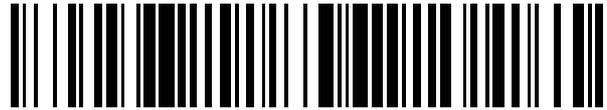


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 469 798**

51 Int. Cl.:

H04W 36/00 (2009.01)

H04W 48/04 (2009.01)

H04W 12/08 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **12.01.2009 E 09737635 (4)**

97 Fecha y número de publicación de la concesión europea: **19.03.2014 EP 2262317**

54 Título: **Método y dispositivo para mantener la continuidad de servicio de usuario**

30 Prioridad:

28.04.2008 CN 200810066885

01.08.2008 CN 200810145545

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

20.06.2014

73 Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129, CN

72 Inventor/es:

YANG, YANMEI y
ZHUANG, XIAOJUN

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 469 798 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Método y dispositivo para mantener la continuidad de servicio de usuario

5 CAMPO DE LA INVENCION

La presente invención se refiere al campo de las tecnologías de comunicaciones y en particular, a una tecnología para mantener la continuidad de servicio de usuario.

10 ANTECEDENTES DE LA INVENCION

Con el desarrollo constante de las tecnologías de comunicaciones, un usuario puede acceder a una red central de un operador por intermedio de cualquiera de los métodos de acceso siguientes: Sistema Global para Comunicaciones Móviles/Tasas de Transmisión de Datos mejorada para Red de Acceso a Radio de Evolución de GSM (GERAN), Red de Acceso a Radio Terrestre de Sistema de Telecomunicaciones Móviles Universal (UTRAN), y red UTRAN evolucionada (eUTRAN).

20 Cuando un usuario se desplaza entre redes para mantener la continuidad de servicios del usuario, se requiere una transferencia, sin discontinuidad entre tecnologías de acceso tales como GERAN, UTRAN, y eUTRAN.

En la técnica anterior, los usuarios que adoptan un Módulo de Identidad de Abonado (SIM) o ejecutan aplicaciones de SIM en una Tarjeta Universal de Circuitos Integrados (UICC) se denominan usuarios de SIM. Cuando un usuario de SIM se comunica en una red UTRAN o una red GERAN y se desplaza a una frontera operativa entre una red eUTRAN y la red UTRAN o GERAN, si la intensidad de la señal de la red eUTRAN es más fuerte que la de otras redes de acceso o si requiere un servicio, la red origen puede seleccionar la red eUTRAN como la red objetivo para transferencia de red y conmutar el usuario a la red eUTRAN temporalmente y por intermedio de un proceso de transferencia normal. En este caso, el usuario del módulo SIM puede utilizar temporalmente los recursos de la red central y luego, ejecutar la Autenticación y Key Acuerdo de Clave (AKA). El módulo SIM, sin embargo, no soporta AKA. Por lo tanto, si el usuario de SIM se identifica durante este proceso, se termina la conexión del usuario del módulo SIM a la red eUTRAN.

Una Patente de Estados Unidos de Martin Stumpert et al, publicada el 12 de agosto de 2004, con número de publicación US2004/0157600 A1, da a conocer un "Método para determinar si conceder, o no, acceso de un equipo de usuario a una red de acceso de radio".

35 El documento 3GPP Draft (3GPP TS 33.401 VI. 1.0, de 19 de abril de 2008, XP050435840) da a conocer que el acceso a E-UTRAN con una aplicación de 2G SIM o de SIM en una UICC no será concedido.

40 Durante la puesta en práctica de la presente invención, el inventor descubre los siguientes inconvenientes en la técnica anterior: La tecnología existente pone en práctica la función de prohibir a un usuario de SIM acceder a una red eUTRAN. El usuario del módulo SIM se conmuta temporalmente a la red eUTRAN, la red eUTRAN rechaza el acceso del usuario del módulo SIM en función del resultado de AKA. En este momento, el usuario del módulo SIM se desconecta de la red originalmente disponible, lo que da lugar a la interrupción del servicio.

45 SUMARIO DE LA INVENCION

Un método, un sistema y un dispositivo para mantener la continuidad de servicio de usuario se dan a conocer en aspectos de la presente invención, para evitar la interrupción del servicio de un usuario de SIM debido al acceso a una red prohibida y para mantener la continuidad de servicio de usuario. A continuación, se enumeran varios aspectos de la invención.

Según el primer aspecto de la idea inventiva, se da a conocer un método para mantener la continuidad de servicio de usuario:

55 cuando un equipo de usuario, UE, necesita realizar una transferencia de red a una Red de Acceso a Radio Terrestre evolucionada de Sistema Universal de Telecomunicaciones Móviles, eUTRAN;

la prohibición, por un controlador RNC o BSC, al equipo de usuario UE acceder a la red eUTRAN antes de que se concluya la transferencia de redistribución cuando el equipo UE adopta una tecnología de aplicación de Módulo de Identidad de Abonado, SIM, para acceso a red según un tipo de triplete del vector de autenticación y

60 la selección, por el controlador RNC o BSC, de una red objetivo accesible para el equipo de usuario UE.

Según el segundo aspecto, un dispositivo para mantener la continuidad de servicio de usuario situado en un Controlador de Red de Radio, RNC, o un Controlador de Estación Base, BSC está provisto de:

65 una unidad de determinación, configurada para determinar si un Equipo de usuario, UE, adopta una tecnología de

aplicación de Módulo de Identidad de Abonado, SIM, para acceso a red, según un tipo de triplete del vector de autenticación cuando el equipo UE necesite realizar una transferencia de red a una Red de Acceso a Radio Terrestre evolucionada de un Sistema de Telecomunicaciones Móviles Universal, eUTRAN; and

5 una unidad de gestión operativa, configurada para prohibir al equipo UE acceder a una red eUTRAN antes de que esté concluida la transferencia de red cuando la unidad de determinación decida que el equipo UE adopte la tecnología de aplicación del módulo SIM para acceso a red y para seleccionar una red objetivo accesible para el equipo UE.

10 Mediante una comparación, puede deducirse que cualquiera de las soluciones técnicas precedentes presenta las siguientes ventajas o efectos beneficiosos sobre la técnica anterior:

En los anteriores aspectos de la presente invención, antes de que un usuario de SIM acceda o temporalmente acceda a una red prohibida, tal como una red eUTRAN, es decir, antes de que se concluya la transferencia, se realiza una determinación sobre un tipo de usuario o tipo de red prohibida. Si el equipo UE es un usuario de SIM, y una red objetivo no permite el acceso de un usuario de SIM, al equipo UE le está prohibido efectuar la transferencia a la red objetivo y se selecciona otra red objetivo para la transferencia. De este modo, se evita la interrupción de servicio que ocurre debido al acceso incorrecto del usuario de la tarjeta SIM a la red eUTRAN y se mantiene la continuidad de servicio de usuario. Además, después de que un equipo UE, en el estado Inactivo se desplaza entre redes, al equipo UE le puede estar prohibido acceder a una red prohibida durante la actualización de ubicación y así se evita la interrupción del servicio causada por el escenario operativo siguiente: Después de que un usuario de SIM, en el estado Inactivo, se desplace a la red eUTRAN y transite desde el estado Inactivo al estado Conectado, la red inicia AKA, pero la tarjeta SIM no soporta AKA. En consecuencia, la continuidad de servicio de usuario se puede mantener en una cierta medida.

25 BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se describe con referencia a algunos dibujos adjuntos como sigue:

30 La Figura 1 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una forma de realización de la presente invención;

La Figura 2 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una primera forma de realización de la presente invención;

35 La Figura 3 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una segunda forma de realización de la presente invención;

La Figura 4 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una tercera forma de realización de la presente invención;

La Figura 5 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una cuarta forma de realización de la presente invención;

45 La Figura 6 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una quinta forma de realización de la presente invención;

La Figura 7 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una séptima forma de realización de la presente invención;

50 La Figura 8 es un diagrama de flujo de un método para mantener la continuidad de servicio de usuario según una octava forma de realización de la presente invención;

La Figura 9 ilustra un sistema de comunicaciones móviles dado a conocer según una novena forma de realización de la presente invención;

La Figura 10 ilustra un dispositivo según una décima forma de realización de la presente invención y

La Figura 11 ilustra una entidad MME según una undécima forma de realización de la presente invención.

60 DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Para conocer mejor la finalidad, la solución técnica, y las ventajas de las formas de realización de la presente invención, a continuación se describen las formas de realización de la presente invención, haciendo referencia a los dibujos, como sigue.

65

Un método para mantener continuidad de servicio de usuario se da a conocer en una forma de realización de la presente invención. Según se ilustra en la Figura 1, el método incluye:

5 Etapa 101: Se realiza una determinación en cuanto a un equipo UE adopta una tecnología de aplicación de SIM para el acceso cuando el equipo UE necesite realizar una transferencia de red.

