404B
라스트 링크
1404A
1404C
라우터 R
1402C
1412C
1402A
1412A
1402B
1412B
1402D
1412D
1402E
1412E
SDNP 게이트웨이 $M_{0,1}$
1401B
1422B
SDNP 게이트웨이 $M_{0,0}$
1401A
1422A
SDNP 게이트웨이 $M_{0,3}$
1401C
1422C

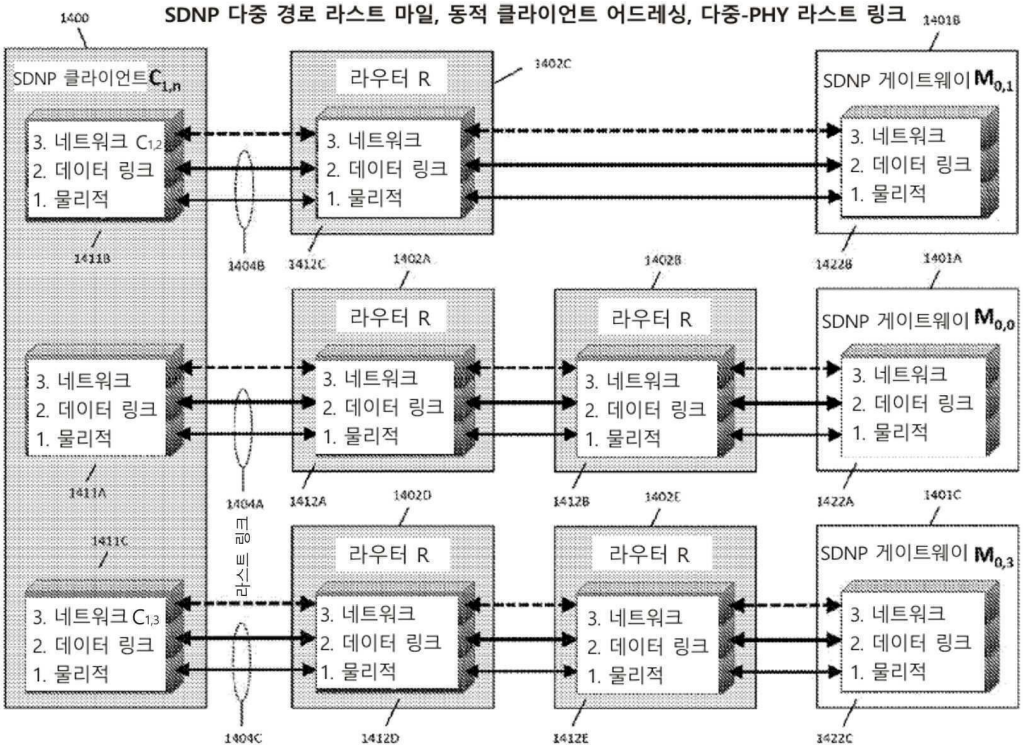
도면45


SDNP 다중경로 라스트 마일, 동적 클라이언트 어드레싱
IP 데이터그램
소스
목적지
페이로드
IP C1,2
IP M0,1
SDNP 2
1405B
1402C
R
라우터
SDNP 게이트웨이
M0,1
1401B
IP 데이터그램
소스
목적지
페이로드
IP C1,1
IP M0,0
SDNP 1
1405A
SDNP 클라이언트
C1,n
1400
1404B
1404A
1404C
라우터
라우터
라우터
라우터
라우터
R
1402A
1402B
1402D
1402E
SDNP 게이트웨이
M0,0
1401A
SDNP 게이트웨이
M0,3
1401C
IP 데이터그램
소스
목적지
페이로드
IP C1,3
IP M0,3
SDNP 3
1405C

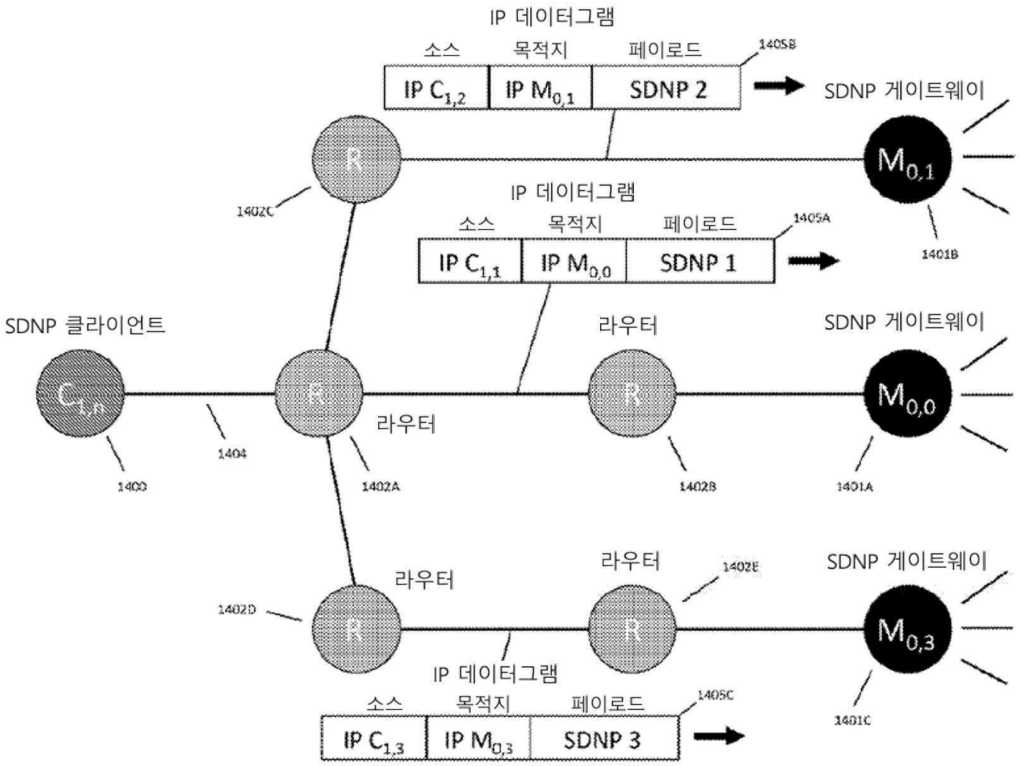
도면46a


SDNP 다중경로 라스트 마일, 동적 클라이언트 어드레싱, 확장된 단일-PHY 라스트 링크
SDNP 클라이언트 C1,n
1400
3. 네트워크 C1,2
1411B
3. 네트워크C1,1
2. 데이터 링크
1. 물리적
1411A
3. 네트워크 C1,3
1411C
라스트 링크
1404
라우터 R
1402C
1412C
라우터 R
1402A
1412A
라우터 R
1402D
1412D
라우터 R
1402B
1412B
라우터 R
1402E
1412E
3. 네트워크
2. 데이터 링크
1. 물리적
SDNP 게이트웨이 M0,1
1401B
1422B
SDNP 게이트웨이 M0,0
1401A
1422A
SDNP 게이트웨이 M0,3
1401C
1422C

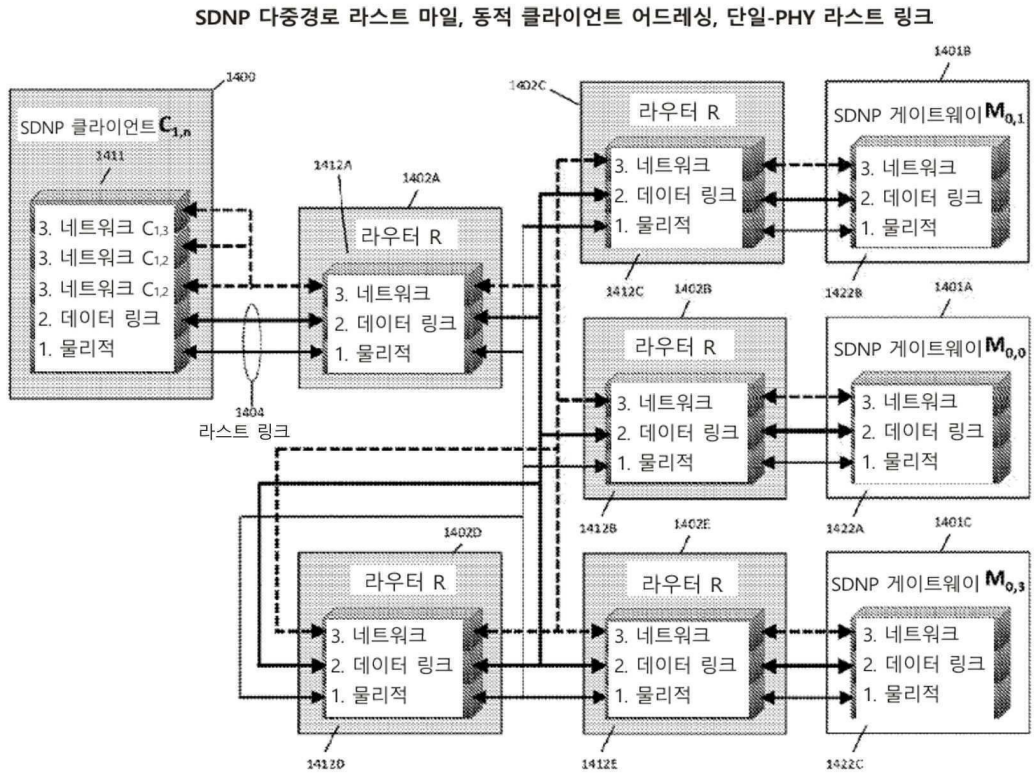
도면46b


SDNP 다중 경로 라스트 마일, 동적 클라이언트 어드레싱, 다중-PHY 라스트 링크
1400
SDNP 클라이언트 $C_{1,n}$
3. 네트워크 $C_{1,2}$
2. 데이터 링크
1. 물리적
1411B
1404B
라우터 R
1402C
1412C
3. 네트워크
2. 데이터 링크
1. 물리적
1401B
SDNP 게이트웨이 $M_{0,1}$
1422B
1402A
1412A
1404A
1411A
3. 네트워크 $C_{1,3}$
1411C
1404C
라스트 링크
1402D
1412D
1402B
1412B
1402E
1412E
SDNP 게이트웨이 $M_{0,0}$
1422A
1401A
SDNP 게이트웨이 $M_{0,3}$
1422C
1401C

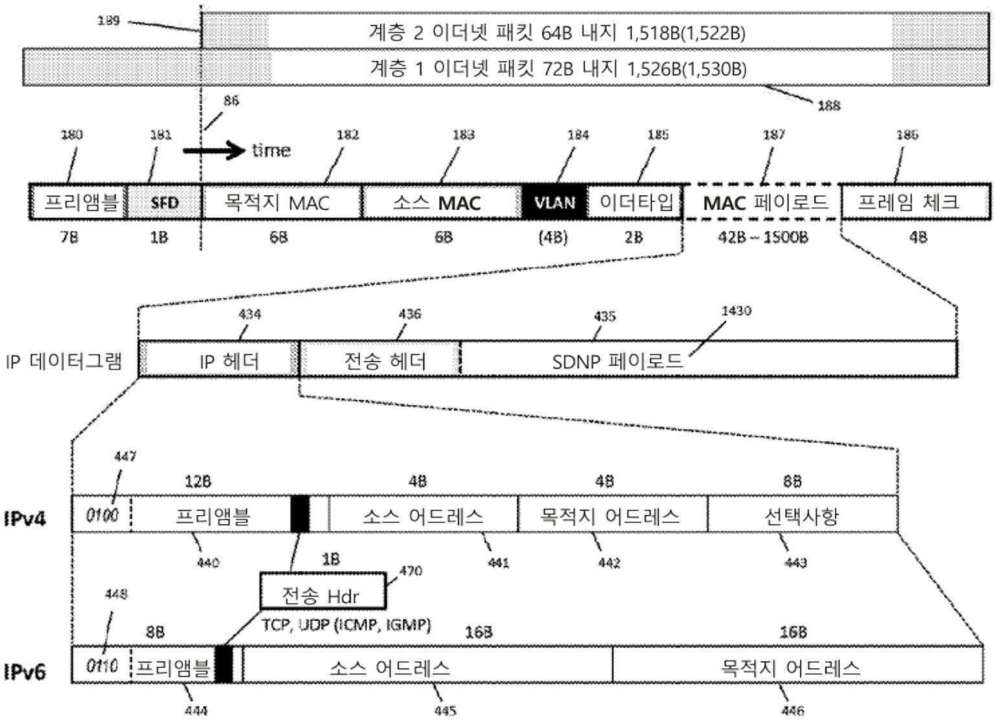
도면47


IP 데이터그램
소스
목적지
페이로드
IP $C_{1,2}$
IP $M_{0,1}$
SDNP 2
1405B
SDNP 게이트웨이
R
$M_{0,1}$
1402C
IP 데이터그램
소스
목적지
페이로드
IP $C_{1,1}$
IP $M_{0,0}$
SDNP 1
1405A
1401B
SDNP 클라이언트
라우터
SDNP 게이트웨이
$C_{1,n}$
R
$M_{0,0}$
1400
1404
1402A
1402B
1401A
라우터
라우터
SDNP 게이트웨이
1402D
R
R
$M_{0,3}$
1402E
IP 데이터그램
소스
목적지
페이로드
IP $C_{1,3}$
IP $M_{0,3}$
SDNP 3
1405C
1401C

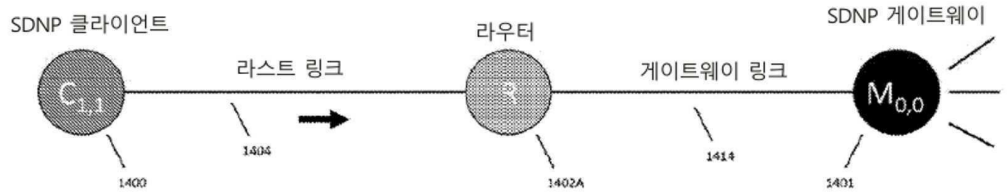
도면48


SDNP 다중경로 라스트 마일, 동적 클라이언트 어드레싱, 단일-PHY 라스트 링크
SDNP 클라이언트 $C_{1,n}$
3. 네트워크 $C_{1,3}$
3. 네트워크 $C_{1,2}$
3. 네트워크 $C_{1,2}$
2. 데이터 링크
1. 물리적
라스트 링크
라우터 R
3. 네트워크
2. 데이터 링크
1. 물리적
SDNP 게이트웨이 $M_{0,1}$
SDNP 게이트웨이 $M_{0,0}$
SDNP 게이트웨이 $M_{0,3}$

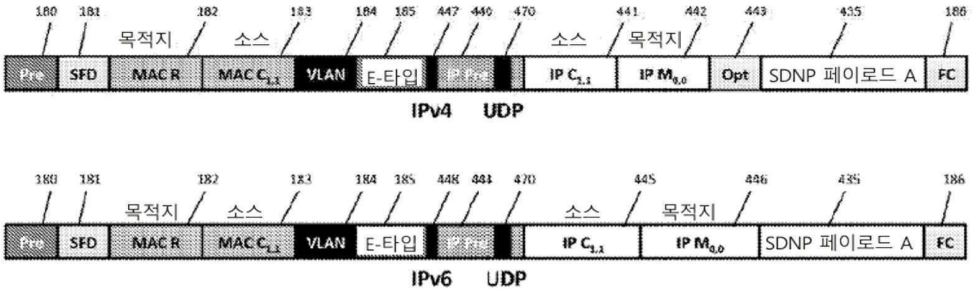
도면49


계층 2 이더넷 패킷 64B 내지 1,518B(1,522B)
계층 1 이더넷 패킷 72B 내지 1,526B(1,530B)
time
프리앰블
SFD
목적지 MAC
소스 MAC
VLAN
이더타입
MAC 페이로드
프레임 체크
IP 데이터그램
IP 헤더
전송 헤더
SDNP 페이로드
IPv4
0100
프리앰블
소스 어드레스
목적지 어드레스
선택사항
전송 Hdr
TCP, UDP (ICMP, IGMP)
IPv6
0110
프리앰블
소스 어드레스
목적지 어드레스

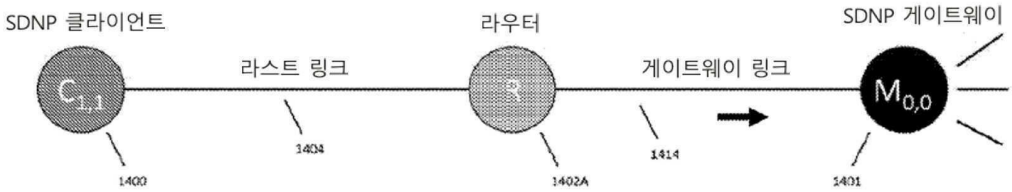
도면50a



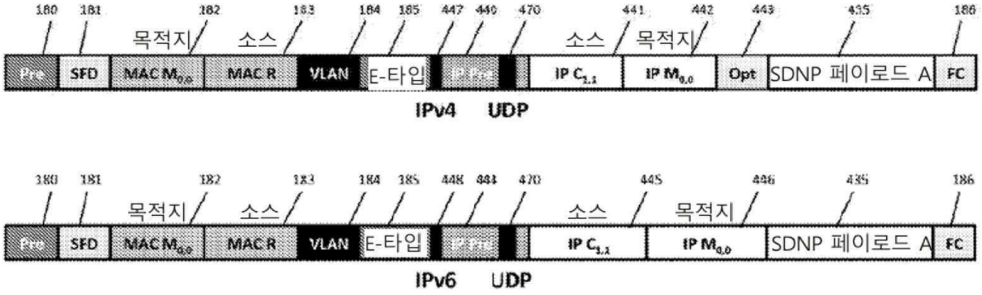

라스트 링크 이더넷 패킷(클라이언트 대 SDNP 클라우드)



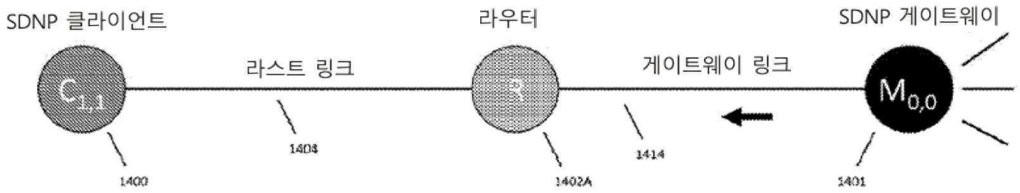

도면50b



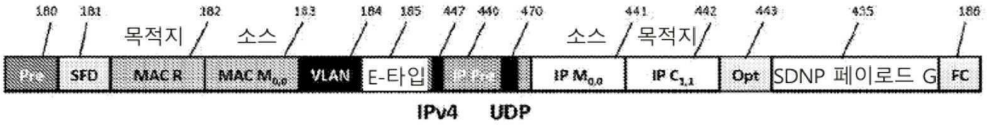

게이트웨이 링크 이더넷 패킷(클라이언트 대 SDNP 클라우드)



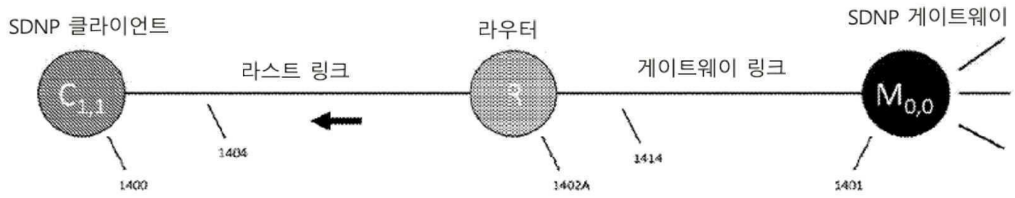
도면50c



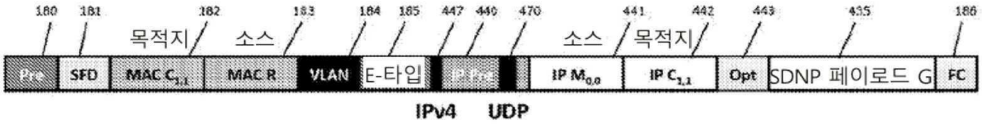

게이트웨이 링크 이더넷 패킷(SDNP 클라우드 대 클라이언트)




도면50d

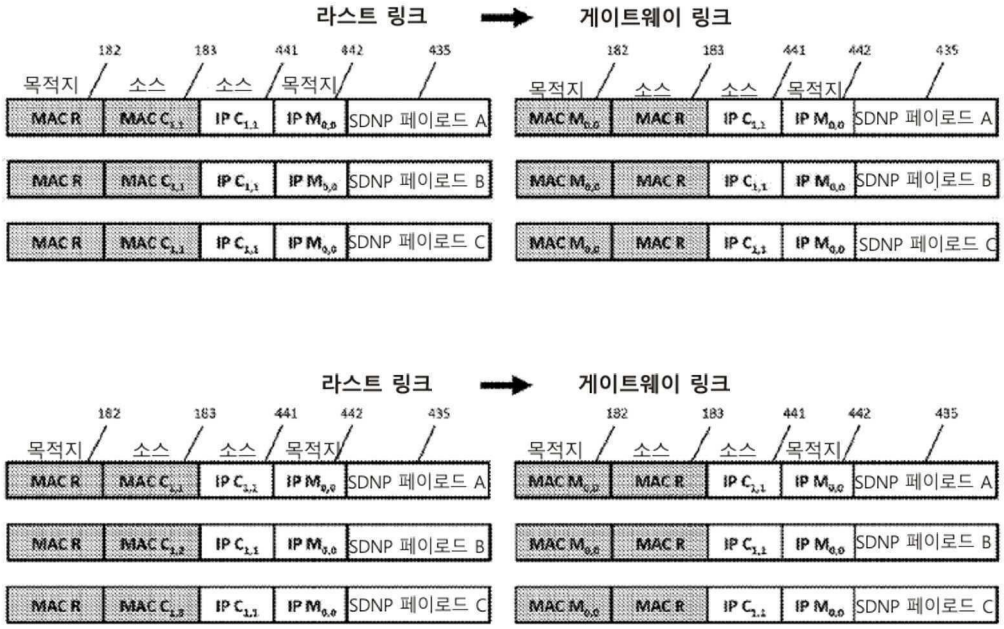



라스트 링크 이더넷 패킷(SDNP 클라우드 대 클라이언트)



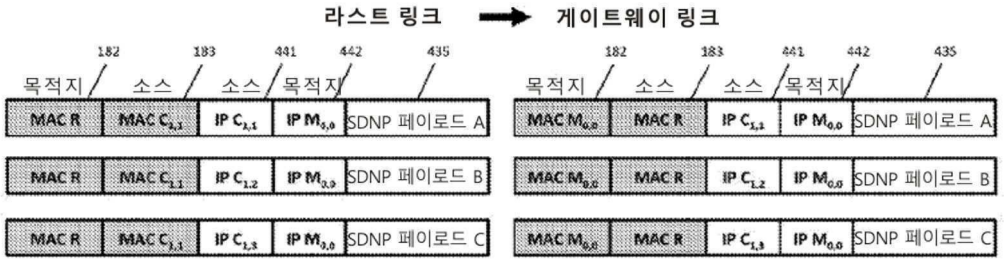
도면51a

SDNP 단일 경로 라스트 마일, 고정 클라이언트 어드레싱, 단일-PHY 라스트 링크

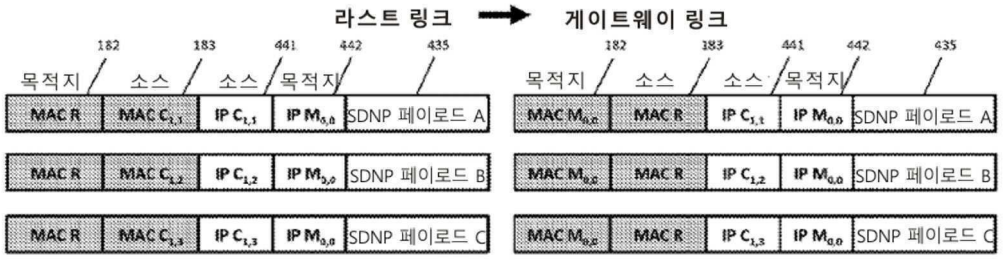



도면51b

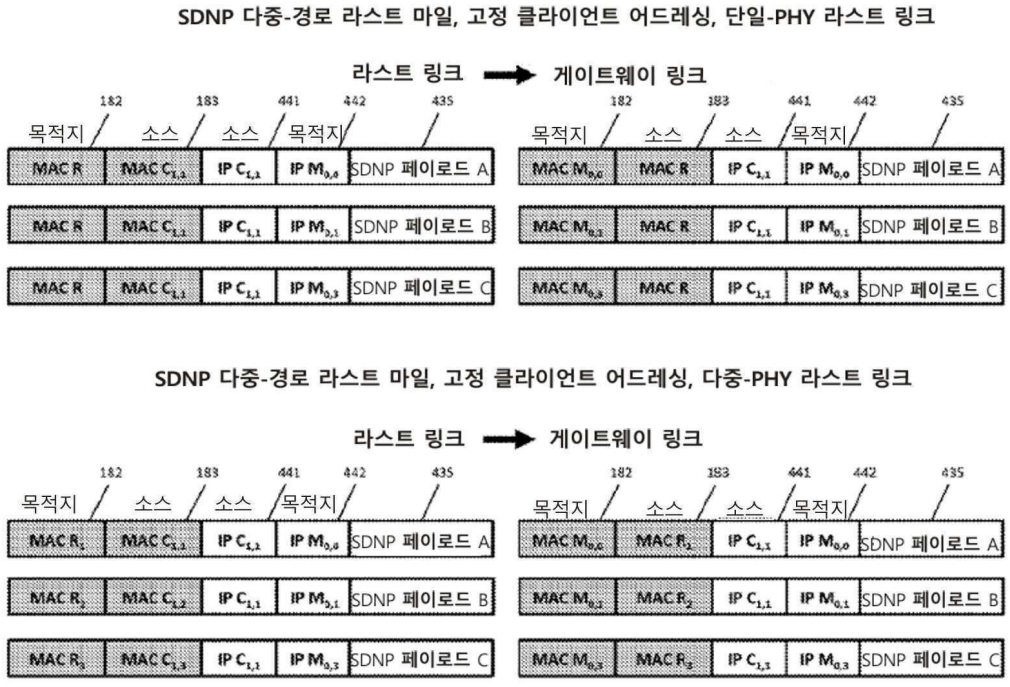
SDNP 단일 경로 라스트 마일, 동적 클라이언트 어드레싱, 단일-PHY 라스트 링크



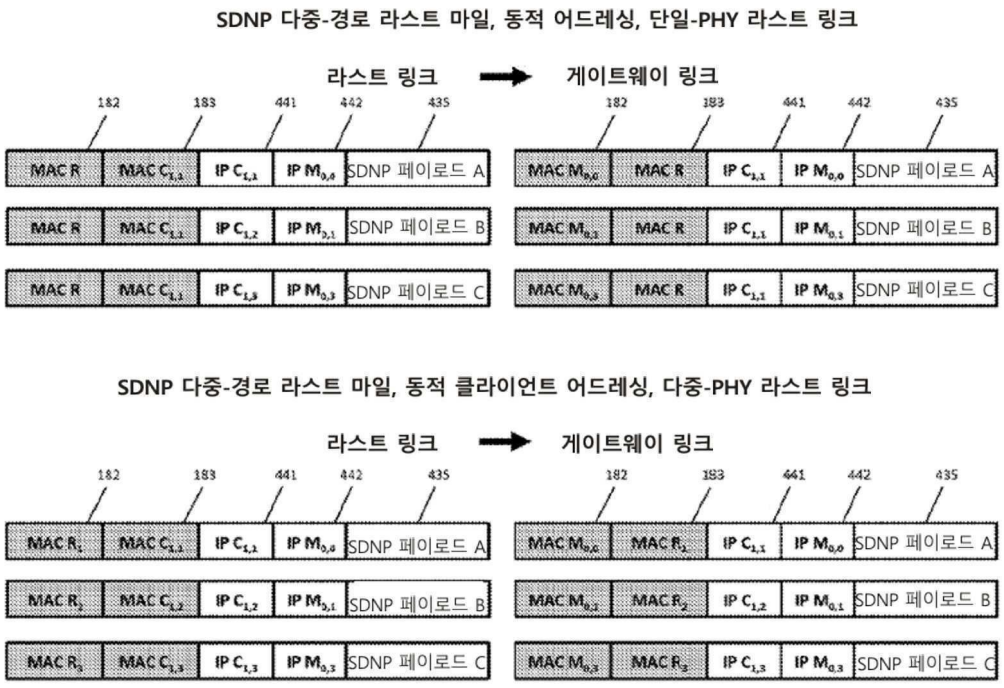

SDNP 단일 경로 라스트 마일, 동적 클라이언트 어드레싱, 다중-PHY 라스트 링크



도면51c


SDNP 다중-경로 라스트 마일, 고정 클라이언트 어드레싱, 단일-PHY 라스트 링크
라스트 링크
게이트웨이 링크
182
183
441
442
435
목적지
소스
소스
목적지
MAC R
SDNP 페이로드 A
SDNP 페이로드 B
SDNP 페이로드 C
SDNP 다중-경로 라스트 마일, 고정 클라이언트 어드레싱, 다중-PHY 라스트 링크
라스트 링크
게이트웨이 링크
목적지
소스
소스
목적지
SDNP 페이로드 A
SDNP 페이로드 B
SDNP 페이로드 C

도면51d

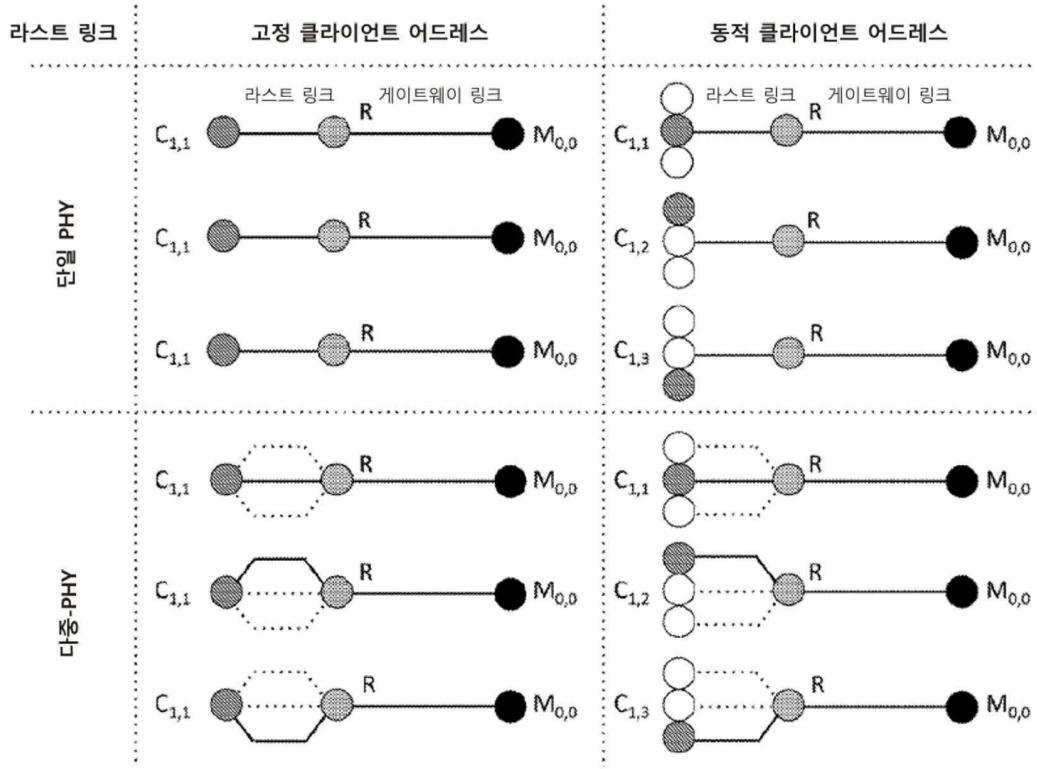

SDNP 다중-경로 라스트 마일, 동적 어드레싱, 단일-PHY 라스트 링크
라스트 링크
게이트웨이 링크
182
183
441
442
435
MAC R
SDNP 페이로드 A
SDNP 페이로드 B
SDNP 페이로드 C
SDNP 다중-경로 라스트 마일, 동적 클라이언트 어드레싱, 다중-PHY 라스트 링크
라스트 링크
게이트웨이 링크
SDNP 페이로드 A
SDNP 페이로드 B
SDNP 페이로드 C

도면52a

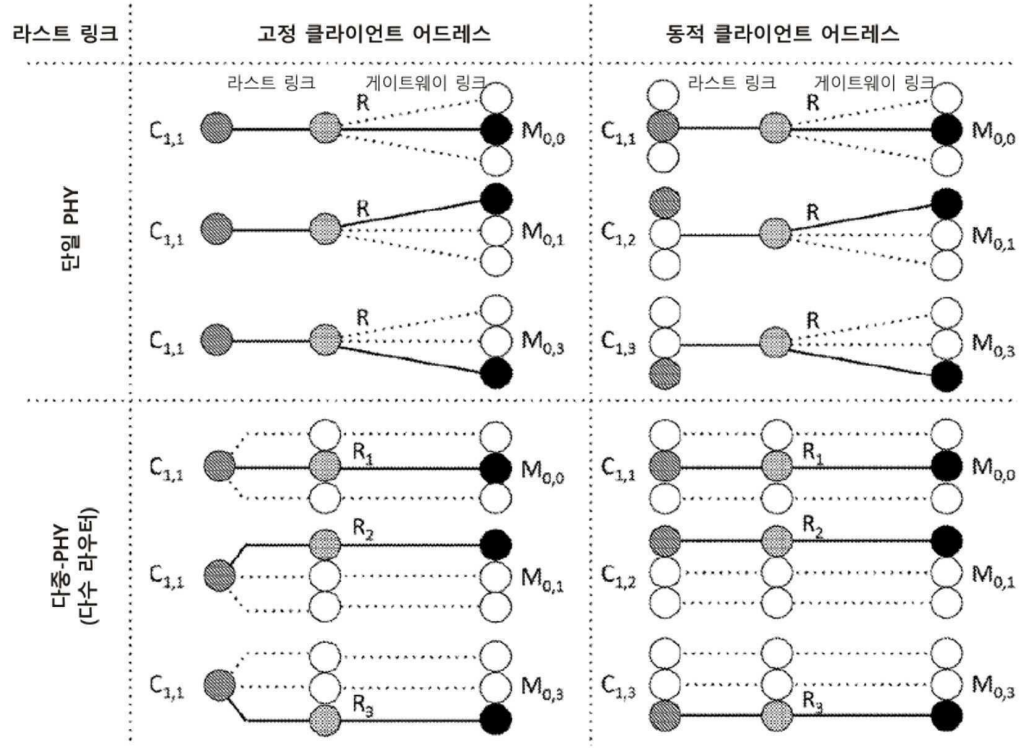
이더넷에 걸친 SDNP 라스트 마일 라우팅

| # | 경로 | 클라이언트 어드레스 | 라스트 링크 | IP 소스 | IP 목적지 | MAC 클라이언트 |
|---|---|---|---|---|---|---|
| 1 | 다중 | 동적 | 다중-PHY | 변수 $C_{1,n}$ | 다중 게이트웨이 $M_{0,n}$ | MAC $C_{1,n}$ 내지 Rn |
| 2 | 다중 | 동적 | 다중-PHY | 변수 $C_{1,n}$ | | MAC $C_{1,n}$ 내지 R |
| 3 | 다중 | 동적 | 단일-PHY | 변수 $C_{1,n}$ | | MAC $C_{1,1}$ 내지 Rn |
| 4 | 다중 | 고정 | 다중-PHY | 고정 $C_{1,1}$ | | MAC $C_{1,n}$ 내지 Rn |
| 5 | 다중 | 고정 | 다중-PHY | 고정 $C_{1,1}$ | | MAC $C_{1,n}$ 내지 R |
| 6 | 다중 | 고정 | 단일-PHY | 고정 $C_{1,1}$ | | MAC $C_{1,1}$ 내지 R |
| 7 | 단일 | 동적 | 다중-PHY | 변수 $C_{1,n}$ | 단일 게이트웨이 $M_{0,0}$ | MAC $C_{1,n}$ 내지 R |
| 8 | 단일 | 동적 | 단일-PHY | 변수 $C_{1,n}$ | | MAC $C_{1,1}$ 내지 R |
| 9 | 단일 | 고정 | 다중-PHY | 고정 $C_{1,1}$ | | MAC $C_{1,n}$ 내지 R |
| 10 | 단일 | 고정 | 단일-PHY | 고정 $C_{1,1}$ | | MAC $C_{1,1}$ 내지 R |

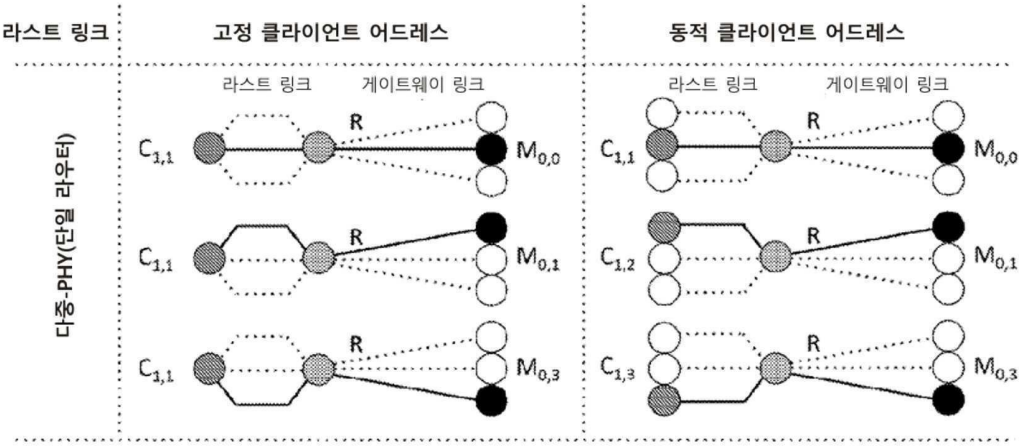
도면52b



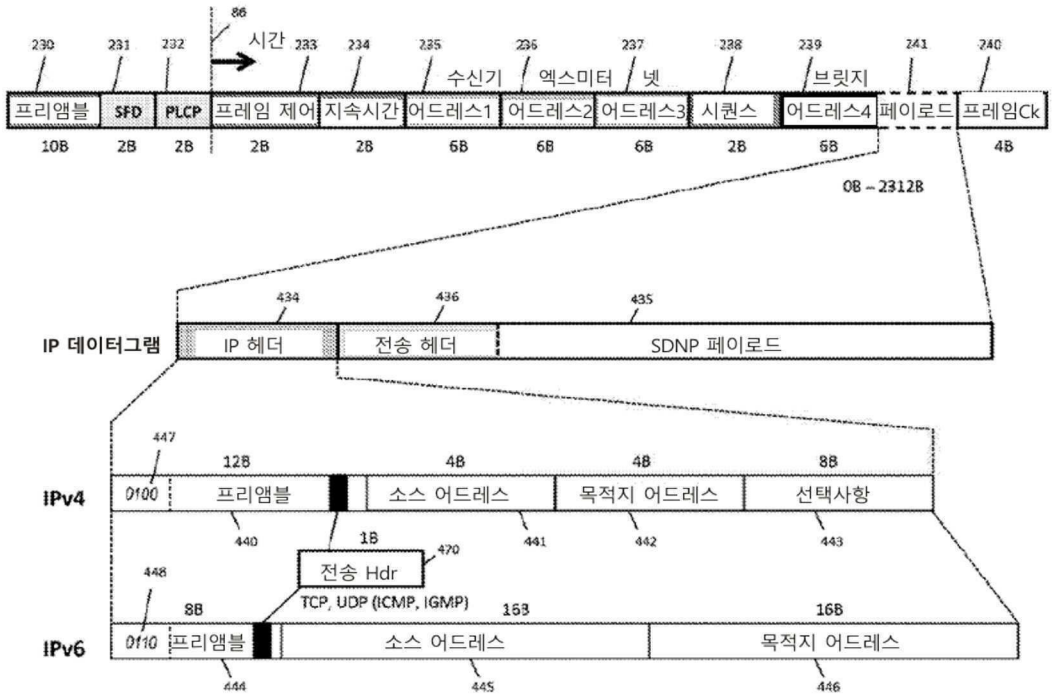
도면52c


라스트 링크
고정 클라이언트 어드레스
동적 클라이언트 어드레스
단일 PHY
다중-PHY
(다수 라우터)
라스트 링크
게이트웨이 링크
R
R1
R2
R3
C1,1
C1,2
C1,3
M0,0
M0,1
M0,3

