(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 501**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04W 88/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.08.2008 E 08873669 (9)**

(97) Fecha y número de publicación de la concesión europea: **30.03.2016 EP 2255560**

(54) Título: **Identificación de una estación base manipulada o con defectos durante un traspaso**

(30) Prioridad:

28.03.2008 US 40269

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2016

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NORRMAN, KARL;
SMEETS, BERNARD (BEN) y
BLOM, ROLF

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Identificación de una estación base manipulada o con defectos durante un traspaso

CAMPO TÉCNICO

La presente invención se refiere a detección de estaciones base manipuladas o con defectos en una red de telecomunicación celular.

ANTECEDENTES

El 3GPP está estandarizando actualmente la Evolución a Largo Plazo (LTE), que es la continuación de redes 3G. En LTE el cifrado y la protección de integridad del plano de usuario y los datos de control de recursos radio se realizan por la estación base, en este contexto conocida normalmente como el Nodo B evolucionado (eNB). Cuando el enlace de comunicación de un terminal, es decir, un Equipo de Usuario (UE), se traspasa desde un eNB a otro eNB, el eNB de origen informa al eNB de destino sobre qué algoritmos se soportan por el UE y qué algoritmos se permiten para uso por la red. De entre los algoritmos permitidos por la red y soportados por el UE y el eNB de destino, el eNB de destino entonces selecciona el algoritmo que se considera que es el mejor, según criterios de selección predefinidos.

En tal situación, un eNB de origen comprometido puede modificar las listas, indicando qué algoritmos soporta el UE, cuáles permite la red y/o el orden de prioridad de los algoritmos que soporta la red. Dado que el eNB de destino no tiene posibilidad de verificar la autenticidad de estas listas, no puede detectar si un eNB de origen malicioso está engañándole en la selección de un algoritmo débil y posiblemente incluso roto. Tal configuración de ataque se conoce típicamente como un ataque de oferta a la baja.

El grupo de trabajo de seguridad en el 3GPP ha acordado proporcionar una solución para detección de este tipo de ataque de oferta a la baja.

Para la compresión de cómo se puede organizar la señalización de traspaso presente, tal procedimiento, según la técnica anterior, se describirá ahora con referencia al diagrama de señalización de la figura 1. La señalización de traspaso descrita cumple con la Especificación Técnica TS 36.300, "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2", mayo de 2008.

En un primer paso 1:1, un eNB de origen 101 configura procedimientos de medición de UE según la información de área restringida. Como se indica con los pasos 1:2 a 1:5, un UE 100 prepara y envía, un informe de medición al eNB 101 al que está unido actualmente, es decir, el eNB de servicio que se llama el eNB de origen en caso de una situación de traspaso, en donde el UE 100 mide la intensidad de los eNB circundantes y notifica el resultado. El eNB de servicio 101 decide traspasar el UE 100 a un eNB de destino 102 seleccionado, como se indica con un siguiente paso 1:6. El eNB de origen 101 entonces solicita un traspaso desde el eNB de destino, pasando información necesaria a un eNB de destino 102, como se indica con un siguiente paso 1:7. En esta etapa, el eNB de destino 102 puede realizar un procedimiento de control de admisión, como se indica con otro paso 1:8, después del cual el eNB de destino 102 acepta la petición, como se indica con un paso 1:9 y en respuesta el eNB de origen 101 envía un comando de traspaso al UE, que se une al eNB de destino y envía un mensaje de confirmación de traspaso a él, como se indica con otro paso 1:11. En los pasos posteriores 1:12-1:18 se ejecutan preparaciones de traspaso, que comprenden, por ejemplo, sincronización, entre el UE 100 y el eNB de destino 102. Cuando el eNB de destino 102 recibe el mensaje de confirmación de traspaso enviado en un paso 1:19, informa a la Entidad de Gestión de Movilidad (MME) 104 en la red central acerca de la nueva ubicación del UE 100, como se indica con un siguiente paso 1:20. En pasos posteriores 1:21-1:28, la MME asegura que todos los datos enviados a y recibidos desde, el UE 100 se realizan ahora a través del eNB de destino 102, como se indica en un paso final 1:29.

Según el procedimiento descrito anteriormente, no hay forma, no obstante, para la MME 103 de verificar que la información que recibió en la petición de conmutación de camino en el paso 1:20 es correcta y digna de confianza. Hay actualmente dos soluciones bajo discusión en el grupo de trabajo de seguridad en el 3GPP (SA WG3) para manejar el problema mencionado anteriormente. Una se proporciona en el documento S3-080169 (P-CR) "AS algorithms selection mismatch indication" Nokia, Nokia Siemens Networks, 25-29 de febrero de 2008. En resumen la solución descrita en este documento sugiere que, anterior a ejecutar un procedimiento de traspaso, un UE está notificando sus capacidades de seguridad a una Entidad de Gestión de Movilidad (MME), que a su vez envía al UE un conjunto de algoritmos permitidos. La MME además envía una lista ordenada por prioridad de algoritmos, conteniendo solamente algoritmos soportados por el UE, al eNB de servicio, que selecciona uno de estos algoritmos para su uso. Si, durante un procedimiento de traspaso, el UE advierte que el algoritmo seleccionado para su uso en la celda de destino no está incluido en el conjunto de algoritmos permitidos, notifica esto a la MME, el informe que incluye la identidad de celda (ID de celda) de la primera celda donde se detectó la falta de coincidencia. No obstante, este método sufre del problema de que no es posible para el eNB de destino o el UE detectar si el eNB de origen ha modificado el orden de los algoritmos en la lista de redes de algoritmos permitidos. Además, el mecanismo de notificación requerido será complejo, dado que se requiere un procedimiento de Estrato No de Acceso (NAS),

permitiendo al UE notificar el evento descrito a la MME. Usar este mecanismo también provocará un aumento de carga en la interfaz aérea entre el UE y el eNB de destino.

Otra solución al mismo problema se propone en el documento S3-080054 “AS algorithm policy handling”, Ericsson, 25-29 de febrero de 2008 y que consta básicamente de los siguientes pasos:

1. El UE envía sus capacidades de seguridad de UE (SCAP de UE), es decir, sus algoritmos soportados, a la MME.
2. La MME selecciona una lista de algoritmos, aquí conocida como MME_prio_list, en orden de prioridad.
3. La MME envía la MME_prio_list y las SCAP de UE al eNB de servicio.
4. La MME envía la MME_prio_list y la integridad de las SCAP de UE protegidas al UE.
5. El eNB de destino se configura a través de Operación y Mantenimiento (O&M) con un conjunto enumerado de algoritmos permitidos, conocido como O&M_allowed_set.
6. El eNB de destino selecciona un algoritmo que se puede identificar en todas de las tres de las SCAP de UE, MME_prio_list y O&M_allowed_set.
7. El UE notifica su MME_prio_list y las SCAP de UE al eNB de destino.
8. Si el eNB de destino determina que la MME_prio_list y las SCAP de UE recibidas desde el UE no son las mismas que las recibidas desde el eNB de origen puede deducir que ha ocurrido un ataque de oferta a la baja y puede tomar la/s acción/acciones adecuada/s.

No obstante, esta solución no solamente requiere una lista separada de algoritmos, configurados en cada eNB, dado que el UE tiene que proporcionar información al eNB de destino en un comando de confirmación de traspaso, también aumenta el uso de ancho de banda en el enlace aéreo establecido.

También el documento S3-070554, “Bidding down attack at eNB to eNB active mode handover”, Ericsson, 10-13 de julio de 2007, aborda este problema. Se sugieren diferentes soluciones, por ejemplo que el UE pueda informar a la MME acerca del algoritmo seleccionado, por lo cual la MME puede compararlo con las capacidades de UE y las capacidades de eNodoB para detectar una falta de coincidencia. No obstante, una coincidencia no significa necesariamente que la información sobre las capacidades del UE recibidas desde el eNodoB de origen no fuese modificada. Además, tal planteamiento basado en UE presentado en el documento S3-070554 implica mensajes adicionales entre el UE y la MME, que se añaden a la complejidad del UE.

COMPENDIO

Es un objeto de la presente invención abordar el problema, al menos algunos de los problemas perfilados anteriormente. Más específicamente es un objeto de la invención proporcionar un procedimiento mejorado para detección de ataques de oferta a la baja en funciones de seguridad que se originan desde una estación base manipulada o con defectos.

