РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 766 440**(13) **C2**

(51) МПК
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04W 12/069 (2021.01)
H04W 12/50 (2021.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 63/0869 (2021.05); H04L 9/3273 (2021.05); H04W 12/069 (2021.05); H04W 12/50 (2021.05)

(21)(22) Заявка: **2019132954, 15.03.2018**

(24) Дата начала отсчета срока действия патента:
15.03.2018

Дата регистрации:
15.03.2022

Приоритет(ы):
(30) Конвенционный приоритет:
20.03.2017 EP 17161856.4

(43) Дата публикации заявки: **21.04.2021** Бюл. № **12**

(45) Опубликовано: **15.03.2022** Бюл. № **8**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **21.10.2019**

(86) Заявка PCT:
EP 2018/056491 (15.03.2018)

(87) Публикация заявки PCT:
WO 2018/172171 (27.09.2018)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
БЕРНСЕН, Йоханнес Арнольдус Корнелис (NL),
ВАН ДЕ ЛАР, Францискус Антониус Мария (NL),
ЛИНДЕРС, Роналд Феликс Альбертус (NL)

(73) Патентообладатель(и):
КОНИНКЛЕЙКЕ ФИЛИПС Н.В. (NL)

(56) Список документов, цитированных в отчете о поиске: **EP 3051744 A1, 03.08.2016. US 2010/0042838 A1, 18.02.2010. US 2013/0036231 A1, 07.02.2013. RU 2575682 C2, 20.02.2016.**

(54) СИСТЕМА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ

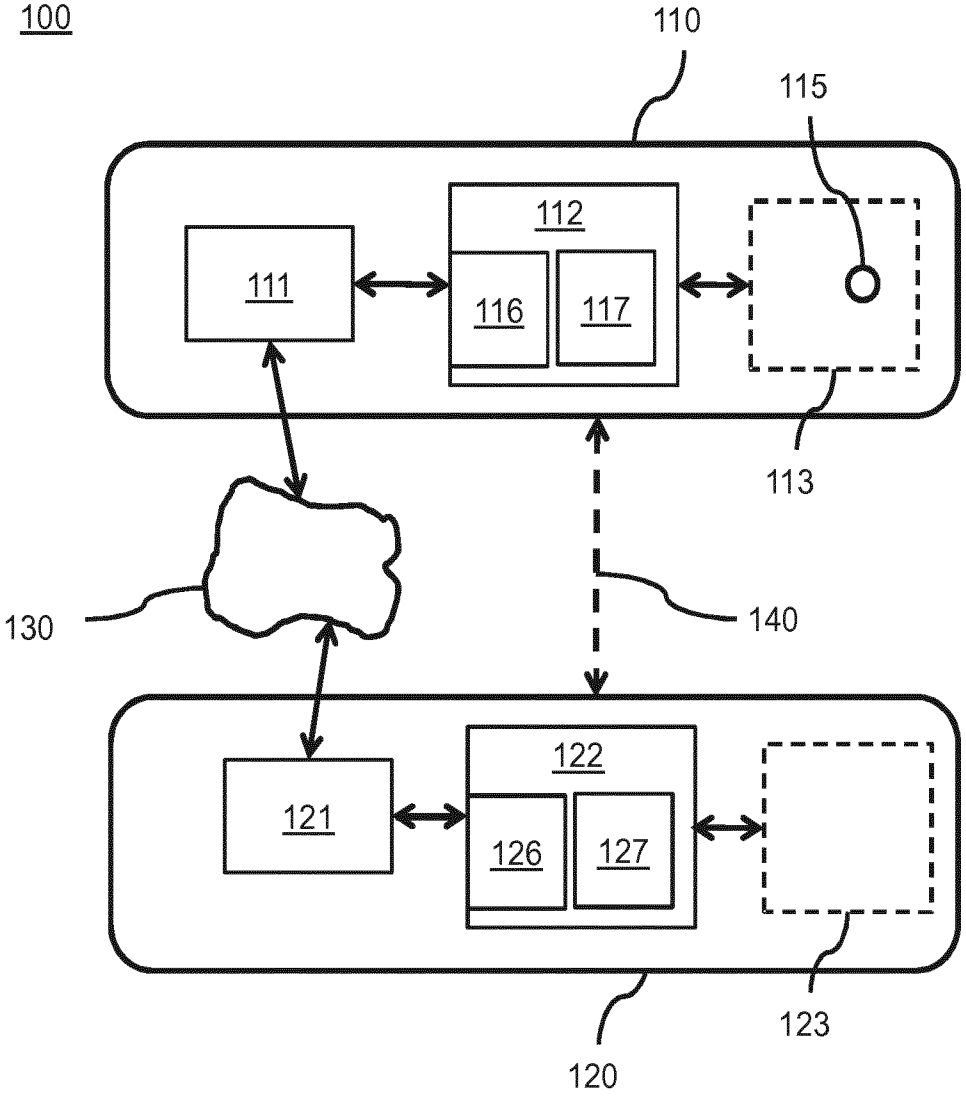
(57) Реферат:

Изобретение относится к системе беспроводной связи, которая обеспечивает одностороннюю аутентификацию устройства–ответчика посредством устройства–инициатора и взаимную аутентификацию обоих устройств. Технический результат заключается в недопущении длительных периодов тайм–аута во время беспроводной связи при одновременном обеспечении возможности инициатору также сообщать ошибки связи пользователю в течение короткого времени. Инициатор могут иметь модуль сообщений и конечный автомат. Инициатор запускается посредством получения общедоступного ключа ответчика через внеполосное действие и отправляет запрос на аутентификацию. Ответчик отправляет ответ по аутентификации, содержащий данные аутентификации ответчика на основе конфиденциального ключа ответчика и статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора через

RU 2766440 C2

RU 2766440 C2

внеполосное действие ответчика. Конечный автомат инициатора выполнен с возможностью предоставлять состояние взаимной аутентификации, активированное при приеме статуса взаимного проведения, для ожидания взаимной аутентификации. 7 н. и 12 з.п. ф-лы, 8 ил.



ФИГ. 1

RU 2766440 C2

RU 2766440 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 766 440**(13) **C2**

(51) Int. Cl.
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04W 12/069 (2021.01)
H04W 12/50 (2021.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 63/0869 (2021.05); H04L 9/3273 (2021.05); H04W 12/069 (2021.05); H04W 12/50 (2021.05)

(21)(22) Application: **2019132954, 15.03.2018**

(24) Effective date for property rights:
15.03.2018

Registration date:
15.03.2022

Priority:
(30) Convention priority:
20.03.2017 EP 17161856.4

(43) Application published: **21.04.2021** Bull. № **12**

(45) Date of publication: **15.03.2022** Bull. № **8**

(85) Commencement of national phase: **21.10.2019**

(86) PCT application:
EP 2018/056491 (15.03.2018)

(87) PCT publication:
WO 2018/172171 (27.09.2018)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
BERNSEN, Johannes Arnoldus Cornelis (NL),
VAN DE LAAR, Franciscus Antonius Maria (NL),
LINDERS, Ronald Felix Albertus (NL)

(73) Proprietor(s):
Koninklijke Philips N.V. (NL)

(54) MUTUAL AUTHENTICATION SYSTEM

(57) Abstract:

FIELD: wireless communication.

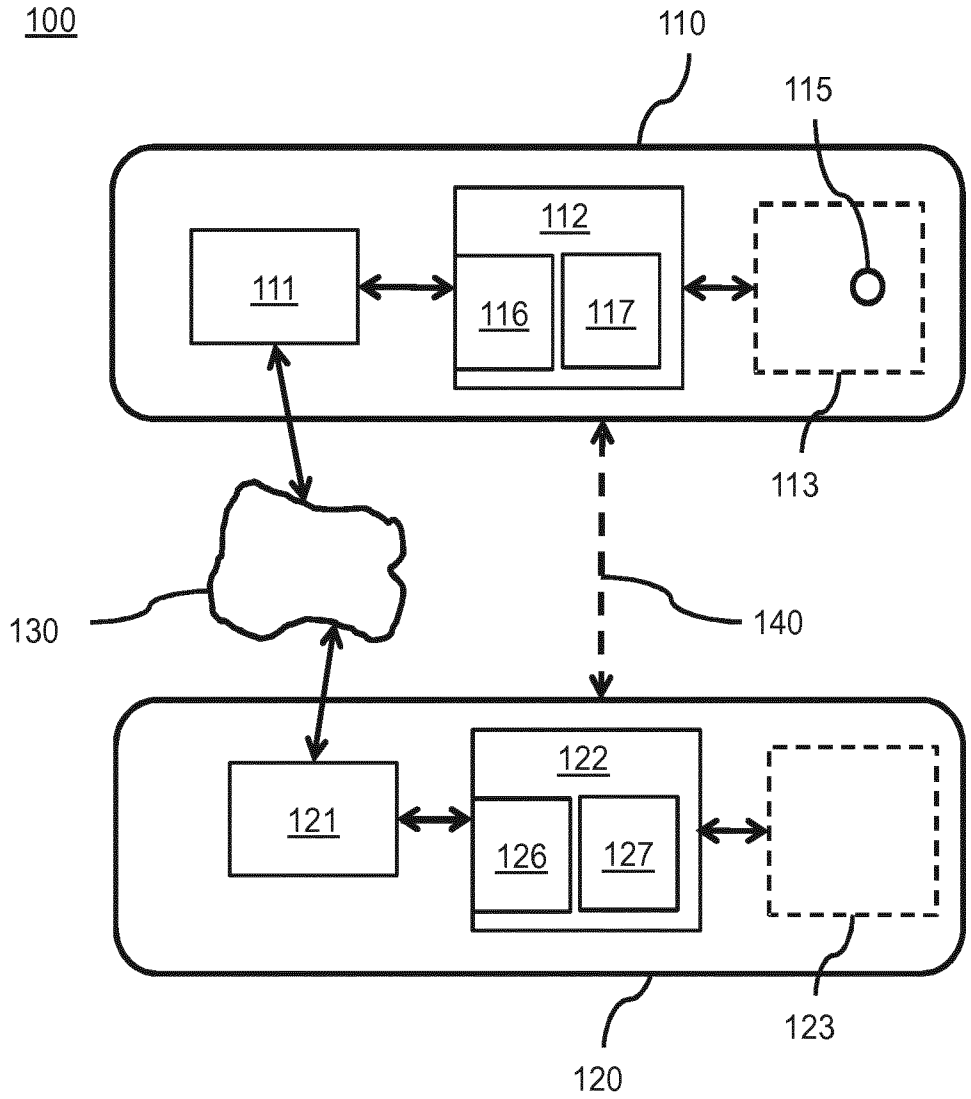
SUBSTANCE: invention relates to a wireless communication system that provides one-way authentication of a respondent device by means of an initiator device and mutual authentication of both devices. The initiator can have a message module and a state machine. The initiator is actuated by obtaining a responder public key through an out-of-band action, and it sends an authentication request. The respondent sends an authentication response containing respondent authentication data based on the respondent confidential key and a mutual conduct status indicating mutual authentication to enable the respondent device to receive an initiator public key through the respondent out-of-band action. The initiator state machine is made with the possibility of providing a mutual authentication state activated when receiving the mutual conduct status to wait for mutual authentication.

EFFECT: prevention of long periods of timeout during wireless communication while simultaneously enabling the initiator to report communication errors to the user within a short time.

19 cl, 8 dwg

RU 2766440 C2

RU 2766440 C2



ФИГ. 1

RU 2766440 C2

RU 2766440 C2

Область техники, к которой относится изобретение

Изобретение относится к устройству–инициатору и к устройству–ответчику, выполненным с возможностью осуществления беспроводной связи согласно протоколу связи, и к способам и компьютерным программным продуктам для использования в таких устройствах. Протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из следующего:

– односторонняя аутентификация устройства–ответчика посредством устройства–инициатора, и

– взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика. Устройство–ответчик содержит приемопередающее устройство ответчика, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи, и процессор ответчика, выполненный с возможностью обработки протокола связи. Устройство–инициатор содержит приемопередающее устройство инициатора, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи, и процессор инициатора, выполненный с возможностью обработки протокола связи.

Настоящее изобретение относится к области техники систем ближней беспроводной связи, например, систем связи в помещениях, и более конкретно, предоставляет различные устройства и способы для защищенного установления беспроводных соединений на основе аутентификации устройства–ответчика и/или устройства–инициатора. Wi–Fi, см. ссылочный документ [1], предоставляет пример протокола связи и механизма для того, чтобы устанавливать соединения беспроводных устройств.

Уровень техники

Общедоступные ключи могут использоваться в качестве средства для того, чтобы идентифицировать и аутентифицировать устройства в беспроводной связи. Конфиденциальный ключ, ассоциированный с общедоступным ключом, должен формироваться в каждом устройстве и защищаться от раскрытия. Устройства используют криптографические технологии с общедоступным ключом для того, чтобы аутентифицировать равноправные устройства, причем устройства должны доказывать владение конфиденциальным ключом, соответствующим их общедоступному ключу, и устанавливать совместно используемые ключи для дополнительной защищенной связи. Эта архитектура безопасности упрощает установление защищенного подключения между устройствами и обеспечивает основу для повышенного удобства и простоты при подготовке и соединении устройств.

Устройство, которое запускает протокол аутентификации, играет роль инициатора. Устройство, которое отвечает на запрос инициатора, играет роль ответчика. Протокол аутентификации может предоставлять аутентификацию ответчика для инициатора и необязательно аутентификацию инициатора для ответчика. Это предполагает то, что инициатор получает самоинициализирующийся ключ ответчика, чтобы выполнять однонаправленную аутентификацию, и обе стороны получают самоинициализирующиеся ключи друг друга, чтобы необязательно выполнять взаимную аутентификацию.

Алгоритм Диффи–Хеллмана, см. ссылочный документ [6], представляет собой известную технологию для установления секретного ключа между двумя сторонами, в которой связь между сторонами не раскрывает информации для третьих сторон относительно установленного секретного ключа. Две стороны используют собственную пару общедоступного/конфиденциального ключа и обмениваются общедоступным

ключом между собой. Каждая сторона имеет возможность вычислять секретный ключ с использованием собственного конфиденциального ключа и общедоступного ключа другой стороны и возможно некоторой другой информации, например, одноразового номера (случайного числа) из каждой стороны. Каждая сторона может формировать пару ключей снова каждый раз, когда она выполняет алгоритм Диффи–Хеллмана, либо она может многократно использовать устаревшую пару ключей.

При выполнении алгоритма Диффи–Хеллмана по сети, устройство, которое принимает общедоступный ключ для выполнения алгоритма Диффи–Хеллмана, не знает то, из какого устройства исходит этот общедоступный ключ. Это может быть использовано посредством взломщика в так называемой атаке по технологии "злоумышленник посередине". Взломщик E может выдавать себя за реальное устройство B, с которым хочет соединяться устройство A. Взломщик E выполняет алгоритм Диффи–Хеллмана с устройством A и устанавливает секретный ключ Kae с устройством A. Аналогично, взломщик выдает себя за устройство A для устройства B и устанавливает секретный ключ Kbe с устройством B. Когда сообщение поступает от одного из устройств A или B, взломщик дешифрует сообщение с помощью одного секретного ключа, шифрует его с помощью другого и перенаправляет его в другое устройство. Таким образом, устройства A и B не замечают ничего странного в своей связи, за исключением некоторой дополнительной задержки. Но взломщик имеет полные сведения относительно того, чем они обмениваются.