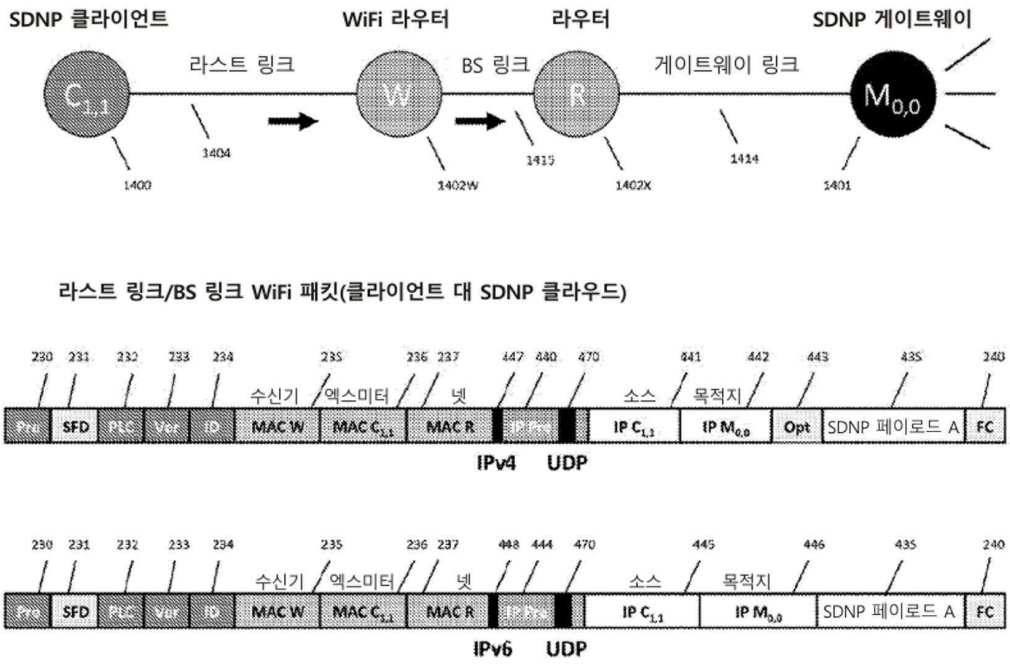
도면52d


라스트 링크
고정 클라이언트 어드레스
동적 클라이언트 어드레스
다중-PHY(단일 라우터)
라스트 링크
게이트웨이 링크
R
C1,1
C1,2
C1,3
M0,0
M0,1
M0,3

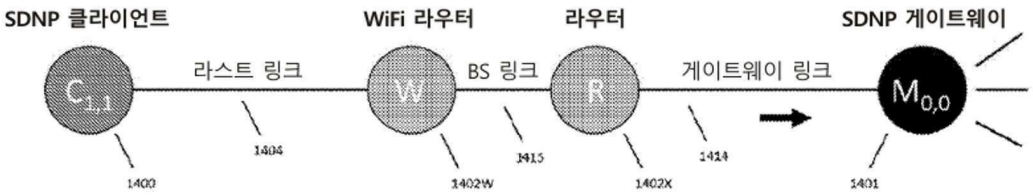
도면53


86
시간
230
231
232
233
234
235
236
237
238
239
241
240
수신기
엑스미터
넷
브릿지
프리앰블
SFD
PLCP
프레임 제어
지속시간
어드레스1
어드레스2
어드레스3
시퀀스
어드레스4
페이로드
프레임Ck
10B
2B
2B
2B
2B
6B
6B
6B
2B
6B
4B
0B – 2312B
IP 데이터그램
434
436
435
IP 헤더
전송 헤더
SDNP 페이로드
IPv4
447
12B
4B
4B
8B
0100
프리앰블
소스 어드레스
목적지 어드레스
선택사항
440
1B
441
442
443
470
전송 Hdr
448
TCP, UDP (ICMP, IGMP)
8B
16B
16B
IPv6
0110
프리앰블
소스 어드레스
목적지 어드레스
444
445
446

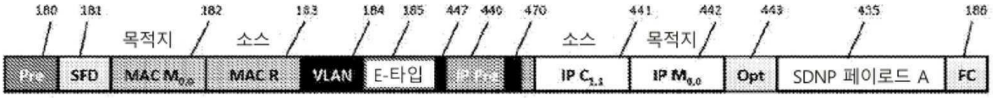
도면54a

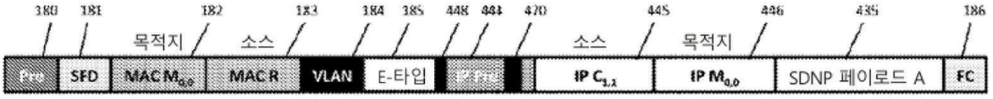

SDNP 클라이언트
WiFi 라우터
라우터
SDNP 게이트웨이
라스트 링크
BS 링크
게이트웨이 링크
C1,1
W
R
M0,0
1400
1404
1402W
1415
1402X
1414
1401
라스트 링크/BS 링크 WiFi 패킷(클라이언트 대 SDNP 클라우드)
230
231
232
233
234
235
236
237
447
480
470
441
442
443
435
240
수신기
엑스미터
넷
소스
목적지
Pre
SFD
PLC
Ver
ID
MAC W
MAC C1,1
MAC R
IP Hdr
IP C1,1
IP M0,0
Opt
SDNP 페이로드 A
FC
IPv4
UDP
230
231
232
233
234
235
236
237
448
444
470
445
446
435
240
수신기
엑스미터
넷
소스
목적지
Pre
SFD
PLC
Ver
ID
MAC W
MAC C1,1
MAC R
IP Hdr
IP C1,1
IP M0,0
SDNP 페이로드 A
FC
IPv6
UDP

도면54b

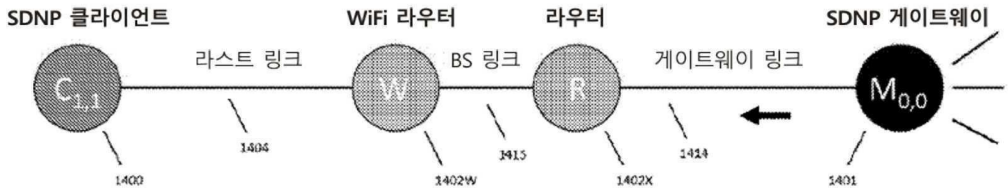



게이트웨이 링크 이더넷 패킷(클라이언트 대 SDNP 클라우드)

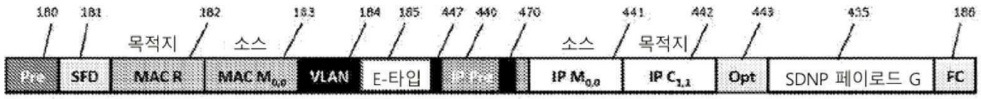


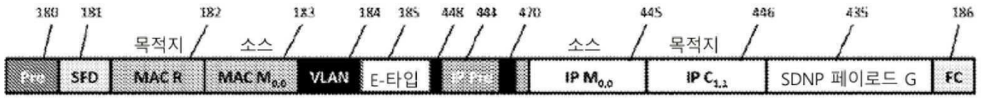




도면54c

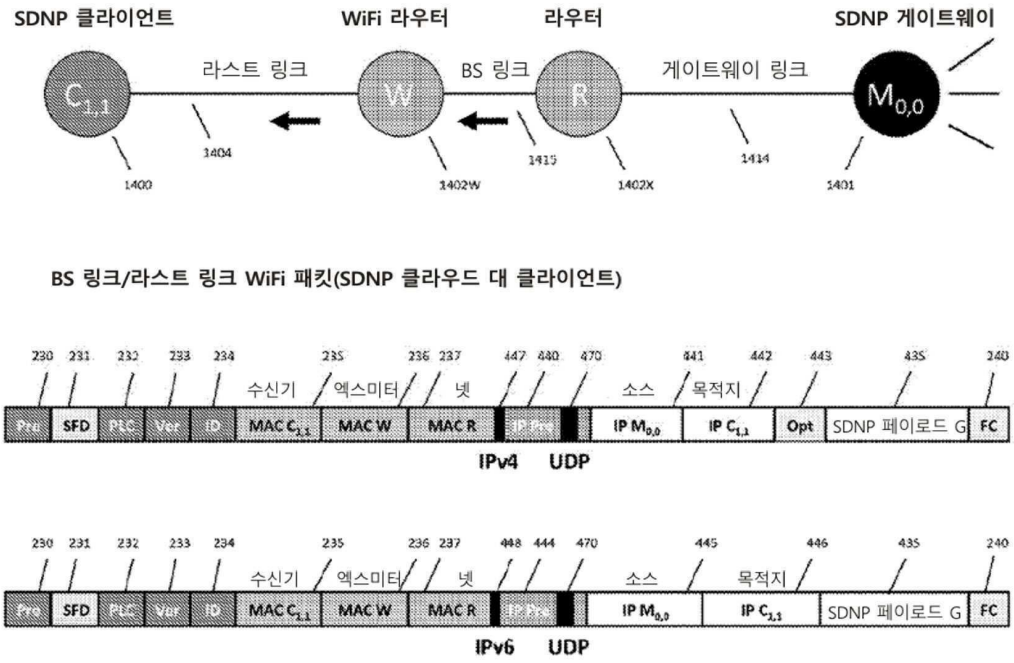



게이트웨이 링크 이더넷 패킷(SDNP 클라우드 대 클라이언트)

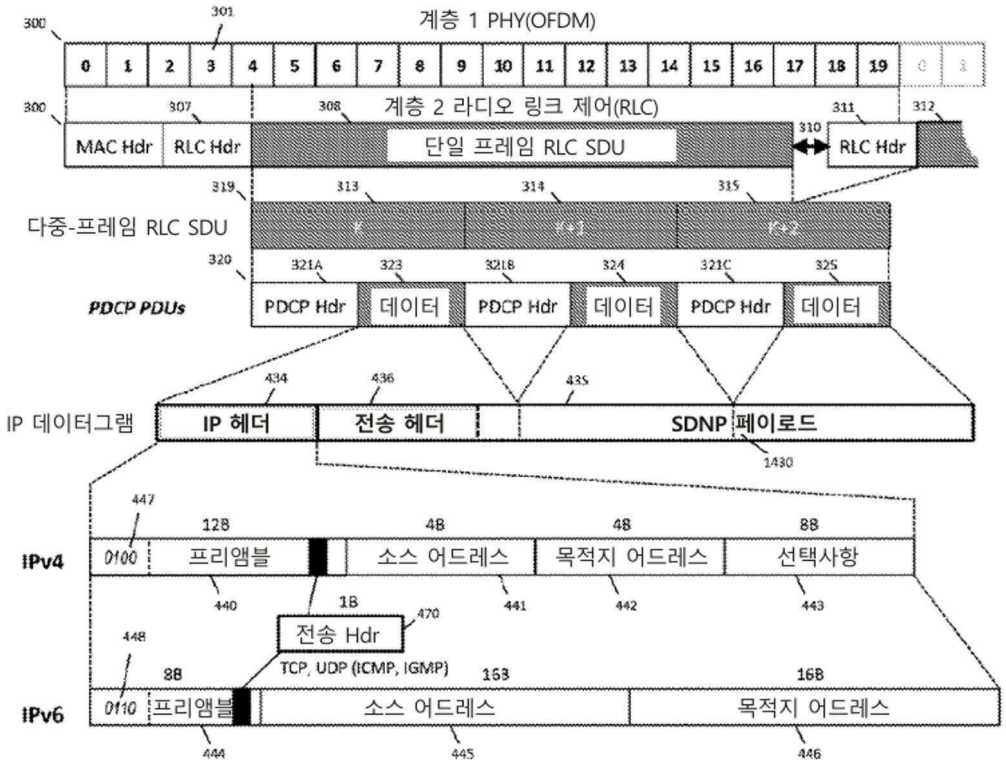


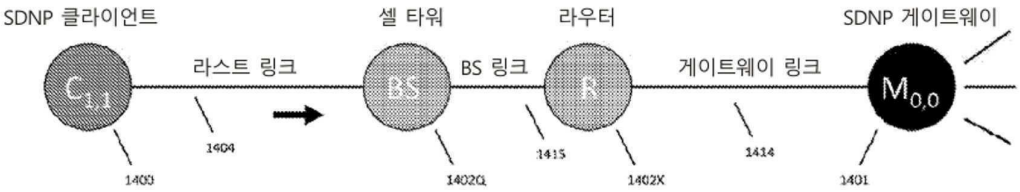
도면54d


SDNP 클라이언트
WiFi 라우터
라우터
SDNP 게이트웨이
라스트 링크
BS 링크
게이트웨이 링크
C1,1
W
R
M0,0
1400
1404
1402W
1415
1402X
1414
1401
BS 링크/라스트 링크 WiFi 패킷(SDNP 클라우드 대 클라이언트)
수신기
엑스미터
넷
소스
목적지
Pre
SFD
PLC
Ver
ID
MAC C1,1
MAC W
MAC R
IP Pro
IP M0,0
IP C1,1
Opt
SDNP 페이로드 G
FC
IPv4
UDP
IPv6
UDP

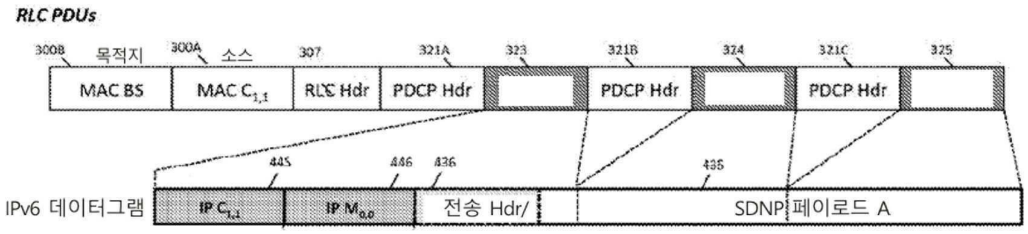
도면55


계층 1 PHY(OFDM)
계층 2 라디오 링크 제어(RLC)
MAC Hdr
RLC Hdr
단일 프레임 RLC SDU
RLC Hdr
다중-프레임 RLC SDU
PDCP PDUs
PDCP Hdr
데이터
IP 데이터그램
IP 헤더
전송 헤더
SDNP 페이로드
IPv4
프리앰블
소스 어드레스
목적지 어드레스
선택사항
전송 Hdr
TCP, UDP (ICMP, IGMP)
IPv6
프리앰블
소스 어드레스
목적지 어드레스

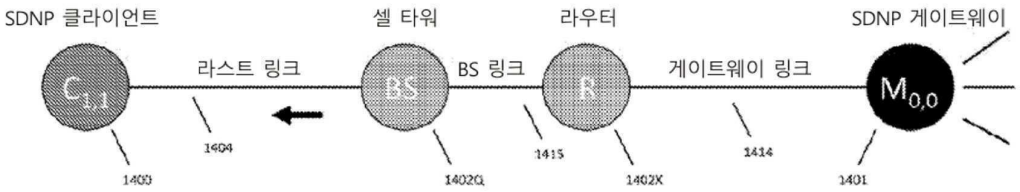
도면56a



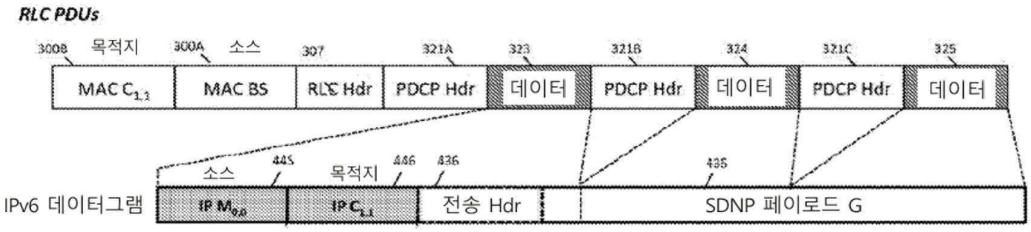

라스트 링크/BS 링크 셀룰러 4G 패킷(클라이언트 대 SDNP 클라우드)



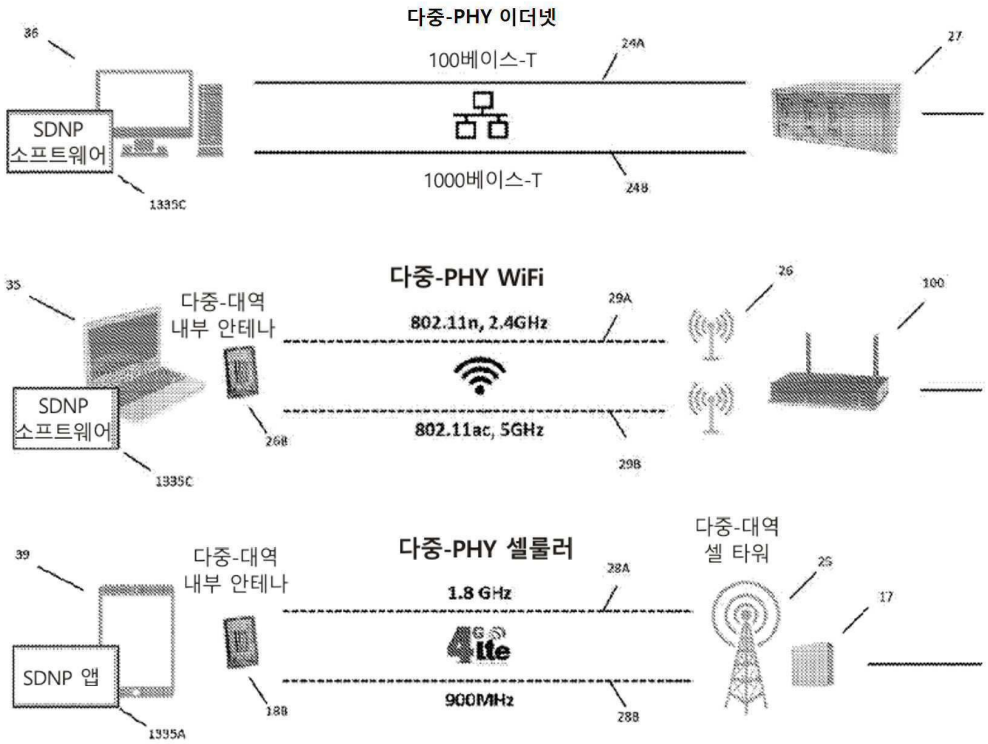

도면56b



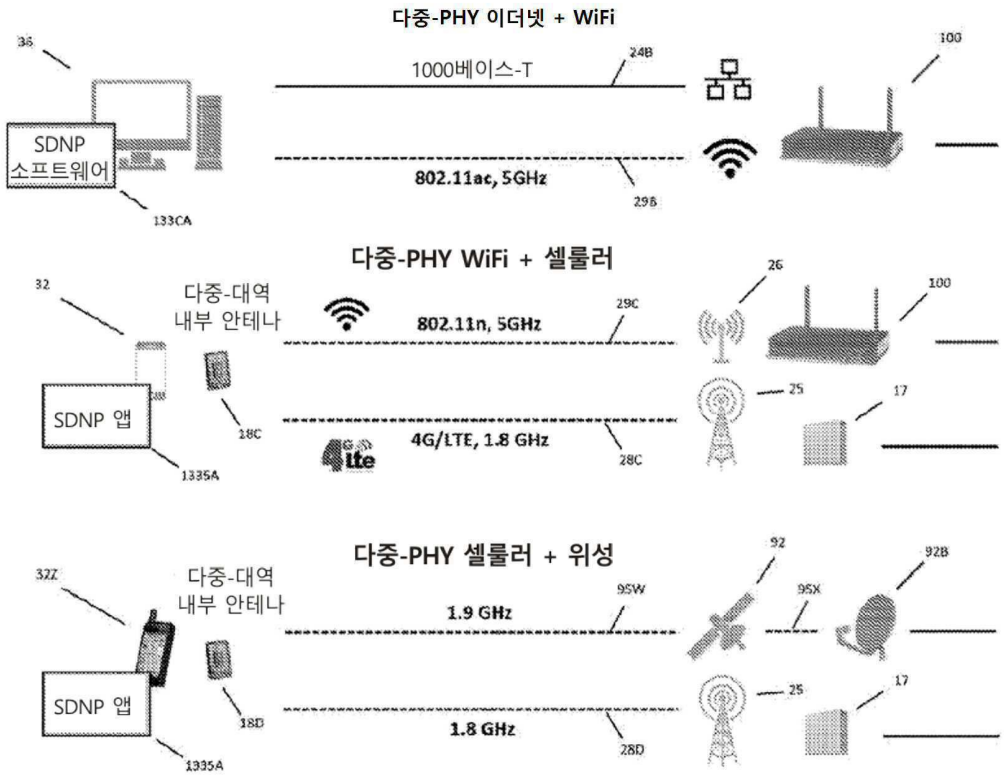

라스트 링크/BS 링크 셀룰러 4G 패킷(클라이언트 대 SDNP 클라우드)



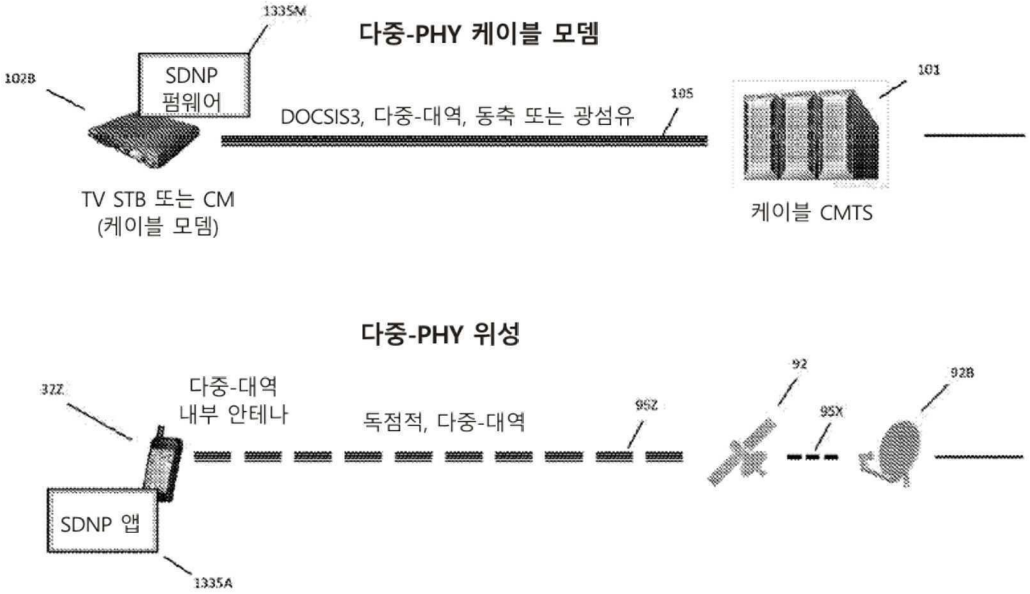
도면57a


다중-PHY 이더넷
100베이스-T
1000베이스-T
SDNP 소프트웨어
다중-PHY WiFi
다중-대역 내부 안테나
802.11n, 2.4GHz
802.11ac, 5GHz
다중-PHY 셀룰러
다중-대역 셀 타워
1.8 GHz
900MHz
SDNP 앱

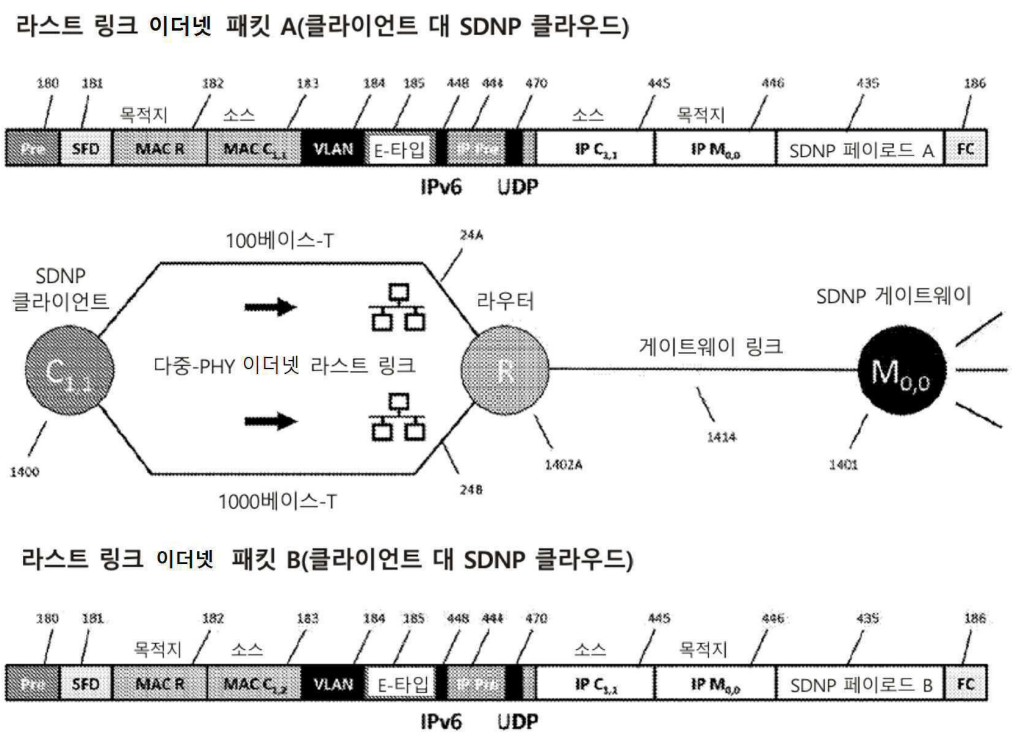
도면57b


다중-PHY 이더넷 + WiFi
1000베이스-T
802.11ac, 5GHz
SDNP 소프트웨어
다중-PHY WiFi + 셀룰러
다중-대역 내부 안테나
802.11n, 5GHz
4G/LTE, 1.8 GHz
SDNP 앱
다중-PHY 셀룰러 + 위성
1.9 GHz
1.8 GHz

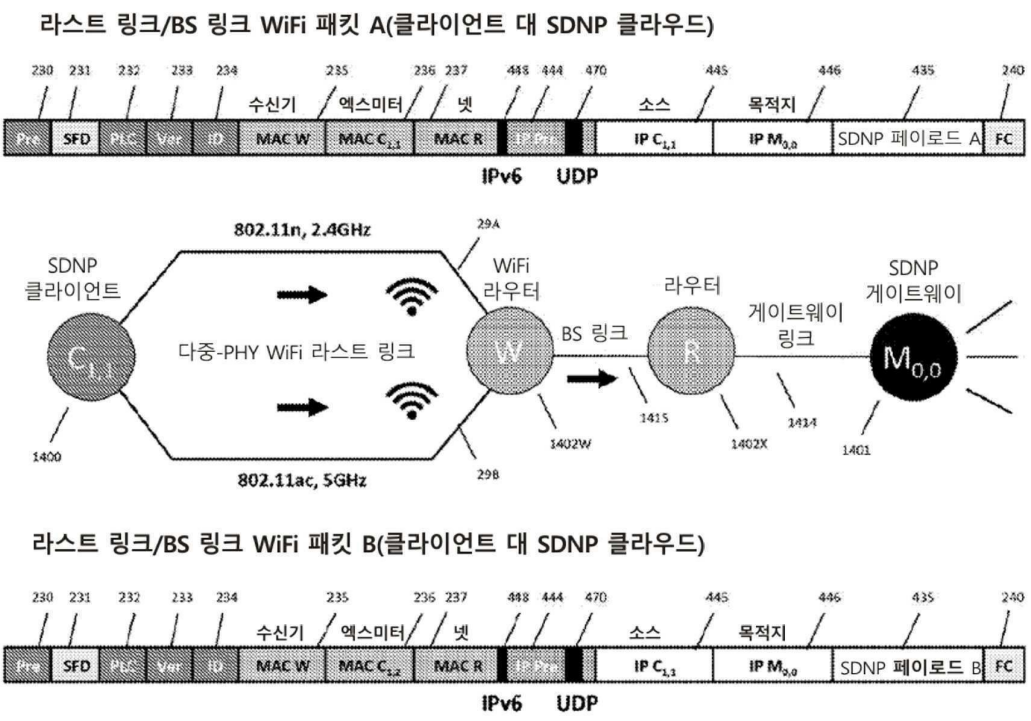
도면57c


다중-PHY 케이블 모뎀
1335M
SDNP
펌웨어
102B
DOCSIS3, 다중-대역, 동축 또는 광섬유
105
101
TV STB 또는 CM
(케이블 모델)
케이블 CMTS
다중-PHY 위성
372
다중-대역
내부 안테나
독점적, 다중-대역
95Z
92
95X
92B
SDNP 앱
1335A

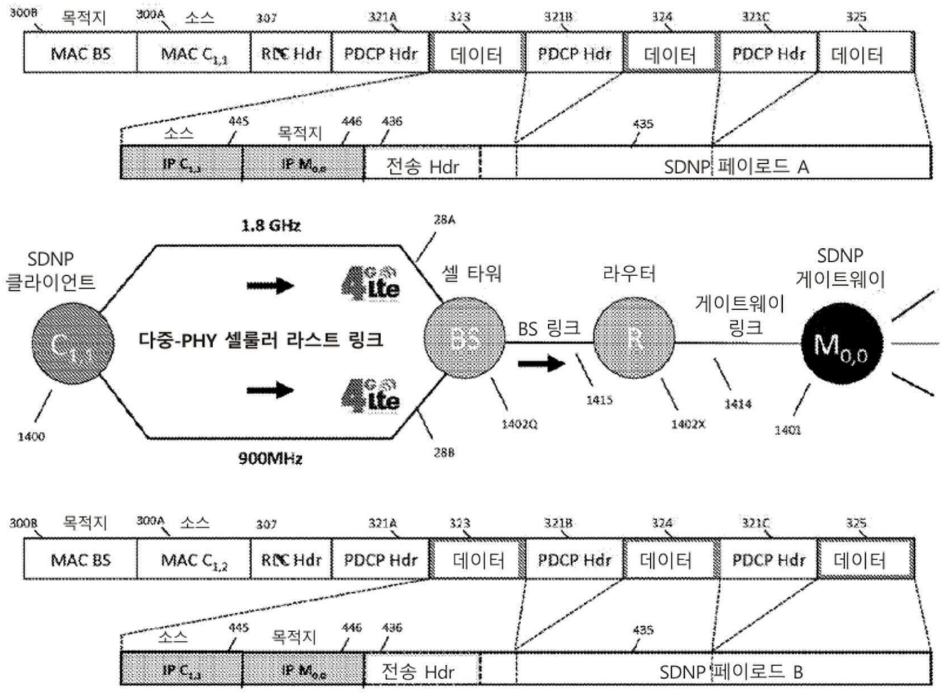
도면58


라스트 링크 이더넷 패킷 A(클라이언트 대 SDNP 클라우드)
180
181
182
183
184
185
448
444
470
445
446
435
186
목적지
소스
소스
목적지
Pre
SFD
MAC R
MAC C1,1
VLAN
E-타입
IP Hdr
IP C1,1
IP M0,0
SDNP 페이로드 A
FC
IPv6
UDP
100베이스-T
24A
SDNP
클라이언트
라우터
SDNP 게이트웨이
다중-PHY 이더넷 라스트 링크
게이트웨이 링크
C1,1
R
M0,0
1414
1400
1402A
1401
24B
1000베이스-T
라스트 링크 이더넷 패킷 B(클라이언트 대 SDNP 클라우드)
180
181
182
183
184
185
448
444
470
445
446
435
186
목적지
소스
소스
목적지
Pre
SFD
MAC R
MAC C1,1
VLAN
E-타입
IP Hdr
IP C1,1
IP M0,0
SDNP 페이로드 B
FC
IPv6
UDP

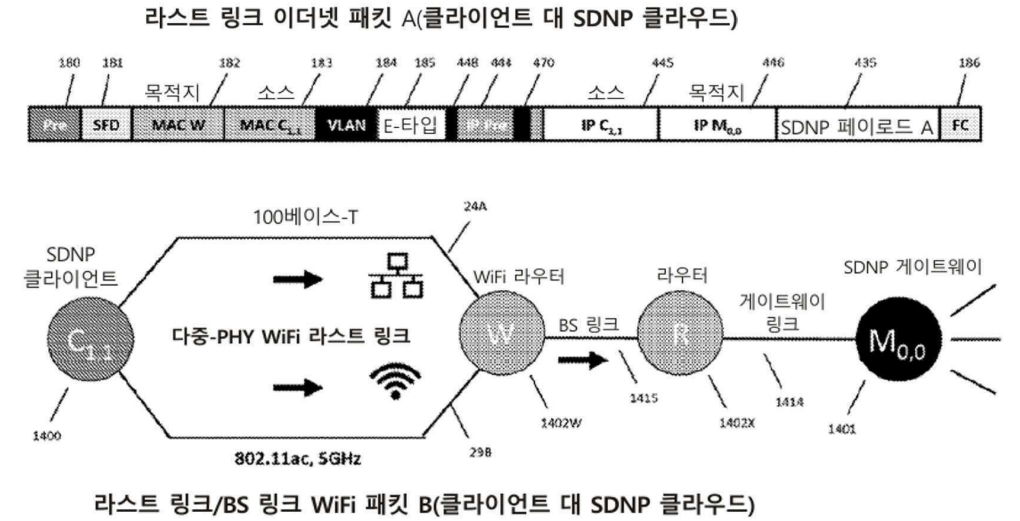
도면59


라스트 링크/BS 링크 WiFi 패킷 A(클라이언트 대 SDNP 클라우드)
수신기
엑스미터
넷
소스
목적지
MAC W
MAC R
SDNP 페이로드 A
IPv6
UDP
802.11n, 2.4GHz
SDNP 클라이언트
다중-PHY WiFi 라스트 링크
WiFi 라우터
BS 링크
라우터
게이트웨이 링크
SDNP 게이트웨이
802.11ac, 5GHz
라스트 링크/BS 링크 WiFi 패킷 B(클라이언트 대 SDNP 클라우드)
SDNP 페이로드 B

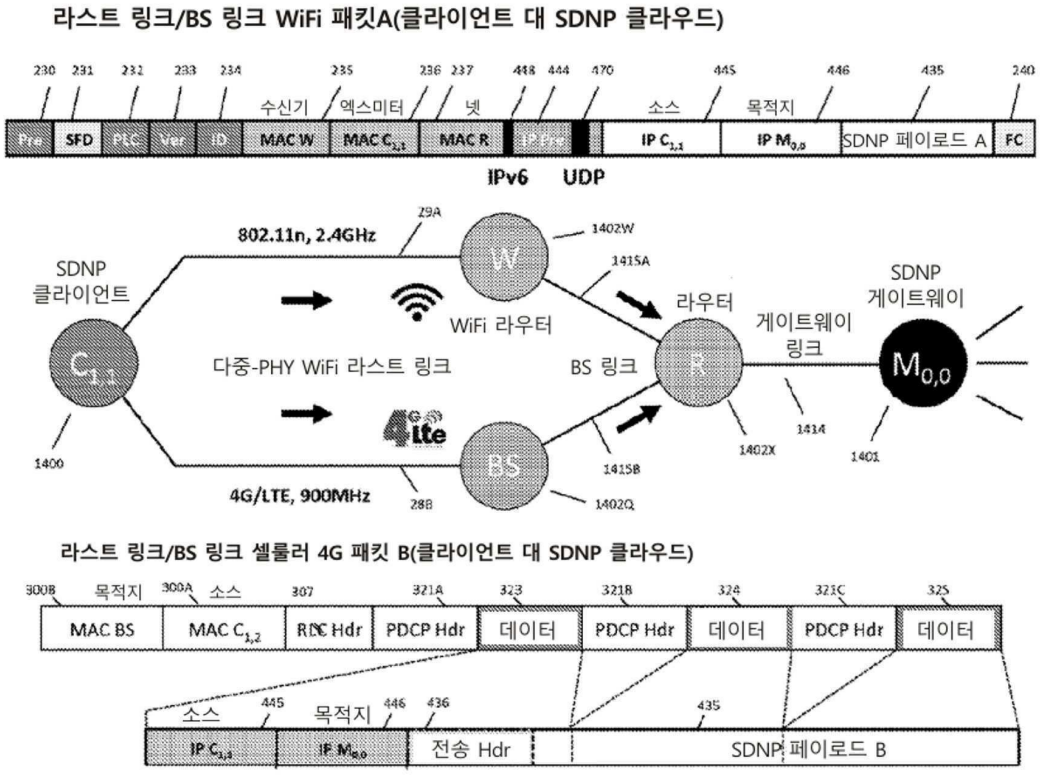
도면60


목적지
소스
MAC BS
PDCP Hdr
데이터
전송 Hdr
SDNP 페이로드 A
1.8 GHz
SDNP 클라이언트
다중-PHY 셀룰러 라스트 링크
셀 타워
BS 링크
라우터
게이트웨이 링크
SDNP 게이트웨이
900MHz
SDNP 페이로드 B