Etapa 102: Al equipo UE le está prohibido acceder a una red prohibida antes de que se concluya la transferencia de red si el equipo UE adopta la tecnología de SIM para el acceso.

10 Etapa 103: Una red objetivo accesible se selecciona para el equipo UE.

En función de la solución precedente, se describen formas de realización, que soportan la solución, como sigue.

15 Una entidad en un lado de la red interviniente en una primera forma de realización de la presente invención incluye un Controlador de Red de Radio (RNC) virgen o un Controlador de Estación Base (BSC) origen, un Nodo de Soporte de GPRS de Servicio (SGSN), y una MME objetivo, según se ilustra en la Figura 2.

20 Etapa 201: Cuando un UE necesite realizar una transferencia de red, el controlador RNC origen o el controlador BSC origen envía un mensaje de Reubicación/Transferencia Requerida al nodo SGSN origen.

Etapa 202: El nodo SGSN origen determina si el equipo UE es, o no, un usuario de SIM.

25 El método para la obtención el tipo de usuario puede ser como sigue: Un Registro de Posiciones Base (HLR) o un Servidor de Abonado Base (HSS) envía una indicación del tipo de usuario a un nodo SGSN. El proceso de envío específico puede ser como sigue: Después de recibir una demanda de vector de autenticación a partir del nodo SGSN, el HLR/HSS envía un vector de autenticación que transmite la indicación del tipo de usuario al nodo SGSN; o bien, el HLR/HSS inserta el tipo de usuario, tal como un usuario de SIM y usuario de USIM, en datos de suscripción de usuario al nodo SGSN.

30 El método para la obtención del tipo de usuario puede ser también como sigue: El nodo SGSN infiere el tipo de usuario en función del tipo del vector de autenticación obtenido a partir del HLR/HSS. A modo de ejemplo, si el nodo SGSN obtiene un quinteto a partir del HLR/HSS, el nodo SGSN determina que el usuario es un usuario de USIM usuario; si es un triplete, el nodo SGSN determina que el usuario es un usuario de SIM.

35 Conviene señalar que cuando el equipo UE realiza la transferencia inter-SGSN o la reelección de célula, un nuevo nodo SGSN necesita obtener la información del tipo de usuario a partir de un nodo SGSN original. La puesta en práctica del método puede ser como sigue: Durante la preparación de la transferencia, el nodo SGSN original envía la información del tipo de usuario al nuevo nodo SGSN, o el nuevo SGSN obtiene la información del tipo de usuario cuando se obtiene el contexto del equipo UE a partir del nodo SGSN original durante la actualización de la ubicación o la actualización de ruta del equipo de usuario UE.

40 Conviene señalar que el nodo SGSN original, en una forma de realización de la presente invención, indica el nodo SGSN que se adopta antes de la transferencia inter-SGSN o una reelección de célula del equipo UE, y el nuevo nodo SGSN indican el nodo SGSN al que pertenece el equipo UE después de la transferencia inter-SGSN o reelección de célula del equipo UE.

45 El método para la obtención del tipo de usuario puede ser también como sigue: el equipo UE transmite la información del tipo de usuario, a modo de ejemplo, información sobre si el UE es un usuario de SIM, en un mensaje de capa 3 inicial, tal como una demanda de conexión, para permitir al nodo SGSN conocer el tipo de usuario del equipo UE.

50 Si se determina que el equipo UE, que necesita realizar una transferencia de red, no es un usuario de SIM en la etapa 202, el proceso prosigue con la etapa 203 para enviar un mensaje de Reubicación/Transferencia Requerida a una MME objetivo, y se realiza el procedimiento subsiguiente. El usuario no de SIM, sin embargo, puede ser rechazado para acceder a la red objetivo, porque no está registrado en la red objetivo. Si el equipo UE es un usuario de SIM y la red objetivo es una red prohibida para el equipo UE, el proceso prosigue con la etapa 204 para enviar un mensaje de Fallo en la Preparación de la Reubicación al controlador RNC origen o al controlador BSC origen. A la recepción de este mensaje, el controlador RNC origen o el controlador BSC origen puede seleccionar otra red de acceso.

55 En esta forma de realización, durante la preparación de la transferencia, cuando se envía un mensaje de Reubicación/Transferencia Requerida al nodo SGSN origen, el nodo SGSN origen determina el tipo de usuario y asimismo, determina si acceder el equipo UE a una red eUTRAN. En este caso, se evita la interrupción del servicio que ocurre debido a un acceso incorrecto de un usuario de SIM a una red eUTRAN por anticipado y se mantiene la continuidad del servicio. Al mismo tiempo, con el método en esta forma de realización, el usuario de SIM no tiene la posibilidad de utilizar la red eUTRAN y esto evita riesgos de seguridad en dicha red eUTRAN.

La segunda forma de realización es básicamente la misma que la primera forma de realización. La diferencia es como sigue: en la segunda forma de realización, la MME objetivo determinar el tipo de UE, según se ilustra en la Figura 3.

5 Etapa 301: El procedimiento es el mismo que el procedimiento en la etapa 201 en la primera forma de realización.

Etapa 302: Después de recibir el mensaje de Reubicación/Transferencia Requerida, el nodo SGSN origen envía un mensaje de Reubicación/Transferencia Requerida a la MME objetivo y envía el tipo de usuario a la MME objetivo. El tipo de usuario puede transmitirse en el mensaje de Reubicación/Transferencia Requerida o enviarse como un mensaje separado.

El método para la obtención del tipo de usuario por el nodo SGSN origen es el mismo que el de la etapa 202 en la primera forma de realización.

15 Etapa 303: Después de recibir el mensaje de Reubicación/Transferencia Requerida, la MME objetivo determina, en función del tipo de usuario recibido, si el equipo UE es un usuario de SIM.

Si se determina que el equipo UE, que necesita la transferencia a la red eUTRAN, es un usuario de SIM en etapa 303, el proceso prosigue con la etapa 304 para reenviar un mensaje de error al nodo SGSN origen. En etapa 305, el nodo SGSN origen reenvía el mensaje de fallo de transferencia al controlador RNC origen o el controlador BSC origen. A continuación, el controlador RNC origen o el controlador BSC origen selecciona otra red de acceso para el equipo UE.

En esta forma de realización, el nodo SGSN obtiene y reenvía el tipo de usuario. Cuando el mensaje de Reubicación/Transferencia Requerida se envía a la MME objetivo, la MME objetivo determina, en función del tipo de usuario si acceder el equipo UE a la red eUTRAN, y esto impide la interrupción de servicio debida a un acceso incorrecto a la red eUTRAN y mantiene la continuidad del servicio. Al mismo tiempo, mediante el método en esta forma de realización, el usuario de SIM no tiene la posibilidad de utilizar la red eUTRAN y así se evita introducir los riesgos de seguridad en la red eUTRAN.

La principal diferencia entre la tercera forma de realización y las primera y segunda formas de realización es como sigue: en la tercera forma de realización, el equipo UE envía el tipo de usuario al lado de la red. Es decir, la base para determinar el tipo de equipo UE es diferente. Véase la Figura 4.

35 Etapa 401: El equipo UE envía una identidad de tipo al controlador RNC origen o al controlador BSC origen.

Esta identidad de tipo puede transmitirse en un mensaje de demanda de conexión de Control de Recursos de Radio (RRC) o de realización durante el establecimiento de conexión de RRC o transmitirse en otros mensajes de RRC, tales como un mensaje de realización de orden en el modo de seguridad.

Conviene señalar que la identidad de tipo en la forma de realización de la presente invención es un parámetro usado para identificar unívocamente un tipo de UE. El tipo de UE puede ser SIM o USIM. Este parámetro puede ser un campo que identifique al usuario, o una identidad reconocida por el lado de la red y el UE. La identidad de tipo es un nombre adoptado simplemente para facilitar la descripción. Este nombre no puede limitar el ámbito aplicable de la forma de realización de la presente invención. Es decir, en algunos sistemas, no puede adoptarse la expresión de identidad de tipo. Sin embargo, no puede estimarse que el sistema técnico, en la forma de realización de la presente invención, no será aplicable a dichos sistemas.

50 Etapa 402: Cuando el equipo UE necesita realizar la transferencia entre las redes GERAN y UTRAN, el controlador RNC origen o el controlador BSC origen envía el mensaje de Reubicación/Transferencia Requerida, que transmite la identidad de tipo de usuario.

Etapa 403: Después de recibir el mensaje de Reubicación/Transferencia Requerida y la identidad de tipo, el nodo SGSN origen determina si conmutar el equipo UE a la red objetivo en función de si el equipo UE es, o no, un usuario de SIM.