Чтобы повышать безопасность беспроводной связи, протокол может использоваться для аутентификации одного или более устройств, участвующих в защищенной беспроводной связи согласно протоколу связи. Такой протокол аутентификации может запускаться посредством первого участвующего устройства, обычно называемого устройством–инициатором, поддерживающего связь со вторым участвующим устройством, обычно называемым устройством–ответчиком. В текущем контексте, устройство–инициатор может представлять собой любое электронное устройство, имеющее возможность для установления соединения с использованием беспроводной связи. Устройство–инициатор может представлять собой стационарное устройство, такое как PC или точка доступа, или беспроводная стыковочная станция, или беспроводной USB–концентратор, или беспроводной видео– или AV–монитор, но также может представлять собой портативное устройство, такое как переносной компьютер или мобильный телефон. Устройство–ответчик аналогично может представлять собой любой тип электронного устройства, имеющего возможность для установления соединения с использованием беспроводной связи.

Таким образом, протокол связи может включать в себя протокол аутентификации для обеспечения аутентификации ответчика и/или инициатора. Аутентификация может представлять собой одностороннюю аутентификацию устройства–ответчика посредством устройства–инициатора. Кроме того, аутентификация может представлять собой взаимную аутентификацию, которая заключает в себе аутентификацию устройства–ответчика посредством устройства–инициатора и аутентификацию устройства–инициатора посредством устройства–ответчика.

Сущность изобретения

В таких протоколах аутентификации, например, чтобы предотвращать атаки по технологии "злоумышленник посередине" при использовании алгоритма Диффи–Хеллмана, другой способ связи может использоваться для обмена общедоступными ключами или хешами общедоступных ключей, т.е. помимо канала беспроводной связи, используемого согласно протоколу беспроводной связи, что

обычно называется внутриполосной связью. Другой способ связи обычно называются внеполосной (ООВ) связью, например, с использованием визуального маркера, такого как штрих–код, или инструктирования пользователю вводить код.

Кроме того, протоколы связи обычно имеют механизм для того, чтобы справляться с шумом и возмущениями беспроводного обмена сообщениями. Например, когда ответ не принимается в пределах предварительно определенного периода тайм–аута, сообщение передается снова. После предварительно определенного числа повторений, протокол связи может прерываться.

Цель изобретения заключается в том, чтобы предоставлять систему защищенной беспроводной связи для надежного установления соединения между устройством–инициатором и устройством–ответчиком, при недопущении ненадлежаще длительных периодов тайм–аута во время аутентификации.

С этой целью, предоставляются устройства и способы, как задано в прилагаемой формуле изобретения.

Согласно аспекту изобретения, устройство–инициатор выполнено с возможностью осуществления беспроводной связи с устройством–ответчиком согласно протоколу связи,

– причем протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из следующего:

– односторонняя аутентификация устройства–ответчика посредством устройства–инициатора, и

– взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

– причем устройство–ответчик содержит:

– приемопередающее устройство ответчика, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи, и

– процессор ответчика, выполненный с возможностью обработки протокола связи,

– при этом устройство–инициатор содержит:

– приемопередающее устройство инициатора, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи,

– процессор инициатора, выполненный с возможностью обработки протокола связи и имеющий:

– модуль сообщений инициатора, чтобы составлять сообщения, которые должны отправляться в устройство–ответчик, и раскладывать сообщения, принимаемые от устройства–ответчика, согласно протоколу аутентификации; и

– конечный автомат инициатора, чтобы предоставлять состояния инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–ответчика, причем состояния инициатора содержат:

– начальное состояние для самоинициализации посредством получения общедоступного ключа ответчика от устройства–ответчика через внеполосное действие инициатора,

– самоинициализированное состояние, указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика, и

– аутентифицированное состояние, указывающее то, что аутентификация успешно выполнена;

– причем модуль сообщений инициатора выполнен с возможностью составлять сообщения, содержащие:

– запрос на аутентификацию, который должен отправляться в самоинициализированном состоянии, содержащий верификатор инициатора для верификации общедоступного ключа инициатора и верификатор ответчика для верификации общедоступного ключа ответчика;

– и выполнен с возможностью раскладывать сообщения, содержащие:

– ответ по аутентификации, содержащий данные односторонней аутентификации ответчика на основе конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика; и

– и выполнен с возможностью составлять:

– подтверждение взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные взаимной аутентификации инициатора на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора.

Согласно дополнительному аспекту изобретения, в дополнение к способу односторонней аутентификации либо в качестве его альтернативы, взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика может выполняться. Согласно этому аспекту, конечный автомат инициатора выполнен с возможностью предоставлять состояние взаимной аутентификации, активированное при приеме статуса взаимного проведения, для ожидания взаимной аутентификации; и

– модуль сообщений инициатора выполнен с возможностью раскладывать:

– ответ по взаимной аутентификации, содержащий данные взаимной аутентификации ответчика на основе общедоступного ключа инициатора и конфиденциального ключа ответчика; и

– конечный автомат инициатора выполнен с возможностью активировать аутентифицированное состояние при приеме ответа по взаимной аутентификации и успешной обработке, посредством процессора инициатора, данных взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора.

Согласно дополнительному аспекту изобретения, устройство–ответчик выполнено с возможностью осуществления беспроводной связи с устройством–инициатором согласно протоколу связи,

– причем протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из следующего:

– односторонняя аутентификация устройства–ответчика посредством устройства–инициатора, и

– взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

– причем устройство–инициатор содержит:

– приемопередающее устройство инициатора, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи,

– процессор инициатора, выполненный с возможностью обработки протокола связи, и

– при этом устройство–ответчик содержит:

– приемопередающее устройство ответчика, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи,

– процессор ответчика, выполненный с возможностью обработки протокола связи и имеющий:

– модуль сообщений ответчика, чтобы составлять сообщения, которые должны отправляться в устройство–инициатор, и раскладывать сообщения, принимаемые от устройства–инициатора, согласно протоколу аутентификации,

– конечный автомат ответчика, чтобы предоставлять состояния ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–инициатора, причем состояния ответчика содержат:

– состояние ожидания для приема сообщений от инициатора, и

– аутентифицированное состояние ответчика, указывающее то, что аутентификация успешно выполнена;

– причем модуль сообщений ответчика выполнен с возможностью составлять сообщения, содержащие:

– ответ по аутентификации, содержащий данные односторонней аутентификации ответчика на основе конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации;

– и выполнен с возможностью раскладывать сообщения, содержащие:

– запрос на аутентификацию, содержащий верификатор инициатора для верификации общедоступного ключа инициатора и верификатор ответчика для верификации общедоступного ключа ответчика.

Согласно дополнительному аспекту изобретения, в дополнение к способу односторонней аутентификации либо в качестве его альтернативы, взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика может выполняться. Согласно этому аспекту, конечный автомат ответчика выполнен с возможностью:

– предоставлять состояние взаимной аутентификации ответчика для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика; и

– модуль сообщений ответчика выполнен с возможностью составлять:

– ответ по взаимной аутентификации, который должен отправляться в состоянии взаимной аутентификации ответчика, содержащий данные взаимной аутентификации ответчика на основе общедоступного ключа инициатора и конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика;

– и выполнен с возможностью раскладывать:

– подтверждение взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные взаимной аутентификации инициатора на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора;

– конечный автомат ответчика выполнен с возможностью, при успешной обработке, посредством процессора ответчика, данных аутентификации инициатора на основе общедоступного ключа инициатора и конфиденциального ключа ответчика, активировать аутентифицированное состояние ответчика.

Согласно дополнительному аспекту изобретения, предусмотрен способ инициатора для использования в устройстве–инициаторе для осуществления беспроводной связи с устройством–ответчиком согласно протоколу связи,

– причем протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из следующего:

– односторонняя аутентификация устройства–ответчика посредством устройства–инициатора, и

– взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

– причем способ содержит:

– предоставление состояний инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–ответчика, причем состояния инициатора содержат:

– начальное состояние для самоинициализации посредством получения общедоступного ключа ответчика от устройства–ответчика через внеполосное действие инициатора,

– самоинициализированное состояние, указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика, и

– аутентифицированное состояние, указывающее то, что аутентификация успешно выполнена;

– составление запроса на аутентификацию, который должен отправляться в самоинициализированном состоянии, содержащего верификатор инициатора для верификации общедоступного ключа инициатора и верификатор ответчика для верификации общедоступного ключа ответчика;

– разложение ответа по аутентификации, содержащего данные односторонней аутентификации ответчика на основе конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика;

– предоставление состояния взаимной аутентификации, активированного при приеме статуса взаимного проведения, для ожидания взаимной аутентификации;

– разложение ответа по взаимной аутентификации, содержащего данные взаимной аутентификации ответчика на основе общедоступного ключа инициатора и конфиденциального ключа ответчика;

– составление подтверждения взаимной аутентификации, содержащего статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные взаимной аутентификации инициатора на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора; и

– активацию аутентифицированного состояния при приеме ответа по взаимной аутентификации и успешной обработке данных взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора.

Согласно дополнительному аспекту изобретения, предусмотрен способ ответчика для использования в устройстве–ответчике для осуществления беспроводной связи с устройством–инициатором согласно протоколу связи,

– причем протокол связи содержит протокол аутентификации для обеспечения

аутентификации, представляющей собой одно из следующего:

– односторонняя аутентификация устройства–ответчика посредством устройства–инициатора, и

– взаимная аутентификация устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

– причем способ содержит:

– предоставление состояний ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–инициатора, причем состояния ответчика содержат:

– состояние ожидания для приема сообщений от инициатора, и

– аутентифицированное состояние ответчика, указывающее то, что аутентификация успешно выполнена;

– составление ответа по аутентификации, содержащего данные односторонней аутентификации ответчика на основе конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации;

– разложение запроса на аутентификацию, содержащего верификатор инициатора для верификации общедоступного ключа инициатора и верификатор ответчика для верификации общедоступного ключа ответчика;

– активацию состояния аутентификации ответчика при успешной обработке запроса на аутентификацию;

– предоставление состояния взаимной аутентификации ответчика для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика;

– составление ответа по взаимной аутентификации, который должен отправляться в состоянии взаимной аутентификации ответчика, содержащего данные взаимной аутентификации ответчика на основе общедоступного ключа инициатора и конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика;

– разложение подтверждения взаимной аутентификации, содержащего статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные взаимной аутентификации инициатора на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора;

– активацию аутентифицированного состояния ответчика при успешной обработке данных взаимной аутентификации инициатора на основе общедоступного ключа инициатора и конфиденциального ключа ответчика.

Согласно дополнительному аспекту изобретения, предусмотрен компьютерный программный продукт, загружаемый из сети и/или сохраненный на машиночитаемом носителе и/или исполняемом микропроцессором носителе, причем продукт содержит инструкции программного кода для реализации вышеописанных способов при осуществлении на компьютере.

Вышеуказанные признаки имеют такое преимущество, что протокол аутентификации поддерживает как одностороннюю аутентификацию, так и взаимную связь. Протокол выполняется посредством обмена различными сообщениями, которые могут составляться и раскладываться посредством соответствующих модулей сообщений инициатора и ответчика. Кроме того, последовательность обмена сообщениями и обработки элементов в сообщениях может управляться через соответствующие конечные

автоматы инициатора и ответчика, которые определяют состояния устройств–инициаторов и ответчиков во время выполнения протокола аутентификации.

Кроме того, протокол аутентификации обеспечивает возможность использования внеполосной (OOB) связи для получения общедоступного ключа ответчика от устройства–ответчика. Внеполосное действие на стороне инициатора может заключать в себе прием непосредственно общедоступного ключа ответчика или кодированных данных общедоступного ключа ответчика, чтобы верифицировать общедоступный ключ ответчика, принимаемый через дополнительное действие при связи, например, принимаемый во внутриполосном сообщении или сохраненный в более раннем сеансе связи. Процесс получения начального количества материала ключа называется самоинициализацией. После успешной самоинициализации, инициатор может активировать состояние аутентификации для выполнения аутентификации устройства–ответчика.

Тем не менее, в случае взаимной аутентификации, устройство–ответчик должно получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика. Обмен кодами через OOB–связь может требовать длительного времени, например, если предусмотрено пользовательское взаимодействие, такое как считывание кода устройства–инициатора и его ввод в устройстве–ответчике или съемка изображения машиночитаемого кода, такого как штрих–код или QR–код, на устройстве–инициаторе (порядка десятых частей секунд). Такое время сравнивается по длине со временем для обмена сообщениями через беспроводную связь (обычно в миллисекунды или меньше). Устройство–инициатор может оставаться, после отправки запроса на аутентификацию, в ожидании ответа по аутентификации. Для обеспечения возможности упомянутой взаимной аутентификации, полный ответ по аутентификации должен предоставлять данные аутентификации ответчика также на основе общедоступного ключа инициатора. Авторы изобретения выявляют то, что полный ответ по аутентификации может передаваться только после относительно длительного времени, достаточного для OOB–действия ответчика. Следовательно, длительный период тайм–аута требуется в традиционном протоколе взаимной аутентификации. Недостаток состоит в том, что в случае, если запрос на аутентификацию не принимается, например, вследствие шума, повторная передача возникает только после упомянутого длительного периода тайм–аута.

Кроме того, в случае если запрос на аутентификацию не принимается, или в случае, если ответ по аутентификации содержит ошибочные данные, приводящие к тому, что аутентификация завершается неудачно, пользователь должен ожидать длительное время до того, как устройство–инициатор может позволять пользователю знать, что аутентификация завершена неудачно. Чтобы не допускать таких длительных периодов тайм–аута, он предоставляет ответ по аутентификации, содержащий данные аутентификации ответчика на основе конфиденциального ключа ответчика, соответствующего общедоступному ключу ответчика, который не заключает в себе ключа инициатора. Преимущественно, такой ответ по аутентификации может передаваться непосредственно после обработки запроса на аутентификацию, обеспечивая короткий тайм–аут в устройстве–инициаторе при отправке запроса на аутентификацию. Следовательно, в случае шума, повторная передача должна возникать на основе упомянутого короткого тайм–аута, и пользователь должен узнавать гораздо быстрее, когда попытка аутентификации завершена неудачно.

Кроме того, авторы изобретения выявляют то, что такой ответ по аутентификации может быть аналогичным ответу для односторонней аутентификации. Тем не менее,

взаимная аутентификация должна выполняться. Таким образом, помимо этого, вышеуказанный улучшенный ответ по аутентификации дополнительно содержит статус взаимного проведения, указывающий проведение взаимной аутентификации. Кроме того, конечный автомат инициатора выполнен с возможностью предоставлять состояние взаимной аутентификации, активированное при приеме статуса взаимного проведения, для ожидания взаимной аутентификации. Преимущественно, в упомянутом состоянии взаимной аутентификации, устройство–инициатор имеет сведения по взаимной аутентификации, что обеспечивает более поздний прием ответа по взаимной аутентификации, содержащего данные взаимной аутентификации ответчика на основе общедоступного ключа инициатора и конфиденциального ключа ответчика. Затем, в случае успешной обработки принимаемых данных взаимной аутентификации ответчика, инициатор передает подтверждение взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные аутентификации инициатора на основе общедоступного ключа ответчика и конфиденциального ключа инициатора, соответствующего общедоступному ключу инициатора.

Следовательно, посредством предоставления дополнительного состояния взаимной аутентификации и статуса взаимного проведения в первом сообщении с ответом по аутентификации, взаимная аутентификация выполняется без необходимости длительных периодов тайм–аута, в то время как в идентичном протоколе аутентификации, также обеспечивает одностороннюю аутентификацию. Преимущественно, в случае плохих условий для осуществления беспроводной связи, повторная передача требуемых сообщений является относительно быстрой вследствие коротких периодов тайм–аута.

