РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(19) **RU** (11) **2 435 319** (13) **C2**

(51) МПК
H04L 12/56 (2006.01)
G06F 21/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2009146555/08, 27.08.2008**

(24) Дата начала отсчета срока действия патента:
27.08.2008

Приоритет(ы):
(30) Конвенционный приоритет:
31.08.2007 CN 200710145703.3
26.09.2007 CN 200710151700.0

(43) Дата публикации заявки: **20.06.2011** Бюл. № 17

(45) Опубликовано: **27.11.2011** Бюл. № **33**

(56) Список документов, цитированных в отчете о поиске: **3RD GENERATION PARTNERSHIP PROJECT: Technical Specification Group Services and System Aspects; GPRS enhancements for E-UTRAN access (Release 8), 3GPP Standard; 3GPP TS 23.401, V1.1.0, июнь 2007, с.1-78, найден [28.12.2010] в сети Интернет по адресу: http://ftp.3gpp.org/Specs/archive/23_series/23.401/. NOKIA SIEMENS NETWORKS ET AL: "Pseudo-CR To TR** (см. прод.)

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **15.12.2009**

(86) Заявка PCT:
CN 2008/072165 (27.08.2008)

(87) Публикация заявки PCT:
WO 2009/030155 (12.03.2009)

Адрес для переписки:
129090, Москва, ул.Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. А.В.Мицу, рег.№ 364

(72) Автор(ы):
ХЭ Чэндун (CN)

(73) Патентообладатель(и):
ХУАВЭЙ ТЕКНОЛОДЖИЗ КО., ЛТД. (CN)

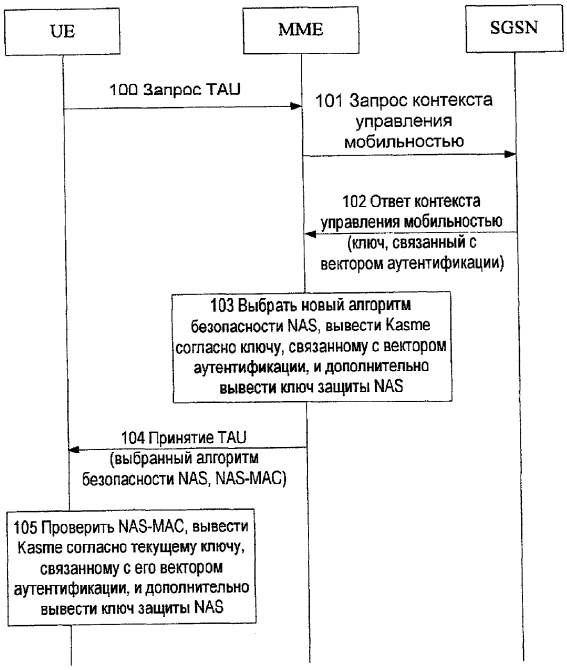
RU 2435319 C2

(54) СПОСОБ, СИСТЕМА И УСТРОЙСТВО ДЛЯ СОГЛАСОВАНИЯ ВОЗМОЖНОСТЕЙ БЕЗОПАСНОСТИ ПРИ ПЕРЕМЕЩЕНИИ ТЕРМИНАЛА

(57) Реферат:

Изобретение относится к способу и системе согласования возможностей безопасности при перемещении пользовательского оборудования (UE) из сети второго/третьего поколения (2G/3G) в сеть long term evolution (LTE). Технический результат заключается в обеспечении безопасности при перемещение

терминала из одной сети в другую. Объект управления мобильностью (MME) получает алгоритм безопасности сигнализации без доступа (NAS), поддерживаемый в UE, и ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации, выбирает алгоритм безопасности NAS, выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации или корневому ключу, и передает сообщение, несущее выбранный алгоритм безопасности NAS, в UE. UE выводит ключ защиты NAS согласно его ключу, связанному с вектором аутентификации. 5 н. и 12 з.п. ф-лы, 4 ил.



ФИГ.1

(56) (продолжение):
33.821: Key Handling On Idle Mode Mobility" S3-070529, 10-13 July 2007, Montreal, Canada, найден [28.12.2010] в сети Интернет по адресу: http: //ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_48_Montreal/Docs/. 3GPP: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 8)". 3GPP TR 33821 VO.3.0, июль 2007, найден [28.12.2010] в сети Интернет по адресу: http://ftp.3 gpp.org/Specs/archive/33_series/33.821/. RU 2174924 C1, 20.10.2001.

RU 2435319 C2

RU 2435319 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 435 319** (13) **C2**

(51) Int. Cl.
H04L 12/56 (2006.01)
G06F 21/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009146555/08, 27.08.2008**

(24) Effective date for property rights:
27.08.2008

Priority:
(30) Priority:
31.08.2007 CN 200710145703.3
26.09.2007 CN 200710151700.0

(43) Application published: **20.06.2011** Bull. 17

(45) Date of publication: **27.11.2011 Bull. 33**

(85) Commencement of national phase: **15.12.2009**

(86) PCT application:
CN 2008/072165 (27.08.2008)

(87) PCT publication:
WO 2009/030155 (12.03.2009)

Mail address:
129090, Moskva, ul.B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. A.V.Mitsu, reg.№ 364

(72) Inventor(s):
KhEh Chehndun (CN)

(73) Proprietor(s):
KhUAVEhJ TEKNOLODZhIZ KO., LTD. (CN)

RU 2435319 C2

(54) METHOD, SYSTEM AND DEVICE TO COORDINATE SECURITY RESOURCES IN PROCESS OF TERMINAL MOVEMENT

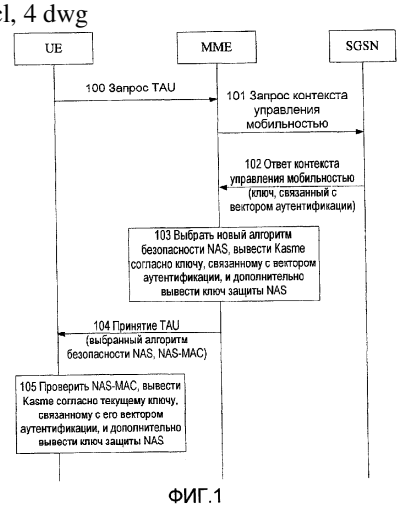
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: mobility management element (MME) receives a logic of no-access alarm security (NAS), supported in UE, and a key joined with an authentication vector, or a root key deduced according to the key joined with the authentication vector, selects a NAS security logic, deduces a NAS protection key according to the key joined with the authentication vector or the root key, and sends a message carrying the selected NAS security logic into UE. UE generates a NAS protection key according to its key joined with the authentication vector.

EFFECT: provision of security as a terminal moves from one network to the other.

17 cl, 4 dwg



ФИГ.1

RU 2435319 C2

Ссылка на родственные заявки

Данная заявка является продолжением международной заявки № PCT/CN2008/072165, поданной 27 августа 2008 г., которая притязает на приоритет китайской патентной заявки №200710145703.3, поданной 31 августа 2007 г., и китайской патентной заявки №200710151700.0, поданной 26 сентября 2007 г., которые все, таким образом, включены сюда в порядке ссылки в полном объеме.

Область техники

Настоящее изобретение относится к области технологии беспроводной связи и, в частности, к способу и системе для согласования возможностей безопасности при перемещении терминала, к объекту (сущности) управления мобильностью (MME) и пользовательскому оборудованию (UE).