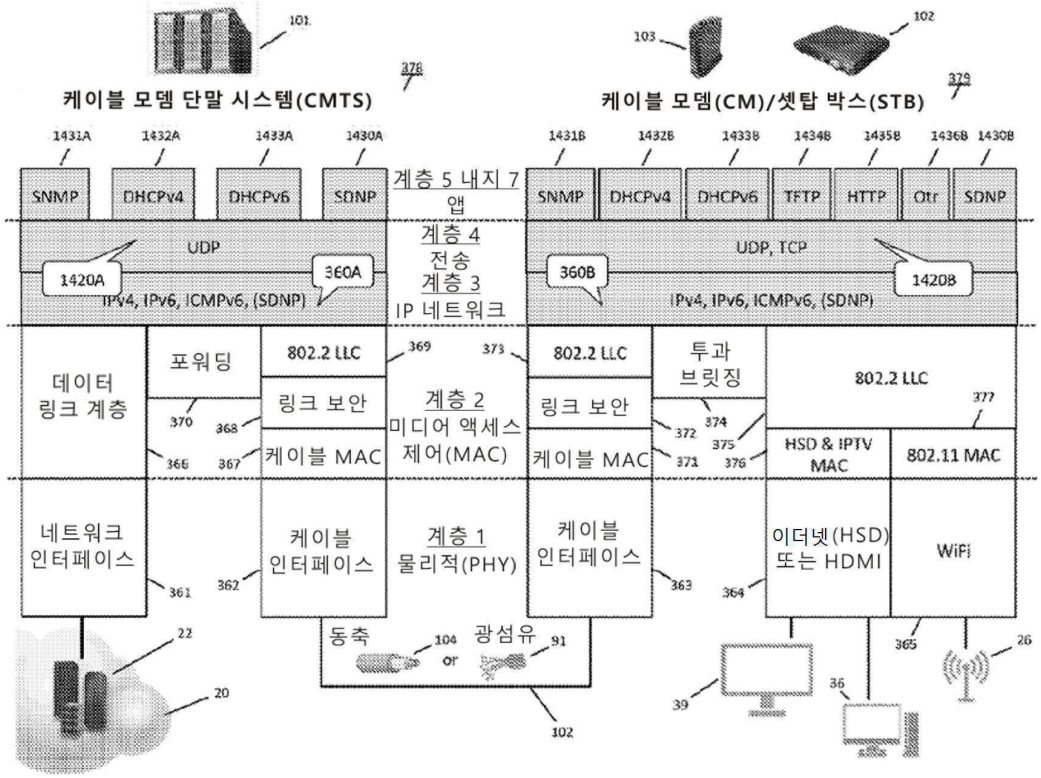
도면61


라스트 링크 이더넷 패킷 A(클라이언트 대 SDNP 클라우드)
목적지
소스
소스
목적지
Pre
SFD
MAC W
VLAN
E-타입
SDNP 페이로드 A
FC
100베이스-T
SDNP 클라이언트
다중-PHY WiFi 라스트 링크
WiFi 라우터
BS 링크
라우터
게이트웨이 링크
SDNP 게이트웨이
802.11ac, 5GHz
라스트 링크/BS 링크 WiFi 패킷 B(클라이언트 대 SDNP 클라우드)
수신기
엑스미터
넷
소스
목적지
Pre
SFD
PLC
Ver
ID
MAC W
MAC R
SDNP 페이로드 B
FC

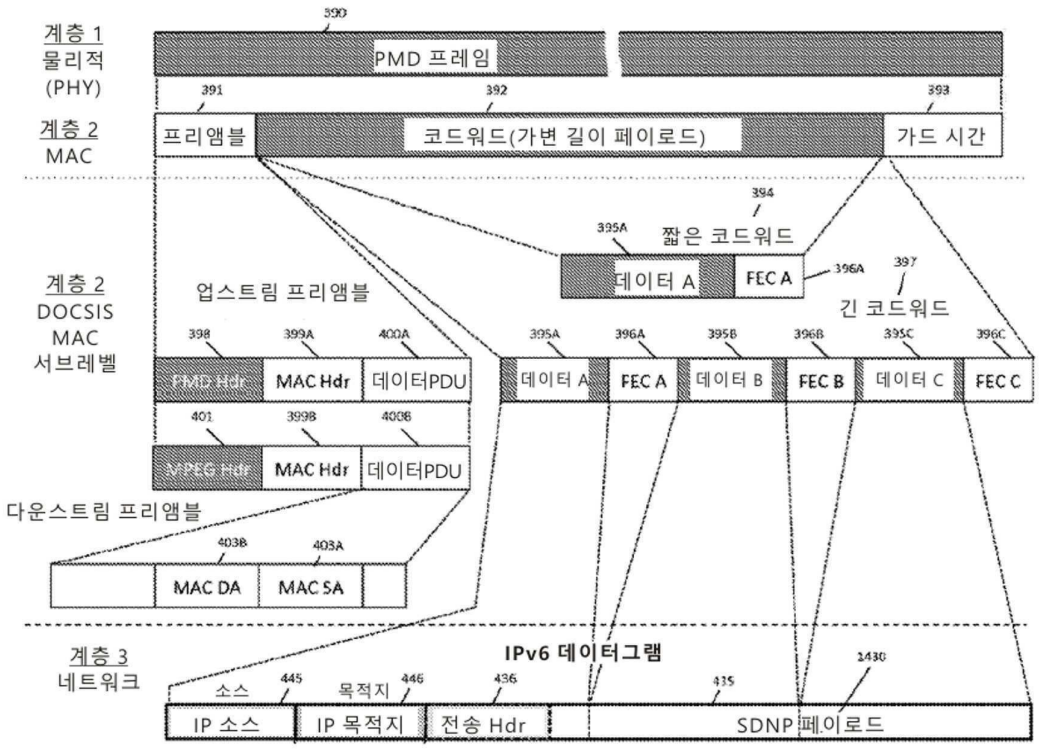
도면62


라스트 링크/BS 링크 WiFi 패킷A(클라이언트 대 SDNP 클라우드)
수신기
엑스미터
넷
소스
목적지
Pre
SFD
PLC
Ver
ID
MAC W
MAC R
SDNP 페이로드 A
FC
IPv6
UDP
802.11n, 2.4GHz
SDNP 클라이언트
다중-PHY WiFi 라스트 링크
WiFi 라우터
BS 링크
라우터
게이트웨이 링크
SDNP 게이트웨이
4G/LTE, 900MHz
라스트 링크/BS 링크 셀룰러 4G 패킷 B(클라이언트 대 SDNP 클라우드)
목적지
소스
MAC BS
데이터
PDCP Hdr
데이터
PDCP Hdr
데이터
소스
목적지
전송 Hdr
SDNP 페이로드 B

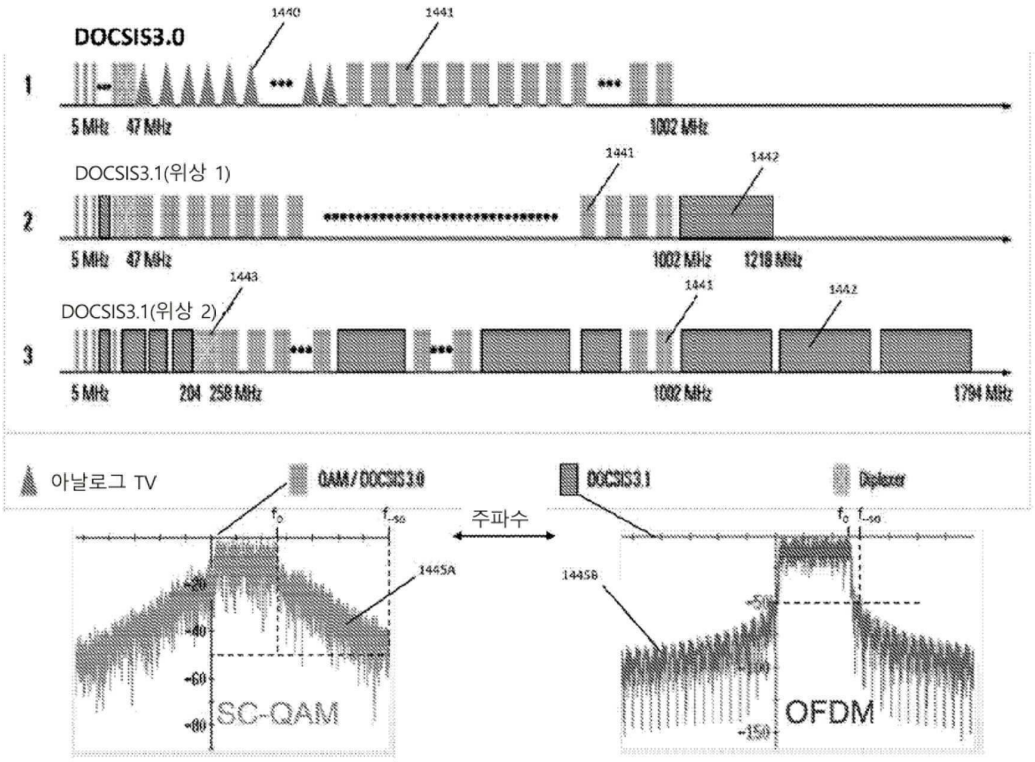
도면63


케이블 모뎀 단말 시스템(CMTS)
케이블 모뎀(CM)/셋탑 박스(STB)
SNMP
DHCPv4
DHCPv6
SDNP
TFTP
HTTP
Otr
계층 5 내지 7
앱
계층 4
전송
계층 3
IP 네트워크
UDP
UDP, TCP
IPv4, IPv6, ICMPv6, (SDNP)
데이터
링크 계층
포워딩
802.2 LLC
링크 보안
케이블 MAC
계층 2
미디어 액세스
제어(MAC)
투과
브릿징
HSD & IPTV
MAC
802.11 MAC
네트워크
인터페이스
케이블
인터페이스
계층 1
물리적(PHY)
이더넷(HSD)
또는 HDMI
WiFi
동축
or
광섬유

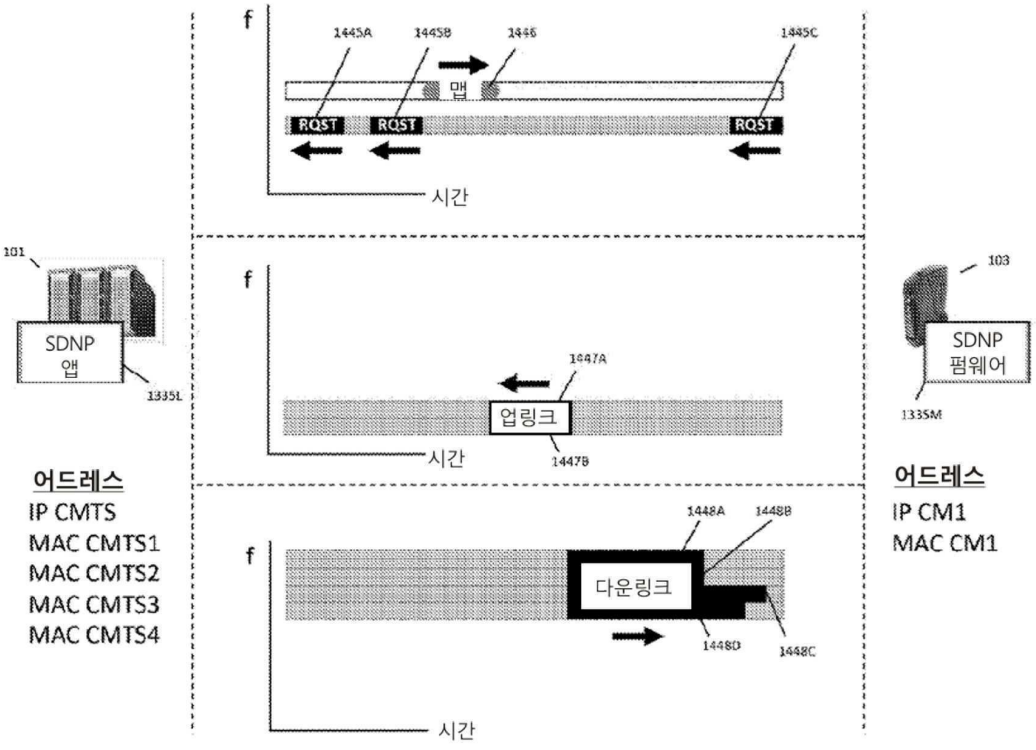
도면64


계층 1
물리적
(PHY)
PMD 프레임
계층 2
MAC
프리앰블
코드워드(가변 길이 페이로드)
가드 시간
짧은 코드워드
데이터 A
FEC A
긴 코드워드
계층 2
DOCSIS
MAC
서브레벨
업스트림 프리앰블
PMD Hdr
MAC Hdr
데이터PDU
데이터 A
FEC A
데이터 B
FEC B
데이터 C
FEC C
다운스트림 프리앰블
MAC DA
MAC SA
계층 3
네트워크
IPv6 데이터그램
소스
목적지
IP 소스
IP 목적지
전송 Hdr
SDNP 페이로드

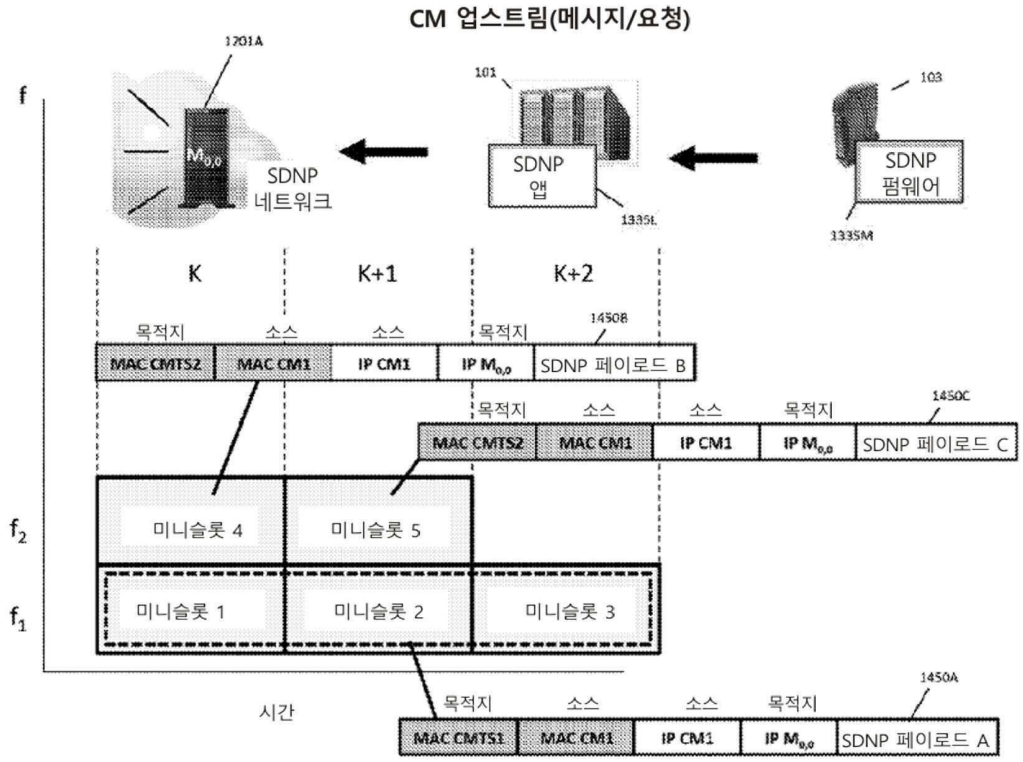
도면65a


DOCSIS3.0
1440
1441
1
5 MHz 47 MHz
1002 MHz
DOCSIS3.1(위상 1)
1441
1442
2
5 MHz 47 MHz
1002 MHz 1218 MHz
DOCSIS3.1(위상 2)
1443
1441
1442
3
5 MHz
204 258 MHz
1002 MHz
1794 MHz
아날로그 TV
QAM/DOCSIS3.0
DOCSIS3.1
Diplexer
주파수
1445A
1445B
SC-QAM
OFDM

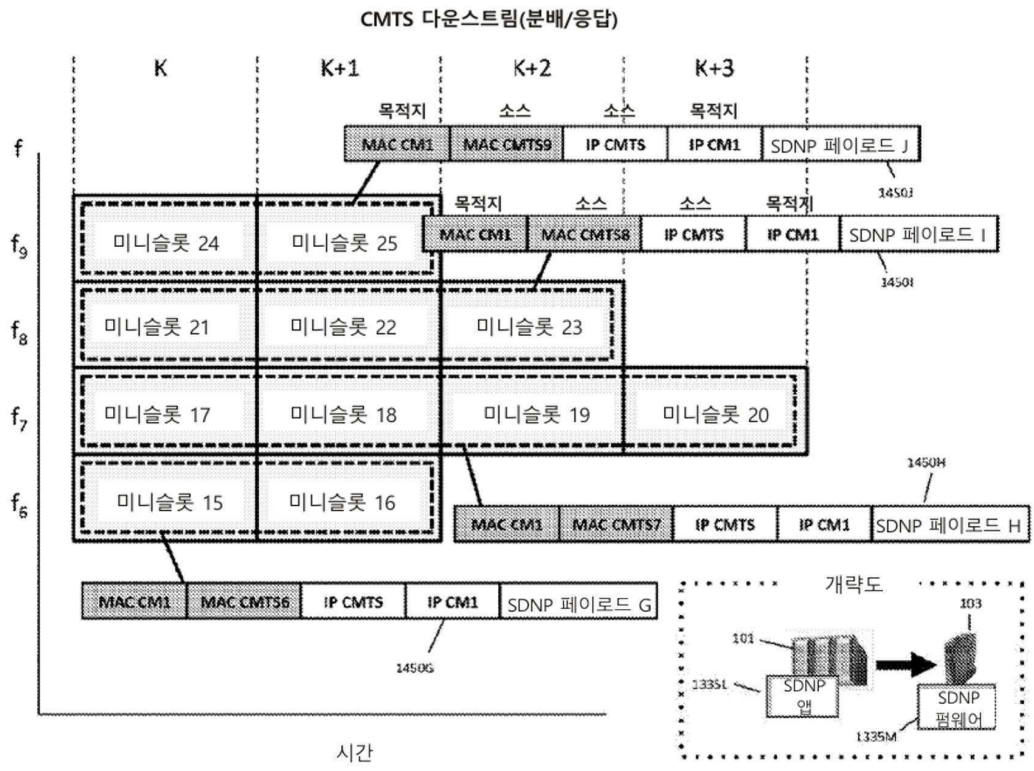
도면65b


f
1445A
1445B
1446
1445C
맵
RQST
RQST
RQST
시간
101
SDNP
앱
1335L
f
1447A
업링크
시간
1447B
103
SDNP
펌웨어
1335M
어드레스
IP CMTS
MAC CMTS1
MAC CMTS2
MAC CMTS3
MAC CMTS4
f
1448A
1448B
다운링크
1448D
1448C
시간
어드레스
IP CM1
MAC CM1

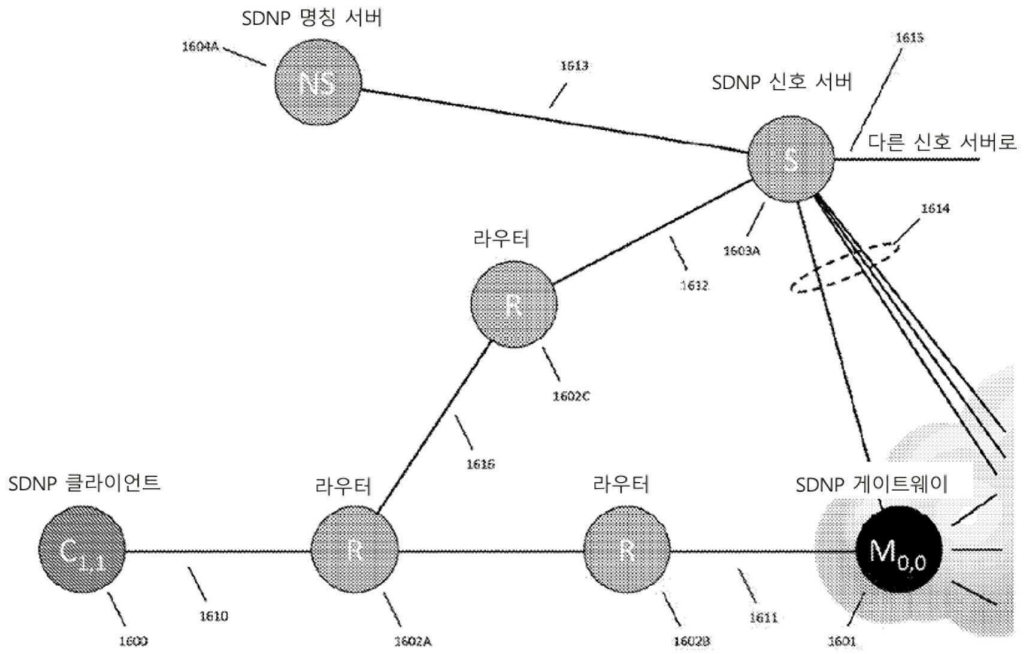
도면65c


CM 업스트림(메시지/요청)
1201A
101
103
SDNP 네트워크
SDNP 앱
SDNP 펌웨어
1335L
1335M
f
K
K+1
K+2
목적지
소스
소스
목적지
14508
MAC CMTS2
MAC CM1
IP CM1
IP M0,0
SDNP 페이로드 B
1450C
SDNP 페이로드 C
f2
f1
미니슬롯 4
미니슬롯 5
미니슬롯 1
미니슬롯 2
미니슬롯 3
시간
1450A
MAC CMTS1
SDNP 페이로드 A

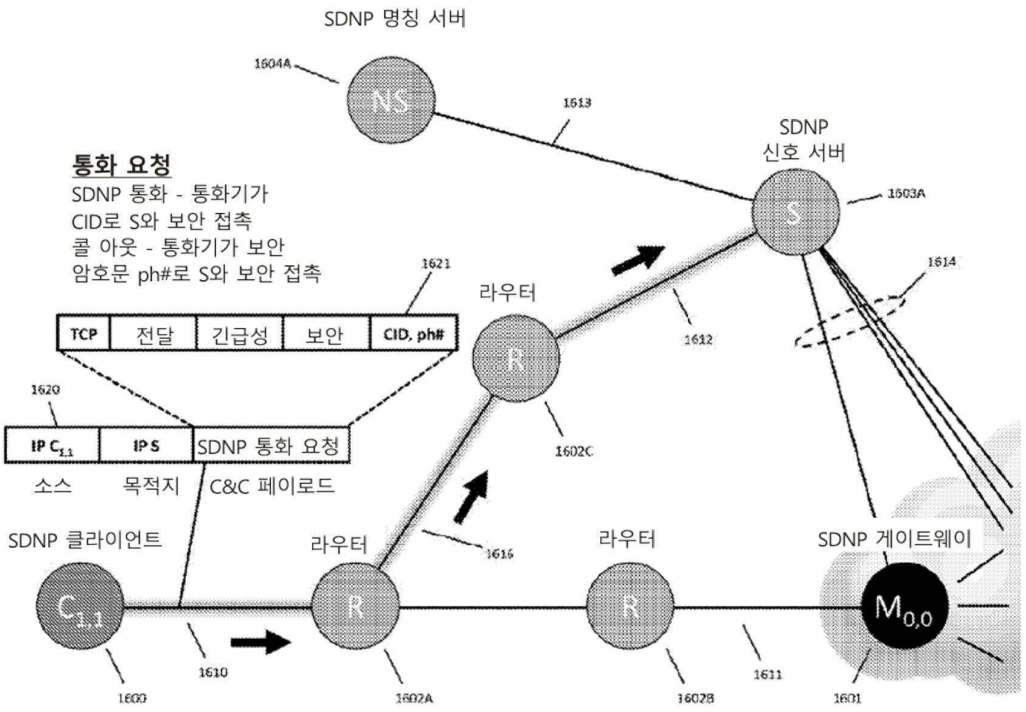
도면65d


CMTS 다운스트림(분배/응답)
K
K+1
K+2
K+3
f
목적지
소스
소스
목적지
MAC CM1
MAC CMTS9
IP CMTS
IP CM1
SDNP 페이로드 J
1450J
MAC CMTS8
SDNP 페이로드 I
1450I
f9
f8
f7
f6
미니슬롯 24
미니슬롯 25
미니슬롯 21
미니슬롯 22
미니슬롯 23
미니슬롯 17
미니슬롯 18
미니슬롯 19
미니슬롯 20
미니슬롯 15
미니슬롯 16
1450H
MAC CMTS7
SDNP 페이로드 H
MAC CMTS6
SDNP 페이로드 G
1450G
개략도
101
103
1335L
SDNP 앱
SDNP 펌웨어
1335M
시간

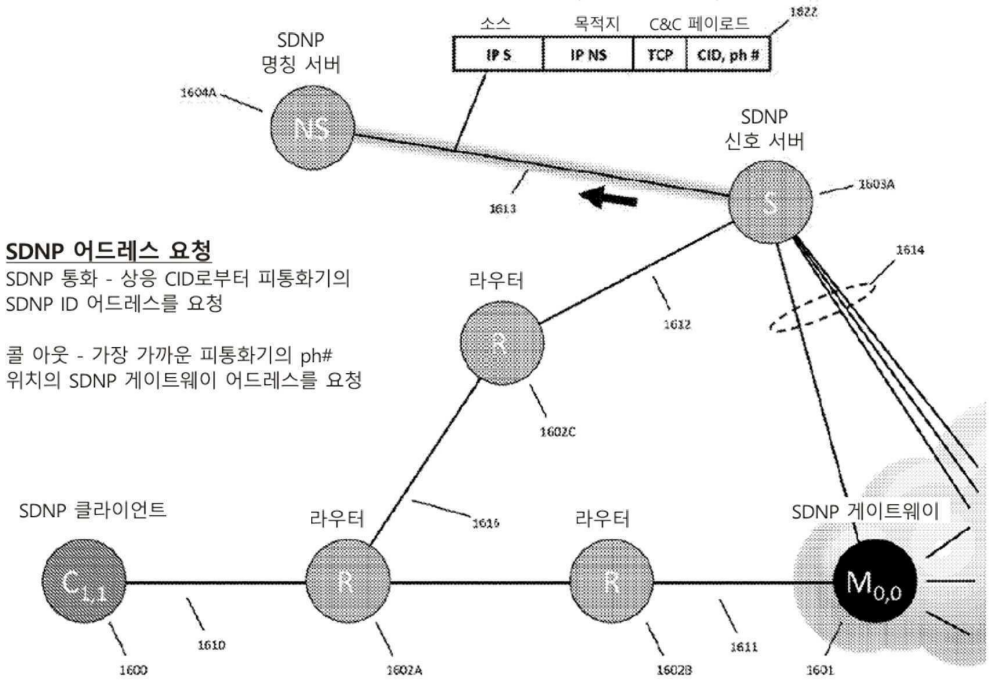
도면66


SDNP 명칭 서버
1604A
NS
1613
SDNP 신호 서버
1615
다른 신호 서버로
S
1614
1603A
라우터
1632
R
1602C
1616
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
C1,1
R
R
M0,0
1600
1610
1602A
1602B
1611
1601

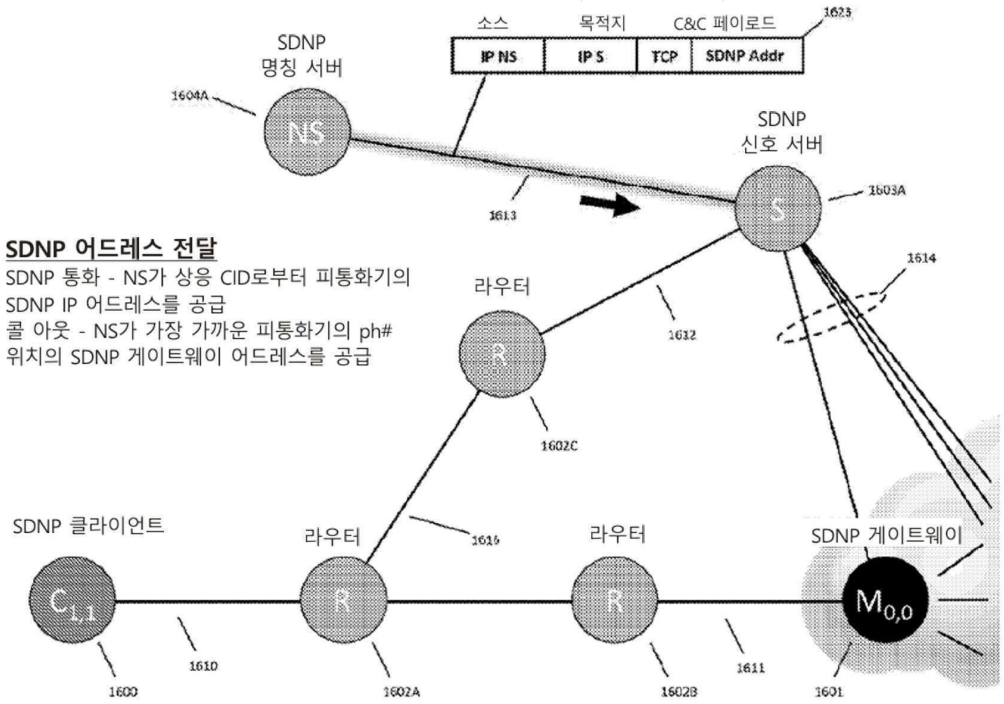
도면67


SDNP 명칭 서버
1604A
NS
1613
SDNP
신호 서버
S
1603A
통화 요청
SDNP 통화 - 통화기가
CID로 S와 보안 접촉
콜 아웃 - 통화기가 보안
암호문 ph#로 S와 보안 접촉
1621
1614
라우터
1612
R
1602C
TCP
전달
긴급성
보안
CID, ph#
1620
IP C1,1
IP S
SDNP 통화 요청
소스
목적지
C&C 페이로드
1616
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
C1,1
R
R
M0,0
1600
1610
1602A
1602B
1611
1601

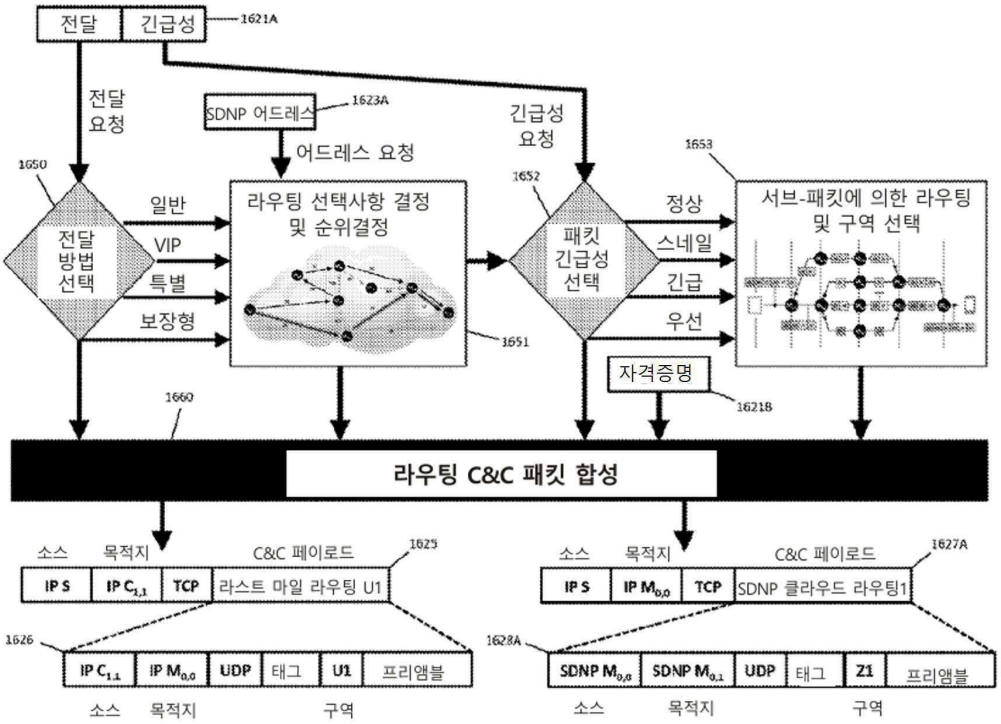
도면68


소스
목적지
C&C 페이로드
1622
IP S
IP NS
TCP
CID, ph #
SDNP
명칭 서버
1604A
NS
SDNP
신호 서버
S
1603A
1613
1614
라우터
R
1612
1602C
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
$C_{1,1}$
R
R
$M_{0,0}$
1615
1610
1600
1602A
1602B
1611
1601
SDNP 어드레스 요청
SDNP 통화 - 상응 CID로부터 피통화기의 SDNP ID 어드레스를 요청
콜 아웃 - 가장 가까운 피통화기의 ph# 위치의 SDNP 게이트웨이 어드레스를 요청

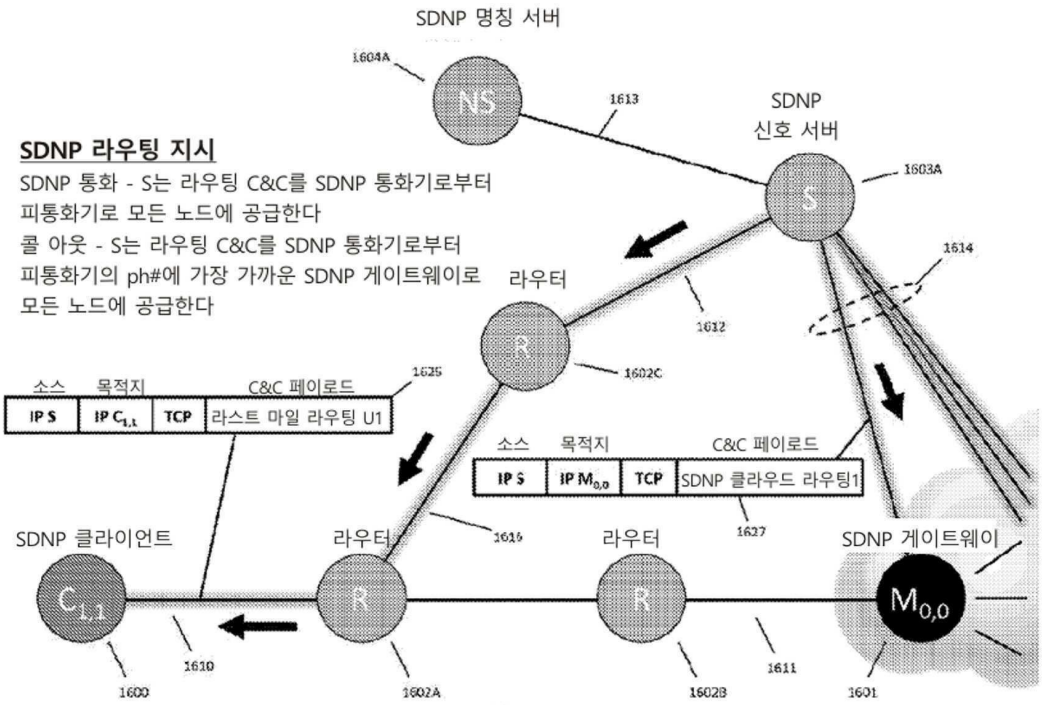
도면69


소스
목적지
C&C 페이로드
1623
IP NS
IP S
TCP
SDNP Addr
SDNP
명칭 서버
1604A
NS
SDNP
신호 서버
S
1603A
1613
1614
라우터
R
1612
1602C
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
$C_{1,1}$
R
R
$M_{0,0}$
1615
1610
1600
1602A
1602B
1611
1601
SDNP 어드레스 전달
SDNP 통화 - NS가 상응 CID로부터 피통화기의 SDNP IP 어드레스를 공급
콜 아웃 - NS가 가장 가까운 피통화기의 ph# 위치의 SDNP 게이트웨이 어드레스를 공급

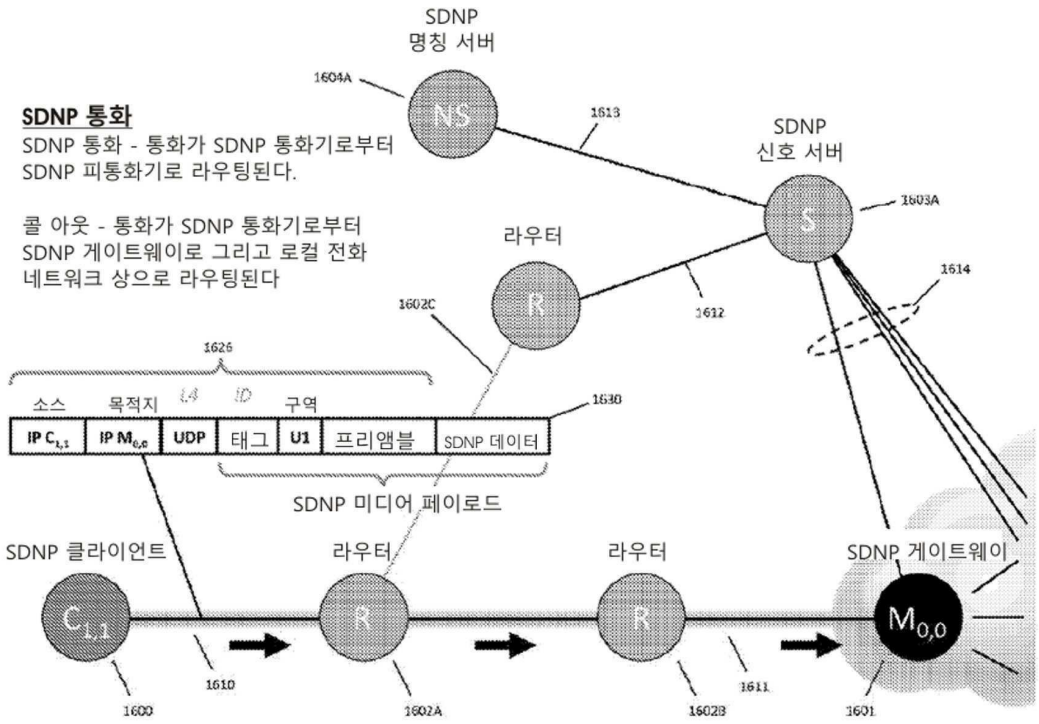
도면70


전달
긴급성
1621A
전달 요청
SDNP 어드레스
1623A
어드레스 요청
긴급성 요청
1650
전달 방법 선택
일반
VIP
특별
보장형
라우팅 선택사항 결정 및 순위결정
1651
1652
패킷 긴급성 선택
정상
스네일
긴급
우선
1653
서브-패킷에 의한 라우팅 및 구역 선택
자격증명
1621B
1660
라우팅 C&C 패킷 합성
소스
목적지
C&C 페이로드
1625
IP S
IP C1,1
TCP
라스트 마일 라우팅 U1
1626
IP C1,1
IP M0,0
UDP
태그
U1
프리앰블
소스
목적지
구역
소스
목적지
C&C 페이로드
1627A
IP S
IP M0,0
TCP
SDNP 클라우드 라우팅1
1628A
SDNP M0,0
SDNP M0,1
UDP
태그
Z1
프리앰블
소스
목적지
구역