Según una realización, se proporciona un método en una estación base de una red de comunicación, que actúa como una estación base de destino, para permitir la detección de una estación base manipulada o con defectos, que actúa como una estación base de origen en conexión con un traspaso de un equipo de usuario (UE; 300), en donde el método comprende los pasos de:

- recibir una lista de algoritmos priorizada (PAL) desde la red, en donde la lista está enumerando algoritmos permitidos para su uso cuando se comunica con el UE en orden de prioridad;
- recibir la información relacionada con las capacidades de seguridad (SCAP) de UE desde la estación base de origen para el UE que se traspasa desde la estación base de origen a la estación base de destino;
- seleccionar al menos un algoritmo que tiene la prioridad más alta según la PAL de entre los algoritmos que se soportan por el UE según la información relacionada con las SCAP de UE y por la estación base de destino y
- notificar la información relacionada con las SCAP de UE recibida a un nodo de red central que tiene conocimiento de las SCAP de UE del UE, permitiendo por ello al nodo de red central usar la información relacionada con las SCAP de UE para detección de una estación base manipulada o con defectos.

Un aspecto adicional de la invención se refiere a un método en un nodo de red central de una red de comunicación para detección de una estación base manipulada o con defectos, que actúa como una estación base de origen, en conexión con un traspaso de un equipo de usuario (UE) a una estación base de destino, en donde el método comprende los pasos de:

- recibir y almacenar una Lista de Algoritmos Priorizada (PAL) desde la red, en donde la lista está enumerando algoritmos permitidos para el UE en orden de prioridad;
- recibir y almacenar capacidades de seguridad (SCAP) de UE desde el UE;
- recibir, desde la estación base de destino, información relacionada con las SCAP de UE del UE, donde la información relacionada con las SCAP de UE se ha notificado desde la estación base de origen a la estación base de destino previamente durante el procedimiento de traspaso y

- verificar la información relacionada con las SCAP de UE recibida desde la estación base de destino a fin de detectar una estación base manipulada o con defectos comparando al menos parte de las SCAP de UE almacenadas con la información relacionada con las SCAP de UE.

Aún otro aspecto de la invención se refiere a una estación base de una red de comunicación, capaz de actuar como una estación base de destino, para permitir la detección de una estación base manipulada o con defectos, que actúa como una estación base de origen, en conexión con un traspaso de un equipo de usuario (UE), en donde la estación base comprende:

- medios de recepción para recibir una lista de algoritmos priorizada (PAL) desde la red, en donde la lista está enumerando algoritmos permitidos para uso cuando se comunica con el UE en orden de prioridad y para recibir información relacionada con las capacidades de seguridad (SCAP) de UE desde la estación base de origen para el UE que se traspasa entre las dos estaciones base;
- medios de selección (502) para seleccionar al menos un algoritmo a partir de la PAL que tiene la prioridad más alta según la PAL de entre los algoritmos que se soportan por el UE según la información relacionada con las SCAP de UE y que se soporta por la estación base y
- medios de notificación (503) para notificar la información relacionada con las SCAP de UE recibida a un nodo de red central (200) que tiene conocimiento de las SCAP de UE del UE a través de unos medios de transmisión (504), permitiendo por ello al nodo de red central usar la información relacionada con las SCAP de UE para detección de una estación base manipulada o con defectos.

Aún otro aspecto de la invención se refiere a un nodo de red central de una red de comunicación para detección de una estación base manipulada o con defectos, que actúa como una estación base de origen, en conexión con un traspaso de un equipo de usuario (UE) a una estación base de destino, en donde el nodo de red central comprende:

- medios de recepción para recibir una Lista de Algoritmos Priorizada (PAL) desde la red y almacenar dicha PAL, en donde la lista está enumerando algoritmos permitidos para el UE en orden de prioridad, para recibir capacidades de seguridad (SCAP) de UE desde el UE y para almacenar las SCAP de UE y para recibir información relacionada con las SCAP de UE del UE desde la estación base de destino, donde las SCAP de UE se han notificado desde la estación base de origen a dicha estación base de destino previamente durante el procedimiento de traspaso y
- medios de verificación (203) para verificar la información relacionada con las SCAP de UE recibida desde la estación base de destino a fin de detectar una estación base manipulada o con defectos comparando al menos parte de las SCAP de UE almacenadas con la información relacionada con las SCAP de UE.

El nodo de red central es típicamente una Entidad de Gestión de Movilidad (MME).

En caso de que se use la misma PAL para todos los UE, se puede comunicar una PAL global desde la red o bien directamente desde el sistema de operación y mantenimiento a cada estación base en la red y a un nodo de red central, tal como, por ejemplo, una MME o bien se puede comunicar al nodo de red central, que a su vez distribuye la PAL global a todas las estaciones base en la red.

También es posible que la misma PAL se envíe a una cierta parte de la red, pero que diferentes partes de la red tengan diferentes PAL. Alternativamente, la PAL es única para cada UE, de manera que puede contener solamente algoritmos que se conoce que son soportados por el UE. En tal caso, la PAL única de UE se distribuye desde la red a la estación base de destino a través de la estación base de origen.

Además, dado que todas las estaciones base son conscientes del orden de prioridad correcto debido a la PAL, la invención proporciona alta granularidad dado que además de detectar que el algoritmo seleccionado para uso en la celda de destino no reside en el conjunto de algoritmos permitidos, además detecta ataques de oferta a la baja entre los algoritmos dentro del conjunto.

Además, el mecanismo sugerido es simple de implementar, dado que no será necesaria una configuración separada de la estación base. Además, no se requieren nuevos procedimientos de señalización dado que toda información asociada con el mecanismo de verificación sugerido se puede llevar a cuestas en mensajes ya existentes. Por ejemplo, cuando la estación base de destino envía un mensaje de conmutación de camino a un nodo de red central, tal como una MME, lleva a cuestas las SCAP de UE recibidas desde la estación base de origen en este mensaje. En este punto el nodo de red central puede verificar que las SCAP de UE recibidas desde la estación base de destino coinciden con las SCAP de UE que se almacenan en el nodo de red central. Si hay una falta de coincidencia, el nodo de red central se puede configurar para tomar una o más acciones adecuadas. La identidad del eNB de origen también se puede llevar a cuestas en el mensaje de conmutación de camino, de manera que el nodo de red central será capaz de determinar qué eNB se está comportando mal o funcionando mal. El UE no necesita estar implicado en el procedimiento descrito, reduciendo por ello la complejidad requerida del terminal. Los recursos radio también se utilizarán más eficientemente cuando se ejecuta el mecanismo sugerido dado que no se requiere señalización separada entre el terminal y el eNB para este propósito.

Otros objetos, ventajas y nuevos rasgos de la invención llegarán a ser evidentes a partir de la siguiente descripción detallada de la invención cuando se considera en conjunto con los dibujos anexos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se describirá ahora en más detalle por medio de realizaciones ejemplares y con referencia a los dibujos adjuntos, en los que:

- La figura 1 es un diagrama de señalización, que ilustra señalización asociada con un procedimiento de traspaso, según la técnica anterior.
- La figura 2a y 2b son esquemas simplificados, que ilustran dos opciones alternativas para distribuir una Lista de Algoritmos Priorizados (PAL) global a las estaciones base de una red.
- La figura 3 es un diagrama de señalización, que ilustra cómo se pueden distribuir unas SCAP de UE, según una realización.
- La figura 4 es un diagrama de señalización, que ilustra un procedimiento de traspaso que comprende los pasos para detectar un eNB de origen malicioso, según una realización.
- La figura 5 es un diagrama de bloques, que ilustra una estación base, adaptado para ejecutar el procedimiento de traspaso de la figura 4, según una realización.
- La figura 6 es un diagrama de flujo, que ilustra los pasos ejecutados por una estación base de destino que ayuda en una detección de una estación base manipulada o con defectos, según una realización.
- La figura 7 es un diagrama de bloques, que ilustra un nodo de red central, adaptado para ser capaz de detectar una estación base manipulada o con defectos, según una realización.
- La figura 8 es un diagrama de flujo, que ilustra los pasos a ser ejecutados por un nodo de red central para detectar una estación base manipulada o con defectos, según una realización.

