(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 717 146**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.03.2009 PCT/IB2009/005129**

(87) Fecha y número de publicación internacional: **08.10.2009 WO09122260**

(96) Fecha de presentación y número de la solicitud europea: **30.03.2009 E 09728383 (2)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2018 EP 2266334**

(54) Título: **Métodos, aparatos y productos de programa informático para proporcionar separación criptográfica de múltiples saltos para traspasos**

(30) Prioridad:

04.04.2008 US 42478 P
10.04.2008 US 43857 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2019

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

FORSBERG, DAN, LARS, ANDERS;
NIEMI, PENTTI VALTTERI y
BLOMMAERT, MARC

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Métodos, aparatos y productos de programa informático para proporcionar separación criptográfica de múltiples saltos para traspasos

Campo de la invención

Realizaciones de la presente invención se refieren en general a tecnología de comunicación inalámbrica y, más particularmente, se refieren a un aparato, un método y un producto de programa informático para proporcionar separación de clave criptográfica tras un traspaso.

Antecedentes de la invención

Tecnologías de red actuales y futuras continúan facilitando la facilidad de transferencia de información y comodidad a usuarios. Para proporcionar transferencia de información más fácil y rápida y comodidad, los proveedores de servicios de la industria de las telecomunicaciones están desarrollando mejoras a redes existentes. Por ejemplo, en la actualidad se está desarrollando la red de acceso de radio terrestre de sistema universal de telecomunicaciones móviles (UMTS) evolucionada (E-UTRAN). La E-UTRAN, que también se conoce como Evolución a Largo Plazo (LTE) o 3.9G, tiene por objetivo actualizar las tecnologías anteriores mejorando la eficiencia, bajando costes, mejorando servicios, haciendo uso de nuevas oportunidades de espectros y proporcionando mejor integración con otras normas abiertas.

Una ventaja de E-UTRAN que continúa compartiéndose con otras normas de telecomunicación anteriores es el hecho de que se habilita que usuarios accedan a una red que emplea tales normas mientras permanece móvil. Por lo tanto, por ejemplo, usuarios que tienen terminales móviles equipados para comunicar de acuerdo con tales normas pueden viajar grandes distancias mientras mantienen la comunicación con la red. En este sentido, en la actualidad es común para un punto de acceso o estación base proporcionando cobertura de red para un área particular (o célula), pasar la comunicación con un terminal móvil particular a una estación base vecina cuando el usuario del terminal móvil particular sale del área de cobertura de la estación base o de otra manera puede servirse de forma más efectiva por la estación base vecina. Este proceso a menudo se denomina como un traspaso.

Un problema persistente con traspaso en E-UTRAN y otras redes de comunicaciones móviles es el problema de separación de clave criptográfica entre puntos de acceso de radio. En este sentido, terminales móviles pueden comunicar datos encriptados a través de puntos de acceso de radio o estaciones base (denominados como "nodos B evolucionados" o "eNB" en E-UTRAN) usando una clave de encriptación conocida para el terminal móvil y el punto de acceso o estación base. Durante traspaso, una clave de encriptación usada por un terminal móvil y su nodo B evolucionado de servicio actual o una derivación de esa clave de encriptación puede comunicarse a un nodo B evolucionado objetivo al que tiene que traspasarse el terminal móvil. El nodo B evolucionado objetivo puede a continuación usar la clave de encriptación recibida desde el nodo B evolucionado anterior. Por lo tanto nodos B evolucionados que han servido anteriormente un terminal móvil pueden conocer o de otra manera ser capaces de calcular una clave de encriptación usada en la actualidad por el terminal móvil y su nodo B evolucionado de servicio y desencriptar datos comunicados entre un terminal móvil y el nodo B evolucionado de servicio en la actualidad, resultando por lo tanto en una falta de seguridad de separación de clave criptográfica.

Proyecto Común de Tecnologías Inalámbricas de la 3ª Generación; Servicios y Aspectos de Sistema de Grupo de Especificación Técnica; Decisiones racionales y de rastreo de seguridad en RAN de Largo Plazo Evolucionada / Evolución de Arquitectura de Sistema (SAE) de 3GPP (Versión 8), 3GPP TR 33.821 V1.0.0, vol. 33.821, n.º v1.0.0 1 de diciembre de 2007 (01-12-2007), páginas 1-116, XP002495037 describe aspectos de seguridad en LTE.

La solicitud de patente de Estados Unidos US 2007/224993 A1 divulga aparato, métodos y productos de programa informático que incorporan mejoras que proporcionan seguridad mejorada durante traspasos en una red de comunicaciones inalámbricas celular.

Por consiguiente, sería deseable desarrollar un protocolo de traspaso que puede proporcionar un grado de seguridad de separación de clave criptográfica de modo que nodos B evolucionados anteriores pueden no ser capaces de derivar la clave de encriptación usada por un terminal móvil y nodo B evolucionado actual. Sería deseable adicionalmente si el protocolo de traspaso no requiriese una cantidad significativa de procesamiento o sobrecarga de transferencia de datos por el terminal móvil, nodo B evolucionado, nodo de soporte de servicio general de paquetes de radio (SGSN) (denominado como una "entidad de gestión de movilidad (MME)" en E-UTRAN), o pasarela de servicio (S-GW), de modo que traspaso y posterior reanudación de comunicación no se retarda de forma perceptible.

Breve sumario de algunas realizaciones de la invención

Métodos de acuerdo con la presente invención se caracterizan por lo que se presenta en las reivindicaciones 1 y 8. Aparatos de acuerdo con la presente invención se caracterizan por lo que se presenta en las reivindicaciones 17 y

19. Productos de programa informático de acuerdo con la presente invención se caracterizan por lo que se presenta en las reivindicaciones 15 y 16.

Se proporcionan también un método, aparato y producto de programa informático que pueden proporcionar separación de clave criptográfica para traspasos. En este sentido, realizaciones de la presente invención proporcionan separación de clave criptográfica después de dos traspasos (también conocidos como dos 'saltos') configurando un SGSN, también denominado en este documento como una MME, para proporcionar el punto de acceso objetivo con un valor de clave intermediaria dentro del mensaje de acuse de recibo de conmutación de trayectoria. Por consiguiente, puntos de acceso objetivos pueden derivar una clave usando una función de derivación de clave que usa el valor intermedio como un parámetro de entrada para obtener una clave que está criptográficamente separada de la clave usada por el punto de acceso fuente. Algunas realizaciones de la invención adicionalmente envían una orden de traspaso a dispositivos de usuario que incluyen una indicación del tipo de traspaso, tal como, por ejemplo, si el traspaso es un traspaso de punto de inter acceso o punto de intra acceso. Por consiguiente, en algunas realizaciones de la invención, dispositivos de usuario se configuran para determinar el tipo de traspaso basándose en la indicación incluida en una orden de traspaso y realizan derivaciones de clave basándose en el tipo de traspaso. Algunas realizaciones de la invención adicionalmente usan la clave intermediaria y/o claves derivadas a partir de la clave intermediaria para proteger el mensaje de conmutación de trayectoria de modo que únicamente los puntos de acceso de radio fuente y objetivo son capaces de enviar un mensaje de conmutación de trayectoria válido y por lo tanto reducen el riesgo de cualquier punto de acceso de radio arbitrario enviando mensajes de conmutación de trayectoria falsos. Realizaciones de la invención pueden proporcionar adicionalmente separación de clave criptográfica mientras reducen o minimizan la sobrecarga requerida de entidades de red durante el proceso de traspaso así como reducen o minimizan el retardo en traspaso.

En una realización ilustrativa, se proporciona un método que incluye calcular, en respuesta a un traspaso de un dispositivo de equipo de usuario desde un punto de acceso fuente a un punto de acceso objetivo, una clave basándose al menos en parte en un primer valor intermedio anteriormente almacenado. El método de esta realización también incluye calcular un segundo valor intermedio basándose al menos en parte en la clave calculada. El método de esta realización adicionalmente incluye enviar un acuse de recibido de conmutación de trayectoria que incluye el segundo valor intermedio al punto de acceso objetivo para uso en un traspaso posterior del dispositivo de equipo de usuario. El método de esta realización puede incluir adicionalmente recibir un mensaje de conmutación de trayectoria que incluye una indicación de una identificación de célula y calcular la clave de encriptación basándose en la identificación de célula. El método de esta realización puede incluir adicionalmente almacenar el segundo valor intermedio. En algunas realizaciones, calcular la clave puede comprender además calcular la clave tras un traspaso de enlace de radio.