Способ согласно изобретению может реализовываться на компьютере в качестве машинореализуемого способа или в выделенных аппаратных средствах либо в комбинации вышеозначенного. Исполняемый код для способа согласно изобретению может сохраняться на компьютерном программном продукте. Примеры компьютерных программных продуктов включают в себя запоминающие устройства, такие как карта памяти в формате Memory Stick, оптические устройства хранения данных, такие как оптический диск, интегральные схемы, серверы, онлайновое программное обеспечение и т.д. Компьютерный программный продукт может содержать энергонезависимый программный код, сохраненный на машиночитаемом носителе для осуществления способа согласно изобретению, когда упомянутый программный продукт выполняется на компьютере. В варианте осуществления, компьютерная программа содержит средство компьютерного программного кода, выполненное с возможностью осуществлять все этапы или стадии способа согласно изобретению, когда компьютерная программа выполняется на компьютере. Предпочтительно, компьютерная программа осуществляется на машиночитаемом носителе. Предусмотрен компьютерный программный продукт, загружаемый из сети и/или сохраненный на машиночитаемом носителе и/или исполняемом микропроцессором носителе, причем продукт содержит инструкции программного кода для реализации способа, как описано выше, при осуществлении на компьютере.

Другой аспект изобретения предоставляет способ обеспечения доступности компьютерной программы для загрузки, например, включенный в приложение. Этот аспект используется, когда компьютерная программа выгружается, например, в Apple App Store, Google Play Store или Microsoft Windows Store, и когда компьютерная программа доступна для загрузки из такого магазина.

Дополнительные предпочтительные варианты осуществления устройств и способ

согласно изобретению приводятся в прилагаемой формуле изобретения, раскрытие сущности которой содержится в данном документе по ссылке.

Краткое описание чертежей

Эти и другие аспекты изобретения должны становиться очевидными и дополнительно истолковываться со ссылкой на варианты осуществления, описанные в качестве примера в нижеприведенном описании, и со ссылкой на прилагаемые чертежи, на которых:

Фиг. 1 показывает устройства для осуществления беспроводной связи и аутентификации,

Фиг. 2 показывает принципиальную схему протокола аутентификации,

Фиг. 3 показывает пример конечного автомата инициатора,

Фиг. 4 показывает пример конечного автомата ответчика,

Фиг. 5 показывает способ для инициатора,

Фиг. 6 показывает способ для ответчика,

Фиг. 7a показывает машиночитаемый носитель, и

Фиг. 7b показывает схематичное представление процессорной системы.

Чертежи являются просто схематичными и не нарисованы в масштабе. На чертежах, элементы, которые соответствуют уже описанным элементам, могут иметь идентичные номера ссылок.

Подробное описание вариантов осуществления

Используются следующие сокращения:

Состояния:

IST – начальное состояние

BST – самоинициализированное

AG1 – аутентификация (инициатор, односторонняя)

AG2 – взаимная аутентификация (инициатор, взаимная)

ATD – аутентифицированное (инициатор)

AWG – ожидание (ответчик)

AR1 – аутентификация (ответчик, односторонняя)

AR2 – взаимная аутентификация (ответчик, взаимная)

ARD – аутентифицированное (ответчик)

Сообщения:

ARQ – запрос на аутентификацию

ARP – ответ по аутентификации

ACF1 – подтверждение аутентификации (односторонней)

ACF2 – подтверждение взаимной аутентификации

ARP1 – ответ по аутентификации (односторонней)

ARP2 – ответ по взаимной аутентификации

События/действия/статус:

OOB – внеполосное (действие при связи)

OOB_I – внеполосное (действие при связи посредством инициатора)

OOB_R – внеполосное (действие при связи посредством ответчика)

BA – плохая аутентификация (событие)

BTG – самоинициализация (событие)

NP – отсутствуют равноправные устройства (событие)

TO – тайм–аут (событие)

TR – триггер (событие)

MPS – статус взаимного проведения

MAS – статус взаимного ожидания

MCS – статус взаимного подтверждения

Ключи:

B_I – общедоступный самоинициализирующийся ключ инициатора

B_R – общедоступный самоинициализирующийся ключ ответчика

P_I – общедоступный ключ инициатора

P_R – общедоступный ключ ответчика

b_I – конфиденциальный ключ инициатора, соответствующий B_I

b_R – конфиденциальный ключ ответчика, соответствующий B_R

Фиг. 1 показывает устройства для осуществления беспроводной связи и аутентификации. Система 100 для осуществления беспроводной связи содержит устройство–инициатор 110 и устройство–ответчик 120, причем устройства являющиеся физически отдельными. Устройство–инициатор имеет приемопередающее устройство 111 инициатора, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи, и процессор 112 инициатора, выполненный с возможностью обрабатывать протокол связи. Аналогично, устройство–ответчик имеет приемопередающее устройство 121 ответчика, выполненное с возможностью осуществления беспроводной связи согласно протоколу связи, и процессор 122 ответчика, выполненный с возможностью обрабатывать протокол связи. Устройства оснащены для осуществления беспроводной связи, как схематично указано посредством формы 130 и стрелок, которые соединяют приемопередающие устройства 111, 121. Устройство–инициатор может иметь пользовательский интерфейс 113, который может включать в себя известные элементы, к примеру, одну или более кнопок 115, клавиатуру, дисплей, сенсорный экран и т.д. Устройство–ответчик также может иметь пользовательский интерфейс 123. Пользовательский интерфейс ответчика может быть выполнен с возможностью обеспечения пользовательского взаимодействия для выполнения внеполосного действия ответчика, чтобы получать общедоступный ключ инициатора из устройства–инициатора.

Устройства выполнены с возможностью осуществления беспроводной связи согласно протоколу связи между устройством–инициатором и устройством–ответчиком. Устройства выполнены с возможностью выполнения протокола аутентификации для обеспечения аутентификации, представляющей собой одно односторонней аутентификации из устройства–ответчика посредством устройства–инициатора и взаимной аутентификации устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика, причем пример подробно приводится ниже со ссылкой на фиг. 2. Протокол связи может включать в себя протокол аутентификации. В примерах, протокол связи представляет собой Wi–Fi согласно IEEE 802.11 [ссылочный документ 1], но также могут использоваться другие беспроводные протоколы, такие как Bluetooth, при предоставлении с соответствующим протоколом аутентификации на основе системы, как пояснено ниже.

Процессор 112 инициатора имеет модуль 116 сообщений инициатора, чтобы составлять сообщения, которые должны отправляться в устройство–ответчик, и раскладывать сообщения, принимаемые из устройства–ответчика, согласно протоколу аутентификации. Процессор инициатора также имеет конечный автомат 117 инициатора, чтобы предоставлять состояния инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–ответчика, причем пример подробно приводится ниже со ссылкой на фиг. 3.

Процессор 122 ответчика имеет модуль 126 сообщений ответчика, чтобы составлять сообщения, которые должны отправляться в устройство–инициатор, и раскладывать сообщения, принимаемые из устройства–инициатора, согласно протоколу аутентификации. Процессор ответчика также имеет конечный автомат ответчика 127, чтобы предоставлять состояния ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–инициатора.

Ниже пояснена функция процессора инициатора и процессора ответчика для обеспечения протокола аутентификации на основе соответствующих сообщений и соответствующих состояний инициатора и ответчика, с использованием соответствующих модулей сообщений и конечных автоматов, со ссылкой на фиг. 2, 3 и 4.

Для аутентификации, предложенная система может использовать любую форму криптографии с общедоступным ключом, такую как RSA, см. [7], или криптографию в эллиптических кривых (ECC), см. [8].

Фиг. 2 показывает принципиальную схему протокола аутентификации. Согласно протоколу 200 аутентификации, первое устройство INIT_DEV обменивается сообщениями со вторым устройством RESP_DEV, как указано посредством стрелок между двумя вертикальными временными шкалами, представляющими прохождение времени в направлении вниз. Первое устройство может представлять собой устройство–инициатор, запускающееся в IST, и второе устройство может представлять собой устройство–ответчик, запускающееся в AWG, но такие роли могут меняться. Сообщения составляются посредством модуля сообщений на отправляющей стороне и раскладываются посредством модуля сообщений на приемной стороне.

В этом описании, B_I указывает общедоступный самоинициализирующийся ключ инициатора, в то время как b_I указывает соответствующий конфиденциальный ключ. Аналогично, B_R указывает общедоступный самоинициализирующийся ключ ответчика, в то время как b_R указывает соответствующий конфиденциальный ключ. H указывает хеш–функцию, например, на основе соответствующего одностороннего хеш–алгоритма, известного по сути. Подходящие примеры хеш–функций содержатся в ссылочном документе [4].

Хешированное значение общедоступного ключа инициатора указывается посредством $H(B_I)$. Хешированное значение может легко верифицироваться, чтобы соответствовать хеш–защищенному значению, но манипулирование таким значением при поддержании идентичного хеша фактически является невозможным. Аутентификационные данные вычисляются на основе одного или более ключей, соответствующих общедоступных ключей и конфиденциальных ключей, например, указываемых посредством $\{auth1\}_{k1}$, что означает значение auth1, зашифрованного посредством ключа k1, в то время как {auth1} означает значение auth1. Такие ключи формируются, используются для кодирования и декодирования, формирования подписей либо управляющих значений и верификации таких значений, как известно по сути, например, из системы шифрования Диффи–Хеллмана, упомянутой ранее.

Первоначально, устройство–инициатор может выполнять самоинициализацию посредством получения общедоступного ключа ответчика из устройства–ответчика через внеполосное действие инициатора. OOB–действие показано посредством пунктирной стрелки, помеченной как OOB–действие (соответственно, указывается на фиг. 1 посредством стрелки 140). Различные примеры OOB–действий описываются в

ссылочном документе [2]; глава 10. Другие примеры представляют собой пользователя, считывающего код устройства–инициатора и вводящего его в устройство–ответчик, пользователя, снимающего изображение с помощью камеры устройства–инициатора машиночитаемого кода, такого как штрих–код или QR–код, который печатается на или отображается посредством устройства–ответчика.

Затем, модуль сообщений инициатора может составлять запрос ARQ на аутентификацию, который должен отправляться в самоинициализированном состоянии. Запрос на аутентификацию может содержать верификатор $H(B_I)$ инициатора для верификации общедоступного ключа инициатора и верификатор $H(B_R)$ ответчика для верификации общедоступного ключа ответчика. ARQ дополнительно может содержать общедоступный ключ P_I инициатора и дополнительные данные инициатора, такие как одноразовый номер I–nonce инициатора и данные I–capabilities характеристик инициатора, которые могут кодироваться с использованием первого ключа K_1, указываемого посредством $\{I\text{–nonce} \mid I\text{–capabilities}\}_{K1}$. Первый ключ K_1 может извлекаться посредством инициатора способом Диффи–Хеллмана из общедоступного ключа B_R ответчика и конфиденциального ключа p_I инициатора, соответствующего общедоступному ключу P_I инициатора. Первый ключ K_1 может извлекаться посредством ответчика способом Диффи–Хеллмана из общедоступного ключа P_I инициатора и конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу B_R ответчика. Соответственно, модуль сообщений ответчика выполнен с возможностью раскладывать запрос ARQ на аутентификацию.

После тайм–аута TO, когда ответ не принимается, ARQ может передаваться снова, например, вплоть до 3 раз. Предполагается, что ответ ARP1 принимается вовремя.

Модуль сообщений ответчика выполнен с возможностью составлять ответ ARP1 по аутентификации, который может содержать данные $\{R\text{–auth1}\}_{k1}$ односторонней аутентификации ответчика. ARP1 дополнительно может содержать общедоступный ключ P_R ответчика и дополнительные данные ответчика, такие как одноразовый номер R–nonce ответчика. Первый промежуточный ключ k_1 может быть основан на общедоступном ключе P_I инициатора, на конфиденциальном ключе (P_R) ответчика, соответствующем общедоступному ключу (P_R) ответчика (если P_R присутствует в ARP1), и на конфиденциальном ключе (b_R) ответчика, соответствующем общедоступному ключу (B_R) ответчика. Первый промежуточный ключ подходит для односторонней аутентификации устройства–ответчика. Значение R–auth1 может представлять собой (хешированную) конкатенацию любого выбора значений, используемых в протоколе аутентификации, таких как одноразовый номер I–nonce инициатора, одноразовый номер R–nonce ответчика и/или используемые общедоступные ключи, такие как P_R, B_R и P_I. Вследствие случайности одноразовых номеров, значение R–auth1 отличается каждый раз, когда протокол выполняется, за счет этого защищая от атаки с повторением пакетов. В случае взаимной аутентификации, ARP1 также может включать в себя статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора из устройства–инициатора через внеполосное действие ответчика. Соответственно, модуль сообщений инициатора выполнен с возможностью раскладывать ответ ARP1 по аутентификации.

В необязательном порядке, модуль сообщений инициатора выполнен с возможностью составлять, при приеме статуса взаимного проведения в состоянии аутентификации, подтверждение ACF1 ожидания аутентификации, содержащее статус взаимного ожидания. ACF1 может содержать данные $\{I–auth1\}_{k1}$ односторонней аутентификации инициатора на основе общедоступного ключа (B_R) ответчика и конфиденциального ключа (p_I) инициатора, соответствующего общедоступному ключу P_I инициатора. Значение {I–auth1} вычисляется идентично {R–auth1} с использованием идентичных вводов. Тем не менее, значение {I–auth1} должно отличаться от значения {R–auth1}, чтобы защищать от атаки с повторением пакетов. Следовательно, порядок вводов при вычислении хеша должен выбираться по–другому, и/или другое постоянное значение должно быть включено в хеш относительно вычисления хеша для {R–auth1}. Соответственно, модуль сообщений ответчика может быть выполнен с возможностью раскладывать подтверждение ACF1 ожидания аутентификации.

Затем устройство–ответчик может выполнять или уже выполняет получение общедоступного ключа инициатора из устройства–инициатора через внеполосное действие ответчика. OOB–действие показано посредством пунктирной стрелки, помеченной как OOB–действие (соответственно, указывается на фиг. 1 посредством стрелки 140). После выполнения упомянутого получения, конечный автомат ответчика продолжает обработку, как пояснено ниже, для отправки ответа ARP2 по взаимной аутентификации.

Модуль сообщений ответчика выполнен с возможностью составлять ответ ARP2 по взаимной аутентификации, содержащий данные $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика. ARP2 дополнительно может содержать общедоступный ключ P_R ответчика и дополнительные данные ответчика, такие как одноразовый номер R–nonce ответчика.Второй промежуточный ключ k_2 может быть основан на общедоступном ключе (B_I) инициатора и конфиденциальном ключе (b_R) ответчика, соответствующем общедоступному ключу (B_R) ответчика. Второй промежуточный ключ подходит для взаимной аутентификации устройства–ответчика и устройства–инициатора. Второй промежуточный ключ может определяться с использованием $\{b_R, P_R, B_I$ и $P_I\}$ в ответчике или $\{p_I, b_I, B_R$ и $P_R\}$ в инициаторе. Значение R–auth2 может представлять собой хеш конкатенации значений, используемых в протоколе аутентификации, таких как одноразовый номер I–nonce инициатора, одноразовый номер R–nonce ответчика и используемые общедоступные ключи, такие как B_I, B_R, P_R и P_I. Вследствие случайности одноразовых номеров, значение {R–auth2} отличается каждый раз, когда протокол выполняется, за счет этого защищая от атаки с повторением пакетов. Соответственно, модуль сообщений инициатора выполнен с возможностью раскладывать ответ ARP2 по аутентификации. Успешная обработка означает то, что процессор инициатора достигает идентичного значения для k_2, что и ответчик, и то, что инициатор находит идентичное значение для {R–auth2}посредством вычисления непосредственно R–auth2 и посредством дешифрования с помощью ключа k_2 значения $\{R–auth2\}_{k2}$, принимаемого в сообщении ARP2.

