



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2013102229/08, 02.06.2011

(24) Дата начала отсчета срока действия патента:
02.06.2011

Приоритет(ы):

(30) Конвенционный приоритет:
30.06.2010 CN 201010218676.X

(43) Дата публикации заявки: 27.07.2014 Бюл. № 21

(45) Опубликовано: 10.04.2015 Бюл. № 10

(56) Список документов, цитированных в отчете о
поиске: US 2010/0034539 A1, 11.02.2010. US
2006/0155855 A1, 13.07.2006. US 2001/0009025
A1, 19.07.2001. US 6754470 B2, 22.06.2004. RU
2209528 C2, 27.07.2003

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 17.01.2013

(86) Заявка РСТ:
CN 2011/075201 (02.06.2011)

(87) Публикация заявки РСТ:
WO 2011/144163 (24.11.2011)

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент"

(72) Автор(ы):

ЧЖАН Вэйвэй (CN),
НЕ Гуалянь (CN),
ЦИНЬ Чжунюй (CN)

(73) Патентообладатель(и):

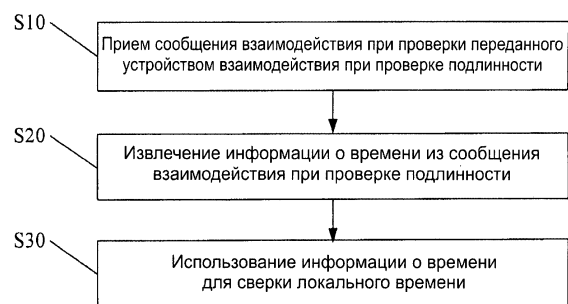
ХУАВЕЙ ТЕКНОЛОДЖИЗ КО., ЛТД.
(CN)

(54) СПОСОБ СВЕРКИ ВРЕМЕНИ И БАЗОВАЯ СТАНЦИЯ

(57) Реферат:

Изобретение относится к области технологий связи и, более конкретно, к способу сверки времени и базовой станции. Технический результат заключается в предотвращении потери ресурсов в базовой станции посредством отсутствия необходимости в установке элемента отсчета времени и аккумулятора, а соответственно и использования ресурсов элементов отсчета времени. Технический результат достигается за счет способа, который включает в себя этапы, на которых: принимают сообщение взаимодействия при проверке подлинности, переданное устройством

взаимодействия при проверке подлинности; извлекают информацию о времени из сообщения взаимодействия при проверке подлинности; и используют информацию о времени для сверки локального времени; до установки соединения IKE по протоколу обмена ключами Интернет между базовой станцией и шлюзом безопасности относительно точное время получают от внешнего устройства взаимодействия для проверки подлинности и используют его для сверки локального времени. 2 н. и 10 з.п. ф-лы, 7 ил.



Фиг. 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) **ABSTRACT OF INVENTION**(21)(22) Application: **2013102229/08, 02.06.2011**(24) Effective date for property rights:
02.06.2011

Priority:

(30) Convention priority:
30.06.2010 CN 201010218676.X(43) Application published: **27.07.2014** Bull. № 21(45) Date of publication: **10.04.2015** Bull. № 10(85) Commencement of national phase: **17.01.2013**(86) PCT application:
CN 2011/075201 (02.06.2011)(87) PCT publication:
WO 2011/144163 (24.11.2011)

Mail address:

109012, Moskva, ul. Il'inka, 5/2, OOO "Sojuzpatent"

(72) Inventor(s):

**ChZhAN Vehjvehj (CN),
NE Gualjan' (CN),
TsIN' Chzhunjuj (CN)**

(73) Proprietor(s):

KhUAVEJ TEKNOLODZhIZ KO., LTD. (CN)(54) **TIME CHECK METHOD AND BASE STATION**

(57) Abstract:

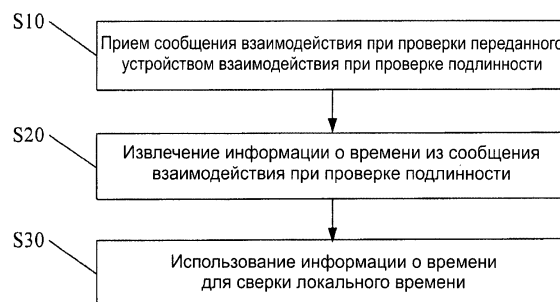
FIELD: radio engineering, communication.

SUBSTANCE: invention relates to communication engineering and more specifically to a time check method and a base station. The technical result is achieved through a method which includes steps of: receiving an authentication interaction message sent by an authentication interaction device; extracting time information from the authentication interaction message; using the time information to check local time; before an internet key exchange (IKE) connection is set up between the base station and a security gateway, relatively accurate time is obtained from an external authentication interaction device and is used for checking the local time.