Si se determina que el equipo UE, que necesita realizar una transferencia de red, no es un usuario de SIM en la etapa 403, el proceso prosigue con la etapa 404 para enviar un mensaje de Reubicación/Transferencia Requerida a una MME objetivo y prosigue el procedimiento subsiguiente. El usuario no de SIM, sin embargo, puede rechazarse para acceder a la red objetivo porque no está registrado en la red objetivo. Si el equipo UE es un usuario de SIM, y la red objetivo es una red prohibida para el equipo UE, el proceso prosigue con la etapa 405 para enviar un mensaje de Fallo en la Preparación de la Reubicación al controlador RNC origen o al controlador BSC origen. A la recepción de este mensaje, el controlador RNC origen o el controlador BSC origen puede seleccionar otra red de acceso.

65 Conviene señalar que un sistema alternativo de esta forma de realización puede ser como sigue: El nodo SGSN origen no determina el tipo de usuario, sino que reenvía el mensaje de Reubicación/Transferencia Requerida y la

identidad de tipo a la MME objetivo, que determina el tipo de usuario; o bien, después de recibir la identidad de tipo del equipo UE, el controlador RNC origen o el controlador BSC origen establece las redes prohibidas durante la fase de decisión de la transferencia. A modo de ejemplo, si el equipo UE es un usuario de SIM, el controlador RNC origen o el controlador BSC origen no selecciona una red que prohíba el acceso de SIM, tal como una red eUTRAN.

5 En esta forma de realización, el equipo UE informa de la identidad de tipo al lado de la red, con lo que se facilita a la entidad, en el lado de la red, la lectura directa de la identidad y determinar el tipo de usuario indicado por esta identidad. En consecuencia, la interrupción de servicio debida a un acceso incorrecto de un usuario de SIM a una red eUTRAN puede evitarse durante la decisión de la transferencia o la preparación de la transferencia y así se mantiene la continuidad de servicio del UE. Además, según se indica en las ventajas de las formas de realización anteriores, pueden evitarse los riesgos de seguridad de la red eUTRAN.

15 La cuarta forma de realización de la presente invención es básicamente la misma que las formas de realización anteriores. La diferencia principal es que: el lado de la red consulta al equipo UE y las acciones posteriores dependerán de la respuesta de dicho equipo UE. Véase Figura 5.

20 Etapa 501: Cuando el equipo UE necesite realizar una transferencia de red, el controlador RNC origen o el controlador BSC origen envía un mensaje de consulta al equipo UE. Este mensaje puede transmitir la identidad de tipo de la red objetivo.

Etapa 502: El controlador RNC origen o el controlador BSC origen recibe una respuesta desde el UE.

25 La respuesta puede enviarse por el UE basada en la determinación del UE sobre si acceder, o no, a la red objetivo. Si el UE es un usuario de SIM, y la red objetivo es una red eUTRAN, la información de rechazo del acceso se transmite en la respuesta. En este caso, el controlador RNC origen o el controlador BSC origen necesita seleccionar otra red objetivo. Si el equipo UE determina que puede acceder a la red objetivo, la respuesta transmite la información de aprobación del acceso. En este caso, el controlador RNC origen o el controlador BSC origen realiza la transferencia de red en función de flujo de transferencia normal.

30 La respuesta puede ser también como sigue: el UE no realiza la determinación precedente, sino que informa directamente de su tipo de usuario o información de red prohibida al lado de la red

35 En esta forma de realización, el equipo UE puede elegir, de forma activa, si acceder a la red o el lado de la red determina, en función de la respuesta desde el UE, si permitir, o no, al UE acceder a la red eUTRAN y así se impide el acceso incorrecto de un usuario de SIM a una red eUTRAN y se mantiene la continuidad del servicio.

En la quinta forma de realización de la presente invención, el controlador RNC origen o el controlador BSC origen obtiene una Lista Prohibida o información del tipo de usuario a partir de la red central, según se ilustra en la Figura 6.

40 Etapa 601: Cuando el equipo UE necesite realizar una transferencia de red, el controlador RNC origen o el controlador BSC origen envía un mensaje de Reubicación/Transferencia Requerida al nodo SGSN origen.

45 Etapa 602: El nodo SGSN origen envía el tipo de red prohibida o el tipo de usuario al controlador RNC origen o al controlador BSC origen.

El tipo de red prohibida puede incluir uno o más elementos de datos. El nodo SGSN puede enviar una Lista Prohibida al controlador RNC origen o al controlador BSC origen.

50 El método para la obtención de los tipos de redes prohibidas por el nodo SGSN puede incluir una Lista Prohibida en la información de suscripción. Cuando el equipo UE se registra con el nodo SGSN, el nodo SGSN obtiene la Lista Prohibida en la información de suscripción desde el HLR o HSS, y envía la Lista Prohibida como contexto seguro durante la transferencia o la reelección de célula. La Lista Prohibida puede generarse también por el nodo SGSN en función del tipo de usuario.

55 Etapa 603: El controlador RNC origen o el controlador BSC origen determina si el UE puede acceder, o no, a una red en función de la información del tipo de usuario recibida, o efectúa la lectura de las redes prohibidas del UE a partir de la Lista Prohibida recibida. De este modo, el controlador RNC origen o el controlador BSC origen selecciona una red accesible para la transferencia.

60 Etapa 604: El controlador RNC origen o el controlador BSC origen selecciona una red accesible para la transferencia y envía, de nuevo, un mensaje de Reubicación/Transferencia Requerida.

65 Conviene señalar que esta Lista Prohibida puede enviarse por el nodo SGSN origen al controlador RNC origen o al controlador BSC origen antes de que el equipo UE necesite realizar una transferencia de red. Cuando el equipo UE necesita realizar una transferencia de red, puede consultarse la Lista Prohibida para determinar las redes accesibles para el UE, y luego, el controlador RNC origen o el controlador BSC origen puede enviar un mensaje de

Reubicación/Transferencia Requerida al nodo SGSN origen.

En esta forma de realización, una Lista Prohibida se establece para impedir que el UE acceda a redes prohibidas. Esta lista puede cubrir todas las redes a las que no puede acceder el UE, con lo que se impide correctamente que un usuario de SIM acceda a una red eUTRAN a su debido tiempo y mantiene la continuidad del servicio.

La diferencia principal entre la sexta forma de realización y la quinta forma de realización es como sigue: Los tipos de redes prohibidas no se determinan por el lado de la red, sino que el UE impide a un usuario de SIM acceder a una red eUTRAN.

El procedimiento detallado puede ser como sigue: Una Lista Prohibida se establece manualmente en el UE. Si el equipo UE es un usuario de SIM, se incluye la red eUTRAN en la Lista Prohibida del UE. De este modo, el equipo UE no necesita detectar señales de una red eUTRAN durante cada activación y no mide la banda de frecuencias de la red eUTRAN durante cada medida inter-frecuencias o notifica al lado de la red, en el informe de medición, que no puede detectar una célula de red eUTRAN. De este modo, el lado de la red no selecciona una red eUTRAN como la red objetivo, con lo que se impide a un usuario de SIM acceder a la red eUTRAN.

El flujo de establecimiento operativo precedente puede realizarse por el UE. Es decir, el equipo UE obtiene el tipo de usuario. Si el tipo de usuario indica un usuario de SIM, redes que prohíben el acceso de SIM, tal como una red eUTRAN, se añaden automáticamente a la Lista Prohibida. O bien, el equipo UE determina una red prohibida cuando recibe una orden de medición y pone en práctica el procesamiento subsiguiente.

Conviene señalar que la Lista Prohibida, en esta forma de realización, significa una lista que se utiliza para memorizar las redes prohibidas del equipo UE. Este nombre se adopta simplemente para facilitar la descripción. Este nombre no puede limitar el ámbito aplicable de la forma de realización de la presente invención. Es decir, en algunos sistemas, la expresión de Lista Prohibida no es adoptada. Sin embargo, no puede estimarse que el sistema técnico en la forma de realización de la presente invención no será aplicable a dichos sistemas.

La diferencia principal entre la séptima forma de realización y la quinta forma de realización es como sigue: en esta forma de realización, antes de que el equipo UE necesite realizar una transferencia de red, el lado de la red envía el tipo de usuario o los tipos de redes prohibidas del equipo UE al controlador RNC origen o al controlador BSC origen, según se ilustra en la Figura 7.

Etapa 701: Una conexión de RRC se establece entre el equipo UE y el controlador RNC origen o el controlador BSC origen.

Etapa 702: El equipo UE envía un mensaje de capa 3 inicial, tal como una demanda de conexión, una demanda de servicio y una demanda de actualización de ruta o de ubicación, a la red central.

Etapa 703: Como alternativa, el nodo SGSN origen inicia un flujo de negociación y de autenticación de clave y antes de ello, si ningún vector de autenticación local inutilizado está disponible, el vector de autenticación necesita obtenerse a partir del HLR o del HSS.

Etapa 704: El nodo SGSN origen envía el tipo de red prohibida o el tipo de usuario al controlador RNC origen o el controlador BSC origen.