Модуль сообщений инициатора выполнен с возможностью составлять подтверждение ACF2 взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора на основе общедоступного ключа (B_R) ответчика и

конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора. Второй промежуточный ключ k_2 может определяться с использованием {p_I, b_I, B_R и P_R} в инициаторе. Значение {I–auth2} вычисляется идентично {R–auth2} с использованием идентичных вводов. Тем не менее, значение {I–auth2} должно отличаться от значения {R–auth2}, чтобы защищать от атаки с повторением пакетов. Следовательно, порядок вводов при вычислении хеша должен выбираться по–другому, и/или другое постоянное значение должно быть включено в хеш относительно вычисления хеша для {R–auth2}. Соответственно, модуль сообщений ответчика выполнен с возможностью раскладывать подтверждение ACF2 взаимной аутентификации. Если ответчик достигает идентичного промежуточного ключа k_2 и получает идентичное значение для данных I–auth2 посредством вычисления непосредственно I–auth2 и посредством дешифрования принимаемого $\{I–auth2\}_{k2}$ с помощью ключа k2, то ответчик аутентифицирует B_I, и обработка данных $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора завершена удачно.

Фиг. 3 показывает пример конечного автомата инициатора. Конечный автомат 300 инициатора предоставляет состояния инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–ответчика. Состояния инициатора могут включать в себя:

– начальное состояние IST для самоинициализации посредством получения общедоступного ключа ответчика из устройства–ответчика через внеполосное действие инициатора;

– самоинициализированное состояние BST, указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика;

– состояние AG1 аутентификации для выполнения аутентификации;

– состояние AG2 взаимной аутентификации для выполнения взаимной аутентификации;

– аутентифицированное состояние ATD, указывающее то, что аутентификация успешно выполнена.

Первоначально, конечный автомат запускается в начальном состоянии IST. Стрелки указывают переходы состояния и помечаются посредством аббревиатуры, указывающей сообщение или событие, соответствующее переходу состояния. Конечный автомат инициатора выполнен с возможностью активировать самоинициализированное состояние BST при успешном выполнении самоинициализации BTG посредством получения общедоступного ключа ответчика.

Конечный автомат инициатора может быть выполнен с возможностью впоследствии активировать состояние аутентификации AG1 при отправке ARQ и/или через инициирующее событие TR пользователем или другое событие, или сразу после упомянутой успешной самоинициализации. После тайм–аута TO, состояние может повторно активироваться после повторной передачи ARQ, при подсчете числа попыток, и после превышения предварительно определенного числа попыток, откатываться к самоинициализированному состоянию BST или к начальному состоянию IST. Состояния BST и AG1 также могут комбинироваться.

Конечный автомат инициатора выполнен с возможностью активировать состояние AG2 взаимной аутентификации, при приеме статуса взаимного проведения в ARP1, для ожидания взаимной аутентификации. В необязательном порядке, может отправляться подтверждение ACF1 ожидания аутентификации, содержащее статус взаимного ожидания.

Конечный автомат инициатора выполнен с возможностью активировать

аутентифицированное состояние ATD при приеме ответа ARP2 по взаимной аутентификации и успешной обработке, посредством процессора инициатора, данных $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора. Затем также может отправляться подтверждение ACF2 взаимной аутентификации, содержащее статус взаимного подтверждения.

В необязательном порядке, конечный автомат инициатора выполнен с возможностью активировать аутентифицированное состояние при приеме ответа по взаимной аутентификации ACF2 в состоянии AG1 аутентификации и успешной обработке, посредством процессора инициатора, данных $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика. Затем также может отправляться подтверждение ACF2 взаимной аутентификации, содержащее статус взаимного подтверждения. Таким образом, эффективно состояние взаимной аутентификации пропускается.

В необязательном порядке, модуль сообщений инициатора выполнен с возможностью раскладывать, в случае односторонней аутентификации, ответ (ARP1) по односторонней аутентификации, содержащий данные $\{R–auth1\}_{k1}$ односторонней аутентификации ответчика на основе конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу B_R ответчика, и статус односторонней аутентификации, указывающий одностороннюю аутентификацию. Кроме того, конечный автомат инициатора выполнен с возможностью активировать аутентифицированное состояние при успешной обработке, посредством процессора инициатора, данных $\{R–auth1\}_{k1}$ односторонней аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа b_I инициатора, соответствующего общедоступному ключу B_I инициатора. Успешная обработка означает то, что процессор инициатора достигает идентичного значения для k_1, что и ответчик, и то, что инициатор находит идентичное значение для {R–auth1}посредством вычисления непосредственно R–auth1 и посредством дешифрования с помощью ключа k_1 значения $\{R–auth1\}_{k1}$, принимаемого в сообщении ARP1.

В необязательном порядке, конечный автомат инициатора выполнен с возможностью активировать самоинициализированное состояние или начальное состояние при приеме ответа ARP1 по аутентификации и неудачной обработке, посредством процессора инициатора, данных $\{R–auth1\}_{k1}$ односторонней аутентификации ответчика. Неудачная обработка может быть обусловлена так называемой плохой аутентификацией BA, либо когда равноправные устройства не обнаружены NP. В таких случаях, конечный автомат инициатора может быть выполнен с возможностью откатываться к самоинициализированному состоянию BST или к начальному состоянию IST, что дополнительно может зависеть от обнаруженного события.

В необязательном порядке, конечный автомат инициатора выполнен с возможностью активировать самоинициализированное состояние или начальное состояние при приеме ответа ARP2 по взаимной аутентификации и неудачной обработке, посредством процессора инициатора, данных $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика. Неудачная обработка может быть обусловлена так называемой плохой аутентификацией BA, либо когда равноправные устройства не обнаружены NP. В таких случаях, конечный автомат инициатора может быть выполнен с возможностью откатываться к

самоинициализированному состоянию BST или к начальному состоянию IST (не показано), что дополнительно может зависеть от обнаруженного события.

Фиг. 4 показывает пример конечного автомата ответчика. Конечный автомат 400 ответчика предоставляет состояния ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–инициатора. Состояния ответчика могут содержать:

– состояние (AWG) ожидания для приема сообщений из инициатора;

– состояние (AR1) аутентификации ответчика для выполнения аутентификации;

– состояние (AR2) взаимной аутентификации ответчика для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора из устройства–инициатора через внеполосное действие ответчика;

– аутентифицированное состояние (ARD) ответчика, указывающее то, что аутентификация успешно выполнена.

Первоначально, конечный автомат ответчика запускается в состоянии AWG ожидания. Состояние может активироваться при пользовательском взаимодействии или любом другом событии, таком как включение устройства–ответчика. Стрелки указывают переходы состояния и помечаются посредством аббревиатуры, указывающей сообщение или событие, соответствующее переходу состояния.

Конечный автомат ответчика может быть выполнен с возможностью активировать состояние AR1 аутентификации ответчика при приеме и успешной обработке запроса ARQ на аутентификацию. Состояния AWG и AR1 также могут комбинироваться в одно состояние.

Неудачная обработка ARQ может означать то, что ответчик определяет то, что верификатор $H(B_R)$ ответчика в принимаемом ARQ не представляет собой хеш своего общедоступного ключа B_R, либо то, что дешифрование $\{I\text{–nonce} \mid I\text{–capabilities}\}_{K1}$ в принимаемом ARQ приводит к ошибке. Пример алгоритма шифрования/дешифрования, который имеет возможность обнаруживать во время дешифрования то, что неправильный ключ используется для дешифрования, либо то, что зашифрованные данные изменены после шифрования, представляет собой AES–SIV, см. [3]. При успешной обработке ARQ, ответ ARP1 по аутентификации, содержащий статус взаимного проведения, указывающий проведение взаимной аутентификации, передается в инициатор.

Конечный автомат ответчика предоставляет и активирует состояние AR2 взаимной аутентификации ответчика при получении, посредством устройства–ответчика, общедоступного ключа инициатора из устройства–инициатора через внеполосное действие ответчика. При упомянутом получении, также ответ ARP2 по взаимной аутентификации отправляется в инициатор.

В необязательном порядке, конечный автомат ответчика выполнен с возможностью принимать и обрабатывать подтверждение ACF1 ожидания аутентификации, содержащее статус взаимного ожидания.

Конечный автомат ответчика в таком случае выполнен с возможностью активировать состояние AR2 взаимной аутентификации ответчика только при приеме статуса взаимного ожидания и упомянутого OOB–действия ответчика. Если ACF1 не принимается в пределах предварительно определенного тайм–аута TO, состояние остается состоянием AR1 аутентификации ответчика, и ARP1 может передаваться снова вплоть до предварительно определенного числа повторений.

Конечный автомат ответчика выполнен с возможностью активировать аутентифицированное состояние ARD ответчика при приеме подтверждения ACF2

взаимной аутентификации и при успешной обработке, посредством процессора ответчика, данных $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора на основе общедоступного ключа B_I инициатора и конфиденциального ключа b_R ответчика.

В необязательном порядке, конечный автомат ответчика выполнен с возможностью активировать аутентифицированное состояние ARD ответчика при приеме подтверждения ACF2 взаимной аутентификации в состоянии AR1 аутентификации ответчика и при успешной обработке, посредством процессора ответчика, данных $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора. Прием ACF2 может возникать при отправке, посредством ответчика непосредственно, при приеме ARQ, ответа ARP2 по взаимной аутентификации в инициатор, например, на основе ответчика, уже обладающего общедоступным ключом инициатора из более раннего сеанса.

В необязательном порядке, модуль сообщений выполнен с возможностью составлять, в случае односторонней аутентификации, ответ ARP1 по односторонней аутентификации, содержащий данные $\{R–auth1\}_{k1}$ односторонней аутентификации ответчика на основе конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу B_R ответчика, и статус односторонней аутентификации, указывающий завершение односторонней аутентификации. Кроме того, конечный автомат ответчика выполнен с возможностью, в случае односторонней аутентификации, активировать аутентифицированное состояние ответчика при приеме подтверждения ACF1 односторонней аутентификации и успешной обработке, посредством процессора ответчика, данных $\{I–auth1\}_{k1}$ односторонней аутентификации инициатора. Успешная обработка означает то, что процессор ответчика достигает идентичного значения для k_1, что и инициатор, и то, что устройство–ответчик находит идентичное значение для I–auth1 посредством вычисления непосредственно I–auth1 и посредством дешифрования с помощью ключа k_1 значения $\{I–auth1\}_{k1}$, принимаемого в сообщении ACF1.

В необязательном порядке, конечный автомат ответчика выполнен с возможностью активировать состояние ожидания при приеме подтверждения ACF2 взаимной аутентификации и неудачной обработке, посредством процессора ответчика, данных $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора, приводя к событию BA плохой аутентификации.

В необязательном порядке, модуль сообщений ответчика выполнен с возможностью дополнительно раскладывать подтверждение ACF1 ожидания аутентификации, содержащее данные $\{I–auth1\}_{k1}$ односторонней аутентификации инициатора и содержащее статус взаимного ожидания. Кроме того, конечный автомат ответчика выполнен с возможностью активировать состояние ожидания при неудачной обработке, посредством процессора ответчика, данных односторонней аутентификации инициатора, приводя к событию BA плохой аутентификации.

В общем, взаимная аутентификация может предусматриваться в протоколе аутентификации, который также указывает одностороннюю аутентификацию. При односторонней аутентификации, (пользователь) ответчик не хочет удостоверяться в том, из какого устройства он принимает запрос на аутентификацию. Ответчик не захватывает общедоступный ключ B_I внеполосного инициатора и в силу этого не может и не отправляет хеш B_I в сообщении с ответом по аутентификации в инициатор. Только односторонняя аутентификация осуществляется, когда ответчик доказывает владение инициатору конфиденциального ключа b_R, который соответствует общедоступному

ключу B_R, который инициатор захватывает внеполосно. Например, посредством использования b_R способом Диффи–Хеллмана, см. ссылочный документ [6], чтобы создавать ключ для шифрования сообщения в инициатор. Такой протокол может использовать две или более пар ключей для каждой стороны, например, одну пару ключей для самоинициализации доверия друг другу и дополнительную пару ключей, из которой общедоступный ключ аутентифицируется для дополнительных операций.

Когда пользователь выполняет действие, которое инициирует выполнение протокола с запросами и ответами по Wi–Fi и дополнительными обменами сообщениями, пользователю не нравится долго ожидать до того, как это действие со всеми обменами завершается. Тем не менее, каждое из сообщений, возможно, не может приниматься посредством другой стороны по ряду причин, например, если сообщение повреждается посредством RF–помех. Таким образом, когда устройство отправляет запрос по Wi–Fi, оно задает таймер для того, чтобы ожидать ответа. Если ответ не поступает в пределах тайм–аута, оно может пытаться отправлять запрос снова. Если ответ не принят после определенного числа попыток, устройство отказывается и сообщает это пользователю. Шансы на успех увеличиваются, когда время ожидания является более длинным, и число разрешенных попыток больше, но пользователь также должен ожидать дольше до получения подтверждения того, что протокол не отрабатывает успешно.

Проблема традиционной взаимной аутентификации состоит в том, что ответчику может требоваться большее количество времени для того, чтобы отвечать сообщением с ответом по аутентификации для взаимной аутентификации, чем в случае односторонней аутентификации, поскольку пользователь устройства–ответчика сначала должен захватывать общедоступный ключ B_I. Кроме того, устройство–инициатор не знает то, хочет устройство–ответчик выполнять аутентификацию или нет. Следовательно, оно должно задавать свое время ожидания и число попыток высоким для того, чтобы предусматривать означенное. Это означает, что в случае, если имеется Wi–Fi–проблема, например, слишком большое количество шума или некоторая другая причина плохих Wi–Fi–переносов между инициатором и ответчиком, устройство–инициатор должно ожидать очень долго до отказа и сообщения этого своему пользователю.

Предложенная система является эффективной, когда возникает пользовательское взаимодействие, требуемое для того, чтобы захватывать общедоступный OOB–ключ B_I инициатора. Примеры такого OOB–действия ответчика являются следующими:

– когда B_I отображается в качестве машиночитаемого кода (например, QR–кода или штрих–кода), и пользователь должен использовать модуль считывания машиночитаемых кодов (такой как камера или лазерный сканер) для того, чтобы считывать B_I;

– когда B_I отображается в человекочитаемой форме, и пользователь должен вводить код в устройстве–ответчике с использованием некоторого устройства ввода (клавиатуры, клавиш, сенсорного дисплея с клавиатурой, отображаемой на нем, мыши и клавиатуры, отображаемых на экране, и т.д.);

– когда B_I переносится с использованием NFC–тега, см. ссылочный документ [5], который пользователь должен приводить в контакт с NFC–модулем считывания для устройства–ответчика, причем NFC–тег с B_I не может использоваться для того, чтобы переносить B_R в устройство–инициатор, одновременно с переносом B_I в устройство–ответчик.

Для разрешения вышеизложенных проблем, в случае если ответчик хочет выполнять взаимную аутентификацию, она сначала создает первый ответ по аутентификации, как

если он хочет выполнять одностороннюю аутентификацию. Он выполняет все криптографические и другие действия, как если он хочет выполнять одностороннюю аутентификацию. Тем не менее, он указывает в своем ответе то, что хочет выполнять взаимную аутентификацию позднее. Этот индикатор может представлять собой специальный статус, например, вместо "статус OK", он может отправлять статус "взаимная аутентификация проводится" в ответе по аутентификации.