En otra realización ilustrativa, se proporciona un método que incluye recibir una orden de traspaso desde un punto de acceso fuente. El método de esta realización incluye adicionalmente calcular, en respuesta a recepción de la orden de traspaso, una clave basándose al menos en parte en un primer valor intermedio. El método de esta realización adicionalmente incluye calcular un segundo valor intermedio basándose al menos en parte en el primer valor intermedio. El segundo valor intermedio puede usarse para el cálculo de una o más claves en un traspaso posterior.

En otra realización ilustrativa, se proporciona un aparato. El aparato puede incluir un procesador y una memoria que almacena instrucciones ejecutables que cuando se ejecutan provocan que el aparato calcule, en respuesta a un traspaso de un dispositivo de equipo de usuario desde un punto de acceso fuente a un punto de acceso objetivo, una clave basándose al menos en parte en un primer valor intermedio anteriormente almacenado. Las instrucciones ejecutables cuando se ejecutan también pueden provocar que el aparato calcule un segundo valor intermedio basándose al menos en parte en la clave calculada. Las instrucciones ejecutables cuando se ejecutan pueden provocar adicionalmente que el aparato envíe un acuse de recibido de conmutación de trayectoria que incluye el segundo valor intermedio al punto de acceso objetivo para uso en un traspaso posterior del dispositivo de equipo de usuario.

En otra realización ilustrativa, se proporciona un aparato. El aparato puede incluir un procesador y una memoria que almacena instrucciones ejecutables que cuando se ejecutan provocaban que el aparato reciba una orden de traspaso desde un punto de acceso fuente. Las instrucciones ejecutables cuando se ejecutan pueden provocar adicionalmente que el aparato calcule, en respuesta a recepción de la orden de traspaso, una clave basándose al menos en parte en un primer valor intermedio. Las instrucciones ejecutables cuando se ejecutan pueden provocar adicionalmente que el aparato calcule un segundo valor intermedio basándose al menos en parte en el primer valor intermedio. El segundo valor intermedio puede usarse para el cálculo de una o más claves en un traspaso posterior.

En otra realización ilustrativa, se proporciona un producto de programa informático. El producto de programa informático puede incluir al menos un medio de almacenamiento legible por ordenador que tiene instrucciones de programa legibles por ordenador almacenadas en el mismo. Las instrucciones de programa legibles por ordenador pueden incluir una pluralidad de instrucciones de programa. Aunque en este sumario, las instrucciones de programa están ordenadas, se apreciará que este sumario se proporciona meramente para propósitos de ejemplo y la ordenación es meramente para facilitar resumir el producto de programa informático. La ordenación de ejemplo no

limita de ninguna forma la implementación de las instrucciones de programa informáticas asociadas. La primera instrucción de programa puede configurarse para calcular, en respuesta a un traspaso de un dispositivo de equipo de usuario desde un punto de acceso fuente a un punto de acceso objetivo, una clave basándose al menos en parte en un primer valor intermedio anteriormente almacenado. La segunda instrucción de programa puede configurarse para calcular un segundo valor intermedio basándose al menos en parte en la clave calculada. La tercera instrucción de programa puede configurarse para enviar un acuse de recibido de conmutación de trayectoria que incluye el segundo valor intermedio al punto de acceso objetivo para uso en un traspaso posterior del dispositivo de equipo de usuario.

En otra realización ilustrativa, se proporciona un producto de programa informático. El producto de programa informático puede incluir al menos un medio de almacenamiento legible por ordenador que tiene instrucciones de programa legibles por ordenador almacenadas en el mismo. Las instrucciones de programa legibles por ordenador pueden incluir una pluralidad de instrucciones de programa. Aunque en este sumario, las instrucciones de programa están ordenadas, se apreciará que este sumario se proporciona meramente para propósitos de ejemplo y la ordenación es meramente para facilitar resumir el producto de programa informático. La ordenación de ejemplo no limita de ninguna forma la implementación de las instrucciones de programa informáticas asociadas. La primera instrucción de programa puede configurarse para recibir una orden de traspaso desde un punto de acceso fuente. La segunda instrucción de programa puede configurarse para calcular, en respuesta a recepción de la orden de traspaso, una clave basándose al menos en parte en un primer valor intermedio. La tercera instrucción de programa puede configurarse para calcular un segundo valor intermedio basándose al menos en parte en el primer valor intermedio. El segundo valor intermedio puede usarse para el cálculo de una o más claves en un traspaso posterior.

En otra realización ilustrativa, se proporciona un aparato, que incluye medios para calcular, en respuesta a un traspaso de un dispositivo de equipo de usuario desde un punto de acceso fuente a un punto de acceso objetivo, una clave basándose al menos en parte en un primer valor intermedio anteriormente almacenado. El aparato de esta realización también incluye medios para calcular un segundo valor intermedio basándose al menos en parte en la clave calculada. El aparato de esta realización incluye adicionalmente medios para enviar un acuse de recibido de conmutación de trayectoria que incluye el segundo valor intermedio al punto de acceso objetivo para uso en un traspaso posterior del dispositivo de equipo de usuario.

En otra realización ilustrativa, se proporciona un aparato, que incluye medios para recibir una orden de traspaso desde un punto de acceso fuente. El aparato de esta realización incluye adicionalmente medios para calcular, en respuesta a recepción de la orden de traspaso, una clave basándose al menos en parte en un primer valor intermedio. El aparato de esta realización adicionalmente incluye medios para calcular un segundo valor intermedio basándose al menos en parte en el primer valor intermedio. El segundo valor intermedio puede usarse para el cálculo de una o más claves en un traspaso posterior.

El sumario anterior se proporciona meramente para propósitos de resumir algunos ejemplos de realizaciones de la invención para proporcionar un entendimiento básico de algunos aspectos de la invención. Por consiguiente, se apreciará que los ejemplos de realizaciones anteriormente descritos son meramente ejemplos y no debería interpretarse para limitar el alcance o espíritu de la invención de ninguna forma. Se apreciará que el alcance de la invención incluye muchas realizaciones potenciales, algunas de las cuales pueden describirse adicionalmente a continuación, además de las resumidas en este punto.

Breve descripción de las varias vistas de los dibujos

Habiendo descrito por lo tanto la invención en términos generales, se hará ahora referencia a los dibujos adjuntos, que no necesariamente se han dibujado a escala, y en los que:

la Figura 1 es un diagrama de bloques esquemático de un terminal móvil de acuerdo con una realización ilustrativa de la presente invención;
la Figura 2 es un diagrama de bloques esquemático de un sistema de comunicaciones inalámbricas de acuerdo con una realización ilustrativa de la presente invención;
la Figura 3 es un diagrama esquemático que muestra un sistema para proporcionar separación de clave criptográfica para traspasos de acuerdo con una realización ilustrativa de la presente invención;
la Figura 4 es un diagrama de flujo de control de señales de comunicación pasadas entre entidades de la realización ilustrativa de la Figura 3 durante un proceso de traspaso de acuerdo con una realización ilustrativa de la presente invención;
la Figura 5 es un diagrama de flujo de acuerdo con un método ilustrativo de provisión de separación de clave criptográfica para traspasos de acuerdo con una realización ilustrativa de la presente invención; y
la Figura 6 es un diagrama de flujo de acuerdo con otro método ilustrativo de provisión de separación de clave criptográfica para traspasos de acuerdo con una realización ilustrativa de la presente invención.

Descripción detallada de la invención

Realizaciones de la presente invención se describirán ahora más completamente en lo sucesivo con referencia a los

dibujos adjuntos en los que se muestran algunas, pero no todas las realizaciones de la invención. De hecho, la invención puede incorporarse de muchas formas diferentes y no debería interpretarse como limitada a las realizaciones expuestas en este documento; en su lugar, estas realizaciones se proporcionan de modo que esta divulgación satisfará los requisitos legales aplicables. Números de referencia similares hacen referencia a elementos similares a lo largo de todo el presente documento.

La Figura 1 ilustra un diagrama de bloques de un terminal móvil 10 que se beneficiaría de realizaciones de la presente invención. Debería entenderse, sin embargo, que un teléfono móvil como se ilustra y en lo sucesivo describe es meramente ilustrativo de un tipo de terminal móvil que se beneficiaría de realizaciones de la presente invención y, por lo tanto, no debería tomarse para limitar el alcance de las realizaciones de la presente invención. Mientras se ilustra una realización del terminal móvil 10 y se describirá en lo sucesivo para propósitos de ejemplo, otros tipos de terminales móviles, tal como asistentes digitales personales (PDA), buscapersonas, ordenadores móviles, televisiones móviles, dispositivos de juegos, ordenadores portátiles, cámaras, grabadores de vídeo, dispositivos de sistema de posicionamiento global (GPS) y otros tipos de sistemas de comunicaciones por voz y texto, pueden emplear fácilmente realizaciones de la presente invención. Adicionalmente, dispositivos que no son móviles también pueden emplear fácilmente realizaciones de la presente invención.