El nodo SGSN origen puede transmitir el tipo de red prohibida o el tipo de usuario en mensaje de orden, en el modo de seguridad, de Parte de Aplicación de Red de Acceso a Radio (RANAP), u otros mensajes de interfaces, tales como un mensaje de asignación de soporte de acceso a radio. Conviene señalar que esta forma de realización no limita los mensajes de interfaces. Los expertos en esta técnica pueden poner en práctica la presente invención utilizando otros mensajes, tales como un mensaje COMMON ID. Para el modo de envío, véase la descripción pertinente en la quinta forma de realización de la presente invención.

Conviene señalar que, si se utiliza un mensaje de asignación de soporte de acceso a radio para transmitir el tipo de red prohibida o el tipo de usuario, un elemento de información (IE) en el mensaje, tal como el IE de transferencia de servicio, puede usarse para informar al controlador RNC origen o el controlador BSC origen si el equipo UE puede acceder, o no, a una red eUTRAN. A modo de ejemplo, los valores del IE incluyen: debe realizarse la transferencia a eUTRAN, no debe realizarse la transferencia a eUTRAN y no deberá realizarse la transferencia a eUTRAN.

Durante la transferencia, si se cambia el RNC o el BSC que rige al UE, el nodo SGSN origen añade el IE de transferencia de servicio a la demanda de reubicación que se envía al controlador RNC origen o al controlador BSC origen para informar al RNC objetivo si el UE puede acceder, o no, a una red eUTRAN.

Conviene señalar que el método para obtener la información del tipo de usuario sobre si el equipo UE es un usuario de SIM por el nodo SGSN incluye: el envío, por el HLR o HSS, de un vector de autenticación o datos de suscripción de usuario al nodo SGSN y la obtención, por el nodo SGSN, de la información del tipo de usuario transmitida en el

- vector de autenticación o datos de suscripción del usuario; o bien, inferir, por el nodo SGSN, la información del tipo de usuario del equipo UE en función del tipo de vector de autenticación obtenido a partir del HLR o HSS; o bien, la obtención, por el controlador RNC o BSC, de la información del tipo de usuario transmitida en un mensaje de RRC enviado por el equipo UE al lado de la red y el envío, por el controlador RNC o BSC, de la información del tipo de usuario al nodo SGSN; o bien, la obtención, por el nuevo nodo SGSN, de la información del tipo de usuario del equipo UE a partir del nodo SGSN original durante la transferencia inter-SGSN o la reelección de célula; o bien, el envío, por el equipo UE, de un mensaje de capa 3 inicial que transmite la información del tipo de usuario al nodo SGSN.
- Además, conviene señalar que el método para la obtención de la información sobre el tipo de red prohibida por el nodo SGSN incluye: inferir el tipo de red prohibida en función de la información del tipo de usuario o bien, la obtención, por el nuevo nodo SGSN, de la información sobre el tipo de red prohibida a partir del nodo SGSN original durante la transferencia inter-SGSN o la reelección de célula; o bien, la obtención de la información sobre el tipo de red prohibida a partir de los datos de suscripción del usuario.
- Etapa 705: El controlador RNC origen o el controlador BSC origen memoriza el tipo de red prohibida obtenido o el tipo de usuario.
- Conviene señalar que antes de la transferencia a una red eUTRAN, si ocurre una transferencia en el interior de una red UTRAN o una red GERAN, UTRAN y GERAN, como alternativa, el RNC origen o el BSC origen antes de la transferencia (RNC o BSC original, en forma abreviada) necesita transferir el tipo de red prohibida o el tipo de usuario obtenido al controlador RNC origen o al controlador BSC origen después de la transferencia (nuevo RNC o BSC, de forma abreviada).
- Etapa 706: El controlador RNC origen o el controlador BSC origen envía la respuesta correspondiente a la etapa 704 a la red central.
- Etapa 707: Cuando el equipo UE necesite realizar una transferencia, el controlador RNC origen o el controlador BSC origen determina las redes accesibles del equipo UE en función de la información del tipo de usuario o del tipo de red prohibida recibida u obtiene las redes prohibidas del UE a partir de la Lista Prohibida recibida. De este modo, el controlador RNC origen o el controlador BSC origen selecciona una red accesible para la transferencia.
- En esta forma de realización, el lado de la red selecciona una red accesible el UE antes de que el equipo UE necesite realizar una transferencia de red. De este modo, el UE puede acceder directamente a la red accesible durante la transferencia de red manteniendo la continuidad de servicio del usuario y mejorando la eficiencia de la transferencia de la red.
- La Figura 8 es un diagrama de flujo de un método para mantener la continuidad de servicio del usuario en una octava forma de realización de la presente invención. En comparación con la tercera forma de realización, el método para mantener la continuidad de servicio del usuario en la octava forma de realización difiere en que el equipo UE se desplaza a una red eUTRAN en el estado inactivo. El método para mantener la continuidad de servicio del usuario en la octava forma de realización incluye:
- Etapa 801: El equipo UE envía una demanda de Actualización del Área de Seguimiento (TAU) a la MME objetivo después del desplazamiento a una red eUTRAN.
- Etapa 802: La MME objetivo envía una demanda de contexto al nodo SGSN origen para obtener la información pertinente del equipo UE.
- Etapa 803: El nodo SGSN origen reenvía una respuesta de contexto a la MME objetivo. Esta respuesta puede incluir el tipo de usuario o el tipo de red prohibida del equipo UE.
- Etapa 804: La MME objetivo realiza una determinación en función del tipo de usuario o del tipo de red prohibida del equipo UE en la respuesta de contexto. Si el equipo UE es un usuario de SIM o le está prohibido acceder a una red eUTRAN, se realiza la etapa 805.
- Etapa 805: La MME objetivo envía un mensaje de rechazo TAU al UE para rechazar el acceso por el usuario de SIM a la red eUTRAN.
- En esta forma de realización, como alternativa, el equipo UE puede informar del tipo de usuario o del tipo de red prohibida en el mensaje TAU, en la etapa 801, a la MME objetivo, de modo que la MME objetivo pueda decidir si enviar, o no, el mensaje de rechazo de TAU en la etapa 804 en función del tipo de usuario o del tipo de red prohibida. A modo de ejemplo, si el equipo UE es un usuario de SIM o el tipo de red prohibida incluye la red eUTRAN, la MME objetivo envía el mensaje de rechazo de TAU al equipo UE para rechazar el acceso por el usuario del SIM a la red eUTRAN.

Además, en esta forma de realización, después de recibir el mensaje de rechazo de TAU, el UE puede seleccionar otra red accesible, con lo que se evita la interrupción del servicio causada por el escenario operativo siguiente: Después de que un usuario de SIM, en el estado inactivo, se desplace a la eUTRAN y transite desde el estado Inactivo al estado Conectado, la red inicia AKA, pero la tarjeta SIM no soporta AKA. En consecuencia, la continuidad de servicio del usuario puede mantenerse en una cierta medida.

En esta forma de realización, el lado de la red selecciona una red accesible durante la actualización de ubicación, de modo que el UE pueda utilizar directamente los recursos de la red accesible después de transitar desde el estado Inactivo al estado Conectado, con lo que se mantiene la continuidad de servicio del usuario y se mejora la experiencia del usuario.

Un sistema de comunicaciones móviles dado a conocer en una forma de realización de la presente invención se describe como sigue. Este sistema puede poner en práctica las etapas en los métodos en las formas de realización precedentes. Es entendible que el sistema, en esta forma de realización de la presente invención, puede incluir otras entidades que pongan en práctica funciones de comunicación. Esas tecnologías que pueden revelarse por la tecnología existente y las tecnologías normalizadas en el campo de las comunicaciones no se incluyen en esta descripción. Para presentar el sistema de puesta en práctica en esta forma de realización, solamente se describen las principales partes de este sistema. Según se ilustra en la Figura 9, este sistema incluye:

una unidad de determinación 901, configurada para determinar si un equipo UE es un usuario de SIM cuando el equipo UE necesite realizar una transferencia de red; y

una unidad de gestión 902, configurada para prohibir al UE acceder a una red prohibida antes que se concluya la transferencia de red cuando dicha unidad determina que el UE es un usuario de SIM y seleccionar una red objetivo accesible para el equipo UE.

Conviene señalar que esta unidad de determinación puede situarse en el lado del terminal y configurarse para realizar una determinación en función de la información del tipo de usuario o del tipo de red prohibida desde el lado del terminal o bien, situarse en el lado de la red y configurarse para realizar una determinación en función de la información de tipo de usuario o del tipo de red prohibida desde el lado de la red.

Un equipo UE se da a conocer en la novena forma de realización de la presente invención. El equipo UE incluye: una unidad de determinación, configurada para determinar el tipo de módulo de identidad de usuario y una unidad de gestión, configurada para proteger un tipo de red prohibida en función del tipo de módulo de identidad de usuario. La unidad de gestión puede incluir, además: una unidad de medida de la prohibición, configurada para prohibir la medición del tipo de red prohibida.