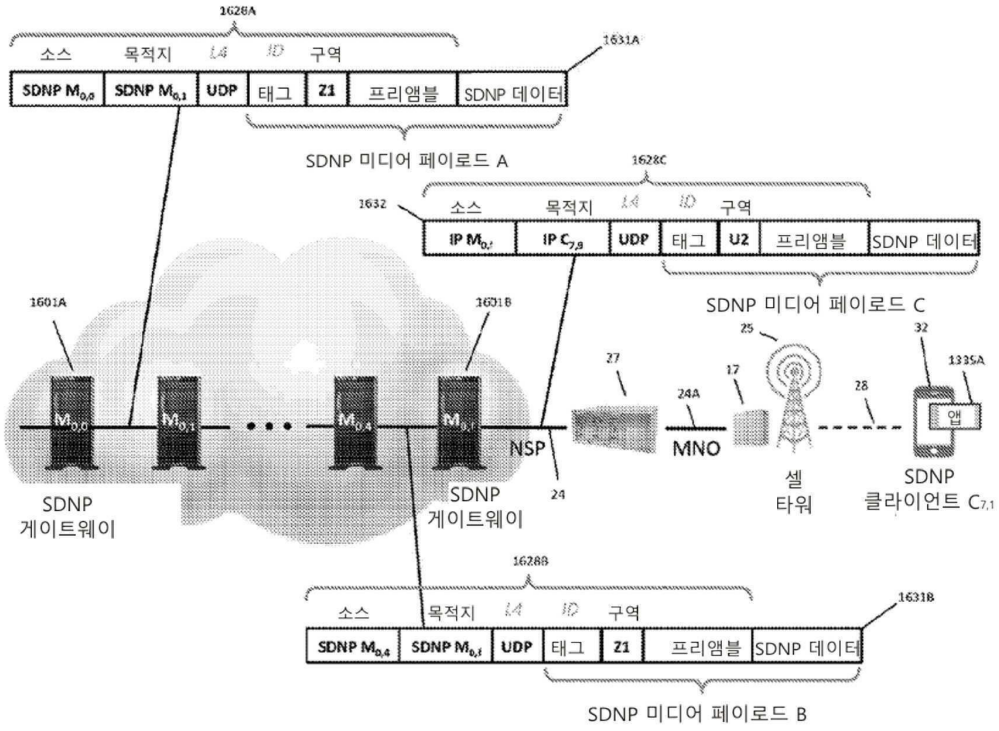
도면71


SDNP 명칭 서버
1604A
NS
1613
SDNP
신호 서버
1603A
S
SDNP 라우팅 지시
SDNP 통화 - S는 라우팅 C&C를 SDNP 통화기로부터 피통화기로 모든 노드에 공급한다
콜 아웃 - S는 라우팅 C&C를 SDNP 통화기로부터 피통화기의 ph#에 가장 가까운 SDNP 게이트웨이로 모든 노드에 공급한다
1614
라우터
1612
R
1602C
소스
목적지
C&C 페이로드
1625
IP S
IP C1,1
TCP
라스트 마일 라우팅 U1
소스
목적지
C&C 페이로드
IP S
IP M0,0
TCP
SDNP 클라우드 라우팅1
1627
SDNP 클라이언트
라우터
1619
라우터
SDNP 게이트웨이
C1,1
R
R
M0,0
1610
1600
1602A
1602B
1611
1601

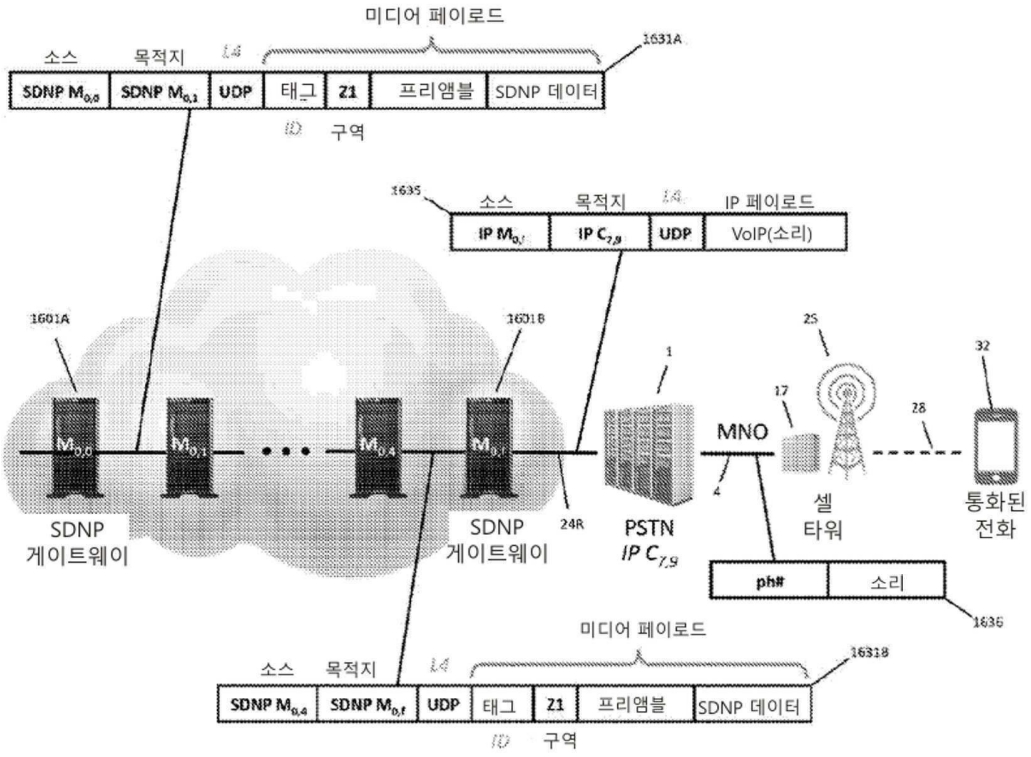
도면72


SDNP
명칭 서버
1604A
NS
1613
SDNP
신호 서버
S
1603A
SDNP 통화
SDNP 통화 - 통화가 SDNP 통화기로부터
SDNP 피통화기로 라우팅된다.
콜 아웃 - 통화가 SDNP 통화기로부터
SDNP 게이트웨이로 그리고 로컬 전화
네트워크 상으로 라우팅된다
라우터
R
1602C
1612
1614
1626
소스
목적지
L4
ID
구역
IP C1,1
IP M0,0
UDP
태그
U1
프리앰블
SDNP 데이터
1630
SDNP 미디어 페이로드
SDNP 클라이언트
라우터
라우터
SDNP 게이트웨이
C1,1
R
R
M0,0
1600
1610
1602A
1602B
1611
1601

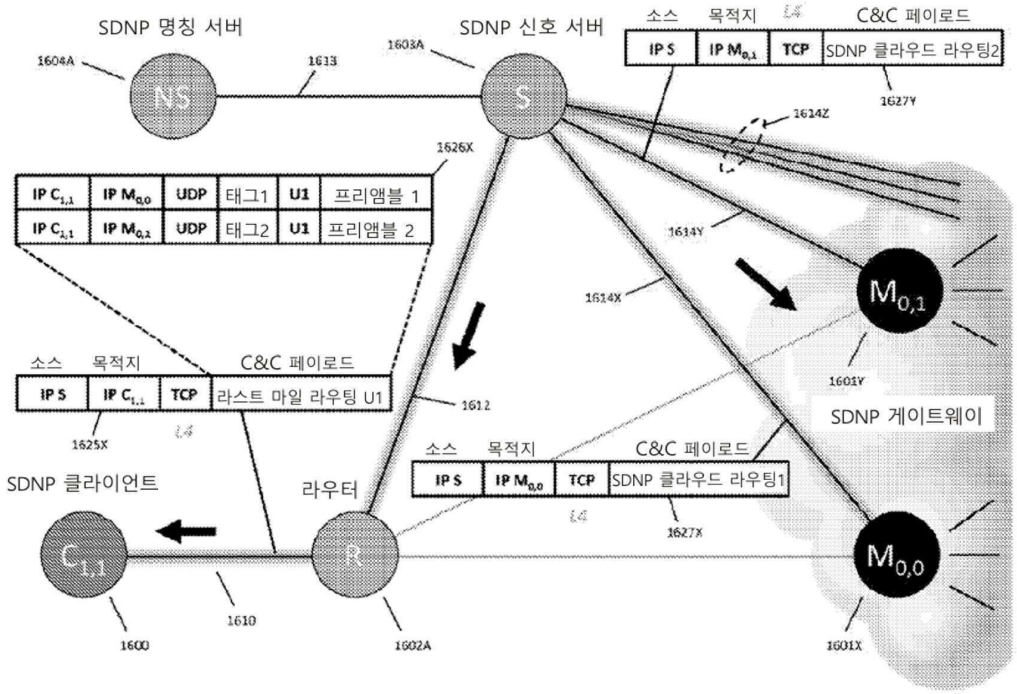
도면73a


1628A
소스
목적지
L4
ID
구역
1631A
SDNP M0,0
SDNP M0,1
UDP
태그
Z1
프리앰블
SDNP 데이터
SDNP 미디어 페이로드 A
1628C
1632
소스
목적지
L4
ID
구역
IP M0,7
IP C7,8
UDP
태그
U2
프리앰블
SDNP 데이터
SDNP 미디어 페이로드 C
1601A
1601B
M0,0
M0,1
M0,4
M0,5
NSP
24
27
24A
MNO
17
25
28
32
1335A
앱
셀
타워
SDNP
클라이언트 C7,1
SDNP
게이트웨이
SDNP
게이트웨이
16288
소스
목적지
L4
ID
구역
1631B
SDNP M0,4
SDNP M0,5
UDP
태그
Z1
프리앰블
SDNP 데이터
SDNP 미디어 페이로드 B

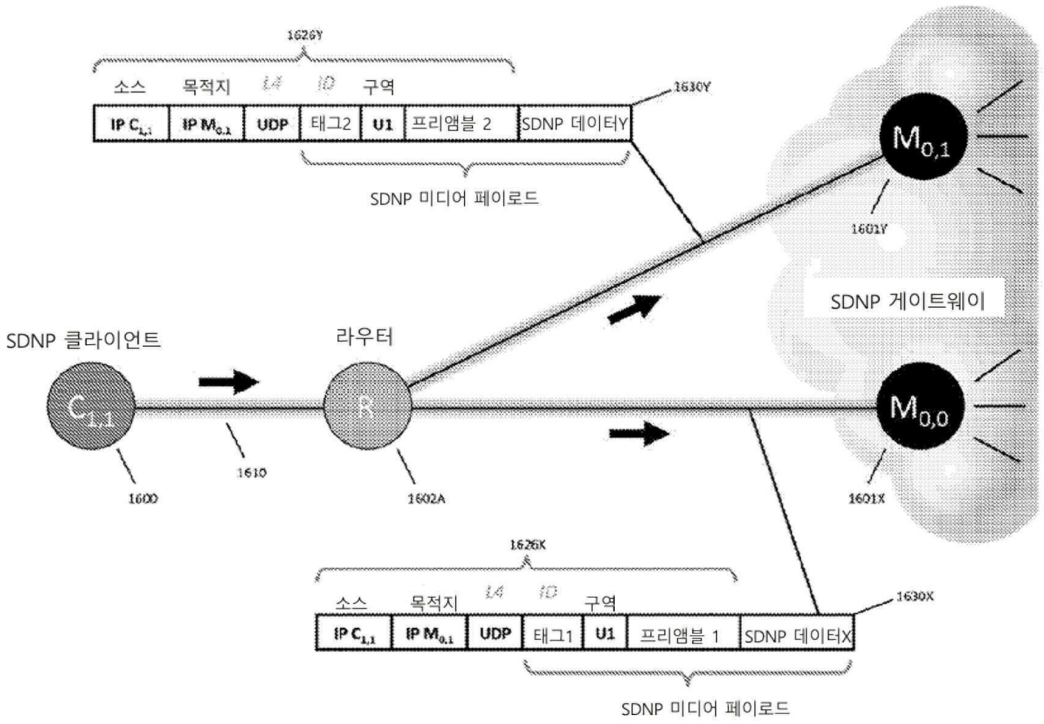
도면73b


미디어 페이로드
소스
목적지
L4
1631A
SDNP $M_{0,0}$
SDNP $M_{0,1}$
UDP
태그
Z1
프리앰블
SDNP 데이터
ID
구역
1635
소스
목적지
L4
IP 페이로드
IP $M_{0,f}$
IP $C_{7,9}$
UDP
VoIP(소리)
1601A
1601B
25
32
1
17
28
MNO
4
셀
타워
통화된
전화
SDNP
게이트웨이
24R
SDNP
게이트웨이
PSTN
IP $C_{7,9}$
ph#
소리
1636
미디어 페이로드
소스
목적지
L4
16318
SDNP $M_{0,4}$
SDNP $M_{0,f}$
UDP
태그
Z1
프리앰블
SDNP 데이터
ID
구역

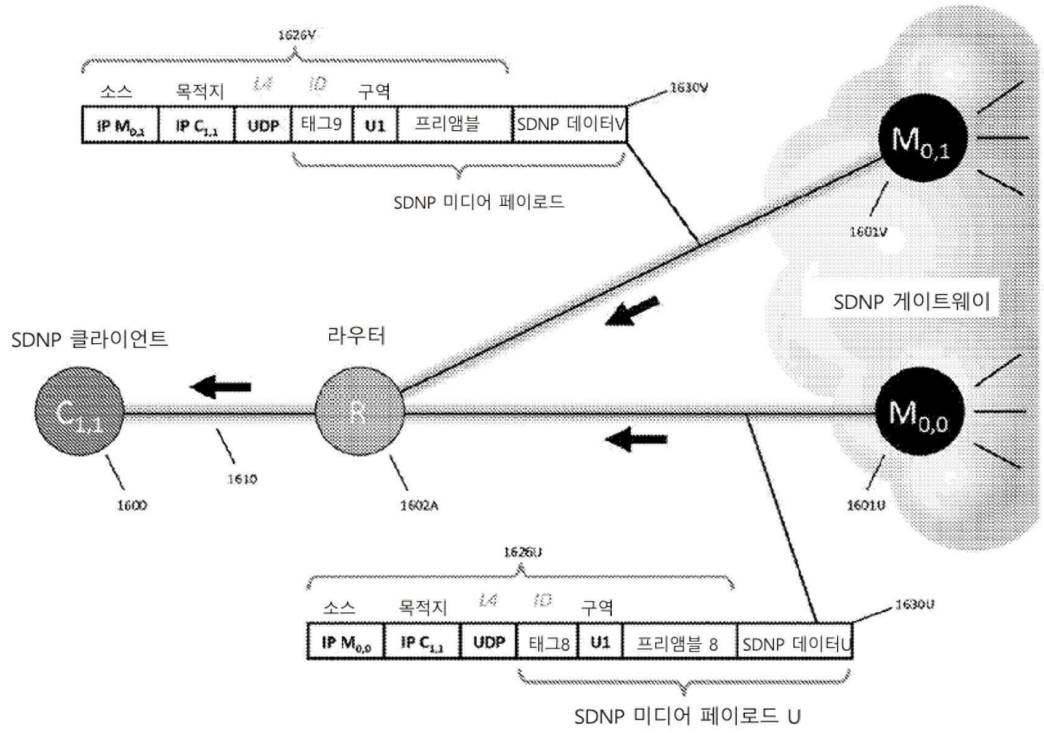
도면74


SDNP 명칭 서버
SDNP 신호 서버
1604A
NS
1613
1603A
S
소스
목적지
L4
C&C 페이로드
IP S
IP $M_{0,1}$
TCP
SDNP 클라우드 라우팅2
1627Y
1614Z
1626X
IP $C_{1,1}$
IP $M_{0,0}$
UDP
태그1
U1
프리앰블 1
IP $C_{1,1}$
IP $M_{0,1}$
UDP
태그2
U1
프리앰블 2
1614Y
1614X
$M_{0,1}$
1601Y
소스
목적지
C&C 페이로드
IP S
IP $C_{1,1}$
TCP
라스트 마일 라우팅 U1
1625X
L4
1612
SDNP 게이트웨이
소스
목적지
C&C 페이로드
IP S
IP $M_{0,0}$
TCP
SDNP 클라우드 라우팅1
L4
1627X
SDNP 클라이언트
라우터
$C_{1,1}$
R
$M_{0,0}$
1600
1610
1602A
1601X

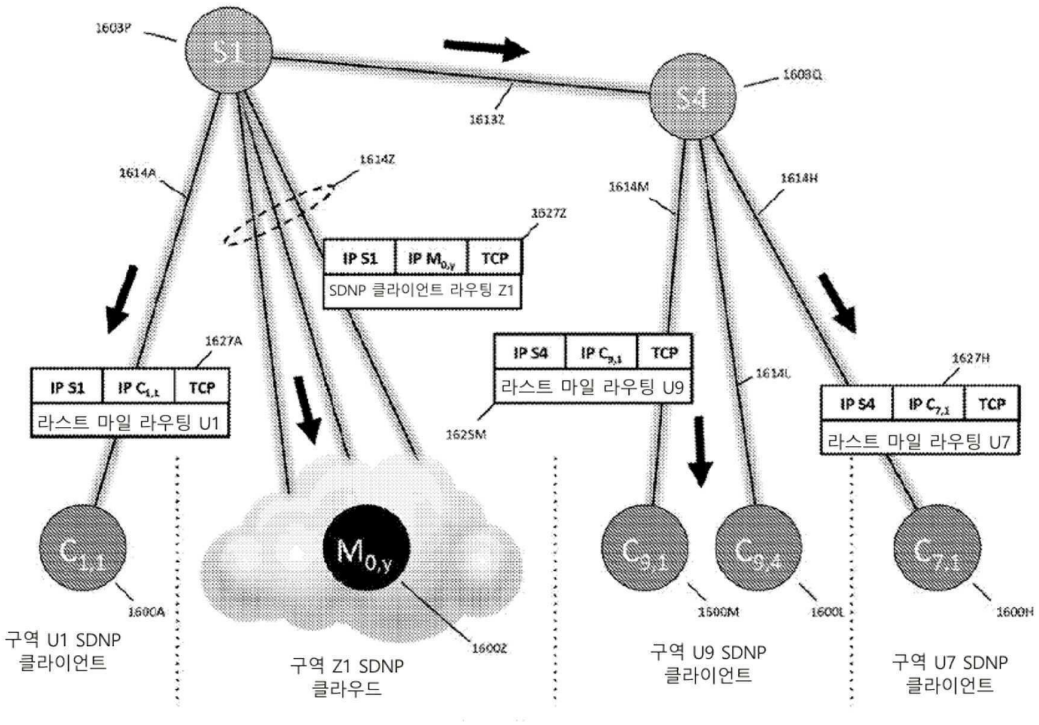
도면75a


1626Y
소스
목적지
L4
ID
구역
1630Y
IP C1,1
IP M0,1
UDP
태그2
U1
프리앰블 2
SDNP 데이터Y
SDNP 미디어 페이로드
M0,1
1601Y
SDNP 게이트웨이
SDNP 클라이언트
라우터
C1,1
R
M0,0
1600
1610
1602A
1601X
1626X
소스
목적지
L4
ID
구역
1630X
IP C1,1
IP M0,1
UDP
태그1
U1
프리앰블 1
SDNP 데이터X
SDNP 미디어 페이로드

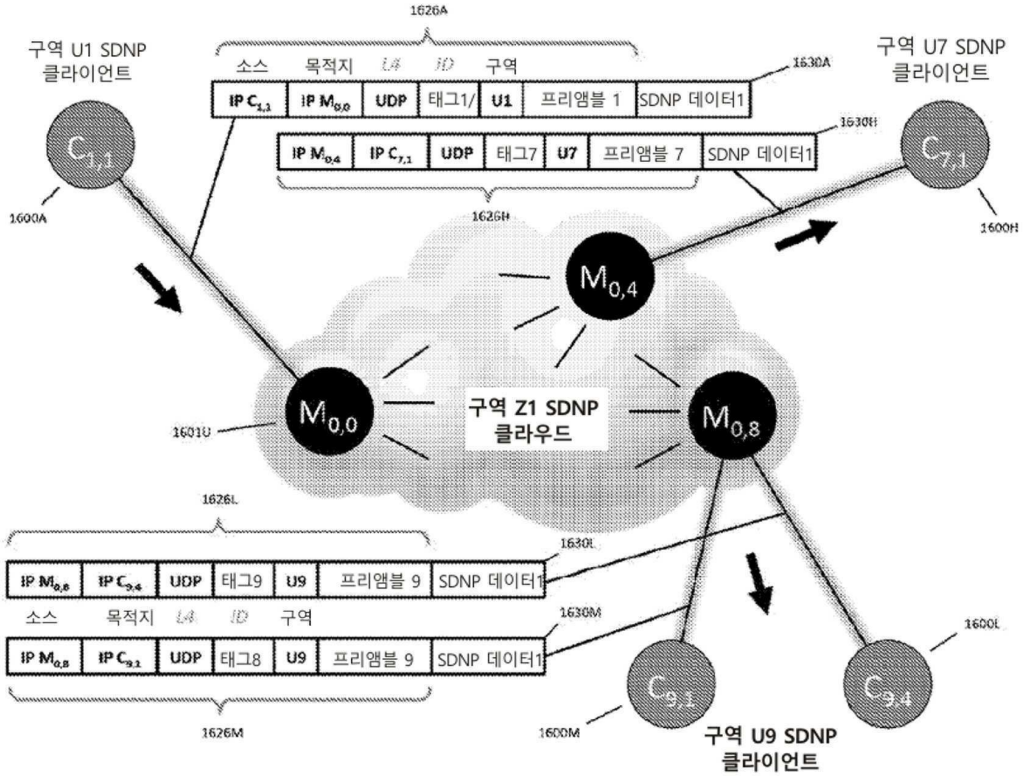
도면75b


1626V
소스
목적지
L4
ID
구역
1630V
IP M0,1
IP C1,1
UDP
태그9
U1
프리앰블
SDNP 데이터V
SDNP 미디어 페이로드
M0,1
1601V
SDNP 게이트웨이
SDNP 클라이언트
라우터
C1,1
R
M0,0
1600
1610
1602A
1601U
1626U
소스
목적지
L4
ID
구역
1630U
IP M0,0
IP C1,1
UDP
태그8
U1
프리앰블 8
SDNP 데이터U
SDNP 미디어 페이로드 U

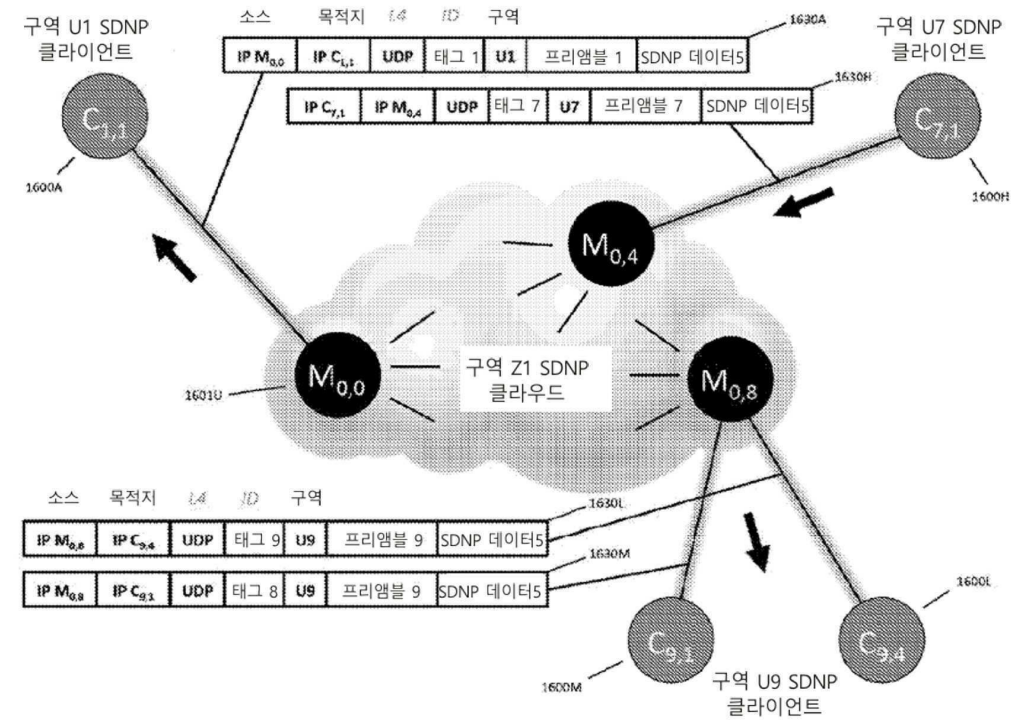
도면76


S1
S4
IP S1 | IP M0,y | TCP
SDNP 클라이언트 라우팅 Z1
IP S1 | IP C1,1 | TCP
라스트 마일 라우팅 U1
IP S4 | IP C3,1 | TCP
라스트 마일 라우팅 U9
IP S4 | IP C7,1 | TCP
라스트 마일 라우팅 U7
C1,1
M0,y
C3,1
C3,4
C7,1
구역 U1 SDNP 클라이언트
구역 Z1 SDNP 클라우드
구역 U9 SDNP 클라이언트
구역 U7 SDNP 클라이언트

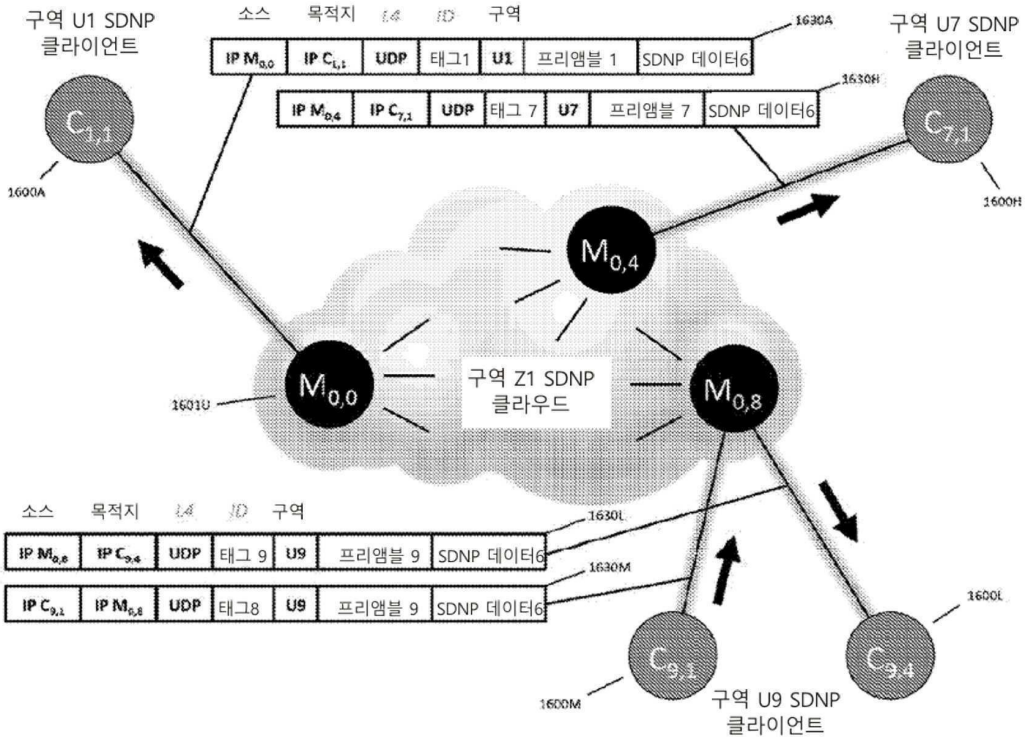
도면77a


구역 U1 SDNP 클라이언트
구역 U7 SDNP 클라이언트
소스 목적지 L4 ID 구역
IP C1,1 | IP M0,0 | UDP | 태그1/ | U1 | 프리앰블 1 | SDNP 데이터1
IP M0,4 | IP C7,1 | UDP | 태그7 | U7 | 프리앰블 7 | SDNP 데이터1
C1,1
C7,1
M0,4
M0,0
M0,8
구역 Z1 SDNP 클라우드
IP M0,8 | IP C3,4 | UDP | 태그9 | U9 | 프리앰블 9 | SDNP 데이터1
소스 목적지 L4 ID 구역
IP M0,8 | IP C3,1 | UDP | 태그8 | U9 | 프리앰블 9 | SDNP 데이터1
C3,1
C3,4
구역 U9 SDNP 클라이언트

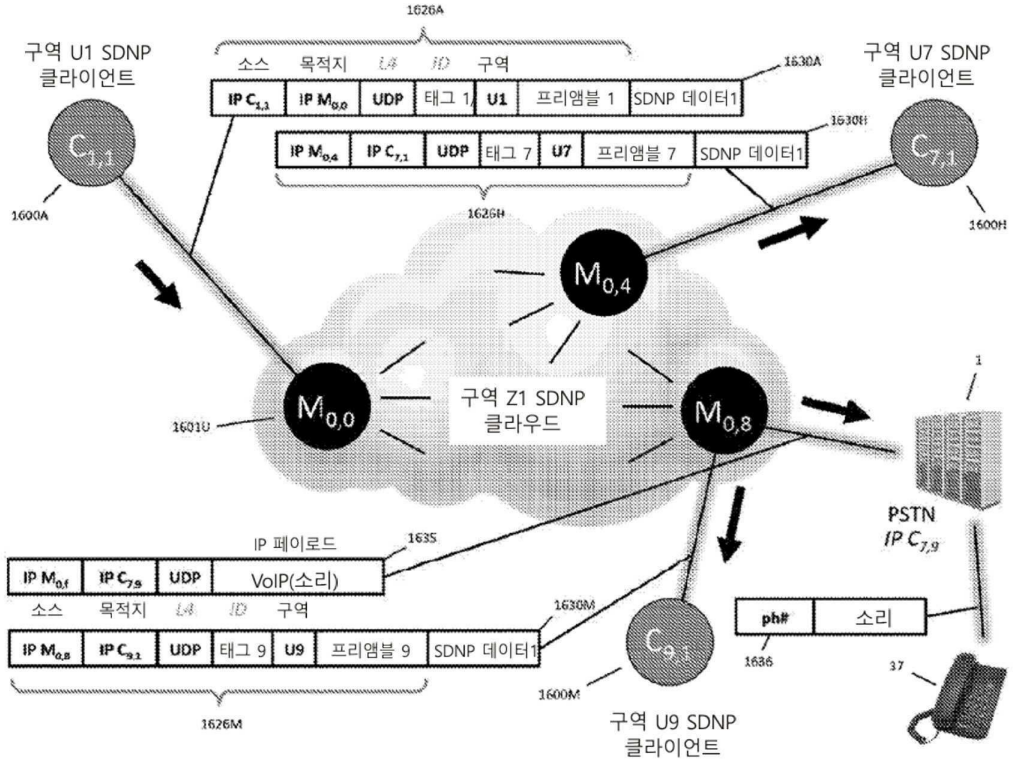
도면77b


구역 U1 SDNP 클라이언트
구역 U7 SDNP 클라이언트
구역 Z1 SDNP 클라우드
구역 U9 SDNP 클라이언트
소스
목적지
L4
ID
구역
UDP
프리앰블 1
프리앰블 7
프리앰블 9
SDNP 데이터5
1630A
1630H
1630L
1630M
1600A
1600H
1600L
1600M
1601U

도면77c


구역 U1 SDNP 클라이언트
구역 U7 SDNP 클라이언트
구역 Z1 SDNP 클라우드
구역 U9 SDNP 클라이언트
소스
목적지
L4
ID
구역
UDP
프리앰블 1
프리앰블 7
프리앰블 9
SDNP 데이터6
1630A
1630H
1630L
1630M
1600A
1600H
1600L
1600M
1601U

도면78




도면79a

| 그룹 통화 클라이언트 | | 정규 통화 | 프라이빗 통화 | |
|---|---|---|---|---|
| 네트워크 노드 | 사용자 인증 | 모든 참여자 | 인증된 SDNP 클라이언트 | 미인증 SDNP 클라이언트 |
| $C_{1,1}$ | SDNP 클라이언트 그룹 호스트 | 듣기, 말하기 | 듣기, 말하기 | - |
| $C_{7,1}$ | SDNP 클라이언트 참여자 | 듣기, 말하기 | 듣기, 말하기 | 마이크로폰 & 스피커 묵음 처리 |
| $C_{9,1}$ | SDNP 클라이언트 참여자 | 듣기, 말하기 | 듣기, 말하기 | |
| $C_{9,4}$ | SDNP 클라이언트 청취자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | |
| Ph #1 | 콜 아웃 참여자 | 듣기, 말하기 | 마이크로폰& 스피커 묵음 | |
| Ph #2 | 콜 아웃 청취자 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | |

도면79b

| 그룹 통화 클라이언트 | | 정규 통화 | 하이퍼-프라이빗 통화 | |
|---|---|---|---|---|
| 네트워크 노드 | 사용자 인증 | 모든 참여자 | 인증된 SDNP 클라이언트 | 미인증 SDNP 클라이언트 |
| $C_{1,1}$ | SDNP 클라이언트 프라이빗 그룹 호스트 | 듣기, 말하기 | 듣기, 말하기 | - |
| $C_{7,1}$ | SDNP 클라이언트 프라이빗 참여자 | 듣기, 말하기 | 듣기, 말하기 | 마이크로폰 & 스피커 묵음 처리 |
| $C_{9,1}$ | SDNP 클라이언트 참여자 | 듣기, 말하기 | 마이크로폰& 스피커 묵음 | |
| $C_{9,4}$ | SDNP 클라이언트 프라이빗 청취자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | |
| $C_{9,5}$ | SDNP 클라이언트 청취자 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | |
| Ph #1 | 콜 아웃 참여자 | 듣기, 말하기 | 마이크로폰& 스피커 묵음 | |
| Ph #2 | 콜 아웃 청취자 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | |

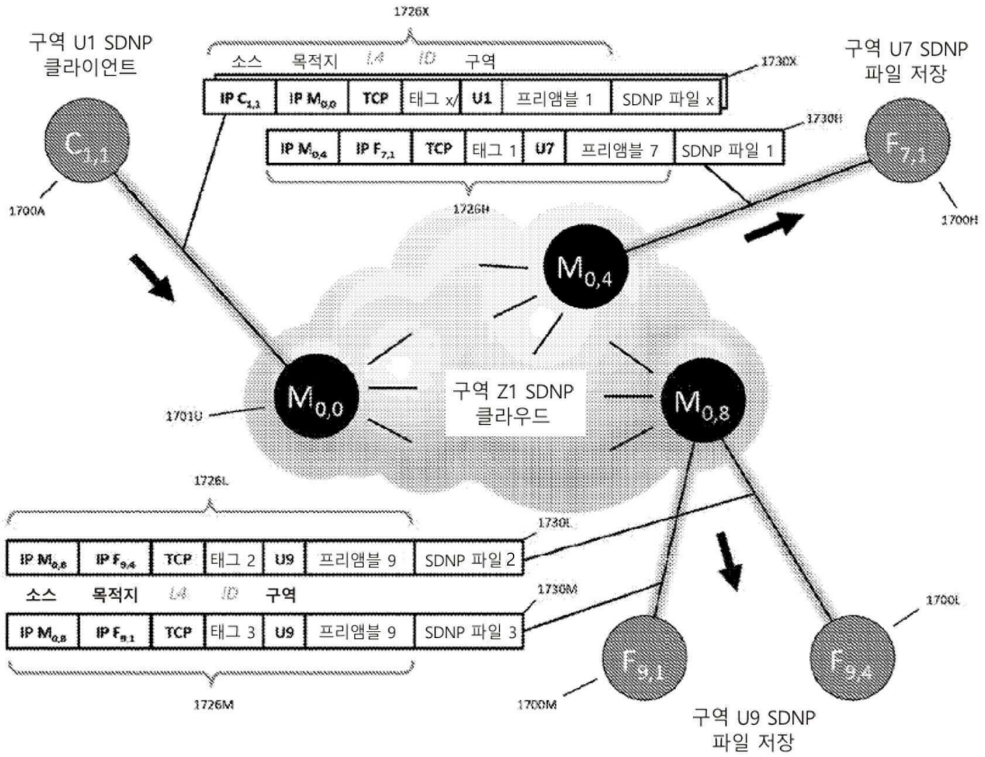
도면80a

| PTT 그룹 통화 클라이언트 | | 정규 푸시-투-토크 | | 프라이빗 푸시-투-토크 | | |
|---|---|---|---|---|---|---|
| 네트워크 노드 | 사용자 인증 | 호스트 PTT | 다른 PTT | 인증된 호스트 PTT | 인증된 다른 PTT | 미인증 당사자 |
| $C_{1,1}$ | SDNP 클라이언트 그룹 호스트 | 말하기, 우선 묵음 | 듣기만, 마이크 묵음 | 말하기, 우선 묵음 | 듣기만, 마이크 묵음 | - |
| $C_{7,1}$ | SDNP 클라이언트 참여자 | 듣기만, 마이크 묵음 | 말하기, 다른것 묵음 | 듣기만, 마이크 묵음 | 말하기, 모든 다른 것 묵음 | 마이크로폰& 스피커 묵음 |
| $C_{9,1}$ | SDNP 클라이언트 참여자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | |
| $C_{9,4}$ | SDNP 클라이언트 청취자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | |
| $C_{9,5}$ | SDNP 클라이언트 청취자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | |
| Ph #1 | 콜 아웃 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | 마이크로폰& 스피커 묵음 | |

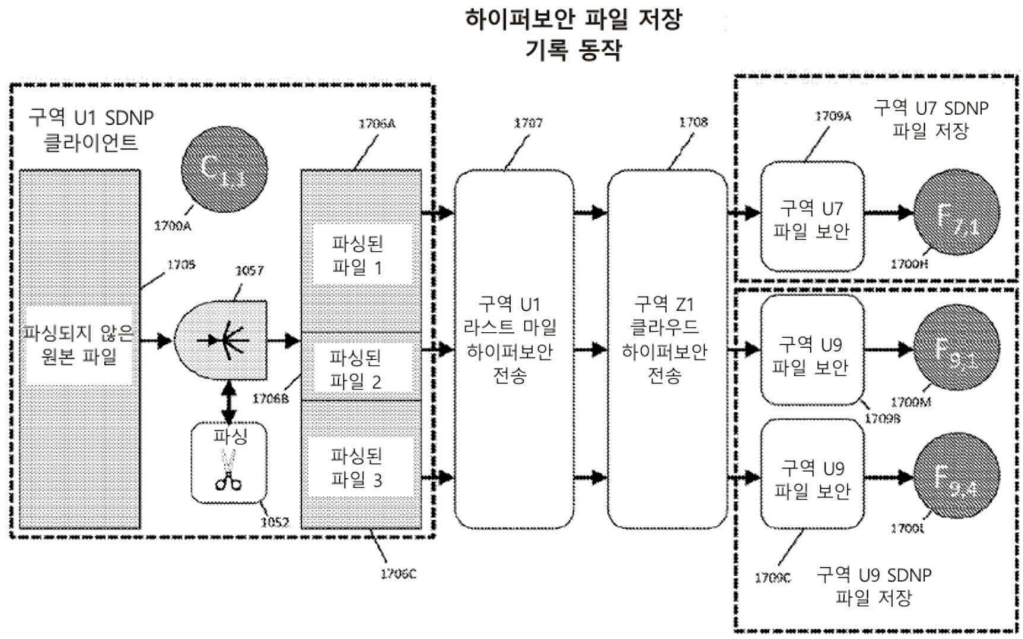
도면80b

| PTT 그룹 통화 클라이언트 | | 정규 푸시-투-토크 | | 하이퍼-프라이빗 푸시-투-토크 | | |
|---|---|---|---|---|---|---|
| 네트워크 노드 | 사용자 인증 | 호스트 PTT | 다른 PTT | 인증된 호스트 PTT | 인증된 다른 PTT | 미인증 당사자 |
| $C_{1,1}$ | SDNP 클라이언트 그룹 호스트 | 말하기, 우선 묵음 | 듣기만, 마이크 묵음 | 말하기, 우선 묵음 | 듣기만, 마이크 묵음 | – |
| $C_{7,1}$ | SDNP 클라이언트 프라이빗 참여자 | 듣기만, 마이크 묵음 | 말하기, 다른 것 묵음 | 듣기만, 마이크 묵음 | 말하기, 다른 것 묵음 | |
| $C_{9,1}$ | SDNP 클라이언트 참여자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | 마이크로폰& 스피커 묵음 | |
| $C_{9,A}$ | SDNP 클라이언트 프라이빗 청취자 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 |
| $C_{9,5}$ | SDNP 클라이언트 듣기만 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | 마이크로폰& 스피커 묵음 | |
| Ph # | 콜 아웃 | 듣기만, 마이크 묵음 | 듣기만, 마이크 묵음 | 마이크로폰& 스피커 묵음 | 마이크로폰& 스피커 묵음 | |