DESCRIPCIÓN DETALLADA

Descrita brevemente, la presente invención se refiere a un método para detectar una estación base manipulada o con defectos durante un procedimiento de traspaso. La presente invención también se refiere a un nodo de red central adaptado para realizar el método sugerido y una estación base adaptada para ayudar en la realización del método sugerido. Se debe observar que incluso aunque la descripción en la presente memoria se proporciona en la configuración de E-UTRAN, es igualmente aplicable a cualquier sistema donde un nodo de red central proporciona un conjunto de opciones de algoritmo a cualquier tipo de estaciones base radio, seleccionando uno o más de los algoritmos para protección del enlace entre ellas y un UE. Por lo tanto, la configuración de E-UTRAN de más adelante se debería considerar solamente como un ejemplo ilustrativo de una aplicación de la invención propuesta. En particular se señala que los mensajes particulares mencionados en los ejemplos en los que se pasa información entre entidades implicadas en un traspaso van a ser considerados solamente como ejemplos que ejemplifican y, de esta manera, que se pueden usar en su lugar otros mensajes alternativos.

Un método sugerido que implica un traspaso de una sesión de UE entre dos estaciones base, aquí conocidas como eNB, se pueden expresar según la realización descrita más adelante, en donde el método comprende los siguientes pasos principales:

1. Una lista de algoritmos permitidos se proporciona a los eNB de una red de comunicación. Esta lista se ordena según una prioridad específica, en donde, típicamente, los algoritmos con la prioridad más alta son los más deseables para su uso. De ahora en adelante, esta lista se conocerá como la Lista de Algoritmos Priorizados (PAL). La PAL puede ser una lista que es única por UE o usada globalmente con todos los UE.
2. Cuando un UE conecta con la red y proporciona sus algoritmos soportados, es decir, las capacidades de seguridad de UE, a partir de aquí en adelante conocidas como las SCAP de UE, el eNB de servicio selecciona el algoritmo con la prioridad más alta según la PAL soportada por el eNB de servicio.
3. Durante el traspaso, el eNB de origen proporciona las SCAP de UE al eNB de destino y el eNB de destino selecciona el algoritmo con la prioridad más alta según la PAL a partir de los algoritmos que están presentes en las SCAP de UE y soportados por el eNB de destino.
4. Posterior al traspaso, el UE y el eNB de destino usan el algoritmo seleccionado por el eNB de destino en el paso 3 en la siguiente comunicación.
5. El eNB de destino notifica las SCAP de UE a la MME, que verifica que el eNB de origen no ha manipulado las SCAP de UE durante el procedimiento de traspaso.

Por supuesto es posible que el eNB de origen comprometido modifique el algoritmo seleccionado antes de darlo al UE. Esto provocará no obstante solamente que el eNB de destino y el UE usen diferentes algoritmos y por lo tanto la conexión dará lugar a basura. En tal situación el eNB liberaría, según las especificaciones actuales en el 3GPP, el UE. El UE respondería estableciendo una nueva conexión tan pronto como tenga datos para enviar. De manera similar, si la red tiene datos para enviar al UE, se buscaría el UE. Por lo tanto, los efectos de tal escenario no serán duraderos.

Aunque el ejemplo anterior se refiere a la selección de un algoritmo, es obvio para cualquier experto en la técnica que el procedimiento descrito se puede usar también para seleccionar diversos tipos de algoritmos, previstos para

diferentes propósitos, por ejemplo, se puede seleccionar un algoritmo para protección de integridad, mientras que se selecciona otro para propósitos de cifrado, usando el mismo mecanismo.

Más adelante, se describirán en más detalle pasos del método del mecanismo de detección sugerido, con referencia a ejemplos no limitantes.

Como se indicó anteriormente, la Lista de Algoritmos de Prioridad (PAL) es una lista de algoritmos ordenados según lo deseables que son para su uso. Esta lista se configura típicamente por el operador de la red y, dependiendo de la elección de implementación, como se explicará en mayor detalle más adelante, se puede configurar de diferentes formas en diferentes áreas cubiertas por la red.

Generalmente, hay dos casos principales a considerar para distribución de la PAL a los eNB. En el primer caso, la PAL es única por UE. En tal caso la PAL típicamente contiene solamente algoritmos que se conoce que son soportados por el UE respectivo. Esta información se puede derivar a partir de las SCAP de UE del UE respectivo y del conocimiento acerca de algoritmos implementados o desaprobados erróneamente, deducidos a partir de la IMEI del UE o similar. Según el ejemplo descrito, una PAL única de UE se distribuye al eNB de servicio cuando el contexto de UE para el UE respectivo se establece en el eNB. En lo sucesivo este tipo de PAL se llamará una PAL única de UE.

Otro caso en su lugar se refiere a una PAL común que se usa con todos los UE en la red. En tal escenario, la PAL se puede distribuir a cualquier eNB en cualquier momento anterior al establecimiento de un contexto de UE en el eNB. De ahora en adelante este tipo de PAL se conocerá como una PAL global.

Hay varias formas en las que este tipo de PAL se puede distribuir a los eNB de una red de comunicación. Una solución posible se ilustra en la figura 2a. Dependiendo de cómo se maneja la política de seguridad en la red, puede ser preferible configurar esta lista en la MME 200 a través de su interfaz de O&M 201 y tener la MME 200 que distribuye la PAL 202 a los eNB 203a, b, c bajo su control.

Una solución alternativa se muestra en la figura 2b, que ilustra cómo se puede fijar el sistema de O&M 201 en su lugar para configurar los eNB 203a, b, c directamente con la PAL 202.

Cuando un UE se une a la red o llega a ser conocido por primera vez en una MME, por ejemplo, debido a una reubicación de MME o movilidad de modo INACTIVO, informará a la MME de la red acerca de sus SCAP de UE o la MME recuperará las SCAP de UE a partir de la MME a la que se conectó previamente el UE.

La figura 3 muestra tal principio, según una realización, donde las SCAP de UE de un UE 300 terminan en un eNB de servicio 301 cuando el UE 300 establece seguridad con él. En un primer paso 3:1 el UE 300 transmite las SCAP de UE a la MME 200. La MME almacena las SCAP de UE en unos medios de almacenamiento, como se indica con el siguiente paso 3:2 y en un paso posterior 3:3 las SCAP de UE se proporcionan al eNB de servicio 301. Como se explicará más adelante la transferencia de las SCAP de UE desde la MME 200 al eNB 301 puede ser implícita, si, por ejemplo, las SCAP de UE se usan para filtrar una PAL única de UE. En tal caso la PAL filtrada se proporcionaría también al eNB de servicio 301 en el paso 3:3a. Como se indica en un paso opcional 3:3, también se puede distribuir una PAL única al UE 300 en un mensaje asegurado entre la MME 200 y el UE 300, por ejemplo, a través de un Comando de Modo de Seguridad NAS.

En base a las SCAP de UE y la PAL, entregadas en el paso 3:3, el eNB de servicio 301 selecciona algoritmo, como se indica en un siguiente paso 3:4. Después de que se ha seleccionado el algoritmo, el UE 300 y el eNB de servicio 301 pueden intercambiar datos que se protegerán por el algoritmo seleccionado. Esto se ilustra como un procedimiento de transmisión de datos, indicado con un paso final 3:5.

También cuando se usa una PAL global, la MME puede modificar las SCAP de UE a fin de bloquear uno o más algoritmos para un cierto UE. En tal escenario, la MME 200 puede enviar las SCAP de UE modificadas al eNB de servicio 301 en el paso 3:3, mientras que las SCAP de UE originales se envían al UE 300.

En casos de reubicación de MME en un traspaso, la MME de origen puede dotar a la MME de destino con las SCAP de UE y en este caso no hay necesidad por supuesto de que el UE las envíe a la red de nuevo. Esto sirve solamente como un ejemplo de cómo se pasa la información desde el UE a la red. El hecho importante a señalar es que la MME almacena las SCAP para el UE.

Durante un traspaso entre los eNB el eNB de origen estará transfiriendo las SCAP de UE al eNB de destino en un comando de petición de traspaso, como se indica en la TS 36.300 referida previamente.

Para que un eNB malicioso engañe al eNB de destino en el uso de un algoritmo menos deseable que el que se elegiría si el eNB de origen tuviera buen comportamiento, la única posibilidad es modificar las SCAP de UE o la PAL en caso de que la PAL sea una PAL única de UE. Un procedimiento para detectar un eNB de origen malicioso

durante un traspaso, según una realización, se describirá ahora en más detalle por lo tanto con referencia a la figura 4.