При приеме такого ARP, устройство–инициатор должно получать быстрый ответ на свой запрос на аутентификацию, когда отсутствуют Wi–Fi–проблемы. Устройство–инициатор может выполнять проверки для односторонней аутентификации для ответчика, устройства–ответчика для выстраивания доверия с устройством–ответчиком. Выполнение проверок для односторонней аутентификации, например, выполнение проверки целостности для возвращенного статуса с использованием ключа Диффи–Хеллмана, также запрещает взломщикам изменять код статуса "взаимная аутентификация проводится" или другие части сообщения с ответом по аутентификации.

Устройство–инициатор может, при обнаружении отсутствия проблем во всех криптографических проверках для принимаемого ответа по аутентификации, отвечать сообщением подтверждения аутентификации со специальным статусом "ожидание ответа по взаимной аутентификации".

(Пользователь) устройство–ответчик затем может захватывать общедоступный ключ B_I в свободное время и после этого отвечать ответом по взаимной аутентификации, содержащим хеш общедоступного ключа B_I инициатора и дополнительный статус "статус OK".

Далее описывается подробный протокол аутентификации. Протокол обеспечивает возможность использования общедоступных ключей внеполосно (OOB), которые отображаются или переносятся полностью, но не используются как таковые по Wi–Fi. Вместо этого, по Wi–Fi, используются хеш–значения общедоступных OOB–ключей таким образом, что эти общедоступные ключи остаются неизвестными другим, прослушивающим передаваемые Wi–Fi–сообщения. Это является полезным в случае, если OOB–ключи являются статическими. Статические OOB–ключи могут использоваться посредством устройств, которые не имеют средства вывода данных OOB, такого как дисплей для QR–кода. Когда протокол требует от ответчика принимать общедоступный ключ внутриполосно, т.е. по Wi–Fi, инициатор может отправлять дополнительный другой общедоступный ключ P_I по Wi–Fi.

Для переноса общедоступных ключей, возможны альтернативные варианты осуществления. Вместо использования хеша общедоступного ключа по Wi–Fi, могут использоваться другие способы запутывать значение, такие как отображение/отправка только ограниченного числа битов общедоступного ключа. Кроме того, вместо полного значения, хеш общедоступных ключей может отображаться/переноситься OOB. Это имеет в качестве преимущества то, что число битов для того, чтобы отображать или переносить OOB, может быть меньшим, так могут использоваться меньшие QR–коды или меньшие NFC–теги, см. ссылочный документ [5]. В таком случае, полное значение общедоступных ключей должно отправляться внутриполосно, т.е. по Wi–Fi. В этом случае, P_I и B_I могут быть идентичными. Общедоступные ключи могут отображаться/переноситься полностью с использованием OOB и по Wi–Fi.

В примерном протоколе, описанном ниже, общедоступные OOB–ключи отображаются в качестве QR–кода и захватываются посредством камеры, но также возможны другие

варианты осуществления для OOB–канала, см. вышеприведенные примеры.

На первой стадии, пользователь устройства–инициатора хочет устанавливать защищенное соединение между устройством–инициатором и конкретным устройство–ответчик. Пользователь запускает протокол аутентификации на устройстве–инициаторе. Устройство–инициатор использует пары B_I/b_I и P_I/p_I общедоступных ключей или формирует новые пары B_I/b_I и P_I/p_I ключей.

В конкретных вариантах осуществления, устройство–ответчик может активно задаваться в режим ответчика. В других вариантах осуществления, устройство–ответчик задается в режим ответчика, когда оно включается в первый раз или после сброса на заводские значения. Задание R в режим ответчика может инициировать формирование новой пары B_R/b_R общедоступных ключей. Устройство–ответчик должно находиться в режиме ответчика, чтобы участвовать в протоколе. В режиме ответчика, устройство–ответчик может отображать общедоступный ключ B_R для использования в качестве общедоступного ключа или одного из общедоступных ключей в алгоритме Диффи–Хеллмана. B_R может быть статическим и быть напечатан на устройстве–ответчике или в его руководстве. Конфиденциальный ключ, соответствующий B_R, представляет собой b_R. Пара B_R/b_R может формироваться снова для каждого нового выполнения алгоритма Диффи–Хеллмана или для каждого временного интервала в x минут. Отображение B_R может осуществляться в человекочитаемой форме или в машиночитаемой форме (QR–код, штрих–код), либо в обоих формах. Предполагаем машиночитаемый код здесь, который может считываться с помощью камеры.

На второй стадии, пользователь устройства–инициатора инициирует протокол аутентификации и наводит камеру устройства–инициатора на машиночитаемый общедоступный ключ B_R устройства–ответчика и инструктирует устройству–инициатору захватывать его. Конечно, эти пользовательские действия могут требовать времени.

На третьей стадии, устройство–инициатор отправляет запрос на аутентификацию в устройство–ответчик по Wi–Fi посредством адресации устройства–ответчика непосредственно, если устройство–инициатор знает MAC–адрес, либо посредством его широковещательной передачи по Wi–Fi. Запрос на аутентификацию содержит хеш общедоступного ключа B_I устройства–инициатора и хеш общедоступного ключа B_R устройства–ответчика, общедоступный ключ P_I инициатора, который должен использоваться при извлечении ключа Диффи–Хеллмана посредством ответчика, и другую информацию инициатора, например, одноразовый номер инициатора, зашифрованный с помощью ключа k1, который извлекается с использованием алгоритма Диффи–Хеллмана с использованием B_R и p_I. Шифрование может осуществляться с помощью симметричного шифра. Тем не менее, когда используется шифр, который также содержит признак проверки целостности его зашифрованных рабочих данных, а также проверки целостности других незашифрованных частей его рабочих данных, например, AES–SIV (см. ссылочный документ [3]), устройство–ответчик может проверять во время дешифрования "другой информации инициатора" то, формирует оно или нет корректный ключ Диффи–Хеллмана, и то, не изменены либо изменены незашифрованные значения в сообщении, такие как код статуса, посредством взломщика. Если AES–SIV дешифрует без ошибок, устройство–ответчик знает наверняка, что устройство–инициатор использует конфиденциальный ключ, соответствующий P_I, так что устройство–инициатор доказывает владение конфиденциальным ключом,

соответствующим P_I, для устройства–ответчика.

На следующей стадии, ответчик видит Wi–Fi–сообщение с хешем своего общедоступного ключа B_R, так что он знает то, что оно предназначено для него. Он также знает то, что отправитель этого сообщения захватывает B_R со своего дисплея, в частности, когда B_R сформирован снова непосредственно перед этим выполнением протокола аутентификации. Тем не менее, устройство–ответчик не имеет подсказки касательно того, из какого устройства отправитель. Следовательно, (пользователь) устройство–ответчик может хотеть дополнительную аутентификацию и для этого захватывает внеполосно общедоступный ключ B_I устройства–инициатора. Пользователь устройства–ответчика может настраивать свое устройство с возможностью выполнять взаимную аутентификацию. Ответчик далее предоставляет быструю обратную связь в устройство–инициатор, так что устройство–инициатор знает то, что линия Wi–Fi–связи работает, и то, что криптографически все OK на данный момент. Ответное сообщение указывает то, что ответ по взаимной аутентификации должен исходить из устройства–ответчика, но при этом то, что этот ответ может требовать времени (порядка от секунд до десятков секунд). Таким образом, ответчик сразу отвечает сообщением с ответом по аутентификации в инициатор со статусом "взаимная аутентификация проводится", в то время как дополнительные данные в сообщении формируются аналогично ответу по односторонней аутентификации. Второе означает то, что при конструировании этого сообщения, "другая информация инициатора", например, одноразовый номер инициатора, из запроса на аутентификацию дешифруется посредством устройства–ответчика с использованием P_I и b_R и используется при конструировании сообщения с ответом по аутентификации таким образом, что инициатор может проверять то, использует или нет ответчик фактически корректную "другую информацию инициатора", например, одноразовый номер инициатора и за счет этого доказывает владение конфиденциальным ключом b_R, который соответствует общедоступному OOB–ключу B_R ответчика.

Различные способы использовать другую информацию инициатора при конструировании сообщения с ответом по аутентификации включают в себя следующее.

– "Другая информация инициатора" может быть помещена в открытой форме в сообщение.

– "Другая информация инициатора" может быть помещена в открытой форме в сообщение при защите целостности посредством ключа, который извлекается с использованием алгоритма Диффи–Хеллмана, например, посредством использования "другой информации инициатора" в качестве AAD (аутентифицированных ассоциированных данных или аутентифицированных дополнительных данных) с AES–SIV.

– "Другая информация инициатора" может использоваться для того, чтобы извлекать дополнительный ключ, например, посредством извлечения сначала ключа с использованием алгоритма Диффи–Хеллмана и использования ключа Диффи–Хеллмана и "другой информации инициатора" в качестве ввода для функции извлечения ключей. Если такой извлеченный ключ используется с AES–SIV, либо если такой извлеченный ключ используется для того, чтобы шифровать что–то, что известно для инициатора, инициатор может проверять то, знает или нет ответчик корректную "другую информацию инициатора".

В необязательном порядке, поле статуса также может использоваться в качестве

AAD для AES–SIV, так что оно не может несанкционированно изменяться без знания устройства–инициатора относительно этого.

На следующей стадии, инициатор принимает сообщение с ответом по аутентификации. Он выполняет все криптографические проверки и может узнавать то, дешифрует или нет устройство–ответчик корректно "другую информацию инициатора", и в силу этого то, обладает или нет устройство–ответчик конфиденциальным ключом b_R, который соответствует общедоступному OOB–ключу B_R, который устройство–инициатор захватывает с помощью своей камеры из устройства–ответчика. Если эти проверки завершаются неудачно, устройство–инициатор прерывает протокол. Если проверки заканчиваются хорошо, устройство–инициатор проверяет поле статуса. Оно должно наблюдать "проведение взаимной аутентификации". Устройство–инициатор теперь знает то, что оно должно ожидать от нескольких секунд до нескольких десятков секунд для второго ответа из устройства–ответчика.

В необязательном порядке, устройство–инициатор подтверждает корректный прием сообщения с ответом по аутентификации с помощью сообщения подтверждения ожидания аутентификации со статусом, указывающего то, что инициатор ожидает ответа по взаимной аутентификации. Сообщение может конструироваться для односторонней аутентификации.

На следующей стадии, пользователь устройства–ответчика наводит камеру устройства–ответчика на общедоступный ключ B_I, отображаемый посредством устройства–инициатора. Когда хеш такого захваченного общедоступного ключа из устройства–инициатора совпадает с хешем общедоступного ключа устройства–инициатора, принимаемого по Wi–Fi в сообщении с запросом на аутентификацию, устройство–ответчик может быть уверено в том, что оно должно использовать правильный общедоступный ключ для выполнения алгоритма Диффи–Хеллмана с устройством–инициатором. Устройство–ответчик должно знать наверняка, что оно обменивается данными с устройством, из которого оно захватывает B_I, когда позднее в протоколе устройство–инициатор доказывает владение соответствующим конфиденциальным ключом b_I.

На следующей стадии, после захвата общедоступного ключа B_I, устройство–ответчик отвечает устройству–инициатору сообщением ответа по взаимной аутентификации, составляемым в качестве ответа по взаимной аутентификации. Сообщение может содержать статус "взаимная аутентификация OK" или просто "OK", хеш B_I и другую информацию ответчика, зашифрованную с помощью ключей, которые извлекаются с использованием алгоритма Диффи–Хеллмана с использованием общедоступных ключей P_I, принимаемых по Wi–Fi в сообщении с запросом на аутентификацию, и Bi, полученного внеполосно из устройства–инициатора. "Другая информация инициатора", отправленная посредством устройства–инициатора, дешифруется посредством устройства–ответчика, с использованием его конфиденциального ключа b_R и принимаемого общедоступного ключа P_I и используется при конструировании сообщения с ответом по аутентификации, как описано выше, так что устройство–ответчик может доказывать владение b_R для устройства–инициатора. Некоторые отличия от ответа по односторонней аутентификации заключаются в том, что ответчик также использует B_I для того, чтобы извлекать ключ Диффи–Хеллмана и присутствие хеша B_I в ответе.

Предусмотрены различные способы, которыми устройство–ответчик может использовать два общедоступных ключа B_I и P_I из инициатора. Например, ответчик может использовать каждый из этих двух общедоступных ключей вместе с одним или двумя собственными конфиденциальными ключами, чтобы извлекать два ключа Диффи–Хеллмана, k3 и k4.

В первом варианте осуществления, ответчик, например, может извлекать k3 с использованием P_I и своего конфиденциального ключа b_R или нового конфиденциального ключа P_R, или суммы b_R и P_R. В случае если он использует P_R, он должен включать соответствующий общедоступный ключ P_R в ответ по аутентификации таким образом, что инициатор может извлекать его. Это может осуществляться посредством отправки P_R в открытой форме или шифрования с помощью ключа, который инициатор имеет возможность извлекать, например, вышеуказанного ключа k1.

Во втором варианте осуществления, ответчик, например, может извлекать k4 с использованием B_I и своего конфиденциального ключа b_R или нового конфиденциального ключа P_R или суммы b_R и P_R. В случае если он использует P_R, он должен включать соответствующий общедоступный ключ P_R в ответ по аутентификации таким образом, что инициатор может извлекать его. Это может осуществляться посредством отправки P_R в открытой форме или шифрования с помощью ключа, который инициатор имеет возможность извлекать, например, вышеуказанного ключа k1. В случае если сумма двух конфиденциальных ключей используется для k3 или для k4, извлечение других ключей должно использовать не сумму P_R и b_R, а только один из этих ключей. Таким образом, устройство–ответчик имеет возможность доказывать владение конфиденциальными ключами вместо только суммы конфиденциальных ключей b_R и P_R.

В дополнительном варианте осуществления, ответчик может использовать оба ключа k3 и k4, каждый из которых шифрует различное значение, которое инициатор знает, например, одноразовый номер инициатора, так что инициатор может проверять то, знает или нет устройство–ответчик конфиденциальные ключи, которые использует ответчик. Помимо этого, ответчик шифрует собственную "другую информацию ответчика", например, одноразовый номер ответчика, для возможности проверять сообщение подтверждения аутентификации.

В дополнительном варианте осуществления, вместо использования ключей k3 и k4, чтобы шифровать различные значения, один из них, "первый", может использоваться для того, чтобы шифровать первое значение, в то время как другой ключ, "второй ключ", используется для того, чтобы шифровать конкатенацию другого значения и зашифрованного первого значения. Второй ключ должен быть таким, что ответчик может формировать этот ключ. Значения, зашифрованные с помощью второго ключа, могут содержать информацию, требуемую для того, чтобы формировать первый ключ, за счет этого помогая выстраивать доверие.

На следующей стадии, инициатор принимает сообщение с ответом по аутентификации, теперь со статусом "OK". Устройство–инициатор сравнивает хеш в нем с хешем своего общедоступного ключа B_I. Когда они совпадают, устройство–инициатор также знает то, что ответчик устройство–ответчик захватывает свой общедоступный ключ B_I со своего дисплея. Устройство–инициатор формирует все требуемые ключи, для которых

ему требуется конфиденциальный ключ b_I и p_I, выполняет все криптографические проверки. Если все эти проверки представляют собой OK, устройство–инициатор знает то, что оно обменивается данными с устройством, которое обладает конфиденциальным ключом b_R и возможно P_R, если последний также использован, и то, что устройство–ответчик успешно получает корректный B_I.

На следующей стадии, если все проверки на предыдущей стадии представляют собой OK, устройство–инициатор отправляет сообщение ответа с подтверждением в устройство–ответчик со статусом "OK", причем, в числе прочего, используется ключ, который извлекается способом Диффи–Хеллмана из b_I таким образом, что устройство–инициатор может доказывать владение b_I для устройства–ответчика. Устройство–инициатор также использует "другую информацию ответчика", например, одноразовый номер ответчика, так что ответчик видит то, что инициатор удачно дешифрует означенное.

