РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 564 251** (13) **C2**

(51) МПК
H04W 12/08 (2009.01)
H04W 76/02 (2009.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2013114721/08, 12.09.2011**

(24) Дата начала отсчета срока действия патента:
12.09.2011

Приоритет(ы):
(30) Конвенционный приоритет:
16.09.2010 US 61/383,475

(43) Дата публикации заявки: **27.10.2014** Бюл. № **30**

(45) Опубликовано: **27.09.2015** Бюл. № **27**

(56) Список документов, цитированных в отчете о поиске: **US 2007/0206527 A1, 06.09.2007. US 2010/0192212 A1, 29.07.2010. EP 1615381 A1, 11.01.2006. WO 03/096554 A2, 20.11.2003. RU 2009102069 A, 27.07.2010**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **16.04.2013**

(86) Заявка PCT:
FI 2011/050778 (12.09.2011)

(87) Публикация заявки PCT:
WO 2012/035203 (22.03.2012)

Адрес для переписки:
191036, Санкт-Петербург, а/я 24, "НЕВИНПАТ"

(72) Автор(ы):
БАЙКО Габор (US),
ПАТИЛ Басаварай (US)

(73) Патентообладатель(и):
Нокиа Корпорейшн (FI)

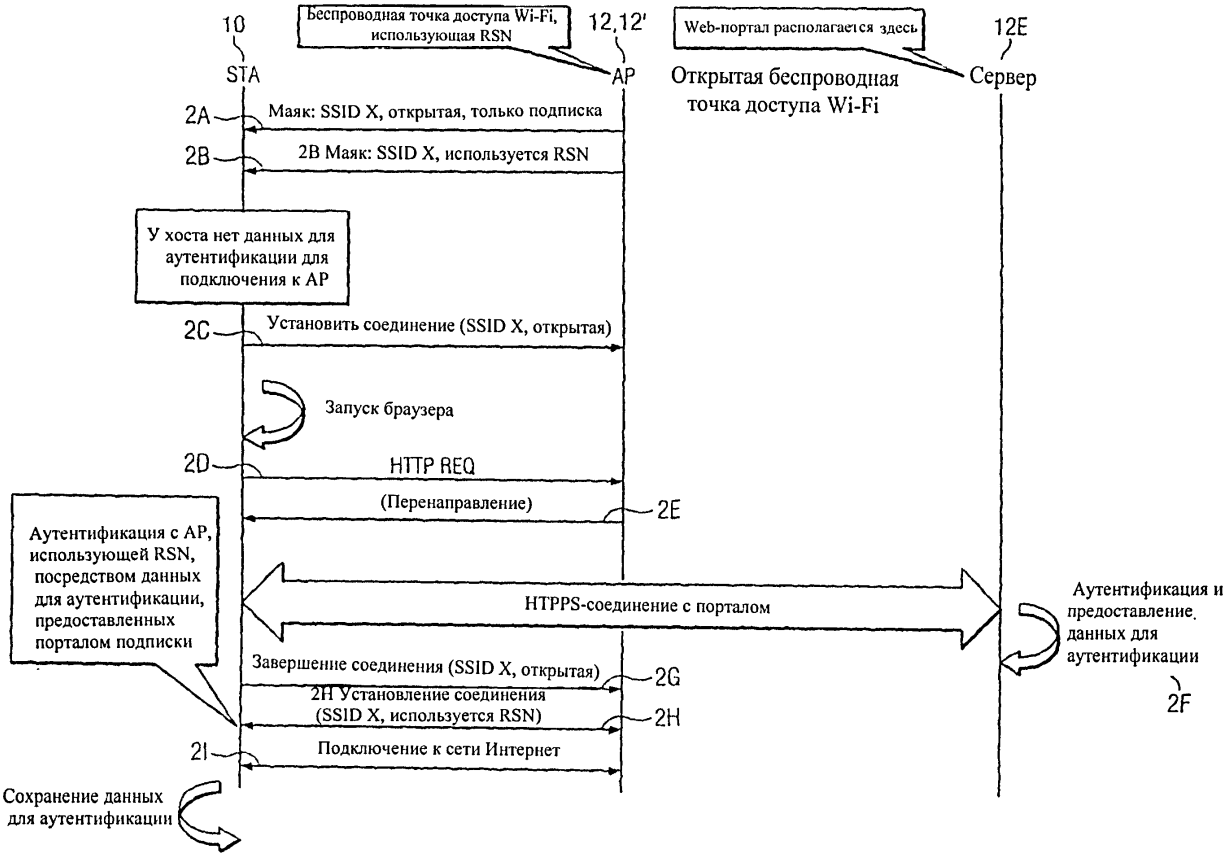
RU 2564251 C2

(54) ДИНАМИЧЕСКОЕ СОЗДАНИЕ АККАУНТА В ЗАЩИЩЕННОЙ СЕТИ С БЕСПРОВОДНОЙ ТОЧКОЙ ДОСТУПА

(57) Реферат:

Изобретение относится к области беспроводной связи. Технический результат - формирование соединения с защищенной точкой доступа к сети для получения доступа к сети Интернет. Устройство беспроводной связи содержит процессор, память, содержащую код компьютерной программы; при этом память с помощью процессора обеспечивает выполнение устройством, по меньшей мере, следующего: приема передаваемого маяка от защищенной точки доступа к сети, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID); формирования предварительного соединения с упомянутой защищенной точкой доступа к сети с использованием сообщаемого идентификатора набора услуг в ответ на определение того, что устройство не обладает данными для аутентификации, необходимыми для подключения к упомянутой защищенной точке доступа к сети; приема или создания, во время предварительного соединения, данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и формирования соединения с защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и сообщаемого идентификатора набора услуг и получения доступа к сети Интернет через

защищенную точку доступа к сети. 6 н. и 12 з.п. ф-лы, 5 ил.



Фиг. 2

RU 2564251 C2

RU 2564251 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 564 251** (13) **C2**

(51) Int. Cl.
H04W 12/08 (2009.01)
H04W 76/02 (2009.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2013114721/08, 12.09.2011**

(24) Effective date for property rights:
12.09.2011

Priority:
(30) Convention priority:
16.09.2010 US 61/383,475

(43) Application published: **27.10.2014** Bull. № **30**

(45) Date of publication: **27.09.2015** Bull. № **27**

(85) Commencement of national phase: **16.04.2013**

(86) PCT application:
FI 2011/050778 (12.09.2011)

(87) PCT publication:
WO 2012/035203 (22.03.2012)

Mail address:
191036, Sankt-Peterburg, a/ja 24, "NEVINPAT"

(72) Inventor(s):
BAJKO Gabor (US),
PATIL Basavaraj (US)

(73) Proprietor(s):
Nokia Corporation (FI)

RU 2564251 C2

(54) DYNAMIC CREATION OF ACCOUNT IN PROTECTED NETWORK WITH WIRELESS ACCESS POINT

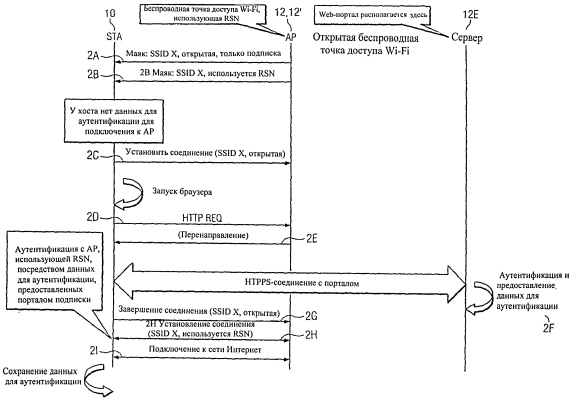
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: invention relates to wireless communication. A wireless communication device includes a processor, a memory containing a computer programme code; with that, the memory ensures that the device performs at least the following by means of the processor: reception of a transmitted mark from the protected access point to the network; with that, the above mark informs a service set identifier (SSID); formation of preliminary connection to the above protected access point to the network using the informed service set identifier in response to determination of the fact that the device has no data for authentication, which is required for connection to the above protected network access point; reception or creation, during preliminary connection, of data for authentication, which is required for connection to the protected network access point, and formation of connection to the protected network access point by using the received or created data for authentication and the informed service set identifier and by getting an access to the Internet through the protected network access point.

EFFECT: formation of connection to the protected network access point to obtain an access to the Internet Y.

18 cl, 5 dwg



Фиг. 2

RU 2564251 C2

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

По данной заявке в соответствии с §119(e) кодекса США (United States Code, U.S.C.) испрашивается приоритет согласно предварительной заявке №61/383,475 на выдачу патента США, поданной 16 сентября 2010 года. Данная приоритетная заявка полностью включена в настоящее описание посредством ссылки.

ОБЛАСТЬ ТЕХНИКИ

Примеры и варианты осуществления данного изобретения, не ограничивающие изобретение, относятся в общем к беспроводным системам связи, способам, устройствам и компьютерным программам и, в частности, к сетям Wi-Fi с беспроводной точкой доступа (hotspot, "горячая точка") и к возможности аутентификации у провайдеров услуг, которые управляют такими сетями.

ПРЕДПОСЫЛКИ СОЗДАНИЯ ИЗОБРЕТЕНИЯ

Данный раздел предназначен для описания предпосылок к созданию изобретения, изложенного в формуле изобретения. Описание данного раздела может включать концепции, которые могут быть реализованы, но не обязательно те, которые были уже рассмотрены или реализованы ранее. Таким образом, если не указано иное, описание, приведенное в данном разделе, не является известным уровнем техники для предлагаемого изобретения и не признается таковым вследствие включения в данный раздел.

Wi-Fi является товарным знаком Wi-Fi Alliance, связанным с различными продуктами, принадлежащими классу устройств беспроводной локальной сети (WLAN, wireless local area network), основанных на стандартах IEEE 802.11. Термин Wi-Fi часто используется как синоним технологии IEEE 802.11.

В настоящее время общественные сети Wi-Fi с беспроводной точкой доступа широко распространены во многих местах, таких как отели, рестораны, кафе, аэропорты, магазины и общественные или частные офисные помещения. Для получения доступа к сети Интернет посредством данных сетей с беспроводной точкой доступа от пользователя требуется либо подписка на получение услуг у оператора данной сети с беспроводной точкой доступа, либо любой другой вид соглашения о роуминге.

В настоящее время действует промышленный форум, называемый Hotspot 2.0, который направлен на упрощение процесса получения доступа к общественным сетям Wi-Fi с беспроводной точкой доступа.

В настоящее время существует два главных типа развертывания общественной сети Wi-Fi:

- открытые сети, к которым устройство может свободно подключиться, но не будет иметь доступа к сети Интернет до тех пор, пока не запустит браузер и не предоставит данные для аутентификации, и

- сети с возможностями RSN, которые для подключения к ним требуют предоставления данных для аутентификации. Технология надежно защищенной сети (RSN, Robust Security Network) является элементом алгоритмов аутентификации и шифрования IEEE 802.11i, используемых для осуществления связи между беспроводными точками доступа (WAP, wireless access point) и клиентами беспроводной сети.