EFFECT: preventing loss of resources in a base

station by avoiding the need to install a battery and time component and therefore the use of time component resources.

12 cl, 7 dwg



Фиг. 1

Область техники, к которой относится изобретение

Настоящее изобретение относится к области технологий связи и, более конкретно, к способу сверки времени и базовой станции.

Уровень техники

5 Система безопасности в архитектуре безопасности сетей LTE (Long Term Evolution (Долгосрочное Развитие)) разделена на три части: уровень радио, уровень передачи и уровень обслуживания.

Для борьбы со злонамеренным вмешательством в передачу базовая станция (Evolved NodeB (Излучающий Узел В)) использует механизм IPSec (безопасность IP) для
10 гарантирования безопасности, целостности и доступности передачи. Механизм IPSec использует согласование IKE (Internet Key Exchange (протокол обмена ключами Интернет)) для выполнения двунаправленной проверки подлинности между узлами.

В случае, когда присутствует шлюз безопасности, то, когда базовой станции необходимо связаться со шлюзом безопасности посредством IKE, базовая станция
15 сначала загружает файл CRL (Certificate Revocation List (Список Аннулированных Сертификатов)) с сервера CRL и затем использует файл CRL для проверки подлинности цифрового сертификата шлюза безопасности. В процессе проверки подлинности локальное время базовой станции используют как основу для оценки срока действия цифрового сертификата шлюза безопасности.

20 Обычно сервер времени размещен в базовой сети после шлюза безопасности. После установления соединения IKE между базовой станцией и шлюзом безопасности локальное время базовой станции может быть сверено со временем сервера времени базовой сети.

В настоящий момент, когда базовую станцию отключают или она прекращает
25 взаимодействие со шлюзом безопасности на длительное время, то значение времени на базовой станции устанавливают в значение по умолчанию (например, январь 2008 г.). Если время на базовой станции не проверено посредством GPS (Global Positioning System (Глобальная Система Определения Местоположения)), то базовая станция не сможет получить время от сервера времени при соединении со шлюзом безопасности.
30 Следовательно, локальное время базовой станции не будет корректным, и являющийся достоверным цифровой сертификат шлюза безопасности не сможет пройти проверку подлинности, или цифровой сертификат шлюза безопасности с истекшим сроком действия пройдет проверку подлинности, что повлечет за собой угрозу безопасности.

В соответствии с предшествующим уровнем техники данная задача решается
35 установкой на базовой станции элемента отсчета времени, получающего электропитание от аккумулятора. Базовая станция считывает корректное время из элемента отсчета времени, так чтобы оно совпадало с локальным временем.

В процессе разработки настоящего изобретения авторы изобретения нашли, по меньшей мере, следующие недостатки, имеющиеся на предшествующем уровне техники.

40 Решение, в соответствии с предшествующим уровнем техники и описанное выше, требует дополнительной установки элемента отсчета времени и аккумулятора, что увеличивает стоимость. Более того, после соединения базовой станции со шлюзом безопасности и как только она получит адрес сервера времени, она начинает сверку времени через сервер времени и необходимость наличия элемента отсчета времени
45 более не требуется, что ведет к потере ресурсов.

Раскрытие изобретения

В вариантах осуществления настоящего изобретения предложены способ сверки времени и базовая станция, позволяющие базовой станции получать относительно

точное время для проверки времени до соединения с сервером времени и не требующие установки каких-либо элементов отсчета времени.

Способ проверки времени, предлагаемый в варианте осуществления настоящего изобретения, включает в себя:

- 5 прием сообщения взаимодействия для проверки подлинности, отправляемого устройством взаимодействия для проверки подлинности;
- извлечение информации о времени из сообщения взаимодействия для проверки подлинности; и
- использование информации о времени для сверки локального времени.
- 10 Базовая станция, предлагаемая в варианте осуществления настоящего изобретения, включает в себя:
 - блок приема, выполненный с возможностью приема сообщения взаимодействия для проверки подлинности, отправляемого устройством взаимодействия для проверки подлинности;
 - 15 блок извлечения, выполненный с возможностью извлечения информации о времени из сообщения взаимодействия для проверки подлинности; и
 - блок совмещения, выполненный с возможностью использования информации о времени для сверки локального времени базовой станции.

- В соответствии со способом сверки времени и базовой станцией, раскрытыми ниже, перед тем, как будет установлено соединение IKE между базовой станцией и шлюзом безопасности, относительно точное время может быть получено от внешнего устройства взаимодействия для проверки подлинности и использовано для сверки локального времени. Следовательно, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и шлюз
- 25 безопасности будет надежно проверен на подлинность.

Краткое описание чертежей

Фиг.1 - блок-схема, иллюстрирующая способ сверки времени согласно первому варианту осуществления настоящего изобретения.