La Figura 10 ilustra un dispositivo en una décima forma de realización de la presente invención. El dispositivo incluye: una unidad de determinación 1001, configurada para determinar si un equipo UE es un usuario de SIM cuando el UE necesite realizar una transferencia de red; y una unidad de gestión 1002, configurada para prohibir el acceso por el equipo UE a las redes prohibidas antes de que se concluya la transferencia cuando la unidad de determinación determine que el UE es un usuario de SIM. El dispositivo puede situarse en SGSN, MME, RNC o BSC.

La Figura 11 ilustra una MME en una undécima forma de realización de la presente invención. La MME incluye: una unidad de obtención 1101, configurada para obtener información sobre el tipo de usuario o información sobre un tipo de red prohibida de un UE, en donde la información sobre el tipo de red prohibida indica la información sobre un tipo de red que no permite el acceso del UE; y una unidad de gestión 1102, configurada para realizar la gestión en función de la información sobre el tipo de usuario o información sobre el tipo de red prohibida del UE obtenida por la unidad de obtención 1101 después de que el equipo UE, en el estado inactivo, se desplace entre redes. La gestión incluye: prohibición al equipo UE de acceder a las redes prohibidas durante la actualización de ubicación cuando el equipo UE es un usuario de SIM.

El método para la obtención de la información sobre el tipo de usuario o la información sobre un tipo de red prohibida del equipo UE por la unidad de obtención 1101 puede ser como sigue: la obtención de la información sobre el tipo de usuario o información sobre el tipo de red prohibida del equipo UE a partir de la respuesta de contexto enviada por el nodo SGSN, o la obtención de la información sobre el tipo de usuario o la información sobre el tipo de red prohibida del equipo UE a partir del mensaje de actualización de ubicación enviado por el UE.

En la unidad de gestión 1102, el proceso de prohibir al UE acceder a las redes prohibidas durante la actualización de ubicación puede incluir: rechazar el acceso por el usuario de SIM a una red prohibida, tal como una red eUTRAN, enviando un mensaje de rechazo de TAU al UE.

Los expertos en esta técnica pueden realizar la totalidad o parte de las etapas, en el método precedente, utilizando un programa informático para dar instrucciones al hardware. El programa puede memorizarse en un medio de soporte de almacenamiento que pueda ser objeto de lectura por un ordenador. Cuando se ejecuta, el programa

puede incluir las etapas siguientes: prohibir a un UE, que necesite realizar una transferencia de red, acceder a una red prohibida si el equipo UE es un usuario de SIM y seleccionar una red objetivo accesible para el UE. El medio de soporte de almacenamiento puede ser una memoria de solamente lectura, un disco o un disco compacto (CD).

5 En la tecnología existente, cuando un usuario de SIM se comunica en una red UTRAN o GERAN y se desplaza a un
borde entre una red eUTRAN y la red UTRAN o GERAN, si la intensidad de la señal de la red eUTRAN es mayor
que para las otras redes de acceso, o en el caso de necesidades del servicio, la red origen puede seleccionar la
eUTRAN como la red objetivo para la transferencia de red y conmutar el usuario a la red eUTRAN temporalmente
10 mediante el proceso de transferencia normal. En este caso, el usuario de SIM puede usar temporalmente los
recursos de la red central y luego, ejecutar AKA. El módulo SIM, sin embargo, no soporta AKA. Por lo tanto, si el
usuario de SIM se identifica durante esta proceso, la conexión del usuario de SIM a la red eUTRAN se termina,
dando lugar a la interrupción del servicio del usuario. A través del sistema en esta forma de realización de la
presente invención, cuando el equipo UE necesite realizar una transferencia de red, al equipo UE le está prohibido
15 acceder a redes prohibidas y se selecciona una red accesible para el UE antes de que se concluya la transferencia,
con lo que se evita la interrupción del servicio del usuario de SIM durante transferencia de red y se mantiene la
continuidad del servicio. Además, mediante el método en esta forma de realización, el usuario de SIM no tiene la
posibilidad de utilizar la red eUTRAN, con lo que se evita los riesgos de la seguridad en la red eUTRAN. La solución
en la forma de realización de la presente invención, se aplica a la interrupción del servicio causada por un acceso
20 incorrecto a otras redes que prohíben el acceso de los usuarios de SIM además de la red eUTRAN.

La presente invención se describe a través de algunas formas de realización preferidas y los dibujos adjuntos. Es
entendible que, sin embargo, los expertos en esta técnica pueden realizar varios cambios en las formas y detalles
sin desviarse por ello del alcance de protección de la presente invención.

25

REIVINDICACIONES

1. Un método para mantener la continuidad de servicio de usuario, que comprende:

5 cuando un equipo de usuario, UE, necesita realizar una transferencia de red hacia una red evolucionada de Acceso a Radio Terrestre para un Sistema de Telecomunicaciones Móviles Universales, eUTRAN;

la prohibición (102), por un controlador RNC o un controlador BSC, al equipo de usuario UE de acceder a la red eUTRAN antes de que se concluya la transferencia de red cuando el equipo de usuario UE adopte una tecnología de aplicación de Módulo de Identidad de Abonado, SIM, con miras a un acceso de red en función de un tipo de triplete del vector de autenticación y

la selección (103), por el controlador RNC o el controlador BSC, de una red objetivo accesible para el equipo de usuario UE.

15 2. El método según la reivindicación 1, en donde el método comprende, además, una de las etapas siguientes:

el envío (201), por el controlador RNC o BSC, de un mensaje de Reubicación o Transferencia Requerida para un Nodo de Soporte de GPRS de Servicio, SGSN; y la recepción de información sobre un tipo de usuario del equipo UE reenviada por el nodo SGSN;

la obtención, por el controlador RNC o BSC, de información sobre un tipo de usuario del equipo de usuario UE a partir del controlador RNC origen o del controlador BSC origen de una red origen antes de que el equipo UE necesite realizar la transferencia de red si ocurre una transferencia en el interior de la red origen y

25 la obtención, por el controlador RNC o BSC, de información sobre un tipo de usuario del equipo de usuario UE antes de la transferencia de red a partir de un nodo SGSN;

30 en donde la información sobre el tipo de usuario del equipo de usuario UE indica si el equipo UE adopta la tecnología de aplicación SIM con miras a un acceso a red en función de un tipo de triplete del vector de autenticación.

3. El método según la reivindicación 2, en donde:

35 la información sobre el tipo de usuario del equipo UE se envía por el nodo SGSN al controlador RNC o BSC por intermedio de una orden en el modo de seguridad o de un mensaje de asignación de soporte de acceso a radio, o de un mensaje general de identificación ID o de una demanda de reubicación.

4. El método según la reivindicación 3, en donde:

40 la información sobre el tipo de usuario del equipo de usuario UE se transmite por el nodo SGSN en un elemento de información, IE, de transferencia de servicio en la demanda de reubicación al controlador RNC.

5. El método según una de las reivindicaciones 2 a 4, en donde:

45 la información sobre el tipo de usuario del equipo de usuario UE se obtiene por el nodo SGSN por intermedio de una las formas siguientes:

50 obtener la información sobre el tipo de usuario del equipo de usuario UE a partir de un vector de autenticación o de datos de suscripción de usuario enviados por un registro de posiciones base, HLR, o servidor de abonado base, HSS;

inferir la información sobre el tipo de usuario del equipo UE en función del tipo de un vector de autenticación obtenido desde el HLR o HSS;

55 obtener, por el controlador RNC o BSC, la información sobre el tipo de usuario del equipo UE transmitida en un mensaje de RRC enviado por el equipo UE al lado de la red; y el envío, por el controlador RNC o BSC, de la información sobre el tipo de usuario del equipo UE al nodo SGSN;

60 obtener, durante la transferencia inter-SGSN o reelección de célula, la información sobre el tipo de usuario del equipo UE a partir de un nodo SGSN original que se adopta antes de la transferencia inter-SGSN o reelección de célula; y

65 obtener la información sobre el tipo de usuario del equipo UE a partir de un mensaje de capa 3 inicial enviado por el equipo UE.

6. El método según una de las reivindicaciones 1 a 5, en donde la prohibición del acceso de UE a la red eUTRAN comprende:

5 enviar, por un controlador RNC o BSC en un lado de la red, un mensaje de consulta al UE que transmite un indicador de tipo de una red objetivo;

10 recibir, por el controlador RNC o BSC, una respuesta que transmite información de rechazo de acceso, en donde la respuesta se envía por el UE en función del indicador de tipo de la red objetivo si el equipo UE adopta la tecnología de aplicación de SIM para el acceso a red en función de un tipo de triplete del vector de autenticación; y

10 prohibir, por el controlador RNC o BSC, el acceso por el equipo UE a la red eUTRAN;

o comprende:

15 enviar, por un controlador RNC o BSC en un lado de la red, un mensaje de consulta al equipo UE;

recibir, por el controlador RNC o BSC, una respuesta que transmite el tipo de usuario desde el equipo UE, si el equipo UE es un equipo SIM UE; y

20 prohibir, por controlador RNC o BSC, el acceso del equipo UE a la red eUTRAN.