Открытые общественные сети Wi-Fi с беспроводной точкой доступа, которые в настоящее время широко распространены, обычно управляются поставщиками Интернет-услуг (ISP, Internet Service Provider), сотовыми операторами или собственно самими организациями. Как правило, для данных сетей требуется оплачиваемая подписка, или они могут предоставляться как часть мобильного тарифного плана или в результате приобретения данного доступа на определенный период времени. Подобные

сети Wi-Fi с беспроводной точкой доступа, как правило, используют технологию, называемую порталом аутентификации (captive portal, "пленный портал"), посредством которой пользователи могут предоставлять свои данные для аутентификации для получения доступа к сети или оплаты такого доступа. Подход, основанный на портале аутентификации, требует от пользователя запуска Web-браузера, который затем перенаправляется на портал, управляемый оператором сети с беспроводной точкой доступа. Данный портал предоставляет информацию о различных тарифных планах, которые могут быть выбраны. Если у пользователя имеется подписка на услуги данного оператора, то портал предоставляет пользователю способ ввода назначенных ему данных для аутентификации и затем обеспечивает доступ к сети Интернет. До тех пор, пока аутентификация не будет выполнена, пользовательское устройство не будет иметь подключения к сети Интернет (за пределами портала аутентификации). Технология Wi-Fi беспроводной точки доступа позволяет пользовательскому устройству подключаться к точке доступа (AP, access point) Wi-Fi и назначает устройству IP-адрес. Однако подключение к сети Интернет за пределами портала аутентификации будет заблокировано до тех пор, пока пользователь не будет аутентифицирован с использованием данных для аутентификации, которые назначаются как часть подписки, или пока пользователь не приобретет доступ на определенный период времени. В настоящее время данный подход широко распространен и успешно функционирует для многих видов используемых приложений и услуг.

В сетях RSN с беспроводной точкой доступа нет возможности использовать подход перенаправления на портал аутентификации, так как сети RSN требуют от устройства выполнения аутентификации посредством 802.1x, а сама аутентификация осуществляется до того, как устройству будет назначен IP-адрес. Поэтому нет возможности перенаправления устройства на страницу портала. Если устройство не имеет необходимых данных для аутентификации и возможности аутентификации посредством протокола 802.1x, то устройство не может использовать сеть Wi-Fi с беспроводной точкой доступа. Протокол 802.1x является протоколом защиты информации, определенным IEEE для аутентификации посредством расширяемого протокола защиты информации (EAP, Extensible Authentication Protocol) (802.1X™, стандарт IEEE для локальных и городских сетей, управление доступом к сети на основе порта, 13 декабря 2004, включен посредством ссылки).

В общем, использование протокола 802.1x для аутентификации в сети Wi-Fi с беспроводной точкой доступа предоставляет более удобный пользовательский интерфейс, так как пользователю не нужно открывать браузер и предоставлять данные для аутентификации. Также не требуется ручного вмешательства пользователя для подключения к сети Интернет посредством такой сети с беспроводной точкой доступа.

Подход на основе протокола 802.1x хорошо работает, когда устройство или пользователь обладают действительными данными для аутентификации в сети Wi-Fi. Однако в случае большого числа операторов беспроводной точки доступа Wi-Fi, которые управляют такими сетями, пользователь может не иметь данных для аутентификации при роуминге или при нахождении в определенном месте. Даже в сетях с возможностями RSN, которые применяют механизмы аутентификации, основанные на протоколе 802.1x, пользователю может предоставляться возможность купить подписку. Операторы сетей Wi-Fi с беспроводной точкой доступа могут получать прибыль посредством гарантии предоставления услуг не только пользователям, имеющим подписки, но также и всем другим пользователям, желающим использовать сеть. Таким образом, оператор беспроводной точки доступа может иметь финансовую

заинтересованность в предложении пользователям возможности купить подписку для доступа к сети.

Рабочая группа Wi-Fi Alliance Hotspot 2.0 в настоящее время сконцентрирована на разработке решений, позволяющих незаметно для пользователя предоставлять доступ к сетям Wi-Fi HS2.0 посредством упрощения процедур аутентификации доступа. Предоставление возможностей онлайн-подписки к сетям RSN является одним из обсуждаемых вопросов.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

В первом аспекте примеров осуществления изобретения предлагается устройство, содержащее по меньшей мере один процессор и по меньшей мере одну память, содержащую код компьютерной программы. В данном аспекте изобретения по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего: приема по меньшей мере одного передаваемого маяка от по меньшей мере одной точки доступа к сети; в ответ на определение того, что устройство не обладает данными для аутентификации, необходимыми для подключения к защищенной точке доступа к сети упомянутой по меньшей мере одной точки доступа к сети, формирования предварительного соединения с упомянутой по меньшей мере одной точкой доступа к сети; во время упомянутого предварительного соединения, приема или создания данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и формирования соединения с защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и получения доступа к сети Интернет через защищенную точку доступа к сети.

Во втором аспекте примеров осуществления изобретения предлагается способ, включающий: прием в пользовательском устройстве по меньшей мере одного передаваемого маяка от по меньшей мере одной точки доступа к сети; формирование предварительного соединения с упомянутой по меньшей мере одной точкой доступа к сети в ответ на определение того, что пользовательское устройство не обладает данными для аутентификации, необходимыми для подключения к защищенной точке доступа к сети упомянутой по меньшей мере одной точки доступа к сети; прием или создание пользовательским устройством, во время упомянутого предварительного соединения, данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и формирование соединения между пользовательским устройством и защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и получение доступа к сети Интернет через защищенную точку доступа к сети.

В третьем аспекте примеров изобретения предлагается машиночитаемый носитель данных, содержащий инструкции компьютерной программы. В данном аспекте исполнение инструкций по меньшей мере одним процессором данных приводит к выполнению операций, включающих: прием в пользовательском устройстве по меньшей мере одного передаваемого маяка от по меньшей мере одной точки доступа к сети; формирование предварительного соединения с упомянутой по меньшей мере одной точкой доступа к сети в ответ на определение того, что пользовательское устройство не обладает данными для аутентификации, необходимыми для подключения к защищенной точке доступа к сети упомянутой по меньшей мере одной точки доступа к сети; прием или создание пользовательским устройством, во время упомянутого предварительного соединения, данных для аутентификации, необходимых для соединения

с защищенной точкой доступа к сети, и формирование соединения между пользовательским устройством и защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и получение доступа к сети Интернет через защищенную точку доступа к сети.

В четвертом аспекте примеров изобретения предлагается устройство, содержащее по меньшей мере один процессор и по меньшей мере одну память, содержащую код компьютерной программы. В данном аспекте изобретения по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего: передачи по меньшей мере одного маяка, включающего идентификатор набора услуг, и предоставления услуги подписки для защищенной точки доступа к сети, работающей с тем же идентификатором набора услуг, что и устройство.

В пятом аспекте примеров осуществления изобретения предлагается способ, включающий: передачу точкой доступа к сети, не использующей технологию надежно защищенной сети RSN, по меньшей мере одного маяка, включающего идентификатор набора услуг, и обеспечение точкой доступа к сети, не использующей технологию надежно защищенной сети RSN, услуги подписки для защищенной точки доступа к сети, работающей с тем же идентификатором набора услуг, что и точка доступа к сети, не использующая технологию надежно защищенной сети RSN.

В шестом аспекте примеров осуществления изобретения предлагается машиночитаемый носитель данных, содержащий инструкции компьютерной программы. В данном аспекте изобретения исполнение инструкций по меньшей мере одним процессором данных приводит к выполнению операций, включающих: передачу точкой доступа к сети, не использующей технологию надежно защищенной сети RSN, по меньшей мере одного маяка, включающего идентификатор набора услуг, и предоставление точкой доступа к сети, не использующей технологию надежно защищенной сети RSN, услуги подписки для защищенной точки доступа к сети, работающей с тем же идентификатором набора услуг, что и точка доступа к сети, не использующая технологию надежно защищенной сети RSN.

В седьмом аспекте примеров осуществления изобретения предлагается устройство, включающее по меньшей мере один процессор и по меньшей мере одну память, содержащую код компьютерной программы. В данном аспекте изобретения по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего: передачи по меньшей мере одного маяка; предоставления пользовательскому устройству идентификатора доступа к сети (NAI, network access identifier) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с устройством; приема от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки, и предоставления пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации.

В восьмом аспекте примеров изобретения предлагается способ, включающий: передачу по меньшей мере одного маяка; предоставление пользовательскому устройству идентификатора доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с устройством; прием от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки, и предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации.

В девятом аспекте примеров осуществления изобретения предлагается машиночитаемый носитель данных, содержащий инструкции компьютерной программы. В данном аспекте изобретения исполнение инструкций по меньшей мере одним процессором данных приводит к выполнению операций, включающих: передачу по меньшей мере одного маяка; предоставление пользовательскому устройству идентификатора доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с устройством; прием от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки, и предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Фиг.1 показывает упрощенную структурную схему различных электронных устройств, которые подходят для практического использования примеров осуществления данного изобретения.

Фиг.2 является схемой взаимодействия между станцией, точкой доступа и сервером Web-портала в соответствии с первым вариантом осуществления данного изобретения.

Фиг.3 является схемой взаимодействия между станцией, точкой доступа и сервером Web-портала в соответствии со вторым вариантом осуществления данного изобретения.

Фиг.4 является логической блок-схемой, которая со стороны пользовательского устройства иллюстрирует способ и результат исполнения инструкций компьютерной программы, хранимых в машиночитаемой памяти, в соответствии с примерами осуществления данного изобретения.

Фиг.5-1 и 5-2 являются логическими блок-схемами, которые со стороны открытой или защищенной точек доступа к сети, соответственно, иллюстрируют способ и результат исполнения инструкций компьютерной программы, хранимых в машиночитаемой памяти, в соответствии с примерами осуществления данного изобретения.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Из предшествующего описания ясно, что имеется проблема, состоящая в том, что нет способа, с помощью которого пользователь мог бы купить подписку в сети, использующей технологию RSN. Упрощенно говоря, пользователь не может получить доступ, поскольку не обладает соответствующими данными для аутентификации в сети, при этом пользователь не может создать или купить соответствующие данные для аутентификации в сети, потому что не имеет доступа к сети. В настоящее время на практике осуществляют передачу пароля на бумаге участникам события, позволяя им получать доступ к сети с помощью данного пароля (каждый имеет один и тот же пароль, называемый в WFA персональным WPA) или формируют для каждого пользователя отдельный маркер, называемый в WFA корпоративным WPA, используя традиционные способы распространения (например, посредством e-mail). Ни один из этих способов не позволяет создавать аккаунт "на лету", так как они требуют от потенциального пользователя либо регистрироваться на событие, либо лично обращаться к администратору и т.д.