El sistema y método de realizaciones de la presente invención se describirán esencialmente a continuación en conjunto con aplicaciones de comunicaciones móviles. Sin embargo, debería entenderse que el sistema y método de realizaciones de la presente invención pueden utilizarse en conjunto con otras diversas aplicaciones, tanto dentro como fuera de las industrias de las comunicaciones móviles.

El terminal móvil 10 de una realización incluye una antena 12 (o múltiples antenas) en comunicación operable con un transmisor 14 y un receptor 16. El terminal móvil 10 puede incluir adicionalmente un controlador 20 u otro elemento de procesamiento que proporciona señales a y recibe señales del transmisor 14 y receptor 16, respectivamente. Las señales pueden incluir información de señalización de acuerdo con la norma de interfaz aérea del sistema celular aplicable, y también voz de usuario, datos recibidos y/o datos generados por usuario. En este sentido, el terminal móvil 10 puede ser capaz de operar con una o más normas de interfaz aéreas, protocolos de comunicación, tipos de modulación y tipos de acceso. Por medio de ilustración, el terminal móvil 10 puede ser capaz de operar de acuerdo con cualquiera de un número de protocolos de comunicación de primera, segunda, tercera y/o cuarta generación o similar. Por ejemplo, el terminal móvil 10 puede ser capaz de operar de acuerdo con protocolos de comunicación inalámbrica de segunda generación (2G) IS-136 (Acceso Múltiple por División en el Tiempo (TDMA)), Sistema Global para Comunicaciones Móviles (GSM) e IS-95 (Acceso Múltiple por División de Código(CDMA)), o con protocolos de comunicación inalámbrica de tercera generación (3G), tal como Sistema Universal de Telecomunicaciones Móviles (UMTS), CDMA2000, Acceso Múltiple por División de Código de Banda Ancha (WCDMA) y Acceso Múltiple por División de Código Síncrono de División de Tiempo (TD-SCDMA), LTE o E-UTRAN, con protocolos de comunicación inalámbrica de cuarta generación (4G) o similar.

Se entiende que el controlador 20 de una realización incluye circuitería deseable para implementar funciones lógicas y de audio del terminal móvil 10. Por ejemplo, el controlador 20 puede comprenderse de un dispositivo de procesador de señales digitales, un dispositivo de microprocesador y diversos convertidores de analógico a digital, convertidores de digital a analógico y otros circuitos de soporte. Pueden asignarse funciones de procesamiento de control y señal del terminal móvil 10 entre estos dispositivos de acuerdo con sus respectivas capacidades. El controlador 20 por lo tanto también puede incluir la funcionalidad para codificar convolucionalmente e intercalar mensajes y datos antes de modulación y transmisión. El controlador 20 puede incluir adicionalmente un codificador de voz interno y puede incluir un módem de datos interno. Además, el controlador 20 puede incluir funcionalidad para operar uno o más programas de software, que pueden almacenarse en memoria. Por ejemplo, el controlador 20 puede ser capaz de operar un programa de conectividad, tal como un navegador web convencional. El programa de conectividad puede a continuación permitir que el terminal móvil 10 transmita y reciba contenido web, tal como contenido basado en ubicación y/u otro contenido de página web, de acuerdo con un Protocolo de Aplicación Inalámbrica (WAP), Protocolo de Transferencia de Hipertexto (HTTP) y/o similar, por ejemplo.

El terminal móvil 10 también puede comprender una interfaz de usuario que incluye un dispositivo de salida tal como un auricular convencional o altavoz 24, un timbre 22, un micrófono 26, un visualizador 28 y una interfaz de entrada de usuario, todos los cuales se acoplan al controlador 20. La interfaz de entrada de usuario, que permite que el terminal móvil 10 reciba datos, puede incluir cualquiera de un número de dispositivos que permiten que el terminal móvil 10 reciba datos, tal como un teclado 30, una pantalla táctil (no mostrada) u otro dispositivo de entrada. En las realizaciones que incluyen el teclado 30, el teclado 30 puede incluir las teclas numéricas convencionales (0-9) y las relacionadas (#, *) y otras teclas usadas para operar el terminal móvil 10. Como alternativa, el teclado 30 puede incluir una disposición de teclado QWERTY convencional. El teclado 30 también puede incluir diversos teclas de función variable con funciones asociadas. Además, o como alternativa, el terminal móvil 10 puede incluir un dispositivo de interfaz tal como una palanca de mandos u otra interfaz de entrada de usuario. El terminal móvil 10 puede incluir adicionalmente una batería 34, tal como un conjunto de baterías vibrantes, para alimentar diversos circuitos que se requieren para operar el terminal móvil 10, así como proporcionando opcionalmente vibración mecánica como una salida detectable.

El terminal móvil 10 puede incluir adicionalmente un módulo de identidad de usuario (UIM) 38. En una realización, el UIM 38 comprende un dispositivo de memoria que tiene un procesador incorporado. El UIM 38 puede incluir, por ejemplo, un módulo de identidad de abonado (SIM), una tarjeta de circuito integrado universal (UICC), un módulo de identidad de abonado universal (USEVI), un módulo de identidad de usuario transportable (R-UDVI), etc. El UIM 38 puede almacenar elementos de información relacionados con un abonado móvil. Además del UIM 38, el terminal móvil 10 puede equiparse con memoria. Por ejemplo, el terminal móvil 10 puede incluir la memoria volátil 40, tal como Memoria de Acceso Aleatorio (RAM) volátil que incluye un área de caché para el almacenamiento temporal de datos. El terminal móvil 10 también puede incluir otra memoria no volátil 42, que puede embeberse y/o puede ser extraíble. La memoria no volátil 42 puede comprender adicionalmente o como alternativa una EEPROM, memoria flash o similar. Las memorias pueden almacenar cualquiera de un número de piezas de información, y datos, usadas por el terminal móvil 10 para implementar las funciones del terminal móvil 10. Por ejemplo, las memorias pueden incluir un identificador, tal como un código de identificación de equipo móvil internacional (IMEI), capaz de identificar inequívocamente el terminal móvil 10.

Haciendo referencia ahora a la Figura 2, se proporciona un diagrama de bloques esquemático de un tipo de sistema de comunicaciones inalámbricas que se beneficiaría de realizaciones de la presente invención. El sistema de la realización ilustrada incluye una pluralidad de dispositivos de red. Como se muestra, uno o más terminales móviles 10 pueden incluir cada uno una antena 12 para transmitir señales a y para recibir señales desde un sitio base o estación base (BS) 44. Mientras una BS puede comprenderse de una o más células, referencia en este documento a una BS genéricamente se refiere a tanto una BS como una célula de la BS. La estación base 44 puede ser una parte de una o más redes celulares o móviles cada una de las cuales incluye elementos requeridos para operar la red, tal como un centro de conmutación móvil (MSC) 46. La red móvil también puede denominarse como una estación base/MSC/Función de interfuncionamiento (BMI). En la operación, el MSC 46 de una realización es capaz de encaminar llamadas a y desde el terminal móvil 10 cuando el terminal móvil 10 está haciendo y recibiendo llamadas. El MSC 46 también puede proporcionar una conexión a enlaces troncales de línea terrestres cuando el terminal móvil 10 está involucrado en una llamada. Además, el MSC 46 puede ser capaz de controlar el reenvío de mensajes a y desde el terminal móvil 10, y también puede controlar el reenvío de mensajes para el terminal móvil 10 a y desde un centro de mensajería. Se ha de observar que aunque el MSC 46 se muestra en el sistema de la Figura 2, el MSC 46 es meramente un dispositivo de red ilustrativo y realizaciones de la presente invención no se limitan a uso en una red que emplea un MSC.

El MSC 46 puede acoplarse a una red de datos, tal como una red de área local (LAN), una red de área metropolitana (MAN) y/o una red de área extensa (WAN). El MSC 46 puede acoplarse directamente a la red de datos. En una realización, sin embargo, el MSC 46 se acopla a un dispositivo de pasarela (GTW) 48, y el GTW 48 se acopla a una WAN, tal como internet 50. A su vez, dispositivos tal como elementos de procesamiento (por ejemplo, ordenadores personales, ordenadores de servidor o similar) pueden acoplarse al terminal móvil 10 a través de la Internet 50. Por ejemplo, como se explica a continuación, los elementos de procesamiento pueden incluir uno o más elementos de procesamiento asociados con un sistema informático 52 (dos mostrados en la Figura 2), servidor de origen 54 (uno mostrado en la Figura 2) o similar, como se describe a continuación.