En un primer paso 4:1, que corresponde al paso 1:1 de la figura 1, se reenvían informes de medición desde el UE 300 al eNB de origen 400. En base a estos informes, el eNB de origen 400 envía una petición de traspaso (HO) a un eNB de destino 401, como se indica con un siguiente paso 4:2. La petición de HO comprenderá las SCAP de UE, transmitidas previamente al eNB 400 desde la MME o desde otro eNB si el eNB 400 estaba actuando como un eNB de destino en un traspaso previo. Como se mencionó anteriormente, la petición de HO también puede comprender la PAL además de las SCAP de UE. Si la PAL y/o las SCAP de UE se proporcionan al eNB 400 como un valor de comprobación aleatoria, el valor de comprobación aleatoria pertinente de la PAL y/o las SCAP de UE se transmitirá en la petición de HO en lugar de las listas reales. Sobre la base de la PAL y/o las SCAP de UE, el eNB de destino 401 selecciona un algoritmo bajo la suposición de que el eNB de origen se comporta bien, como se indica con otro paso 4:3.

El eNB de destino 401 responde al eNB 400, que representa ahora el eNB de origen, con un reconocimiento de petición de HO, que comprende una indicación del algoritmo seleccionado. Esto se indica con un paso 4:4 en la figura 4. En un siguiente paso 4:5, el eNB de origen 400 transmite un comando de traspaso, que comprende una indicación del algoritmo seleccionado, al UE 300. Como se indica con otro paso 4:6, el tráfico entre el UE 300 y el eNB de destino 401 se protegerá de ahora en adelante con el algoritmo seleccionado. El UE 300 entonces confirma el traspaso ejecutado al eNB de destino 401, en un siguiente paso 4:7. Una vez que se ha completado el traspaso desde el punto de vista de red radio, el eNB de destino 401 envía un mensaje de conmutación de camino, típicamente una petición de conmutación de camino, que comprende las SCAP de UE a la MME 200 para informar a la MME que el UE 300 ha cambiado la ubicación. Esto se indica con un paso 4:8. Las SCAP de UE se pueden llevar a cuestas en el mensaje de conmutación de camino. Si el eNB de destino 401 no tenía una PAL anterior al procedimiento de HO o si la PAL es única de UE, es decir, la PAL se filtró por la MME 200, usando las SCAP de UE a fin de crear una PAL única de UE y, por lo tanto, se proporcionó al eNB de destino 401 desde el eNB de origen 400 en el paso 4:2, también la PAL se añade al mensaje de conmutación de camino. La razón para hacer esto es ser capaz de verificar que la PAL no se ha manipulado por el eNB de origen. Como se mencionó anteriormente, los valores de comprobación aleatoria que representan la PAL y/o las SCAP de UE respectivas se pueden añadir al mensaje de conmutación de camino en lugar de la lista respectiva. Si las SCAP de UE enviadas previamente al eNB de servicio fueron unas SCAP de UE modificadas, estas SCAP de UE modificadas se envían al eNB de destino 401 en el paso 4:2 y a la MME 200 en el paso 4:8.

Cuando la MME 200 ha recuperado el mensaje de conmutación de camino a partir del eNB de destino 401, puede verificar que las SCAP de UE son las mismas que las que ya se almacenaron en la MME, como se indica con un paso 4:9 y, en caso de que también se enviase la PAL única de UE, que coincide con la copia de la PAL almacenada en la MME. Si cualquiera de estas comprobaciones falla, la MME toma una acción adecuada, como se indica con un paso posterior 4:10. Tal acción adecuada puede comprender, por ejemplo, liberar el UE de la red, registrar el evento y elevar una alarma al sistema de O&M.

Según otra realización, alternativa, la solución propuesta se puede hacer incluso más eficientemente sustituyendo la notificación de las SCAP de UE y posiblemente también la PAL, con un valor de comprobación aleatoria de las SCAP de UE y la PAL si es aplicable, en lugar de notificar los valores respectivos por tanto a la MME. En tal caso las SCAP de UE/PAL se comprueban aleatoriamente por el eNB de destino 401 y en lugar de las SCAP de UE/PAL se envía/n el/los valor/es de comprobación aleatoria a la MME 200 en la petición de conmutación de camino en el paso 4:8 y la comparación hecha en el paso 4:9 se hace sobre la base de los valores de comprobación aleatoria de la PAL y/o las SCAP de UE respectivas.

El tamaño del valor de comprobación aleatoria se puede elegir para ser justo lo bastante grande para obtener una probabilidad suficientemente baja de unas SCAP de UE erróneas no detectadas. Típicamente el numero de bits para el valor de comprobación aleatoria se selecciona que sea menor que las SCAP de UE comprimidas en sí mismas. La MME también puede retener el valor de comprobación aleatoria de las SCAP de UE iniciales. En esta configuración solamente necesitan ser comparados los dos valores de comprobación aleatoria de las SCAP de UE y no las SCAP de UE reales en sí mismas. Se puede usar un truco similar en caso de que la PAL necesite ser enviada desde el eNB de destino a la MME.

En caso de que, a través de cálculos previos, se descubra por la MME 200 que dos SCAP de UE diferentes tienen el mismo valor de comprobación aleatoria la MME se puede configurar para comprobar aleatoriamente las SCAP de UE y un desplazamiento que la MME selecciona, por ejemplo, unas SCAP de UE concatenadas con una cadena de 32 bits, aquí conocida como la cadena MME_OFFS. La cadena MME_OFFS se envía entonces por la MME 200 al eNB de servicio 301 junto con las SCAP de UE o PAL en el paso 3:3 de la figura 3. Esta cadena se envía entonces junto con la SCAP de UE o PAL respectiva en los pasos 4:2 y 4:8 de la figura 4, antes de que se use también en el paso de comparación 4:9, permitiendo por ello la distinción de las diferentes listas unas de otras.

La seguridad se puede fortalecer incluso más si el valor de desplazamiento se notifica de vuelta a la MME por el eNB de destino junto con la comprobación aleatoria de las SCAP de UE y desplazamiento en el paso 4:8. Incluso

una cadena combinada según esta realización alternativa puede ser más corta que la lista de SCAP de UE en sí misma.

Los valores de comprobación aleatoria se pueden generar e identificar usando cualquier técnica convencional y, de esta manera, estos procedimientos no se describirán en ningún detalle adicional en este documento. Ejemplos de funciones de comprobación aleatoria adecuadas pueden ser, por ejemplo, cualquier versión truncada de SHA1, RIPEMD-160, que permiten un truncamiento de la cadena de salida de la función de comprobación aleatoria.

También puede ser de interés conocer qué eNB ha manipulado cualquiera de las listas. Esto se puede lograr incluyendo también la identidad (ID de eNB) del eNB de origen en la petición de conmutación de camino enviada en el paso 4:8. Alternativamente, la MME puede ser capaz de identificar el eNB de origen de otra forma distinta de a través de este mensaje. Cuando la ID de eNB del eNB de origen se proporciona a la MME, tal información se debería manejar con cuidado sin embargo. En lugar de rechazar automáticamente un eNB desde la red que parece ser erróneo sobre la base de una ID de eNB, la información se debería registrar preferiblemente y se debería comprobar el eNB. La razón para esto es que un eNB malicioso puede enviar un mensaje de conmutación de camino falsificado para rechazar los eNB que se comportan bien. Parece por lo tanto más adecuado, por ejemplo, elevar una alarma y enviar un técnico de campo para comprobar el eNB de origen sospechoso.

Una estación base, típicamente un eNB, que ayudará a un nodo de red central, típicamente una MME, a identificar un eNB de origen malicioso según los pasos de procedimiento mencionados anteriormente, tendrá que ser adaptada en consecuencia. Tal estación base, capaz de operar o actuar como una estación base de destino, según una realización ejemplar, se describirá ahora en más detalle con referencia a la figura 5.

