РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 316 903** (13) **C2**

(51) МПК
H04L 12/28 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005134506/09, 07.06.2004**

(24) Дата начала отсчета срока действия патента:
07.06.2004

(30) Конвенционный приоритет:
06.06.2003 CN 03140977.6

(43) Дата публикации заявки: **10.06.2006**

(45) Опубликовано: **10.02.2008 Бюл. № 4**

(56) Список документов, цитированных в отчете о поиске: **RU 2201034 C2, 20.03.2003. RU 2129754 C1, 27.04.1999. WO 02082730 A1, 17.10.2002. US 2003084282 A1, 01.05.2003.**

(85) Дата перевода заявки PCT на национальную фазу:
10.01.2006

(86) Заявка PCT:
CN 2004/000614 (07.06.2004)

(87) Публикация PCT:
WO 2004/109980 (16.12.2004)

Адрес для переписки:
191002, Санкт-Петербург, а/я 5, ООО "Ляпунов и партнеры", пат.пов. Ю.В.Кузнецовой

(72) Автор(ы):
ЧЖАН Вэньлинь (CN)

(73) Патентообладатель(и):
Хювэй Текнолоджиз Ко., Лтд. (CN)

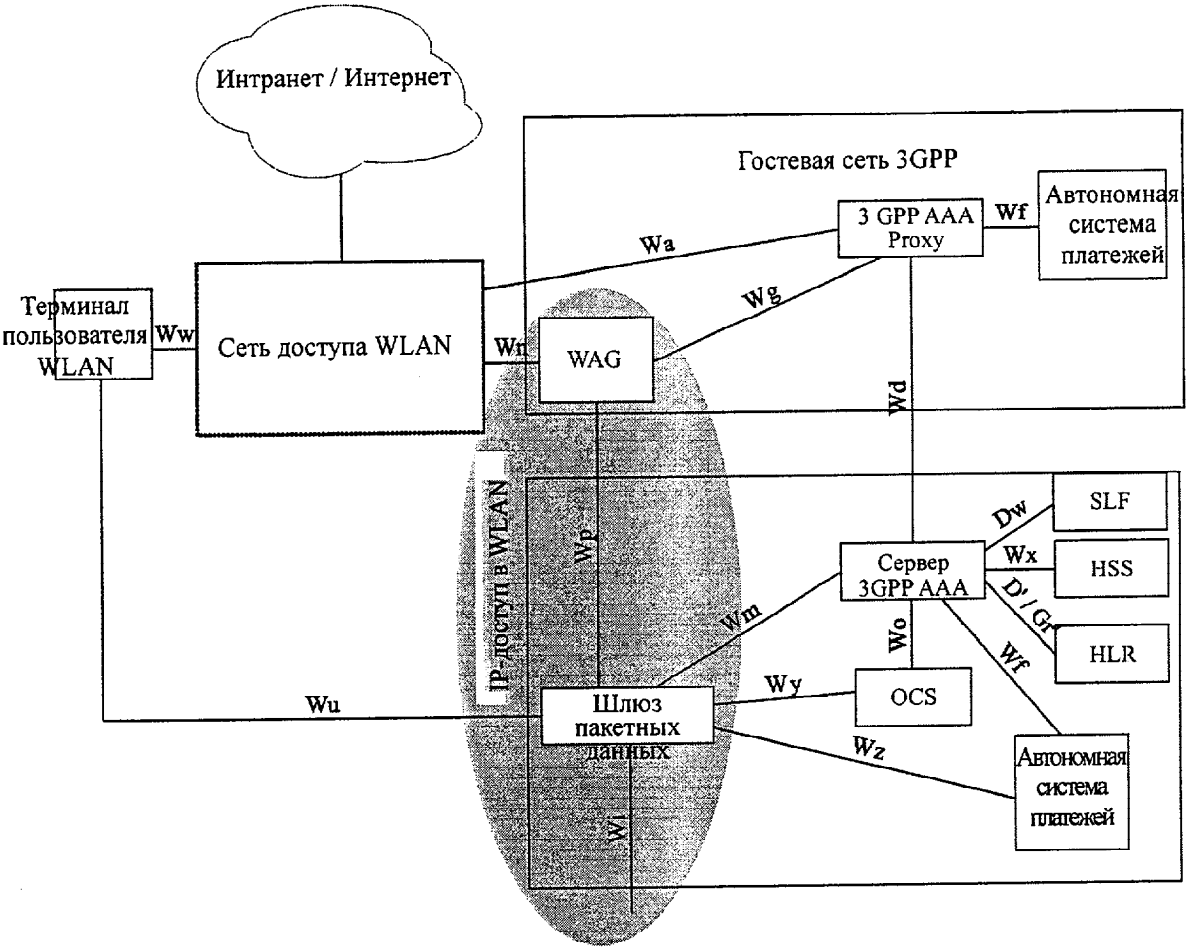
RU 2316903 C2

(54) СПОСОБ ПРОВЕРКИ ПОЛНОМОЧИЙ ДОСТУПА ПОЛЬЗОВАТЕЛЯ В БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ

(57) Реферат:

Настоящее изобретение раскрывает способ проверки полномочий доступа пользователя в беспроводных локальных сетях. В процессе получения терминалом пользователя беспроводной локальной сети (Wireless Local Area Network - WLAN) доступа к действующей WLAN во время проведения идентификации данного терминала пользователя WLAN сеть WLAN выясняет, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий, оказывающими влияние на доступ данного терминала пользователя WLAN; если разрешен, то сеть WLAN устанавливает правила доступа для данного терминала пользователя WLAN в соответствии с указанными условиями проверки полномочий; в противном случае сеть WLAN уведомляет терминал пользователя WLAN об отказе. Используя способ согласно данному изобретению, можно контролировать доступ в сеть различных пользователей в соответствии с разными условиями проверки полномочий и после получения ими доступа ограничивать разными правилами доступа. В результате расширяются возможности беспроводной локальной сети по управлению доступом и повышается производительность сети. 11 з.п. ф-лы, 5 ил.

