

(19)



**Евразийское
патентное
ведомство**

(11) **035283**

(13) **B1**

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ**

(45) Дата публикации и выдачи патента
2020.05.25

(51) Int. Cl. **H04W 8/02 (2009.01)**
H04W 60/06 (2009.01)

(21) Номер заявки
201590159

(22) Дата подачи заявки
2013.07.01

(54) **СПОСОБ ПРИКРЕПЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННОГО ТЕРМИНАЛА В РОУМИНГЕ К СЕТИ ГОСТЕВОГО ОПЕРАТОРА**

(31) **12305812.5**

(56) EP-A2-1463366
US-A1-2008020756
WO-A1-2011094709

(32) **2012.07.06**

(33) **EP**

(43) **2015.04.30**

(86) **PCT/EP2013/063869**

(87) **WO 2014/006009 2014.01.09**

(71)(73) Заявитель и патентовладелец:
ЖЕМАЛЬТО СА (FR)

(72) Изобретатель:
**Тюилье Эдмон, Кюк Жан-Франсуа
(FR)**

(74) Представитель:
Медведев В.Н. (RU)

(57) Изобретение представляет собой способ прикрепления телекоммуникационного терминала в роуминге к гостевой сети, причем этот терминал содержит защитный элемент, который представляет собой одно из SIM-карты, UICC, USIM или eUICC. Сущность способа заключается в том, что из домашней сети на терминал передают сообщение отклонения RNA и/или UDV, которое основано на данных о технических характеристиках упомянутого терминала и упомянутого защитного элемента.

B1

035283

035283

B1

Изобретение имеет отношение к способу прикрепления телекоммуникационного терминала в роуминге к сети гостевого оператора.

Управление роумингом, или "предпочтительным роумингом", является процессом, посредством которого мобильный оператор решает, какого партнера их абоненты будут использовать во время роуминга. В мире есть множество операторов, или поставщиков, мобильной или сотовой сети, часто больше одного в одной стране. Эти операторы сети включают в себя, но не ограничены этим, операторов, которые предоставляют услуги мобильной связи с использованием технологии GSM, GPRS, 3G, CDMA, TDMA и WCDMA. Эти операторы сети предоставляют услуги передачи голоса и данных своим собственным абонентам и абонентам из других сетей. Когда оператор сети предоставляет услугу абоненту из зарубежной страны, это называется "международным роумингом". Когда оператор сети предоставляет услугу абоненту из другой сети в той же стране, это называется "национальным роумингом".

Когда абонент регистрируется в сети, с которой он имеет прямые расчетные отношения, обслуживающая сеть часто называется домашней сетью мобильной связи общего пользования или HPMN. Если абонент находится в сети, с которой он не имеет прямых расчетных отношений, обслуживающая сеть называется гостевой сетью мобильной связи общего пользования или VPMN, и абонент называется данной VPMN прибывающим роумером. Тот же абонент называется данной HPMN убывающим роумером. В таком случае прибывающие роумеры обрабатываются как временные абоненты исходя из перспективы доступности обслуживания, тогда как выставление счета за использование, совершенное ими, осуществляется посредством межоператорских расчетов через домашнюю сеть абонента.

Различные операторы сети имеют партнерские соглашения друг с другом, которые включают в себя более благоприятную стоимость роуминга, чем принимают непартнеры. Партнерские сети являются "предпочтительными" сетями для абонента сети оператора для регистрации при роуминге. Непартнерские сети являются "непредпочтительными" сетями для абонента. Операторы сети могут максимизировать свою маржу, и роумеры могут получить более привлекательные цены на роуминг и услуги, если роумеры осуществляют роуминг в предпочтительных партнерских сетях их домашнего мобильного оператора.

Когда "домашние" абоненты осуществляют роуминг в гостевых сетях, они могут осуществлять роуминг в одной, двух или более VPMN, любой одной за раз, на основе различных критериев. Чтобы лучше это понять, рассмотрим случаи, когда телефонная трубка может быть в одном из двух режимов: режиме автоматического выбора сети; или режиме ручного выбора сети.