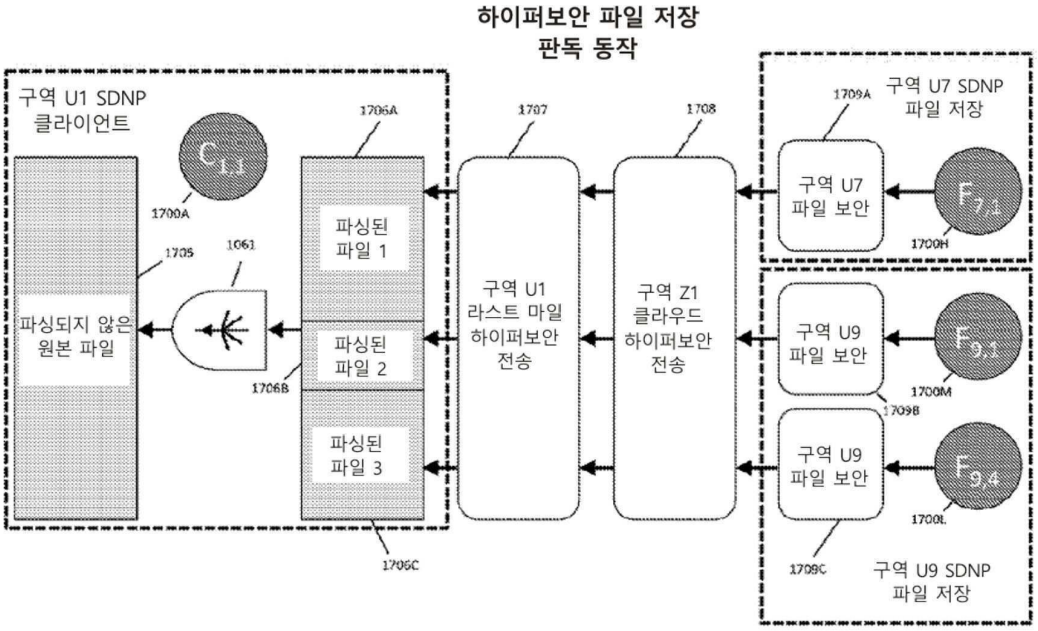
도면81



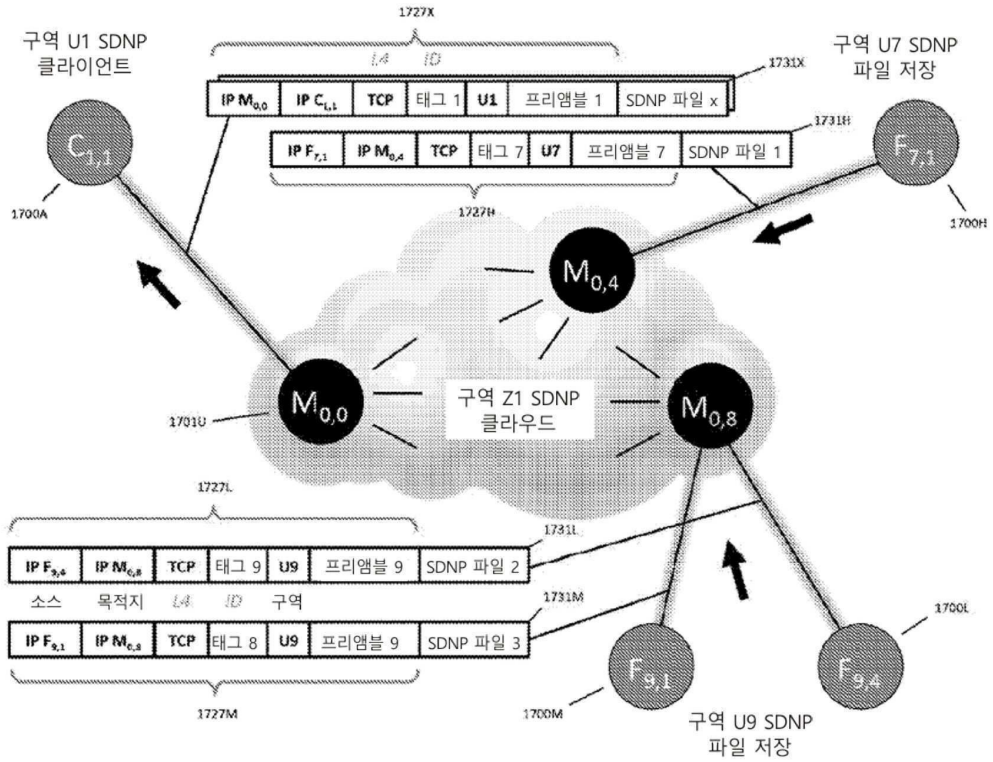
도면82a


하이퍼보안 파일 저장
기록 동작
구역 U1 SDNP
클라이언트
$C_{1,1}$
1700A
1706A
1707
1708
1709A
구역 U7 SDNP
파일 저장
파싱된
파일 1
구역 U1
라스트 마일
하이퍼보안
전송
구역 Z1
클라이언트
하이퍼보안
전송
구역 U7
파일 보안
$F_{7,1}$
1700H
1705
1057
파싱되지 않은
원본 파일
파싱된
파일 2
1706B
구역 U9
파일 보안
$F_{9,1}$
1700M
1709B
파싱
파싱된
파일 3
구역 U9
파일 보안
$F_{9,4}$
1700L
1052
1706C
1709C
구역 U9 SDNP
파일 저장

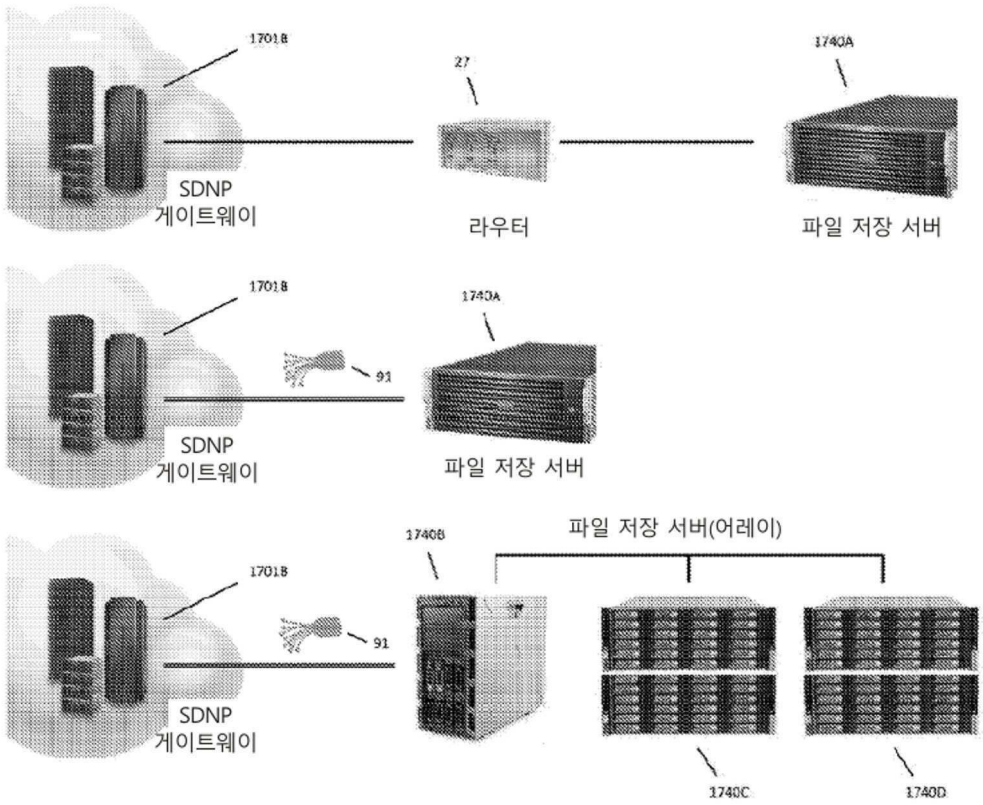
도면82b


하이퍼보안 파일 저장
판독 동작
구역 U1 SDNP
클라이언트
$C_{1,1}$
1700A
1706A
1707
1708
1709A
구역 U7 SDNP
파일 저장
파싱된
파일 1
구역 U1
라스트 마일
하이퍼보안
전송
구역 Z1
클라이언트
하이퍼보안
전송
구역 U7
파일 보안
$F_{7,1}$
1700H
1705
1061
파싱되지 않은
원본 파일
파싱된
파일 2
1706B
구역 U9
파일 보안
$F_{9,1}$
1700M
1709B
파싱된
파일 3
구역 U9
파일 보안
$F_{9,4}$
1700L
1706C
1709C
구역 U9 SDNP
파일 저장

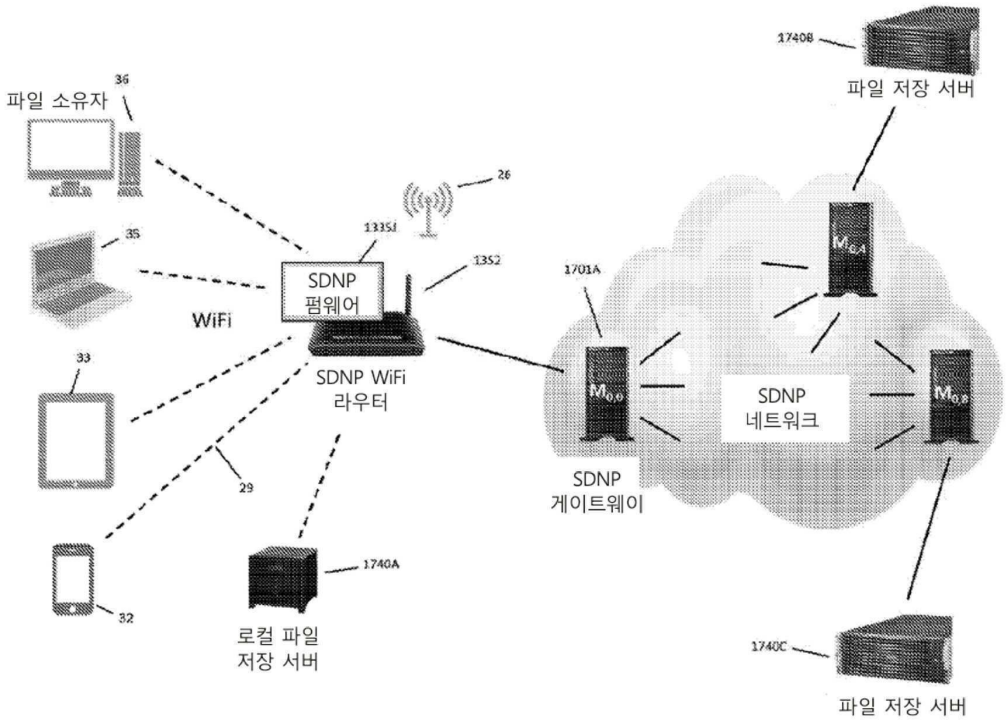
도면83


구역 U1 SDNP
클라이언트
구역 U7 SDNP
파일 저장
구역 Z1 SDNP
클라우드
구역 U9 SDNP
파일 저장
IP M0,0
IP C1,1
TCP
태그 1
U1
프리앰블 1
SDNP 파일 x
IP F7,1
IP M0,4
TCP
태그 7
U7
프리앰블 7
SDNP 파일 1
IP F9,6
IP M6,8
TCP
태그 9
U9
프리앰블 9
SDNP 파일 2
소스
목적지
L4
ID
구역
IP F9,1
IP M6,8
TCP
태그 8
U9
프리앰블 9
SDNP 파일 3
1727X
1731X
1731H
1727H
1700A
1700H
1701U
1727L
1731L
1731M
1700L
1727M
1700M

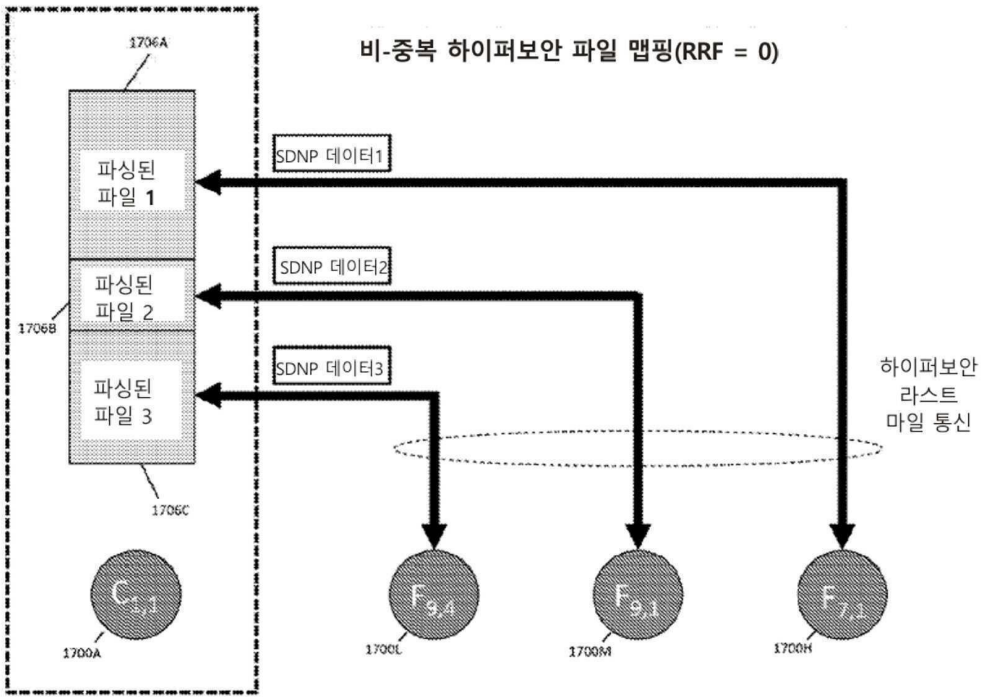
도면84a


1701B
SDNP
게이트웨이
27
라우터
1740A
파일 저장 서버
1701B
91
SDNP
게이트웨이
1740A
파일 저장 서버
파일 저장 서버(어레이)
1701B
91
SDNP
게이트웨이
1740B
1740C
1740D

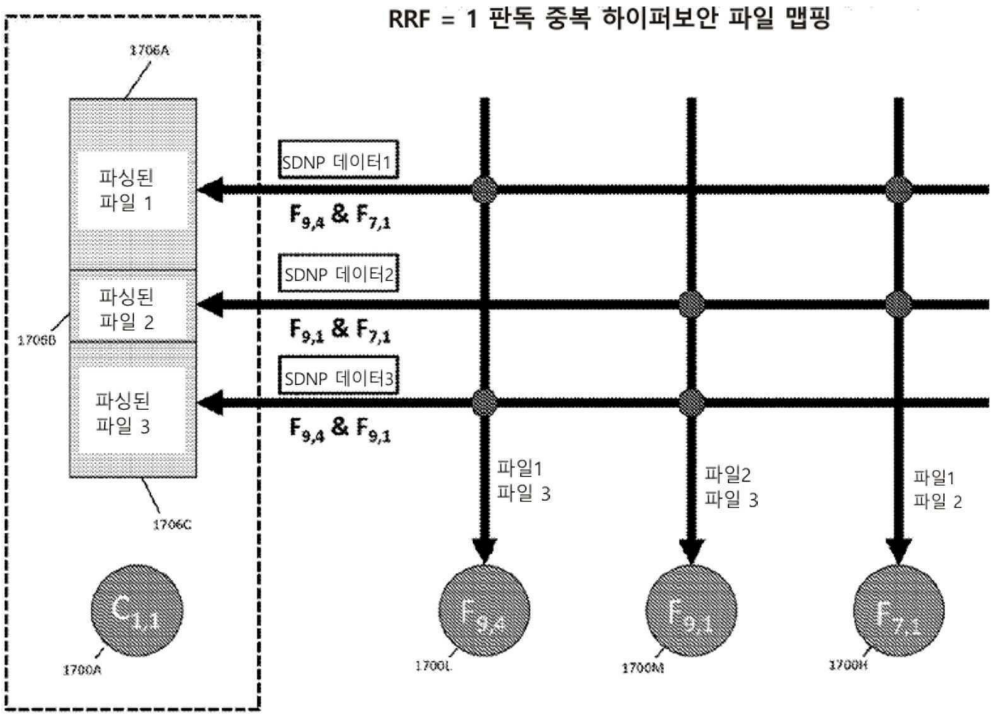
도면84b


파일 소유자
36
35
33
32
WiFi
SDNP
펌웨어
SDNP WiFi
라우터
26
1335J
1352
29
1740A
로컬 파일
저장 서버
1740B
파일 저장 서버
1701A
SDNP
네트워크
SDNP
게이트웨이
1740C
파일 저장 서버

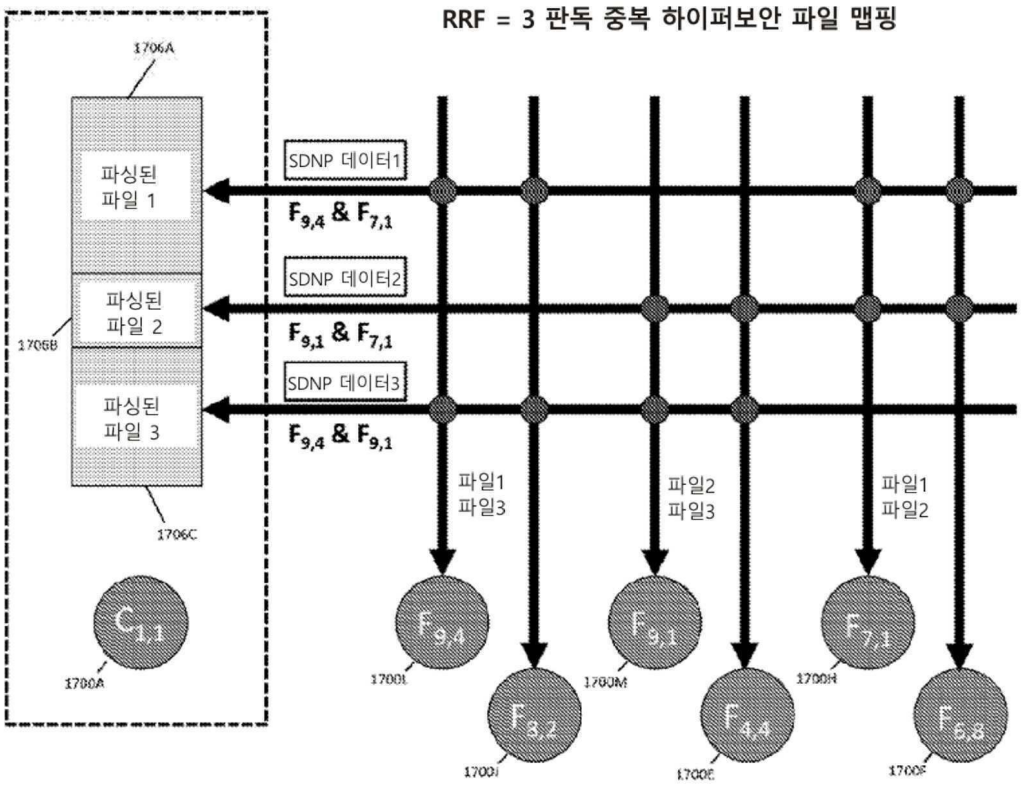
도면85a


비-중복 하이퍼보안 파일 맵핑(RRF = 0)
1706A
파싱된
파일 1
파싱된
파일 2
1706B
파싱된
파일 3
1706C
SDNP 데이터1
SDNP 데이터2
SDNP 데이터3
하이퍼보안
라스트
마일 통신
1700A
1700L
1700M
1700H

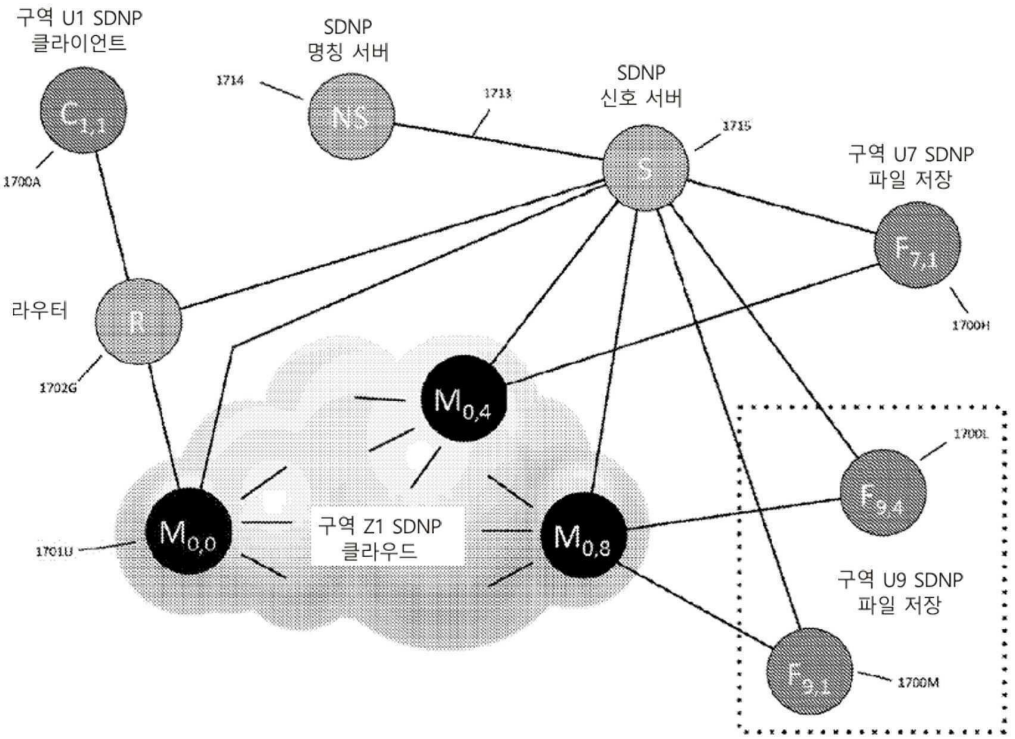
도면85b


RRF = 1 판독 중복 하이퍼보안 파일 맵핑
1706A
파싱된 파일 1
파싱된 파일 2
파싱된 파일 3
1706B
1706C
SDNP 데이터1
F9,4 & F7,1
SDNP 데이터2
F9,1 & F7,1
SDNP 데이터3
F9,4 & F9,1
파일1 파일 3
파일2 파일 3
파일1 파일 2
C1,1
1700A
F9,4
1700L
F9,1
1700M
F7,1
1700H

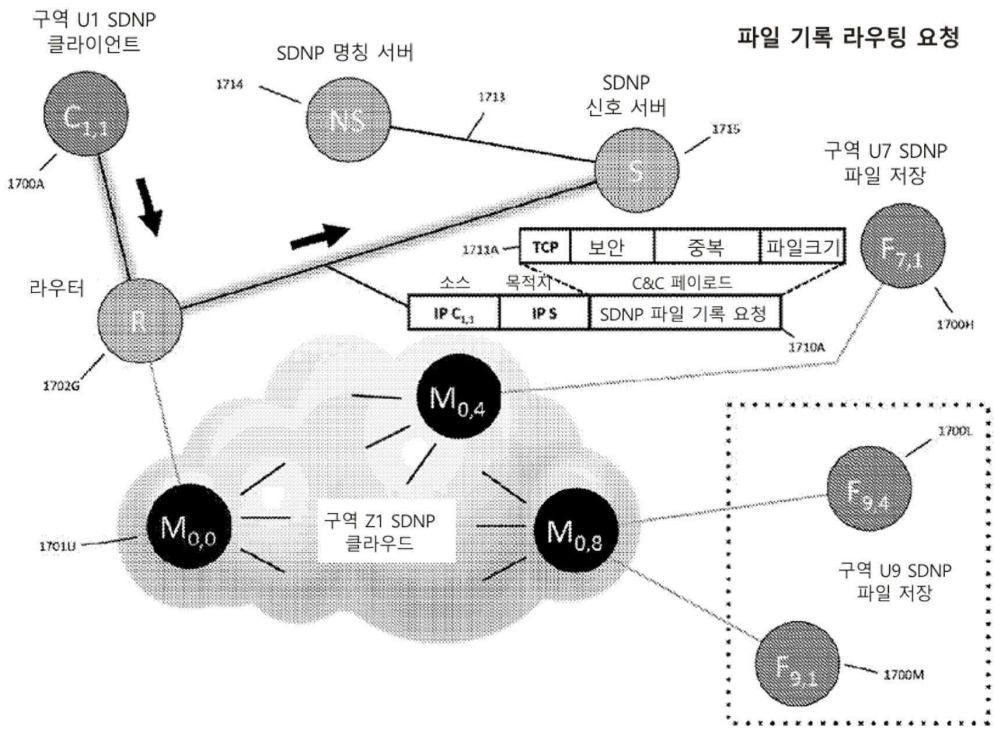
도면85c


RRF = 3 판독 중복 하이퍼보안 파일 맵핑
1706A
파싱된 파일 1
파싱된 파일 2
파싱된 파일 3
1706B
1706C
SDNP 데이터1
F9,4 & F7,1
SDNP 데이터2
F9,1 & F7,1
SDNP 데이터3
F9,4 & F9,1
파일1 파일3
파일2 파일3
파일1 파일2
C1,1
1700A
F9,4
1700L
F9,1
1700M
F7,1
1700H
F3,2
1700I
F4,4
1700E
F6,8
1700F

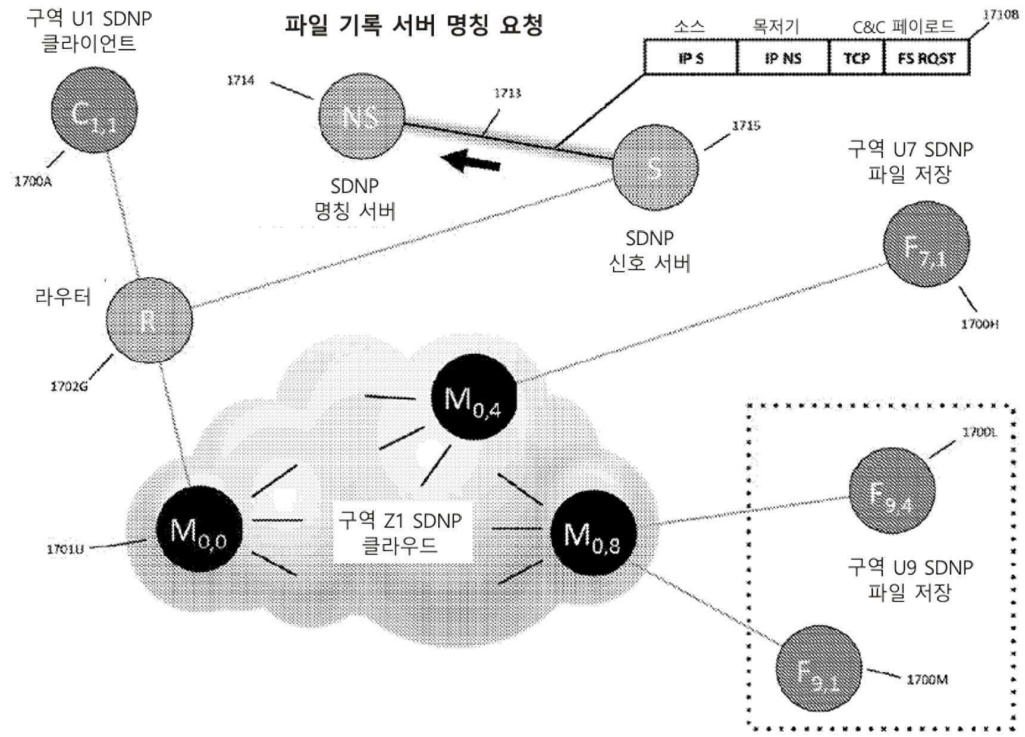
도면86


구역 U1 SDNP
클라이언트
SDNP
명칭 서버
SDNP
신호 서버
구역 U7 SDNP
파일 저장
라우터
구역 Z1 SDNP
클라우드
구역 U9 SDNP
파일 저장
1700A
1714
1713
1715
1700H
1702G
1700L
1701U
1700M

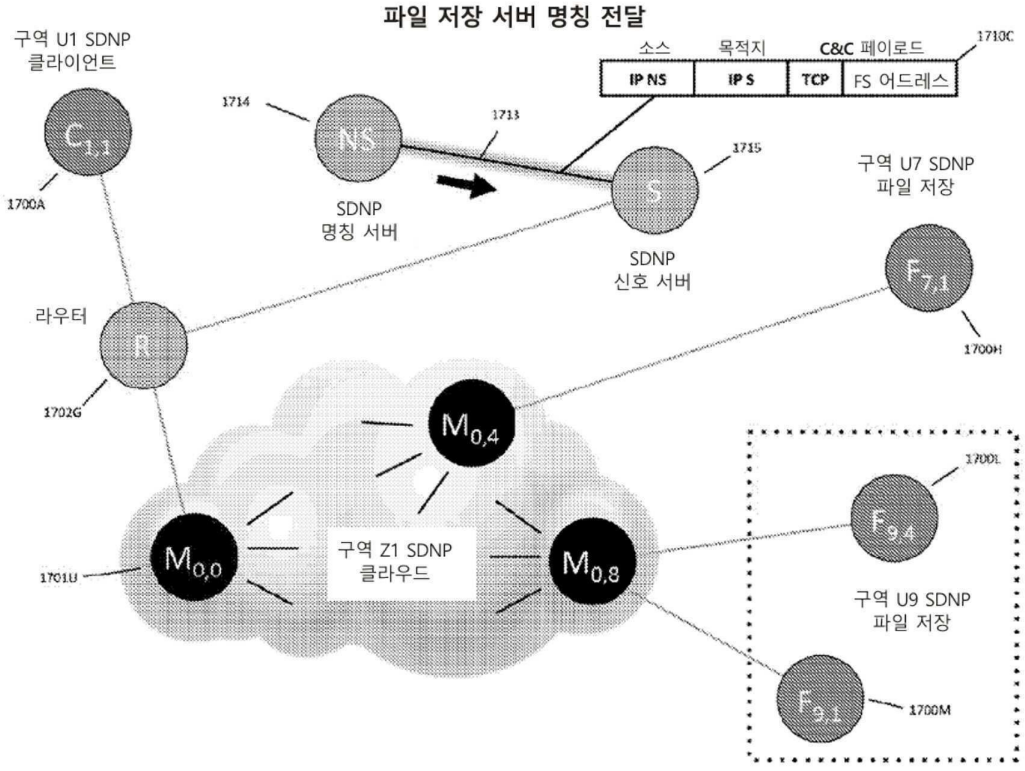
도면87a


파일 기록 라우팅 요청
구역 U1 SDNP
클라이언트
SDNP 명칭 서버
SDNP
신호 서버
구역 U7 SDNP
파일 저장
라우터
구역 Z1 SDNP
클라우드
구역 U9 SDNP
파일 저장
TCP
보안
중복
파일크기
소스
목적지
C&C 페이로드
IP S
SDNP 파일 기록 요청
1711A
1710A
1700A
1714
1713
1715
1700H
1702G
1700L
1701U
1700M

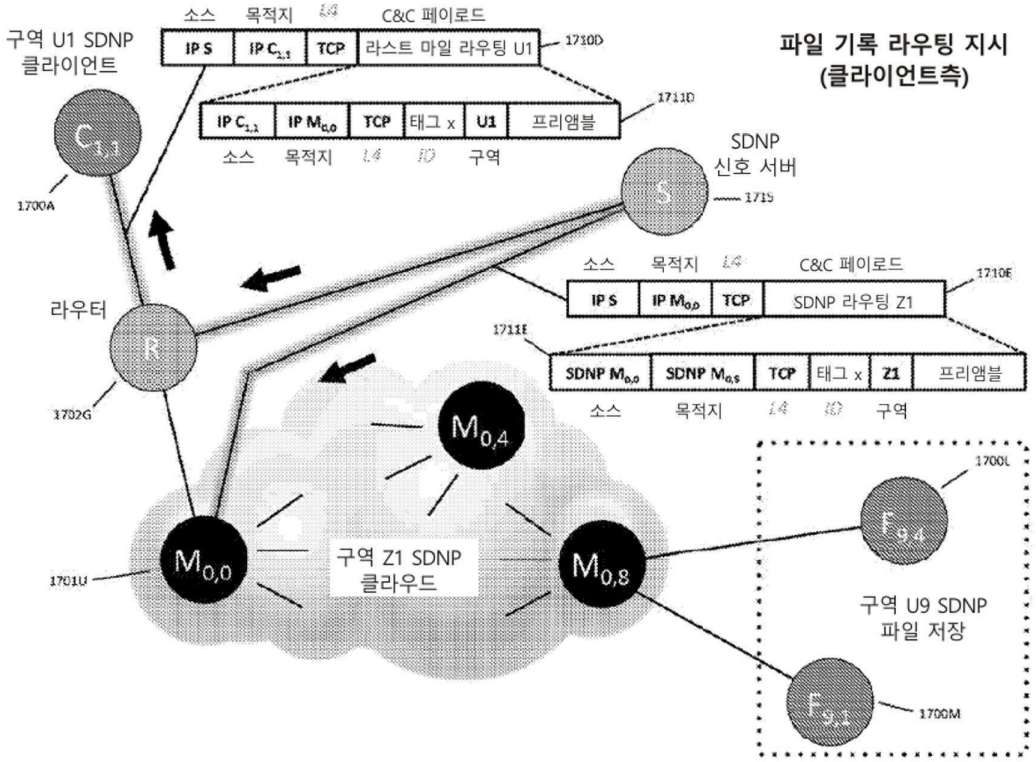
도면87b


파일 기록 서버 명칭 요청
구역 U1 SDNP 클라이언트
소스
목적지
C&C 페이로드
IP S
IP NS
TCP
FS RQST
1710B
1714
NS
1713
1715
S
SDNP 명칭 서버
SDNP 신호 서버
구역 U7 SDNP 파일 저장
$C_{1,1}$
1700A
라우터
R
1702G
$F_{7,1}$
1700H
$M_{0,4}$
$M_{0,0}$
$M_{0,8}$
1701U
구역 Z1 SDNP 클라이언트
1700L
$F_{9,4}$
구역 U9 SDNP 파일 저장
$F_{9,1}$
1700M

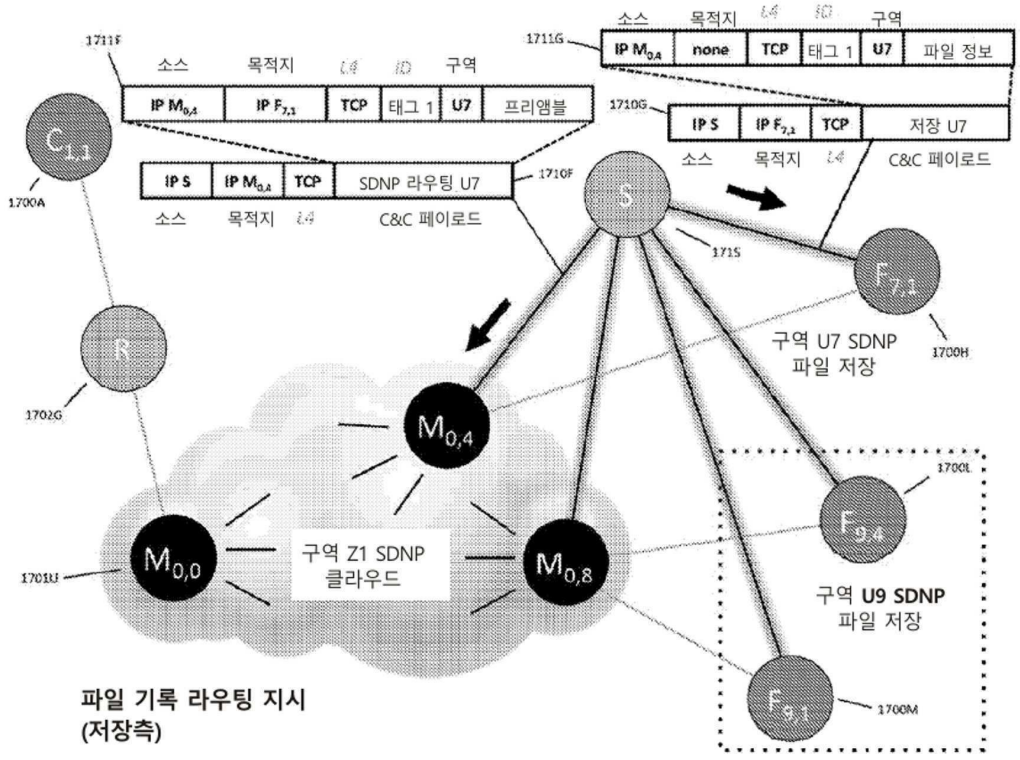
도면87c


파일 저장 서버 명칭 전달
구역 U1 SDNP 클라이언트
소스
목적지
C&C 페이로드
IP NS
IP S
TCP
FS 어드레스
1710C
1714
NS
1713
1715
S
SDNP 명칭 서버
SDNP 신호 서버
구역 U7 SDNP 파일 저장
$C_{1,1}$
1700A
라우터
R
1702G
$F_{7,1}$
1700H
$M_{0,4}$
$M_{0,0}$
$M_{0,8}$
1701U
구역 Z1 SDNP 클라이언트
1700L
$F_{9,4}$
구역 U9 SDNP 파일 저장
$F_{9,1}$
1700M

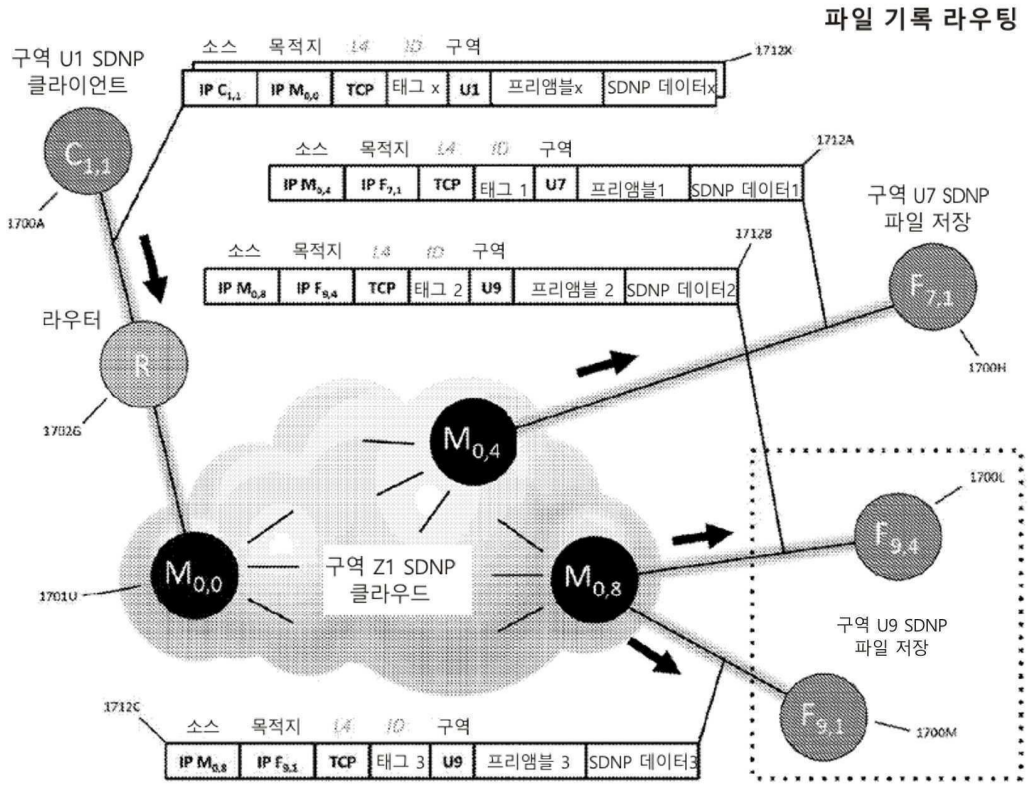
도면87d


파일 기록 라우팅 지시
(클라이언트측)
구역 U1 SDNP
클라이언트
소스 목적지 L4 C&C 페이로드
IP S | IP C1,1 | TCP | 라스트 마일 라우팅 U1
1710D
IP C1,1 | IP M0,0 | TCP | 태그 x | U1 | 프리앰블
1711D
소스 목적지 L4 ID 구역
SDNP
신호 서버
S
1715
C1,1
1700A
라우터
R
1702G
소스 목적지 L4 C&C 페이로드
IP S | IP M0,0 | TCP | SDNP 라우팅 Z1
1710E
SDNP M0,0 | SDNP M0,8 | TCP | 태그 x | Z1 | 프리앰블
1711E
소스 목적지 L4 ID 구역
M0,4
M0,0
1701U
구역 Z1 SDNP
클라우드
M0,8
F9,4
1700L
구역 U9 SDNP
파일 저장
F9,1
1700M