RU 2316903 C2



Фиг. 1

RU 2316903 C2

RU 2316903 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 316 903** (13) **C2**

(51) Int. Cl.
H04L 12/28 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005134506/09, 07.06.2004**

(24) Effective date for property rights: **07.06.2004**

(30) Priority:
06.06.2003 CN 03140977.6

(43) Application published: **10.06.2006**

(45) Date of publication: **10.02.2008 Bull. 4**

(85) Commencement of national phase: **10.01.2006**

(86) PCT application:
CN 2004/000614 (07.06.2004)

(87) PCT publication:
WO 2004/109980 (16.12.2004)

Mail address:
191002, Sankt-Peterburg, a/ja 5, OOO "Ljapunov i partnery", pat.pov. Ju.V.Kuznetsovoj

(72) Inventor(s):
ChZhAN Vehn'lin' (CN)

(73) Proprietor(s):
Khjuvehj Teknolodzhiz Ko., Ltd. (CN)

RU 2316903 C2

(54) METHOD FOR CHECKING USER ACCESS PRIVILEGES IN A WIRELESS LOCAL NETWORK

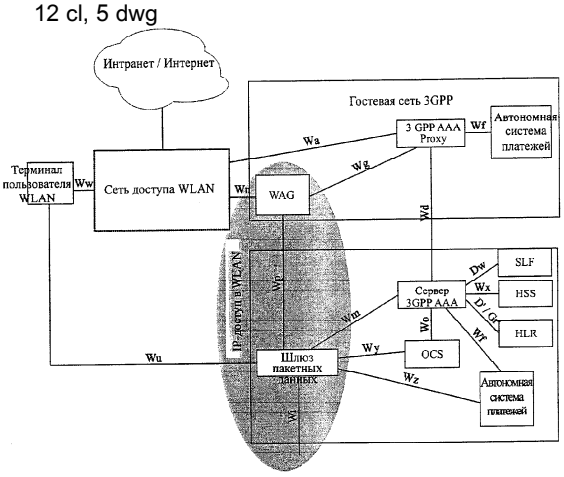
(57) Abstract:

FIELD: methods for checking user access privileges in wireless local networks.

SUBSTANCE: in accordance to the invention, in process of receipt by user terminal of wireless local area network (WLAN) of access to active WLAN the WLAN network determines whether the given WLAN user terminal is allowed access in accordance with privilege check conditions which influence access to given terminal by WLAN user; if access is allowed, then WLAN network sets access rules for given terminal of WLAN user in accordance to given privilege check conditions; in opposite case WLAN network notifies the terminal of WLAN user about access denial. Using the method according to the invention, it is possible to regulate access to network of different users in accordance with different privilege check conditions and to limit these by different access rules after access is granted.

EFFECT: expanded functional capabilities of wireless local network in terms of access control, increased productivity of network.

12 cl, 5 dwg



Фиг. 1

RU 2316903 C2

Предмет изобретения

Настоящее изобретение относится к средствам идентификации и проверки полномочий в сети, в частности к способу проверки полномочий доступа пользователя в действующей беспроводной локальной сети (WLAN - Wireless Local Area Network).

Уровень техники

С ростом предъявляемых пользователями требований к скорости беспроводного доступа в соответствии с этими требованиями времени появилась беспроводная локальная сеть (WLAN), которая может обеспечить высокоскоростной беспроводной доступ к данным в пределах небольшой зоны охвата. В сеть WLAN входят различные технические средства, среди которых широко применяется технический стандарт IEEE 802.11b, который использует диапазон частот 2,4 ГГц, и где самая высокая скорость передачи данных может достигать 11 Мб/сек. Стандарт ШЕЕ 8 02.11 g и технология Bluetooth также используют этот диапазон частот, а самая высокая скорость передачи данных стандарта 802.11g может достигать 54 Мб/сек. Другие новые стандарты, такие как ШЕЕ 802.11 a и ETSI BRAN Hiperlan2, используют диапазон частот 5 ГГц; самая высокая скорость передачи также может достигать 54 Мб/сек.

Несмотря на существование различных средств беспроводного доступа, большинство сетей WLAN используют для передачи пакет данных протокол Internet (Internet Protocol - IP). В беспроводных сетях IP используют специальный способ доступа WLAN, являющийся прозрачным для протокола IP верхнего уровня. Пользователи получают доступ к беспроводной сети IP через точки доступа (Access Point - AP), а устройства управления сетью и обеспечения связи соединены и образуют IP-сеть передачи данных.

С расширением и развитием технологии WLAN взаимодействие между WLAN и различными беспроводными мобильными сетями связи становится предметом текущих исследований, при этом мобильной сетью связи может быть глобальная система мобильной связи (Global System for.Mobile communications - GSM), система множественного доступа с кодовым разделением (Code Division Multiple Access - CDMA), широкополосная система множественного доступа с кодовым разделением (Wideband Code Division Multiple Access - WCDMA), система множественного доступа с синхронным разделением по времени и частоте (Time Division-Synchronous Code Division Multiple Access - TD-SCDMA) и система CDMA2000. В соответствии со стандартами Проекта сотрудничества третьего поколения (Third Generation Partnership Project - 3GPP) терминал пользователя может быть подключен через сеть доступа WLAN к сети Интернет или Интранет или может быть подключен через сеть доступа WLAN к домашней сети системы 3GPP или к гостевой сети системы 3GPP. Точнее говоря, получая доступ локально, терминал пользователя WLAN подключается через сеть доступа WLAN к домашней сети 3GPP; при использовании роуминга терминал пользователя WLAN подключается через сеть доступа WLAN к гостевой сети 3GPP. Некоторые объекты в гостевой сети 3GPP соединяются с соответствующими объектами, имеющими такие же функции в домашней сети 3GPP; это, например, Proxy сервер 3GPP идентификации, проверки полномочий и учета (AAA - Authentication, Authorization and Accounting) в гостевой сети 3GPP и сервер 3GPP идентификации, проверки полномочий и учета (AAA) в домашней сети 3GPP; шлюз доступа WLAN (WLAN Access Gateway - WAG) в гостевой сети 3GPP и шлюз пакетных данных (Packet Data Gateway - PDG) в домашней сети 3GPP и т.д., как изображено на фиг.1.

Как показано на фиг.1, система 3GPP состоит, в основном, из домашнего сервера подписчика/домашнего регистра местоположения (Ноше Subscriber Server - HSS/Home Location Register - HLR), сервера 3GPP AAA, 3GPP AAA Proxy, WAG, шлюза пакетных данных, автономной системы платежей и системы платежей по сети (Online Charging System - OCS). Терминал пользователя WLAN (WLAN UE), сеть доступа WLAN и все объекты системы 3GPP образуют сеть 3GPP-WLAN, обеспечивающую межсетевой обмен; эта обеспечивающая межсетевой обмен сеть 3GPP-WLAN может рассматриваться как система обслуживания WLAN. Сервер 3GPP AAA отвечает за идентификацию, проверку

полномочий и учет пользователей, а также за сбор информации о загрузке, передаваемой сетью доступа WLAN, и за передачу собранной информации системе платежей. Шлюз пакетных данных отвечает за передачу пользовательских данных через сеть доступа WLAN в сеть 3GPP или другие пакетные сети. Система платежей, в основном, принимает и записывает информацию о платежах конкретного пользователя, передаваемую из сети. Система OCS управляет работой сети по периодической передаче информации о платежах в систему учета расходов пользователя, осуществляющего оплату по сети, и выполняет соответствующие статистические и управляющие операции.