В автоматическом режиме телефонная трубка автоматически использует набор правил, чтобы найти сеть для регистрации в ней. Порядок этих правил может зависеть от поставщика телефонной трубки; однако, промышленные спецификации указывают нижеследующий порядок:

- 1) последняя выбранная сеть (из EFLOC1 на UICC, причем UICC является, например, SIM-картой или встроенной UICC, неизвлекаемой из терминала, также называемой e-UICC);
- 2) домашняя сеть, если она доступна (на основе MCC и MNC из IMSI, хранящегося в UICC);
- 3) если последняя зарегистрированная сеть не найдена, телефонная трубка пытается зарегистрироваться в списке сетей списка предпочтительных PLMN (EFPLMNSEL на UICC) в приоритетном порядке, исключая ранее выбранную PLMN (телефонная трубка сканирует частотный диапазон GSM 900 до того, как она сканирует частотный диапазон GSM 1800);
- 4) другая PLMN с уровнем принимаемого сигнала выше -85 дБ/мВт в случайном порядке, исключая ранее выбранную PLMN; и
- 5) любая другая PLMN, исключая ранее выбранную PLMN, в порядке уменьшения силы сигнала, или в качестве альтернативы может быть выбрана ранее выбранная PLMN, игнорируя силу ее сигнала.

В ручном режиме телефонная трубка показывает пользователю список доступных сетей. Пользователь выбирает одну из них, и телефонная трубка пытается зарегистрироваться в этой сети. Если регистрация не успешна, телефонная трубка снова показывает пользователю список сетей. В ручном режиме пользователь выбрал конкретную сеть, так выбор предпочтительной VPMN с позиции HPMN не должен применяться. Однако большинство текущих телефонных трубок находятся в режиме автоматического выбора, и HPMN продолжает управлять и/или влиять на сеть роуминга, выбранную ее убывающими роумерами. Также, так как HPMN хотела бы обеспечить режим ручного выбора, она должна идентифицировать текущие настройки на телефонной трубке. Однако реализация цельного механизма, чтобы это сделать, была до сих пор трудной задачей.

За последние несколько лет доходы операторов сети от домашних абонентов постоянно ухудшаются из-за увеличившейся конкуренции и возникающего в результате давления цен. С другой стороны, доходы от роумеров постоянно росли в тот же период из-за увеличившегося проникновения мобильной связи на местные рынки и увеличения путешествий. Более того, доходы от роуминга являются высокомаржинальными доходами, которые обычно содержат между 8-25% общих доходов оператора сети. Поэтому, защита существующих доходов от роуминга и дополнительное их повышение стали важным приоритетом для операторов сетей по всему миру.

Некоторые операторы также владеют сетями в различных странах. Эти операторы хотели бы быть уверенными, что их убывающие роумеры остаются внутри групповой собственности, или остаются в пред-

почтительных сетях, для того чтобы получить наилучший опыт обслуживания даже во время роуминга. Они также будут иметь возможность предложения тарифных планов на основе географического местоположения (например, единая цена по всей западной Европе и юго-восточной Азии) для пользователей, которые подписались на такие планы. В дополнение, по мере внедрения новых технологий, они могут управлять расписанием рассылок в своей собственной собственности и также быть уверенными, что позаботились о проблемах взаимодействия. Удержание абонентов в роуминге в предпочтительных сетях дает наилучший опыт обслуживания абоненту. Однако текущие способы управления тем, в какой сети регистрируется абонент при роуминге, имеют недостатки.

Например, широко используемый способ осуществления попытки предохранения абонентов в роуминге от регистрации в неpreferred сетях включает в себя хранение списка preferred сетей на SIM в телефонной трубке абонента (списка preferred сетей PLMN). Список может быть обновлен с использованием сообщений "по воздуху" (OTA-сообщений). Этот список влияет на изначальный выбор preferred сети. Однако по различным причинам (например, preferred сеть недоступна в текущий момент, или есть временная потеря покрытия), телефонная трубка может также выбрать неpreferred сеть. После того как пользователь оказался в неpreferred сети, он/она будет оставаться там, пока неpreferred сеть не потеряет радиопокрытие. Даже когда питание телефонной трубки выключено, неpreferred сеть остается в SIM-карте, и при следующем включении питания она будет выбрана согласно правилам, описанным в настоящем документе. Таким образом, как только телефонная трубка инициирует попытку регистрации в неpreferred сети, оператор сети теряет управление роумером. Для того чтобы управлять телефонной трубкой в preferred сети, на телефонную трубку могут быть отправлены SS7- (системы сигнализации № 7) сообщения отклонения (сообщения отклонения RNA или UDV). Однако такие сообщения отклонения не гарантируют, что телефонная трубка соединится с preferred сетью, особенно когда сигнал мощности, принятый от базовой станции preferred сети, ниже заданной пороговой величины (-85 дБ). В этом случае телефонная трубка будет автоматически пытаться соединиться с другой сетью, даже если не присутствует в списке preferred сетей, причем эта другая сеть представляет сигнал с лучшей мощностью, чем preferred сеть.