Вышеуказанная система может реализовываться в портативных устройствах, портативных компьютерах, PC, точках Wi–Fi–доступа, равноправных Wi–Fi–устройствах, Bluetooth–устройствах, ZigBee–устройствах. В случае если используется Wi–Fi, изобретение типично реализуется в программном обеспечении Wpa_supplicant, см., например, https://en.wikipedia.org/wiki/wpa_supplicant.

В варианте осуществления, протокол аутентификации между первым и вторым устройством содержит дополнительный атрибут или дополнительное сообщение, которое, например, может добавляться в протокол аутентификации, как задано в IEEE 802.11, см. ссылочный документ [1], содержащее учетные данные (например, общедоступный ключ) или хеш учетных данных, или зашифрованные учетные данные. Второе устройство должно включать в себя такие учетные данные или хеш учетных данных, или зашифрованные учетные данные в качестве части обмена сообщениями для протокола аутентификации. Для симметрии, также первое устройство должно включать в себя такие учетные данные, хеш учетных данных или зашифрованные учетные данные. Предпочтительное поле, содержащее учетные данные или хеш учетных данных, или зашифрованные учетные данные в сообщении протокола аутентификации, представляет собой поле, для которого сигнал или, по меньшей мере, часть сигнала, переносящего это поле, используется для того, чтобы измерять время передачи или время поступления сообщения, так что очень затруднительно, если не невозможно, для другого устройства вставлять свои учетные данные или хеш своих учетных данных, или свои зашифрованные учетные данные в сообщение.

В одном варианте осуществления, первый процессор сообщений выполнен с возможностью обрабатывать эти учетные данные или хеш учетных данных, или зашифрованные учетные данные и верифицировать то, совпадают они или нет с учетными данными, которые ранее использованы посредством устройства, с которым он успешно выполняет аутентификацию устройства и устанавливает взаимное доверие, к примеру, посредством использования протокола защищенного установления Wi–Fi–соединения, протокола подготовки устройств, обмена ключами Диффи–Хеллмана и/или 4–сторонней процедуры установления связи WPA2, см. [1]. Если совпадение найдено, первое устройство может предполагать то, что второе устройство может быть доверенным и считается надежным. Если совпадение не найдено, первое устройство не должно доверять второму устройству и выполнять дополнительные этапы, чтобы верифицировать надежность.

В альтернативном варианте осуществления, второе устройство должно включать в

себя учетные данные или хеш учетных данных, или зашифрованные учетные данные, которые используются во время последующего установления соединения. Первый процессор сообщений выполнен с возможностью обрабатывать и сохранять принимаемые учетные данные или хеш учетных данных, или зашифрованные учетные данные в сочетании с другими параметрами второго устройства, чтобы защищенно коррелироваться с конкретным устройством, которое соединяется с этими учетными данными. При установлении соединения между первым и вторым устройством, первое устройство верифицирует то, используются или нет идентичные учетные данные либо их дериватив при выполнении аутентификации устройства, к примеру, во время выполнения протокола защищенного установления Wi–Fi–соединения, протокола подготовки устройств, обмена ключами Диффи–Хеллмана и/или при выполнении 4–сторонней процедуры установления связи WPA2. За счет этого, первое устройство может определять то, что устройство, с которым оно соединяется, является идентичным устройству, для которого осуществлена более ранняя аутентификация. В частности, если учетные данные представляют собой общедоступный ключ, и если установление соединения между первым и вторым устройством включает в себя то, что второе устройство успешно доказывает первому устройству то, что оно имеет во владении конфиденциальный ключ, принадлежащий общедоступному ключу, в качестве учетных данных, первое устройство может быть уверено, что второе устройство представляет собой то, чем оно притворяется, а не самозванца.

Фиг. 5 показывает способ для инициатора. Способ предназначен для использования в устройстве–инициаторе для осуществления беспроводной связи с устройством–ответчиком согласно протоколу связи и протоколу аутентификации для обеспечения аутентификации. Протокол требует состояний инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–ответчика.

Способ начинается в узле "начало" 501. На первой стадии, способ задает начальное состояние для самоинициализации.

На следующем этапе ACRPK 502, способ активирует получение общедоступного ключа B_R ответчика из устройства–ответчика через внеполосное действие инициатора. При успешном получении B_R, способ, на этапе SARQ 503, активирует самоинициализированное состояние, указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика. Затем способ продолжается посредством составления запроса ARQ на аутентификацию, содержащего верификатор ($H(B_I)$) инициатора для верификации общедоступного ключа инициатора и верификатор ($H(B_R)$) ответчика для верификации общедоступного ключа ответчика. ARQ сообщения отправляется в самоинициализированном состоянии. Затем способ ждет приема ответа по аутентификации. Если не принимается в течение предварительно определенного времени, способ снова отправляет ARQ, как указано посредством стрелки 513.

На следующей стадии RARP1 504, состояние аутентификации для выполнения аутентификации активируется. Затем, способ принимает и раскладывает ответ ARP1 по аутентификации, содержащий примкнутые данные аутентификации ответчика $\{R–auth1\}_{k1}$ на основе конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу B_R ответчика. ARP1 имеет статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора из

устройства–инициатора через внеполосное действие ответчика.

На следующей стадии AWMUT 505, состояние взаимной аутентификации активируется при приеме статуса взаимного проведения для ожидания взаимной аутентификации. Затем, ответ ARP2 по взаимной аутентификации принимается и раскладывается. ARP2 содержит данные $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика на основе общедоступного ключа B_I инициатора и конфиденциального ключа b_R ответчика.

На следующей стадии MUTC 506, активируется аутентифицированное состояние, указывающее то, что аутентификация успешно выполнена. Это заключает в себе прием ответа ARP2 по взаимной аутентификации и успешную обработку данных $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора. Затем способ продолжается посредством составления подтверждения ACF2 взаимной аутентификации, содержащего статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации. ACF2 также содержит данные $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора на основе общедоступного ключа B_R ответчика и конфиденциального ключа b_I инициатора, соответствующего общедоступному ключу B_I инициатора. После этого способ завершается в узле "Конец" 507.

Фиг. 6 показывает способ для ответчика. Способ предназначен для использования в устройстве–ответчике для осуществления беспроводной связи с устройством–инициатором согласно протоколу связи и протоколу аутентификации для обеспечения аутентификации. Протокол требует состояний ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых из устройства–инициатора.

Способ начинается в узле "начало" 601. На первой стадии RARQ 602, ответчик активирует состояние ожидания для приема сообщений из инициатора. Запрос ARQ на аутентификацию принимается и раскладывается. ARQ содержит верификатор $H(B_I)$ инициатора для верификации общедоступного ключа инициатора и верификатор $H(B_R)$ ответчика для верификации общедоступного ключа ответчика.

На следующей стадии SARP1 603, способ активирует состояние аутентификации ответчика для выполнения аутентификации. Состояние аутентификации ответчика активируется при успешной обработке запроса на аутентификацию. После этого составляется ответ ARP1 по аутентификации, содержащий данные $\{R–auth1\}_{k1}$ односторонней аутентификации ответчика на основе конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу B_R ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации.

На следующей стадии MUTA 604, состояние взаимной аутентификации ответчика активируется. Далее (пользователю) ответчику предоставляется возможность получать общедоступный ключ инициатора из устройства–инициатора через внеполосное действие ответчика. Это может требовать времени, как указано посредством стрелки 614, для повторного перехода в состояние. После успешного получения общедоступного ключа инициатора, ответ ARP2 по взаимной аутентификации составляется и отправляется в состоянии взаимной аутентификации ответчика. ARP2 содержит данные $\{R–auth2\}_{k2}$ взаимной аутентификации ответчика на основе общедоступного ключа B_I инициатора и конфиденциального ключа b_R ответчика, соответствующего общедоступному ключу

B_R ответчика.

На следующей стадии WMUC 605, активируется аутентифицированное состояние ответчика, указывающее то, что аутентификация успешно выполнена. Подтверждение ACF2 взаимной аутентификации принимается и раскладывается. ACF2 содержит статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные $\{I–auth2\}_{k2}$ взаимной аутентификации инициатора на основе общедоступного ключа B_R ответчика и конфиденциального ключа b_I инициатора, соответствующего общедоступному ключу (B_I) инициатора. Аутентифицированное состояние активируется при успешной обработке данных взаимной аутентификации инициатора на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика. Далее способ завершается в узле "Конец" 606.

Предусмотрены компьютерные программные продукты, загружаемые из сети и/или сохраненные на машиночитаемом носителе и/или исполняемом микропроцессором носителе, которые содержат инструкции программного кода для реализации вышеописанных способов при осуществлении на компьютере для защиты информации местоположения, как пояснено дополнительно ниже.

Вышеуказанная система может применяться, например, в системах ближней беспроводной связи в помещениях и вне помещений, в которых аутентификация поддерживается через протокол аутентификации. Например, система может применяться в портативных устройствах и стационарных устройствах, поддерживающих стандарт Wi–Fi, стандарт Wi–Fi Aware или стандарт Wi–Fi Direct.

Типично, устройство–инициатор и устройство–ответчик, которые взаимодействуют, содержат процессор, который выполняет соответствующее программное обеспечение, сохраненное в устройствах; например, это программное обеспечение, возможно, загружено и/или сохранено в соответствующем запоминающем устройстве, например, в энергозависимом запоминающем устройстве, таком как RAM, или в энергонезависимом запоминающем устройстве, таком как флэш–память (не показана). Устройства и серверы, например, могут быть оснащены микропроцессорами и запоминающими устройствами (не показаны). Альтернативно, устройства и север могут, полностью или частично, реализовываться в программируемой логике, например, в качестве программируемой пользователем вентильной матрицы (FPGA). Устройства и сервер могут реализовываться, полностью или частично, в качестве так называемой специализированной интегральной схемы (ASIC), т.е. интегральной схемы (IC), специально разработанной для конкретного использования. Например, схемы могут реализовываться в CMOS, например, с использованием языка описания аппаратных средств, такого как Verilog, VHDL и т.д.

Специалистам в данной области техники должно быть очевидным, что возможно множество различных вариантов осуществления способа. Например, порядок стадий этапов может варьироваться, либо некоторые стадии могут выполняться параллельно. Кроме того, между этапами могут вставляться другие этапы способа. Вставленные этапы могут представлять уточнения способа, к примеру, описанного в данном документе, или могут быть не связаны со способом.

Способ согласно изобретению может осуществляться с использованием программного обеспечения, которое содержит инструкции для инструктирования процессорной системе осуществлять соответствующий способ. Программное обеспечение может включать только в себя этапы, осуществляемые посредством конкретного подобъекта системы. Программное обеспечение может сохраняться на подходящем

носителе хранения данных, к примеру, на жестком диске, на дискете, в запоминающем устройстве и т.д. Программное обеспечение может отправляться в качестве сигнала проводным или беспроводным способом либо с использованием сети передачи данных, например, Интернета. Программное обеспечение может становиться доступным для скачивания и/или для удаленного использования на сервере. Способ согласно изобретению может осуществляться с использованием потока битов, выполненного с возможностью конфигурировать программируемую логику, например, программируемую пользователем вентильную матрицу (FPGA), с тем чтобы осуществлять способ. Следует принимать во внимание, что программное обеспечение может иметь форму исходного кода, объектного кода, кода, промежуточного между исходным и объектным кодом, к примеру, частично компилированную форму, либо любую другую форму, подходящую для использования при реализации способа согласно изобретению. Вариант осуществления, связанный с компьютерным программным продуктом, содержит машиноисполняемые инструкции, соответствующие каждому из этапов обработки, по меньшей мере, одного из изложенных способов. Эти инструкции могут подразделяться на подпрограммы и/или сохраняться в одном или более файлов, которые могут быть связаны статически или динамически. Другой вариант осуществления, связанный с компьютерным программным продуктом, содержит машиноисполняемые инструкции, соответствующие каждому из средств, по меньшей мере, одной из изложенных систем и/или продуктов.

Фиг. 7a показывает машиночитаемый носитель 1000, имеющий записываемую часть 1010, содержащую компьютерную программу 1020, причем компьютерная программа 1020 содержит инструкции для инструктирования процессорной системе осуществлять один или более вышеописанных способов в системе, как описано выше. Компьютерная программа 1020 может быть осуществлена на энергонезависимом машиночитаемом носителе 1000 в качестве физических меток либо посредством намагничивания элементов машиночитаемого носителя 1000. Тем не менее, также возможен любой другой подходящий вариант осуществления. Кроме того, следует принимать во внимание, что хотя машиночитаемый носитель 1000 показан здесь в качестве оптического диска, машиночитаемый носитель 1000 может представлять собой любой подходящий машиночитаемый носитель, такой как жесткий диск, полупроводниковое запоминающее устройство, флэш–память и т.д., и может быть незаписываемым или записываемым. Компьютерная программа 1020 содержит инструкции для инструктирования процессорной системе осуществлять упомянутые способы.

Фиг. 7b показывает схематичное представление процессорной системы 1100 согласно варианту осуществления устройства или сервера, как описано выше. Процессорная система может содержать схему 1110, например, одну или более интегральных схем. Архитектура схемы 1110 схематично показана на чертеже. Схема 1110 содержит модуль 1120 обработки, например, CPU, для выполнения компьютерных программных компонентов, чтобы осуществлять способ согласно варианту осуществления и/или реализовывать его модули или блоки. Схема 1110 содержит запоминающее устройство 1122 для сохранения программного кода, данных и т.д. Часть запоминающего устройства 1122 может быть неперезаписываемой. Схема 1110 может содержать элемент 1126 связи, например, антенну, разъемы либо и то, и другое и т.п. Схема 1110 может содержать специализированную интегральную схему 1124 для выполнения части или всей обработки, заданной в способе. Процессор 1120, запоминающее устройство 1122, специализированная IC 1124 и элемент 1126 связи могут соединяться между собой через межкомпонентное соединение 1130, скажем, шину. Процессорная система 1110 может

быть выполнена с возможностью контактной и/или бесконтактной связи, с использованием антенны и/или разъемов, соответственно.

В общих словах, система беспроводной связи может иметь устройство–инициатор и устройство–ответчик, выполненные с возможностью осуществления беспроводной связи. Система беспроводной связи обеспечивает одностороннюю аутентификацию устройства–ответчика посредством устройства–инициатора и взаимную аутентификацию обоих устройств. Варианты осуществления инициатора могут иметь модуль сообщений и конечный автомат. Инициатор запускается посредством получения общедоступного ключа ответчика через внеполосное действие и отправляет запрос на аутентификацию. Ответчик отправляет ответ по аутентификации, содержащий данные аутентификации ответчика на основе конфиденциального ключа ответчика и статус взаимного проведения, указывающий проведение взаимной аутентификации для обеспечения возможности устройству–ответчику получать общедоступный ключ инициатора через внеполосное действие ответчика. Конечный автомат инициатора выполнен с возможностью предоставлять состояние взаимной аутентификации, активированное при приеме статуса взаимного проведения, для ожидания взаимной аутентификации. В силу этого длительные периоды тайм–аута во время беспроводной связи не допускаются при одновременном обеспечении возможности инициатору также сообщать ошибки связи пользователю в течение короткого времени.