В обычных условиях, когда терминалу пользователя WLAN нужно получить доступ к сети 3GPP-WLAN, данный терминал пользователя отправляет запрос доступа соответствующему устройству идентификации в сети 3GPP-WLAN через сеть доступа WLAN; устройство идентификации доступа, которым обычно является сервер 3GPP AAA, получив запрос, выполняет его идентификацию. Если запрос проходит идентификацию, то этому терминалу пользователя будут просто открыты все порты. Однако структура действующей WLAN намного сложнее, чем упрощенная структура сети, показанная на фиг.1. Здесь под названной действующей WLAN имеется в виду WLAN, в которой можно работать и которой можно управлять, которая будет не только выполнять идентификацию, проверку полномочий и учет пользователей, но также будет обеспечивать один или несколько видов сетевого доступа и сетевых услуг, например, различные сервисы локальных сетей (LAN) в местных гостиницах или аэропортах и игры по локальным сетям, а также доступ к LAN, которая может предоставлять различные сервисы, доступ в Интернет и сервисы на основе пакетной сети 3GPP.

Поскольку действующая WLAN может получать доступ к различным сетям LAN одновременно, а правила эксплуатации сравнительно сложны, то можно задавать разные правила доступа в зависимости от учетной записи пользователя и времени доступа. Поэтому традиционный способ проверки полномочий доступа, основанный только на результате идентификации, оказывается неконтролируемым и неудобным при эксплуатации.

Краткое изложение сущности изобретения

Таким образом, основной целью настоящего изобретения является предоставление способа проверки полномочий доступа пользователя в WLAN, позволяющего управлять доступом разных терминалов пользователей в WLAN при разных ограничивающих условиях, в связи с чем могут быть улучшены возможности контроля доступа и увеличена эффективность эксплуатации сети.

Чтобы достичь вышеуказанную цель, в настоящем изобретении предложена следующая техническая схема.

Способ проверки полномочий доступа пользователя в беспроводной локальной сети, содержащий следующие шаги.

В процессе получения терминалом пользователя доступа к действующей беспроводной локальной сети (Wireless Local Area Network - WLAN), во время проведения идентификации данного терминала пользователя WLAN, действующая сеть WLAN выясняет, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий, оказывающими влияние на доступ данного терминала пользователя WLAN; если доступ разрешен, то в соответствии с названными условиями проверки полномочий определяют правила доступа для данного терминала пользователя WLAN; в противном случае терминал пользователя WLAN уведомляют об отказе.

Способ содержит дополнительные шаги: направление установленных правил доступа одному или нескольким соответствующим объектам, обеспечивающим выполнение правила доступа, для обеспечения соблюдения ограничения на доступ данного терминала пользователя.

В вышеупомянутой схеме процедура идентификации и проверки полномочий терминала пользователя WLAN заключается в следующем: после того, как терминал пользователя WLAN отправляет запрос доступа действующей сети WLAN, действующая сеть WLAN

выполняет идентификацию правомочности получения доступа текущим терминалом пользователя WLAN; если терминал пользователя WLAN проходит идентификацию, действующая сеть WLAN продолжает выяснять, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий; в противном случае действующая сеть WLAN передает данному терминалу пользователя WLAN информацию об отказе в доступе.

Вышеуказанные условия проверки полномочий, оказывающие влияние на доступ терминала пользователя WLAN, содержат: условия учетной записи пользователя, информацию о подписке пользователя, правила эксплуатации или любую комбинацию трех вышеперечисленных. Названная информация о подписке пользователя содержит список с указанием сетевых сервисов, к которым данному пользователю разрешен доступ. Правила доступа устанавливает сервер AAA в действующей сети WLAN.

Названные правила доступа являются ограничительными условиями, применяемыми для определения области или пути доступа для текущего терминала пользователя, или ограничительными условиями, применяемыми для определения времени доступа для текущего терминала пользователя, или пустыми условиями, а именно - отсутствием ограничительного условия на доступ для данного терминала пользователя.

Объектом, обеспечивающим выполнение названного правила, являются AAA, шлюз доступа WLAN (WAG), контроллер доступа (Access Controller - AC), точка доступа (Access Point - AP) или терминал пользователя. Если объектом, обеспечивающим выполнение правил, является терминал пользователя, то способ дополнительно содержит следующие шаги: после определения правил доступа сеть одновременно передает терминалу пользователя информацию об успешности идентификации доступа и проверки полномочий текущего терминала пользователя WLAN и правила доступа, о которых необходимо проинформировать данный терминал пользователя.

В вышеуказанной схеме действующая сеть WLAN является обеспечивающей межсетевой обмен сетью 3GPP-WLAN, сетью 3GPP2-WLAN или другой действующей сетью WLAN, имеющей пользователей-подписчиков.

На вышеуказанной схеме видно, что ключевой момент настоящего изобретения заключается в следующем: при обращении терминала пользователя WLAN за доступом к действующей сети WLAN, во время проведения идентификации данного терминала пользователя, эта сеть выясняет, разрешен ли доступ данному терминалу пользователя в соответствии с условиями проверки полномочий данного терминала пользователя, определяет соответствующие правила доступа для данного терминала пользователя в соответствии с условиями проверки полномочий, а затем в соответствии с установленными правилами доступа ограничивает область, путь или время доступа для данного пользователя в последующих процедурах или последующих сервисных приложениях.

Поэтому в способе, предусмотренном настоящим изобретением, контроль доступа терминала пользователя содержит не только идентификацию правомочности, но также определение других условий проверки полномочий и правил доступа, настроенных в соответствии с условиями проверки полномочий. Поэтому разные терминалы пользователей WLAN будут получать доступ к действующей сети WLAN в соответствии с разными условиями проверки полномочий и после получения доступа будут подчиняться ограничениям, накладываемым разными правилами доступа. Соответственно, расширяются возможности WLAN по проверке полномочий доступа. Кроме того, когда терминал пользователя WLAN запрашивает сервис, действующая сеть WLAN интерпретирует терминал пользователя в соответствии с соответствующими правилами доступа и предоставляет сервисы текущему терминалу пользователя, получающему доступ, только в ограниченной области, на ограниченном пути и на ограниченное время. Соответственно, работоспособность сети и эффективность ее эксплуатации могут быть увеличены, и сеть сможет предоставлять доступ к различным областям или различным путям или на разное время одному и тому же пользователю или разным пользователям, таким образом облегчая управление доступом и обеспечивая возможность разнообразных

сервисов.