Примеры осуществления данного изобретения направлены на решение этих и других проблем посредством предоставления перемещающимся пользователям способа обеспечения возможностей онлайн-подписки в сетях с беспроводной точкой доступа, использующей технологию RSN.

Примеры осуществления данного изобретения относятся по меньшей мере частично к сетям Wi-Fi HS2.0 и предлагают возможность динамического создания подписки у оператора сети с беспроводной точкой доступа.

Перед дальнейшим подробным описанием примеров осуществления данного изобретения обратимся к фиг.1, показывающей упрощенную структурную схему различных электронных устройств, которые подходят для использования на практике примеров осуществления данного изобретения. На фиг.1 сеть Wi-Fi сконфигурирована для осуществления связи посредством беспроводной линии 11 связи с устройством, таким как устройство мобильной связи, которое может называться здесь станцией (STA, station) или пользовательским устройством (UD, user device) 10, через узел или точку доступа к сети. На фиг.1 показаны две точки доступа к сети (NWAP, network access point), одна из которых представляет сеть 12, использующую технологию RSN, а другая - открытую сеть 12' (сеть, не использующую технологию RSN). По меньшей мере точка NWAP (беспроводная точка доступа) 12, использующая технологию RSN, предоставляет доступ к одной или более сетям передачи данных (например, к сети Интернет). Устройство UD 10 включает контроллер, такой как по меньшей мере один компьютер или процессор 10A данных (DP, data processor), по меньшей мере один машиночитаемый носитель данных, реализованный как память (MEM, memory) 10B, которая хранит программу (PROG, program) 10C из компьютерных инструкций, и по меньшей мере один подходящий радиочастотный (RF, radio frequency) приемопередатчик 10D (пара из передатчика и приемника) для осуществления двусторонней беспроводной связи с узлами или точками 12, 12' доступа к сети посредством одной или более антенн. Точка NWAP 12 также включает контроллер, такой как по меньшей мере один компьютер или процессор 12A данных (DP), по меньшей мере один машиночитаемый носитель данных, реализованный как память (MEM) 12B, которая хранит программу (PROG) 12C из компьютерных инструкций, и по меньшей мере один подходящий радиочастотный приемопередатчик 12D (пара из передатчика и приемника) для осуществления связи с устройством UD 10 посредством одной или более антенн. Можно предположить, что точка NWAP 12' сконструирована аналогично и включает контроллер, такой как по меньшей мере один компьютер или процессор 12A' данных (DP), по меньшей мере один машиночитаемый носитель данных, реализованный как память (MEM) 12B', которая хранит программу (PROG) 12C из компьютерных инструкций, и по меньшей мере один подходящий радиочастотный приемопередатчик 12D' (пара из передатчика и приемника) для осуществления связи с устройством UD 10 посредством одной или более антенн.

Необходимо отметить, что хотя точка NWAP 12, использующая технологию RSN, и открытая (не использующая технологию RSN) точка NWAP 12' показаны как две отдельные точки доступа, на практике их функциональность может быть объединена внутри одной аппаратной/программной системы точки доступа.

Для описания примеров осуществления данного изобретения может предполагаться, что устройство UD 10 также включает браузер 10E, хранилище 10F данных для аутентификации и менеджер 10G соединений (CM, connection manager). На практике браузер 10E и менеджер 10G соединений могут формировать часть программного обеспечения 10C, а хранилище 10F данных для аутентификации может быть реализовано в виде одной или более областей хранения данных в памяти 10B, хотя на фиг.1 данные элементы выделены в отдельные блоки. Как точка NWAP 12, использующая технологию RSN, так и открытая (не использующая технологию RSN) точка NWAP 12' могут включать страницу 12E, 12E' портала или иным образом иметь доступ к серверу, на котором расположена страница Web-портала.

Необходимо отметить, что устройство UD 10 может включать специализированную интегральную схему или чип или модуль WLAN, реализующие всю функциональность или по меньшей мере часть функциональности, необходимую для соединения WLAN и

соответствующих операций.

Предполагается, что по меньшей мере одна из программ PROG 10C и 12C включает инструкции программы, которые при их исполнении соответствующим процессором DP позволяют устройству работать в соответствии с примерами осуществления данного изобретения, как будет более подробно описано далее. То есть примеры осуществления данного изобретения могут быть реализованы по меньшей мере частично посредством компьютерного программного обеспечения, исполняемого процессором DP 10A устройства UD10 и/или процессором DP 12A точки NWAP 12, или посредством аппаратного обеспечения или посредством комбинации программного обеспечения и аппаратного обеспечения (и встроенного программного обеспечения).

В общем, различные варианты осуществления устройства UD 10 могут включать, не ограничиваясь этим, карманные компьютеры (PDA, personal digital assistant) с возможностями беспроводной вязи, портативные компьютеры с возможностями беспроводной связи, устройства захвата изображений, такие как цифровые камеры, с возможностями беспроводной связи, игровые устройства с возможностями беспроводной связи, устройства для хранения и воспроизведения музыки с возможностями беспроводной связи, Интернет-устройства, обеспечивающие беспроводной доступ к сети Интернет и просмотр Web-страниц, сотовые телефоны с возможностями связи Wi-Fi, а также портативные устройства или терминалы, реализующие комбинации данных функций.

Блоки машиночитаемой памяти MEM 10B и 12B могут быть любого типа, подходящего для конкретного локального технического окружения, и могут быть реализованы посредством использования любых подходящих технологий хранения данных, таких как запоминающие устройства на основе полупроводников, оперативная память, постоянная память, программируемая постоянная память, флэш-память, магнитные запоминающие устройства и системы, оптические запоминающие устройства и системы, встроенная память и съемная память. Процессоры DP 10A и 12A могут быть любого типа, подходящего для конкретного локального технического окружения, и могут включать, не ограничиваясь этим, один или более универсальных компьютеров, специализированных компьютеров, микропроцессоров, устройств цифровой обработки сигналов (DSP, digital signal processor) и процессоров, реализованных на основе многоядерной процессорной архитектуры.

В соответствии с примерами осуществления данного изобретения предлагаются решения для онлайн-подписки устройства UD10, а также упрощенный (незаметный для пользователя) механизм формирования данных для аутентификации.

В первом варианте осуществления изобретения (см. также фиг.2) для случая сети 12, использующей технологию RSN, также представлена соответствующая сеть 12', не использующая технологию RSN (то есть открытая сеть). Открытая сеть 12' обеспечивает по меньшей мере возможность онлайн-подписки для устройства UD 10 и, как правило, не предоставляет доступ к сети Интернет или любой другой услуге.

Процесс происходит следующим образом. Открытая сеть 12' указывает в своих возможностях (например, в новой заданной возможности или возможности, зависящей от производителя) на то, что она предоставляет только услугу онлайн-подписки для создания данных для аутентификации, используемых в RSN-сети 12 (с тем же самым идентификатором SSID). Как известно, идентификатор набора услуг, или SSID, является именем, которое однозначно определяет конкретную беспроводную локальную сеть 802.11. Клиентское устройство принимает широковещательные сообщения от всех точек доступа в диапазоне сообщаемых идентификаторов SSID. Затем клиентское

устройство может либо вручную, либо автоматически, в зависимости от конфигурации, выбрать сеть для подключения. Идентификатор SSID может быть длиной до 32 символов.

Когда устройство UD 10 выполняет процедуру обнаружения и выбора сети (NDS, Network Discovery and Selection) и находит как открытую сеть 12', так и сеть 12, использующую технологию RSN, с одним и тем же идентификатором SSID, то оно сначала проверяет у себя наличие действительных данных для аутентификации в сети 12, использующей технологию RSN. Если устройство UD 10 определяет, что оно не имеет нужных RSN-данных для аутентификации, то оно обнаруживает возможности открытой сети 12' с тем же самым идентификатором SSID. Если возможности сети 12' указывают на то, что она поддерживает только процедуру подписки, то устройство UD 10 устанавливает связь с открытой сетью 12', запускает браузер 10E и формирует некоторый (например, холостой) http-трафик (например, посредством http-запроса на некоторый IP-адрес, такой как http://dummyhomepage.net). Открытая сеть NWAP 12' перенаправляет данный http-трафик на страницу 12E портала (и традиционным способом предлагает устройству UD 10 свой сертификат). После того, как терминал аутентифицируется на странице портала посредством использования предоставленных данных для аутентификации, для устройства UD 10 на странице 12E портала предлагается на выбор один из тарифных планов и способ оплаты (например, посредством кредитной карты). Также устройству UD 10 может быть предложена возможность создания пользовательских данных для аутентификации, или же данные для аутентификации будут созданы страницей 12E портала (создание данных для аутентификации будет описано ниже).

Когда браузер 10E принимает данные для аутентификации, он может временно сохранить их в хранилище 10F данных для аутентификации и инициировать сообщение об отключении (например, посредством использования программных интерфейсов приложения (API, application program interface) WLAN-чипа, доступных через интерфейс командной строки). Затем устройство UD 10 инициирует сообщение о подключении к сети 12, использующей технологию RSN, посредством указания идентификатора SSID, для которого только что были созданы данные для аутентификации (например, через интерфейс командной строки WLAN-чипа). Альтернативно, если идентификатор SSID не указан, устройство UD 10 может начать новую процедуру NDS, обнаружить идентификатор SSID, для которого только что были созданы данные для аутентификации, и подключиться к данной сети. Как только будут запрошены данные для аутентификации, менеджер 10G соединений предоставит в устройство UD 10 недавно созданные данные для аутентификации. После успешной аутентификации менеджер 10G соединений будет считать данные для аутентификации проверенными и соответственно обновит их статус в хранилище 10F данных для аутентификации.

Если данные для аутентификации не являются рабочими или действительными, или истек срок их действия, аутентификация не будет произведена. Вместо передачи пользователю сообщения об ошибке, устройство UD 10 может автоматически установить соединение с открытой сетью NWAP 12' с тем же самым идентификатором SSID, сформировать http-трафик, перенаправляемый на страницу 12E' портала, которая в свою очередь отобразит пользователю, какие шаги он должен предпринять далее (например, отобразит телефонный номер службы технической поддержки), когда определит, что устройство UD 10 (с уникальным MAC-адресом) намеревается создать данные для аутентификации, но по какой-то причине не может этого сделать.