Следует принимать во внимание, что для понятности, вышеприведенное описание описывает варианты осуществления изобретения со ссылкой на различные функциональные модули и процессоры. Тем не менее, должно быть очевидным, что любое надлежащее распределение функциональности между различными функциональными модулями или процессорами может быть использовано без отступления от изобретения. Например, функциональность, проиллюстрированная как выполняемая посредством отдельных модулей, процессоров или контроллеров, может быть выполнена посредством одного процессора или контроллера. Следовательно, ссылки на конкретные функциональные модули должны рассматриваться только как ссылки на надлежащее средство предоставления описанной функциональности, а не обозначать точную логическую или физическую структуру либо организацию. Изобретение может реализовываться в любой надлежащей форме, включающей в себя аппаратные средства, программное обеспечение, микропрограммное обеспечение или любую комбинацию вышеозначенного.

Следует отметить, что в этом документе слово "содержащий" не исключает наличия элементов или этапов, отличных от перечисленных элементов или этапов, а упоминание элемента в единственном числе не исключает наличия множества таких элементов, что ссылки с номерами не ограничивают объем формулы изобретения, что изобретение может реализовываться посредством как аппаратных средств, так и программного обеспечения, и что несколько "средств" или "модулей" могут представляться посредством идентичного элемента аппаратных средств или программного обеспечения, и процессор может осуществлять функцию одного или более модулей, возможно совместно с аппаратными элементами. Дополнительно, изобретение не ограничено вариантами осуществления, и изобретение заключается в каждом новом признаке или в комбинации признаков, описанных выше или изложенных во взаимно различных зависимых пунктах формулы изобретения.

Справочные документы:

[1] IEEE Computer Society, "IEEE Standard for Information Technology– Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific

requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications") 802.11–2016), декабрь 2016 года

[2] Wi–Fi Simple Configuration – Technical Specification – Version 2.0.5 "Specification for easy, secure setup and introduction of devices into WPA2–enabled 802.11 networks", Wi–Fi Alliance, 2014 год.

[3] RFC 5297, Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES), октябрь 2008 года, (https://datatracker.ietf.org/doc/rfc5297/)

[4] FIPS180–4, "Secure Hash Standard", United States of America, National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 180–4

[5] NFC Forum Connection Handover Candidate Technical Specification, декабрь 2015 года (http://nfc–forum.org/product/nfc–forum–connection–handover–candidate–technical–specification–version–1–4/)

[6] Diffie, W.; Hellman, M. (1976), "New directions in cryptography", IEEE Transactions on Information Theory, 22 (6): 644–654

[7] Rivest, R.; Shamir, A.; Adleman, L. (февраль 1978 года). "A Method for Obtaining Digital Signatures and Public–Key Cryptosystems", Communications of the ACM. 21 (2): 120–126.

[8] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203–209.

(57) Формула изобретения

1. Устройство–инициатор, выполненное с возможностью осуществления беспроводной связи с устройством–ответчиком согласно протоколу связи,

причем данный протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из:

односторонней аутентификации устройства–ответчика посредством устройства–инициатора и

взаимной аутентификации устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

при этом устройство–ответчик (120) содержит:

приемопередающее устройство ответчика, выполненное с возможностью осуществления беспроводной связи согласно упомянутому протоколу связи, и

процессор ответчика, выполненный с возможностью обработки данного протокола связи,

при этом устройство–инициатор (110) содержит:

приемопередающее устройство (111) инициатора, выполненное с возможностью осуществления беспроводной связи согласно упомянутому протоколу связи,

процессор (112) инициатора, выполненный с возможностью обработки данного протокола связи и имеющий:

модуль (116) сообщений инициатора, чтобы составлять сообщения, которые должны отправляться в устройство–ответчик, и разлагать сообщения, принимаемые от устройства–ответчика, согласно протоколу аутентификации; и

конечный автомат (117) инициатора, чтобы предоставлять состояния инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–ответчика, причем состояния инициатора содержат:

начальное состояние (IST) для самоинициализации посредством получения общедоступного ключа ответчика от устройства–ответчика через внеполосное действие

инициатора,

самоинициализированное состояние (BST), указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика, и

аутентифицированное состояние (ATD), указывающее то, что аутентификация успешно выполнена;

причем модуль сообщений инициатора выполнен с возможностью:

составлять сообщения, содержащие запрос (ARQ) аутентификации, который должен отправляться в самоинициализированном состоянии, содержащий верификатор ($H(B_I)$) инициатора для верификации общедоступного ключа инициатора и верификатор ($H(B_R)$) ответчика для верификации общедоступного ключа ответчика, и

разлагать сообщения, содержащие ответ (ARP1) аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус (MPS) взаимного проведения, указывающий проведение взаимной аутентификации, для обеспечения устройству–ответчику возможности получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика; и

при этом конечный автомат инициатора выполнен с возможностью предоставлять состояние взаимной аутентификации, активированное при приеме статуса взаимного проведения, для ожидания взаимной аутентификации;

модуль сообщений инициатора выполнен с возможностью:

разлагать ответ (ARP2) взаимной аутентификации, содержащий данные ($\{R–auth2\}_{k2}$) взаимной аутентификации ответчика, на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика, и

составлять подтверждение (ACF2) взаимной аутентификации, содержащее статус (MCS) взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные ($\{I–auth2\}_{k2}$) взаимной аутентификации инициатора, на основе общедоступного ключа (B_R) ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора.

2. Устройство–инициатор по п.1, в котором конечный автомат инициатора выполнен с возможностью активировать аутентифицированное состояние при приеме ответа (ARP2) взаимной аутентификации и успешной обработке, посредством процессора инициатора, данных взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора.

3. Устройство–инициатор по п.1, в котором:

модуль сообщений инициатора выполнен с возможностью разлагать, в случае односторонней аутентификации, ответ (ARP1) односторонней аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус односторонней аутентификации, указывающий одностороннюю аутентификацию; и

конечный автомат инициатора выполнен с возможностью активировать аутентифицированное состояние при успешной обработке, посредством процессора инициатора, данных ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика на основе

общедоступного ключа ответчика и конфиденциального ключа (p_I) инициатора, соответствующего общедоступному ключу (P_I) инициатора.

4. Устройство–инициатор по п.2 или 3, в котором конечный автомат инициатора выполнен с возможностью активировать самоинициализированное состояние или начальное состояние при приеме ответа (ARP1) аутентификации и неудачной обработке, посредством процессора инициатора, данных ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика.

5. Устройство–инициатор по п.2, в котором конечный автомат инициатора выполнен с возможностью активировать самоинициализированное состояние или начальное состояние при приеме ответа (ARP2) взаимной аутентификации и неудачной обработке, посредством процессора инициатора, данных ($\{R–auth2\}_{k2}$) взаимной аутентификации ответчика.

6. Устройство–инициатор по п.2 или 5, в котором модуль сообщений инициатора выполнен с возможностью составлять, при приеме статуса взаимного проведения, подтверждение (ACF1) ожидания аутентификации, содержащее статус (MAS) взаимного ожидания.

7. Устройство–ответчик, выполненное с возможностью осуществления беспроводной связи с устройством–инициатором согласно протоколу связи,

причем данный протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из:

односторонней аутентификации устройства–ответчика посредством устройства–инициатора и

взаимной аутентификации устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

при этом устройство–инициатор (110) содержит:

приемопередающее устройство (111) инициатора, выполненное с возможностью осуществления беспроводной связи согласно упомянутому протоколу связи,

процессор (112) инициатора, выполненный с возможностью обработки данного протокола связи, и

при этом устройство–ответчик (120) содержит:

приемопередающее устройство (121) ответчика, выполненное с возможностью осуществления беспроводной связи согласно упомянутому протоколу связи,

процессор (122) ответчика, выполненный с возможностью обработки данного протокола связи и имеющий:

модуль (126) сообщений ответчика, чтобы составлять сообщения, которые должны отправляться в устройство–инициатор, и разлагать сообщения, принимаемые от устройства–инициатора, согласно протоколу аутентификации,

конечный автомат (127) ответчика, чтобы предоставлять состояния ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–инициатора, причем состояния ответчика содержат:

состояние (AWG) ожидания для приема сообщений от инициатора и

аутентифицированное состояние (ATD) ответчика, указывающее то, что аутентификация успешно выполнена;

причем конечный автомат ответчика выполнен с возможностью предоставлять состояние (AR2) взаимной аутентификации ответчика для обеспечения устройству–ответчику возможности получать общедоступный ключ инициатора от

устройства–инициатора через внеполосное действие ответчика; и

причем модуль сообщений ответчика выполнен с возможностью:

составлять сообщения, содержащие ответ (ARP1) аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации, и

разлагать сообщения, содержащие запрос (ARQ) аутентификации, содержащий верификатор ($H(B_I)$) инициатора для верификации общедоступного ключа инициатора и верификатор ($H(B_R)$) ответчика для верификации общедоступного ключа ответчика;

конечный автомат ответчика выполнен с возможностью, при успешной обработке, посредством процессора ответчика, данных ($\{I–auth2\}$) аутентификации инициатора на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика, активировать аутентифицированное состояние ответчика.

8. Устройство–ответчик по п.7, в котором модуль сообщений ответчика выполнен с возможностью:

составлять ответ (ARP2) взаимной аутентификации, который должен отправляться в состоянии взаимной аутентификации ответчика, содержащий данные ($\{R–auth2\}_{k2}$) взаимной аутентификации ответчика, на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и

разлагать подтверждение (ACF2) взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные ($\{I–auth2\}_{k2}$) взаимной аутентификации инициатора, на основе общедоступного ключа (B_R) ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора.

9. Устройство–ответчик по п.7 или 8, в котором:

модуль сообщений ответчика выполнен с возможностью составлять, в случае односторонней аутентификации, ответ (ARP1) односторонней аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус односторонней аутентификации, указывающий одностороннюю аутентификацию; и

конечный автомат ответчика выполнен с возможностью, в случае односторонней аутентификации, активировать аутентифицированное состояние ответчика при приеме подтверждения (ACF1) односторонней аутентификации и успешной обработке, посредством процессора ответчика, данных ($\{I–auth1\}_{k1}$) односторонней аутентификации инициатора.

10. Устройство–ответчик по п.8, в котором конечный автомат ответчика выполнен с возможностью активировать состояние ожидания при приеме подтверждения (ACF2) взаимной аутентификации и неудачной обработке, посредством процессора ответчика, данных ($\{I–auth2\}_{k2}$) взаимной аутентификации инициатора.

11. Устройство–ответчик по п.8 или 10, в котором:

модуль сообщений ответчика выполнен с возможностью разлагать подтверждение

(ACF1) ожидания аутентификации, содержащее статус взаимного ожидания, и

конечный автомат ответчика выполнен с возможностью активировать состояние (AR2) взаимной аутентификации ответчика при приеме статуса взаимного ожидания.

12. Устройство–ответчик по п.11, в котором:

модуль сообщений ответчика выполнен с возможностью дополнительно разлагать подтверждение (ACF1) ожидания аутентификации, содержащее данные ($\{I–auth1\}_{k1}$) односторонней аутентификации инициатора, и

конечный автомат ответчика выполнен с возможностью активировать состояние ожидания при неудачной обработке, посредством процессора ответчика, данных односторонней аутентификации инициатора.

13. Устройство–ответчик по любому из пп.7–12, при этом устройство–ответчик содержит пользовательский интерфейс (123) ответчика, выполненный с возможностью обеспечения пользовательского взаимодействия для выполнения внеполосного действия ответчика, с тем чтобы получать общедоступный ключ инициатора от устройства–инициатора.

14. Система беспроводной связи, содержащая устройство–инициатор (110) по любому из пп.1–6 и устройство–ответчик (120,120') по любому из пп.7–13.

15. Способ инициатора для использования в устройстве–инициаторе (110) для осуществления беспроводной связи с устройством–ответчиком согласно протоколу связи,

причем данный протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из:

односторонней аутентификации устройства–ответчика посредством устройства–инициатора и

взаимной аутентификации устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

при этом способ содержит этапы, на которых:

предоставляют состояния инициатора согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–ответчика, причем состояния инициатора содержат:

начальное состояние для самоинициализации посредством получения общедоступного ключа ответчика от устройства–ответчика через внеполосное действие инициатора,

самоинициализированное состояние, указывающее то, что самоинициализация успешно выполнена посредством получения общедоступного ключа ответчика, и

аутентифицированное состояние, указывающее то, что аутентификация успешно выполнена;

составляют запрос (ARQ) аутентификации, который должен отправляться в самоинициализированном состоянии, содержащий верификатор ($H(B_I)$) инициатора для верификации общедоступного ключа инициатора и верификатор ($H(B_R)$) ответчика для верификации общедоступного ключа ответчика;

разлагают ответ (ARP1) аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации, для обеспечения устройству–ответчику возможности получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика;

предоставляют состояние взаимной аутентификации, активированное при приеме

статуса взаимного проведения, для ожидания взаимной аутентификации;

разлагают ответ (ARP2) взаимной аутентификации, содержащий данные ($\{R–auth2\}_{k2}$) взаимной аутентификации ответчика, на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика;

составляют подтверждение (ACF2) взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные ($\{I–auth2\}_{k2}$) взаимной аутентификации инициатора, на основе общедоступного ключа (B_R) ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора; и

активируют аутентифицированное состояние при приеме ответа (ARP2) взаимной аутентификации и успешной обработке данных взаимной аутентификации ответчика на основе общедоступного ключа ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора.

16. Способ ответчика для использования в устройстве–ответчике для осуществления беспроводной связи с устройством–инициатором согласно протоколу связи,

причем данный протокол связи содержит протокол аутентификации для обеспечения аутентификации, представляющей собой одно из:

односторонней аутентификации устройства–ответчика посредством устройства–инициатора и

взаимной аутентификации устройства–ответчика посредством устройства–инициатора и устройства–инициатора посредством устройства–ответчика;

при этом способ содержит этапы, на которых:

предоставляют состояния ответчика согласно протоколу аутентификации в зависимости от пользовательского взаимодействия и сообщений, принимаемых от устройства–инициатора, причем состояния ответчика содержат:

состояние ожидания для приема сообщений от инициатора и

аутентифицированное состояние ответчика, указывающее то, что аутентификация успешно выполнена;

составляют ответ (ARP1) аутентификации, содержащий данные ($\{R–auth1\}_{k1}$) односторонней аутентификации ответчика, на основе конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика, и статус взаимного проведения, указывающий проведение взаимной аутентификации;

предоставляют состояние (AR2) взаимной аутентификации ответчика для обеспечения устройству–ответчику возможности получать общедоступный ключ инициатора от устройства–инициатора через внеполосное действие ответчика;

составляют ответ (ARP2) взаимной аутентификации, который должен отправляться в состоянии взаимной аутентификации ответчика, содержащий данные ($\{R–auth2\}_{k2}$) взаимной аутентификации ответчика, на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика, соответствующего общедоступному ключу (B_R) ответчика;

разлагают запрос (ARQ) аутентификации, содержащий верификатор ($H(B_I)$) инициатора для верификации общедоступного ключа инициатора и верификатор ($H(B_R)$) ответчика для верификации общедоступного ключа ответчика;

активируют состояние аутентификации ответчика (AG1) при успешной обработке

запроса на аутентификацию.