La BS 44 también puede acoplarse a un nodo de soporte de GPRS (Servicio General de Paquetes de Radio) de servicio (SGSN) 56. El SGSN 56 de una realización es capaz de realizar funciones similares al MSC 46 para servicios conmutados por paquetes. El SGSN 56, como el MSC 46, puede acoplarse a una red de datos, tal como internet 50. El SGSN 56 puede acoplarse directamente a la red de datos. En otra realización, sin embargo, el SGSN 56 se acopla a una red principal de conmutación de paquetes, tal como una red principal de GPRS 58. La red principal de conmutación de paquetes de esta realización se acopla a continuación a otro GTW 48, tal como un nodo de soporte de GPRS de pasarela (GGSN) 60, y el GGSN 60 se acopla a la Internet 50. Además del GGSN 60, la red principal de conmutación de paquetes también puede acoplarse a un GTW 48. También, el GGSN 60 puede acoplarse a un centro de mensajería. En este sentido, el GGSN 60 y el SGSN 56, como el MSC 46, pueden ser capaces de controlar el reenvío de mensajes, tal como mensajes de servicio de mensajería multimedia (MMS). El GGSN 60 y SGSN 56 también pueden ser capaces de controlar el reenvío de mensajes para el terminal móvil 10 a y desde el centro de mensajería.

Además, acoplando el SGSN 56 a la red principal de GPRS 58 y el GGSN 60, dispositivos tal como un sistema informático 52 y/o servidor de origen 54 pueden acoplarse al terminal móvil 10 a través de la Internet 50, SGSN 56 y GGSN 60. En este sentido, dispositivos tal como el sistema informático 52 y/o servidor de origen 54 pueden comunicar con el terminal móvil 10 a través del SGSN 56, red principal de GPRS 58 y el GGSN 60. Conectando directa o indirectamente terminales móviles 10 y los otros dispositivos (por ejemplo, sistema informático 52, servidor de origen 54, etc.) a la Internet 50, los terminales móviles 10 pueden comunicar con los otros dispositivos y entre sí, tal como de acuerdo con el Protocolo de Transferencia de Hipertexto (HTTP) y/o similar, para efectuar de este modo diversas funciones de los terminales móviles 10.

Aunque no se muestra y describe cada elemento de cada red móvil posible en este documento, debería apreciarse que el terminal móvil 10 puede acoplarse a uno o más de cualquiera de un número de diferentes redes a través de la BS 44. En este sentido, la red o redes pueden ser capaces de soportar comunicación de acuerdo con uno cualquiera o más de un número de protocolos de comunicación móvil de primera generación (1G), segunda generación (2G),

2.5G, tercera generación (3G), 3.9G, cuarta generación (4G) o similar. Por ejemplo, uno o más de la red o redes pueden ser capaces de soportar comunicación de acuerdo con protocolos de comunicación inalámbrica 2G IS-136 (TDMA), GSM e IS-95 (CDMA). También, por ejemplo, uno o más de la red o redes pueden ser capaces de soportar comunicación de acuerdo con protocolos de comunicación inalámbrica 2.5G GPRS, Entorno de GSM de Datos Mejorado (EDGE) o similar. Además, por ejemplo, una o más de la red o redes pueden ser capaces de soportar comunicación de acuerdo con protocolos de comunicación inalámbrica 3G tal como una red de Sistema de Telefonía Móvil Universal (UMTS) que emplea Tecnología de Acceso de Radio de Acceso Múltiple por División de Código de Banda Ancha (WCDMA). Adicionalmente, por ejemplo, una o más de la red o redes pueden ser capaces de soportar comunicación de acuerdo con protocolos de comunicación inalámbrica 3.9G tal como E-UTRAN. Algunas red o redes de AMPS de banda estrecha (NAMPS), así como Sistema de Comunicación de Acceso Total (TACS), también pueden beneficiarse de realizaciones de la presente invención, como harían terminales móviles de modo dual o superior (por ejemplo, digitales/analógicos o TDMA/CDMA/teléfonos analógicos).

El terminal móvil 10 puede acoplarse adicionalmente a uno o más puntos de acceso inalámbricos (AP) 62. Los AP 62 pueden comprender puntos de acceso configurados para comunicar con el terminal móvil 10 de acuerdo con técnicas tal como, por ejemplo, frecuencia de radio (RF), infrarrojo (IrDA) o cualquiera de un número de diferentes técnicas de interconexión inalámbrica, incluyendo técnicas de LAN inalámbrica (WLAN) tal como IEEE 802.11 (por ejemplo, 802.11a, 802.11b, 802.11g, 802.11n, etc.), técnicas de Interoperabilidad Mundial para Acceso por Microondas (WiMAX) tal como IEEE 802.16 y/o técnicas de Red de Área Personal Inalámbrica (WPAN) tal como IEEE 802.15, BlueTooth (BT), banda ultra ancha (UWB) y/o similar. Los AP 62 pueden acoplarse a la Internet 50. Como con el MSC 46, los AP 62 pueden acoplarse directamente a la Internet 50. En una realización, sin embargo, los AP 62 se acoplan indirectamente a la Internet 50 a través de un GTW 48. Adicionalmente, en una realización, la BS 44 puede considerarse como otro AP 62. Como se apreciará, conectando directa o indirectamente los terminales móviles 10 y el sistema informático 52, el servidor de origen 54 y/o cualquiera de un número de otros dispositivos, a la Internet 50, los terminales móviles 10 pueden comunicarse entre sí, con el sistema informático, etc., para de este modo efectuar diversas funciones de los terminales móviles 10, tal como para transmitir datos, contenido o similar a y/o para recibir contenido, datos o similar desde, el sistema informático 52. Como se usa en este documento, los términos "datos," "contenido," "información" y términos similares pueden usarse de forma intercambiable para referirse a datos capaces de transmitirse, recibirse y/o almacenarse de acuerdo con realizaciones de la presente invención. Por lo tanto, el uso de cualquiera de estos términos no deberían tomarse para limitar el espíritu y alcance de realizaciones de la presente invención.

Aunque no se muestra en la Figura 2, además de o en lugar de acoplar el terminal móvil 10 a sistemas informáticos 52 a través de la Internet 50, el terminal móvil 10 y sistema informático 52 pueden acoplarse entre sí y comunicarse de acuerdo con, por ejemplo, RF, BT, IrDA o cualquiera de un número de diferentes técnicas de comunicación alámbrica o inalámbrica, incluyendo LAN, WLAN, WiMAX, UWB técnicas y/o similar. Uno o más de los sistemas informáticos 52 pueden incluir adicionalmente, o como alternativa, una memoria extraíble capaz de almacenar contenido, que puede transferirse posteriormente al terminal móvil 10. Además, el terminal móvil 10 puede acoplarse a uno o más dispositivos electrónicos, tal como impresoras, proyectores digitales y/u otros dispositivos de captura, producción y/o almacenamiento multimedia (por ejemplo, otros terminales). Como con los sistemas informáticos 52, el terminal móvil 10 puede configurarse para comunicarse con los dispositivos electrónicos portátiles de acuerdo con técnicas tal como, por ejemplo, RF, BT, IrDA o cualquiera de un número de diferentes técnicas de comunicación alámbrica o inalámbrica, incluyendo técnicas de Bus Serial Universal (USB), LAN, WLAN, WiMAX, UWB y/o similares.

En una realización ilustrativa, contenido o datos pueden comunicarse a través del sistema de la Figura 2 entre un terminal móvil, que puede ser similar al terminal móvil 10 de la Figura 1 y un dispositivo de red del sistema de la Figura 2 para ejecutar aplicaciones para establecer comunicación entre el terminal móvil 10 y otros terminales móviles, por ejemplo, a través del sistema de la Figura 2. Como tal, debería entenderse que el sistema de la Figura 2 no necesita emplearse para comunicación entre terminales móviles o entre un dispositivo de red y el terminal móvil, sino que la Figura 2 se proporciona meramente para propósitos de ejemplo.

Se describirá ahora con referencia a la Figura 3 una realización ilustrativa de la invención, en la que se visualizan ciertos elementos de un sistema para facilitar recuperación de fallo de traspaso. El sistema de la Figura 3 representa una realización específica de una red tal como la red generada visualizada en la Figura 2, excepto que la Figura 3 representa un diagrama de bloques general de una E-UTRAN. Como tal, en conexión con la Figura 3, el equipo de usuario (UE) 70 puede ser ilustrativo de una realización del terminal móvil 10 de la Figura 1 y el nodo B evolucionado fuente 72 y nodo B evolucionado objetivo 74 pueden ser ilustrativos de realizaciones de o bien la BS 44 o bien el AP 62 de la Figura 2. Por consiguiente, aunque la expresión "nodo B evolucionado" se usará posteriormente, un nodo B evolucionado es meramente una realización de un punto de acceso y la expresión "punto de acceso" puede incluir puntos de acceso, estaciones base y nodos B evolucionados. Por lo tanto, aunque realizaciones de la invención se analizan en relación con normas de E-UTRAN, realizaciones de la invención no se limitan de esta forma y pueden usarse con cualquier protocolo de comunicaciones. Además, el sistema de la Figura 3, también puede emplearse en conexión con otros diversos dispositivos, tanto móviles como fijos y, por lo tanto, realizaciones la presente invención no debería limitarse a aplicación en dispositivos tal como el terminal móvil 10 de la Figura 1 o los dispositivos de red de la Figura 2.