На фиг.1 приведена принципиальная схема, отображающая структуру системы сетей WLAN и 3GPP, обеспечивающей межсетевой обмен.

На фиг.2 приведена принципиальная схема, отображающая структуру действующей сети WLAN.

На фиг.3 приведена блок-схема, иллюстрирующая идентификацию доступа и проверку полномочий действующей сетью WLAN в соответствии с настоящим изобретением.

На фиг.4 приведена принципиальная схема, иллюстрирующая сетевую структуру действующей сети WLAN в реализации настоящего изобретения.

На фиг.5 приведена блок-схема идентификации доступа и проверки полномочий в реализации, изображенной на фиг.4.

Подробное описание реализации изобретения

Для пояснения цели, технической схемы и преимуществ настоящего изобретения далее идет подробное описание настоящего изобретения со ссылками на сопровождающие чертежи и конкретные реализации.

На фиг.2 приведена принципиальная схема, иллюстрирующая сетевую структуру действующей сети WLAN. Как показано на фиг.2, сеть WLAN на фиг.2 является действующей сетью WLAN, в которой сеть доступа не только напрямую подсоединена к глобальным сетям, как Интернет, другие сети Интранет и глобальные частные сети, но подсоединена также, напрямую или через шлюз доступа действующей сети, к различным сетям, например, локальным сетям местных гостиниц или аэропортов и мобильным действующим сетям, таким как домен сети 3GPP PS. Названные мобильные действующие сети могут быть глобальными или локальными сетями. Шлюз доступа действующей сети подсоединен одновременно к домашней сети и к гостевой сети текущего терминала пользователя, а также к устройству идентификации и проверки полномочий доступа сети WLAN, например, к серверу 3GPP AAA.

Для терминала пользователя WLAN, которому требуется определенный сервис через действующую сеть WLAN, непосредственный доступ к определенным сетям или доступ через шлюз может быть ограничен в момент подписки на основе принципа диверсификации сервисов. Например, терминалу пользователя может быть не разрешен доступ к сети Интранет внутри аэропорта, соединенной с сетью доступа WLAN, но он может получать доступ в Интернет; или терминал пользователя должен получать доступ в Интернет или в определенные частные сети по подписке; или данный терминал пользователя динамически ограничивается в непосредственном доступе или доступе через шлюз к некоторым специальным сетям в течение определенного периода или в определенной области в соответствии с такими условиями, как учетная информация терминала пользователя, правила управления или эксплуатационные правила данного оператора. Поэтому при получении доступа к действующей сети WLAN терминал пользователя должен быть ограничен скорее правилами доступа, соответствующими условиям, оказывающим влияние на полномочия, и эти правила доступа должны применяться к соответствующим шлюзам сети, осуществляющим переключение или маршрутизацию, а не получать полномочия на доступ только в соответствии с результатами идентификации.

В практических применениях названная проверка полномочий доступа по настоящему изобретению не имеет отношения к проверке разрешения сервиса, относящейся к мобильной сети. Названную проверку полномочий доступа используют для определения того, разрешен ли терминалу пользователя доступ или при каком условии терминал пользователя может получить доступ к определенной сети, перед проверкой разрешения сервиса. Решение относительно того, может ли текущий терминал пользователя, получающий доступ к WLAN, пользоваться соответствующими сервисами, должно приниматься последующими процедурами разрешения сервиса. Различие между проверкой полномочий доступа и проверкой разрешения сервиса раскрыто на следующем примере: предположим, что терминал пользователя запрашивает доступ в Интернет, в то время как текущая сеть может предоставить два вида доступа в Интернет, один из

которых является прямым доступом в Интернет через сеть доступа WLAN, а другой заключается в получении доступа в Интернет через сеть доступа WLAN, а затем через WAG; тогда, если для текущего терминала пользователя нет ограничений на доступ, терминал пользователя может произвольным образом выбрать один из двух режимов получения доступа либо предоставить средствам проверки разрешения сервиса выбор используемого режима доступа; однако в случае ограничения на получение прямого доступа в Интернет через сеть доступа WLAN текущий терминал пользователя может получить доступ в Интернет только через WAG, в то время как возможность предоставления сервисов Интернет данному терминалу пользователя должна определяться в ходе проверки разрешения сервиса.

Процедура проверки полномочий доступа для терминала пользователя в настоящем изобретении изображена на фиг.3 и включает следующие шаги:

Шаг 301-302: когда терминал пользователя WLAN запрашивает доступ в сеть, сеть выполняет идентификацию доступа для данного терминала пользователя. Иначе говоря, устройство идентификации доступа и проверки полномочий в сети запускает процедуру проверки полномочий между терминалом пользователя и сетью через устройство управления доступом: терминал пользователя отправляет требуемую для идентификации информацию устройству идентификации доступа и проверки полномочий через устройство управления доступом; после получения соответствующей информации терминала пользователя устройство идентификации и проверки полномочий само выполняет идентификацию доступа; если идентификация завершается успешно, то осуществляется переход к следующему шагу, в противном случае терминал пользователя уведомляется об неудаче идентификации доступа, и текущая процедура идентификации доступа завершается. Устройством управления доступом здесь может быть контроллер доступа (Access Controller - AC) в сети доступа WLAN, шлюз доступа WLAN (WAG) или комбинация двух вышеперечисленных; устройством идентификации доступа и проверки полномочий может быть сервер 3GPPAAA.

Шаг 303: после успешной идентификации доступа терминала пользователя устройство идентификации доступа и проверки полномочий принимает решение, разрешить ли доступ терминалу пользователя, сообразуясь с условиями проверки полномочий для данного терминала; если в доступе отказано, уведомляет данный терминал пользователя о неудаче проверки полномочий доступа, а затем завершает текущую процедуру проверки полномочий; в противном случае выполняет определение правил доступа для текущего терминала пользователя, получающего доступ, в соответствии с его условиями полномочий, причем данные правила доступа указывают, какие ограничительные принципы действуют во время получения доступа терминалом пользователя, получившим разрешение. Названные условия проверки полномочий содержат: информацию об учетной записи пользователя, данные подписки пользователя, эксплуатационные правила операторов или любую комбинацию трех вышеперечисленных. Названные правила доступа, в основном, относятся к ограничению на область сети или на пути, по которым должен осуществляться доступ, например: доступные шлюз и область, соединенные с сетью, сетевое оборудование для доступа. Правила могут также содержать ограничения на время доступа. Устройство идентификации доступа и проверки полномочий может явным образом задать пустое правило доступа, что указывает на отсутствие специфических ограничений на доступ данного терминала пользователя.