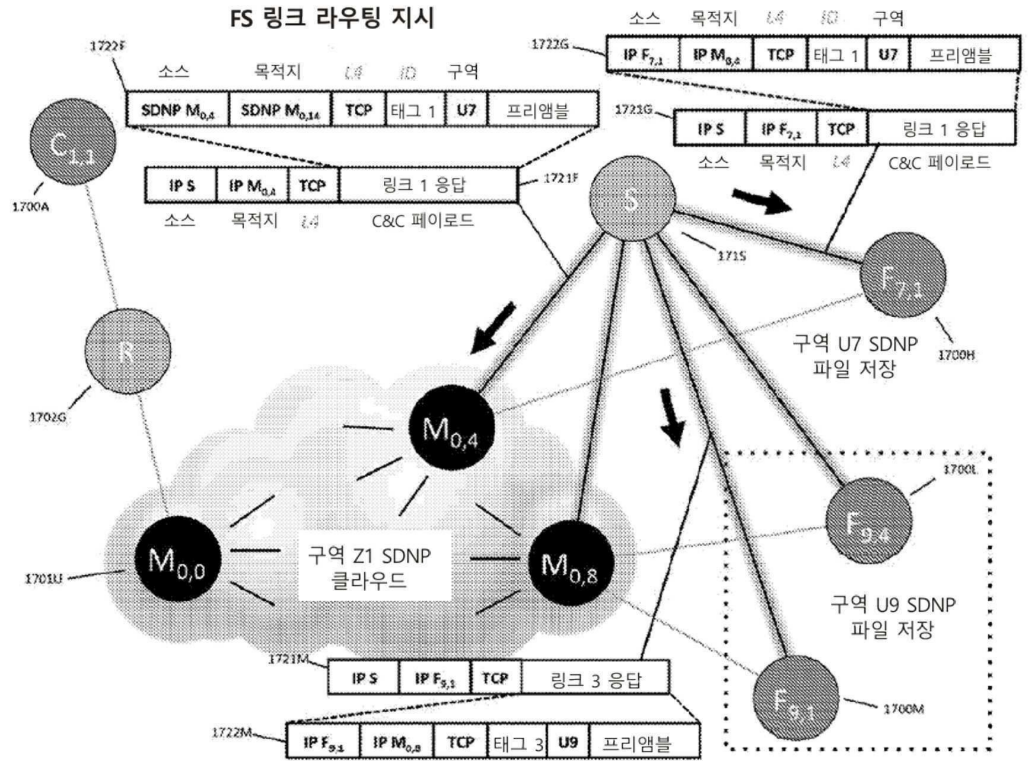
도면87e


소스 목적지 L4 ID 구역
IP M0,4 | none | TCP | 태그 1 | U7 | 파일 정보
1711G
1711F
소스 목적지 L4 ID 구역
IP M0,4 | IP F7,1 | TCP | 태그 1 | U7 | 프리앰블
1710G
IP S | IP F7,1 | TCP | 저장 U7
소스 목적지 L4 C&C 페이로드
IP S | IP M0,4 | TCP | SDNP 라우팅 U7
1710F
소스 목적지 L4 C&C 페이로드
C1,1
1700A
S
1715
F7,1
1700H
구역 U7 SDNP
파일 저장
R
1702G
M0,4
M0,0
1701U
구역 Z1 SDNP
클라우드
M0,8
F9,4
1700L
구역 U9 SDNP
파일 저장
F9,1
1700M
파일 기록 라우팅 지시
(저장측)

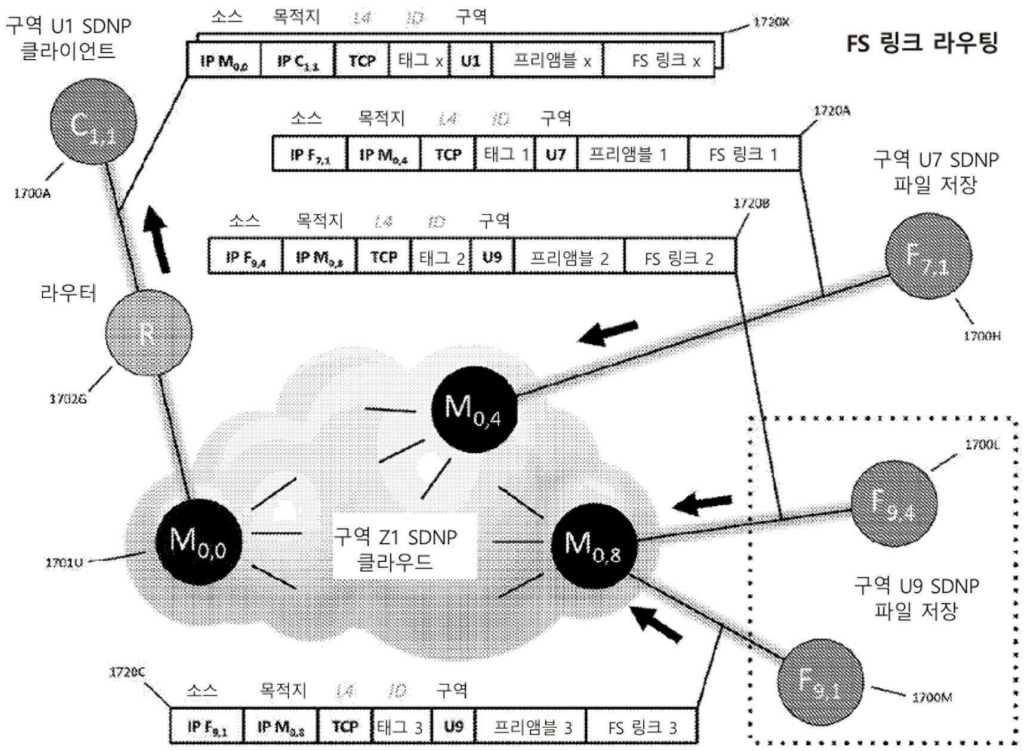
도면88


파일 기록 라우팅
구역 U1 SDNP
클라이언트
소스 목적지 L4 ID 구역
IP C1,1 IP M0,0 TCP 태그 x U1 프리앰블x SDNP 데이터x
1712X
1700A
소스 목적지 L4 ID 구역
IP M0,4 IP F7,1 TCP 태그 1 U7 프리앰블1 SDNP 데이터1
1712A
구역 U7 SDNP
파일 저장
소스 목적지 L4 ID 구역
IP M0,8 IP F9,4 TCP 태그 2 U9 프리앰블 2 SDNP 데이터2
1712B
라우터
1702G
1700H
1700L
구역 Z1 SDNP
클라우드
1701U
구역 U9 SDNP
파일 저장
1712C
소스 목적지 L4 ID 구역
IP M0,8 IP F9,1 TCP 태그 3 U9 프리앰블 3 SDNP 데이터3
1700M

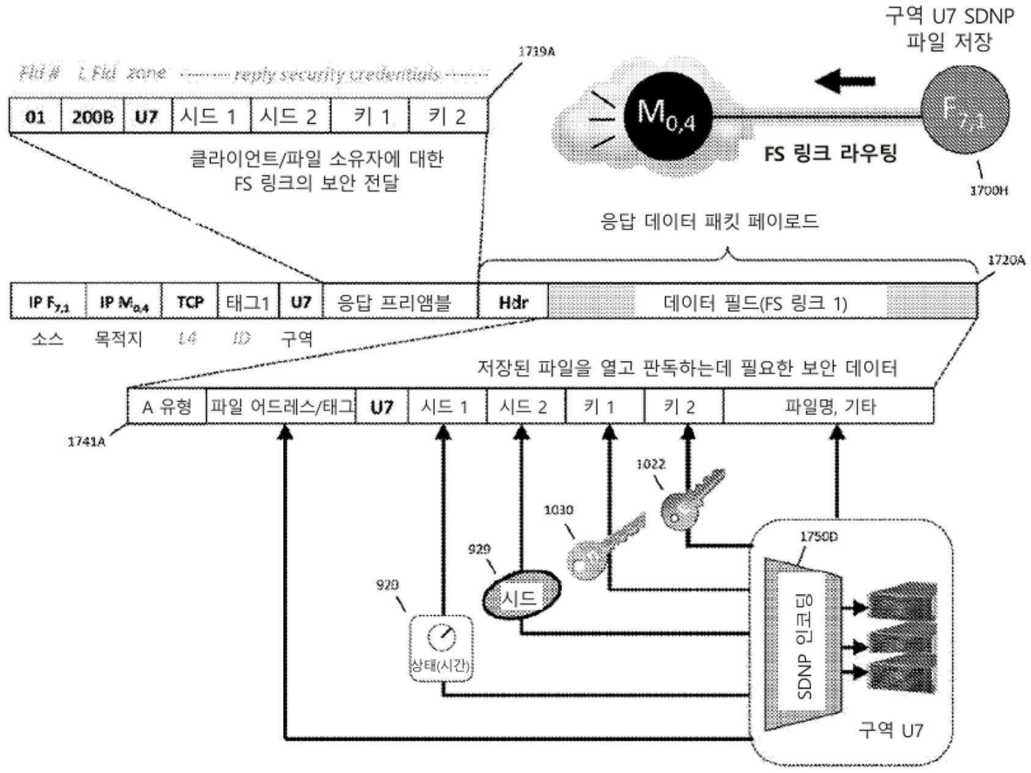
도면89a


FS 링크 라우팅 지시
1722F
소스 목적지 L4 ID 구역
SDNP M0,4 SDNP M0,14 TCP 태그 1 U7 프리앰블
1722G
소스 목적지 L4 ID 구역
IP F7,1 IP M0,4 TCP 태그 1 U7 프리앰블
1721G
IP S IP F7,1 TCP 링크 1 응답
소스 목적지 L4 C&C 페이로드
IP S IP M0,4 TCP 링크 1 응답
소스 목적지 L4 C&C 페이로드
1721F
1700A
1715
구역 U7 SDNP
파일 저장
1700H
1702G
1700L
구역 Z1 SDNP
클라우드
1701U
구역 U9 SDNP
파일 저장
1721M
IP S IP F9,1 TCP 링크 3 응답
1722M
IP F9,1 IP M0,8 TCP 태그 3 U9 프리앰블
1700M

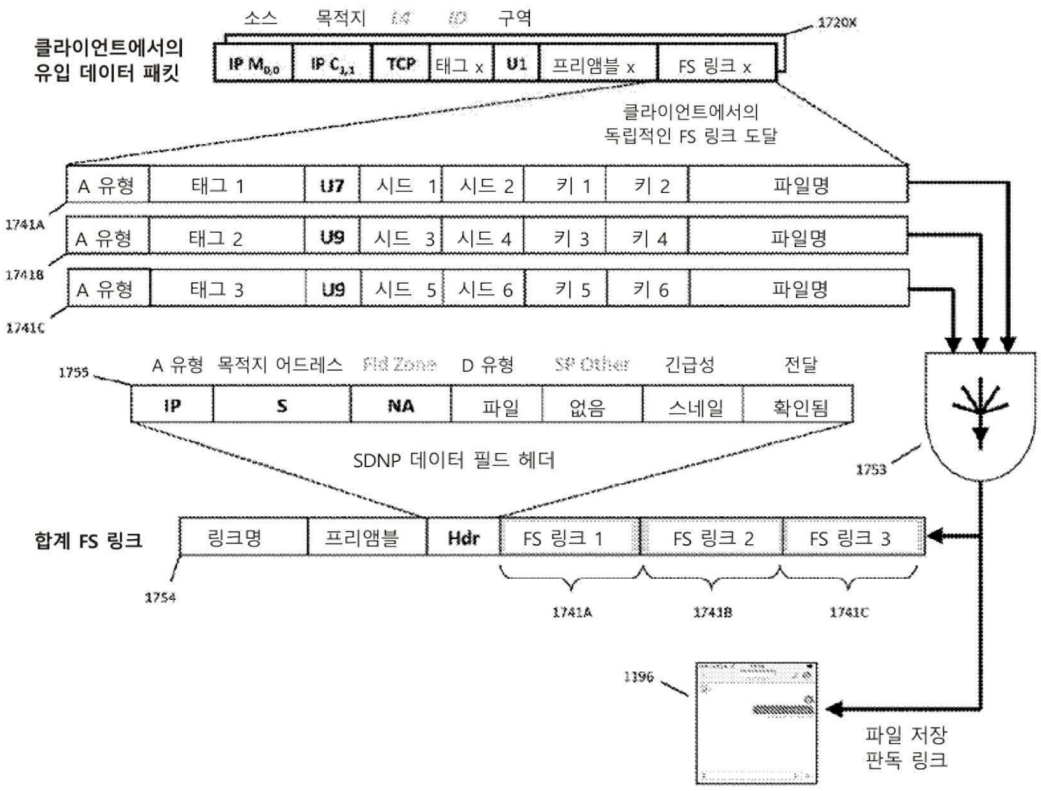
도면89b


구역 U1 SDNP
클라이언트
소스 목적지 L4 ID 구역
IP M0,0 IP C1,1 TCP 태그 x U1 프리앰블 x FS 링크 x
1720X
FS 링크 라우팅
C1,1
1700A
소스 목적지 L4 ID 구역
IP F7,1 IP M0,4 TCP 태그 1 U7 프리앰블 1 FS 링크 1
1720A
구역 U7 SDNP
파일 저장
소스 목적지 L4 ID 구역
IP F9,4 IP M0,8 TCP 태그 2 U9 프리앰블 2 FS 링크 2
1720B
F7,1
1700H
라우터
R
1702G
M0,4
1700L
F9,4
M0,0
1701U
구역 Z1 SDNP
클라우드
M0,8
구역 U9 SDNP
파일 저장
F9,1
1700M
1720C
소스 목적지 L4 ID 구역
IP F9,1 IP M0,8 TCP 태그 3 U9 프리앰블 3 FS 링크 3

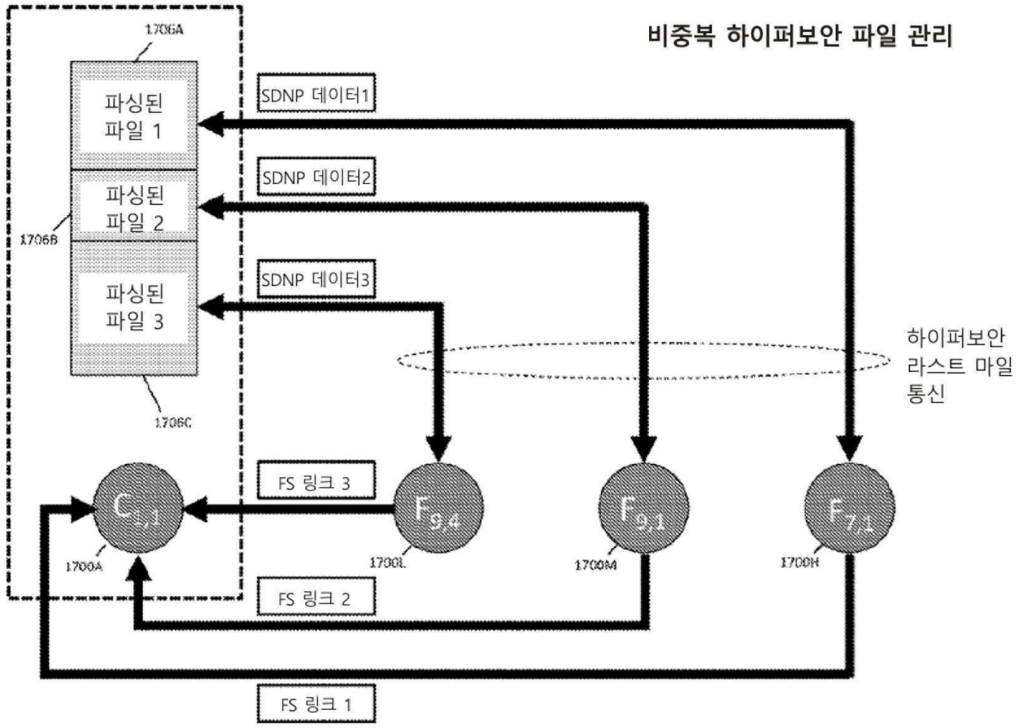
도면89c


구역 U7 SDNP
파일 저장
Fld # L Fld zone ····· reply security credentials ·····
1719A
01 200B U7 시드 1 시드 2 키 1 키 2
클라이언트/파일 소유자에 대한
FS 링크의 보안 전달
M0,4
F7,1
FS 링크 라우팅
1700H
응답 데이터 패킷 페이로드
1720A
IP F7,1 IP M0,4 TCP 태그1 U7 응답 프리앰블 Hdr 데이터 필드(FS 링크 1)
소스 목적지 L4 ID 구역
저장된 파일을 열고 판독하는데 필요한 보안 데이터
A 유형 파일 어드레스/태그 U7 시드 1 시드 2 키 1 키 2 파일명, 기타
1741A
1022
1030
929
시드
920
상태(시간)
1750D
SDNP 인코딩
구역 U7

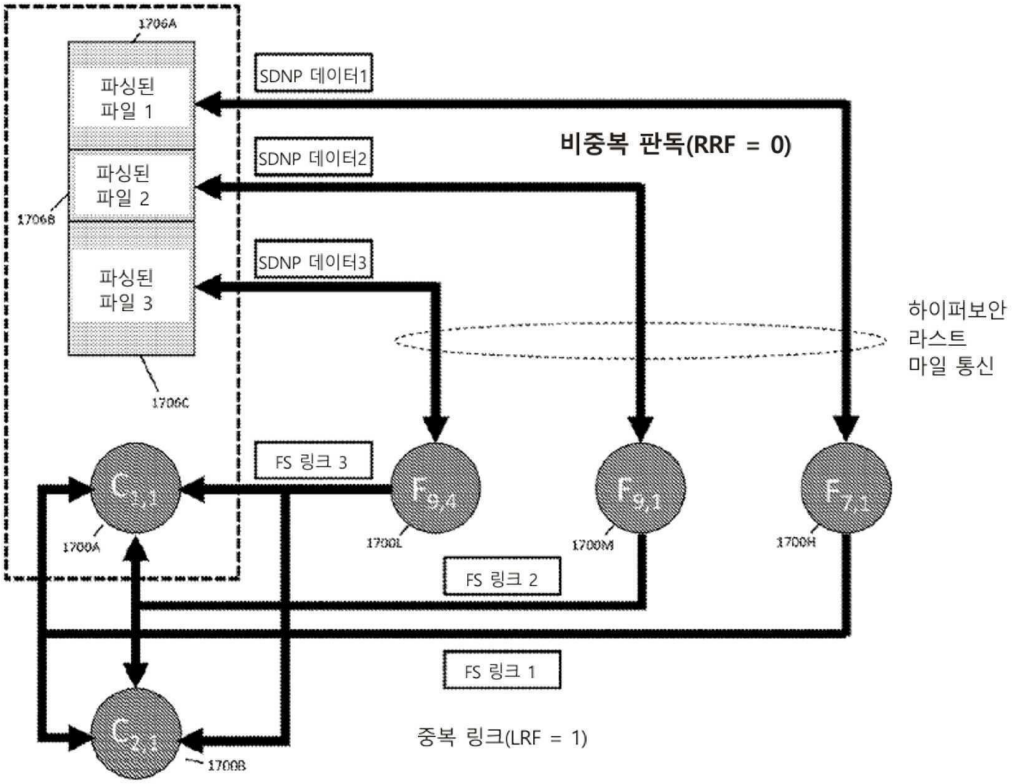
도면89d


소스
목적지
구역
1720X
클라이언트에서의
유입 데이터 패킷
IP M0,0
IP C1,1
TCP
태그 x
U1
프리앰블 x
FS 링크 x
클라이언트에서의
독립적인 FS 링크 도달
A 유형
태그 1
U7
시드 1
시드 2
키 1
키 2
파일명
1741A
A 유형
태그 2
U9
시드 3
시드 4
키 3
키 4
파일명
1741B
A 유형
태그 3
U9
시드 5
시드 6
키 5
키 6
파일명
1741C
1755
A 유형
목적지 어드레스
D 유형
긴급성
전달
IP
S
NA
파일
없음
스네일
확인됨
SDNP 데이터 필드 헤더
1753
합계 FS 링크
링크명
프리앰블
Hdr
FS 링크 1
FS 링크 2
FS 링크 3
1754
1741A
1741B
1741C
1196
파일 저장
판독 링크

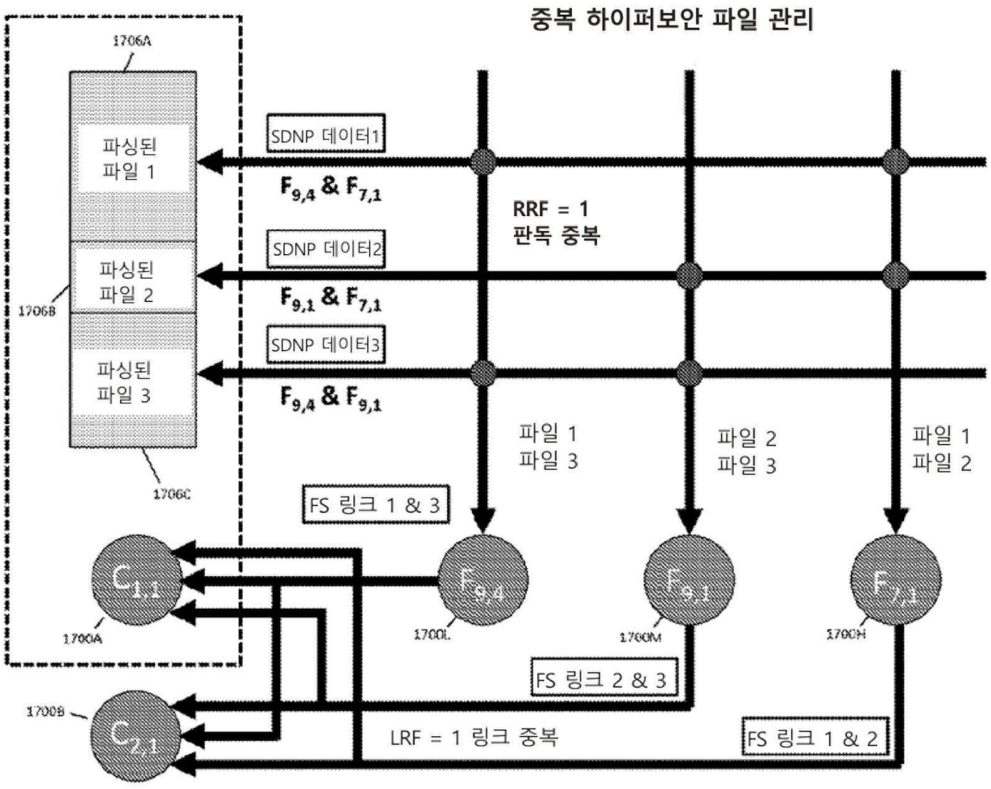
도면90a


비중복 하이퍼보안 파일 관리
1706A
파싱된
파일 1
파싱된
파일 2
파싱된
파일 3
1706B
1706C
SDNP 데이터1
SDNP 데이터2
SDNP 데이터3
하이퍼보안
라스트 마일
통신
FS 링크 3
FS 링크 2
FS 링크 1
C1,1
F9,4
F9,1
F7,1
1700A
1700L
1700M
1700H

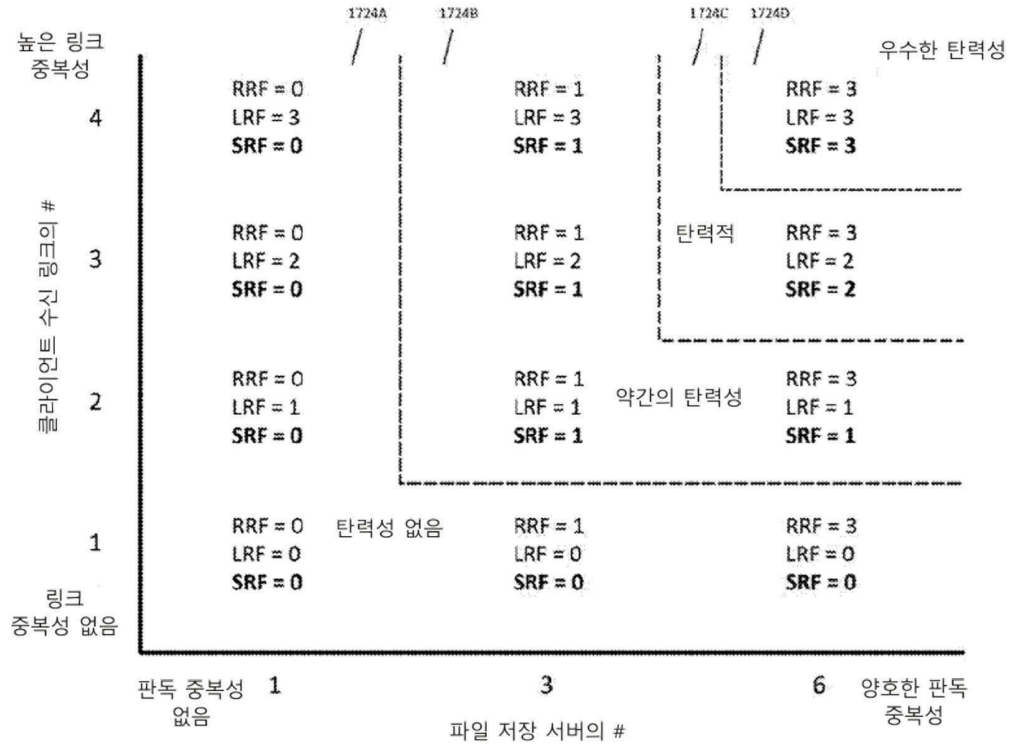
도면90b


1706A
파싱된 파일 1
파싱된 파일 2
파싱된 파일 3
1706B
1706C
SDNP 데이터1
SDNP 데이터2
SDNP 데이터3
비중복 판독(RRF = 0)
하이퍼보안 라스트 마일 통신
FS 링크 3
FS 링크 2
FS 링크 1
$C_{1,1}$
$C_{2,1}$
$F_{9,4}$
$F_{9,1}$
$F_{7,1}$
1700A
1700B
1700L
1700M
1700H
중복 링크(LRF = 1)

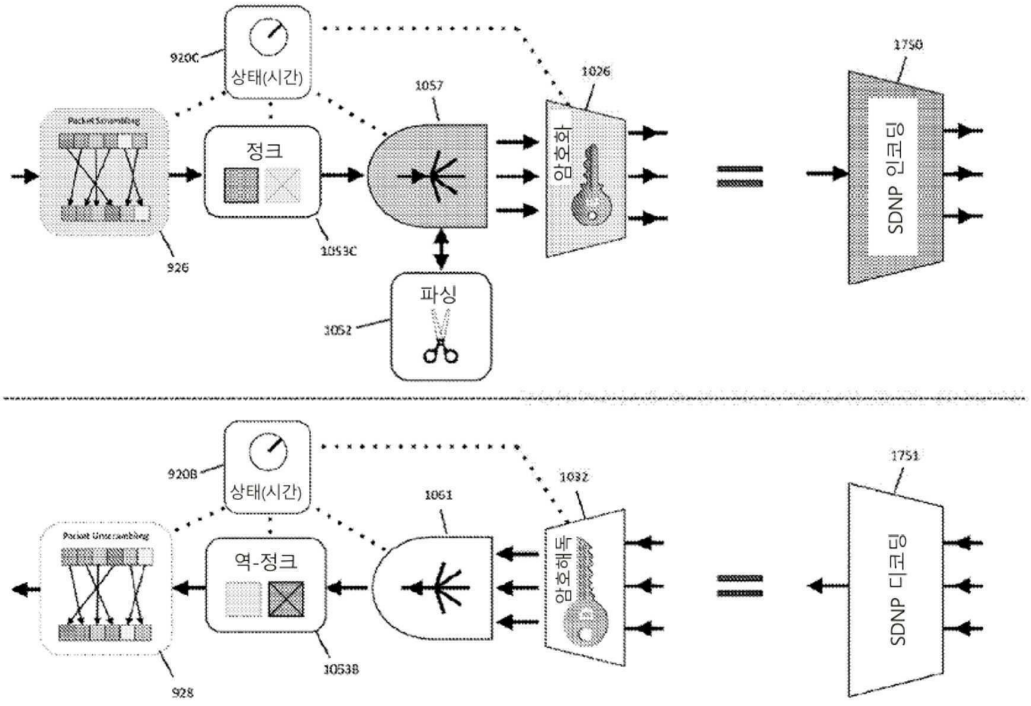
도면90c


중복 하이퍼보안 파일 관리
1706A
파싱된 파일 1
파싱된 파일 2
파싱된 파일 3
1706B
1706C
SDNP 데이터1
SDNP 데이터2
SDNP 데이터3
$F_{9,4}$ & $F_{7,1}$
$F_{9,1}$ & $F_{7,1}$
$F_{9,4}$ & $F_{9,1}$
RRF = 1
판독 중복
파일 1
파일 3
파일 2
파일 3
파일 1
파일 2
FS 링크 1 & 3
FS 링크 2 & 3
FS 링크 1 & 2
LRF = 1 링크 중복
$C_{1,1}$
$C_{2,1}$
$F_{9,4}$
$F_{9,1}$
$F_{7,1}$
1700A
1700B
1700L
1700M
1700H

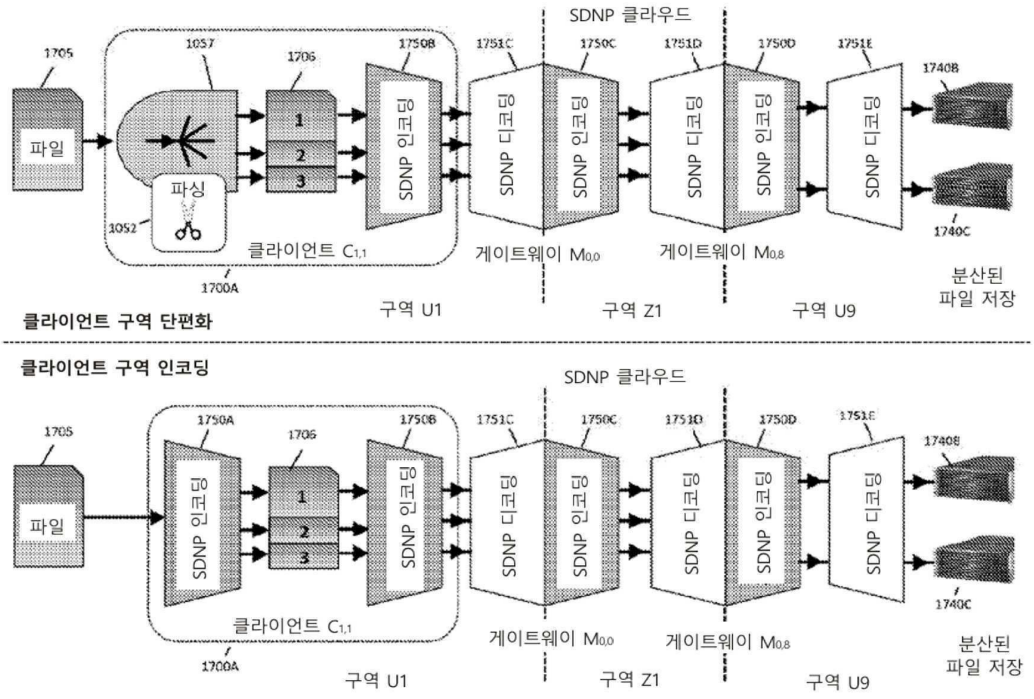
도면91


1724A
1724B
1724C
1724D
높은 링크 중복성
우수한 탄력성
RRF = 0
LRF = 3
SRF = 0
RRF = 1
LRF = 3
SRF = 1
RRF = 3
LRF = 3
SRF = 3
4
3
2
1
클라이언트 수신 링크의 #
RRF = 0
LRF = 2
SRF = 0
RRF = 1
LRF = 2
SRF = 1
탄력적
RRF = 3
LRF = 2
SRF = 2
RRF = 0
LRF = 1
SRF = 0
RRF = 1
LRF = 1
SRF = 1
약간의 탄력성
RRF = 3
LRF = 1
SRF = 1
RRF = 0
LRF = 0
SRF = 0
탄력성 없음
RRF = 1
LRF = 0
SRF = 0
RRF = 3
LRF = 0
SRF = 0
링크 중복성 없음
판독 중복성 없음
1
3
6
양호한 판독 중복성
파일 저장 서버의 #

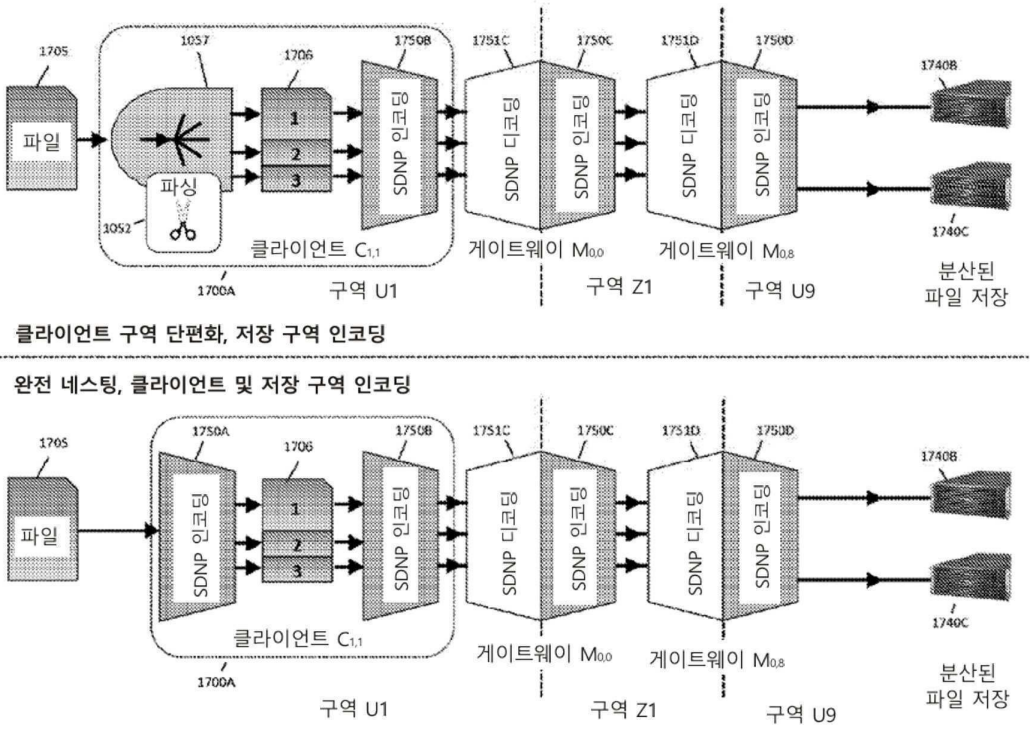
도면92


920C
상태(시간)
1057
1026
정크
암호화
1053C
926
파싱
1052
1750
SDNP 인코딩
920B
상태(시간)
1061
1032
역-정크
암호해독
1053B
928
1751
SDNP 디코딩

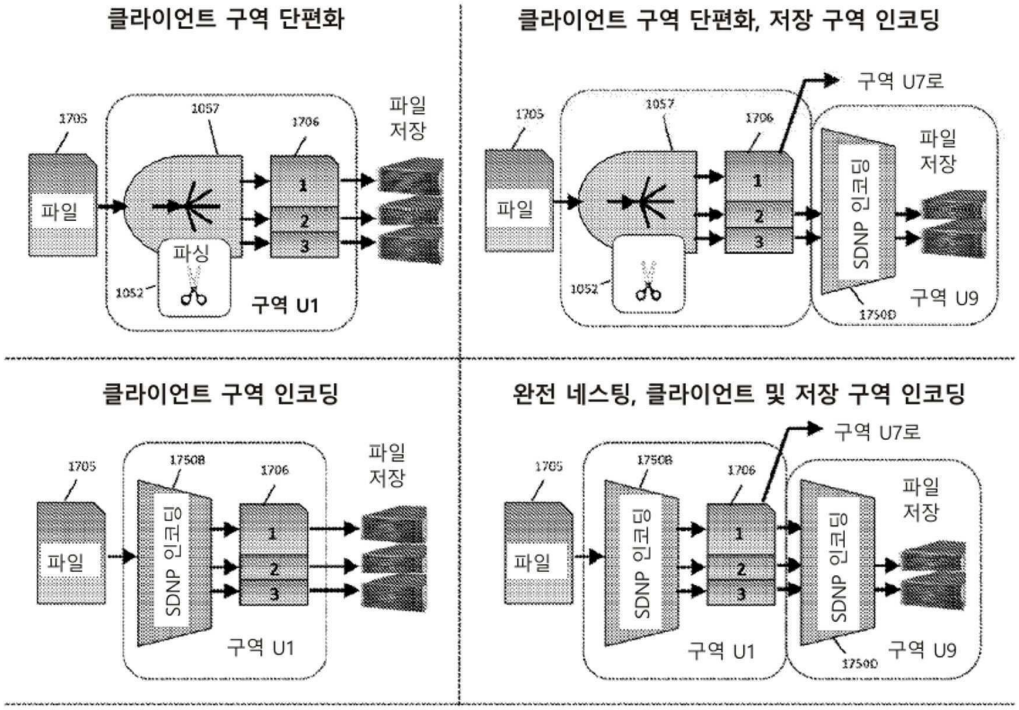
도면93a


SDNP 클라우드
파일
파싱
클라이언트 $C_{1,1}$
SDNP 인코딩
SDNP 디코딩
게이트웨이 $M_{0,0}$
게이트웨이 $M_{0,8}$
구역 U1
구역 Z1
구역 U9
분산된 파일 저장
클라이언트 구역 단편화
클라이언트 구역 인코딩