Было бы предпочтительно для оператора сети сохранять некоторый контроль над телефонной трубкой абонента в роуминге, даже когда телефонная трубка инициировала попытку регистрации в preferred сети по какой-либо причине, такой как сбой списка сетей в SIM, чтобы произвести регистрацию в preferred сети.

Известно, что некоторые способы управления не работают на некотором мобильном оборудовании (мобильные телефоны, компьютеры, транспортные средства, содержащие UICC или e-UICC). SS7-сеть является сетью, отвечающей за транспортировку сообщений, обмениваемых между шлюзами (MSC, коммутаторами) и базами данных HPMN и VPMN (HLR, VLR, EIR, ...). SS7 является набором телефонных протоколов сигнализации, которые используются для установки большинства телефонных вызовов мировых коммутируемых телефонных сетей общего пользования. Главной целью является установка и разрыв телефонных вызовов. Другие использования включают в себя трансляцию номера, переносимость местного номера, механизмы предварительной оплаты счетов, услуги передачи коротких сообщений (SMS), и разнообразие других услуг массового рынка. Международный протокол SS7 задан посредством ITU-T в его рекомендациях семейства Q.700.

MAP является одной из составляющих протоколов SS7. Означает "прикладную подсистему мобильной связи". MAP предназначена для обнаружения, что мобильное оборудование осуществляет роуминг. Мобильное оборудование прослушивает доступные гостевые сети и пытается соединиться с сетью, представляющей самый сильный сигнал на ее BCCH-канале. Мобильное оборудование отправляет запрос на соединение (запрос обновления местоположения) с его HLR (из HPLMN), и этот запрос перехватывается оборудованием "управления роумингом" из HPLMN (оборудование "управления роумингом" является HLR-выделенным для приема запросов обновления местоположения). Если сеть, с которой оборудование желает соединиться, не является preferred сетью, сеть отправляет сообщение об ошибке на оборудование. Последнее затем пытается соединиться с другой сетью.

Другим способом управления является обновление EFPLMNSEL.

Но это требует, чтобы мобильное оборудование и UICC (или e-UICC) поддерживали команды OTA.

Настоящее изобретение предлагает способ эффективного управления направлением мобильного оборудования в гостевую сеть и, тем самым, увеличивая процент успешных прикреплений роумеров к preferred гостевым сетям.

Настоящее изобретение предлагает способ прикрепления телекоммуникационного терминала в роуминге к гостевой сети, причем этот терминал, содержит защитный элемент, причем способ состоит в передаче из домашней сети на терминал сообщения отклонения, которое зависит от характеристик терминала и защитного элемента.

Предпочтительно, способ состоит в предварительной отправке идентификатора телекоммуникационного терминала от упомянутого телекоммуникационного терминала в HLR сети.

Идентификатором телекоммуникационного терминала является, например, IMEI терминала.

Защитным элементом является, например, UICC.

Сообщением отклонения является сообщение отклонения UDV, сообщение отклонения RNA, сообщение управления по OTA или сообщение OTA - обновления.

Предпочтительно, защитный элемент хранит учетные данные из домашней сети.

Другие признаки и преимущества данного изобретения будут более понятны после прочтения нижеследующего описания предпочтительного варианта осуществления данного изобретения, приведенного посредством только неограничивающего примерного варианта осуществления и исходя из прилагаемых чертежей.

Краткое описание чертежей

Фигура является упрощенной блок-схемой примера способа согласно настоящему изобретению.

Для того чтобы прикрепить находящийся в роуминге телекоммуникационный терминал, содержащий защитный элемент, к гостевой сети оператора (или виртуального оператора) данное изобретение предлагает передавать из домашней сети на терминал сообщение отклонения, которое зависит от характеристик терминала и защитного элемента, который он содержит.

Характеристиками терминала являются, например, удерживаемые из его IMEI, который является уникальным для каждого терминала. Ими может также быть комбинация из по меньшей мере двух из нижеследующих сведений: производитель, модель, тип, версия, ... для того, чтобы точно знать, какой терминал пытается соединиться с гостевой сетью.