Названные данные подписки пользователя могут представлять собой список с указанием доступных сервисов, на которые подписан пользователь, например, Интернет, локальная игровая сеть, сеть цепи предприятий Starbuck, IPv6-Intemet и т.д.

Шаг 304: после определения правил доступа, с одной стороны, устройство идентификации доступа и проверки полномочий уведомляет терминал пользователя и устройство управления доступом об успешной идентификации доступа и проверки полномочий для данного терминала пользователя и сохраняет правила доступа, которые были определены; с другой стороны, устройство идентификации доступа и проверки

полномочий уведомляет все соответствующие объекты, обеспечивающие выполнение правил доступа, о правилах доступа, которые были определены, здесь под соответствующими объектами, обеспечивающими выполнение правил доступа, понимают один или несколько сетевых объектов, которые могут выполнять эти правила, например, 3GPP-AAA, устройство проверки разрешения сервиса, AC, AP, устройство DHCP, шлюз доступа действующей сети и т.д. Устройство идентификации доступа и проверки полномочий может также уведомить терминал пользователя обо всех или части установленных правил доступа, таким образом терминал пользователя может знать или принимать участие в обеспечении выполнения названных правил доступа. Уведомление о правилах доступа может быть отправлено терминалу пользователя с уведомлением об успешности идентификации доступа и проверки полномочий.

Шаг 305: объект, обеспечивающий выполнение правил доступа, например, устройство проверки разрешения сервиса, показанное на фиг.3, сохраняет правила после их получения и выполняет правила доступа, когда терминал пользователя запрашивает сервис сети WLAN через данный объект. Например, в соответствии с правилами доступа, устройство проверки разрешения сервиса может принять решение разрешить текущему терминалу пользователя доступ к указанной области сети в течение данного периода времени и определить, откуда он должен получать доступ. Как правило, оба устройства - разрешения сервиса и проверки полномочий доступа - находятся на AAA.

Выполнение конкретных правил доступа может обеспечиваться существующими способами, такими как средства фильтрации, схема распределения IP, виртуальная локальная сеть (VLAN), разделение на подсети, виртуальная частная сеть (VPN - Virtual Private Network), двухуровневое разделение пользователей и т.д. Например, при помощи средств VLAN или IP-назначения устройство управления доступом может поместить текущий терминал пользователя, запрашивающий сервис, на уровень подсети, подчиняясь правилам доступа, или выделить независимый адрес подсети текущему терминалу пользователя, запрашивающему такой сервис, к которому данный терминал пользователя может получить доступ только через подсеть или область, указанную сетью VLAN. Когда выполнение правил доступа обеспечивается устройством проверки разрешения сервиса, если пользователь запросил соответствующие сервисы, устройство разрешения сервиса принимает решение о том, отвечают ли запрошенные сервисы требованию правил доступа, соответствующих текущему терминалу пользователя; если запрос не соответствует правилам доступа, то он будет отклонен до проверки разрешения сервиса.

Проверку полномочий доступа в соответствии с настоящим изобретением выполняют при получении пользователем доступа к действующей сети WLAN, обычно после того, как сеть завершает идентификацию правомочности объекта текущего терминала пользователя, получающего доступ, как описано в шагах 301 -305. Очевидно, что проверку полномочий доступа можно выполнить до идентификации пользователя, т.е. сначала принимают решение относительно условий проверки полномочия текущего терминала пользователя, получающего доступ, и определяют правила доступа, а затем выполняют идентификацию правомочности объекта, за исключением того, что этот процесс является относительно сложным. Когда уведомляют терминал пользователя, результат идентификации и результат проверки полномочий обычно передают в одном уведомляющем сообщении, например, сообщении протокола EAP об успешности EAP. О результате идентификации и результате проверки полномочий можно сообщить также раздельно, например сообщить о результате идентификации до сообщения о результате проверки полномочий. Названная действующая сеть WLAN в настоящем изобретении включает обеспечивающую межсетевой обмен сеть 3GPP-WLAN, обеспечивающую межсетевой обмен сеть 3GPP2-WLAN или другие действующие сети WLAN, имеющие пользователей-подписчиков.

На фиг.4 приведена принципиальная схема, иллюстрирующая сетевую структуру действующей сети WLAN в реализации настоящего изобретения. Как показано на фиг.4, в данной обеспечивающей межсетевой обмен действующей сети 3GPP-WLAN, 3GPP-AAA

является устройством идентификации и проверки полномочий доступа; участок доступа WLAN состоит, в основном, из AC и AP; а AC, WAG или комбинация AC и WAG является устройством управления доступом. Через участок доступа WLAN действующая сеть WLAN может напрямую предоставлять сервис 41 локальной сети и сервис 42 доступа в Интернет терминалам пользователей в некоторых «горячих точках», таких как аэропорт или гостиницы. Через участок доступа WLAN и WAG действующая сеть WLAN может также предоставлять характерный для 3GPP сервис 43 для терминалов пользователей WLAN посредством доступа к действующей сети 3GPP. Данная действующая сеть WLAN включает также HSS/HLR, используемый для хранения различной информации о терминале пользователя, например, информацию о подписке.

Снова обращаясь к фиг.4, отметим, что характерный для 3GPP сервис 43, который терминал пользователя WLAN может получить через действующую сеть WLAN, содержит: сервис 431 доступа в Интернет, предоставляемый оператором сети 3GPP через WAG, специальный сервис 432 локальной сети и мобильные сервисы на основе домена с коммутацией пакетов (PS - packet switched) мобильной сети, например, различные сервисы гостевой наземной мобильной сети общего пользования (Visited Public Land Mobile Network - VPLMN) 433 и сервисы HPLMN 434. Сервис 431 доступа в Интернет может предоставлять более широкую полосу пропускания, чем полоса пропускания прямого доступа в Интернет в «горячих точках». Другими словами, при предоставлении одного и того же сервиса сервис 431 доступа в Интернет гораздо быстрее, чем сервис 42 доступа в Интернет, но первый может оказаться гораздо дороже второго. Специальный сервис 432 локальной сети означает, что оператор частной сети может предоставлять терминалам пользователей такие внутренние интерактивные специальные сервисы, как менеджмент или игра. Названные различные сервисы 433 и 434 содержат по меньшей мере такие специальные сервисы мобильной сети, как сервис мультимедийной IP-подсистемы (IP Multimedia Subsystem - IMS), сервис коротких сообщений (Short Message Service - SMS), сервис мультимедийных сообщений (Multimedia Message Service - MMS) и сервис определения местоположения (LoCation Service - LCS).