- Фиг.2 - блок-схема, иллюстрирующая способ сверки времени согласно второму варианту осуществления настоящего изобретения.
- 30

Фиг.3 - блок-схема, иллюстрирующая способ сверки времени согласно третьему варианту осуществления настоящего изобретения.

Фиг.4 - схематическая структурная схема заголовка сообщения отклика на первое FTP-квотирование.

- Фиг.5 - блок-схема, иллюстрирующая способ проверки времени согласно четвертому варианту осуществления настоящего изобретения.
- 35

Фиг.6 - схематическая структурная схема сообщения отклика на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением.

- Фиг.7 - блок-схема, иллюстрирующая базовую станцию согласно варианту осуществления настоящего изобретения.
- 40

Осуществление изобретения

Для того чтобы задачи, признаки и достоинства технических решений по настоящему изобретению стали более понятными, ниже приведено подробное описание вариантов осуществления настоящего изобретения со ссылками на сопроводительные чертежи.

- Первый вариант осуществления
- 45

Как показано на фиг.1, способ сверки времени согласно данному варианту осуществления включает в себя следующие этапы:

S10: прием сообщения взаимодействия для проверки подлинности, отправленного

устройством взаимодействия для проверки подлинности.

Устройством взаимодействия для проверки подлинности может быть сервер CRL, шлюз безопасности и т.д.; и сообщение взаимодействия для проверки подлинности является сообщением, предназначенным для базовой станции, среди других сообщений, передаваемых между устройством взаимодействия для проверки подлинности и базовой станцией перед успешной установкой соединения IKE между базовой станцией и шлюзом безопасности.

S20: извлечение информации о времени из сообщения взаимодействия для проверки подлинности.

В данном варианте осуществления, информация о времени меняется в зависимости от устройства взаимодействия для проверки подлинности и сообщения взаимодействия для проверки подлинности. Например, если устройством взаимодействия для проверки подлинности является сервер CRL и сообщение взаимодействия для проверки подлинности откликом на загрузку, отправленным сервером CRL, то информация о времени является временем обновления файла CRL; в то же время, если устройством взаимодействия для проверки подлинности является сервер CRL и сообщение взаимодействия для проверки подлинности является откликом на первое FTP-квитирование, то информация о времени является текущим временем, установленным на сервере CRL.

S30: использование информации о времени для сверки локального времени.

После того как базовая станция получила относительно точную информацию о времени, может быть сверено локальное время базовой станции, и, следовательно, проверка подлинности шлюза безопасности может быть выполнена надежно и безопасно.

В соответствии со способом проверки времени по настоящему варианту осуществления, перед тем, как будет установлено соединение IKE между базовой станцией и шлюзом безопасности, относительно точное время может быть получено от внешнего устройства взаимодействия для проверки подлинности и использовано для синхронизации локального времени. Следовательно, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и проверка подлинности шлюза безопасности будет надежной.

Второй вариант осуществления

Как показано на фиг.2, способ сверки времени согласно данному варианту осуществления включает в себя следующие этапы:

S101: базовая станция принимает отклик на загрузку от сервера CRL.

Перед проверкой подлинности шлюза безопасности базовой станции необходимо получить файл CRL. Следовательно, после завершения FTP-квитирования с сервером CRL, базовая станция отправляет запрос на загрузку серверу CRL. Сервер CRL отправляет базовой станции отклик на загрузку, содержащий файл CRL.

S102: базовая станция извлекает время обновления из файла CRL, содержащимся в отклике на загрузку.

Файл CRL включает в себя поле времени, и сервер CRL периодически обновляет файл CRL. Период обновления является достаточно коротким (обычно, несколько часов). Данное относительно точное время соответствует требованиям к проверке подлинности в базовой станции. Поскольку срок действия цифрового сертификата шлюза безопасности не является настолько коротким, как несколько часов, проверка подлинности цифрового сертификата шлюза безопасности будет гарантировано точной до тех пор, пока разница во времени для полученного файла CRL и фактическим текущим

временем меньше, чем срок действия цифрового сертификата шлюза безопасности. Следовательно, информация в поле времени файла CRL может быть использована для сверки времени базовой станции, и локальное время в базовой станции может быть синхронизировано с относительно точным временем.