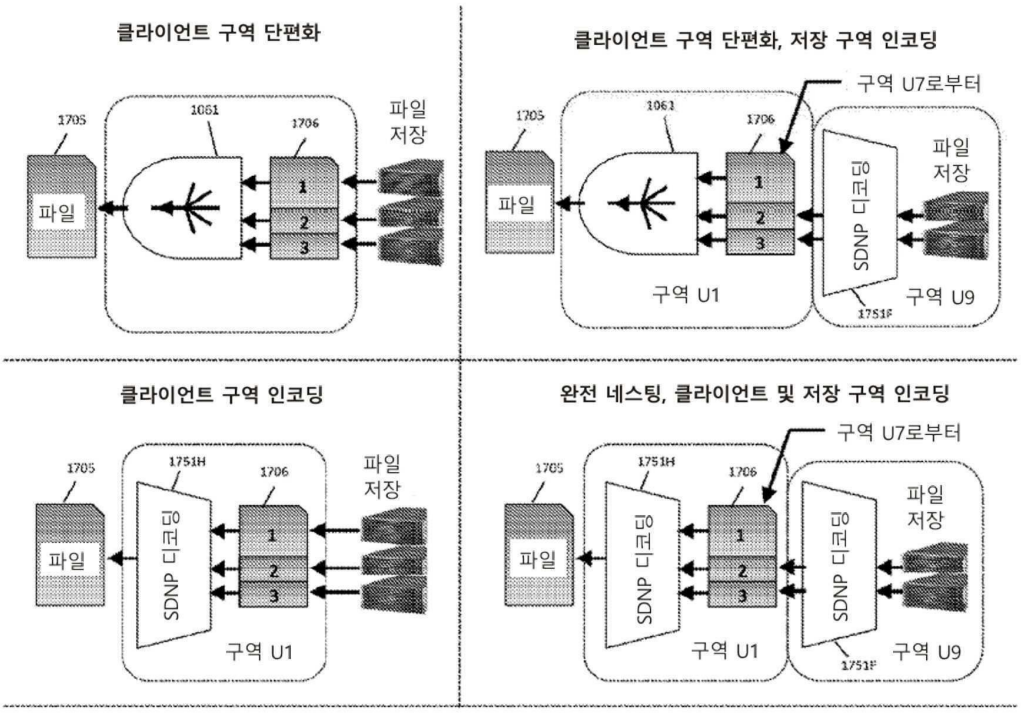
도면93b


파일
파싱
클라이언트 $C_{1,1}$
SDNP 인코딩
SDNP 디코딩
게이트웨이 $M_{0,0}$
게이트웨이 $M_{0,8}$
구역 U1
구역 Z1
구역 U9
분산된 파일 저장
클라이언트 구역 단편화, 저장 구역 인코딩
완전 네스팅, 클라이언트 및 저장 구역 인코딩

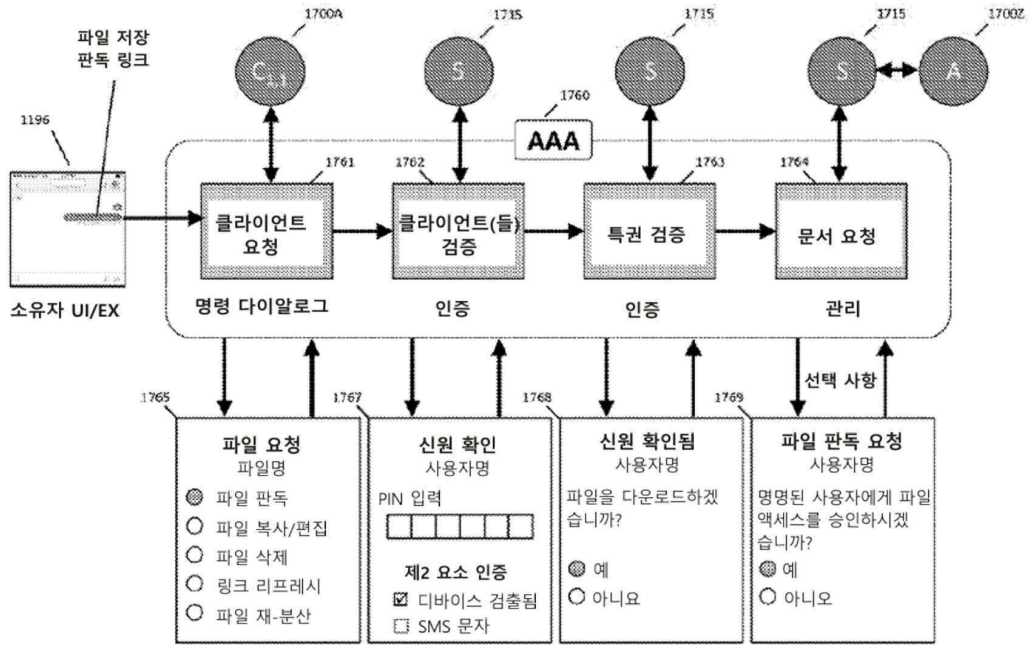
도면94


클라이언트 구역 단편화
파일
파일 저장
파싱
구역 U1
클라이언트 구역 단편화, 저장 구역 인코딩
구역 U7로
SDNP 인코딩
구역 U9
클라이언트 구역 인코딩
SDNP 인코딩
완전 네스팅, 클라이언트 및 저장 구역 인코딩

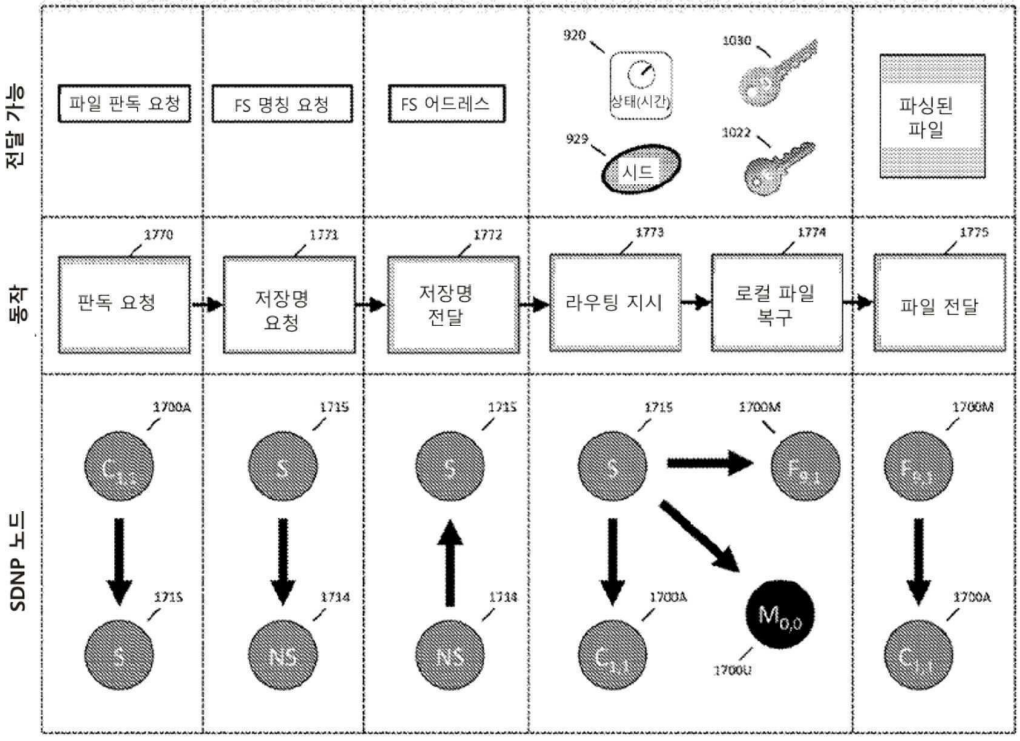
도면95


클라이언트 구역 단편화
파일
파일 저장
구역 U1
클라이언트 구역 단편화, 저장 구역 인코딩
구역 U7로부터
SDNP 디코딩
구역 U9
클라이언트 구역 인코딩
완전 네스팅, 클라이언트 및 저장 구역 인코딩

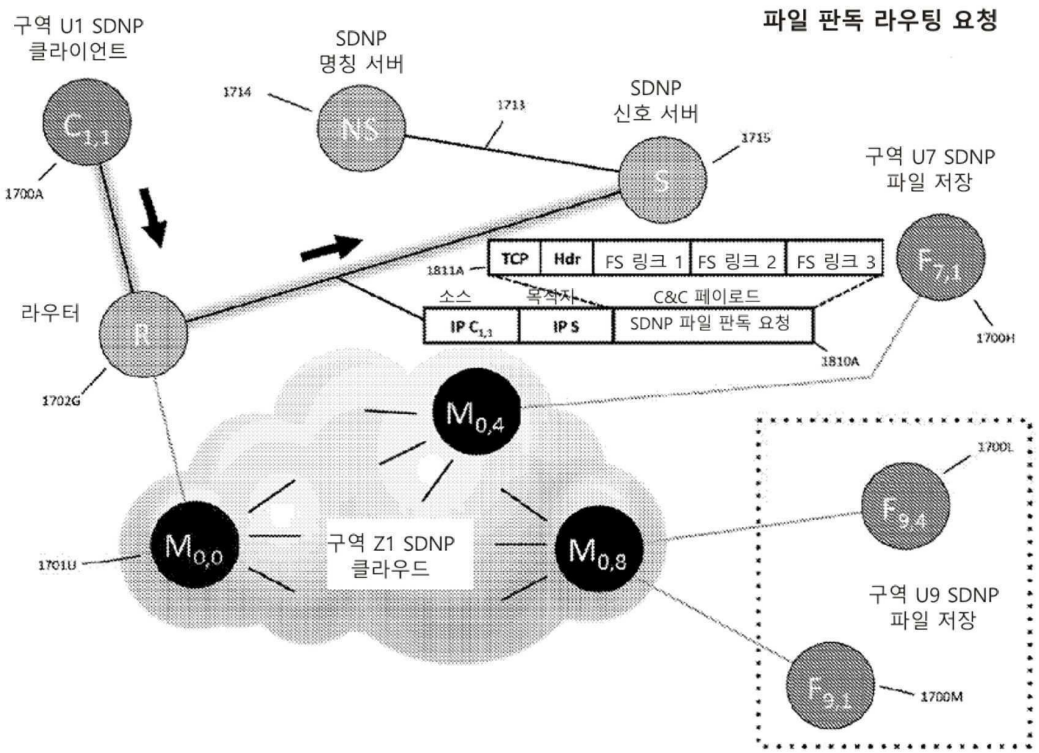
도면96a


파일 저장
판독 링크
1196
1700A
1715
1715
1715
1700Z
1760
AAA
1761
1762
1763
1764
클라이언트 요청
클라이언트(들) 검증
특권 검증
문서 요청
소유자 UI/EX
명령 다이알로그
인증
인증
관리
선택 사항
1765
1767
1768
1769
파일 요청
파일명
파일 판독
파일 복사/편집
파일 삭제
링크 리프레시
파일 재-분산
신원 확인
사용자명
PIN 입력
제2 요소 인증
디바이스 검출됨
SMS 문자
신원 확인됨
사용자명
파일을 다운로드하겠습니까?
예
아니요
파일 판독 요청
사용자명
명명된 사용자에게 파일 액세스를 승인하시겠습니까?
예
아니오

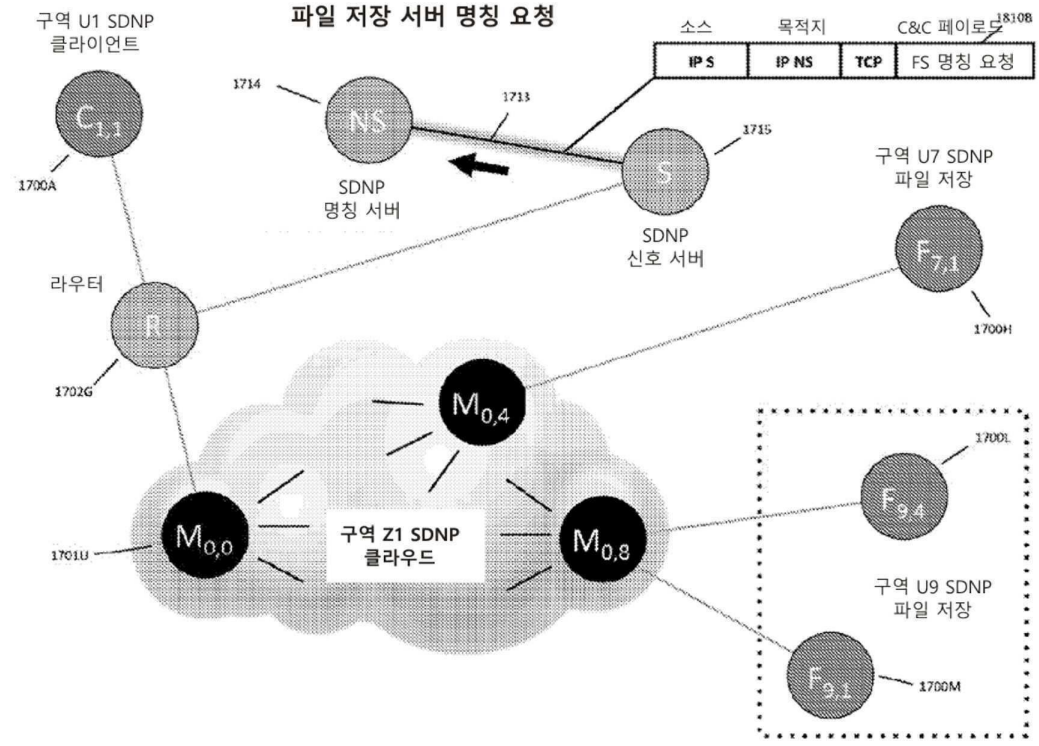
도면96b


전달 가능
동작
SDNP 노드
파일 판독 요청
FS 명칭 요청
FS 어드레스
920
상태(시간)
929
시드
1030
1022
파싱된 파일
1770
판독 요청
1771
저장명 요청
1772
저장명 전달
1773
라우팅 지시
1774
로컬 파일 복구
1775
파일 전달
1700A
1715
1714
1718
1700M
1700U

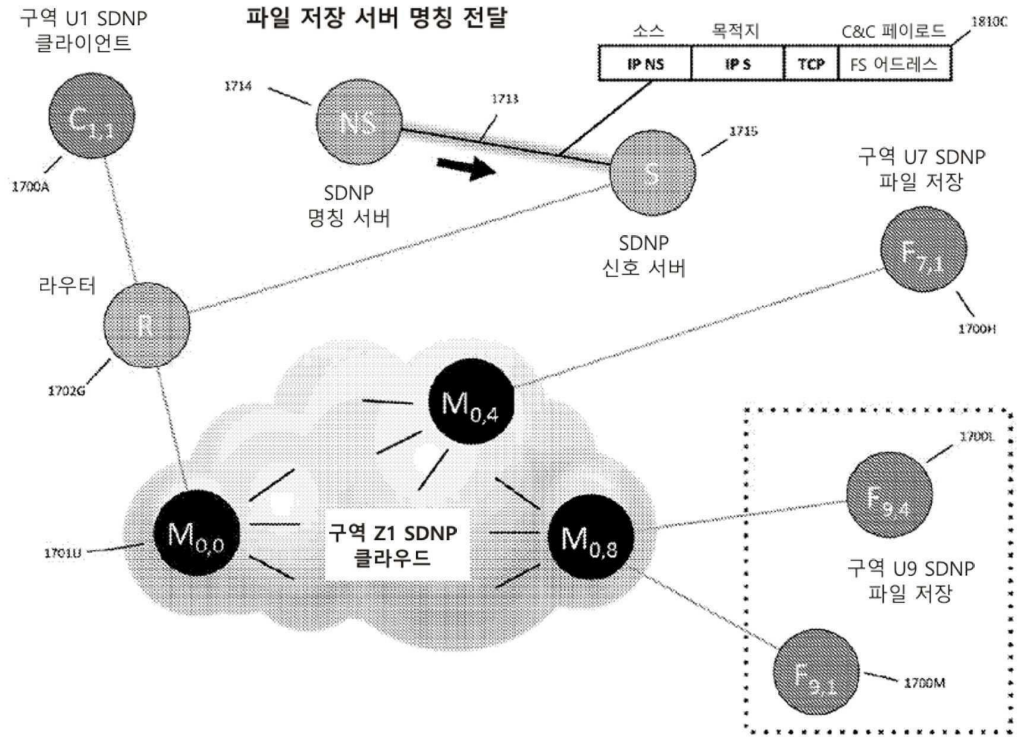
도면97a


파일 판독 라우팅 요청
구역 U1 SDNP
클라이언트
SDNP
명칭 서버
SDNP
신호 서버
구역 U7 SDNP
파일 저장
라우터
구역 Z1 SDNP
클라우드
구역 U9 SDNP
파일 저장
TCP
Hdr
FS 링크 1
FS 링크 2
FS 링크 3
소스
목적지
C&C 페이로드
IP S
SDNP 파일 판독 요청

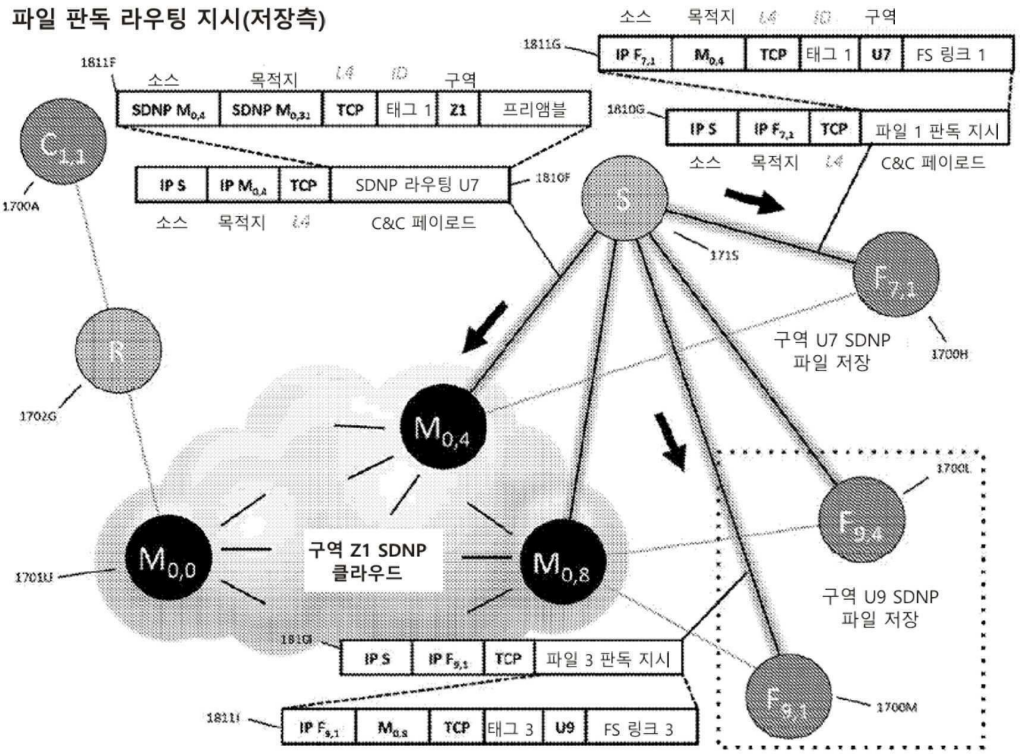
도면97b


파일 저장 서버 명칭 요청
구역 U1 SDNP
클라이언트
SDNP
명칭 서버
SDNP
신호 서버
구역 U7 SDNP
파일 저장
라우터
구역 Z1 SDNP
클라우드
구역 U9 SDNP
파일 저장
소스
목적지
C&C 페이로드
IP S
IP NS
TCP
FS 명칭 요청

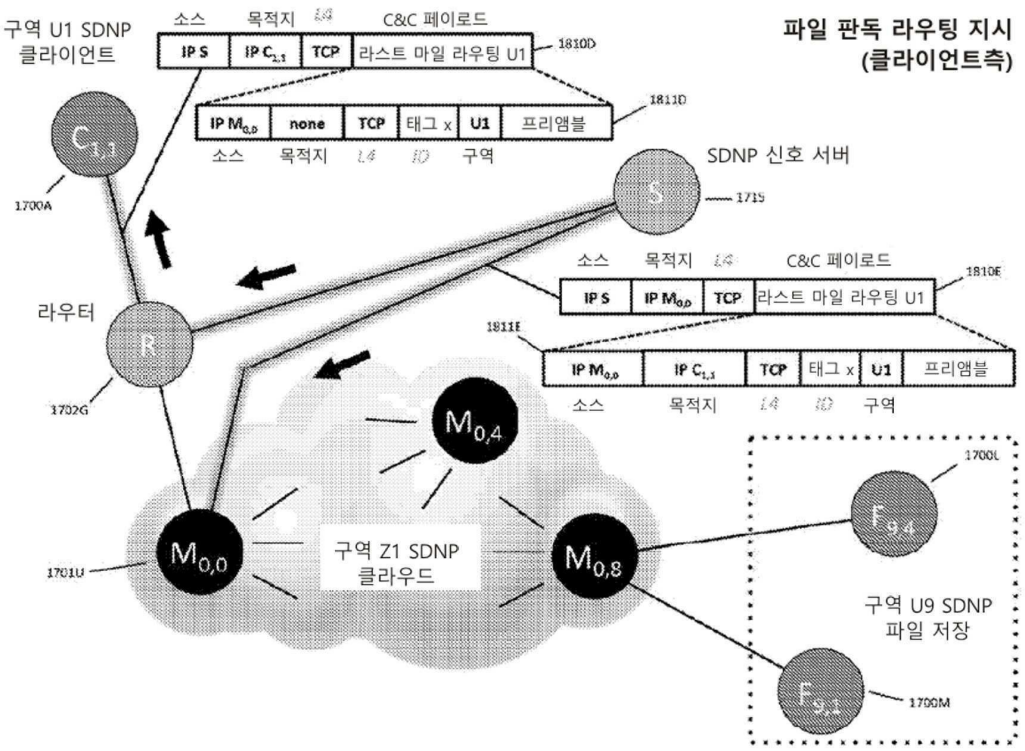
도면97c


구역 U1 SDNP
클라이언트
파일 저장 서버 명칭 전달
소스
목적지
C&C 페이로드
1810C
IP NS
IP S
TCP
FS 어드레스
1714
NS
1713
1715
S
SDNP
명칭 서버
SDNP
신호 서버
구역 U7 SDNP
파일 저장
$C_{1,1}$
1700A
라우터
R
1702G
$F_{7,1}$
1700H
$M_{0,4}$
$M_{0,0}$
$M_{0,8}$
1701U
구역 Z1 SDNP
클라이언트
1700L
$F_{9,4}$
구역 U9 SDNP
파일 저장
$F_{9,1}$
1700M

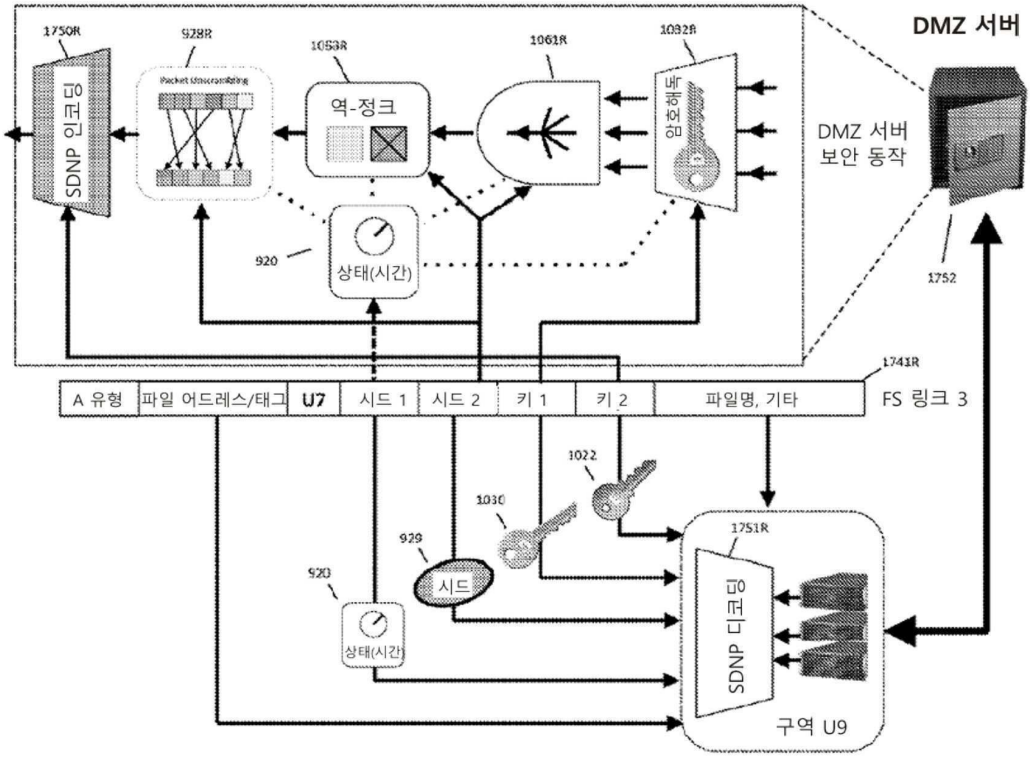
도면97d


파일 판독 라우팅 지시(저장측)
소스
목적지
구역
1811G
IP $F_{7,1}$
$M_{0,4}$
TCP
태그 1
U7
FS 링크 1
1811F
SDNP $M_{0,4}$
SDNP $M_{0,3}$
Z1
프리앰블
1810G
IP S
IP $F_{7,1}$
파일 1 판독 지시
C&C 페이로드
IP $M_{0,4}$
SDNP 라우팅 U7
1810F
$C_{1,1}$
1700A
S
1715
$F_{7,1}$
구역 U7 SDNP
파일 저장
1700H
R
1702G
$M_{0,4}$
$M_{0,0}$
$M_{0,8}$
1701U
구역 Z1 SDNP
클라이언트
1700L
$F_{9,4}$
구역 U9 SDNP
파일 저장
1810I
IP $F_{9,1}$
파일 3 판독 지시
1811I
$M_{0,8}$
태그 3
U9
FS 링크 3
$F_{9,1}$
1700M

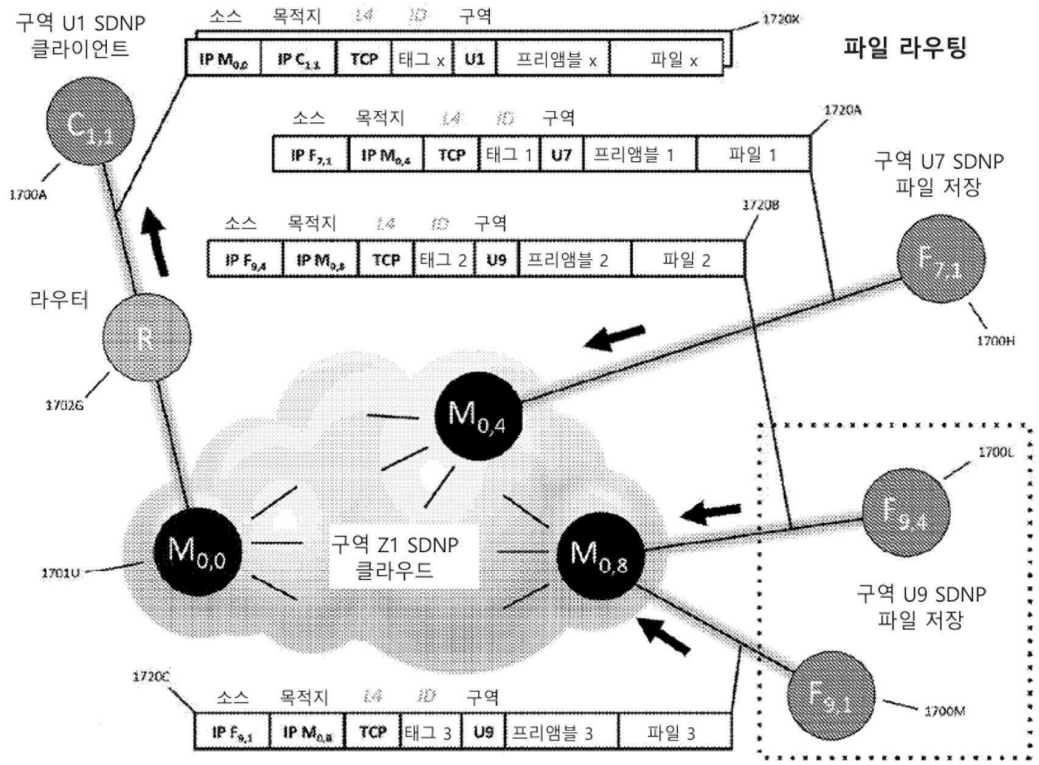
도면97e


구역 U1 SDNP
클라이언트
소스
목적지
L4
C&C 페이로드
IP S
IP C1,1
TCP
라스트 마일 라우팅 U1
1810D
파일 판독 라우팅 지시
(클라이언트측)
IP M0,0
none
TCP
태그 x
U1
프리앰블
1811D
소스
목적지
L4
ID
구역
C1,1
1700A
SDNP 신호 서버
S
1715
라우터
R
1702G
1810E
1811E
IP C1,1
M0,4
M0,0
M0,8
1701U
구역 Z1 SDNP
클라우드
1700L
F9,4
F9,1
1700M
구역 U9 SDNP
파일 저장

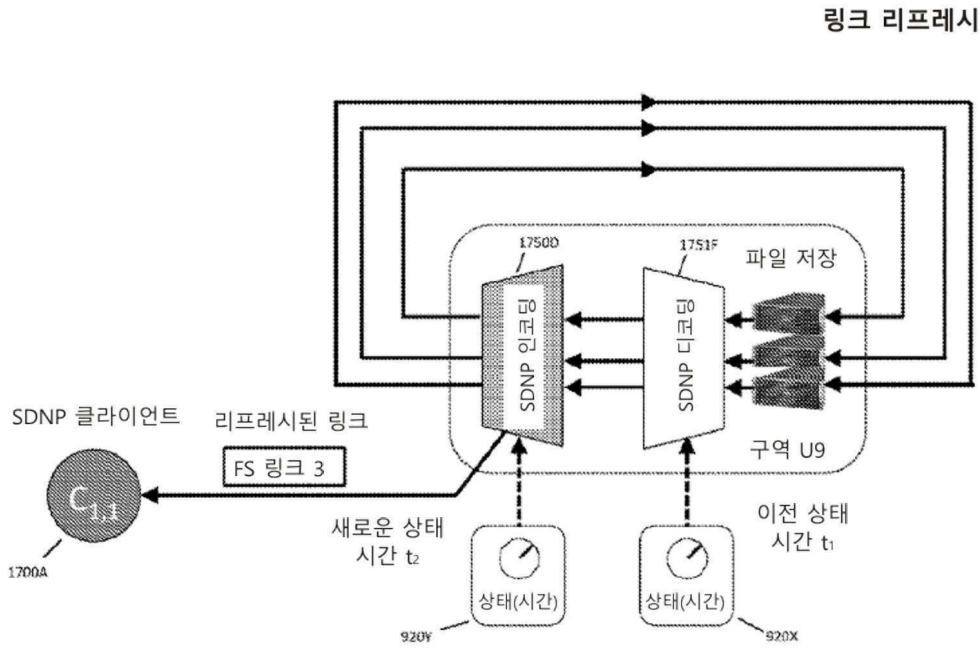
도면98


DMZ 서버
1750R
928R
1053R
1061R
1032R
SDNP 인코딩
역-정크
내용 허용
DMZ 서버
보안 동작
920
상태(시간)
1752
1741R
A 유형
파일 어드레스/태그
U7
시드 1
시드 2
키 1
키 2
파일명, 기타
FS 링크 3
1022
1030
929
시드
920
상태(시간)
1751R
SDNP 디코딩
구역 U9

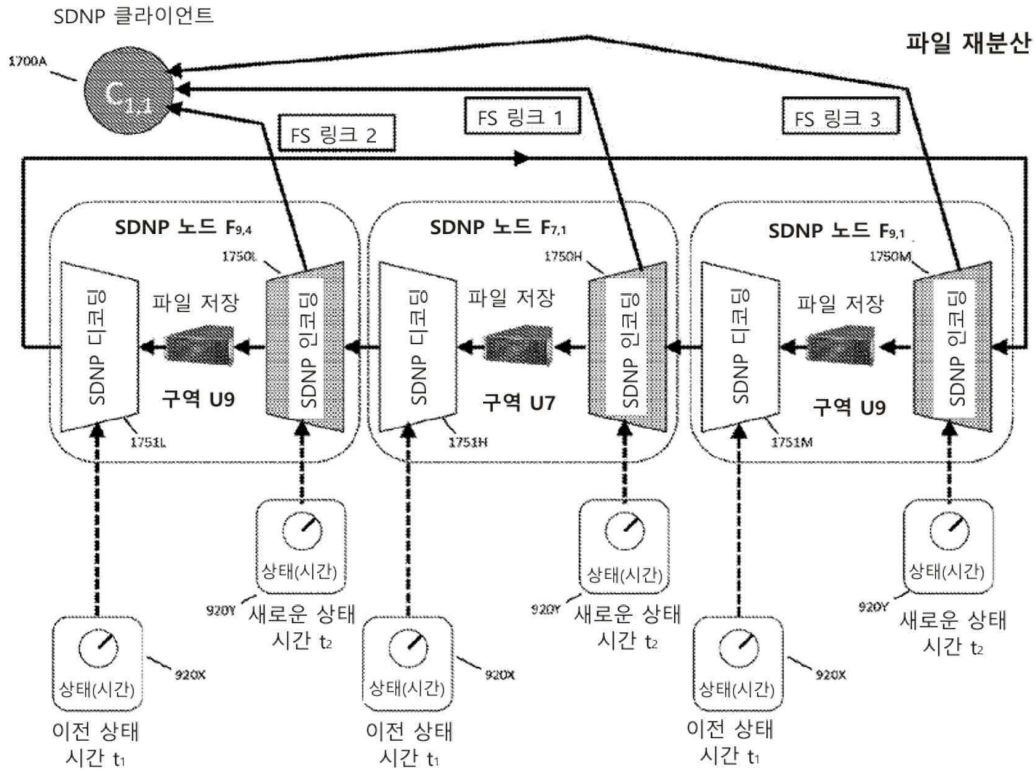
도면99


구역 U1 SDNP
클라이언트
소스 목적지 L4 ID 구역
1720X
IP M0,0 IP C1,1 TCP 태그 x U1 프리앰블 x 파일 x
파일 라우팅
C1,1
1700A
소스 목적지 L4 ID 구역
1720A
IP F7,1 IP M0,4 TCP 태그 1 U7 프리앰블 1 파일 1
구역 U7 SDNP
파일 저장
소스 목적지 L4 ID 구역
1720B
IP F9,4 IP M0,8 TCP 태그 2 U9 프리앰블 2 파일 2
F7,1
1700H
라우터
R
1702G
M0,4
1700L
F9,4
M0,0
1701U
구역 Z1 SDNP
클라우드
M0,8
구역 U9 SDNP
파일 저장
1720C
소스 목적지 L4 ID 구역
IP F9,1 IP M0,8 TCP 태그 3 U9 프리앰블 3 파일 3
F9,1
1700M

도면100


링크 리프레시
1750D
1751F
파일 저장
SDNP 인터페이스
SDNP 디바이스
SDNP 클라이언트
리프레시된 링크
FS 링크 3
구역 U9
C1,1
1700A
새로운 상태
시간 t2
이전 상태
시간 t1
상태(시간)
상태(시간)
920Y
920X

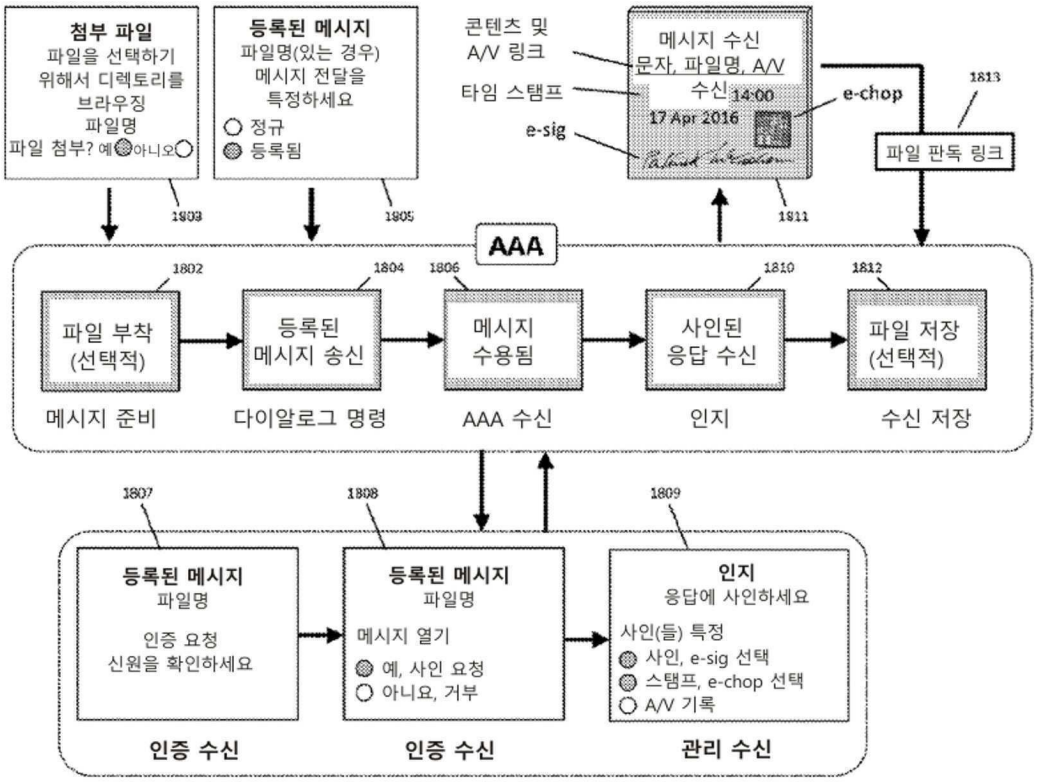
도면101


SDNP 클라이언트
파일 재분산
1700A
$C_{1,1}$
FS 링크 2
FS 링크 1
FS 링크 3
SDNP 노드 $F_{9,4}$
SDNP 노드 $F_{7,1}$
SDNP 노드 $F_{9,1}$
1750L
1750H
1750M
SDNP 디코더
파일 저장
SDNP 인코더
구역 U9
구역 U7
구역 U9
1751L
1751H
1751M
상태(시간)
920Y
새로운 상태
시간 $t_2$
920X
이전 상태
시간 $t_1$