Haciendo referencia ahora a la Figura 3, se proporciona un diagrama de bloques esquemático que muestra un sistema para proporcionar separación de clave criptográfica para traspasos de acuerdo con una realización ilustrativa de la presente invención. El sistema incluye una E-UTRAN 76 que puede incluir, entre otras cosas, una pluralidad de nodos B evolucionados en comunicación con un núcleo de paquetes evolucionado (EPC) 78 que puede incluir una o más entidades gestión de movilidad (MME) 80 y una o más pasarelas de evolución de arquitectura de sistema (SAE). Los nodos B evolucionados (incluyendo nodo B evolucionado fuente 72 y nodo B evolucionado objetivo 74) pueden ser nodos B evolucionados (por ejemplo, eNB) y también pueden estar en comunicación con el UE 70 y otros UE.

Los nodos B evolucionados pueden proporcionar terminaciones de protocolo de plano de usuario y plano de control (control de recursos de radio (RRC)) de acceso de radio terrestre de sistema universal de telecomunicaciones móviles evolucionado (E-UTRA) para el UE 70. Los nodos B evolucionados pueden proporcionar funcionalidad que alojan tales funciones como gestión de recursos de radio, control de portador de radio, control de admisión de radio, control de movilidad de conexión, asignación dinámica de recursos a UE tanto en enlace ascendente como enlace descendente, selección de una MME 80 en fijación de UE, compresión y encriptación de encabezamiento de Protocolo de Internet (IP), planificación de información de radiobúsqueda y difusión, encaminamiento de datos, medición y notificación de medición para movilidad de configuración y similares.

La MME 80 puede alojar funciones tal como distribución de mensajes a respectivos nodos B evolucionados, control de seguridad, control de movilidad de estado en reposo, control de portador de SAE, cifrado y protección de integridad de señalización de estrato sin acceso (NAS) y similares. Aunque denominado en este documento como una "MME" de conformidad con la norma de E-UTRAN, se apreciará que realizaciones de la invención no se limitan a operación de acuerdo con la norma de E-UTRAN y que la MME 80 también puede ser entidades operables con otras normas de interconexión. En este sentido, la MME 80 puede ser, por ejemplo, un SGSN 56 del sistema de la Figura 2. La pasarela de SAE puede alojar funciones tal como terminación y conmutación de ciertos paquetes para radiobúsqueda y soporte de movilidad de UE. En una realización ilustrativa, el EPC 78 puede proporcionar conexión a una red tal como internet.

Como se muestra en la Figura 3, cada punto de acceso, tal como, por ejemplo, un nodo B evolucionado, puede incluir un procesador 88 configurado para ejecutar funciones asociadas con cada correspondiente punto de acceso. Tales funciones pueden asociarse, por ejemplo, con instrucciones almacenadas que cuando se ejecutan por el procesador 88 efectúan las correspondientes funciones asociadas con las instrucciones. Un procesador tal como los descritos anteriormente pueden incorporarse de muchas formas. Por ejemplo, el procesador 88 puede incorporarse como un procesador, un coprocesador, un controlador o diversos otros medios de procesamiento o dispositivos que incluyen circuitos integrados tal como, por ejemplo, un ASIC (circuito integrado de aplicación específica), un campo de matriz de puertas programables (FPGA) y/u otros elementos de hardware y/o software programados y configurados adecuadamente.

En una realización ilustrativa, cada de los nodos B evolucionados también puede incluir un elemento de gestión de traspaso 90. El elemento de gestión de traspaso 90 puede ser cualquier dispositivo o medio incorporado en o bien hardware, un producto de programa informático o bien una combinación de hardware y software y puede incorporarse como o de otra manera controlarse por el procesador 88. El elemento de gestión de traspaso 90 puede configurarse para determinar si solicitar un traspaso con otro nodo B evolucionado basándose, por ejemplo, en informes de medición recibidos desde el UE 70. En este sentido, por ejemplo, si informes de medición recibidos en el nodo B evolucionado fuente 72 indican la presencia de una condición para la que es deseable un traspaso (por ejemplo, baja intensidad de señal), el nodo B evolucionado fuente 72 puede enviar una petición de traspaso al nodo B evolucionado objetivo 74. En una realización ilustrativa de la presente invención, el elemento de gestión de traspaso 90 puede configurarse para incluir con la solicitud de traspaso, una clave de encriptación que puede usarse para facilitar comunicación con el UE 70. En este sentido, el elemento de gestión de traspaso 90 puede configurarse para utilizar claves de encriptación recibidas desde otro dispositivo de red, tal como, por ejemplo otro nodo B evolucionado o una MME 80, para comunicar con un UE 70 y/o para usar parámetros recibidos desde otro dispositivo de red para derivar o de otra manera calcular claves de encriptación para usar en comunicaciones con un UE 70.

El elemento de gestión de traspaso 90 puede configurarse adicionalmente para comunicar con una MME 80. En este sentido, el elemento de gestión de traspaso 90 puede configurarse para recibir un mensaje de petición de configuración de contexto inicial desde una MME 80. El mensaje de petición de configuración de contexto puede incluir una o más claves de encriptación, que pueden facilitar comunicación con un UE 70, como parámetros. El mensaje de petición de configuración de contexto puede incluir adicionalmente uno o más parámetros que pueden usarse por el elemento de gestión de traspaso para calcular claves de encriptación adicionales. El elemento de gestión de traspaso 90 puede configurarse adicionalmente para transmitir una petición de conmutación de trayectoria a una MME 80 así como recibir desde la MME 80 un mensaje de acuse de recibo de conmutación de trayectoria que puede incluir uno o más parámetros que pueden usarse para derivaciones de clave de encriptación. En algunas realizaciones, el elemento de gestión de traspaso 90 puede configurarse adicionalmente para proteger el mensaje de conmutación de trayectoria con una clave intermediaria y/o cualquier clave derivada a partir de la clave intermediaria. La protección puede conseguirse a través de cualquiera de varios medios, tal como, por ejemplo, a

través de suma de control de protección de integridad en el mensaje de conmutación de trayectoria o a través de un testigo de autenticación calculado basándose en la clave intermediaria y/o claves derivadas a partir de la clave intermediaria y algunos elementos adicionales que pueden incluirse en el mensaje de conmutación de trayectoria y/o compartirse entre el punto de acceso de radio objetivo y la entidad de gestión de movilidad (MME).

El elemento de gestión de traspaso 90 puede configurarse adicionalmente para comunicar mensajes relacionados con un traspaso con un UE 70. En este sentido, el elemento de gestión de traspaso 90 de un nodo B evolucionado fuente 72 puede configurarse para enviar una orden de traspaso a un UE 70, tal como en respuesta a una decisión de traspaso hecha basándose en informes de medición recibidos desde el UE 70. La orden de traspaso puede incluir un indicador de si el traspaso es un traspaso inter nodo B evolucionado. En una realización ilustrativa, este indicador puede ser simplemente un indicador de bandera de 1 bit en el que el UE 70 puede determinar si el traspaso es un traspaso intra nodo B evolucionado o inter nodo B evolucionado basándose en si se establece la bandera de 1 bit. En realizaciones alternativas, pueden usarse otros medios de indicación, tal como, por ejemplo, pasar un parámetro adicional con el mensaje de comando de traspaso.

Una MME 80 puede incluir un procesador 82, controlador de traspaso 84 y memoria 86. El procesador 82 puede incorporarse como un procesador, un coprocesador, un controlador o diversos otros medios de procesamiento o dispositivos que incluyen circuitos integrados tal como, por ejemplo, un ASIC (circuito integrado de aplicación específica), un campo de matriz de puertas programables (FPGA) y/u otro hardware programado o configurado adecuadamente y/o producto de programa informático. El controlador de traspaso 84 puede ser cualquier dispositivo o medio incorporado en o bien hardware, uno o más productos de programa informático o bien una combinación de hardware y software y puede incorporarse como o de otra manera controlarse por el procesador 82. El controlador de traspaso 84 puede configurarse para comunicar con nodos B evolucionados y gestionar el traspaso de un UE 70. El controlador de traspaso 84 puede configurarse adicionalmente para comunicar con una pasarela de SAE de servicio. En este sentido, el controlador de traspaso 84 puede configurarse para enviar peticiones de actualización de plano U a una pasarela de servicio y recibir respuestas de actualización de plano U desde una pasarela de servicio.