Сообщение отклонения также следит за защитным элементом (заданным в широком смысле посредством UICC или e-UICC), взаимодействующим с терминалом: им может быть Sim, USIM,... Характеристики UICC могут быть удержаны из его ICCID или его IMSI.

Характеристики терминала и UICC могут быть переданы самим терминалом на HPLMN при попытке соединения с гостевой сетью. Терминал может отправить идентификатор в HPLMN, например свой IMEI. Также возможно отправить только IMSI из UICC в HPLMN, а HPLMN ассоциирует характеристики терминала, которые должны быть ассоциированы с этим UICC (HPLMN знает, в какой терминал наиболее вероятно вставлен UICC). Когда UICC встроен в терминал в неизвлекаемом виде (e-UICC), HPLMN может удерживать характеристики терминала из IMSI или из ICCID.

Главное заключается в том, что HPLMN, или точнее, оборудование "управления роумингом" сети HPLMN, должно точно знать, каковы характеристики терминала и ассоциированного UICC, который пытается соединиться с гостевой сетью.

Благодаря этой информации HPLMN может отправить сообщение отклонения терминалу/UICC, которое адаптировано для этого терминала и UICC, которую он содержит или с которой работает совместно. Терминал и UICC затем имеют возможность понимания и исполнения команд, принятых из HPLMN.

В качестве примера, бесполезно отправлять на мобильное оборудование сообщение отклонения RNA (роуминг не разрешен) или сообщение отклонения UDV (неожиданное значение данных), если это мобильное устройство не способно понять или управлять им. На стороне UICC бесполезно отправлять команду "Refresh Initialization" ("Обновить инициализацию"), если UICC не имеет возможности его исполнения, даже если мобильное оборудование принимает команды "Refresh STK".

При точном знании характеристик мобильного оборудования и UICC HPLMN имеет возможность отправки команд на мобильное оборудование/UICC, которые будут управлять направлением мобильного устройства в предпочтительную гостевую сеть.

Фигура является упрощенной блок-схемой примера способа согласно настоящему изобретению, причем этот способ реализован на уровне HPLMN роумера в VPLMN.

Способ начинается с начального этапа 1. При приеме запроса обновления местоположения мобильного оборудования (ME), пытающегося прицепиться к гостевой сети, HPLMN, зная характеристики ME и связанной с ним UICC, проверяет, поддерживает ли ME команды RNA (этап 2). Если да, проверяют, поддерживает ли ME команды "STK refresh" (этап 3). Целью этой команды является попросить ME считать файлы, которые были обновлены в UICC во время процедуры управления. Затем проверяют, поддерживает ли UICC команды "Refresh File" (этап 4). Если да, HPLMN отвечает на запрос обновления местоположения с помощью ответа обновления местоположения, содержащего причину отклонения RNA (этап 5), принуждающего ME попытаться соединиться с другой VPLMN.

Если ответы на тесты этапов 3 или 4 отрицательные, процесс переходит на этап 9.

Когда ME пытается прицепиться к предпочтительной сети, HPLMN принимает запрос обновления местоположения. Затем ME обычно соединяется с предпочтительной гостевой сетью (этап 6). Согласно стандарту 3GPP 23.122, когда HPLMN отклоняет запрос обновления местоположения с использованием причины отклонения RNA, ME должно записать отклоненную сеть в список запрещенных сетей для UICC. В результате, ME никогда не будет пытаться снова прицепиться к этой сети. Это может воздействовать на опыт пользователя по причине потери покрытия в случае, когда ME теряет радиосигнал предпочтительной сети, к которой он был прикреплён. Затем HPLMN дает указание очистить по OTA список запрещенных PLMN в UICC и запускает "Refresh file" (этап 7).

Если ME все еще не соединено с предпочтительной сетью после процедуры RNA, HPLMN запускает процедуру управления по OTA, которая состоит из очистки списка запрещенных PLMN, обновления

списка предпочтительных PLMN, очистки зарегистрированной сети в UICC, и запускает "refresh initialization" в UICC (этап 8). После этого этапа 8, ME инициирует процедуру соединения с сетью, принуждающую ME соединиться с предпочтительной сетью оператора HPLMN.

Следует отметить, что этапы 5 и 6 могут быть повторены заданное число раз (например, максимум 3), как показано пунктирной линией 20, если значение счетчика 21 не достигнуто. Это разрешает попытаться соединить ME с предпочтительной сетью несколько раз до этапа 8, если не удалось.