Se tiene que entender que, además de los medios de estación base descritos en este ejemplo que se adaptan para proporcionar funcionalidad de estación base de destino a la estación base, la estación base también comprende medios convencionales adicionales, que permiten a la estación base manejar tareas adicionales relacionadas con la estación base, incluyendo operar como una estación base de origen, todas según las circunstancias actuales. No obstante, por razones de simplicidad se ha omitido cualquier medio que no sea necesario para la comprensión del mecanismo que está en lo presentado en este documento. La estación base 401 comprende unos medios de recepción convencionales 501, adaptados a recibir una petición de HO, que comprenden la PAL y/o las SCAP de UE de una estación base de origen 400. Los medios de recepción 501 también se pueden adaptar para recibir una PAL global desde un nodo de red central 200, tal como una MME. La estación base 401 también comprende unos medios de selección 502, adaptados para seleccionar uno de los algoritmos que soporta, sobre la base de la información proporcionada a los medios de recepción 501 y, si la PAL se recibió previamente desde la MME 200, también sobre la base de esta información.

Una vez que los medios de selección 502 han seleccionado un algoritmo, se adaptan para iniciar una notificación de la información respectiva proporcionada a los medios de selección, es decir, la PAL y/o las SCAP de UE, a la MME. La notificación se realiza por unos medios de notificación 503, que transmiten la información a la MME a través de una petición de conmutación de camino, a través de unos medios de transmisión convencionales 504. Los medios de notificación 503 de la estación base también se configuran para proporcionar una SCAP de UE/PAL para un UE que se traspasa desde la estación base a una estación base de destino cuando la estación base está actuando como una estación base de origen, como se indica con el paso 4:2 en la figura 4.

Si va a ser aplicada la notificación de valores de comprobación aleatoria, los medios de notificación también se adaptan para proporcionar un valor de comprobación aleatoria de unas SCAP de UE/PAL, que se notifica al nodo de red central 200 a través de los medios de transmisión 504. Tal funcionalidad de comprobación aleatoria se puede proporcionar usando cualquier técnica convencional adaptada por lo tanto.

La función de la estación base descrita anteriormente cuando ayuda a un nodo de red central en una detección de una estación base manipulada o con defectos se puede ilustrar con un diagrama de bloques, como se ilustra con la figura 6.

En un primer paso 600, la estación base recibe una PAL, que puede ser una PAL global, transmitida a todas las estaciones base de la red anterior al traspaso o una PAL transmitida desde una estación base de origen durante un procedimiento de traspaso, tal como la descrita anteriormente, con referencia a la figura 4.

En un siguiente paso 601, la estación base recibe unas SCAP de UE desde el UE en el que va a ser realizado el traspaso. En un paso posterior 602, la estación base usa la PAL y las SCAP de UE para seleccionar uno o más algoritmos. En un paso final 603, la estación base notifica las SCAP de UE y posiblemente también la PAL, a la MME, permitiendo a la MME usar esta información para los propósitos de verificación requeridos.

También el nodo de red central, en las realizaciones descritas ejemplificadas como una MME, tendrán que ser adaptados en consecuencia y, de esta manera, tal nodo de red central, según una realización ejemplificada se describirá ahora en mayor detalle con referencia a la figura 7. En semejanza con la estación base, también la

arquitectura descrita del nodo de red central se simplifica para omitir cualquier medio que no sean necesario para la comprensión de los mecanismos descritos en el foco en este documento.

El nodo de red central 200, comprende unos medios de recepción convencionales 701, adaptados pare recibir unas SCAP de UE tanto desde un UE 300 como desde una estación base de destino 401. Los medios de recepción también están adaptados para recibir una PAL desde la red, como se indicó anteriormente, con referencia o bien a la figura 2a o bien 2b. El nodo de red central 200 también comprende unos medios de almacenamiento 702 para almacenar unas SCAP de UE que se han recibido desde un UE como se describió anteriormente. Unas SCAP de UE recibidas desde una estación base de destino 401 se reenvían a unos medios de verificación 703, que están adaptados para comparar el valor recibido con el valor almacenado correspondiente. El nodo de red central 200 también comprende unos medios de transmisión 704, adaptados para comunicar con una estación base de servicio, como se indicó anteriormente con referencia a la figura 3a o 3b. Si se usan valores de comprobación aleatoria, los medios de verificación 203 según la realización ejemplificada también se adaptan a generar un valor de comprobación aleatoria respectivo para la PAL y/o las SCAP de UE de un UE específico. Tales medios de verificación están adaptados además para comparar un valor de comprobación aleatoria recibido desde una estación base de destino con el valor de comprobación aleatoria correspondiente de unas SCAP de UE o una PAL almacenadas. Además, la unidad de verificación también se puede adaptar con una funcionalidad para identificar valores de comprobación aleatoria idénticos, tanto como, una funcionalidad para generar valores de desplazamiento para distinguir los valores de comprobación aleatoria unos de otros y, en una etapa posterior, para comparar tales valores. Como se indicó anteriormente, tal funcionalidad de generación y comparación, así como una funcionalidad para manejar valores de desplazamiento, se pueden proporcionar usando cualquier técnica convencional y, de esta manera, esta técnica no se describe más allá en esta arquitectura de nodo de red central ejemplificada. Dependiendo del resultado de un procesamiento de información proporcionada al nodo de red central en una petición de conmutación de camino, los medios de transmisión se pueden adaptar para comunicar con cualquier otro nodo adecuado, en donde los medios de verificación 203 se pueden configurar para generar y para reenviar uno o más mensajes a un nodo de notificación 705 a fin de permitir que sea ejecutado un procesamiento adicional adecuado, siguiendo la detección de una estación base errónea o manipulada sospechosa.

En la figura 8 un esquema de bloques ilustra en más detalle la operación de un nodo de red central según una realización ejemplar. En un primer paso 800 el nodo de red central 200 recibe y almacena una PAL, típicamente de una O&M, como se determinó previamente.

En un siguiente paso 801 el nodo recibe y almacena unas SCAP de UE desde un UE. Cuando el UE está a punto de experimentar un HO, el nodo de red también recibe unas SCAP de UE desde la estación base de destino, como se indica en un siguiente paso 802. Ambas SCAP de UE se comparan en otro paso 803. Si se reconoce una falta de coincidencia, como se indica con un paso 804, el nodo de red central toma las acciones adecuadas, como se indica con el paso condicional 805, mientras que el procedimiento termina con un paso final 806 si la comparación resultó con éxito.

Las realizaciones presentes tienen que ser consideradas en todos los aspectos como ilustrativas y no restrictivas. Por lo tanto se tiene que entender que la presente invención también se puede llevar a cabo de otras formas distintas a las expuestas específicamente en la presente memoria sin apartarse de las características esenciales de la invención.

LISTA DE ABREVIATURAS

eNB	Estación base radio LTE
LTE	Evolución a Largo Plazo
MME	Entidad de Gestión de Movilidad
NAS	Estrato No de Acceso
O&M	Operación y Mantenimiento
PAL	Lista de Algoritmos Priorizada
SCAP	Capacidades de Seguridad de UE
UE	Equipo de Usuario

REIVINDICACIONES

1. Un método en una estación base de una red de comunicación, que actúa como una estación base de destino (401), para permitir detección de una estación base manipulada o con defectos, que actúa como una estación base de origen (400), en conexión con un traspaso de un equipo de usuario -UE- (300), dicho método que comprende los pasos de:

- recibir (600) una lista de algoritmos priorizada -PAL- desde la red, dicha lista que enumera algoritmos permitidos para su uso cuando se comunica dicho UE en orden de prioridad;
- recibir (601) información relacionada con las capacidades de seguridad -SCAP- de UE desde la estación base de origen para el UE que se traspasa entre las dos estaciones base;
- seleccionar (602) al menos un algoritmo que tiene la prioridad más alta según la PAL de entre los algoritmos que se soportan por dicho UE según dicha información relacionada con las SCAP de UE y por la estación base de destino**, caracterizado por** el paso de

- notificar (603) la información relacionada con las SCAP de UE recibida a un nodo de red central que tiene conocimiento de las SCAP de UE de dicho UE, permitiendo por ello a dicho nodo de red central usar dicha información relacionada con las SCAP de UE para detección de una estación base manipulada o con defectos.

2. Un método según la reivindicación 1, en donde dicha PAL es una PAL global.

3. Un método según la reivindicación 2, en donde dicha PAL global se distribuye a las estaciones base desde dicho sistema de Operación y Mantenimiento de redes.

4. Un método según la reivindicación 2, en donde dicha PAL global se distribuye a las estaciones base a través del nodo de red central.

5. Un método según la reivindicación 1, en donde dicha PAL es una PAL que es única para dicho UE.

6. Un método según la reivindicación 5, en donde dicha PAL única de UE se distribuye a la estación base de destino a través de la estación base de origen.