Уровень техники

Беспроводная сеть включает в себя сеть радиодоступа и базовую сеть. Базовая сеть беспроводной сети long term evolution (LTE) включает в себя MME. Функции MME аналогичны функциям узла поддержки (SGSN) радиослужбы пакетной передачи данных (GPRS) сети второго/третьего поколения (2G/3G), и она, в основном, отвечает за управление мобильностью и аутентификацию пользователя. Когда UE находится в неактивном состоянии в беспроводной сети 2G/3G или LTE, UE приходится, соответственно, согласовывать возможности безопасности сигнализации без доступа (NAS) с SGSN или MME. Возможности безопасности включают в себя алгоритм шифрования сигнализации NAS, соответствующий ключ защиты целостности NAS Knas-int, алгоритм защиты целостности NAS и соответствующий ключ защиты конфиденциальности NAS Knas-enc, которые используются для передачи сигнализации между UE и системой, что гарантирует нормальной прием сигнализации UE и безопасность системы связи.

Когда UE, осуществляющий доступ к граничной сети радиодоступа (GERAN) глобальной системы мобильной связи (GSM) 2G или наземной сети радиодоступа (UTRAN) универсальной системы мобильной связи (UMTS) 3G, перемещается в неактивном состоянии, UE может перемещаться в зону слежения сети радиодоступа LTE, и, таким образом, UE может вновь осуществлять доступ к сети посредством LTE. При этом осуществляется процедура обновления зоны слежения (TAU), т.е. процедура TAU осуществляется между неоднородными сетями. В ходе процедуры, поскольку сущность, осуществляющая согласование возможностей безопасности для UE меняется, например, с SGSN на MME, и сущности могут иметь разные возможности безопасности, процедуру согласования возможностей безопасности необходимо осуществлять заново, чтобы гарантировать безопасность последующего взаимодействия между UE и сетью. Следует заметить, что для сети LTE согласование возможностей безопасности включает в себя согласование алгоритма защиты конфиденциальности NAS и алгоритма защиты целостности NAS, алгоритм защиты конфиденциальности управления радиоресурсами (RRC) и алгоритма защиты целостности RRC, и алгоритма защиты конфиденциальности в пользовательском плане (UP).

Для процедуры TAU, инициируемой UE в неактивном состоянии, необходимо разрешать согласование алгоритма защиты конфиденциальности NAS, алгоритма защиты целостности NAS и соответствующих ключей защиты NAS.

В ходе реализации настоящего изобретения автор обнаружил, что в уровне техники не существует способа согласования возможностей безопасности в ходе процедуры TAU между неоднородными сетями, из-за чего при перемещении UE из

сети 2G/3G в сеть LTE невозможно осуществлять согласование возможностей безопасности, в связи с чем невозможно гарантировать безопасность последующего взаимодействия между UE и сетью.

Сущность изобретения

Соответственно настоящее изобретение предусматривает способ согласования возможностей безопасности при перемещении терминала, благодаря чему, при перемещении из сети 2G/3G в сеть LTE, UE в неактивном состоянии может согласовывать возможности безопасности.

Настоящее изобретение дополнительно предусматривает систему для согласования возможностей безопасности при перемещении терминала, благодаря чему, при перемещении из сети 2G/3G в сеть LTE, UE в неактивном состоянии может согласовывать возможности безопасности.

Настоящее изобретение дополнительно предусматривает MME, благодаря чему, при перемещении из сети 2G/3G в сеть LTE, UE в неактивном состоянии может согласовывать возможности безопасности.

Настоящее изобретение дополнительно предусматривает устройство UE, благодаря чему, при перемещении из сети 2G/3G в сеть LTE, UE в неактивном состоянии может согласовывать возможности безопасности.

Для достижения целей изобретения технические решения настоящего изобретения реализуются следующим образом.

Предусмотрен способ согласования возможностей безопасности при перемещении терминала, который включает в себя следующие этапы.

MME принимает сообщение запроса TAU, переданное от UE, и получает алгоритм безопасности NAS, поддерживаемый в UE, и ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации.

MME выбирает алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации или корневому ключу, и передает сообщение, несущее выбранный алгоритм безопасности NAS, в UE.

UE выводит ключ защиты NAS согласно его ключу, связанному с вектором аутентификации.

Предусмотрена система для согласования возможностей безопасности при перемещении терминала, которая включает в себя UE и MME.

UE выполнено с возможностью передачи сообщения запроса TAU на MME, приема сообщения, несущего выбранный алгоритм безопасности NAS, переданного от MME, и вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации.

MME выполнена с возможностью: приема сообщения запроса TAU, переданного от UE; получения ключа, связанного с вектором аутентификации, или корневого ключа, выведенного согласно ключу, связанному с вектором аутентификации, и алгоритма безопасности NAS, поддерживаемого в UE; выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и генерации и передачи сообщения, несущего выбранный алгоритм безопасности NAS, в UE; и вывода ключа защиты NAS согласно полученному ключу, связанному с вектором аутентификации, или корневому ключу.

Предусмотрен MME, который включает в себя модуль получения, модуль выбора и модуль вывода ключа.

Модуль получения выполнен с возможностью приема сообщения запроса TAU,

переданного от UE, получения ключа, связанного с вектором аутентификации, или корневого ключа, выведенного согласно ключу, связанному с вектором аутентификации, и алгоритма безопасности NAS, поддерживаемого в UE.

Модуль выбора выполнен с возможностью выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и полученному модулем получения, генерации сообщения, несущего выбранный алгоритм безопасности NAS, и передачи сообщения в UE.

Модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации, или корневому ключу, выведенному согласно ключу, связанному с вектором аутентификации, полученному модулем получения, и алгоритму безопасности NAS выбранному модулем выбора.

Предусмотрен UE, который включает в себя модуль обновления, модуль вывода ключа, модуль хранения и модуль обнаружения.

Модуль обновления выполнен с возможностью передачи на MME сообщения запроса TAU, несущего информацию возможностей безопасности, поддерживаемую в UE и хранящуюся в модуле хранения, и приема сообщения, несущего выбранный алгоритм безопасности NAS, переданного от MME.

Модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации, и алгоритму безопасности NAS, принятому модулем обновления.

Модуль хранения выполнен с возможностью хранения информации возможностей безопасности, поддерживаемой в UE.

Модуль обнаружения выполнен с возможностью определения, что атака за счет деградации происходит, при обнаружении, что информация возможностей безопасности, поддерживаемая в UE и принятая от MME, не согласуется с информацией возможностей безопасности, поддерживаемой в UE и хранящейся в модуле хранения.

Способ согласования возможностей безопасности при перемещении терминала, в котором, когда пользовательское оборудование (UE) перемещается из сети второго/третьего поколения (2G/3G) в сеть long term evolution (LTE), способ содержит этапы, на которых:

принимают посредством сущности управления мобильностью (MME) сообщение запроса обновления зоны слежения (TAU), переданное от UE, и получают алгоритм безопасности сигнализации без доступа (NAS), поддерживаемый в UE, и ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации;

выбирают посредством MME алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, выводят ключ защиты NAS согласно ключу, связанному с вектором аутентификации или корневому ключу, и передают сообщение, несущее выбранный алгоритм безопасности NAS, в UE.

В технических решениях настоящего изобретения MME принимает сообщение запроса TAU переданное от UE, и получает ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации, и алгоритму безопасности NAS, поддерживаемому в UE; затем выбирает алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, генерирует сообщение, несущее выбранный алгоритм безопасности NAS, и передает сообщение в UE, что позволяет UE и MME совместно использовать алгоритм безопасности NAS. Кроме того, MME выводит ключ

защиты NAS согласно ключу, связанному с вектором аутентификации, или корневому ключу, выведенному согласно ключу, связанному с вектором аутентификации, и UE выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации, что позволяет MME и UE совместно использовать ключ защиты NAS. Таким образом, при перемещении из сети 2G/3G в сеть LTE, UE может согласовывать алгоритм безопасности NAS и ключ защиты NAS с MME, что обеспечивает процесс согласования возможностей безопасности в процедуре TAU между неоднородными сетями, что гарантирует безопасность последующего взаимодействия между UE и сетью.