7. Un dispositivo para mantener la continuidad de servicio de usuario situado en un Controlador de Red de Radio, RNC, o un Controlador de Estación Base, BSC, que comprende:

25 una unidad de determinación (1001), configurada para determinar si un equipo de usuario, UE, adopta una tecnología de aplicación de Módulo de Identidad de Abonado, SIM, para el acceso a red en función de un tipo de triplete del vector de autenticación cuando el equipo UE necesite realizar una transferencia de red a una Red de Acceso a Radio Terrestre de Sistema de Telecomunicaciones Móviles Universal, eUTRAN evolucionada; y

30 una unidad de gestión (1002), configurada para prohibir al equipo UE acceder a la red eUTRAN antes de que se concluya la transferencia de red cuando la unidad de determinación determina que el equipo UE adopta la tecnología de aplicación de SIM para el acceso a red y para seleccionar una red objetivo accesible para el equipo UE.

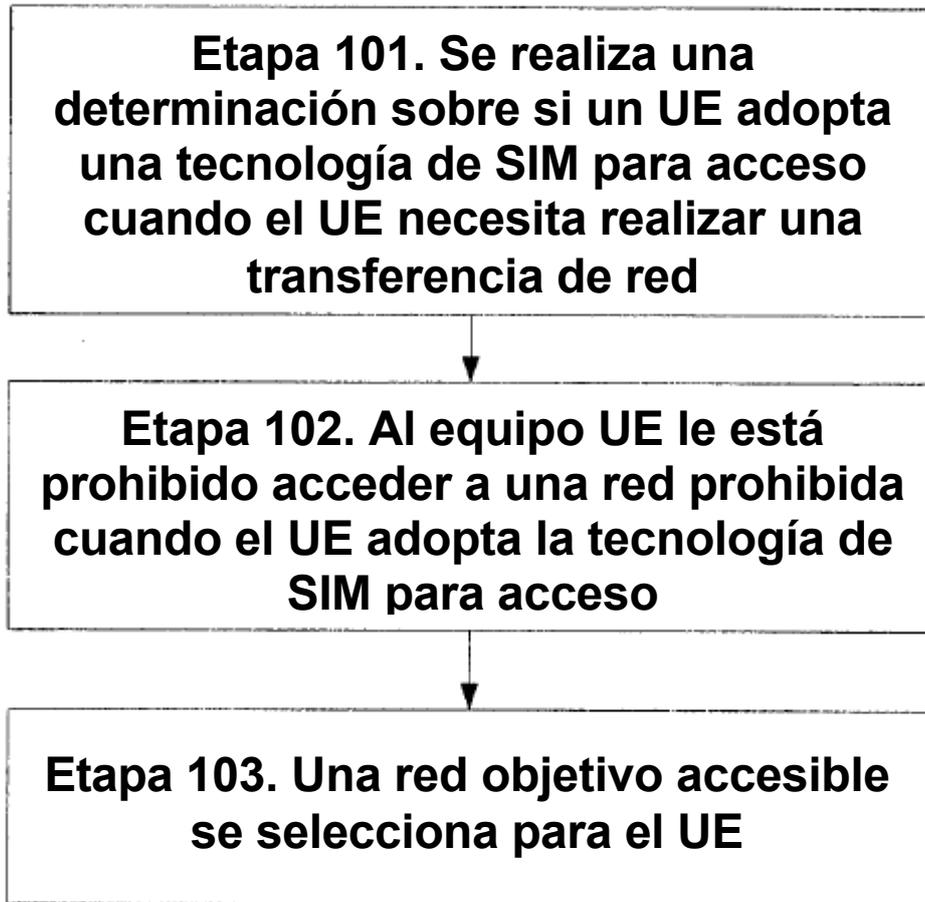


FIG 1