7. Un método según cualquiera de las reivindicaciones precedentes, en donde dicho paso de notificación además comprende una notificación de la PAL.

8. Un método en un nodo de red central de una red de comunicación para detección de una estación base manipulada o con defectos, que actúa como una estación base de origen, en conexión con un traspaso de un equipo de usuario -UE- a una estación base de destino, dicho método que comprende el paso de:

- recibir (800) y almacenar una Lista de Algoritmos Priorizada -PAL- desde la red, dicha lista que enumera algoritmos permitidos para dicho UE en orden de prioridad;
- recibir (801) y almacenar capacidades de seguridad -SCAP- de UE desde dicho UE; **caracterizado por** los pasos de

- recibir (802), desde dicha estación base de destino, información relacionada con las SCAP de UE de dicho UE, dicha información relacionada con las SCAP de UE que se ha notificado desde la estación base de origen a dicha estación base de destino previamente durante dicho traspaso,
- verificar (803) la información relacionada con las SCAP de UE recibida desde la estación base de destino a fin de detectar una estación base manipulada o con defectos comparando al menos parte de las SCAP de UE almacenadas con la información relacionada con las SCAP de UE.

9. Un método según la reivindicación 8, en donde la PAL se recibe desde dicho sistema de operación y mantenimiento -O&M- de redes.

10. Un método según la reivindicación 8 o 9, en donde la información relacionada con las SCAP de UE comprende una PAL única de UE que se ha filtrado usando las SCAP de UE respectivas.

11. Un método según cualquiera de las reivindicaciones previas, en donde la información relacionada con las SCAP de UE recibida desde la estación base de destino se lleva a cuestas en otro mensaje recibido desde dicha estación base de destino.

12. Un método según la reivindicación 11, en donde dicho otro mensaje es una petición de conmutación de camino.

13. Un método según cualquiera de las reivindicaciones previas, en donde dicho paso de recepción de información relacionada con las SCAP de UE desde la estación base de destino además comprende recibir la identidad de la estación base de origen.

14. Un método según cualquiera de las reivindicaciones previas, en donde dicha información relacionada con las SCAP de UE comprende un valor de comprobación aleatoria respectivo de la PAL y/o las SCAP de UE de dicho UE.

15. Una estación base (401) de una red de comunicación, capaz de actuar como una estación base de destino, para permitir la detección de una estación base manipulada o con defectos, que actúa como una estación base de origen (400), en conexión con un traspaso de un equipo de usuario -UE-, dicha estación base que comprende:

- medios de recepción (501) para recibir una lista de algoritmos priorizada -PAL- desde la red, dicha lista que enumera algoritmos permitidos para uso cuando se comunica con dicho UE en orden de prioridad y para recibir información relacionada con las capacidades de seguridad -SCAP- de UE desde la estación base de origen para el UE que se traspasa entre las dos estaciones base;
- medios de selección (502) para seleccionar al menos un algoritmo a partir de la PAL que tiene la prioridad más alta según la PAL de entre los algoritmos que se soportan por dicho UE según dicha información relacionada con las SCAP de UE y que se soporta por dicha estación base, **caracterizada por**

  - medios de notificación (503) para notificar la información relacionada con las SCAP de UE recibida a un nodo de red central (200) que tiene conocimiento de las SCAP de UE de dicho UE a través de unos medios de transmisión (504), permitiendo por ello a dicho nodo de red central usar dicha información relacionada con las SCAP de UE para detección de una estación base manipulada o con defectos.

16. Una estación base según la reivindicación 15, en donde la estación base es un eNB.

17. Un nodo de red central (200) de una red de comunicación para detección de una estación base manipulada o con defectos, que actúa como una estación base de origen (301), en conexión con un traspaso de un equipo de usuario -UE- (300) a una estación base de destino (401), dicho nodo de red central que comprende:

- medios de recepción (701) para recibir una Lista de Algoritmos Priorizada -PAL- desde la red y almacenar dicha PAL, dicha lista que enumera algoritmos permitidos para dicho UE en orden de prioridad, para recibir capacidades de seguridad -SCAP- de UE desde dicho UE y para almacenar dichas SCAP de UE, **caracterizado por**

  - medios de recepción (701) pare recibir información relacionada con las SCAP de UE de dicho UE desde dicha estación base de destino, dichas SCAP de UE que se han notificado desde la estación base de origen a dicha estación base de destino previamente durante dicho traspaso y
  - medios de verificación (203) para verificar la información relacionada con las SCAP de UE recibida desde la estación base de destino a fin de detectar una estación base manipulada o con defectos comparando al menos parte de dichas SCAP de UE almacenadas con la información relacionada con las SCAP de UE.

18. Un nodo de red central según la reivindicación 17, en donde dicho nodo de red central es una Entidad de Gestión de Movilidad -MME-.

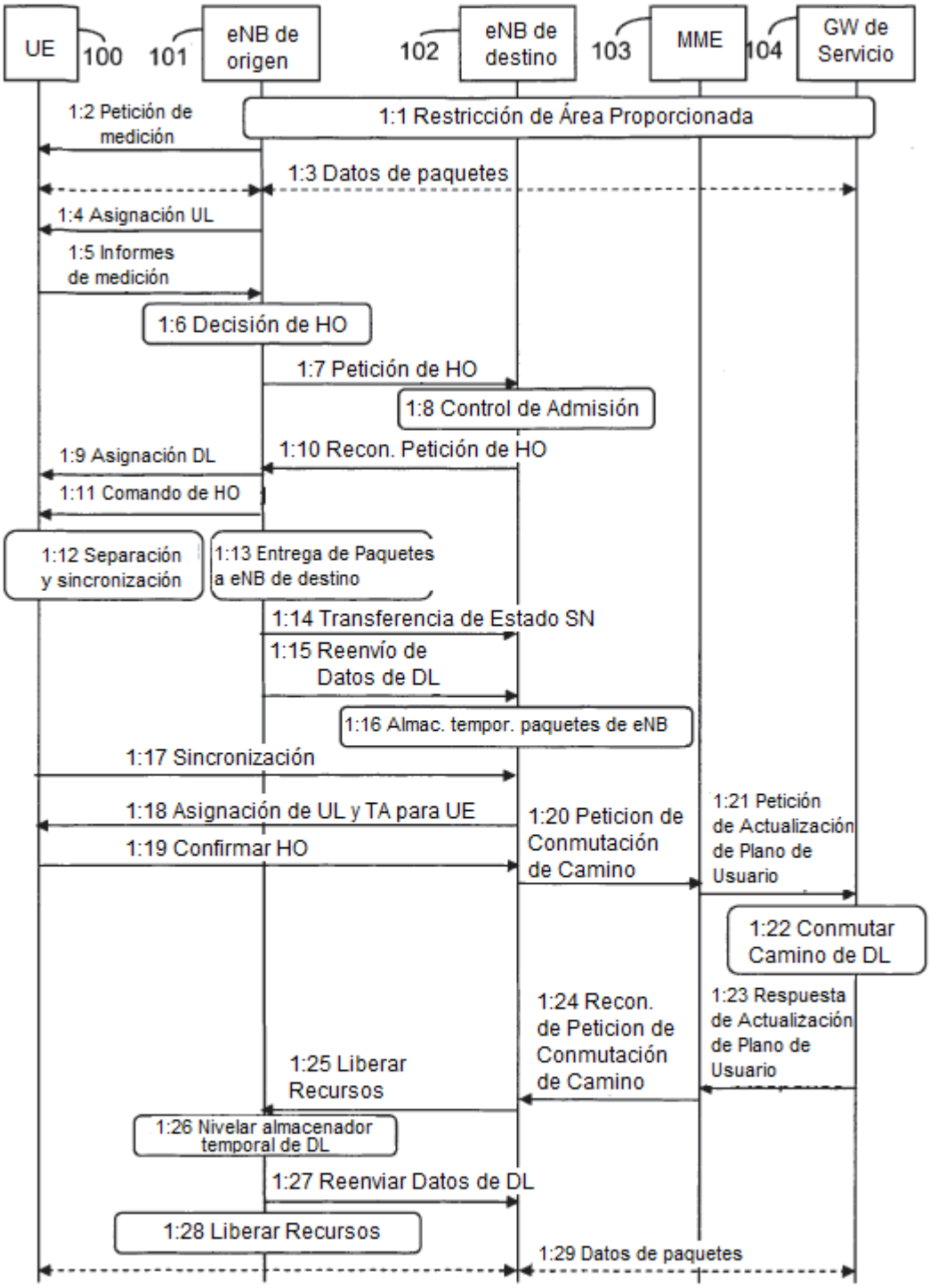

Figura 1 (TÉCNICA ANTERIOR)