En una realización ilustrativa, el controlador de traspaso 84 puede configurarse para calcular claves de encriptación así como valores intermedios que pueden usarse por nodos B evolucionados para la derivación de claves de encriptación adicionales. El controlador de traspaso 84 puede configurarse para almacenar uno o más de estas claves de encriptación y valores intermedios en memoria 86. El controlador de traspaso 84 puede configurarse para enviar un mensaje de petición de configuración de contexto inicial a un nodo B evolucionado fuente 72. El mensaje de petición de configuración de contexto puede incluir como parámetros uno o más valores de clave de encriptación que pueden facilitar comunicación del nodo B evolucionado con un UE 70. El mensaje de petición de configuración de contexto puede incluir adicionalmente o como alternativa uno o más valores intermedios como parámetros que pueden usarse por el nodo B evolucionado para calcular claves de encriptación adicionales. El controlador de traspaso 84 puede configurarse adicionalmente para recibir una petición de conmutación de trayectoria desde un nodo B evolucionado así como para enviar a un nodo B evolucionado un mensaje de acuse de recibo de conmutación de trayectoria que puede incluir uno o más parámetros que pueden usarse por el nodo B evolucionado de recepción para derivaciones de clave de encriptación. En algunas realizaciones, el controlador de traspaso 84 puede configurarse para verificar un mensaje de conmutación de trayectoria recibido para garantizar que el mensaje de conmutación de trayectoria se recibe desde un nodo B evolucionado válido. Esta verificación puede basarse en, por ejemplo, una o más claves, tal como, por ejemplo, una clave intermediaria y/o una o más claves derivadas a partir de la clave intermediaria.

En una realización ilustrativa, a UE 70 puede incluir un procesador 92, un gestor de traspaso 94 y memoria 86. El procesador 92 puede incorporarse como un procesador, un coprocesador, un controlador o diversos otros medios de procesamiento o dispositivos que incluyen circuitos integrados tal como, por ejemplo, un ASIC (circuito integrado de aplicación específica), un campo de matriz de puertas programables (FPGA) y/u otro hardware programado o configurado adecuadamente y/o elementos de software. En algunas realizaciones, el procesador 92 puede ser un controlador 20 de un terminal móvil 10. El gestor de traspaso 94 puede ser cualquier dispositivo o medio incorporado en o bien hardware, uno o más productos de programa informático o bien una combinación de hardware y software y puede incorporarse como o de otra manera controlarse por el procesador 92. En algunas realizaciones, la memoria 96 puede ser la memoria volátil 40 o memoria no volátil 42 de un terminal móvil 10.

El gestor de traspaso 94 puede configurarse para comunicar con el nodo B evolucionado fuente 72 y nodo B evolucionado objetivo 74 y calcular claves de encriptación a usar en comunicaciones con nodos B evolucionados para facilitar un traspaso del UE 70 desde un nodo B evolucionado fuente 72 a un nodo B evolucionado objetivo 74. El gestor de traspaso puede configurarse para enviar informes de medición a y recibir una orden de traspaso desde el nodo B evolucionado fuente 72. En algunas realizaciones, una orden de traspaso recibida puede incluir un indicador de si el traspaso es un traspaso inter nodo B evolucionado. El gestor de traspaso 94 puede configurarse a continuación para realizar derivaciones de clave de encriptación basándose en el indicador recibido. En este sentido, realizaciones de la invención divulgadas en este documento pueden realizar un proceso de derivación de clave si un traspaso es un traspaso inter nodo B evolucionado y otra derivación de clave proceso si un traspaso es un traspaso intra nodo B evolucionado.

En el caso de un fallo de enlace de radio (RLF), el gestor de traspaso 94 puede configurarse adicionalmente para recibir un mensaje de reconfiguración de control de recursos de radio (RRC). El mensaje de RRC puede incluir un indicador en cuanto a si la célula a la que tiene que fijarse el UE es un nodo B evolucionado diferente al que estaba fijado anteriormente el UE. Por consiguiente, el gestor de traspaso 94 puede configurarse para determinar si el UE se fija a un nuevo nodo B evolucionado tras un fallo de enlace de radio y para realizar derivaciones de clave intermedia basándose en la determinación.

La Figura 4 es un diagrama de flujo de control de señales de comunicación pasadas entre entidades de la realización ilustrativa de la Figura 3 así como operaciones realizadas por las entidades durante un proceso de traspaso inter nodo B evolucionado de acuerdo con una realización ilustrativa de la presente invención. Las operaciones 400-404 comprenden operaciones de inicialización que pueden producirse tras una fijación inicial y/o una transición de estado en reposo a activo en la que no hay ningún mensaje de conmutación de trayectoria. Estas operaciones de inicialización pueden servir para proporcionar claves intermedias y/u otros valores que pueden usarse para derivar encriptado y claves de protección de integridad y para usarse después de un traspaso posterior para derivar nuevas claves intermedias. En la operación 400, la MME puede calcular opcionalmente la clave intermedia KeNB si la MME no tiene aún de otra manera acceso a la clave, tal como la clave que se calculó anteriormente y almacenó en la memoria. Este cálculo puede realizarse usando cualquier función de derivación de clave que se conoce tanto por la MME como el UE. Esta función de derivación de clave puede usar la clave KASME y número de secuencia (SN) de enlace ascendente de NAS como parámetros de entrada. KASME es parte de un contexto de seguridad y se conoce tanto por la MME como el UE después de autenticación del abonado o después de haber recibido algún contexto de seguridad después de un traspaso inter tecnología de radio que ha inicializado por lo tanto el contexto de seguridad. De forma similar el SN de enlace ascendente de NAS es parte de este mismo contexto de seguridad y se conoce tanto por la MME como el UE. En este sentido, el SN de enlace ascendente de NAS puede determinarse a partir del mensaje de Petición de Servicio en la transición de estado en reposo a activo y/o el valor de reinicio 0 después de autenticación o inicializado después de traspaso (HO) desde un traspaso inter RAT. La operación 400 puede incluir adicionalmente calcular un valor intermedio que puede usarse por nodos B evolucionados para derivar claves. Este valor intermedio, identificado como Siguiente-Salto-KeNB1 en la Figura 4, puede calcularse de acuerdo con cualquier función de derivación de clave que se conoce tanto por la MME como UE. La función de derivación de clave puede usar los valores de KASME y KeNB como parámetros de entrada. La MME puede a continuación enviar un mensaje de petición de configuración de contexto inicial, que puede incluir los valores de KeNB y Siguiente-Salto-KeNB1 al nodo B evolucionado fuente en la operación 402. En la operación 404, el UE puede calcular opcionalmente el valor de KeNB si el UE no tiene aún de otra manera acceso a la clave, tal como la clave que se calculó anteriormente y almacenó en la memoria. La operación 404 puede comprender además que el UE calcule el valor de Siguiente-Salto-KeNB1 usando la misma función de derivación de clave y parámetros de entrada como la MME usada en la etapa 400. En este sentido, KeNB es una clave que puede usarse para facilitar comunicaciones entre UE y el nodo B evolucionado fuente. Siguiente-Salto-KeNB1 es un parámetro intermedio que puede usarse para derivar el valor de una clave usada para facilitar comunicaciones entre el UE y un nodo B evolucionado objetivo tras un traspaso. Aunque no se ilustra, la operación 404 puede comprender además que el UE derive las claves de RRC y UP a partir del valor de KeNB y/o a partir de valor de clave posterior derivado a partir de este KeNB mediante las funciones de derivación de clave predefinidas.

La operación 406 representa una primera operación que puede realizarse para iniciar un traspaso de un UE desde un nodo B evolucionado fuente a un nodo B evolucionado objetivo. En este sentido, el UE puede enviar informes de medición al nodo B evolucionado fuente en la operación 406. El nodo B evolucionado fuente puede a continuación tomar una decisión de traspaso en la operación 408 basándose en los informes de medición. Por ejemplo, el nodo B evolucionado fuente puede tomar una decisión para traspasar el UE si los informes de medición indican que el UE puede recibir una señal más fuerte o de otra manera más fiable desde otro nodo B evolucionado. La operación 408 puede comprender además calcular la clave de encriptación KeNB* usando cualquier función de derivación de clave que también se conoce por el UE. La función de derivación de clave puede usar el valor intermedio Siguiente-Salto-KeNB1 (este valor intermedio puede proporcionarse anteriormente al nodo B evolucionado fuente en una petición de configuración de contexto inicial, tal como en la operación 402, y/o en un mensaje de acuse de recibo de conmutación de trayectoria, tal como en la operación 430), así como ID de célula o ID de célula física, que es una indicación de la identificación de la célula objetivo seleccionada, como parámetros de entrada. En una realización alternativa, sin embargo, la función de derivación de clave puede no usar ninguna indicación de la célula objetivo seleccionada como un parámetro de entrada. En una realización alternativa de este tipo, la función de derivación de clave puede depender solamente del valor intermedio Siguiente-Salto-KeNB1 o puede usar el valor intermedio Siguiente-Salto-KeNB 1 en combinación con uno o más otros valores conocidos como parámetros de entrada. La operación 410 puede comprender el nodo B evolucionado fuente enviar una petición de traspaso que incluye el valor de KeNB* como un parámetro al nodo B evolucionado objetivo. En este sentido, KeNB* es la clave que puede usarse para facilitar comunicación entre el UE y el nodo B evolucionado objetivo.