Теперь обратимся к примеру схемы взаимодействия на фиг.2, где на шаге 2A

принимают от открытой сети NWAP 12' маяк: SSID X, Open, Online Sign-up only (SSID X, открытая, только онлайн-подписка). На шаге 2B принимают маяк: SSID X, RSN-enabled (SSID X, используется RSN). Необходимо отметить, что в некоторых случаях порядок приема маяков на шагах 2A и 2B может быть обратным. Так как на шаге 2A указывают только на онлайн-подписку (что означает отсутствие какого-либо доступа к сети Интернет за пределами страниц/страницы подписки), устройство UD 10 продолжает поиск сети, которая предоставляет доступ к сети Интернет. В ответ на определение того, что хост (устройство UD 10) не имеет данных для аутентификации для подключения к сети посредством точки AP, использующей технологию RSN, в точку NWAP 12' для создания аккаунта передают сообщение установления связи Associate (SSID X, Open) (SSID X, открытая). Устройство UD 10 запускает браузер 10E и на шаге 2D передает в точку NWAP 12' запрос HTTP Req (являющийся упомянутым выше холостым http-трафиком). На шаге 2E устройство UD 10 в ответ принимает HTTP-Resp (Перенаправление), а на шаге 2F устанавливают HTTPS-соединение со страницей 12E портала, где устройство UD 10 аутентифицируется в сети, и ему предоставляют необходимые данные для аутентификации, как только оно предоставит информацию об оплате. На шаге 2F устройство UD 10 передает в точку NWAP 12' сообщение об отключении Disassociate (SSID X, Open) (SSID X, открытая). На шаге 2H устройство UD10 передает сообщение установления связи Associate (SSID X, RSN-enabled) (SSID X, используется RSN) и аутентифицируется с помощью точки NWAP 12, использующей технологию RSN, посредством использования данных для аутентификации, предоставленных сервером 12E подписки Web-портала во время HTTPS-соединения на шаге 2F. Необходимо отметить, что идентификатор SSID X, используемый на шагах 2G и 2H, является тем же идентификатором SSID, что и принятый на шагах 2A и 2B. На шаге 2I устройство UD 10 получает доступ к сети Интернет за пределами страниц (страницы) подписки посредством точки NWAP 12, использующей технологию RSN, а данные для аутентификации, принятые во время HTTPS-соединения на шаге 2F, могут быть сохранены в хранилище 10F данных для аутентификации для дальнейшего использования.

Во втором варианте осуществления изобретения (см. также фиг.3), когда имеется сеть 12, использующая технологию RSN, для которой у устройства UD 10 нет данных для аутентификации, устройство UD 10 сначала проверяет возможности сети 12, использующей технологию RSN. Если поддерживается возможность онлайн-подписки (как в настоящее время определено в стандарте 802.11u в таблице 7-43bo), в соответствии с аспектос примера данного изобретения сеть 12, использующая технологию RSN, предоставляет во время нахождения в состоянии предварительного соединения специальный идентификатор доступа к сети (NAI, network access identifier) (например, см. RFC4282) для подписки. Такой идентификатор NAI может быть определен так, как в документе 802.11u в таблице 7-43bn, или как элемент специфичного для производителя списка протокола очереди доступа к сети (ANQP, access network query protocol), так что, когда сеть 12, использующая технологию RSN, поддерживает возможность онлайн-подписки, должен предоставляться идентификатор NAI для подписки. Тогда устройство UD 10 во время нахождения в состоянии предварительного соединения может использовать, например, протокол ANQP (определенный в 802.11u) совместно, например, с только что определенным информационным именем (Info-name) для запроса от сети 12, использующей технологию RSN, для идентификатора NAI для подписки. Когда идентификатор NAI для подписки получен, устройство UD 10 использует данный идентификатор NAI в качестве идентификации протокола расширенной аутентификации

(EAP, Extensible Authentication Protocol) во время аутентификации 802.1x. Когда сеть 12, использующая технологию RSN, принимает сообщение идентификации EAP-ответа от устройства UD 10 с идентификатором NAI для подписки в качестве идентификации пользователя, сеть 12, использующая RSN, будет знать, что данный пользователь хочет осуществить подписку. В данном случае аутентификация осуществляется только на стороне сервера, и сеть 12, использующая технологию RSN, не должна запрашивать пользовательские данные для аутентификации (это и является целью определения идентификатора NAI для подписки, так как пользователь не обладает данными для аутентификации). Как только устройство UD 10 успешно аутентифицируется в сети 12, использующей технологию RSN, и соединение установится (со сформированными ключами сессии 802.1x), устройство UD 10 запустит браузер 10E и сформирует некоторый (например, холостой) http-трафик. Сеть 12, использующая технологию RSN, перенаправит данный http-трафик на страницу 12E портала. Необходимо отметить, что даже несмотря на то, что включена защита на уровне соединения, данный вариант осуществления изобретения предполагает, что страница 12 портала предоставляет устройству UD 10 сертификат, и устанавливается https-соединение (защищенное http-соединение) для предотвращения в сети 12, использующей технологию RSN, перехвата данных для аутентификации, формируемых пользователем или предоставляемых страницей портала. Затем пользователю предлагаются тарифные планы, при этом пользователя запрашивают выбрать один из них, а также ввести информацию для оплаты. Пользователю также может быть предложена возможность создать пользовательские данные для аутентификации, или же страница 12 портала создаст данные для аутентификации (создание данных для аутентификации описано ниже). Когда браузер 10E принимает данные для аутентификации, он может временно сохранить их в хранилище 10F данных для аутентификации, инициировать сообщение завершения соединения и инициировать сообщение соединения с той же самой сетью 12, использующей технологию RSN, посредством указания идентификатора SSID, для которого только что были созданы данные для аутентификации. Когда сеть 12, использующая технологию RSN, отправит запрос идентификации EAP, устройство UD 10 предоставит только что созданные данные идентификации (часть из только что созданного набора данных для аутентификации), а не идентификатор NAI для подписки.

Теперь обратимся к примеру схемы взаимодействия на фиг.3, где на шаге 3A устройство UD 10 принимает от сети NWAP 12, использующей технологию RSN, маяк: SSID X, RSN-enabled (SSID X, используется RSN), с указанием поддержки онлайн-подписки. В случае, когда определяют, что хост (устройство UD 10) не обладает необходимыми данными для аутентификации, принимают решение использовать идентификатор NAI для подписки. На шаге 3B в состоянии предварительного соединения устройство UD 10 передает запрос на получение идентификатора NAI для подписки, а на шаге 3C принимает идентификатор NAI для подписки (в состоянии предварительного соединения) от точки NWAP 12, использующей технологию RSN. На шаге 3D устройство UD 10 и точка NWAP 12, использующая технологию RSN, устанавливают соединение (используя аутентификацию только на стороне сервера). Затем устройство UD 10 запускает браузер 10E. На шаге 3E передают запрос HTTP Req (например, холостой http-трафик), и на шаге 3F точка NWAP 12 отправляет ответ HTTP Resp (Перенаправление). На шаге 3F устройство UD 10 принимает в ответ HTTP Resp (Перенаправление), и на шаге 3G устанавливают HTTPS-соединение со страницей 12E портала, на которой устройство UD 10 аутентифицируется и формирует, или же ему предоставляют, необходимые данные для аутентификации. На шаге 3H устройство UD

10 передает сообщение завершения соединения Disassociate (SSID X, RSN-Enabled, SU-NAI) (SSID X, используется RSN, SU-NAI), на шаге 31 устройство UD 10 передает сообщение соединения Associate (SSID X, RSN-enabled) (SSID X, используется RSN) и аутентифицируется с помощью точки NWAP 12, использующей технологию RSN, с использованием данных для аутентификации, полученных от сервера 12E подписки Web-портала во время HTTPS-соединения 3G. На шаге 3J устройство UD 10 получает доступ к сети Интернет посредством точки NWAP 12, использующей технологию RSN, а данные для аутентификации, полученные во время HTTPS-соединения на шаге 3G, могут быть сохранены в хранилище 10F данных для аутентификации для дальнейшего использования.

Далее будет описан процесс создания данных для аутентификации. Существует два типа данных для аутентификации, которые могут быть созданы в онлайн-режиме для перемещающихся пользователей: имя пользователя / пароль и сертификат. Оба из этих типов могут быть как постоянными, так и ограниченными во времени (например, ваучер). Если они являются постоянными, то наиболее вероятно, что имеется некоторая сумма кредита, связанная с этими данными для аутентификации. Когда сумма кредита истекает, пользователю необходимо приобрести дополнительный кредит для использования данных для аутентификации.

Клиентский сертификат формируется программным обеспечением, а пара имя пользователя / пароль может быть также сформирована и самим пользователем. Однако нет причины заставлять пользователя вводить имя пользователя / пароль. Программное обеспечение может также формировать случайные строки в качестве имени пользователя / пароля, так как в Hotspot 2.0 одним из требований является необходимость того, чтобы устройство UD 10 не запрашивало пользователя вводить данные для аутентификации. То есть эти данные для аутентификации предназначены не для пользователя, а для устройства.

Поэтому в соответствии с примерами осуществления изобретения, когда пользователя перенаправляют на страницу (12, 12') портала, страница портала должна иметь опцию для выбора пользователем либо ручного, либо автоматического формирования данных для аутентификации, при этом автоматическое формирование данных для аутентификации установлено по умолчанию (независимо от того, требуется ли сети в качестве данных для аутентификации имя пользователя / пароль или сертификат). При автоматическом формировании данных для аутентификации страница 12, 12' формирует требуемые данные для аутентификации (либо имя пользователя / пароль, либо клиентский сертификат) и предоставляет устройству UD 10 сформированные данные для аутентификации. Как только устройство UD 10 примет данные для аутентификации, оно сохраняет их в хранилище 12F данных для аутентификации и использует их при необходимости. Так как устройство UD 10 автоматически предоставляет точке NWAP 12, 12' данные для аутентификации, пользователю нет необходимости знать данные для аутентификации. Таким образом, данные для аутентификации не обязательно должны быть представлены в читаемой человеком форме. Кроме того, пользователю не нужно знать тип принимаемых данных для аутентификации (являются ли они парой имя пользователя / пароль или клиентским сертификатом).

На стороне устройства UD 10 реализация примеров осуществления изобретения может выступать частью клиента или процесса менеджера 10G соединений. Когда устройство UD 10 обнаруживает доступность сети Wi-Fi с беспроводной точкой доступа HS2.0, использующей технологию RSN, и определяет, что оно не обладает данными для аутентификации для подключения к данной сети, оно может предоставить

возможности логических схем и пользовательского интерфейса, которые позволили бы пользователю купить доступ к данной сети.

При использовании примеров осуществления изобретения достигается множество преимуществ и технических результатов. Например, изобретение обеспечивает способ, посредством которого конечный пользователь / покупатель может купить доступ к сети Wi-Fi с беспроводной точкой доступа HS2.0, использующей технологию RSN. Кроме того, например, использование примеров осуществления изобретения удовлетворит интересы оператора беспроводной точки доступа Wi-Fi, обеспечивая возможность приобретения подписки любым, кто находится в радиусе действия данной сети. Кроме того, примеры осуществления изобретения обеспечивают средства защиты, посредством которых происходит обмен информацией о платежах и данных для аутентификации. Кроме того, примеры осуществления изобретения могут быть реализованы посредством использования уже существующих протоколов. Эти протоколы реализованы в большинстве устройств UD 10, поэтому не требуется каких-либо усовершенствований протоколов и/или программного обеспечения менеджера 10G соединений.