Кроме того, настоящее изобретение также применимо к процедуре согласования возможностей безопасности, при перемещении UE в сети LTE.

Краткое описание чертежей

Фиг.1 - логическая блок-схема способа согласно первому варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала.

Фиг.2 - логическая блок-схема способа согласно второму варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала.

Фиг.3 - логическая блок-схема способа согласно третьему варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала.

Фиг.4 - блок-схема системы согласно варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала.

Подробное описание вариантов осуществления

Согласно способу согласования возможностей безопасности при перемещении терминала, предусмотренному в вариантах осуществления настоящего изобретения, когда UE перемещается из сети 2G/3G в сеть LTE, MME принимает сообщение запроса TAU, переданное от UE, и получает алгоритм безопасности NAS, поддерживаемый в UE, и ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации. Затем MME выбирает алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации или корневому ключу, выведенный согласно ключу, связанному с вектором аутентификации, и передает сообщение, несущее выбранный алгоритм безопасности NAS, в UE. UE выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации.

Варианты осуществления настоящего изобретения подробно представлены ниже со ссылкой на конкретные варианты осуществления и прилагаемые чертежи.

Предполагается, что UE осуществил доступ к UTRAN/GERAN, будучи в неактивном состоянии. В этом случае при перемещении в зону слежения сети LTE, UE инициирует процедуру TAU.

На фиг.1 показана логическая блок-схема способа согласно первому варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала. Согласно фиг.1 способ включает в себя следующие этапы.

На этапе 100, UE передает запрос TAU на MME.

На этом этапе UE передает запрос TAU на новую MME посредством evolved Node B

(eNB) сети радиодоступа LTE. Для удобства описания связь между UE и MME посредством eNB в нижеследующем описании сводится к связи между UE и MME.

Запрос TAU, переданный от UE на MME на этом этапе, не только переносит некоторые параметры, как то «temporary mobile subscriber identity» (TMSI), известный специалистам в данной области техники, но также может нести информацию возможностей безопасности, поддерживаемую в UE. Информация возможностей безопасности включает в себя алгоритм безопасности NAS (алгоритм защиты целостности NAS и/или алгоритм защиты конфиденциальности NAS) и также может включать в себя алгоритм безопасности RRC (алгоритм защиты целостности RRC и/или алгоритм защиты конфиденциальности RRC) или алгоритм безопасности UP (алгоритм защиты конфиденциальности UP).

На этапах 101-102 MME получает алгоритм безопасности NAS, поддерживаемый в UE, и передает сообщение запроса контекста управления мобильностью на SGSN. После приема сообщения SGSN передает сообщение ответа контекста управления мобильностью, несущее ключ, связанный с вектором аутентификации, на MME.

Если на этапе 100, UE не переносит алгоритм безопасности NAS, поддерживаемый в UE, в запросе TAU, переданном на MME, после приема сообщения запроса контекста управления мобильностью SGSN запрашивает алгоритм безопасности NAS, поддерживаемый в UE, и переносит запрошенный алгоритм безопасности NAS, поддерживаемый в UE, в сообщении ответа контекста управления мобильностью, переданном на MME. Алгоритм безопасности NAS является алгоритмом защиты целостности NAS и/или алгоритмом защиты конфиденциальности NAS.

Когда UE перемещается из сети 2G в зону слежения сети LTE, SGSN в вышеописанном процессе является SGSN сети 2G, и ключ, связанный с вектором аутентификации, включает в себя, по меньшей мере, ключ шифрования Kc или значение Kc', полученное после осуществления одностороннего преобразования на Kc. Когда UE перемещается из сети 3G в зону слежения сети LTE, SGSN в вышеописанном процессе является SGSN сети 3G, и ключ, связанный с вектором аутентификации, по меньшей мере, включает в себя ключ целостности IK и ключ шифрования CK, или значения IK' и CK' после осуществления одностороннего преобразования на IK и CK.

Одностороннее преобразование - это процедура преобразования, в которой исходный параметр преобразуется с использованием определенного алгоритма для получения конечного параметра, но исходный параметр нельзя вывести из конечного параметра. Например, для Kc, если Kc' получается с использованием алгоритма f(Kc), но Kc нельзя вывести из Kc' с использованием какого-либо обратного алгоритма, преобразование называется односторонним преобразованием.

На этапе 103 MME выбирает новый алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и алгоритму безопасности NAS, поддерживаемому на MME, а также алгоритму безопасности NAS, разрешенному системой, выводит корневой ключ Kasme согласно ключу, связанному с вектором аутентификации, и затем выводит ключ защиты NAS согласно Kasme. Ключ защиты NAS включает в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

На этапе 104 MME генерирует сообщение принятия TAU, несущее выбранный алгоритм безопасности NAS.

На этом этапе MME может дополнительно осуществлять защиту целостности NAS на сообщение принятия TAU. Например, MME выводит значение кода аутентификации сообщения защиты целостности NAS (NAS-MAC) согласно ключу защиты

целостности NAS Knas-int, выведенному на этапе 103, информация в сообщении принятия TAU, и алгоритм защиты целостности NAS в выбранном алгоритме безопасности NAS, затем переносит значение в сообщении принятия TAU и передает сообщение принятия TAU в UE.

Сообщение принятия TAU на этом этапе может дополнительно нести информацию возможностей безопасности, поддерживаемую в UE.

На этапе 105 UE принимает сообщение принятия TAU, несущее алгоритм безопасности NAS, выбранный MME, и получает согласованный алгоритм безопасности NAS; и затем выводит корневой ключ Kasme согласно текущему ключу, связанному с его вектором аутентификации (например, IK и CK, или IK' и CK' выведенный согласно IK и CK, когда исходная сеть является сетью 3G, или Kc или Kc', выведенному согласно Kc, когда исходная сеть является сетью 2G), и выводит ключ защиты NAS согласно корневому ключу. Ключ защиты NAS включает в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

На этом этапе UE может дополнительно определять, верна ли защита целостности, осуществляемая на сообщении принятия TAU. Если нет, производится определение, что текущее согласование возможностей безопасности не удалось, и процедура согласования возможностей безопасности может инициироваться повторно. Например, UE выводит NAS-MAC согласно выведенному ключу защиты конфиденциальности NAS Knas-enc, информации в сообщении принятия TAU и алгоритма защиты целостности NAS, переносимого в сообщении принятия TAU, и затем определяет, совпадает ли выведенный NAS-MAC с NAS-MAC, переносимым в сообщении принятия TAU. Если да, он указывает, что сообщение не изменяется в ходе передачи; в противном случае, предполагается, что сообщение изменяется в ходе передачи, и, таким образом, делается вывод, что текущее согласование возможностей безопасности не удалось.

Если на этапе 104 сообщение принятия TAU дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE, на этом этапе, UE может дополнительно сравнивать информацию возможностей безопасности, поддерживаемую в UE и переносимую в сообщении принятия TAU, с информацией возможностей безопасности, хранящейся на нем. Если они согласуются друг с другом, производится определение, что атаки за счет деградации не происходит; в противном случае производится определение, что атака за счет деградации имеет место и что текущее согласование возможностей безопасности не удалось, и процедура согласования возможностей безопасности может инициироваться повторно, тем самым, препятствуя атаке за счет деградации.