La operación 414 puede comprender el nodo B evolucionado objetivo confirmando la solicitud de traspaso al nodo B evolucionado fuente. El nodo B evolucionado fuente puede a continuación enviar una orden de traspaso al UE en la operación 416. Esta orden de traspaso puede incluir un indicador de tipo de traspaso que identifica si el traspaso es un traspaso inter nodo B evolucionado. En algunas realizaciones, el proceso de derivación de clave puede diferir de los procesos divulgados en este documento para traspasos de intra nodo B evolucionado. Por consiguiente, el UE

puede usar el indicador de tipo de traspaso para determinar un proceso de derivación de clave apropiado. En realizaciones en las que en una indicación de la identificación de la célula objetivo se usa para funciones de derivación de clave e ID de célula se usa en lugar de ID de célula física, la orden de traspaso puede incluir adicionalmente una indicación del ID de célula objetivo.

El UE puede a continuación calcular valores para KeNB* y Siguiente-Salto-KeNB2 en la operación 418. El UE puede calcular KeNB* usando la misma función de derivación de clave y parámetros de entrada usados por el nodo B evolucionado fuente en la operación 408. Siguiente-Salto-KeNB2 es un valor intermedio calculado usando la misma función de derivación de clave como Siguiente-Salto-KeNB 1 que puede usarse para calcular clave o claves intermedias en un traspaso posterior. Por consiguiente, Siguiente-Salto-KeNB2 puede almacenarse por el UE para uso en un proceso de traspaso posterior desde el nodo B evolucionado objetivo a un tercer nodo B evolucionado. En la operación 420, el UE puede enviar un mensaje de conformación de traspaso al nodo B evolucionado objetivo.

El nodo B evolucionado objetivo puede a continuación enviar un mensaje de conmutación de trayectoria a la MME en la operación 422. En las realizaciones, tal como se ilustra en la Figura 4, en la que se usa una indicación de la identificación de la célula objetivo para funciones de derivación de clave y se usa ID de célula física en lugar de ID de célula, el mensaje de conmutación de trayectoria puede incluir una indicación del ID de célula física de modo que el ID de célula física puede determinarse por la MME a partir del mensaje de conmutación de trayectoria. En realizaciones alternativas en las que no se usa ninguna indicación de la célula objetivo para función de derivación de clave en las operaciones 408, 418 y 426, el mensaje de conmutación de trayectoria no necesita incluir una indicación del ID de célula física. En algunas realizaciones, el mensaje de conmutación de trayectoria puede incluir adicionalmente una clave de firma u otros medios para permitir que la MME verifique que el mensaje de conmutación de trayectoria se envió desde un nodo B evolucionado válido. Esta clave de firma puede ser, por ejemplo, un valor intermedio, tal como Siguiente-Salto-KeNB 1, y/o claves derivadas a partir del valor intermedio. El nodo B evolucionado objetivo puede determinar si enviar el mensaje de conmutación de trayectoria basándose en el escenario de traspaso.

En algunas realizaciones, el nodo B evolucionado objetivo puede enviar el mensaje de conmutación de trayectoria de operación 422 únicamente si el traspaso es un traspaso inter nodo B evolucionado, tal como el escenario de traspaso ilustrado en la Figura 4. En un escenario alternativo, que no se ilustra en la Figura 4, un traspaso puede ser un traspaso inter célula pero ser aún un traspaso en el que los nodos B evolucionados fuente y objetivo son los mismos (también denominado como un intra eNB, traspaso inter célula). En otro escenario alternativo, que no se ilustra en la Figura 4, el traspaso puede ser un traspaso intra célula. Por consiguiente, en una realización alternativa, el nodo B evolucionado objetivo puede configurarse para enviar el mensaje de conmutación de trayectoria en la operación 422 para todos los traspasos inter célula, es decir, tanto traspasos inter eNB como traspasos intra eNB, inter célula. En una realización alternativa de este tipo, la MME puede configurarse para distinguir traspasos inter célula desde traspasos intra célula, tal como, por ejemplo, basándose en cambiar ID de célula. En otra realización alternativa, el nodo B evolucionado objetivo puede configurarse para enviar el mensaje de conmutación de trayectoria en la operación 422 incluso para traspasos intra célula. En esta realización alternativa, la MME puede configurarse para distinguir retransmisiones de mensaje de conmutación de trayectoria de mensajes de conmutación de trayectoria intra célula.

La operación 424 puede comprender que la MME envía una petición de actualización de plano U a la pasarela de servicio. La operación 426 puede comprender que la MME calcule el valor de KeNB* usando la misma función de derivación de clave y parámetros de entrada usados por el nodo B evolucionado fuente en la operación 408. La operación 426 puede comprender además que la MME calcule Siguiente-Salto-KeNB2 usando la misma función de derivación de clave como se usa por el UE en la operación 418 basándose en los valores de KASME y KeNB*. La MME puede a continuación almacenar Siguiente-Salto-KeNB2 en memoria. La pasarela de servicio puede a continuación enviar una respuesta de actualización de plano U a la MME en la operación 428. La operación 430 puede comprender la MME enviar un acuse de recibido de conmutación de trayectoria al nodo B evolucionado objetivo. El acuse de recibido de conmutación de trayectoria puede incluir el valor de Siguiente-Salto-KeNB2 como un parámetro.

El nodo B evolucionado objetivo puede a continuación almacenar el valor de Siguiente-Salto-KeNB2 en memoria en la operación 432. En este sentido, Siguiente-Salto-KeNB2 puede usarse por el nodo B evolucionado objetivo como un parámetro intermedio para calcular KeNB* en un traspaso posterior. El nodo B evolucionado objetivo puede a continuación enviar un mensaje al nodo B evolucionado fuente en la operación 434 que libera nodo B evolucionado fuente.

Las Figuras 5 y 6 son diagramas de flujo de un sistema, método y producto de programa de acuerdo con realizaciones ilustrativas de la invención. Se entenderá que cada bloque o etapa de los diagramas de flujo, y combinaciones de bloques en los diagramas de flujo, puede implementarse mediante diversos medios, tal como hardware, firmware y/o producto de programa informático que incluye una o más instrucciones de programa informáticas. Por ejemplo, uno o más de los procedimientos descritos anteriormente pueden incorporarse mediante un producto de programa informático que incluye instrucciones de programa informáticas. En este sentido, las instrucciones de programa informáticas que incorporan los procedimientos descritos anteriormente pueden

almacenarse por un dispositivo de memoria del terminal móvil y ejecutarse por un procesador en el terminal móvil y/o un procesador de otra entidad de red, tal como, por ejemplo, un SGSN o MME. Como se apreciará, cualesquiera instrucciones de programa informáticas tales pueden cargarse en un ordenador u otro aparato programable (es decir, hardware) para producir una máquina, de tal forma que las instrucciones almacenadas en memoria que se ejecutan en el ordenador u otro aparato programable crean medios para implementar las funciones especificadas en el bloque o bloques o etapa o etapas de los diagramas de flujo. Estas instrucciones de programa informáticas también pueden almacenarse en una memoria legible por ordenador que puede dirigir un ordenador u otro aparato programable para funcionar de una manera particular, de tal forma que las instrucciones almacenadas en la memoria legible por ordenador produce un artículo de fabricación que incluye medios de instrucciones que implementan la función especificada en el bloque o bloques o etapa o etapas de los diagramas de flujo. Las instrucciones de programa informáticas también pueden cargarse en un ordenador u otro aparato programable para provocar que se realicen una serie de etapas operacionales en el ordenador u otro aparato programable para producir un proceso implementado en ordenador de tal forma que las instrucciones almacenadas en memoria que se ejecutan en el ordenador u otro aparato programable proporcionan etapas para implementar las funciones especificadas en el bloque o bloques o etapa o etapas de los diagramas de flujo.