Ниже приведен пример структуры файла CRL. В данной структуре поле "thisUpdate" указывает на дату обновления файла CRL (файл CRL обновляется периодически и данное поле времени указывает на время обновления).

```
typedef struct stCRLInfo
```

```
{
```

```
SEC_AsnInt* pVersion/*если присутствует, ДОЛЖНО иметь значение v2*/
```

```
SEC_ALG_IDENTIFIER_S* pstSignatureAlgo /*Поле signatureAlgorithm содержит  
идентификатор алгоритма, используемого издателем CRL для подписи CertificateList*/
```

```
SEC_NAME_S* issuer /*Поле определяет субъект, подписавший и издавший CRL*/
```

```
SEC_TIME_S* thisUpdate /*Данное поле указывает на дату выпуска данного CRL*/
```

```
SEC_TIME_S* nextUpdate /*Данное поле указывает на дату следующего обновления  
данного CRL. Является необязательным*/
```

```
X509_REVOKED_LIST* revokedCertificates /*Список аннулированных сертификатов  
узлов. Является необязательным*/
```

```
Extensions* crlExtensions /*Формат X.509 v2 CRL также позволяет различным  
сообществам определять свои расширения для передачи информации, уникальной для  
данного сообщества. Является необязательным*/
```

```
} X509_CRLINFO_S;
```

S103: базовая станция использует время обновления для сверки локального времени.

После успешной установки соединения IKE между базовой станцией и шлюзом безопасности базовая станция получает адрес сервера времени от системы управления сетью, прекращает сверку локального времени базовой станции с использованием файла CRL и осуществляет сверку времени с сервером времени.

Способ сверки согласно данному варианту осуществления использует существующие сообщения и процедуры, которые не требуют изменения в существующих сообщениях и процедурах, что делает его простым для реализации.

В данном варианте осуществления способа сверки времени, время обновления извлекают из файла CRL, принятого от сервера CRL как отклик на запрос загрузки. Следовательно, базовая станция получает относительно точное время для сверки локального времени перед установкой успешного соединения IKE между базовой станцией и шлюзом безопасности. Таким образом, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и проверка подлинности шлюза безопасности будет надежной.

Третий вариант осуществления

Как показано на фиг.3, способ сверки времени согласно данному варианту осуществления включает в себя следующие этапы:

S201: базовая станция принимает отклик на первое FTP-квитирование от сервера CRL. Отклик на первое FTP-квитирование содержит текущее время.

Перед тем, как базовая станция получит файл CRL от сервера CRL, ей необходимо установить соединение с сервером CRL по протоколу FTP посредством трех запросов FTP-квитирования. Сначала базовая станция отправляет первый запрос FTP-квитирования на сервер CRL. После приема первого запроса FTP-квитирования сервер CRL возвращает базовой станции отклик на первый запрос FTP-квитирования. Первый отклик FTP-квитирования также содержит второй запрос FTP-квитирования сервера

CRL. После приема второго запроса FTP-квитирования базовая станция возвращает отклик на второй запрос FTP-квитирования серверу CRL и после этого устанавливает соединение FTP с сервером CRL.

5 Время на сервере CRL может считаться относительно точным. Следовательно, от сервера CRL может быть получено относительно точное время. В данном варианте осуществления отклик на первое FTP-квитирование содержит текущее время сервера CRL. На практике поле времени может быть добавлено в структуру сообщения отклика на FTP-квитирование. Например, на фиг.4 показан заголовок сообщения, и поле времени может быть расположено в заголовке сообщения отклика на первое FTP-квитирование. 10 Конкретное местоположение поля времени ничем не ограничено и может быть установлено в соответствии с конкретным способом применения, однако поле времени должно быть расположено в заголовке сообщения отклика на первое FTP-квитирование. Поле времени может иметь любой формат, если с помощью него можно передать текущее время сервера CRL. Текущее время также может быть передано в 15 неиспользуемом поле, содержащемся в структуре сообщения отклика на первое FTP-квитирование.

S202: базовая станция извлекает текущее время из отклика на первое FTP-квитирование.

S203: базовая станция использует текущее время для сверки локального времени. 20 После установки успешного соединения IKE между базовой станцией и шлюзом безопасности базовая станция получает адрес сервера времени от системы управления сетью и сверяет время с сервером времени.

В данном варианте осуществления способа сверки времени, отклик на первое FTP-квитирование содержит текущее время сервера CRL. Следовательно, базовая станция 25 получает относительно точное время для сверки локального времени перед установкой успешного соединения IKE между базовой станцией и шлюзом безопасности. Таким образом, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и проверка подлинности шлюза безопасности будет надежной.

30 Четвертый вариант осуществления

Как показано на фиг.5, способ сверки времени согласно данному варианту осуществления включает в себя следующие этапы:

S301: базовая станция принимает отклик на взаимодействие первой стадии, передаваемый шлюзом безопасности. Отклик на взаимодействие первой стадии содержит 35 текущее время.

Установка соединения IKE между базовой станцией и шлюзом безопасности происходит в две стадии. Первую стадию используют для согласования параметров IKE SA (Security Association (Безопасная Ассоциация)) канала связи, проверки подлинности канала связи и обеспечения безопасности, а также для службы проверки 40 подлинности источника сообщения и проверки целостности сообщения при дальнейшем осуществлении связи IKE между двумя сторонами. На второй стадии настраивают IPSec SA на основе существующего IKE SA.