В отношении атаки за счет деградации предполагается, что UE одновременно поддерживает два алгоритма безопасности, а именно сильный алгоритм A1 и слабый алгоритм A2, и MME также поддерживает два алгоритма. Таким образом, сильный алгоритм A1 подлежит согласованию между UE и MME. Однако, если на пути, по которому UE передает информацию возможностей безопасности, поддерживаемую в UE, на MME, взломщик изменяет информацию возможностей безопасности UE, например поддерживается только слабый алгоритм A2, или когда MME выбирает алгоритм безопасности NAS, информация возможностей безопасности, поддерживаемая в UE, изменяется взломщиком, и поддерживается только слабый алгоритм A2, MME может выбирать и передавать в UE только слабый алгоритм A2. Таким образом, благодаря согласованию между UE и MME получается слабый

алгоритм A2, а не сильный алгоритм A1, что позволяет взломщику легче осуществлять атаку, которая является так называемой атакой за счет деградации. Согласно варианту осуществления настоящего изобретения MME передает информацию возможностей безопасности, поддерживаемую в UE, в UE, и UE определяет, согласуется ли информация возможностей безопасности, поддерживаемая в UE, с информацией возможностей безопасности, поддерживаемой в UE, что позволяет обнаруживать и дополнительно предотвращать атаку за счет деградации.

Процедура, в которой MME окончательно выводит ключ защиты NAS согласно ключу, связанному с вектором аутентификации, на этапе 103, не ограничивается какой-либо временной последовательностью в отношении этапа 104 и этапа 105, и процедура может осуществляться до этапа 104, или между этапом 104 и этапом 105, или после этапа 105.

В вышеописанном процессе MME и UE также могут непосредственно выводить ключ защиты NAS согласно ключу, связанному с вектором аутентификации, без вывода корневого ключа и последующего вывода ключа защиты NAS согласно корневому ключу.

Специалистам в данной области техники очевидно, что, в вышеописанном процессе способ вывода, используемый в UE для вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации, должен быть таким же, как используемый стороной сети для вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации. Способ вывода может использовать любое одностороннее преобразование, например Kasme=f(IK, CK, другие параметры), Knas-enc=f(Kasme, алгоритм защиты конфиденциальности NAS, другие параметры) и Knas-int=f(Kasme, алгоритм защиты целостности NAS, другие параметры).

Кроме того, для выделения этого варианта осуществления настоящего изобретения процедуры, которые не связаны с безопасностью, опущены между этапами 102 и 104 в вышеописанном процессе.

Благодаря вышеописанному процессу, UE и MME могут совместно использовать алгоритм безопасности NAS и ключ защиты NAS, тем самым реализуя согласование возможностей безопасности NAS.

На фиг.2 показана логическая блок-схема способа, согласно второму варианту осуществления настоящего изобретения, для согласования возможностей безопасности при перемещении терминала. Согласно фиг.2 способ включает в себя следующие этапы.

Этап 200 идентичен этапу 100, поэтому его описание здесь опущено.

На этапах 201-203 MME получает алгоритм безопасности NAS, поддерживаемый в UE, и передает сообщение запроса контекста на SGSN. После приема сообщения запроса контекста SGSN выводит корневой ключ согласно ключу, связанному с его вектором аутентификации, и затем передает сообщение ответа контекста, несущее корневой ключ, на MME.

В других вариантах осуществления настоящего изобретения, если на этапе 200, UE не переносит алгоритм безопасности NAS, поддерживаемый в UE, в запросе TAU, переданном на MME, после приема сообщения запроса контекста управления мобильностью, SGSN запрашивает алгоритм безопасности NAS, поддерживаемый в UE, и переносит запрошенный алгоритм безопасности NAS, поддерживаемый в UE, в сообщении ответа контекста управления мобильностью, переданном на MME. Алгоритм безопасности NAS является алгоритмом защиты целостности NAS и/или алгоритмом защиты конфиденциальности NAS.

Когда UE перемещается из сети 2G в зону слежения сети LTE, SGSN в вышеописанном процессе является SGSN сети 2G, и корневой ключ является корневым ключом Kasme, выведенным SGSN согласно Kc, или Kc', полученным после осуществления одностороннего преобразования на Kc. Когда UE перемещается из сети 3G в зону слежения сети LTE, SGSN в вышеописанном процессе является SGSN сети 3G, и корневой ключ является Kasme, выведенным SGSN согласно IK и CK, или IK' и CK' после осуществления одностороннего преобразования на IK и CK.

На этапе 204 MME выбирает новый алгоритм безопасности NAS, согласно алгоритму безопасности NAS, поддерживаемому в UE, и алгоритму безопасности NAS, поддерживаемому на MME, а также алгоритму безопасности NAS, разрешенному системой; и затем выводит ключ защиты NAS согласно корневому ключу. Ключ защиты NAS включает в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

На этапе 205 MME генерирует сообщение принятия TAU, несущее выбранный алгоритм безопасности NAS.

На этом этапе MME может дополнительно осуществлять защиту целостности NAS на сообщении принятия TAU. Сообщение принятия TAU на этом этапе может дополнительно нести информацию возможностей безопасности, поддерживаемую в UE.

На этапе 206 UE принимает сообщение принятия TAU, несущее алгоритм безопасности NAS, выбранный MME, и получает согласованный алгоритм безопасности NAS; и затем выводит корневой ключ Kasme согласно текущему ключу, связанному с вектором аутентификации (например, IK и CK, или IK' и CK', выведенный согласно IK и CK, когда исходная сеть является сетью 3G, или Kc или Kc', выведенному согласно Kc, когда исходная сеть является сетью 2G), и выводит ключ защиты NAS согласно корневому ключу. Ключ защиты NAS включает в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

На этом этапе UE может дополнительно определять, верна ли защита целостности, осуществляемая на сообщении принятия TAU. Если нет, производится определение, что текущее согласование возможностей безопасности не удалось, и процедура согласования возможностей безопасности может инициироваться повторно.

В других вариантах осуществления настоящего изобретения, если на этапе 205 сообщение принятия TAU дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE, на этом этапе UE может дополнительно сравнивать информацию возможностей безопасности, поддерживаемую в UE, переносимую в сообщении принятия TAU, с информацией возможностей безопасности, поддерживаемой в UE. Если они согласуются друг с другом, производится определение, что атаки за счет деградации не происходит; в противном случае производится определение, что атака за счет деградации имеет место и что текущее согласование возможностей безопасности не удалось, и процедура согласования возможностей безопасности может инициироваться повторно, тем самым, препятствуя атаке за счет деградации.

В других вариантах осуществления настоящего изобретения процедура, в которой MME выводит ключ защиты NAS согласно корневому ключу на этапе 204, не ограничивается какой-либо временной последовательностью в отношении этапа 205 и этапа 206, и процедура может осуществляться до этапа 205, или между этапом 205 и этапом 206, или после этапа 206.

Специалистам в данной области техники очевидно, что, в вышеописанном процессе,

способ вывода, используемый в UE для вывода ключа защиты NAS, согласно ключу, связанному с вектором аутентификации, должен быть таким же, как используемый стороной сети для вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации.

Благодаря вышеописанному процессу, UE и MME могут совместно использовать алгоритм безопасности NAS и ключ защиты NAS, тем самым реализуя согласование возможностей безопасности NAS.

На фиг.3 показана логическая блок-схема способа согласно третьему варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала. Согласно фиг.3 способ включает в себя следующие этапы.

Этап 300 идентичен этапу 100, поэтому его описание здесь опущено.

На этапах 301-302 MME получает алгоритм безопасности NAS, поддерживаемый в UE, от SGSN посредством сообщений запроса и ответа контекста управления мобильностью.

В других вариантах осуществления настоящего изобретения, если на этапе 300, UE не переносит алгоритм безопасности NAS, поддерживаемый в UE, в запросе TAU, переданном на MME, после приема сообщения запроса контекста управления мобильностью, SGSN запрашивает алгоритм безопасности NAS, поддерживаемый в UE, и переносит запрошенный алгоритм безопасности NAS, поддерживаемый в UE, в сообщении ответа контекста управления мобильностью, переданном на MME. Алгоритм безопасности NAS является алгоритмом защиты целостности NAS и/или алгоритмом защиты конфиденциальности NAS.