Из представленного выше описания должно быть понятно, что примеры осуществления данного изобретения обеспечивают способ, устройство и компьютерную (компьютерные) программу (программы) для обеспечения возможности установления соединения между различными типами устройств, станций и терминалов, использующих локальную беспроводную связь различного типа, например, совместимых с системами связи типа IEEE 802.

Фиг.4 является логической блок-схемой, которая со стороны устройства UD 10 иллюстрирует способ и результат исполнения инструкций компьютерной программы в соответствии с примерами осуществления данного изобретения. В соответствии с этими примерами осуществления изобретения способ включает на шаге 4A прием в пользовательском устройстве по меньшей мере одного маяка от по меньшей мере одной точки доступа к сети. В одном варианте осуществления изобретения от незащищенной точки доступа к сети принимают первый маяк, указывающий только на RSN-подписку, а также второй маяк от защищенной точки доступа к сети, при этом первый и второй маяки имеют один и тот же идентификатор набора услуг. В другом варианте осуществления изобретения принимают только один маяк от защищенной точки доступа к сети. В ответ на определение на шаге 4A того, что пользовательское устройство не имеет данных для аутентификации, необходимых для подключения к защищенной точке доступа к сети, на шаге 4B осуществляют предварительное соединение с защищенной или незащищенной точками доступа к сети в соответствии с различными вариантами осуществления изобретения, указанными выше. Например, в одном из этих вариантов осуществления изобретения перед выполнением предварительного соединения с точкой доступа RSN на шаге 4B устройство UD 10 вначале получает идентификатор NAI для подписки от точки доступа RSN, находясь в состоянии предварительного соединения с ней. На шаге 4C передают http-трафик в точку доступа, с которой было установлено соединение на шаге 4B. Как было отмечено ранее, данный http-трафик является холостым трафиком или обычным (реальным) трафиком. На шаге 4D происходит перенаправление и формирование защищенного http-соединения со страницей портала. На шаге 4E пользовательское устройство аутентифицируется на странице портала и принимает от страницы портала данные для аутентификации, необходимые для осуществления связи с защищенной точкой доступа к сети. Альтернативно, пользовательское устройство может само создавать данные для аутентификации, что также указано на шаге 4E. На

шаге 4F завершают предварительное соединение, и на шаге 4G формируют соединение с защищенной точкой доступа к сети посредством использования принятых данных для аутентификации и получают доступ к сети Интернет через защищенную точку доступа к сети.

В способе, показанном на фиг.4, на шаге 4A принимают первый маяк от незащищенной точки доступа, которая является точкой доступа к сети, не использующей технологию RSN, и которая оповещает только о возможности подписки, при этом защищенная точка доступа к сети является другой точкой доступа, использующей технологию RSN. В другом варианте осуществления изобретения защищенная и незащищенная точки доступа к сети выполнены в одном физическом узле, который функционально работает в защищенной сети и незащищенной сети, соответственно.

В способе, указанном в предыдущем абзаце, пользовательское устройство на шаге 4B формирует предварительное соединение с точкой доступа к сети, использующей технологию RSN, передает http-трафик (например, холостой http-трафик) в точку доступа к сети, не использующую технологию RSN, прекращает предварительное соединение с точкой доступа к сети, не использующей технологию RSN, и формирует соединение с точкой доступа, использующей технологию RSN, посредством использования принятых данных для аутентификации.

В способе, показанном на фиг.4, принимают маяк от точки доступа к сети, использующей технологию надежно защищенной сети (RSN), при этом маяк указывает на то, что точка доступа к сети, использующая технологию RSN, поддерживает возможности подписки для пользовательского устройства, причем способ также включает передачу, в состоянии предварительного соединения, запроса в точку доступа к сети, использующей технологию RSN, для идентификатора доступа к сети (NAI) для подписки, прием запрашиваемого идентификатора NAI для подписки и установление соединения с точкой доступа, использующей технологию RSN, посредством использования аутентификации только на стороне сервера.

В способе, указанном в предыдущем абзаце, пользовательское устройство передает http-трафик (например, холостой http-трафик) в точку доступа к сети, использующую технологию RSN, завершает на шаге 4F предварительное соединение, которое использовало идентификатор NAI для подписки для соединения с точкой доступа, использующей технологию RSN, и формирует соединение с точкой доступа к сети, использующей технологию RSN, с помощью принятых данных для аутентификации.

В способе, показанном на фиг.4 или описанном в любом из предыдущих абзацев, во время соединения со страницей портала пользователь может выбирать ручное или автоматическое формирование данных для аутентификации.

В способе, указанном в предыдущем абзаце, при автоматическом формировании данных для аутентификации страница 12 портала формирует данные для аутентификации либо как пару имя пользователя / пароль, либо как клиентский сертификат и предоставляет сформированные данные для аутентификации пользовательскому устройству, которое сохраняет их и автоматически предоставляет данные для аутентификации точке доступа к сети, использующей технологию RSN, без необходимости знания пользователем содержимого данных для аутентификации. В варианте осуществления изобретения пользователь может вручную вводить сформированные данные для аутентификации.

Фиг.5-1 является логической блок-схемой, которая со стороны точки AP 12', не использующей технологию RSN, иллюстрирует способ и результат исполнения инструкций компьютерной программы в соответствии с примерами осуществления

данного изобретения. В соответствии с данными примерами осуществления изобретения способ включает на шаге 5A передачу точкой доступа к сети, не использующей технологию RSN, по меньшей мере одного маяка, включающего идентификатор набора услуг, а на шаге 5B точка доступа к сети, не использующая технологию RSN, предоставляет услугу подписки для защищенной точки доступа к сети, работающей с тем же самым идентификатором набора услуг. В одном варианте осуществления изобретения по меньшей мере один передаваемый маяк также включает указание возможностей, указывающее на то, что точка доступа к сети, не использующая технологию RSN, предоставляет возможность только подписки RSN.

Подписку в примерах осуществления изобретения осуществляют следующим образом. На шаге 5C точка доступа, не использующая технологию RSN, устанавливает связь с пользовательским устройством, например, посредством приема запроса на соединение от пользовательского устройства, а на шаге 5D осуществляется прием точкой доступа, не использующей технологию RSN, http-трафика от пользовательского устройства. Как было указано ранее, данный http-трафик может быть холостым трафиком или любым другим трафиком. На шаге 5E осуществляют перенаправление трафика на страницу портала, и для одного конкретного варианта осуществления изобретения на шаге 5F осуществляют формирование защищенного http-соединения с пользовательским устройством для создания данных для аутентификации, посредством которых пользовательское устройство может получить доступ к защищенной точке доступа к сети. На шаге 5G представлен вариант, в котором происходит аутентификация пользовательского устройства на странице портала, где пользовательское устройство создает данные для аутентификации. На шаге 5H представлен другой вариант, когда при аутентификации пользовательского устройства на странице портала данные для аутентификации, необходимые для установления связи с защищенной (RSN) точкой доступа, отправляют в пользовательское устройство со страницы портала. Может использоваться предварительное соединение с незащищенной точкой доступа, как было описано выше после описания фиг.4. На шаге 5I точка доступа, не использующая технологию RSN, прекращает соединение с пользовательским устройством.

Фиг.5-2 является логической блок-схемой, которая со стороны точки AP 12, использующей технологию RSN, иллюстрирует способ и результат исполнения инструкций компьютерной программы в соответствии с примерами осуществления данного изобретения. Узел доступа RSN может быть совмещен с узлом доступа, не использующим технологию RSN, таким образом, что оба узла, реализованные в одном и том же узле, выполняют разные функции. На шаге 5J узел доступа RSN передает по меньшей мере один маяк, а на шаге 5K в одном конкретном варианте осуществления изобретения точка доступа RSN предоставляет пользовательскому устройству идентификатор NAI для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с точкой доступа RSN. На шаге 5L осуществляют прием от пользовательского устройства запроса на установление соединения, который включает идентификатор NAI для подписки, а на шаге 5M осуществляют предоставление пользовательскому устройству (ограниченного) доступа к сети для создания данных для аутентификации. Шаги 5D-5H на фиг.5-2 аналогичны описанным ранее шагам на фиг.5-1. Далее на шаге 5N точка доступа RSN завершает предварительное соединение, которое было предоставлено на шаге 5M, и формирует на шаге 5O соединение с пользовательским устройством посредством использования данных для аутентификации и предоставляет пользовательскому устройству доступ к сети Интернет через точку доступа RSN.

Варианты осуществления изобретения также охватывают машиночитаемые носители данных, содержащие инструкции программного обеспечения, исполнение которых по меньшей мере одним процессором данных приводит к выполнению операций, включающих выполнение шагов способа, показанных на фиг.4 и 5-1 и 5-2 и описанных в соответствующих предыдущих абзацах.

Таким образом, различные шаги, показанные на фиг.4, 5-1 и 5-2, могут рассматриваться как шаги способа и/или как операции, которые происходят в результате исполнения операций кода компьютерной программы, и/или как множество связанных элементов логической цепи, собранных для выполнения соответствующих функций.

Примеры осуществления изобретения также относятся к устройству, которое включает процессор и память, содержащую код компьютерной программы. Память и код компьютерной программы сконфигурированы так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере приема в пользовательском устройстве по меньшей мере одного передаваемого маяка от по меньшей мере одной точки доступа к сети и в ответ на определение того, что пользовательское устройство не обладает данными для аутентификации, необходимыми для подключения к точке доступа к сети, формирования предварительного соединения с точкой доступа к сети, передачи http-трафика (например, холостого http-трафика) в точку доступа к сети и, в ответ на перенаправление и формирование защищенного http-соединения со страницей портала, осуществления аутентификации пользовательского устройства на странице портала и приема со страницы портала данных для аутентификации, необходимых для установления соединения с точкой доступа к сети. Кроме того, память и код компьютерной программы сконфигурированы так, чтобы с помощью процессора завершать предварительное соединение с точкой доступа к сети и формировать соединение с точкой доступа к сети посредством использования принятых данных для аутентификации таким образом, чтобы получить доступ к сети Интернет через точку доступа к сети.

В общем, различные примеры осуществления изобретения могут быть реализованы в аппаратном обеспечении или с помощью специализированных схем, программного обеспечения, логики, чипсетов, например, с помощью чипсета или чипсетов WLAN, или любой их комбинации. Например, некоторые аспекты изобретения могут быть реализованы в аппаратном обеспечении, тогда как другие аспекты изобретения могут быть реализованы во встроенном программном обеспечении или программном обеспечении, которое может исполняться контроллером, микропроцессором или другим вычислительным устройством, хотя изобретение этим не ограничивается. Хотя различные аспекты примеров осуществления данного изобретения могут быть проиллюстрированы и описаны с помощью структурных схем, блок-схем или посредством использования каких-либо других графических представлений, необходимо понимать, что данные блоки, устройства, системы, технологии или способы, описанные здесь, могут быть реализованы, например, не ограничиваясь этим, в аппаратном обеспечении, программном обеспечении, встроенном программном обеспечении, специализированных схемах или логике, универсальном аппаратном обеспечении или контроллере или в любом другом вычислительном устройстве или их комбинации.