Шлюз безопасности соединен с сервером времени и время на шлюзе безопасности является точным. Следовательно, от сервера безопасности можно получить корректное 45 время. Поскольку вторую стадию выполняют при условии прохождения шлюзом безопасности проверки подлинности в базовой станции, в данном варианте осуществления отклик взаимосвязи на первой стадии содержит текущее время шлюза безопасности.

Первая стадия содержит три сообщения: запрос на обмен согласования политики обмена, отклик на обмен в виде совместно используемого значения по алгоритму Диффи-Хеллмана и одноразового значения и отклик на обмен достоверности проверки подлинности. Отклик на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением может содержать текущее время шлюза безопасности. Следовательно, отклик на взаимодействия первой стадии может быть откликом обмена значением по алгоритму Диффи-Хеллмана и одноразовым значением.

Фактически, в структуру сообщения отклика на взаимодействие первой стадии может быть добавлено поле времени, содержащее текущее время шлюза безопасности.

Например, на фиг.6 показана структура сообщения отклика на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением. Поле времени может быть добавлено в отклик на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением. Конкретное расположение поля времени ничем не ограничено до тех пор, пока оно содержится в отклике на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значения. Расположение поля времени может быть установлено в зависимости от конкретного применения, и поле времени может иметь любой формат, в котором присутствует текущее время шлюза безопасности. Текущее время также может быть передано в неиспользуемом поле структуры сообщения отклика на взаимодействие первой стадии.

S302: базовая станция извлекает текущее время из отклика на взаимодействие первой стадии.

S303: базовая станция использует текущее время для сверки локального времени.

После установки успешного соединения IKE между базовой станцией и шлюзом безопасности базовая станция получает адрес сервера времени от системы управления сетью и сверяет время с сервером времени.

В данном варианте осуществления способа сверки времени, отклик на взаимодействие первой стадии содержит текущее время шлюза безопасности. Следовательно, базовая станция получает относительно точное время для синхронизации локального времени перед установкой успешного соединения IKE между базовой станцией и шлюзом безопасности. Таким образом, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и проверка подлинности шлюза безопасности будет надежной.

Пятый вариант осуществления

Как показано на фиг.7, базовая станция, согласно данному варианту осуществления, включает в себя: блок 10 приема, блок 20 извлечения и блок 30 совмещения.

Блок 10 приема выполнен с возможностью приема сообщения взаимодействия для проверки подлинности, отправленного устройством взаимодействия для проверки подлинности.

Устройством взаимодействия для проверки подлинности может быть сервер CRL, шлюз безопасности и т.д.; сообщение взаимодействия для проверки подлинности является сообщением, предназначенным для базовой станции, среди других сообщений взаимодействия между устройством взаимодействия для проверки подлинности и базовой станцией перед успешной установкой соединения IKE между базовой станцией и шлюзом безопасности.

Блок 20 извлечения выполнен с возможностью извлечения информации о времени из сообщения взаимодействия для проверки подлинности.

Информация о времени различается в зависимости от устройства взаимодействия

для проверки подлинности и сообщения взаимодействия для проверки подлинности. Например, если устройством взаимодействия для проверки подлинности является сервер CRL и сообщение взаимодействия для проверки подлинности является откликом на загрузку, отправленным сервером CRL, то информацией о времени является время обновления файла CRL; в то же время, если устройством взаимодействия для проверки подлинности является шлюз безопасности и сообщением взаимодействия для проверки подлинности является отклик на взаимодействие первой стадии, то информацией о времени является текущее время шлюза безопасности.

Блок 30 совмещения выполнен с возможностью использования информации о времени для сверки локального времени базовой станции.

Опционально, блок 10 приема включает в себя первый модуль приема, выполненный с возможностью приема отклика на загрузку, отправляемого сервером CRL; и блок 20 извлечения включает в себя первый модуль извлечения, выполненный с возможностью извлечения, в качестве информации о времени, времени обновления файла CRL, содержащегося в отклике на загрузку.

Опционально, блок 10 приема включает в себя второй модуль приема, выполненный с возможностью приема отклика на первое FTP-квитирование, отправленного сервером CRL, где отклик на первое FTP-квитирование содержит текущее время; и блок 20 извлечения включает в себя второй модуль извлечения, выполненный с возможностью извлечения, в качестве информации о времени, текущего времени, содержащегося в отклике на первое FTP-квитирование.

Опционально, блок 10 приема включает в себя третий модуль приема, выполненный с возможностью приема отклика на взаимодействие первой стадии, отправленного шлюзом безопасности, где отклик на взаимодействие первой стадии содержит текущее время; и третий модуль приема, в частности, выполнен с возможностью принимать отклик на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением. Блок 20 извлечения включает в себя третий модуль извлечения, выполненный с возможностью извлечения, в качестве информации о времени, текущего времени, содержащегося в отклике на взаимодействие первой стадии.