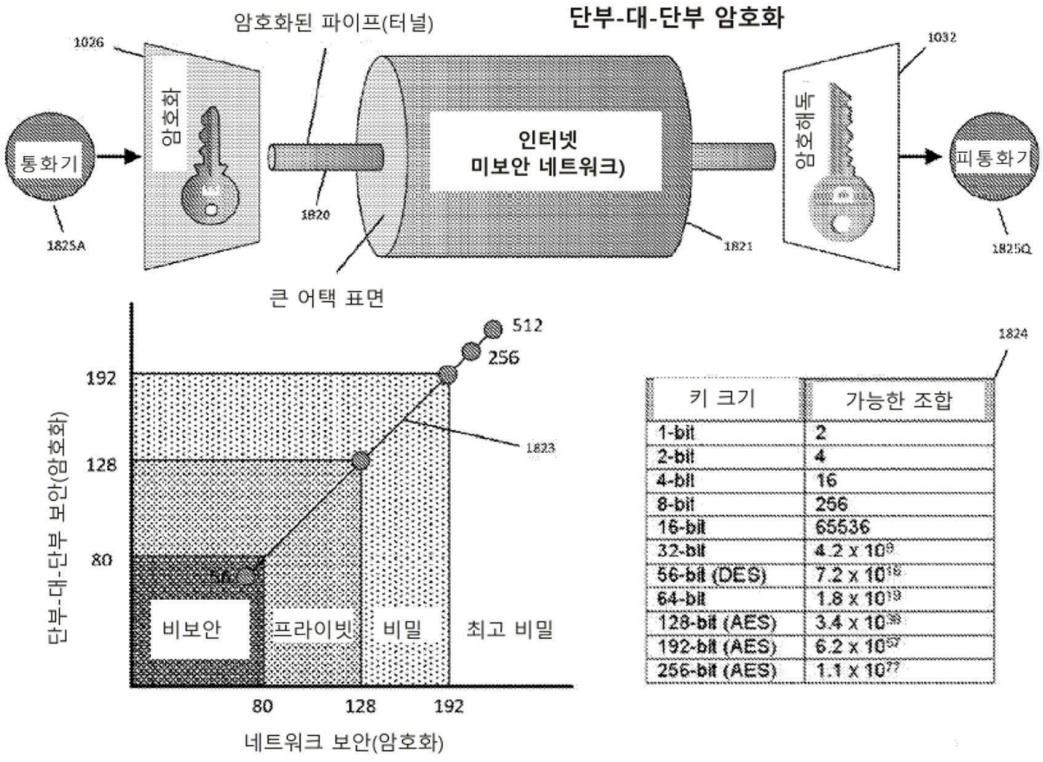
도면102


1800
텔코 LTE
8:02 AM
SDNP 사용자
13 Apr 2016
이것은 테스트입니다.
송신 13 Apr 08:04 AM
전달 17 Apr 08:38 PM
확인 17 Apr 08:38 PM
1801A
17 Apr 2016
알았음
송신 17 Apr 08:36 PM
전달 17 Apr 08:38 PM
확인 17 Apr 08:38 PM
1801B

도면103

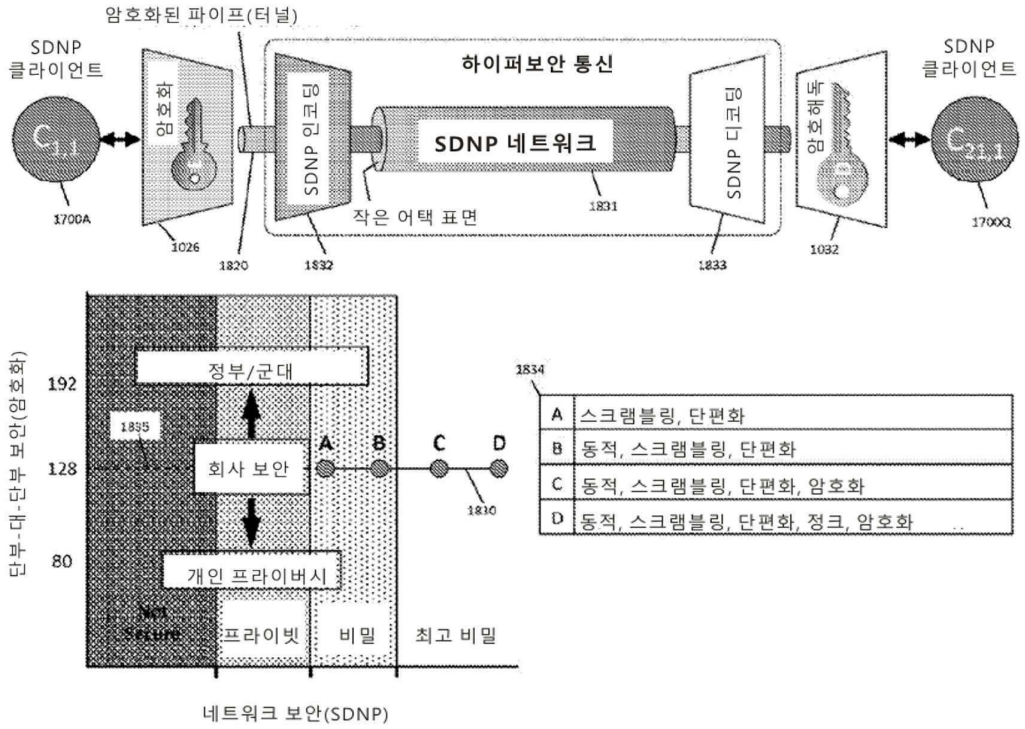



도면104a

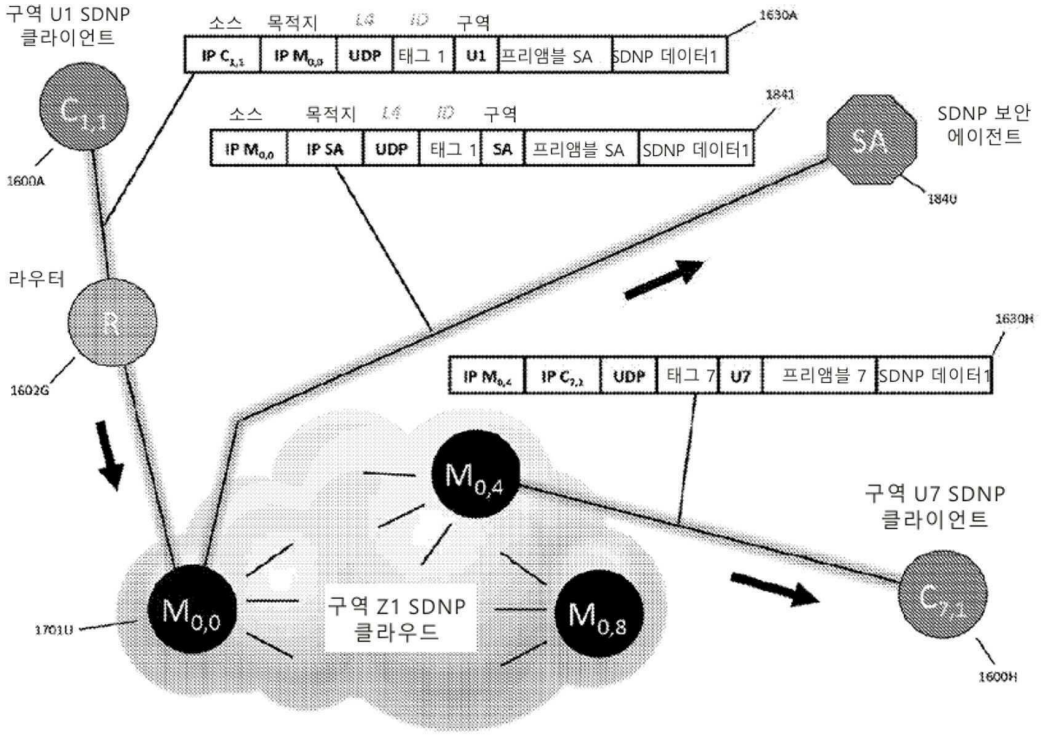



| 키 크기 | 가능한 조합 |
|---|---|
| 1-bit | 2 |
| 2-bit | 4 |
| 4-bit | 16 |
| 8-bit | 256 |
| 16-bit | 65536 |
| 32-bit | $4.2 \times 10^{9}$ |
| 56-bit (DES) | $7.2 \times 10^{16}$ |
| 64-bit | $1.8 \times 10^{19}$ |
| 128-bit (AES) | $3.4 \times 10^{38}$ |
| 192-bit (AES) | $6.2 \times 10^{57}$ |
| 256-bit (AES) | $1.1 \times 10^{77}$ |

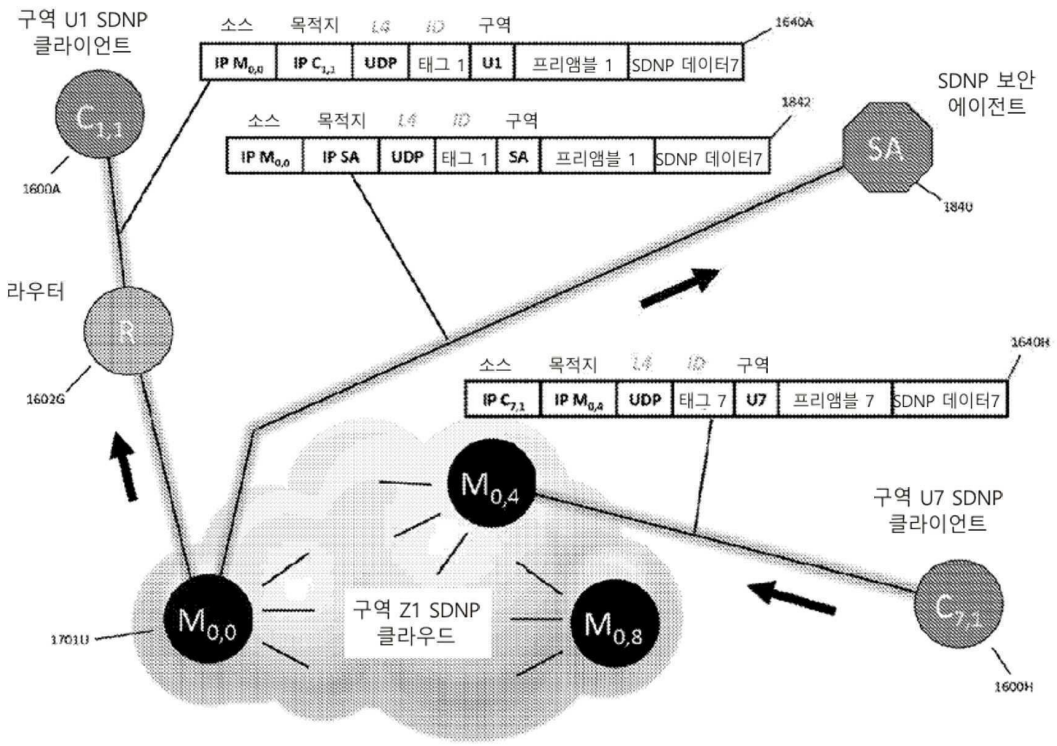
도면104b



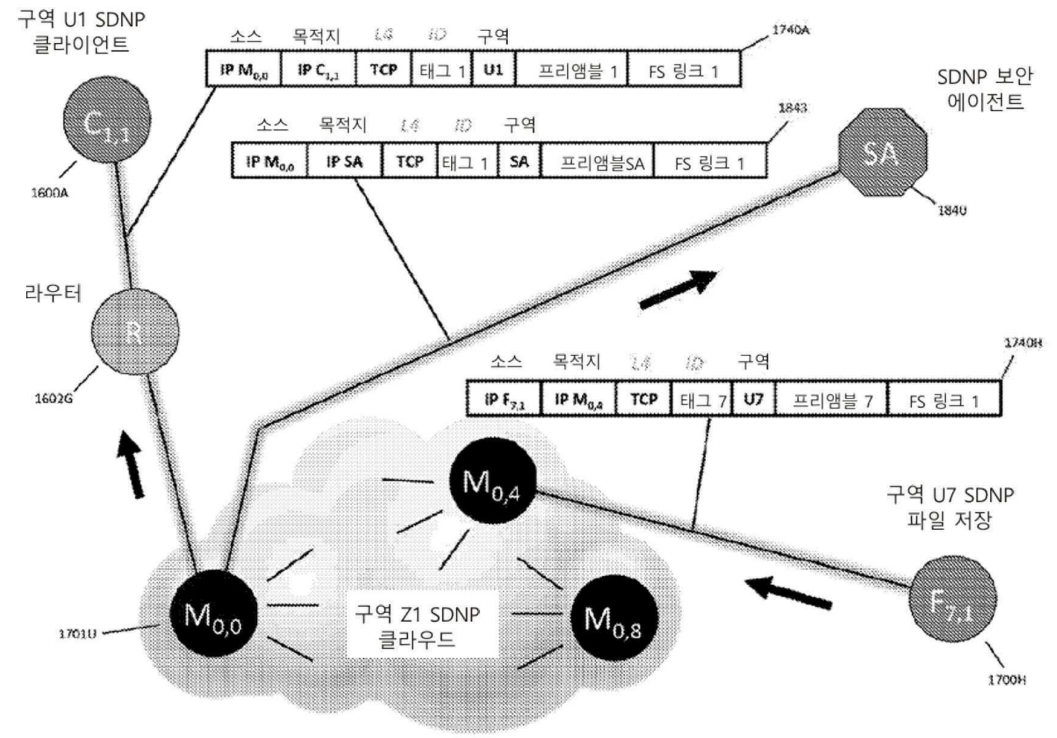

도면105a



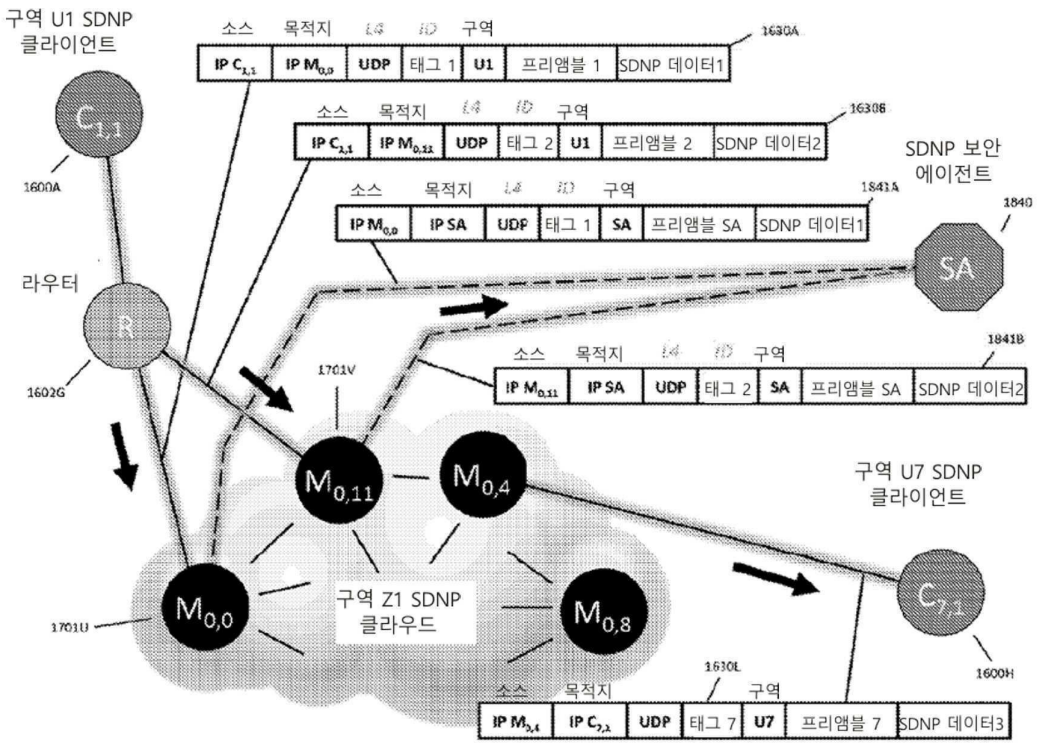
도면105b



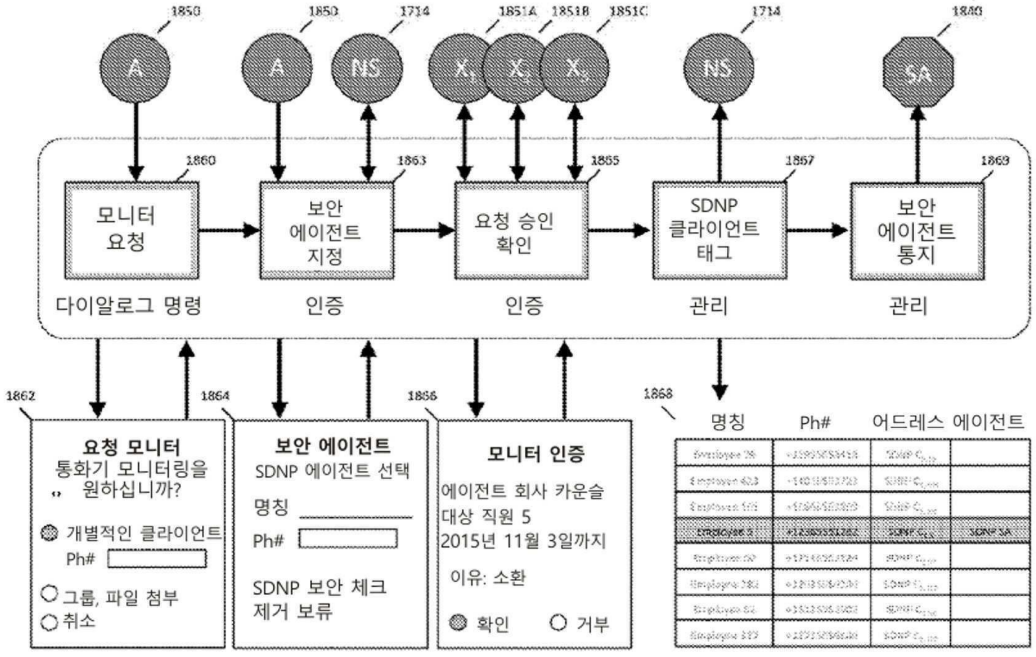

도면106



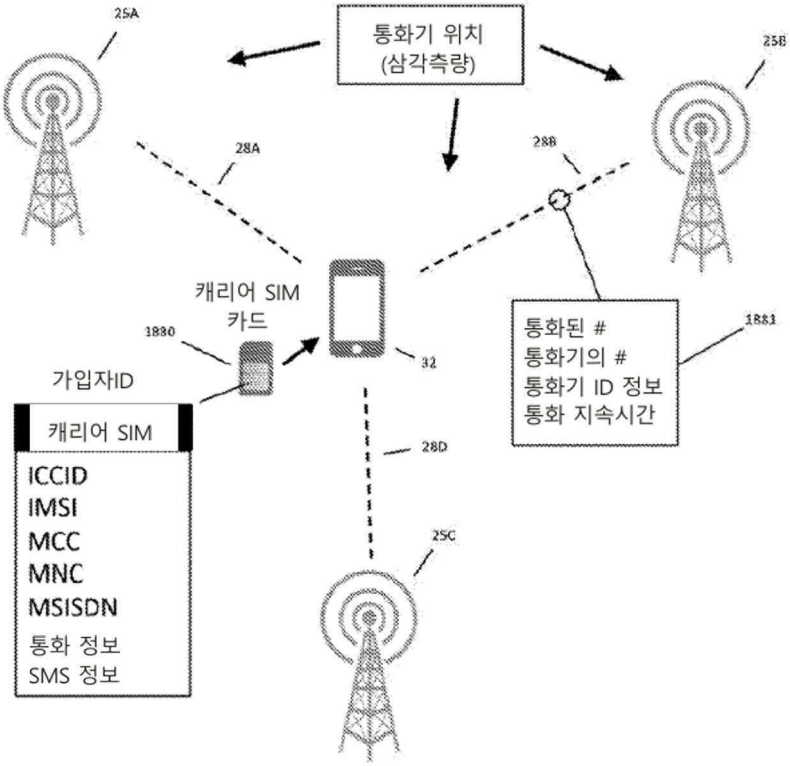
도면107


구역 U1 SDNP
클라이언트
소스 목적지 L4 ID 구역
IP C1,1 | IP M0,0 | UDP | 태그 1 | U1 | 프리앰블 1 | SDNP 데이터1
1630A
C1,1
1600A
소스 목적지 L4 ID 구역
IP C1,1 | IP M0,11 | UDP | 태그 2 | U1 | 프리앰블 2 | SDNP 데이터2
1630B
SDNP 보안
에이전트
소스 목적지 L4 ID 구역
IP M0,0 | IP SA | UDP | 태그 1 | SA | 프리앰블 SA | SDNP 데이터1
1841A
1840
SA
라우터
R
1602G
1701V
소스 목적지 L4 ID 구역
IP M0,11 | IP SA | UDP | 태그 2 | SA | 프리앰블 SA | SDNP 데이터2
1841B
M0,11
M0,4
구역 U7 SDNP
클라이언트
M0,0
1701U
구역 Z1 SDNP
클라우드
M0,8
C7,1
1600H
소스 목적지 L4 ID 구역
IP M3,4 | IP C7,1 | UDP | 태그 7 | U7 | 프리앰블 7 | SDNP 데이터3
1630L

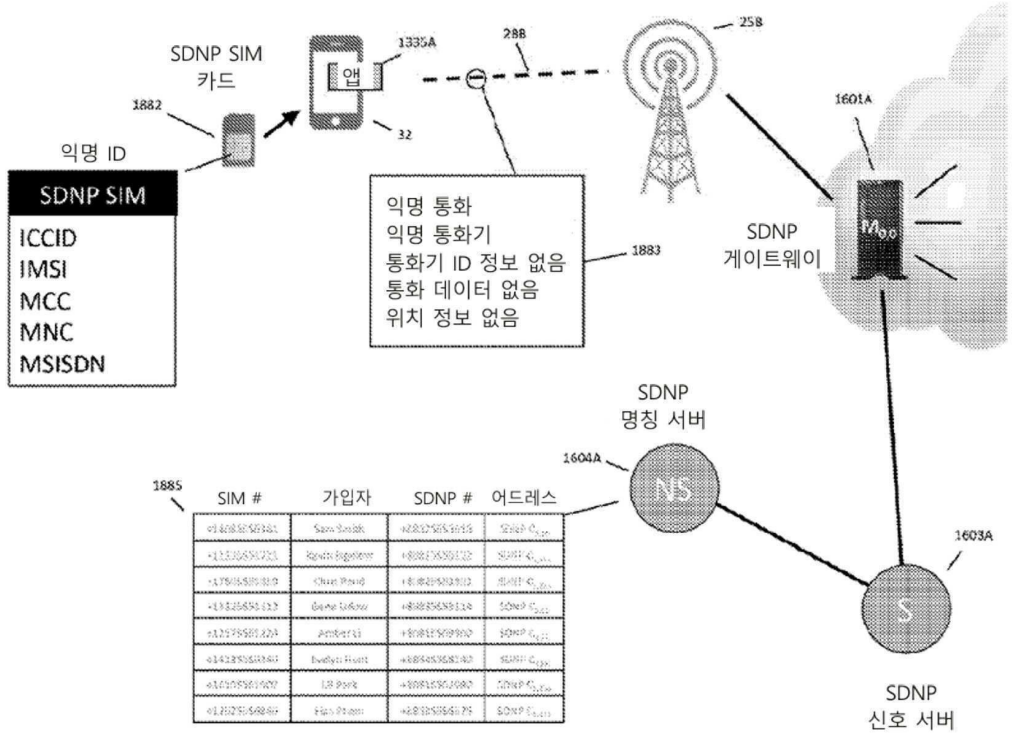
도면108


1850
A
1850
A
1714
NS
1851A
X1
1851B
X2
1851C
X3
1714
NS
1840
SA
1860
모니터
요청
1863
보안
에이전트
지정
1865
요청 승인
확인
1867
SDNP
클라이언트
태그
1869
보안
에이전트
통지
다이알로그 명령
인증
인증
관리
관리
1862
요청 모니터
통화기 모니터링을
원하십니까?
개별적인 클라이언트
Ph#
그룹, 파일 첨부
취소
1864
보안 에이전트
SDNP 에이전트 선택
명칭
Ph#
SDNP 보안 체크
제거 보류
1866
모니터 인증
에이전트 회사 카운슬
대상 직원 5
2015년 11월 3일까지
이유: 소환
확인
거부
1868
명칭
Ph#
어드레스 에이전트

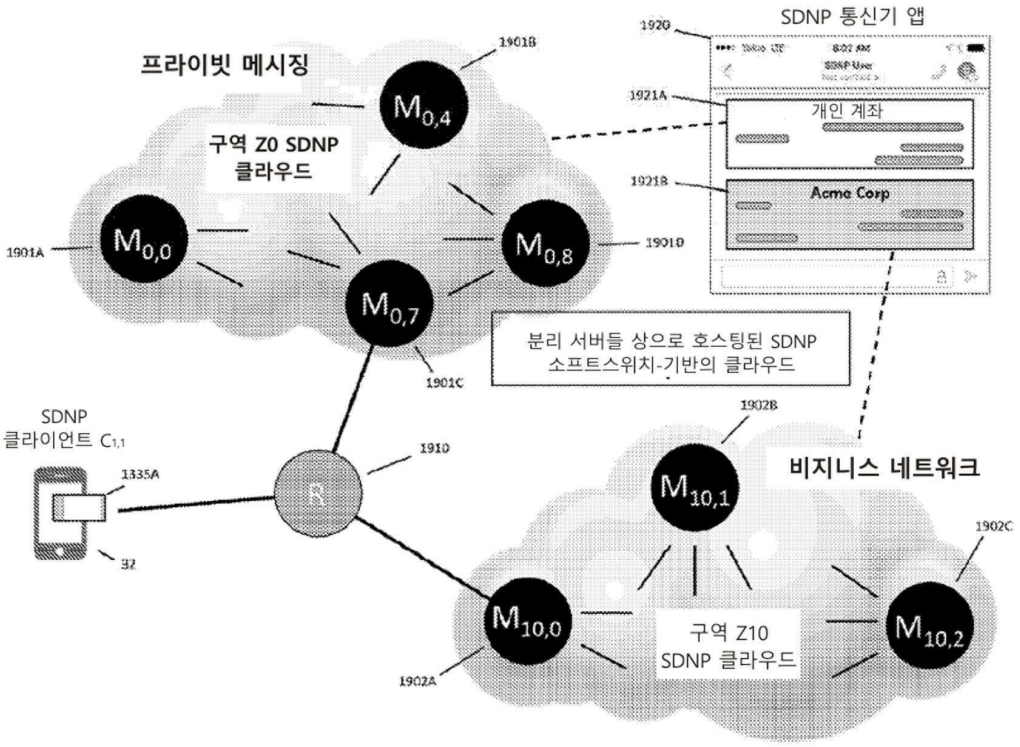
도면109


25A
통화기 위치
(삼각측량)
25B
28A
28B
캐리어 SIM
카드
1880
32
가입자ID
캐리어 SIM
ICCID
IMSI
MCC
MNC
MSISDN
통화 정보
SMS 정보
28D
25C
통화된 #
통화기의 #
통화기 ID 정보
통화 지속시간
1881

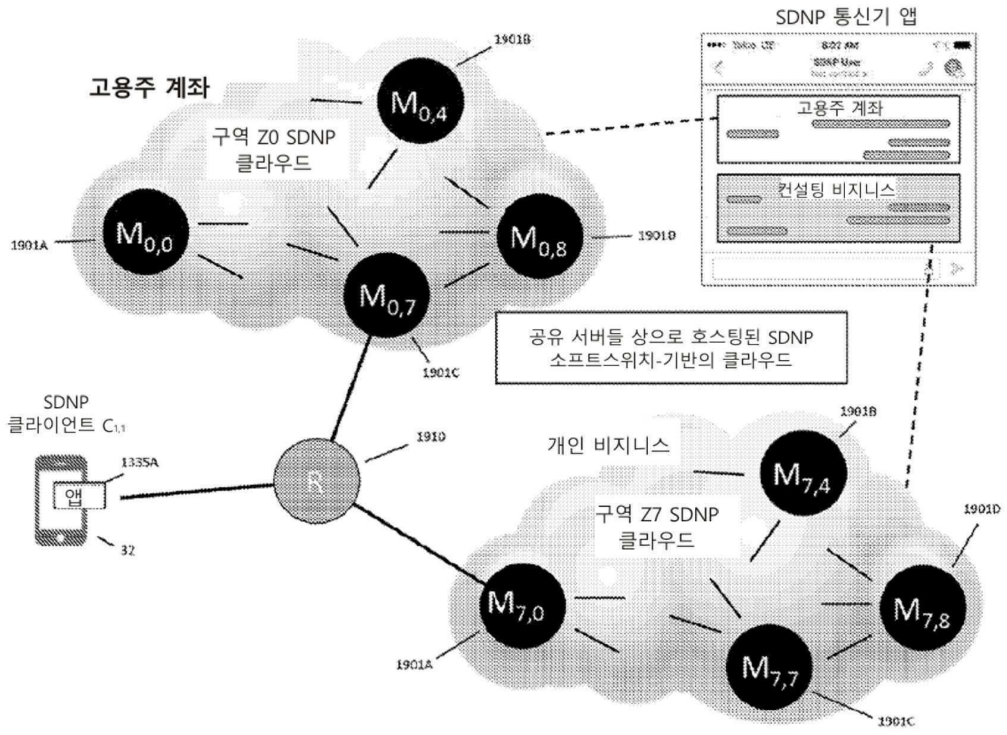
도면110


SDNP SIM
카드
1335A
앱
28B
25B
1882
32
익명 ID
SDNP SIM
ICCID
IMSI
MCC
MNC
MSISDN
익명 통화
익명 통화기
통화기 ID 정보 없음
통화 데이터 없음
위치 정보 없음
1883
1601A
SDNP
게이트웨이
SDNP
명칭 서버
1604A
NS
1885
SIM #
가입자
SDNP #
어드레스
1603A
S
SDNP
신호 서버

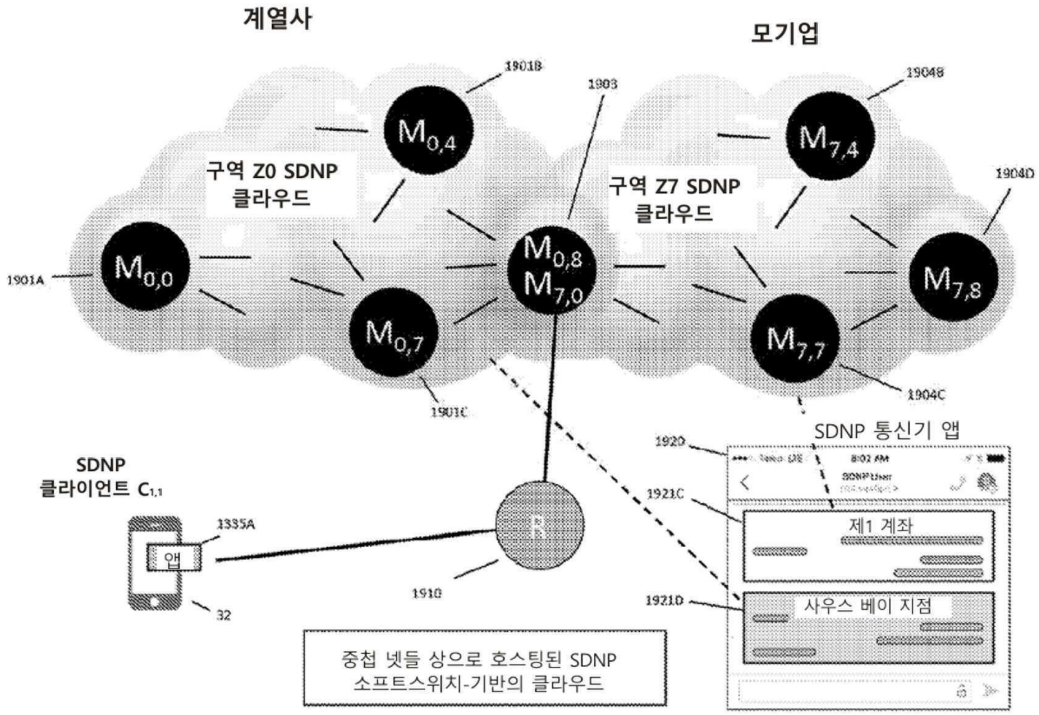
도면111


SDNP 통신기 앱
1920
프라이빗 메시징
1901B
$M_{0,4}$
구역 Z0 SDNP
클라우드
1921A
개인 계좌
1921B
Acme Corp
1901A
$M_{0,0}$
$M_{0,8}$
1901D
$M_{0,7}$
1901C
분리 서버들 상으로 호스팅된 SDNP
소프트스위치-기반의 클라우드
SDNP
클라이언트 $C_{1,1}$
1335A
32
1910
1902B
$M_{10,1}$
비지니스 네트워크
1902C
$M_{10,0}$
구역 Z10
SDNP 클라우드
$M_{10,2}$
1902A

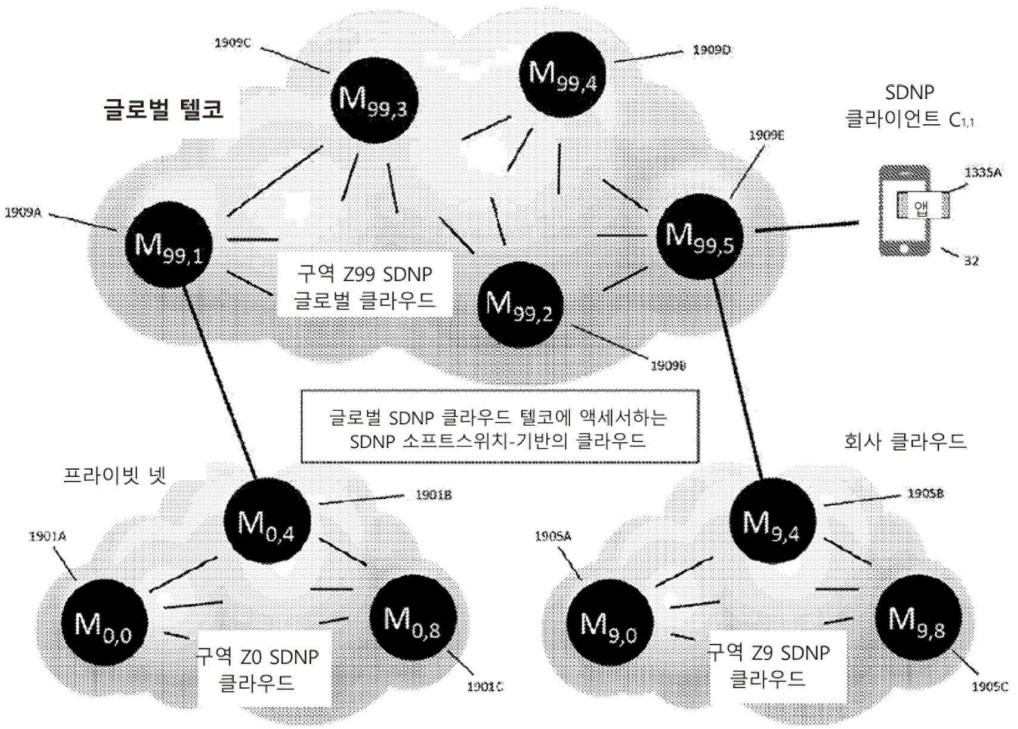
도면112


SDNP 통신기 앱
고용주 계좌
1901B
$M_{0,4}$
구역 Z0 SDNP
클라우드
고용주 계좌
컨설팅 비지니스
1901A
$M_{0,0}$
$M_{0,8}$
1901D
$M_{0,7}$
1901C
공유 서버들 상으로 호스팅된 SDNP
소프트스위치-기반의 클라우드
SDNP
클라이언트 $C_{1,1}$
1335A
앱
32
1910
개인 비지니스
1901B
$M_{7,4}$
구역 Z7 SDNP
클라우드
1901D
$M_{7,0}$
$M_{7,8}$
1901A
$M_{7,7}$
1901C

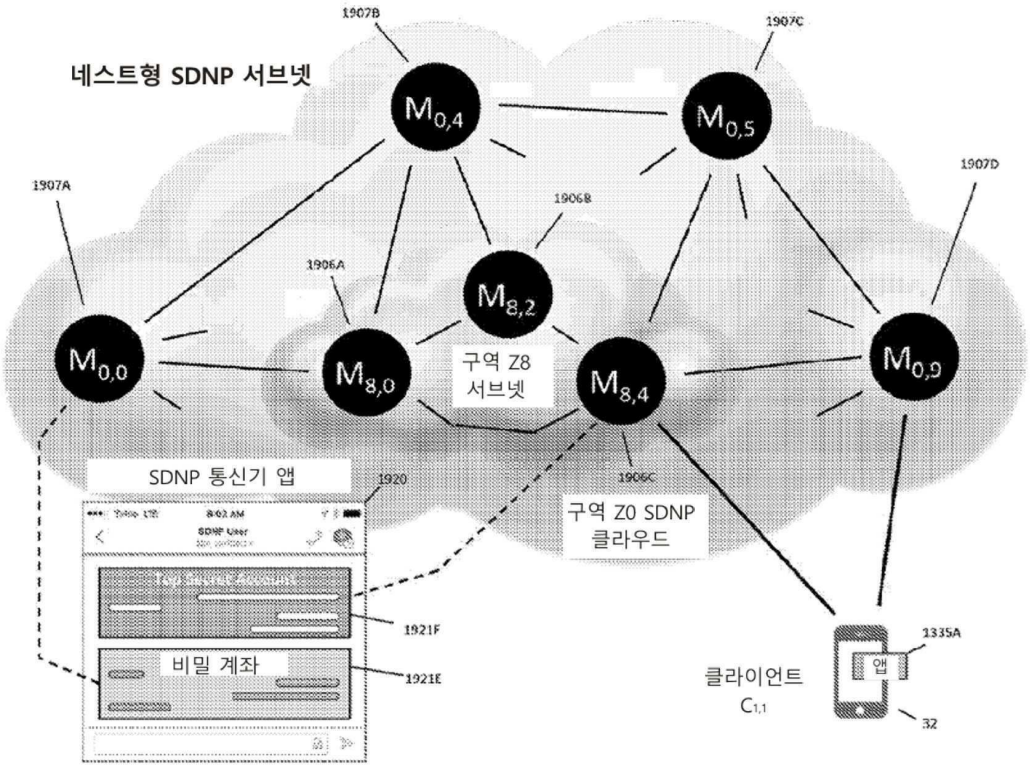
도면113


계열사
모기업
구역 Z0 SDNP
클라우드
구역 Z7 SDNP
클라우드
SDNP
클라이언트 C1,1
SDNP 통신기 앱
제1 계좌
사우스 베이 지점
앱
중첩 넷들 상으로 호스팅된 SDNP
소프트스위치-기반의 클라우드

도면114


글로벌 텔코
구역 Z99 SDNP
글로벌 클라우드
SDNP
클라이언트 C1,1
앱
글로벌 SDNP 클라우드 텔코에 액세서하는
SDNP 소프트스위치-기반의 클라우드
프라이빗 넷
구역 Z0 SDNP
클라우드
회사 클라우드
구역 Z9 SDNP
클라우드

도면115


네스트형 SDNP 서브넷
1907B
1907C
1907A
1907D
1906B
1906A
$M_{0,4}$
$M_{0,5}$
$M_{8,2}$
$M_{0,0}$
$M_{8,0}$
$M_{8,4}$
$M_{0,9}$
구역 Z8
서브넷
SDNP 통신기 앱
1920
1906C
구역 Z0 SDNP
클라우드
1921F
비밀 계좌
1921E
클라이언트
$C_{1,1}$
1335A
앱
32