На этапе 303 MME получает корневой ключ Kasme, выведенный согласно ключу, связанному с вектором аутентификации, от домашнего абонентского сервера (HSS) посредством процедуры аутентификации и согласования ключей (AKA).

На этапе 304 MME выбирает новый алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и алгоритму безопасности NAS, поддерживаемому на MME, а также алгоритму безопасности NAS, разрешенному системой; и затем выводит другие ключи защиты NAS согласно Kasme. Ключи защиты NAS включают в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

На этапе 305 MME генерирует и передает в UE сообщение запроса команды безопасного режима (SMC) NAS, несущее выбранный алгоритм безопасности NAS. Сообщение запроса SMC может переноситься в сообщении принятия TAU.

На этом этапе MME может дополнительно осуществлять защиту целостности NAS на сообщении принятия SMC. Например, MME выводит значение кода аутентификации сообщения защиты целостности NAS (NAS-MAC) согласно ключу защиты целостности NAS Knas-int, выведенному на этапе 304, информации в сообщении запроса SMC и алгоритму защиты целостности NAS в выбранном алгоритме безопасности NAS, затем переносит значение в сообщении запроса SMC и передает сообщение запроса SMC в UE.

Сообщение запроса SMC на этом этапе может дополнительно нести информацию возможностей безопасности, поддерживаемую в UE.

На этапе 306 UE принимает сообщение запроса SMC, несущее алгоритм безопасности NAS, выбранный MME, и получает алгоритм безопасности NAS, поддерживаемый в UE и выбранный на MME; затем выводит корневой ключ согласно текущему ключу, связанному с вектором аутентификации, полученному в его

процедуре AKA, и выводит ключ защиты NAS согласно корневому ключу. Ключ защиты NAS включает в себя ключ защиты целостности NAS Knas-int и/или ключ защиты конфиденциальности NAS Knas-enc.

В этом варианте осуществления, на этом этапе, UE может дополнительно определять, верна ли защита целостности, осуществляемая на сообщении принятия TAU. Если нет, производится определение, что текущее согласование возможностей безопасности не удалось, и процедура согласования возможностей безопасности может инициироваться повторно. Например, UE выводит NAS-MAC согласно выведенному ключу защиты конфиденциальности NAS Knas-enc, информации в сообщении принятия TAU и алгоритма защиты целостности NAS, переносимого в сообщении принятия TAU, и затем определяет, совпадает ли выведенный NAS-MAC с NAS-MAC, переносимым в сообщении принятия TAU. Если да, он указывает, что сообщение не изменяется в ходе передачи; в противном случае, предполагается, что сообщение изменяется в ходе передачи, и, таким образом, делается вывод, что текущее согласование возможностей безопасности не удалось.

В других вариантах осуществления настоящего изобретения, если на этапе 305 сообщение запроса SMC дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE, на этом этапе UE может дополнительно сравнивать информацию возможностей безопасности, поддерживаемую в UE и переносимую в сообщении запроса SMC, с информацией возможностей безопасности, поддерживаемой в UE. Если они согласуются друг с другом, производится определение, что атаки за счет деградации не происходит; в противном случае производится определение, что атака за счет деградации имеет место и что текущее согласование возможностей безопасности не удалось, то процедура согласования возможностей безопасности может инициироваться повторно, тем самым, препятствуя атаке за счет деградации.

На этапе 307 UE передает сообщение ответа завершения SMC на MME. Сообщение ответа завершения SMC может переноситься в сообщении завершения TAU.

На этапе 308 MME возвращает сообщение принятия TAU.

В других вариантах осуществления настоящего изобретения, когда сообщение запроса SMC передается в UE путем переноса сообщения запроса SMC в сообщении принятия TAU на этапе 305, этап 308 объединяется с этапом 305.

На этапе 309 UE возвращает сообщение завершения TAU.

В других вариантах осуществления настоящего изобретения, когда сообщение ответа завершения SMC переносится в сообщении завершения TAU на этапе 307, этап 309 объединяется с этапом 307.

Благодаря вышеописанному процессу, реализуется согласование возможностей безопасности NAS.

Специалистам в данной области техники будет очевидно, что все или некоторые этапы способа согласно вариантам осуществления настоящего изобретения можно реализовать в виде программы, управляющей соответствующим оборудованием, и программа может храниться на компьютерно-считываемом носителе информации, например, в постоянной памяти (ПЗУ)/оперативной памяти (ОЗУ), на магнитном диске или на оптическом диске.

На фиг.4 показана блок-схема системы согласно варианту осуществления настоящего изобретения для согласования возможностей безопасности при перемещении терминала. Согласно фиг.4 система включает в себя UE и MME.

UE выполнено с возможностью передачи сообщения запроса TAU на MME, приема

сообщения, несущего выбранный алгоритм безопасности NAS, переданного от MME, и вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации.

MME выполнена с возможностью: приема сообщения запроса TAU, переданного от UE; получения ключа, связанного с вектором аутентификации, или корневого ключа, выведенного согласно ключу, связанному с вектором аутентификации, и алгоритма безопасности NAS, поддерживаемого в UE; выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и генерации и передачи сообщения, несущего выбранный алгоритм безопасности NAS, в UE; и вывода ключа защиты NAS согласно полученному ключу, связанному с вектором аутентификации, или корневому ключу, выведенному согласно ключу, связанному с вектором аутентификации.

В системе MME дополнительно получает информацию возможностей безопасности, поддерживаемую в UE, и дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE, в сообщении, несущем выбранный алгоритм безопасности NAS, переданном в UE, и UE дополнительно определяет, происходит ли атака за счет деградации, путем определения, согласуется ли информация возможностей безопасности, поддерживаемая в UE и передаваемая от MME, с информацией возможностей безопасности, поддерживаемой в UE.

В частности MME включает в себя модуль получения, модуль выбора и модуль вывода ключа.

Модуль получения выполнен с возможностью приема сообщения запроса TAU, переданного от UE, получения ключа, связанного с вектором аутентификации, или корневого ключа, выведенного согласно ключу, связанному с вектором аутентификации, и алгоритма безопасности NAS, поддерживаемого в UE. Модуль выбора выполнен с возможностью выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE и полученному модулем получения, генерации и передачи сообщения, несущего выбранный алгоритм безопасности NAS, в UE. Модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS, согласно ключу, связанному с вектором аутентификации, или корневому ключу, выведенному согласно ключу, связанному с вектором аутентификации, полученному модулем получения, и выбранному алгоритму безопасности NAS.

Модуль получения дополнительно получает информацию возможностей безопасности, поддерживаемую в UE, и модуль выбора дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE и полученную модулем получения в сообщении, несущем выбранный алгоритм безопасности NAS.

UE включает в себя модуль обновления, модуль вывода ключа, модуль хранения и модуль обнаружения.

Модуль обновления выполнен с возможностью передачи сообщения запроса TAU, несущего информацию возможностей безопасности, поддерживаемую в UE и хранящуюся в модуле хранения на MME, и приема сообщения, несущего выбранный алгоритм безопасности NAS, переданного от MME. Модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS согласно ключу, связанному с вектором аутентификации, и выбранному алгоритму безопасности NAS, принятому модулем обновления. Модуль хранения выполнен с возможностью хранения информации возможностей безопасности, поддерживаемой в UE. Модуль обнаружения выполнен с возможностью определения, что атака за счет деградации происходит, при обнаружении, что информация возможностей безопасности, поддерживаемая в UE и

принятая от MME, не согласуется с информацией возможностей безопасности, поддерживаемой в UE и хранящейся в модуле хранения. Сообщение, несущее выбранный алгоритм безопасности NAS, переданное от MME, дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE.