Первая реализация

На основе сетевой структуры, представленной на фиг.4, при условии, что терминал пользователя A подписан только на локальный сервис Интернета в области «горячей точки» и в списке проверки полномочий доступа с информацией о подписке пользователя есть только сервис Интернета, тогда, как показано на фиг.5, процедура проверки полномочий доступа для пользователя терминала A состоит в следующем:

Шаг 501-502: запрашивая доступ в сеть 3GPP-WLAN, как показано на фиг.4, терминал пользователя A отправляет запрос доступа и информацию, необходимую для идентификации, в сеть 3GPP-AAA через AC; затем 3GPP-AAA проводит идентификацию правомочности объекта терминала пользователя A и, если терминал пользователя A проходит идентификацию, выполняет шаг 503 и продолжает принимать решение относительно условий проверки полномочий терминала пользователя A; в противном случае возвращает информацию о неудаче идентификации доступа терминалу пользователя A и завершает процедуру.

Шаг 503: 3GPP-AAA решает, разрешить ли доступ терминалу пользователя A в соответствии со всеми условиями проверки полномочий данного терминала; если доступ не разрешен, то 3GPP-AAA возвращает информацию о неудаче проверки полномочий доступа терминалу пользователя A и завершает процедуру; в противном случае 3GPP-AAA определяет правила доступа терминала пользователя A в соответствии с условиями проверки полномочий данного терминала. Таким образом, в соответствии с данными подписки терминала пользователя A, правила доступа терминала пользователя A определяют как "доступ только к локальному Интернету области «горячей точки»".

Шаг 504: 3GPP-AAA уведомляет терминал пользователя A об успешной идентификации доступа и проверки полномочий, а также о правилах доступа, установленных на шаге 503, и уведомляет AC сети доступа WLAN, чтобы AC мог обеспечить выполнение правил

доступа.

Шаг 505: AC сохраняет установленные правила доступа после их получения, когда терминал пользователя запрашивает сервисы Интернет; в соответствии с сохраненными правилами доступа AC выясняет, что данный терминал пользователя может получить доступ только к локальному Интернету в области «горячей точки», и выясняет, находится ли данный терминал пользователя в текущий момент в области «горячей точки»; если "да", то предоставляет терминалу пользователя прямой доступ к локальному Интернету через AC; в противном случае - через средства VLAN или через IP-назначение AC помещает терминал пользователя в подсеть, которая может быть соединена только с локальным Интернетом в области «горячей точки», или выделяет независимый адрес подсети для терминала пользователя A, отличающийся тем, что данной подсети разрешен доступ только в локальный Интернет. Таким образом, терминал пользователя A может получить доступ только в локальный Интернет.

Вторая реализация

Основана на сетевой структуре, показанной на фиг.4, при условии, что терминалу пользователя B разрешен доступ в сеть только через WAG и запрещено получать доступ локально в области «горячей точки». Как показано на фиг.5, процедура проверки полномочий доступа терминала пользователя B, по существу, точно такая же, как соответствующая процедура для терминала пользователя A в первой реализации, за исключением того, что на шаге 503 правила доступа терминала пользователя B установлены как "разрешено получать доступ через WAG, запрещено получать локальный доступ в области «горячей точки»". Таким образом, на шаге 505 AC будет следить за тем, чтобы терминал пользователя B имел доступ только к WAG, и не разрешит терминалу пользователя B соединяться с другими сетями. Когда терминал пользователя B запрашивает сервисы Интернета, сервис 42 доступа в Интернет не может быть использован терминалом пользователя B, пока доступен только сервис 431 доступа в Интернет, а именно, терминал пользователя B может только получить доступ к действующей сети 3GPP через WAG, чтобы воспользоваться сервисом доступа в Интернет, предоставляемым действующей сетью 3GPP.

Третья реализация

Основана на сетевой структуре, показанной на фиг.4, при условии, что терминалу пользователя C не разрешено получать доступ в гостевую наземную мобильную сеть общего пользования (Visited Public Land Mobile Network - VPLMN). Как показано на фиг.5, процедура проверки полномочий доступа терминала пользователя C, по существу, точно такая же, как соответствующая процедура для терминала пользователя A в первой реализации, за исключением того, что на шаге 503 правила доступа терминала пользователя C установлены как «не разрешено получать доступ в гостевую наземную мобильную сеть общего пользования». На основе правил доступа терминал пользователя C имеет больше прав доступа и в соответствии со своими запросами сервисов может получать доступ к различным сетям, соединенным с сетью доступа WLAN, за исключением гостевой наземной мобильной сети общего пользования. Чтобы пользователь не мог получить доступ в гостевую наземную мобильную сеть общего пользования, выполнение правил доступа может быть обеспечено в WAG или непосредственно в 3GPP-AAA. Например, если терминал пользователя C запрашивает соответствующий сервис, то согласно правилам доступа терминала пользователя C будет принято решение относительно соответствия запрашиваемого сервиса правилам доступа данного терминала; если "нет", т.е. если терминал пользователя C в текущий момент находится в гостевой наземной мобильной сети общего пользования и запрашивает сервис, предоставляемый данной наземной мобильной сетью общего пользования, то данный запрос отклоняется до проверки разрешения сервиса; в противном случае выполняется проверка разрешения сервиса.

Вышеприведенное описание является только предпочтительным вариантом реализации настоящего изобретения и не ограничивает объем настоящего изобретения.

Формула изобретения

1. Способ проверки полномочий доступа пользователя в беспроводной локальной сети, содержащий следующие шаги: осуществление терминалом пользователя беспроводной локальной сети WLAN (Wireless Local Area Network) доступа к действующей WLAN; выяснение действующей сетью WLAN, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий, влияющими на доступ данного терминала пользователя WLAN; и определение действующей сетью WLAN правил доступа данного терминала пользователя WLAN в соответствии с указанными условиями проверки полномочий, если доступ данному терминалу пользователя WLAN разрешен; выполнение управления, по меньшей мере, по одному из показателей: область доступа, путь доступа, время доступа и качество доступа сервиса, терминалом пользователя WLAN на основании указанных правил доступа.

2. Способ по п.1, в котором указанный шаг выполнения управления, по меньшей мере, по одному из показателей: область доступа, путь доступа, время доступа и качество доступа сервиса, терминалом пользователя WLAN содержит направление указанных правил доступа одному или нескольким соответствующим объектам; ограничение указанными одним или несколькими соответствующими объектами, по меньшей мере, одного из показателей: область доступа, путь доступа, время доступа и качество доступа сервиса, терминала пользователя WLAN на основании указанных правил доступа.