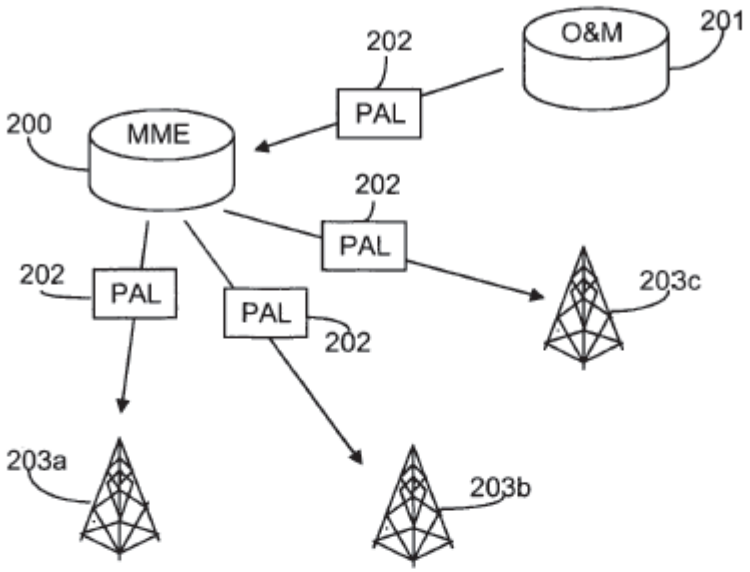

Figura 2a

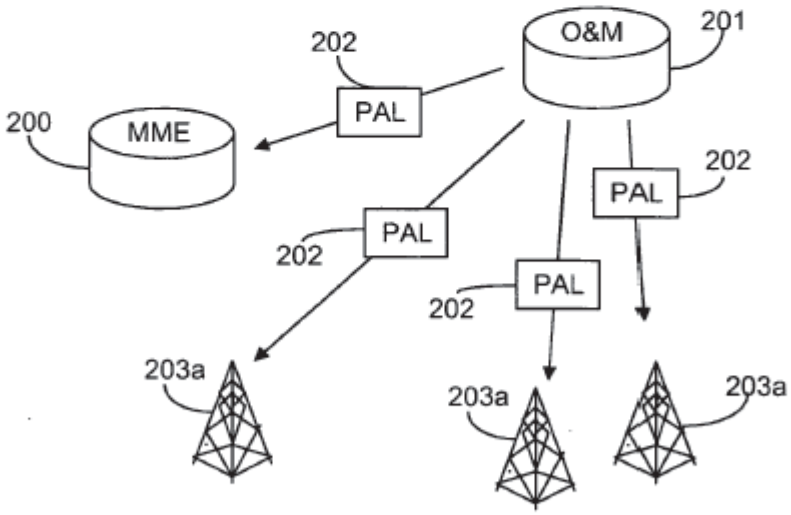

Figura 2b

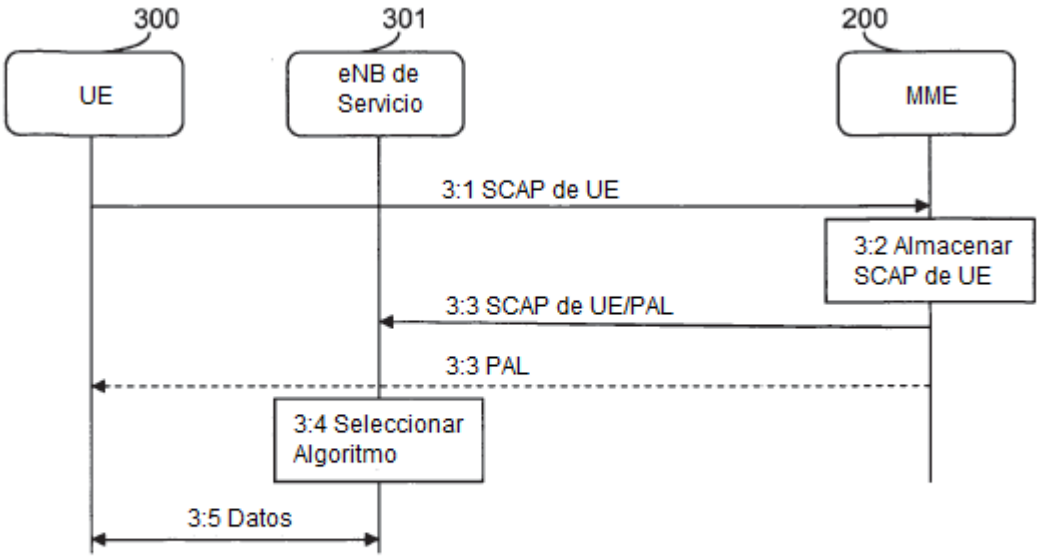

Figura 3

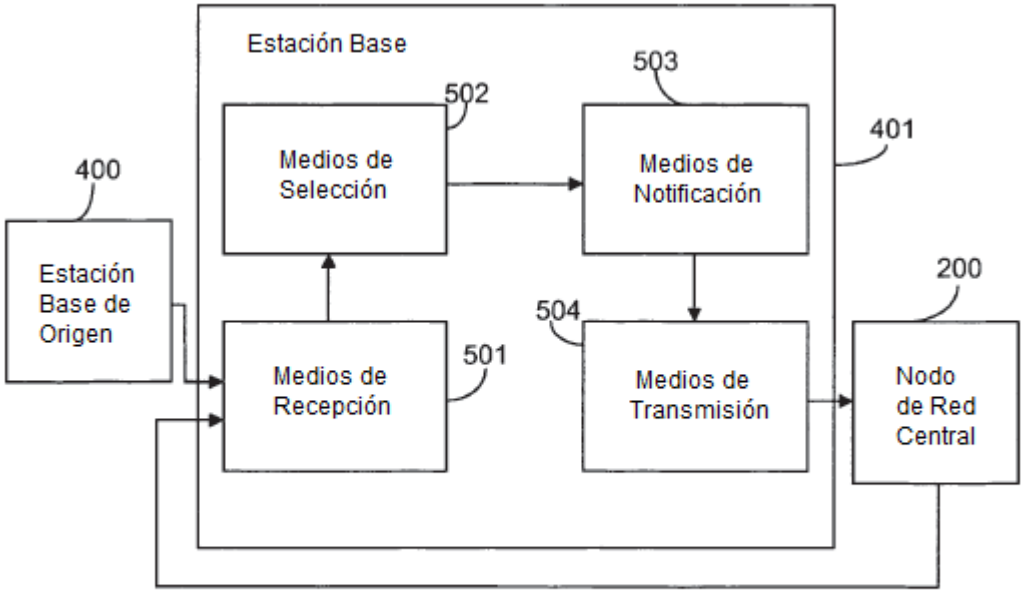

Figura 5

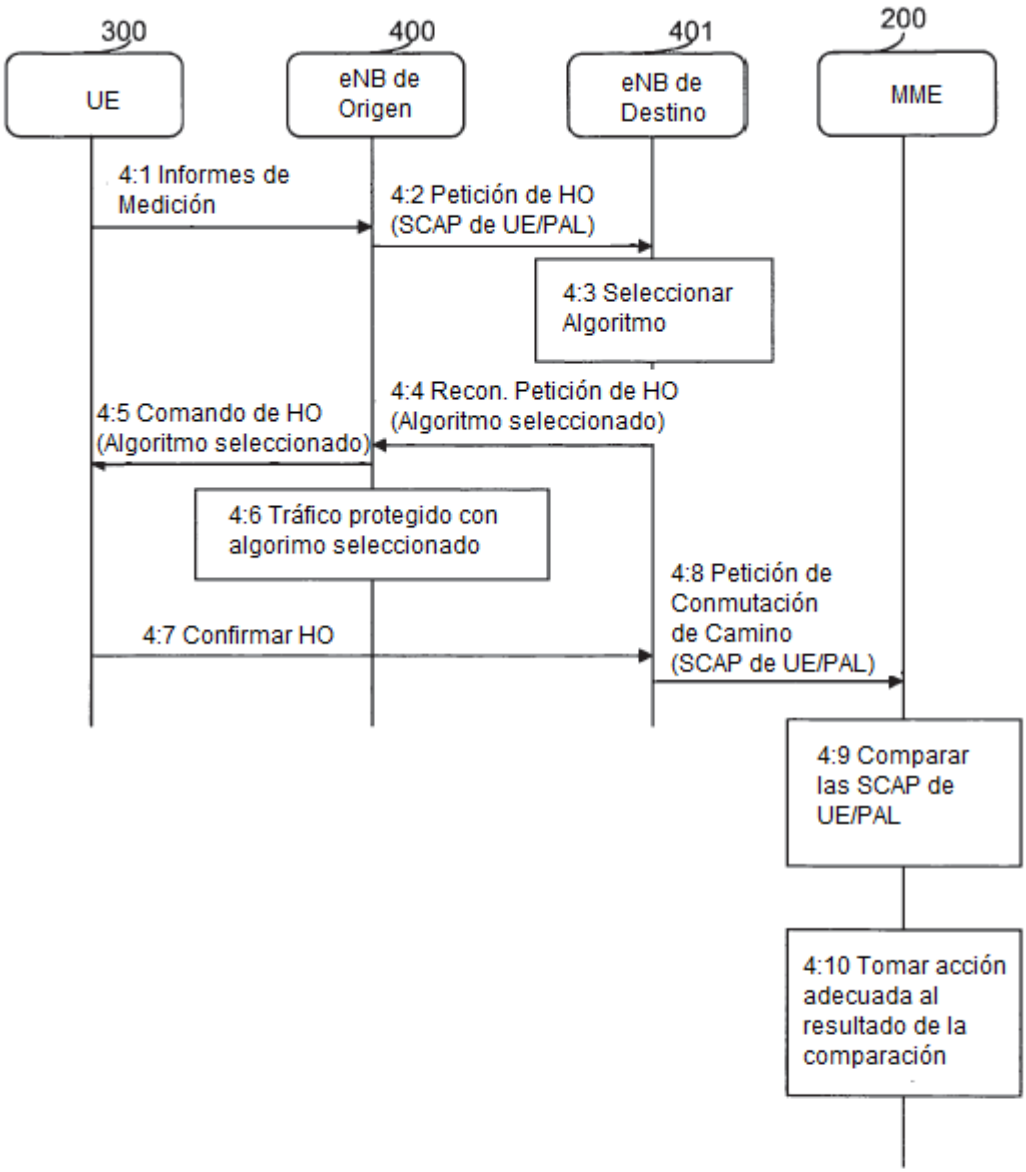
300
UE
400
eNB de Origen
401
eNB de Destino
200
MME
4:1 Informes de Medición
4:2 Petición de HO (SCAP de UE/PAL)
4:3 Seleccionar Algoritmo
4:4 Recon. Petición de HO (Algoritmo seleccionado)
4:5 Comando de HO (Algoritmo seleccionado)
4:6 Tráfico protegido con algorimo seleccionado
4:8 Petición de Conmutación de Camino (SCAP de UE/PAL)