Из вышеприведенного описания следует, что в технических решениях, предусмотренных согласно вариантам осуществления настоящего изобретения, MME принимает сообщение запроса TAU, переданное от UE, и получает алгоритм безопасности NAS, поддерживаемый в UE, и ключ, связанный с вектором аутентификации, или корневой ключ, выведенный согласно ключу, связанному с вектором аутентификации; и затем выбирает алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и генерирует, и передает сообщение, несущее выбранный алгоритм безопасности NAS, в UE, что позволяет UE и MME совместно использовать алгоритм безопасности NAS. Кроме того, UE и MME выводят ключ защиты NAS согласно ключу, связанному с вектором аутентификации, или корневому ключу, выведенному согласно ключу, связанному с вектором аутентификации, что позволяет MME и UE совместно использовать ключ защиты NAS. Таким образом, при перемещении из сети 2G/3G в сеть LTE, UE может согласовывать алгоритм безопасности NAS и ключ защиты NAS с MME, что обеспечивает процесс согласования возможностей безопасности в процедуре TAU между неоднородными сетями, что гарантирует безопасность последующего взаимодействия между UE и сетью.

Настоящее изобретение позволяет дополнительно предотвращать атаку за счет деградации. MME также возвращает информацию возможностей безопасности, поддерживаемую в UE, посредством сообщения принятия TAU, и UE определяет, согласуется ли информация возможностей безопасности, поддерживаемая в UE, с текущей информацией возможностей безопасности, поддерживаемой в UE. Если да, значит текущее согласование возможностей безопасности успешно и можно использовать алгоритм безопасности NAS и ключ защиты NAS, полученный посредством согласования. Если нет, производится определение, что атака за счет деградации имеет место, текущее согласование возможностей безопасности не удалось, и согласование возможностей безопасности необходимо осуществлять заново. Вышеописанные решения позволяют определить, подвергается ли атаке информация возможностей безопасности, поддерживаемая в UE, до того, как MME получит информацию возможностей безопасности, поддерживаемую в UE, тем самым, препятствуя атаке за счет деградации и гарантируя безопасность последующего взаимодействия между UE и сетью.

Вышеприведенные описания представляют лишь предпочтительные варианты осуществления настоящего изобретения, но не призваны ограничивать объем защиты настоящего изобретения. Любые модификации, эквивалентные замены и усовершенствования, не выходящие за рамки сущности и принципов настоящего изобретения, отвечают объему защиты настоящего изобретения.

Формула изобретения

1. Способ согласования возможностей безопасности при перемещении терминала, в котором, когда пользовательское оборудование (UE) перемещается из сети второго/третьего поколения (2G/3G) в сеть long term evolution (LTE), способ содержит этапы, на которых:

принимают, посредством объекта управления мобильностью (MME), сообщение

запроса обновления зоны слежения (TAU), переданное от UE, и получают алгоритм безопасности сигнализации без доступа (NAS), поддерживаемый в UE, и ключ, связанный с вектором аутентификации,

выбирают, посредством MME, алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, выводят корневой ключ согласно ключу, связанному с вектором аутентификации, и затем выводят ключ защиты NAS согласно выведенному корневому ключу, и передают сообщение, несущее выбранный алгоритм безопасности NAS, в UE, и

выводят, посредством UE, корневой ключ согласно ключу, связанному с вектором аутентификации, и затем выводят ключ защиты NAS согласно выведенному корневому ключу, причем

когда UE перемещается из сети 2G в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ шифрования Kc или значение, полученное после осуществления одностороннего преобразования ключа шифрования Kc; или

когда UE перемещается из сети 3G в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ целостности IK и ключ шифрования CK, или значения, полученные после осуществления одностороннего преобразования IK и ключа шифрования CK.

2. Способ по п.1, в котором на этапе получения, посредством MME, алгоритма безопасности NAS, поддерживаемого в UE,

получают, посредством MME, информацию возможностей безопасности, поддерживаемую в UE, из сообщения запроса TAU, переданного от UE, причем сообщение запроса TAU содержит алгоритм безопасности NAS, поддерживаемый в UE.

3. Способ по п.1, в котором на этапе получения, посредством MME, алгоритма безопасности NAS, поддерживаемого в UE,

получают, посредством MME, информацию возможностей безопасности, поддерживаемую в UE, из сообщения ответа контекста управления мобильностью, переданного от узла поддержки (SGSN) радиослужбы пакетной передачи данных (GPRS), причем сообщение ответа контекста управления мобильностью содержит алгоритм безопасности NAS, поддерживаемый в UE.

4. Способ по п.1, в котором

на этапе получения, посредством MME, ключа, связанного с вектором аутентификации, получают, посредством MME, ключ, связанный с вектором аутентификации, из сообщения ответа контекста управления мобильностью, переданного от SGSN.

5. Способ по п.1, в котором, до передачи, посредством MME, сообщения, несущего выбранный алгоритм безопасности NAS, в UE, способ дополнительно содержит этапы, на которых

осуществляют, посредством MME, защиту целостности в отношении сообщения, несущего выбранный алгоритм безопасности NAS, и

определяют, посредством UE, является ли защита целостности, осуществляемая в отношении сообщения, несущего выбранный алгоритм безопасности NAS, правильной, согласно выведенному ключу защиты NAS, после приема сообщения, несущего выбранный алгоритм безопасности NAS.

6. Способ по п.2 или 3, в котором сообщение, несущее выбранный алгоритм безопасности NAS, дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE, и

способ дополнительно содержит этап, на котором определяют, посредством UE, происходит ли атака за счет деградации, путем определения того, согласуется ли принятая информация возможностей безопасности, поддерживаемая в UE, с информацией возможностей безопасности, поддерживаемой в UE.

7. Система для согласования возможностей безопасности при перемещении терминала, содержащая пользовательское оборудование (UE) и объект управления мобильностью (MME), причем

UE выполнено с возможностью передачи сообщения запроса обновления зоны слежения (TAU) на MME, приема сообщения, несущего выбранный алгоритм безопасности сигнализации без доступа (NAS), переданного от MME, и вывода ключа защиты NAS согласно корневому ключу, который выведен согласно ключу, связанному с вектором аутентификации, и

MME выполнена с возможностью: приема сообщения запроса TAU, переданного от UE, получения ключа, связанного с вектором аутентификации, и алгоритма безопасности NAS, поддерживаемого в UE, выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и генерации и передачи сообщения, несущего выбранный алгоритм безопасности NAS, в UE, и вывода ключа защиты NAS согласно корневому ключу, который выведен согласно полученному ключу, связанному с вектором аутентификации, причем,

когда UE перемещается из сети второго поколения (2G) в сеть long term evolution (LTE), ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ шифрования Kc или значение, полученное после осуществления одностороннего преобразования ключа шифрования Kc; или

когда UE перемещается из сети третьего поколения (3G) в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ целостности IK и ключ шифрования CK, или значения, полученные после осуществления одностороннего преобразования IK и ключа шифрования CK.

8. Система по п.7, в которой MME дополнительно получает информацию возможностей безопасности, поддерживаемую в UE, и переносит информацию возможностей безопасности, поддерживаемую в UE, в сообщении, несущем выбранный алгоритм безопасности NAS, переданном в UE, и

UE дополнительно определяет, происходит ли атака за счет деградации, путем определения того, согласуется ли информация возможностей безопасности, поддерживаемая в UE и передаваемая от MME, с информацией возможностей безопасности, поддерживаемой в UE.

9. Система по п.7, в которой MME получает ключ, связанный с вектором аутентификации, из сообщения ответа контекста управления мобильностью, переданного от узла поддержки (SGSN) радиослужбы пакетной передачи данных.