Если ME не соответствует ME RNA (этап 2) или не поддерживает команду "STK Refresh" (этап 3), или если UICC не поддерживает команду "Refresh file" (этап 4) (отвечает "нет" на одном из этапов 2-4), HPLMN проверяет, поддерживает ли ME команды UDV (этап 9). Если да, HPLMN может управлять ME посредством использования SS7-сообщения отклонения UDV (этап 10). После этой процедуры управления UDV ME может быть прикреплено к предпочтительной сети или нет (этап 11). Если ME соединяется с предпочтительной сетью, HPLMN проверяет, принимает ли ME команды "STK Refresh file" (этап 12). Если да, HPLMN проверяет, принимает ли UICC команду "Refresh File" (этап 13). Если да, HPLMN дает указание обновления по OTA списка предпочтительных PLMN в UICC, и она запускает "Refresh file" для ME посредством UICC (этап 7).

Как ранее указано пунктирной линией 22, счетчик может разрешить отправку ограниченного числа (максимум 3, например) сообщений отклонения UDV для того, чтобы принудить ME соединиться с предпочтительной сетью.

Если ME не принимает команды "STK Refresh" (этап 12), или если UICC не принимает команду "Refresh File" (этап 13), HPLMN дает указание обновления по OTA списка предпочтительных PLMN (EFPLMNSEL) на UICC и просит пользователя перезагрузить свое ME (посредством отправки ему SMS, просящего так сделать) (этап 14).

Если ME не соединяется с предпочтительной сетью на этапе 11 (после процедуры UDV), HPLMN проверяет, принимает ли ME команду инициализации "STK Refresh" (этап 15). Если да, HPLMN проверяет, принимает ли UICC команду "Refresh Init" (этап 16). Если да, HPLMN дает указание управления по OTA, как описано выше (этап 8). Если ME не принимает команду "Refresh STK" (этап 15), или если UICC не принимает команду "Refresh Init" (этап 16), HPLMN дает указание обновления по OTA списка предпочтительных PLMN на UICC, и просит пользователя перезагрузить его ME (посредством отправки ему SMS, просящего так сделать) (этап 14).

Эти разные этапы могут быть выполнены посредством HPLMN, знающей характеристики ME и UICC. HPLMN может создать таблицу для каждого типа ME и UICC, причем эта таблица указывает, какая команда может быть успешно отправлена на ME/UICC в зависимости от характеристик этих элементов.

Следует отметить, что способ настоящего изобретения необязательно начинается с тестирования, является ли ME RNA-совместимым. Начальный этап 1 может быть привязан к этапу 9. Также возможно начать процесс с этапа 15, если оператор решает не использовать SS7-команды управления, например если он подозревает, что в VPLMN установлена система управления, противоположная SS7.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ прикрепления телекоммуникационного терминала в роуминге к гостевой сети, причем упомянутый терминал содержит защитный элемент, представляющий собой одно из SIM-карты, UICC, USIM или eUICC, причем упомянутый способ состоит в том, что
 - определяют технические характеристики терминала на основании его IMEI или на основании комбинации по меньшей мере из двух из следующих сведений: производитель, модель, тип, версия;
 - определяют технические характеристики защитного элемента на основании его ICCID или его IMSI;
 - передают из домашней сети на упомянутый терминал сообщение отклонения, которое основано на данных о технических характеристиках упомянутого терминала и упомянутого защитного элемента, для принуждения упомянутого терминала подсоединиться к упомянутой гостевой сети на основании переданного сообщения отклонения.
2. Способ по п.1, при этом он состоит в предварительной отправке идентификатора упомянутого телекоммуникационного терминала от упомянутого телекоммуникационного терминала в HLR сети.
3. Способ по п.2, при этом упомянутым идентификатором является IMEI упомянутого терминала.
4. Способ по любому из пп.1-3, при этом упомянутым защитным элементом является UICC.
5. Способ по любому из пп.1-4, в котором упомянутое сообщение является сообщением отклонения UDV.
6. Способ по любому из пп.1-4, в котором упомянутое сообщение является сообщением отклонения RNA.
7. Способ по любому из пп.1-4, в котором упомянутое сообщение является сообщением управления по OTA.
8. Способ по любому из пп.1-4, в котором вышеуказанное сообщение является сообщением OTA - обновления.

9. Способ по любому из пп.1-4, в котором упомянутый защитный элемент хранит учетные данные из упомянутой домашней сети.