4:7 Confirmar HO
4:9 Comparar las SCAP de UE/PAL
4:10 Tomar acción adecuada al resultado de la comparación

Figura 4

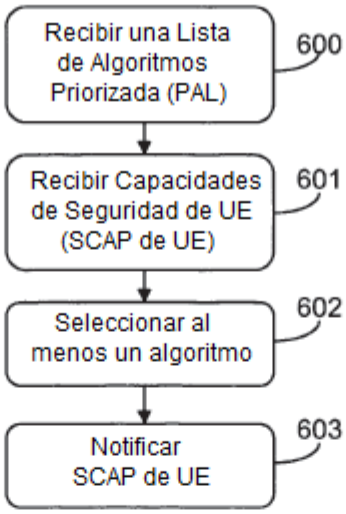

Figura 6

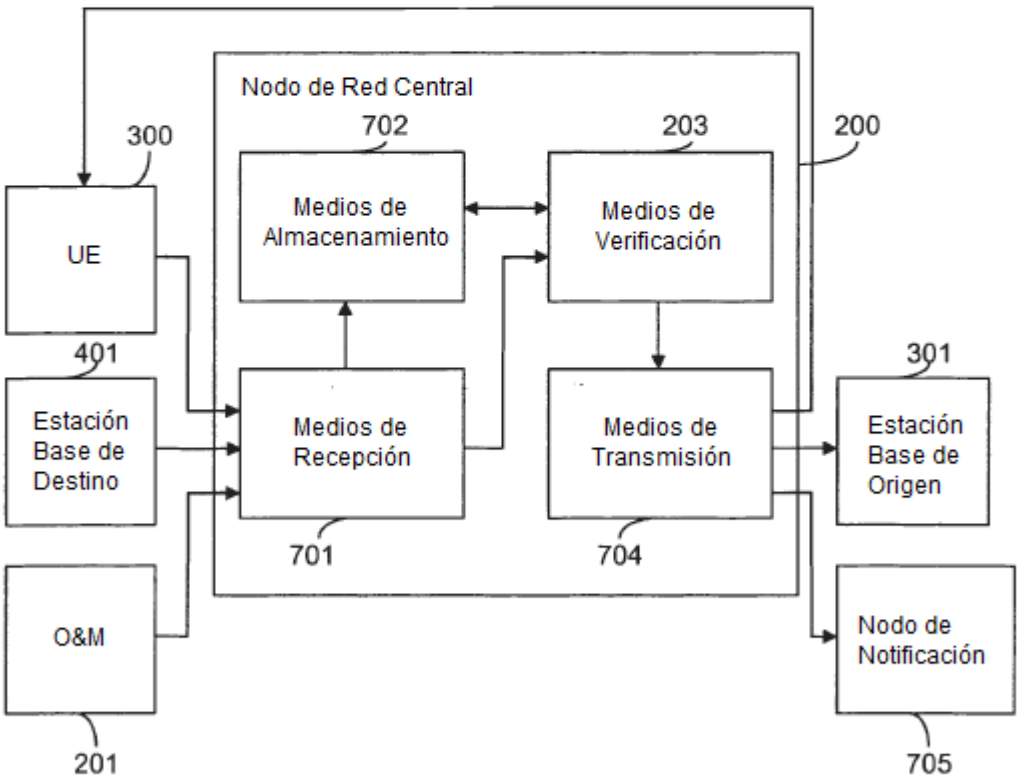

Figura 7

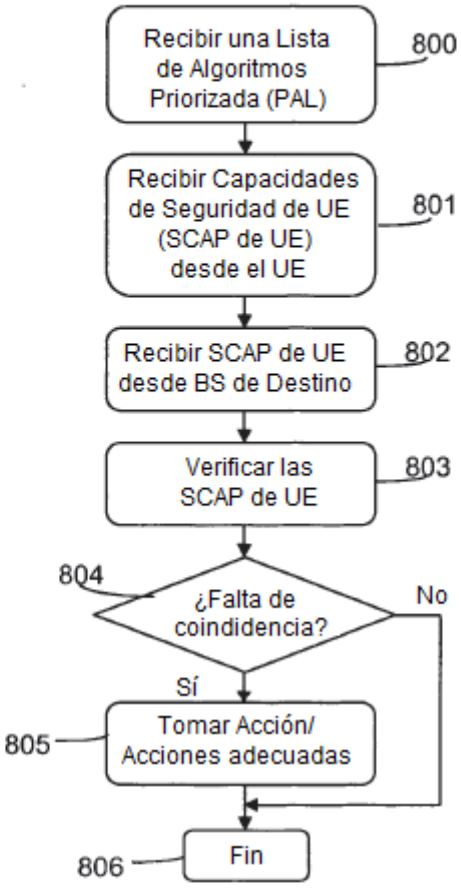
Recibir una Lista de Algoritmos Priorizada (PAL)
800
Recibir Capacidades de Seguridad de UE (SCAP de UE) desde el UE
801
Recibir SCAP de UE desde BS de Destino
802
Verificar las SCAP de UE
803
804
¿Falta de coindidencia?
No
Sí
805
Tomar Acción/ Acciones adecuadas
806
Fin

Figura 8