10. Объект управления мобильностью (MME), содержащий модуль получения, модуль выбора и модуль вывода ключа, в котором

модуль получения выполнен с возможностью приема сообщения запроса обновления зоны слежения (TAU), переданного от пользовательского оборудования (UE), получения ключа, связанного с вектором аутентификации, и алгоритма безопасности сигнализации без доступа (NAS), поддерживаемого в UE,

модуль выбора выполнен с возможностью выбора алгоритма безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, и полученному модулем получения, генерации и передачи сообщения, несущего выбранный алгоритм безопасности NAS, в UE, и

модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS согласно корневому ключу, который выведен согласно ключу, связанному с вектором аутентификации, полученному модулем получения, и алгоритму безопасности NAS, выбранному модулем выбора, причем

когда UE перемещается из сети второго поколения (2G) в сеть long term evolution (LTE), ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ шифрования Kc или значение, полученное после осуществления одностороннего преобразования ключа шифрования Kc; или

когда UE перемещается из сети третьего поколения (3G) в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ целостности IK и ключ шифрования CK, или значения, полученные после осуществления одностороннего преобразования IK и ключа шифрования CK.

11. Объект по п.10, в котором модуль получения дополнительно получает информацию возможностей безопасности, поддерживаемую в UE, и модуль выбора дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE и полученную модулем получения в сообщении, несущем выбранный алгоритм безопасности NAS.

12. Объект по п.10, в которой модуль получения выполнен с возможностью получения ключа, связанного с вектором аутентификации, из сообщения ответа контекста управления мобильностью, переданного от узла поддержки (SGSN) радиослужбы пакетной передачи данных.

13. Пользовательское оборудование (UE), содержащее модуль обновления, модуль вывода ключа, модуль хранения и модуль обнаружения, в котором

модуль обновления выполнен с возможностью передачи сообщения запроса обновления зоны слежения (TAU), несущего информацию возможностей безопасности, поддерживаемую в UE и хранящуюся в модуле хранения, в объект управления мобильностью (MME), и приема сообщения, несущего выбранный алгоритм безопасности сигнализации без доступа (NAS), переданного от MME,

модуль вывода ключа выполнен с возможностью вывода ключа защиты NAS согласно корневому ключу, который выведен согласно ключу, связанному с вектором аутентификации, и алгоритму безопасности NAS, принятому модулем обновления,

модуль хранения выполнен с возможностью хранения информации возможностей безопасности, поддерживаемой в UE, и

модуль обнаружения выполнен с возможностью определения того, что происходит атака за счет деградации, при обнаружении того, что информация возможностей безопасности, поддерживаемая в UE и принятая от MME, не согласуется с информацией возможностей безопасности, поддерживаемой в UE и хранящейся в модуле хранения.

14. Пользовательское оборудование по п.13, в котором сообщение, несущее выбранный алгоритм безопасности NAS, переданное от MME, дополнительно переносит информацию возможностей безопасности, поддерживаемую в UE.

15. Способ согласования возможностей безопасности при перемещении терминала, причем, когда пользовательское оборудование (UE) перемещается из сети второго/третьего поколения (2G/3G) в сеть long term evolution (LTE), способ содержит этапы, на которых

принимают, посредством объекта управления мобильностью (MME), сообщение запроса обновления зоны слежения (TAU), переданное от UE, и получают алгоритм безопасности сигнализации без доступа (NAS), поддерживаемый в UE, и ключ,

связанный с вектором аутентификации,

выбирают, посредством MME, алгоритм безопасности NAS согласно алгоритму безопасности NAS, поддерживаемому в UE, выводят ключ защиты NAS согласно корневому ключу, который выведен согласно ключу, связанному с вектором аутентификации, и передают сообщение, несущее выбранный алгоритм безопасности NAS, в UE, причем

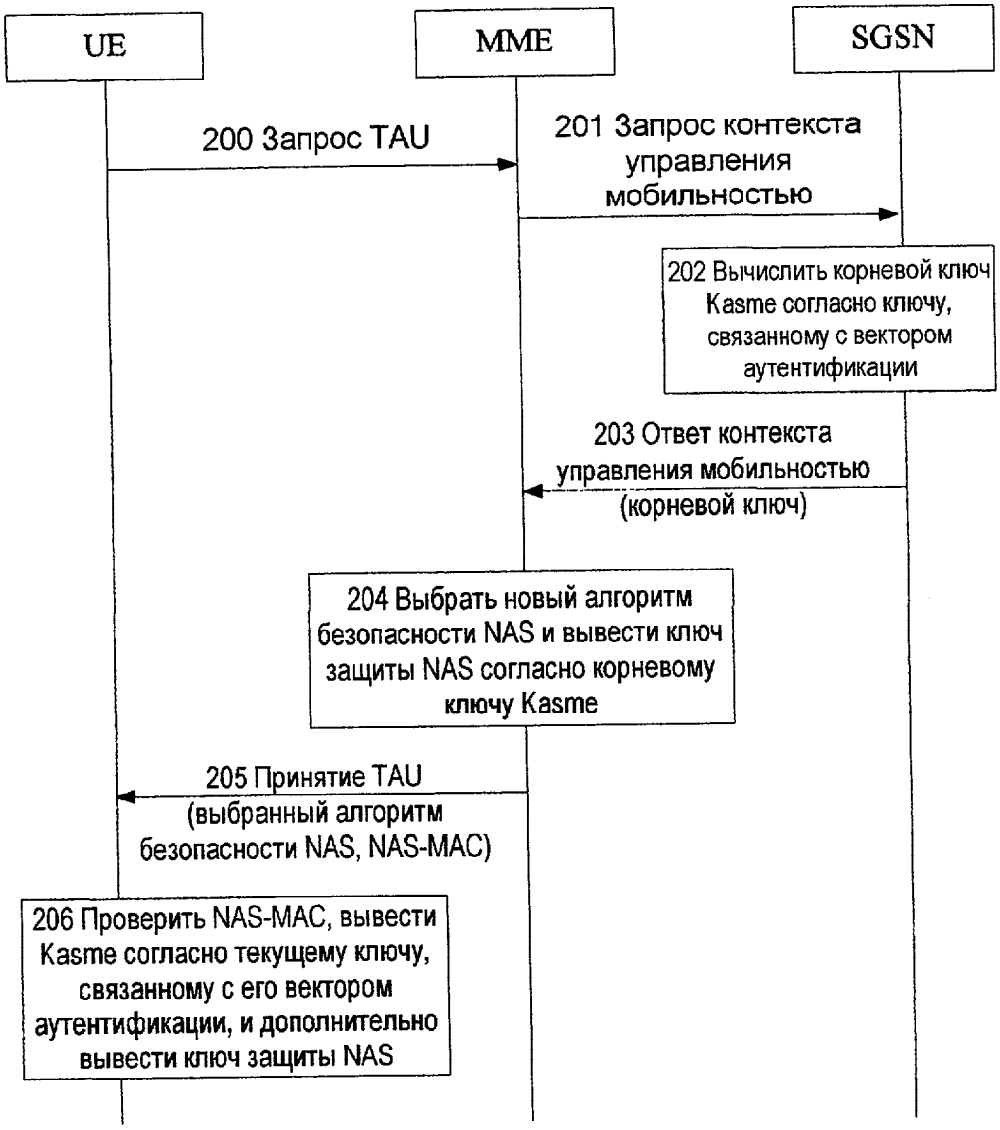
когда UE перемещается из сети 2G в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ шифрования Kc или значение, полученное после осуществления одностороннего преобразования ключа шифрования Kc; или

когда UE перемещается из сети 3G в сеть LTE, ключ, связанный с вектором аутентификации, содержит по меньшей мере ключ целостности IK и ключ шифрования CK, или значения, полученные после осуществления одностороннего преобразования IK и ключа шифрования CK.