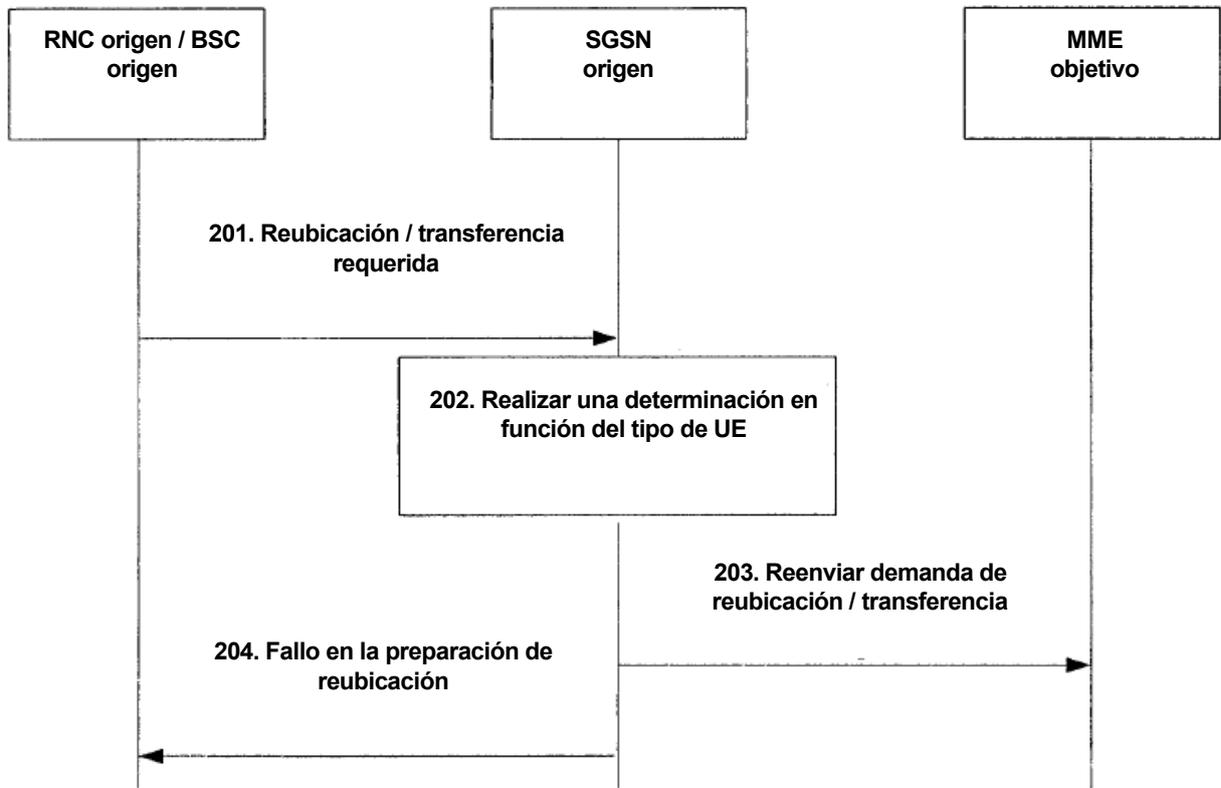


FIG 2

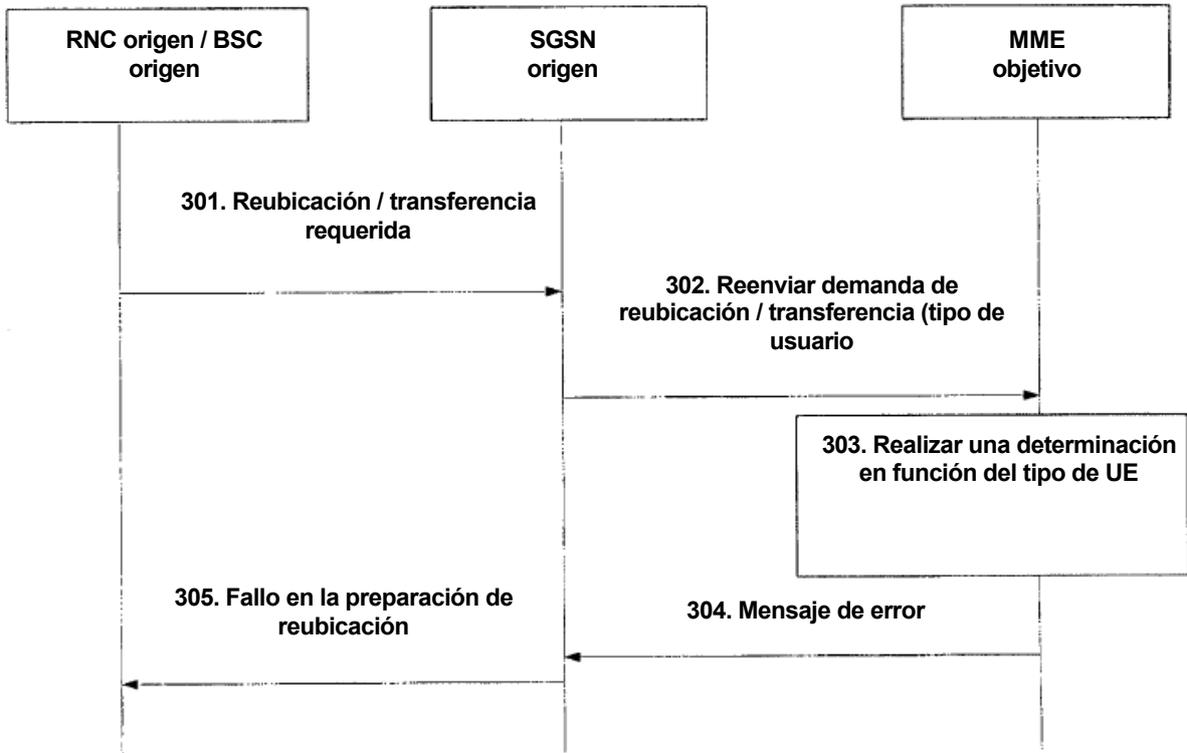


FIG 3

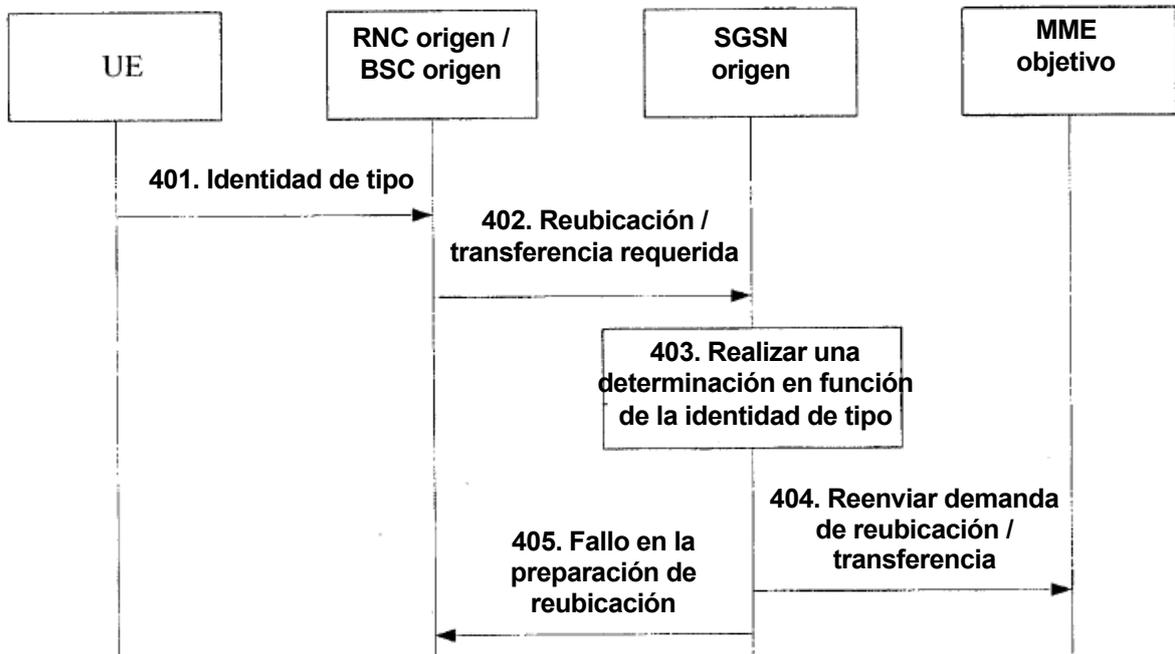


FIG 4

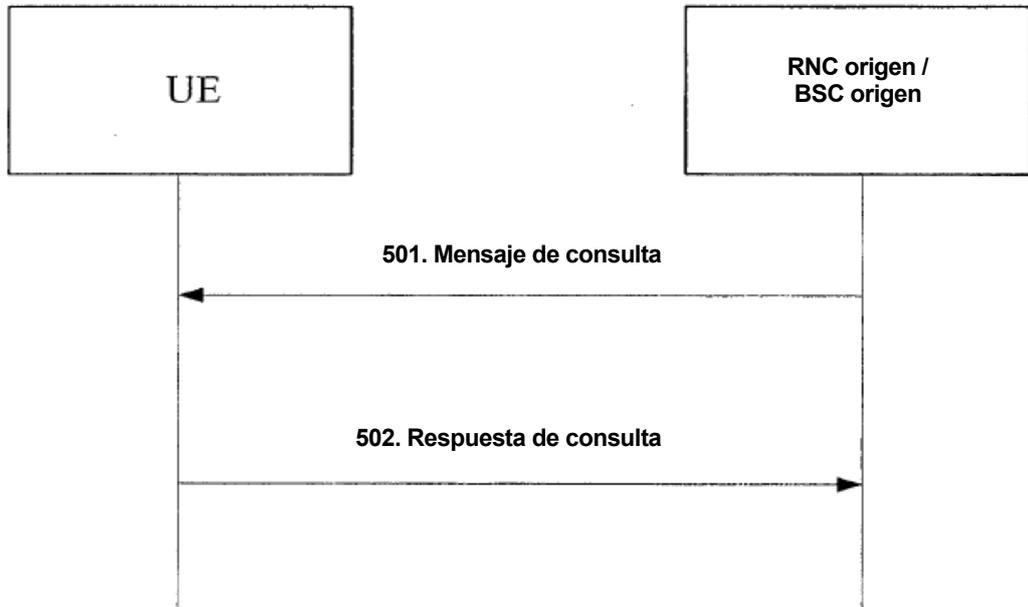


FIG 5

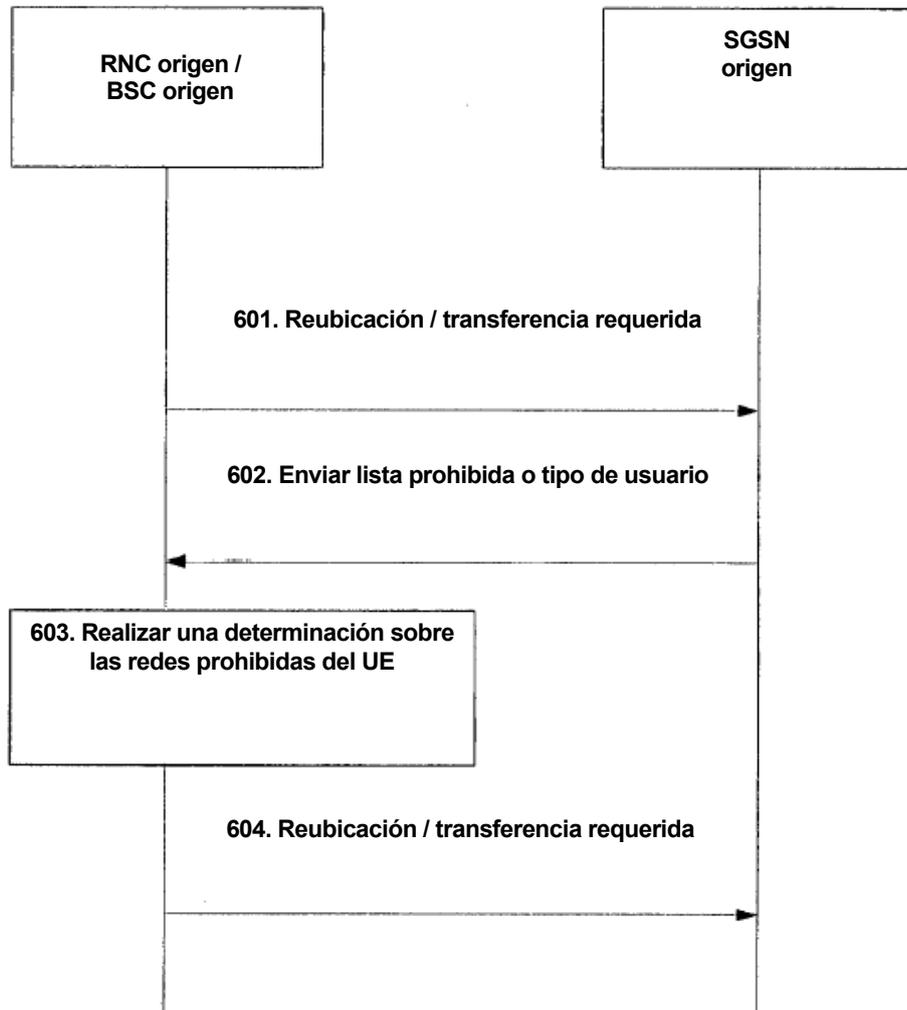


FIG 6

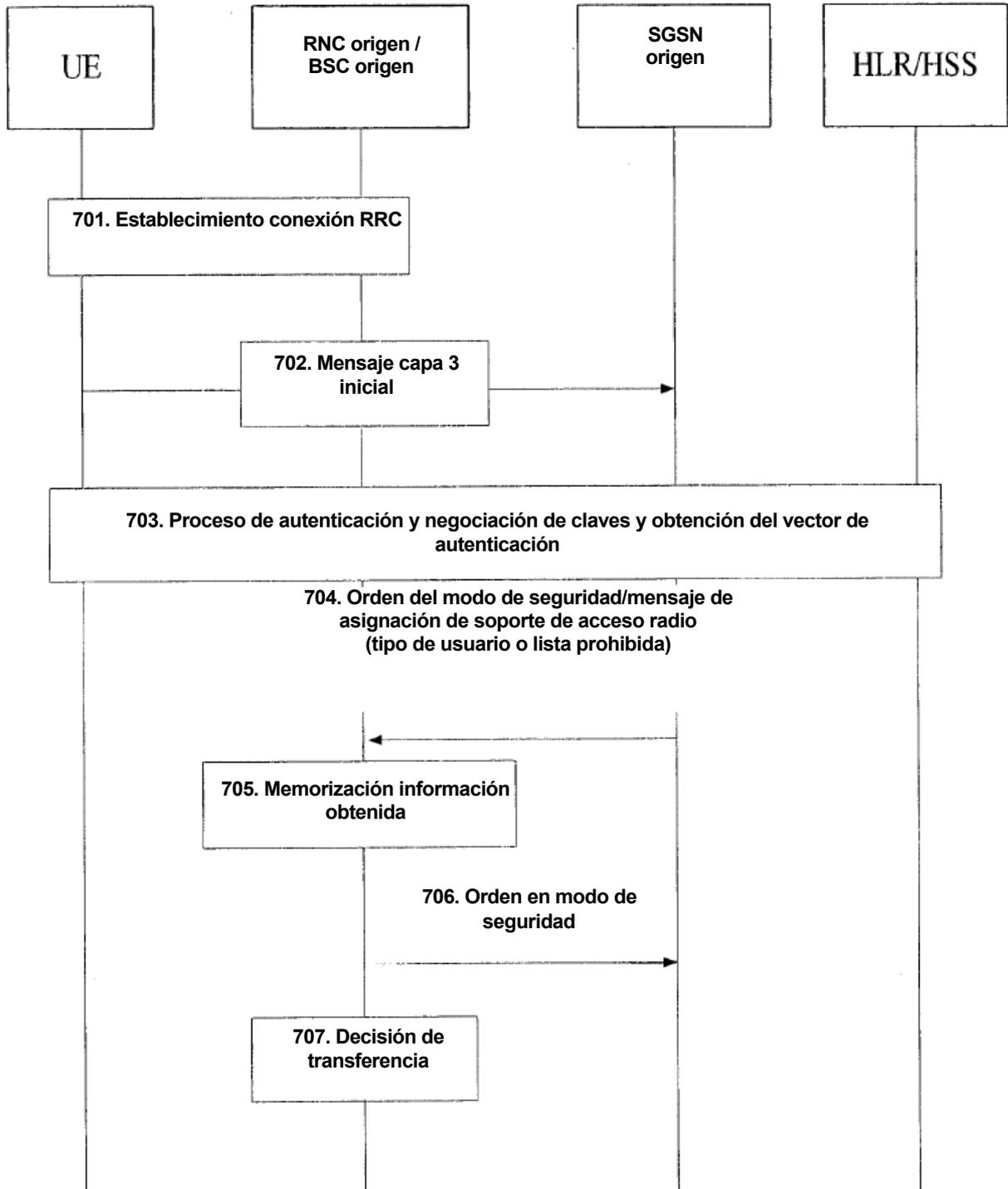


FIG 7

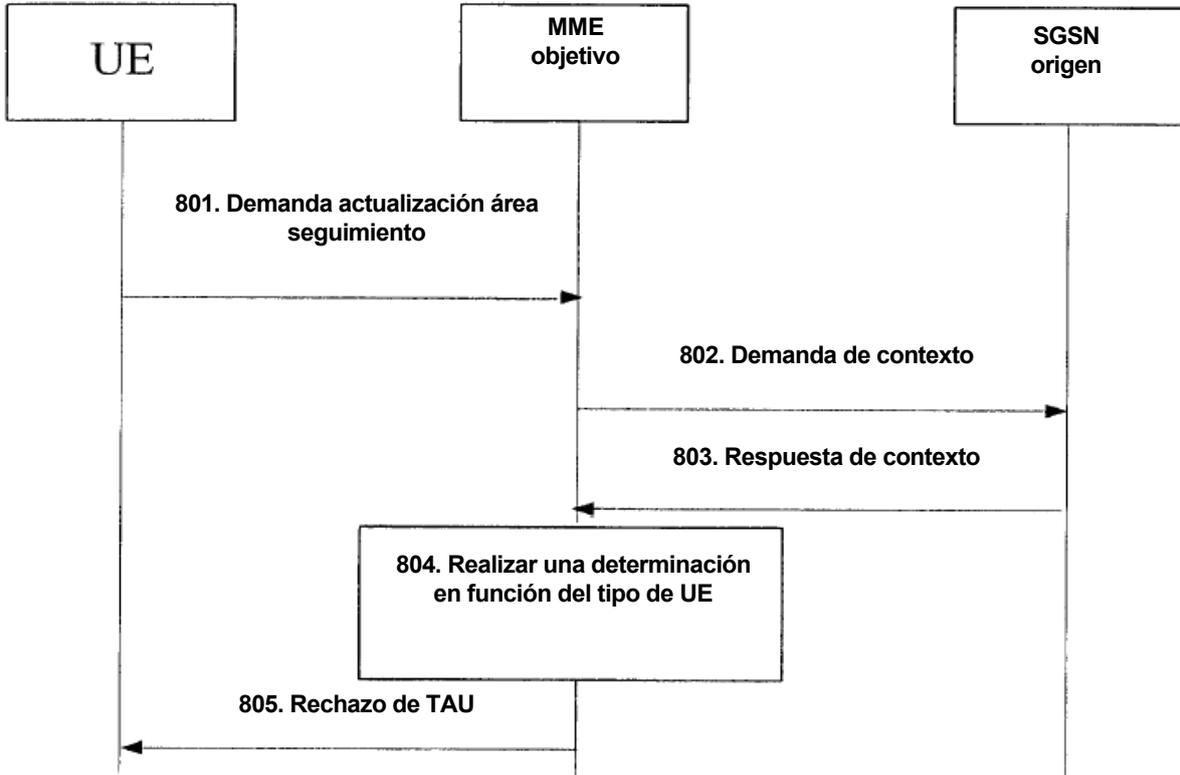


FIG 8

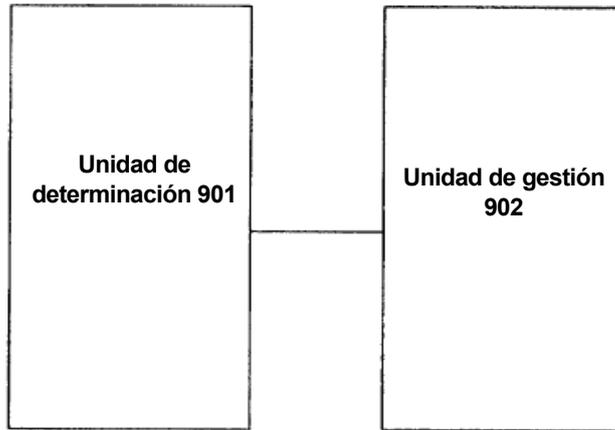


FIG 9

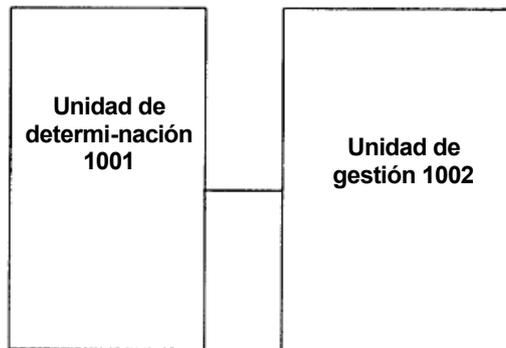


FIG 10

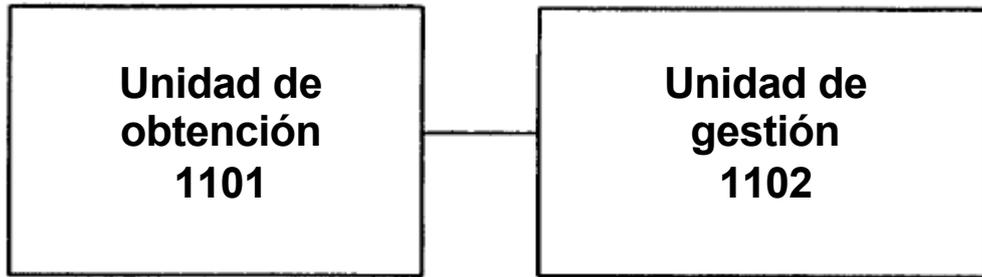


FIG 11