После установки успешного соединения IKE между базовой станцией и шлюзом безопасности базовая станция получает адрес сервера времени от системы управления сетью и сверяет время с сервером времени.

В данном варианте осуществления, базовая станция получает от устройства взаимодействия для проверки подлинности относительно точное время для сверки локального времени перед установкой успешного соединения IKE между базовой станцией и шлюзом безопасности. Таким образом, можно избежать затрат на установку элемента отсчета времени и аккумулятора, при этом время на базовой станции будет достоверным и проверка подлинности шлюза безопасности будет надежной.

Специалистам в данной области техники должно быть понятно, что все или часть этапов способа согласно вышеприведенным вариантам осуществления могут быть реализованы с помощью программы для соответствующего оборудования. Программа может храниться на машиночитаемом носителе данных, например ПЗУ/ОЗУ (ROM/RAM), магнитном диске или CD-ROM. Работа программы включает в себя выполнение следующих этапов: прием сообщения взаимодействия для проверки подлинности, отправленного устройством взаимодействия для проверки подлинности; извлечение из сообщения взаимодействия для проверки подлинности информации о времени; и использование информации о времени для сверки локального времени.

В приведенном описании, термины "первый" и "второй" использованы для отличия

одного элемента или действия от другого и не обязательно означают какое-либо практическое взаимоотношение элементов или порядок действий. Кроме того, термины "включает в себя", "содержит" и любые их варианты означают "включает в себя, но этим не ограничено". Следовательно, в случае процесса, способа, предмета или устройства, включающих в себя набор элементов, процесс, способ, предмет или устройство включают в себя не только данные элементы, но также включают в себя другие элементы, которые не указаны явно или могут включать в себя элементы, присущие процессу, способу, предмету или устройству. Если не указано обратное, контекст терминов "включает в себя" или "содержит" подразумевает, что процесс, способ, предмет или устройство, которые включают в себя или содержат некоторые элементы, могут включать в себя другие подобные элементы.

Вышеприведенное описание является лишь иллюстрацией предпочтительных вариантов осуществления, которыми не ограничен объем настоящего изобретения. Любые модификации, эквивалентные замены или улучшения, сделанные в соответствии с идеей и принципами настоящего изобретения, попадают под объем настоящего изобретения.

Формула изобретения

1. Способ сверки времени, содержащий этапы, на которых:
 - принимают с помощью базовой станции сообщение взаимодействия при проверке подлинности, переданное устройством взаимодействия при проверке подлинности, при этом сообщение взаимодействия при проверке подлинности принято до установки протокола обмена ключами Интернет (IKE) безопасной ассоциации (SA) между базовой станцией и шлюзом безопасности и содержит информацию о времени;
 - извлекают с помощью базовой станции информацию о времени из сообщения взаимодействия при проверке подлинности; и
 - используют информацию о времени для сверки локального времени для установки указанного IKE SA между базовой станцией и шлюзом безопасности.
2. Способ по п. 1, в котором устройством взаимодействия при проверке подлинности является сервер списка отозванных сертификатов (CRL), сообщением взаимодействия при проверке подлинности является отклик загрузки, а информацией о времени является время обновления файла CRL.
3. Способ по п. 2, в котором
 - этап приема содержит этап, на котором:
 - принимают базовой станцией отклик загрузки, переданный сервером CRL; а этап извлечения содержит этап, на котором:
 - извлекают базовой станцией время обновления файла CRL, являющегося откликом загрузки.
4. Способ по п. 1, в котором устройством взаимодействия при проверке подлинности является сервер списка отозванных сертификатов (CRL), сообщением взаимодействия при проверке подлинности является отклик на первое FTP-квитирование по протоколу передачи файлов (FTP), а информацией о времени является текущее время сервера CRL.
5. Способ по п. 4, в котором
 - этап приема содержит этап, на котором:
 - принимают базовой станцией отклик на первое FTP-квитирование, переданный сервером CRL, причем отклик на первое FTP-квитирование содержит текущее время, а этап извлечения содержит этап, на котором:
 - извлекают базовой станцией текущее время сервера CRL из отклика на первое FTP-

квितिование.

6. Способ по п. 1, в котором устройством взаимодействия при проверке подлинности является шлюз безопасности, сообщением взаимодействия при проверке подлинности является отклик на взаимодействие первой стадии, а информацией о времени является

5 текущее время шлюза безопасности.

7. Способ по п. 6, в котором

этап приема содержит этап, на котором:

принимают базовой станцией отклик на взаимодействие первой стадии, переданный шлюзом безопасности, причем отклик на взаимодействие первой стадии содержит

10 текущее время; а

этап извлечения содержит этап, на котором:

извлекают базовой станцией текущее время из отклика на взаимодействие первой стадии.