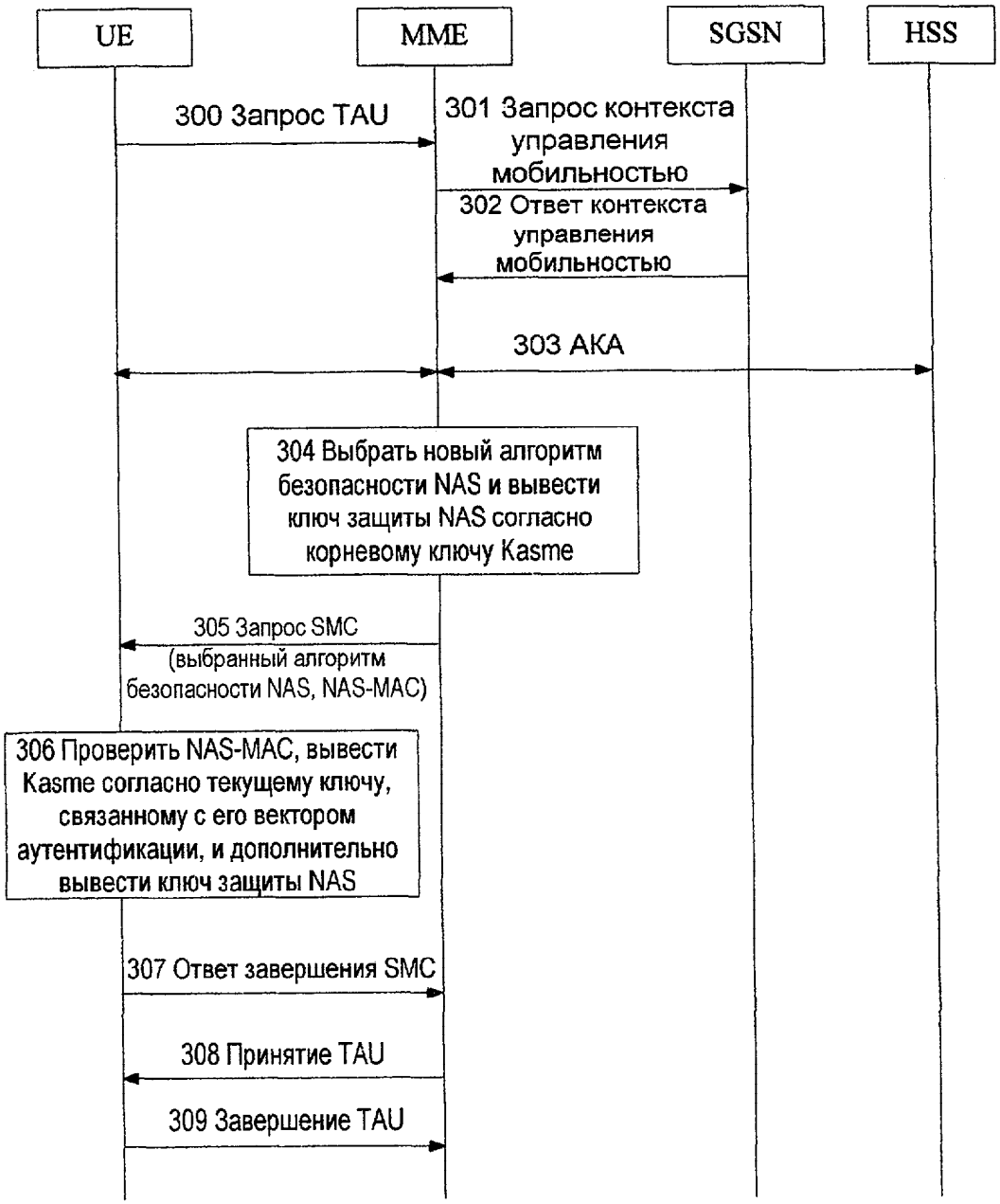
16. Способ по п.15, в котором на этапе получения, посредством MME, алгоритма безопасности NAS, поддерживаемого в UE получают, посредством MME, информацию возможностей безопасности, поддерживаемую в UE, из сообщения запроса TAU, переданного от UE, причем сообщение запроса TAU содержит алгоритм безопасности NAS, поддерживаемый в UE.

17. Способ по п.15, в котором на этапе получения, посредством MME, алгоритма безопасности NAS, поддерживаемого в UE,

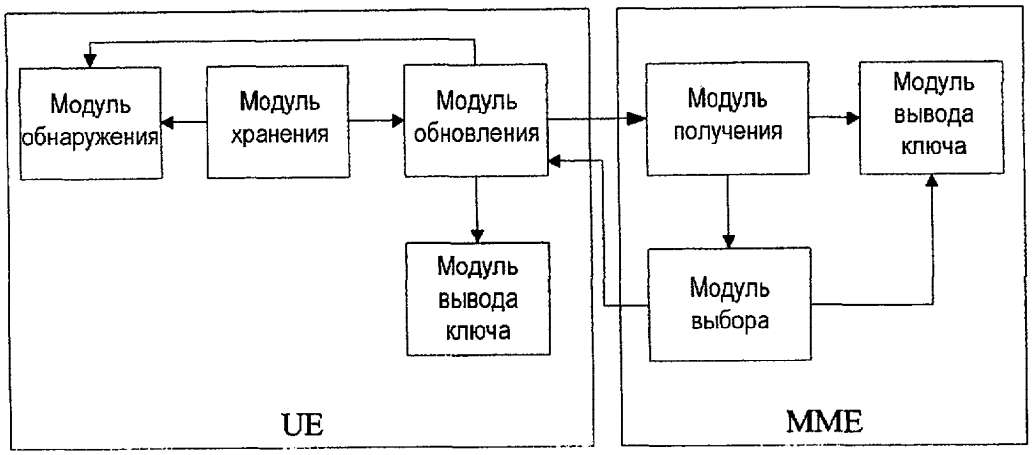
получают, посредством MME, информацию возможностей безопасности, поддерживаемую в UE, из сообщения ответа контекста управления мобильностью, переданного от узла поддержки (SGSN) радиослужбы пакетной передачи данных (GPRS), причем сообщение ответа контекста управления мобильностью содержит алгоритм безопасности NAS, поддерживаемый в UE.


UE
MME
SGSN
200 Запрос TAU
201 Запрос контекста управления мобильностью
202 Вычислить корневой ключ Kasme согласно ключу, связанному с вектором аутентификации
203 Ответ контекста управления мобильностью (корневой ключ)
204 Выбрать новый алгоритм безопасности NAS и вывести ключ защиты NAS согласно корневому ключу Kasme
205 Принятие TAU (выбранный алгоритм безопасности NAS, NAS-MAC)
206 Проверить NAS-MAC, вывести Kasme согласно текущему ключу, связанному с его вектором аутентификации, и дополнительно вывести ключ защиты NAS

ФИГ.2


UE
MME
SGSN
HSS
300 Запрос TAU
301 Запрос контекста управления мобильностью
302 Ответ контекста управления мобильностью
303 АКА
304 Выбрать новый алгоритм безопасности NAS и вывести ключ защиты NAS согласно корневому ключу Kasme
305 Запрос SMC (выбранный алгоритм безопасности NAS, NAS-MAC)
306 Проверить NAS-MAC, вывести Kasme согласно текущему ключу, связанному с его вектором аутентификации, и дополнительно вывести ключ защиты NAS
307 Ответ завершения SMC
308 Принятие TAU
309 Завершение TAU

ФИГ.3


Модуль обнаружения
Модуль хранения
Модуль обновления
Модуль вывода ключа
UE
Модуль получения
Модуль вывода ключа
Модуль выбора
MME

ФИГ.4