17. Способ ответчика по п.16, дополнительно содержащий этапы, на которых:

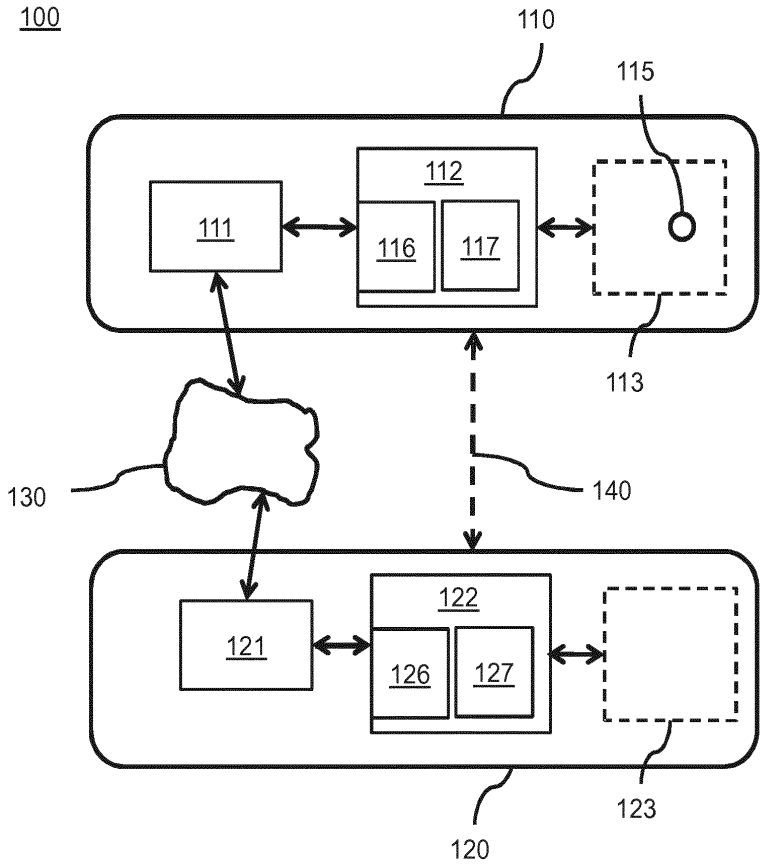
разлагают подтверждение (ACF2) взаимной аутентификации, содержащее статус взаимного подтверждения, указывающий подтверждение взаимной аутентификации, и данные ($\{I–auth2\}_{k2}$) взаимной аутентификации инициатора, на основе общедоступного ключа (B_R) ответчика и конфиденциального ключа (b_I) инициатора, соответствующего общедоступному ключу (B_I) инициатора;

активируют аутентифицированное состояние ответчика при успешной обработке данных взаимной аутентификации инициатора на основе общедоступного ключа (B_I) инициатора и конфиденциального ключа (b_R) ответчика.

18. Машиночитаемый носитель, на котором сохранены инструкции программного кода для реализации способа по п.15 при его исполнении на компьютере.

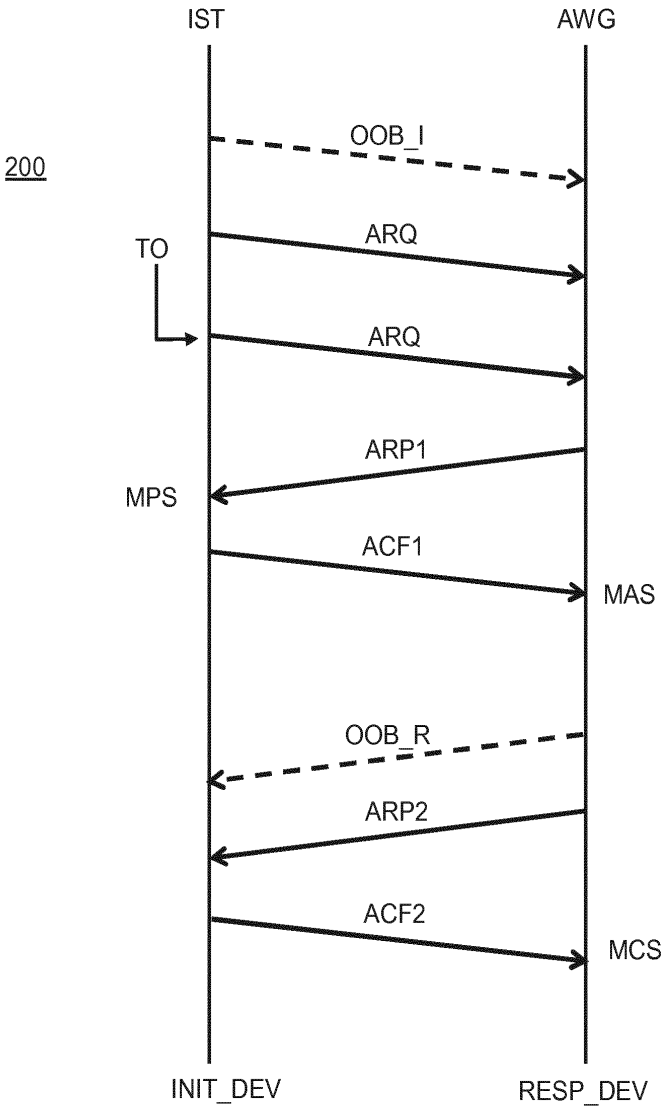
19. Машиночитаемый носитель, на котором сохранены инструкции программного кода для реализации способа по п.16 при его исполнении на компьютере.

1



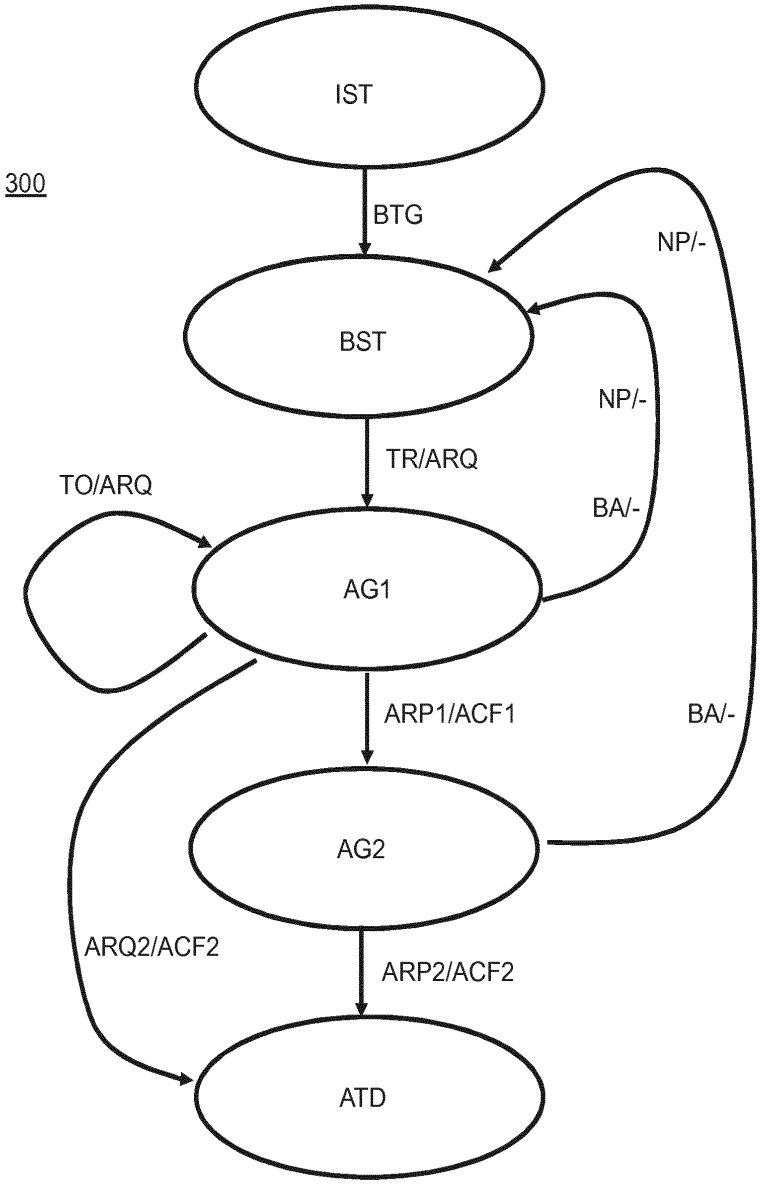
ФИГ. 1

2


IST
AWG
200
OOB_I
TO
ARQ
ARQ
ARP1
MPS
ACF1
MAS
OOB_R
ARP2
ACF2
MCS
INIT_DEV
RESP_DEV

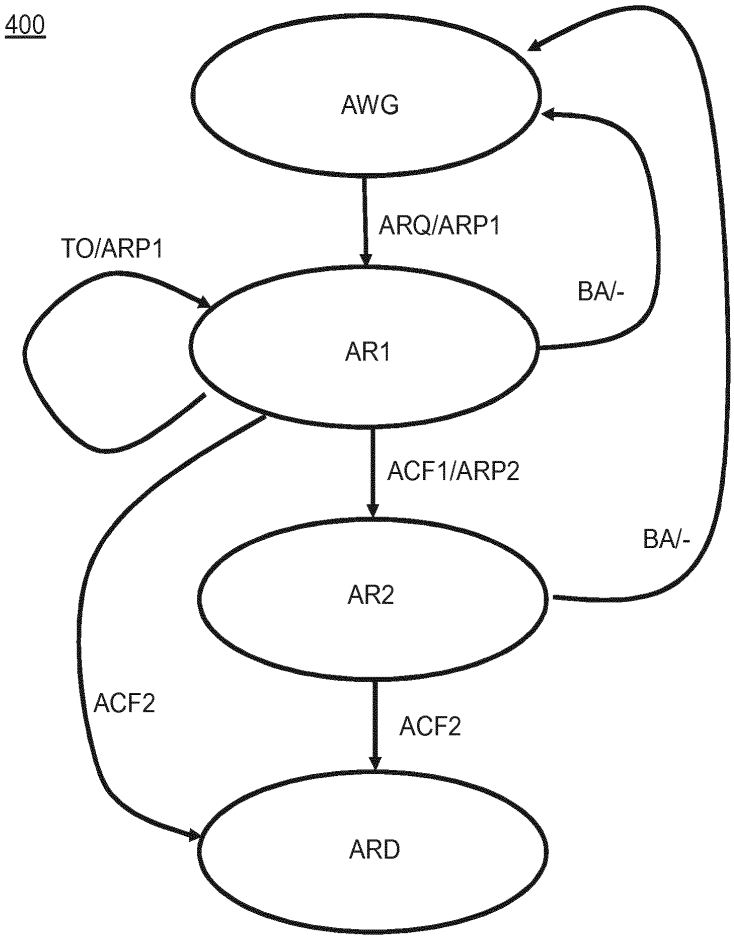
ФИГ. 2

3

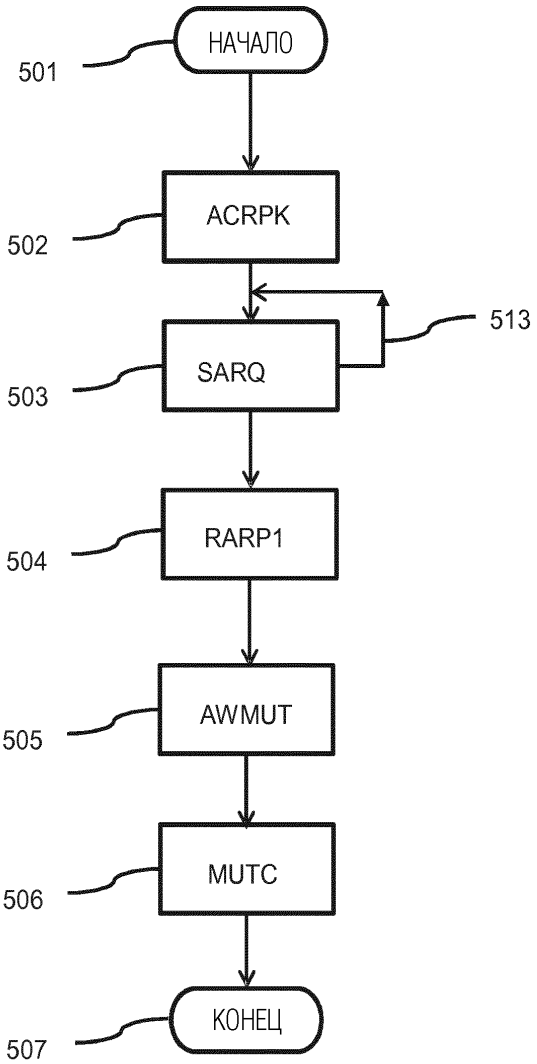

300
IST
BTG
BST
NP/-
NP/-
TR/ARQ
TO/ARQ
BA/-
AG1
ARP1/ACF1
BA/-
AG2
ARQ2/ACF2
ARP2/ACF2
ATD

ФИГ. 3

4

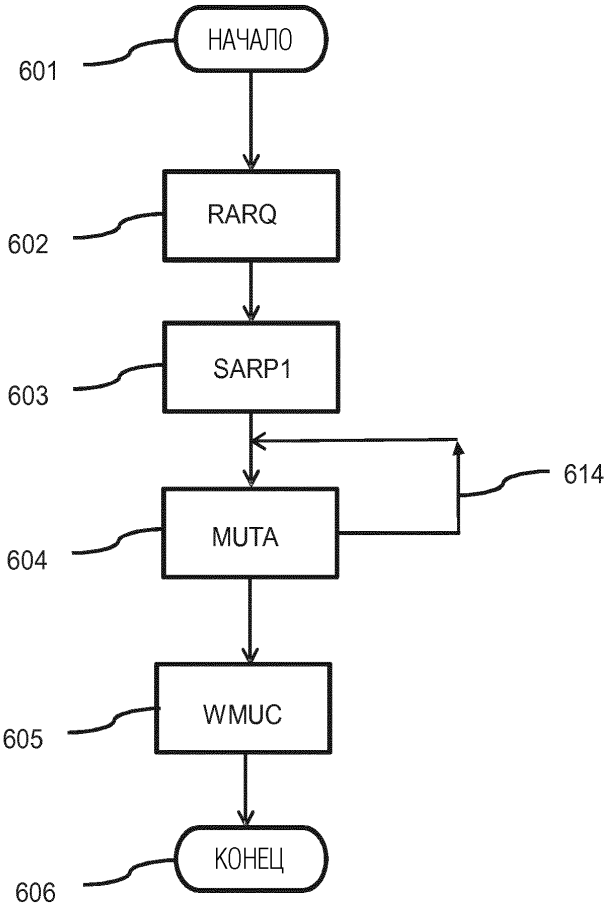


ФИГ. 4


НАЧАЛО
501
ACRPK
502
513
SARQ
503
RARP1
504
AWMUT
505
MUTC
506
КОНЕЦ
507

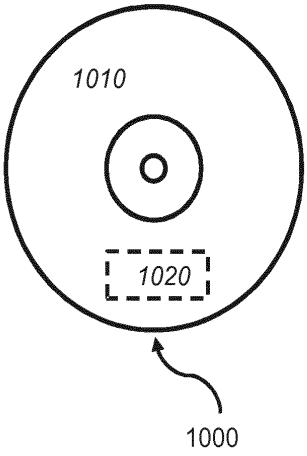
ФИГ. 5

6

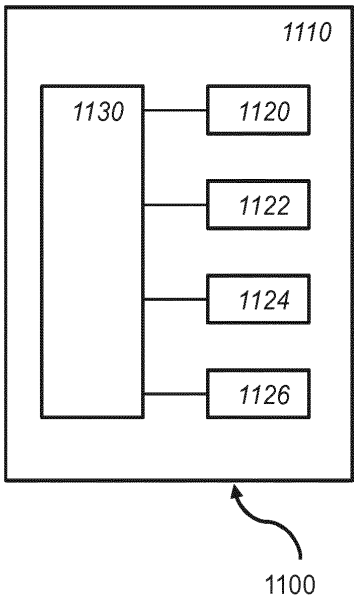


ФИГ. 6

7



ФИГ. 7A



ФИГ. 7B