3. Способ по п.1 или 2, дополнительно содержащий шаги: после того, как терминал пользователя WLAN отправляет запрос доступа к действующей сети WLAN, действующая сеть WLAN сначала выполняет идентификацию правомочности получения доступа текущим терминалом пользователя WLAN; если терминал пользователя WLAN проходит идентификацию, то сеть WLAN выясняет, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий; в противном случае отправляет данному терминалу пользователя WLAN информацию об отказе в доступе.

4. Способ по п.1, отличающийся тем, что указанные условия проверки полномочий, оказывающие влияние на доступ терминала пользователя WLAN, содержат условия учетной записи пользователя, информацию о подписке пользователя, правила эксплуатации или любую комбинацию трех вышеперечисленных.

5. Способ по п.1, отличающийся тем, что правила доступа устанавливает сервер идентификации, проверки полномочий и учета AAA (Authentication Authorization and Accounting) в действующей сети WLAN.

6. Способ по п.1, отличающийся тем, что указанное качество доступа сервиса содержит полосу пропускания терминала пользователя, получающего в текущий момент доступ к WLAN.

7. Способ по п.1, отличающийся тем, что названное правило доступа задают пустым условием, если нет ограничений на доступ для данного терминала пользователя WLAN.

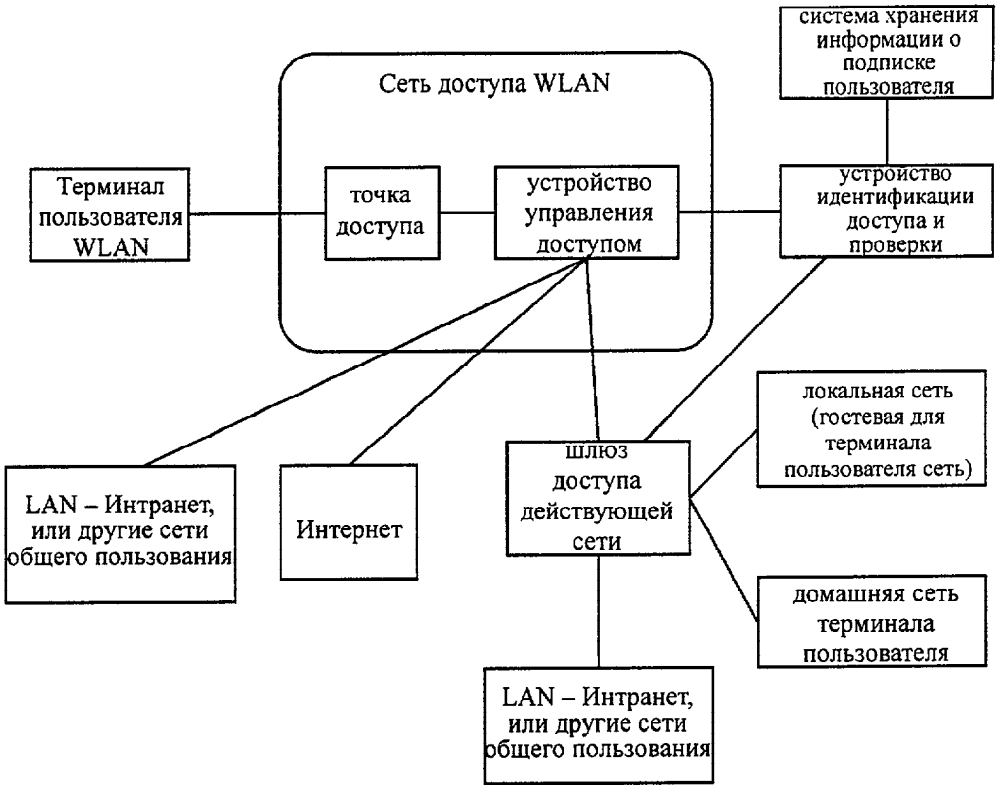
8. Способ по п.2, отличающийся тем, что названный соответствующий объект содержит сервер AAA, шлюз доступа WLAN, контроллер доступа AC (Access Controller), точку доступа AP (Access Point) или терминал пользователя WLAN.

9. Способ по п.8, содержащий дополнительные шаги: после установления правил доступа сеть одновременно передает терминалу пользователя WLAN информацию об успешности идентификации доступа и проверки полномочий текущего терминала пользователя WLAN и правила доступа, о которых необходимо проинформировать терминал пользователя WLAN.

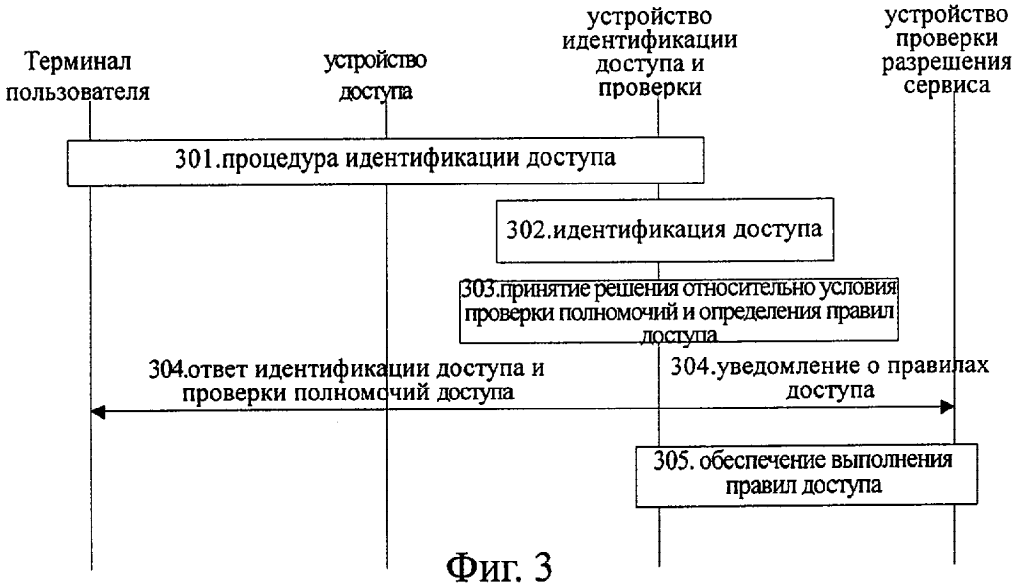
10. Способ по п.1, отличающийся тем, что действующая сеть WLAN является обеспечивающей межсетевое взаимодействие сетью 3GPP-WLAN или обеспечивающей межсетевое взаимодействие сетью 3GPP2-WLAN.

11. Способ по п.4, отличающийся тем, что указанная информация о подписке пользователя содержит список с указанием доступных пользователю сетевых сервисов.