Таким образом, необходимо понимать, что по меньшей мере часть аспектов примеров осуществления изобретения может быть реализована на практике в различных компонентах, таких как чипы и модули интегральных схем, и примеры осуществления данного изобретения могут быть реализованы в устройстве, выполненном в интегральной схеме. Интегральная схема или схемы могут включать схемы (а также,

возможно, и встроенное программное обеспечение) для реализации по меньшей мере одного или более процессоров данных, устройств цифровой обработки сигналов, схем основной полосы частот и радиочастотной схемы, которые сконфигурированы для работы в соответствии с примерами осуществления данного изобретения.

Из представленного выше описания и прилагаемых чертежей для специалистов могут стать очевидными различные изменения и адаптации представленных выше примеров осуществления данного изобретения. Однако любые и все такие модификации находятся в пределах сущности примеров осуществления данного изобретения.

Например, несмотря на то, что примеры осуществления изобретения, представленные выше, были описаны в контексте систем типа IEEE 802, необходимо понимать, что изобретение не ограничено использованием конкретного типа системы беспроводной связи и может обеспечивать преимущества и в других системах беспроводной связи.

Необходимо отметить, что термины «соединенный», «связанный» или любые их варианты означают любое соединение или связь, прямую или косвенную, между двумя или более элементами и охватывают также наличие одного или более промежуточных элементов между двумя элементами, которые «соединены» или «связаны» друг с другом. Соединение или связь между элементами могут быть физическими, логическими или их комбинацией. Два элемента могут рассматриваться как «соединенные» или «связанные» друг с другом посредством, например, не ограничиваясь этим, одного или более проводов, кабелей и/или печатных электрических соединений, а также посредством использования электромагнитной энергии, такой как электромагнитная энергия с длинами волн в радиочастотном диапазоне, диапазоне СВЧ и в оптическом (как видимом, так и невидимом) диапазоне.

Кроме того, различные названия, используемые для описываемых параметров (например, SSID и т.д.) не предназначены для ограничения изобретения, так как данные параметры могут быть определены любыми подходящими названиями. Кроме того, различные названия, назначенные различным сетевым соединениям (например, HTTP, HTTPS и т.д.) не предназначены для ограничения изобретения, так как эти различные соединения могут быть определены любыми подходящими названиями.

Кроме того, некоторые признаки различных примеров осуществления данного изобретения могут использоваться с обеспечением преимуществ без использования других признаков. Поэтому изложенное выше описание должно рассматриваться лишь в качестве иллюстрации принципов, основ и примеров осуществления данного изобретения, а не в качестве ограничения изобретения.

Формула изобретения

1. Устройство беспроводной связи, содержащее:

по меньшей мере один процессор и

по меньшей мере одну память, содержащую код компьютерной программы;

при этом по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего:

приема передаваемого маяка от защищенной точки доступа к сети, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

формирования предварительного соединения с упомянутой защищенной точкой доступа к сети с использованием сообщаемого идентификатора набора услуг в ответ на определение того, что устройство не обладает данными для аутентификации, необходимыми для подключения к упомянутой защищенной точке доступа к сети;

приема или создания, во время упомянутого предварительного соединения, данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и

формирования соединения с защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и сообщаемого идентификатора набора услуг и получения доступа к сети Интернет через защищенную точку доступа к сети.

2. Устройство по п. 1, в котором по меньшей мере одна память с кодом компьютерной программы также сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего:

передачи http-трафика в упомянутую защищенную точку доступа, с которой формируется предварительное соединение, и

формирования защищенного http-соединения со страницей портала, на которую устройство перенаправляется в ответ на передачу http-трафика,

при этом устройство сконфигурировано для приема или создания данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, во время защищенного http-соединения со страницей портала.

3. Устройство по п. 2, в котором во время соединения со страницей портала пользователь имеет возможность выбора, посредством устройства, либо ручного, либо автоматического формирования данных для аутентификации.

4. Устройство по п. 3, в котором при автоматическом формировании данных для аутентификации устройство принимает от страницы портала сформированные данные для аутентификации, которые включают одно из следующего: имя пользователя, пароль и клиентский сертификат, при этом устройство сконфигурировано для хранения принятых данных для аутентификации в упомянутой по меньшей мере одной памяти и автоматического предоставления защищенной точке доступа к сети сохраненных данных для аутентификации без необходимости знания пользователем содержимого данных для аутентификации.

5. Устройство по п. 1, в котором упомянутый маяк, принятый от защищенной точки доступа к сети, указывает на то, что упомянутая защищенная точка доступа к сети поддерживает онлайн-подписку.

6. Устройство по п. 1, в котором по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего:

передачи в защищенную точку доступа к сети запроса на идентификатор доступа к сети (NAI) для подписки, когда устройство находится в состоянии предварительного соединения;

приема запрашиваемого идентификатора доступа к сети для подписки и последующего формирования предварительного соединения с защищенной точкой доступа к сети с использованием идентификатора доступа к сети и аутентификации только на стороне сервера.

7. Способ беспроводной связи, включающий:

прием в пользовательском устройстве по меньшей мере одного передаваемого маяка от защищенной точки доступа к сети, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

формирование предварительного соединения с упомянутой защищенной точкой доступа к сети с использованием сообщаемого идентификатора набора услуг в ответ

на определение того, что пользовательское устройство не обладает данными для аутентификации, необходимыми для подключения к упомянутой защищенной точке доступа к сети;

прием или создание пользовательским устройством, во время упомянутого предварительного соединения, данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и

формирование соединения между пользовательским устройством и защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и сообщаемого идентификатора набора услуг и получение доступа к сети Интернет через защищенную точку доступа к сети.

8. Способ по п. 7, также включающий:

передачу http-трафика в упомянутую защищенную точку доступа, с которой формируют предварительное соединение, и

формирование защищенного http-соединения со страницей портала, на которую перенаправляют пользовательское устройство в ответ на передачу http-трафика;

при этом пользовательское устройство принимает или создает данные для аутентификации, необходимые для соединения с защищенной точкой доступа к сети, во время защищенного http-соединения со страницей портала.

9. Способ по п. 7, в котором упомянутый маяк, принятый от защищенной точки доступа к сети, указывает на то, что упомянутая защищенная точка доступа к сети поддерживает онлайн-подписку.

10. Способ по п. 7, включающий

передачу в защищенную точку доступа к сети запроса на идентификатор доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения;

прием запрашиваемого идентификатора доступа к сети для подписки и

последующее формирование предварительного соединения с защищенной точкой доступа к сети посредством использования идентификатора доступа к сети и аутентификации только на стороне сервера.

11. Машиночитаемый носитель данных, который включает инструкции компьютерной программы, которые при их исполнении по меньшей мере одним процессором данных приводят к выполнению операций, включающих:

прием в пользовательском устройстве от защищенной точки доступа к сети по меньшей мере одного передаваемого маяка, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

формирование предварительного соединения с упомянутой защищенной точкой доступа к сети с использованием сообщаемого идентификатора набора услуг в ответ на определение того, что пользовательское устройство не обладает данными для аутентификации, необходимыми для подключения к упомянутой защищенной точке доступа к сети;

прием или создание пользовательским устройством, во время упомянутого предварительного соединения, данных для аутентификации, необходимых для соединения с защищенной точкой доступа к сети, и

формирование соединения между пользовательским устройством и защищенной точкой доступа к сети посредством использования принятых или созданных данных для аутентификации и сообщаемого идентификатора набора услуг и получение доступа к сети Интернет через защищенную точку доступа к сети.

12. Устройство беспроводной связи, содержащее:

по меньшей мере один процессор и

по меньшей мере одну память, содержащую код компьютерной программы;

при этом по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере следующего:

передачи по меньшей мере одного маяка, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

предоставления пользовательскому устройству идентификатора доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с использованием сообщаемого идентификатора набора услуг;

приема от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки,

предоставления пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации и,

с использованием созданных данных для аутентификации, предоставления пользовательскому устройству доступа к сети Интернет посредством сообщаемого идентификатора набора услуг.

13. Устройство по п. 12, в котором предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации включает:

установление предварительного соединения с пользовательским устройством;

перенаправление http-трафика, принятого от пользовательского устройства, на страницу портала;

формирование защищенного http-соединения с пользовательским устройством для создания данных для аутентификации и

завершение упомянутого предварительного соединения с пользовательским устройством.

14. Устройство по п. 12 или 13, включающее точку доступа к сети, использующую технологию надежно защищенной сети RSN, при этом по меньшей мере одна память с кодом компьютерной программы сконфигурирована так, чтобы с помощью упомянутого по меньшей мере одного процессора обеспечивать выполнение устройством по меньшей мере

формирования соединения с пользовательским устройством с использованием данных для аутентификации и последующего предоставления пользовательскому устройству доступа к сети Интернет через упомянутое устройство.

15. Способ беспроводной связи, включающий:

передачу по меньшей мере одного маяка, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

предоставление пользовательскому устройству идентификатора доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с использованием сообщаемого идентификатора набора услуг;

прием от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки,

предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации и,

с использованием созданных данных для аутентификации, предоставления пользовательскому устройству доступа к сети Интернет посредством сообщаемого

идентификатора набора услуг.

16. Способ по п. 15, в котором предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации включает:

установление предварительного соединения с пользовательским устройством;

перенаправление http-трафика, принятого от пользовательского устройства, на страницу портала;

формирование защищенного http-соединения с пользовательским устройством для создания данных для аутентификации и

завершение упомянутого предварительного соединения с пользовательским устройством.

17. Способ по п. 15 или 16, выполняемый точкой доступа к сети, использующей технологию надежно защищенной сети RSN, при этом способ также включает:

формирование соединения с пользовательским устройством с использованием данных для аутентификации и последующее предоставление пользовательскому устройству доступа к сети Интернет через точку доступа к сети, использующую технологию надежно защищенной сети RSN.