8. Способ по п. 6 или 7, в котором

15 отклик на взаимодействие первой стадии является откликом на обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением, при этом обмен совместно используемым значением по алгоритму Диффи-Хеллмана и одноразовым значением содержит обмен текущим временем шлюза безопасности.

9. Базовая станция, содержащая:

20 блок приема, выполненный с возможностью приема сообщения взаимодействия при проверке подлинности, передаваемого устройством взаимодействия при проверке подлинности, при этом сообщение взаимодействия при проверке подлинности принято до установки протокола обмена ключами Интернет (IKE) безопасной ассоциации (SA) между базовой станцией и шлюзом безопасности и содержит информацию о времени;

25 блок извлечения, выполненный с возможностью извлечения указанной информации о времени из сообщения взаимодействия при проверке подлинности; и

блок совмещения, выполненный с возможностью использования информации о времени для сверки локального времени для установки указанного IKE SA между базовой станцией и шлюзом безопасности.

30 10. Базовая станция по п. 9, в которой

блок приема содержит первый модуль приема, выполненный с возможностью приема базовой станцией отклика загрузки, передаваемого сервером списка отозванных сертификатов (CRL); а

35 блок извлечения содержит первый модуль извлечения, выполненный с возможностью извлечения времени обновления из файла CRL, который является откликом загрузки, при этом информация о времени является временем обновления файла CRL.

11. Базовая станция по п. 9, в которой

40 блок приема содержит второй модуль приема, выполненный с возможностью приема отклика на первое FTP-квитиование по протоколу передачи файлов (FTP), переданного сервером списка отозванных сертификатов (CRL), причем отклик на первое FTP-квитиование содержит текущее время сервера CRL; а

блок извлечения содержит второй модуль извлечения, выполненный с возможностью извлечения текущего времени из отклика на первое FTP-квитиование, при этом информация о времени является текущим временем сервера CRL.

45 12. Базовая станция по п. 9, в которой

блок приема содержит третий модуль приема, выполненный с возможностью приема отклика на взаимодействие первой стадии, передаваемого шлюзом безопасности, при этом отклик на взаимодействие первой стадии содержит текущее время шлюза

безопасности; а

блок извлечения содержит третий модуль извлечения, выполненный с возможностью извлечения текущего времени из отклика на взаимодействие первой стадии, при этом отклик на взаимодействие первой стадии содержит текущее время шлюза безопасности.