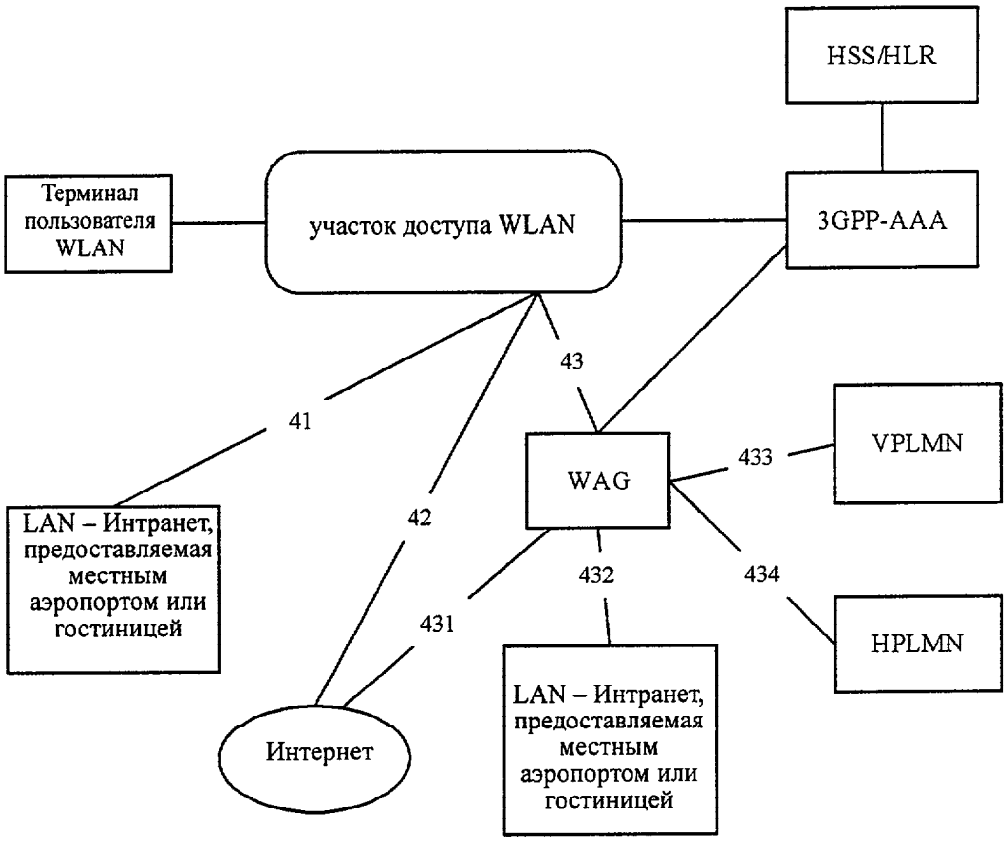
12. Способ по п.1, отличающийся тем, что указанный шаг выяснения действующей сетью WLAN, разрешен ли доступ данному терминалу пользователя WLAN в соответствии с условиями проверки полномочий, выполняют перед тем, как действующая сеть WLAN идентифицирует правомочность терминала пользователя WLAN.


система хранения информации о подписке пользователя
Сеть доступа WLAN
Терминал пользователя WLAN
точка доступа
устройство управления доступом
устройство идентификации доступа и проверки
локальная сеть (гостевая для терминала пользователя сеть)
шлюз доступа действующей сети
LAN – Интранет, или другие сети общего пользования
Интернет
домашняя сеть терминала пользователя
LAN – Интранет, или другие сети общего пользования

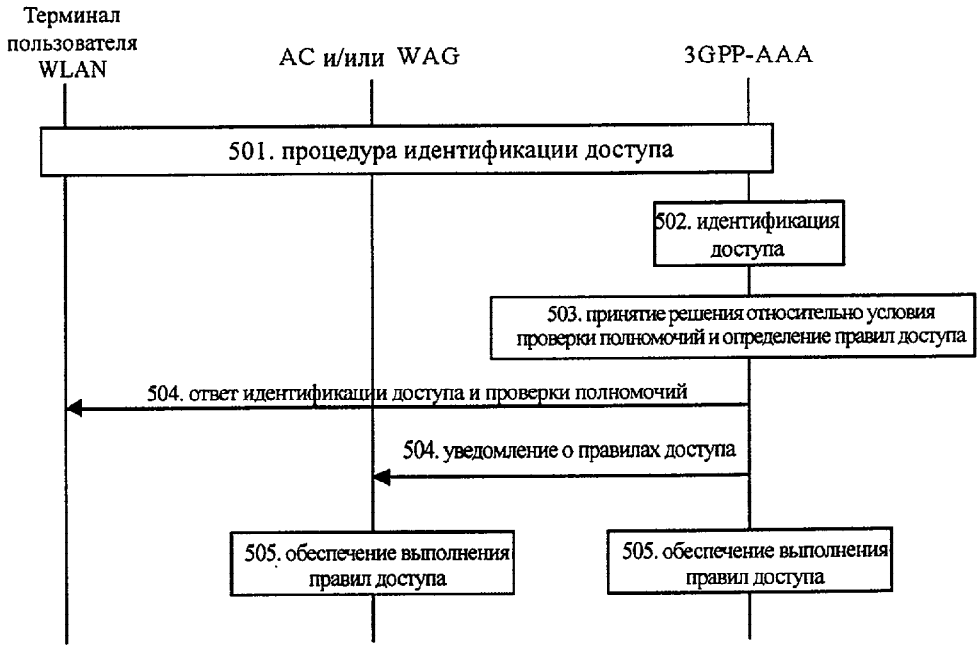
Фиг. 2


Терминал пользователя
устройство доступа
устройство идентификации доступа и проверки
устройство проверки разрешения сервиса
301.процедура идентификации доступа
302.идентификация доступа
303.принятие решения относительно условия проверки полномочий и определения правил доступа
304.ответ идентификации доступа и проверки полномочий доступа
304.уведомление о правилах доступа
305. обеспечение выполнения правил доступа

Фиг. 3


HSS/HLR
Терминал пользователя WLAN
участок доступа WLAN
3GPP-AAA
43
41
WAG
433
VPLMN
LAN – Интранет, предоставляемая местным аэропортом или гостиницей
42
432
434
431
HPLMN
Интернет
LAN – Интранет, предоставляемая местным аэропортом или гостиницей

Фиг. 4


Терминал пользователя WLAN
AC и/или WAG
3GPP-AAA
501. процедура идентификации доступа
502. идентификация доступа
503. принятие решения относительно условия проверки полномочий и определение правил доступа
504. ответ идентификации доступа и проверки полномочий
504. уведомление о правилах доступа
505. обеспечение выполнения правил доступа
505. обеспечение выполнения правил доступа

Фиг. 5