18. Машиночитаемый носитель данных, содержащий инструкции компьютерной программы, которые при их исполнении по меньшей мере одним процессором данных приводят к выполнению операций, включающих:

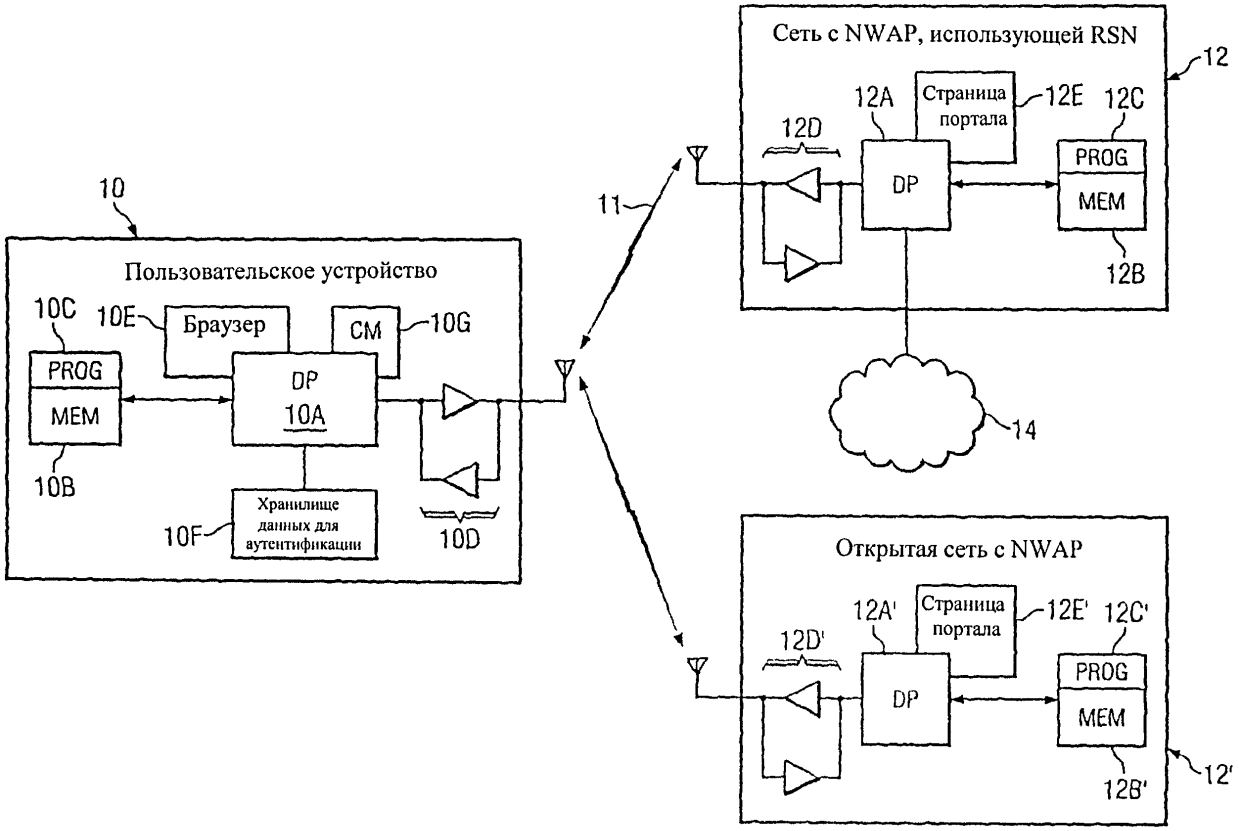
передачу по меньшей мере одного маяка, при этом упомянутый маяк сообщает идентификатор набора услуг (SSID);

предоставление пользовательскому устройству идентификатора доступа к сети (NAI) для подписки, когда пользовательское устройство находится в состоянии предварительного соединения с использованием сообщаемого идентификатора набора услуг;

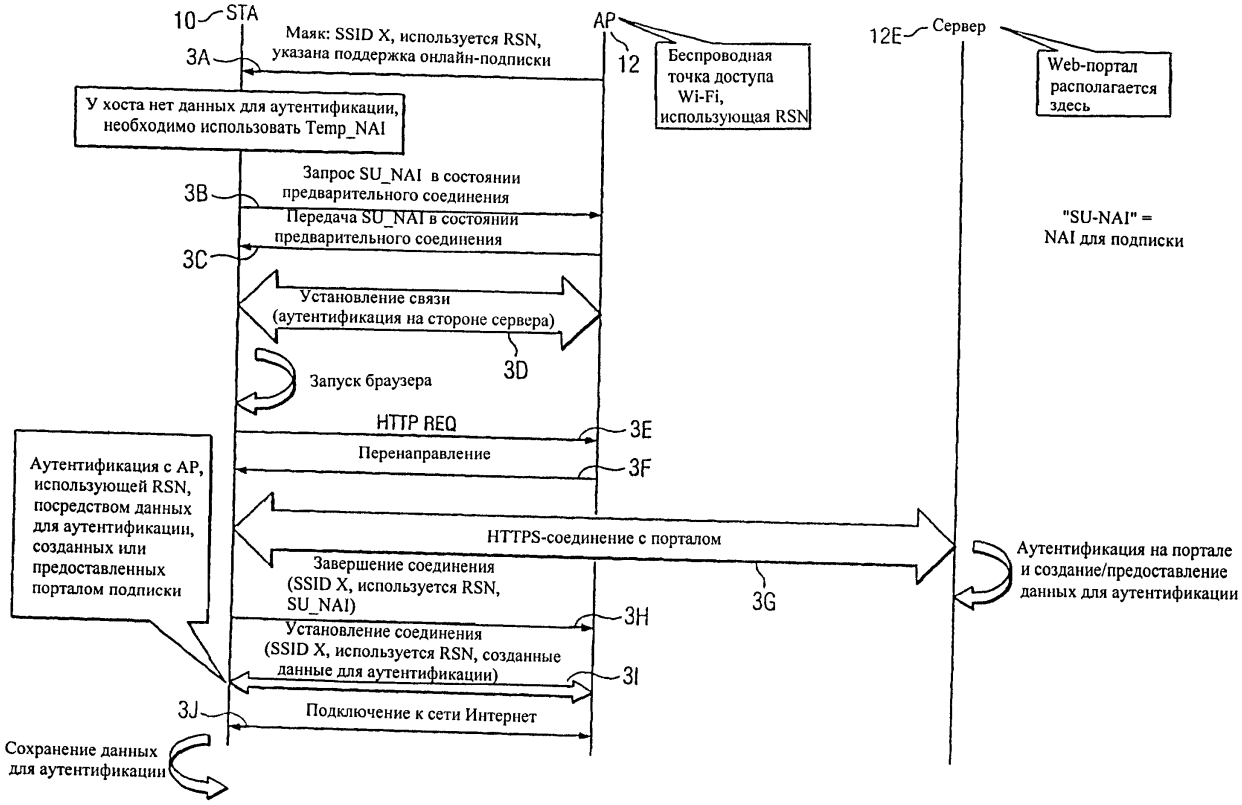
прием от пользовательского устройства запроса на установление соединения, который включает идентификатор доступа к сети (NAI) для подписки,

предоставление пользовательскому устройству ограниченного доступа к сети для создания данных для аутентификации и,

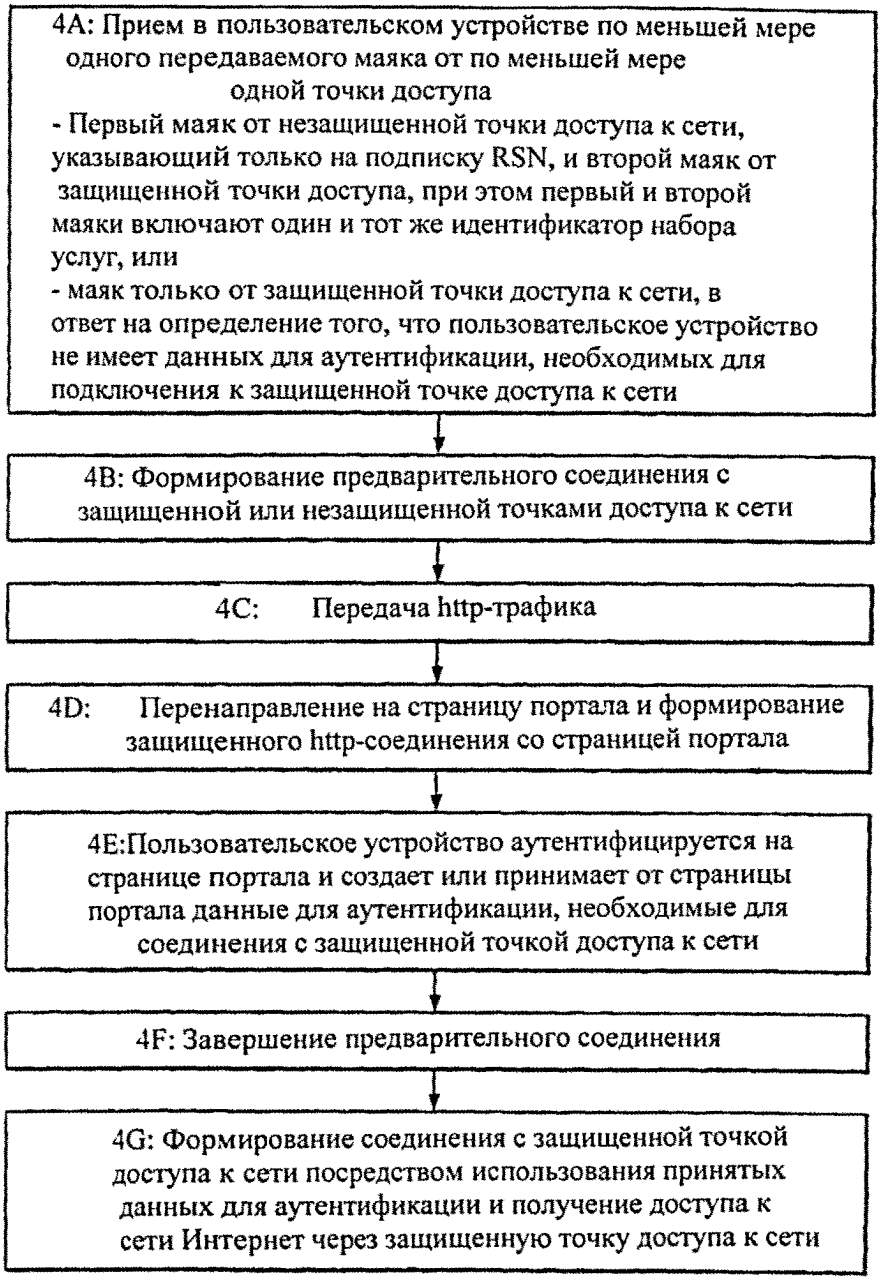
с использованием созданных данных для аутентификации, предоставления пользовательскому устройству доступа к сети Интернет посредством сообщаемого идентификатора набора услуг.