5

10

15

20

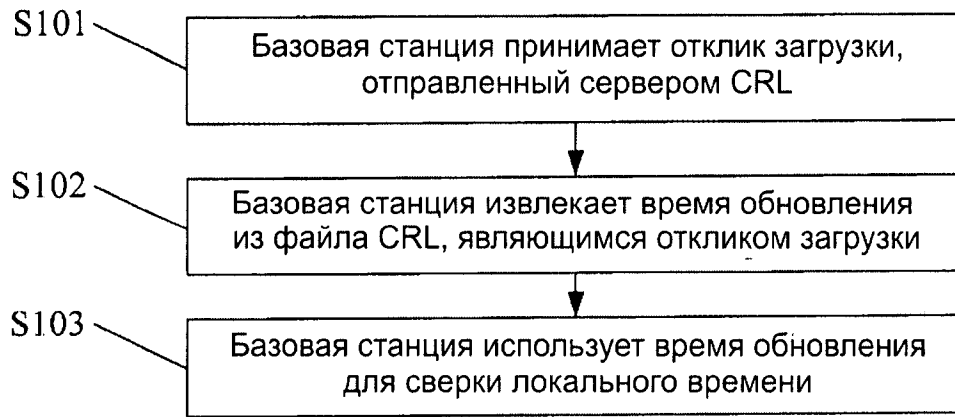
25

30

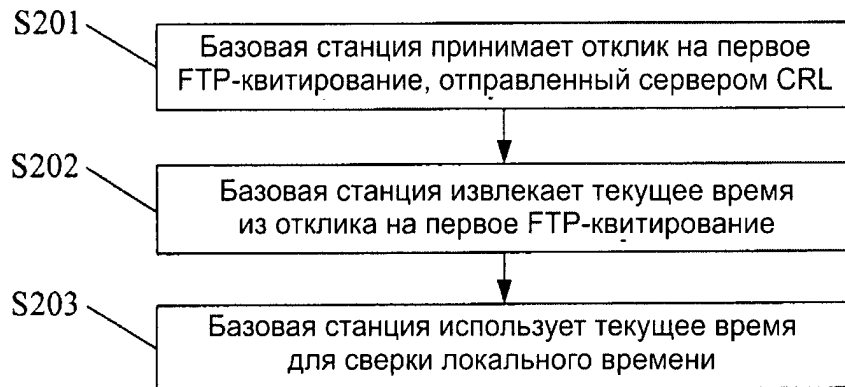
35

40

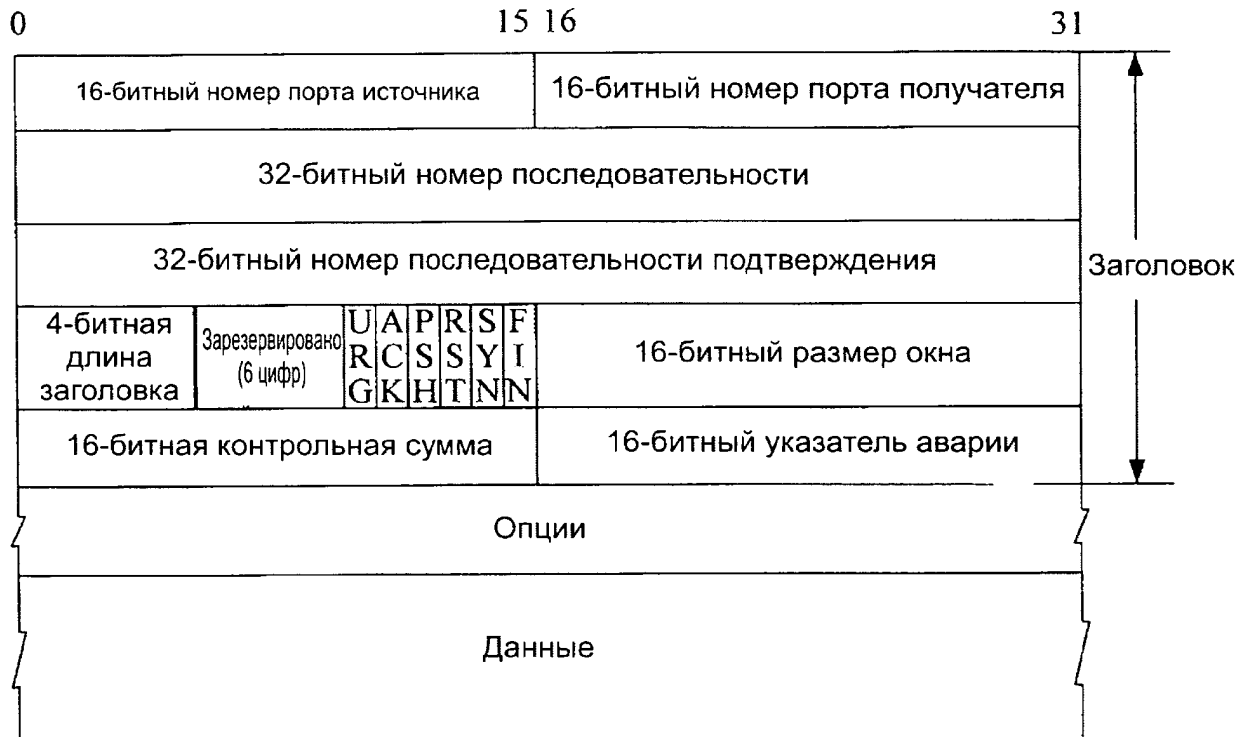
45



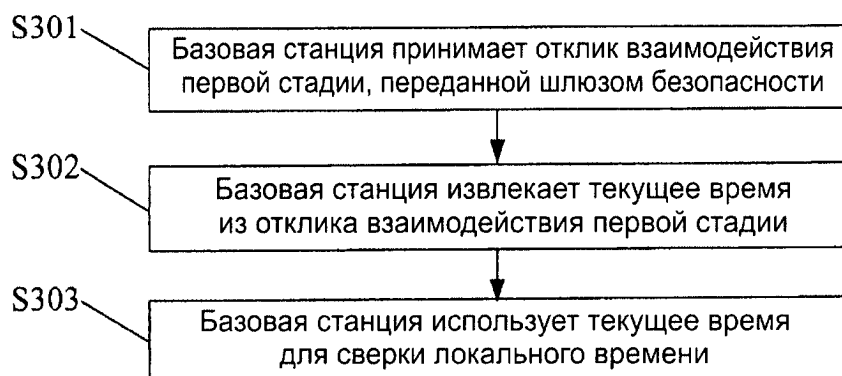
Фиг. 2



Фиг. 3



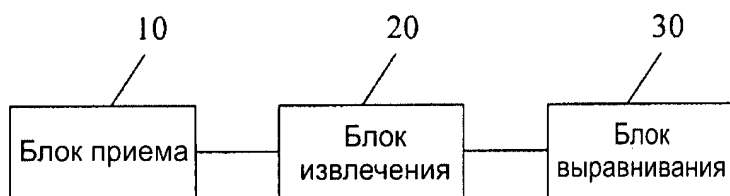
Фиг. 4



Фиг. 5



Фиг. 6



Фиг. 7