Сеть с NWAP, использующей RSN
12
12A
Страница портала
12E
12C
12D
DP
PROG
MEM
12B
10
11
Пользовательское устройство
10C
10E
Браузер
CM
10G
PROG
MEM
DP
10A
10B
Хранилище данных для аутентификации
10F
10D
14
Открытая сеть с NWAP
12A'
Страница портала
12E'
12C'
12D'
DP
PROG
MEM
12B'
12'

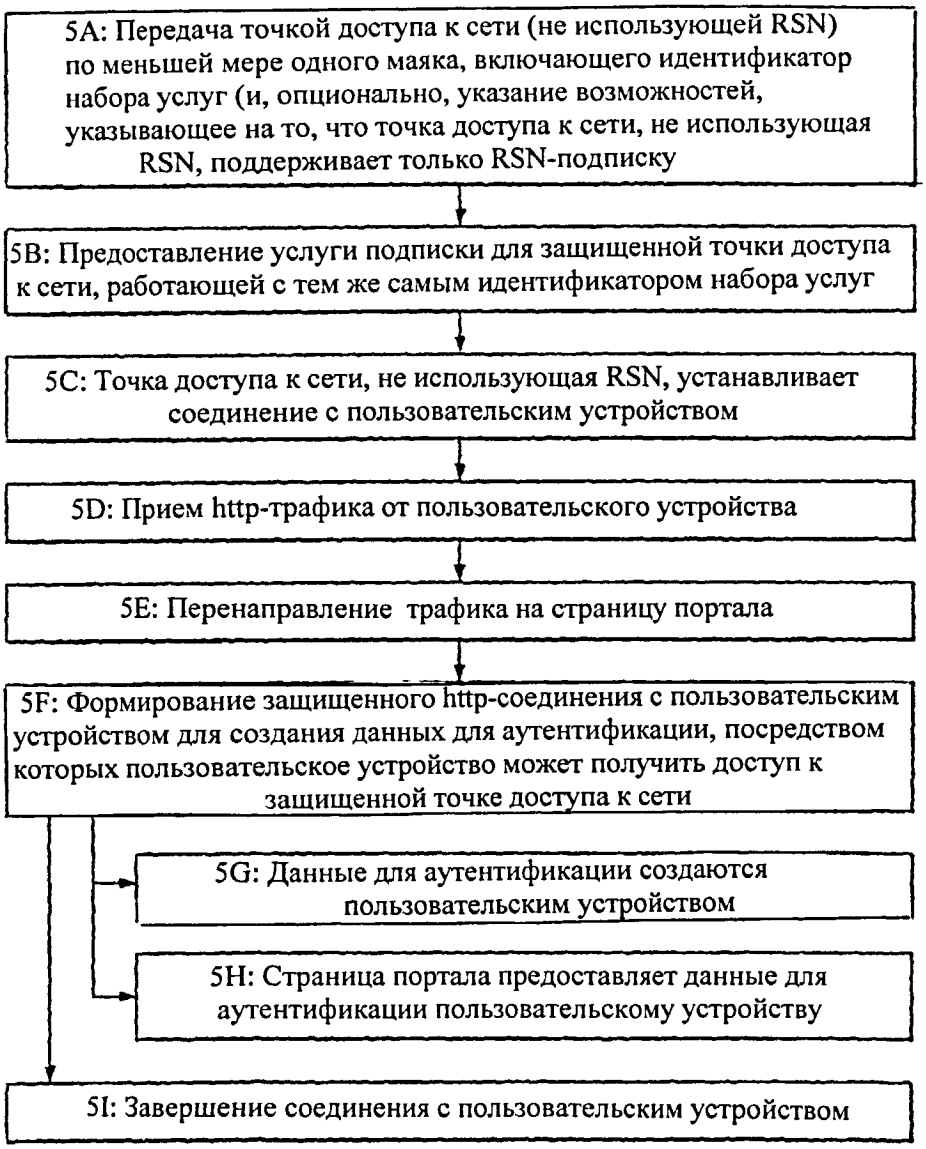
Фиг.1


10 STA
AP
12E Сервер
Маяк: SSID X, используется RSN, указана поддержка онлайн-подписки
3A
12
Беспроводная точка доступа Wi-Fi, использующая RSN
Web-портал располагается здесь
У хоста нет данных для аутентификации, необходимо использовать Temp_NAI
Запрос SU_NAI в состоянии предварительного соединения
3B
Передача SU_NAI в состоянии предварительного соединения
"SU-NAI" = NAI для подписки
3C
Установление связи (аутентификация на стороне сервера)
3D
Запуск браузера
HTTP REQ
3E
Перенаправление
3F
Аутентификация с AP, использующей RSN, посредством данных для аутентификации, созданных или предоставленных порталом подписки
HTTPS-соединение с порталом
Аутентификация на портале и создание/предоставление данных для аутентификации
3G
Завершение соединения (SSID X, используется RSN, SU_NAI)
3H
Установление соединения (SSID X, используется RSN, созданные данные для аутентификации)
3I
3J
Подключение к сети Интернет
Сохранение данных для аутентификации

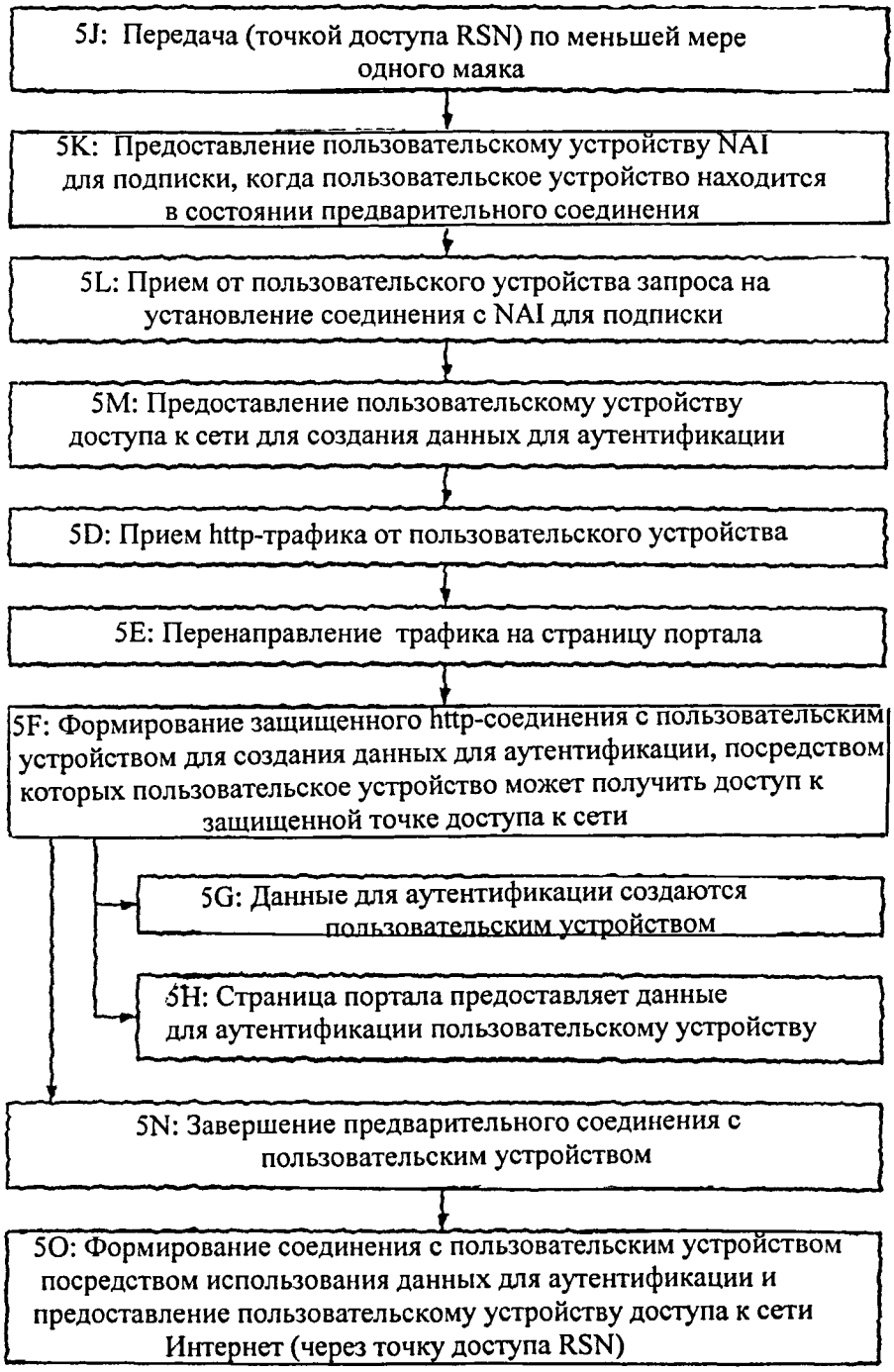
Фиг. 3


4A: Прием в пользовательском устройстве по меньшей мере одного передаваемого маяка от по меньшей мере одной точки доступа
- Первый маяк от незащищенной точки доступа к сети, указывающий только на подписку RSN, и второй маяк от защищенной точки доступа, при этом первый и второй маяки включают один и тот же идентификатор набора услуг, или
- маяк только от защищенной точки доступа к сети, в ответ на определение того, что пользовательское устройство не имеет данных для аутентификации, необходимых для подключения к защищенной точке доступа к сети
4B: Формирование предварительного соединения с защищенной или незащищенной точками доступа к сети
4C: Передача http-трафика
4D: Перенаправление на страницу портала и формирование защищенного http-соединения со страницей портала
4E:Пользовательское устройство аутентифицируется на странице портала и создает или принимает от страницы портала данные для аутентификации, необходимые для соединения с защищенной точкой доступа к сети
4F: Завершение предварительного соединения
4G: Формирование соединения с защищенной точкой доступа к сети посредством использования принятых данных для аутентификации и получение доступа к сети Интернет через защищенную точку доступа к сети

Фиг. 4


5A: Передача точкой доступа к сети (не использующей RSN) по меньшей мере одного маяка, включающего идентификатор набора услуг (и, опционально, указание возможностей, указывающее на то, что точка доступа к сети, не использующая RSN, поддерживает только RSN-подписку
5B: Предоставление услуги подписки для защищенной точки доступа к сети, работающей с тем же самым идентификатором набора услуг
5C: Точка доступа к сети, не использующая RSN, устанавливает соединение с пользовательским устройством
5D: Прием http-трафика от пользовательского устройства
5E: Перенаправление трафика на страницу портала
5F: Формирование защищенного http-соединения с пользовательским устройством для создания данных для аутентификации, посредством которых пользовательское устройство может получить доступ к защищенной точке доступа к сети
5G: Данные для аутентификации создаются пользовательским устройством
5H: Страница портала предоставляет данные для аутентификации пользовательскому устройству
5I: Завершение соединения с пользовательским устройством

Фиг. 5-1


5J: Передача (точкой доступа RSN) по меньшей мере одного маяка
5K: Предоставление пользовательскому устройству NAI для подписки, когда пользовательское устройство находится в состоянии предварительного соединения
5L: Прием от пользовательского устройства запроса на установление соединения с NAI для подписки
5M: Предоставление пользовательскому устройству доступа к сети для создания данных для аутентификации
5D: Прием http-трафика от пользовательского устройства
5E: Перенаправление трафика на страницу портала
5F: Формирование защищенного http-соединения с пользовательским устройством для создания данных для аутентификации, посредством которых пользовательское устройство может получить доступ к защищенной точке доступа к сети
5G: Данные для аутентификации создаются пользовательским устройством
5H: Страница портала предоставляет данные для аутентификации пользовательскому устройству
5N: Завершение предварительного соединения с пользовательским устройством
5O: Формирование соединения с пользовательским устройством посредством использования данных для аутентификации и предоставление пользовательскому устройству доступа к сети Интернет (через точку доступа RSN)

Фиг. 5-2