Por consiguiente, bloques o etapas de los diagramas de flujo soportan combinaciones de medios para realizar las funciones especificadas, combinaciones de etapas para realizar las funciones especificadas y un producto de programa informático que incluye instrucciones de programa para realizar las funciones especificadas. Se entenderá también que uno o más bloques o etapas de los diagramas de flujo, y combinaciones de bloques o etapas en los diagramas de flujo, pueden implementarse mediante sistemas informáticos basados en hardware de fin especial que realizan las funciones especificadas o etapas, o combinaciones de hardware de fin especial e instrucciones informáticas.

La Figura 5 ilustra una realización de un método para proporcionar separación de clave criptográfica para traspasos, que ilustra operaciones que pueden producirse en una pasarela de señalización, tal como, por ejemplo, un SGSN o una entidad de gestión de movilidad (MME), durante un proceso de traspaso. En este sentido, una realización del método ilustrado en la Figura 5 incluye que la MME calcule KeNB y Siguiente-Salto-KeNB1 en la operación 500. La MME puede a continuación enviar una petición de configuración de contexto inicial que puede incluir KeNB y Siguiente-Salto-KeNB1 a un punto de acceso de servicio, tal como un nodo B evolucionado de servicio, en la operación 510. Se apreciará que las operaciones 500 y 510 comprenden operaciones de inicialización opcionales que pueden producirse tras una fijación inicial y/o una transición de estado en reposo a activo en la que no hay ningún mensaje de conmutación de trayectoria. Estas operaciones de inicialización pueden servir para proporcionar claves intermedias y/u otros valores que pueden usarse para derivar encriptado y claves de protección de integridad y para usarse después de un traspaso posterior para derivar nuevas claves intermedias. Por consiguiente, en algunas situaciones, las operaciones 500 y 510 pueden no producirse. Esta petición de configuración de contexto puede incluir los valores de KeNB y Siguiente-Salto-KeNB1 como parámetros. En la operación 520, la MME puede recibir una petición de conmutación de trayectoria desde un punto de acceso objetivo, tal como un nodo B evolucionado objetivo. En algunas realizaciones, la MME también puede verificar opcionalmente el mensaje de conmutación de trayectoria basándose en la clave de Siguiente-Salto-KeNB1 y/o claves derivadas a partir del Siguiente-Salto-KeNB1 en la operación 530. En algunas realizaciones, la petición de conmutación de trayectoria también puede incluir un ID de célula objetivo física. La MME puede a continuación enviar una petición de actualización de plano U a una pasarela de servicio en respuesta a la petición de conmutación de trayectoria en la operación 540. La operación 550 puede comprender que la MME calcule KeNB* y Siguiente-Salto-KeNB2. La MME puede a continuación almacenar el valor de Siguiente-Salto-KeNB2 en memoria. La operación 560 puede comprender la MME recibir una respuesta de actualización de plano U desde la pasarela de servicio. La MME puede enviar adicionalmente un acuse de recibido de conmutación de trayectoria que incluye el valor de Siguiente-Salto-KeNB2 al nodo B evolucionado objetivo en la operación 570.

La Figura 6 ilustra otra realización ilustrativa de un método para proporcionar separación de clave criptográfica para traspasos. En este sentido, la Figura 6 ilustra operaciones que pueden producirse en un UE durante un proceso de traspaso. El método puede incluir calcular KeNB en la operación 600. El UE puede a continuación calcular Siguiente-Salto-KeNB 1 en la operación 610 y envían informes de medición a un punto de acceso fuente, tal como a nodo B evolucionado fuente, en la operación 620. La operación 630 puede comprender que el UE reciba una orden de traspaso desde un punto de acceso fuente, tal como a nodo B evolucionado fuente. El UE puede a continuación calcular KeNB* y Siguiente-Salto-KeNB2 en la operación 640. El UE puede derivar claves de RRC y UP a partir del valor calculado de KeNB*. La operación 650 puede comprender que el UE envíe un mensaje de conformación de traspaso a un punto de acceso objetivo, tal como el nodo B evolucionado objetivo.

Las funciones descritas anteriormente pueden efectuarse de muchas formas. Por ejemplo, para efectuar la invención puede emplearse cualquier medio adecuado para efectuar cada una de las funciones descritas anteriormente. En una realización, todos o una porción de los elementos de la invención generalmente operan bajo el control de un producto de programa informático. Para realizar los métodos de realizaciones de la invención el producto de programa informático incluye un medio de almacenamiento legible por ordenador, tal como el medio de almacenamiento no volátil, y porciones de código de programa legible por ordenador, tal como una serie de instrucciones informáticas, incorporadas en el medio de almacenamiento legible por ordenador.

Por consiguiente, realizaciones de la presente invención proporcionan claves intermedias criptográficamente separadas para traspasos después de dos traspasos (también conocidos como 'saltos') configurando la pasarela de señalización o entidad de gestión de movilidad, tal como una MME, para proporcionar el punto de acceso objetivo con un parámetro de Siguiente-Salto-KeNB dentro de un acuse de recibo/respuesta de actualización de ubicación o mensaje de acuse de recibo/respuesta de actualización vinculante, tal como, por ejemplo, un mensaje de acuse de recibo de conmutación de trayectoria. En este sentido, derivar una clave usando una función de derivación de clave que usa tanto el KASME como Siguiente-Salto-KeNB como parámetros de entrada puede derivar en una clave que está criptográficamente separada del KeNB usado por el punto de acceso fuente. Al menos algunas realizaciones de la presente invención proporcionan separación de clave criptográfica después de dos traspasos porque el mensaje de acuse de recibo de conmutación de trayectoria se proporciona después del traspaso de enlace de radio y por lo tanal punto de acceso fuente proporciona los valores clave usados por el punto de acceso objetivo. Sin embargo, después de un traspaso adicional, el punto de acceso fuente puede no calcular las claves que el punto de acceso objetivo usa para preparar traspaso a un punto de acceso objetivo posterior ya que los valores usados por el punto de acceso objetivo se proporcionan por la MME en el mensaje de acuse de recibo de conmutación de trayectoria.

Además, realizaciones de la presente invención pueden proporcionar separación de clave criptográfica para traspasos con mínimo impacto a entidades de red en términos de sobrecarga. En algunas realizaciones, la MME realiza una derivación de clave adicional por traspaso y almacena el Siguiente-Salto-KeNB actual de modo que puede usar el valor del Siguiente-Salto-KeNB actual en una función de derivación de clave para producir un nuevo KeNB y un nuevo Siguiente-Salto-KeNB. Un UE, en algunas realizaciones, ejecuta un cálculo adicional para derivar un valor intermedio antes de calcular Valores de KeNB*.

Muchas modificaciones y otras realizaciones de las invenciones expuestas en este documento vendrán a la mente a un experto en la materia a la que pertenecen estas invenciones teniendo el beneficio de los contenidos presentados en las descripciones anteriores y los dibujos asociados. Por ejemplo, aunque realizaciones de la invención se describieron en conexión con la norma de E-UTRAN, realizaciones de la invención pueden emplearse con otras redes y protocolos de comunicación. Por lo tanto, debe apreciarse que las invenciones no deben limitarse a las realizaciones específicas divulgadas y que modificaciones y otras realizaciones se conciben para incluirse dentro del alcance de las reivindicaciones adjuntas. Además, aunque las descripciones anteriores y los dibujos asociados describen realizaciones ilustrativas en el contexto de ciertas combinaciones ilustrativas de elementos y/o funciones, debería apreciarse que pueden proporcionarse diferentes combinaciones de elementos y/o funciones mediante realizaciones alternativas sin alejarse del alcance de las reivindicaciones adjuntas. En este sentido, por ejemplo, diferentes combinaciones de elementos y/o funciones de las descritas explícitamente anteriormente también se contemplan como que pueden exponerse en algunas de las reivindicaciones adjuntas. Aunque se emplean términos específicos en este documento, se usan únicamente en un sentido genérico y descriptivo y no para propósitos de limitación.

REIVINDICACIONES

1. Un método implementado en una entidad de gestión de movilidad (80), comprendiendo el método:

calcular (426), en respuesta a un traspaso de un dispositivo de equipo de usuario (70) desde un punto de acceso fuente (72) a un punto de acceso objetivo (74), una clave criptográfica por medio de una primera función usando al menos un primer valor intermedio anteriormente almacenado como su parámetro;
calcular (426) un segundo valor intermedio por medio de una segunda función usando al menos la clave criptográfica calculada como su parámetro; y
enviar (430) un mensaje de acuse de recibo de conmutación de trayectoria, que incluye el segundo valor intermedio, al punto de acceso objetivo (74) para uso en un traspaso posterior del dispositivo de equipo de usuario (70).

2. El método de la reivindicación 1, que comprende adicionalmente:

recibir un mensaje de conmutación de trayectoria desde el punto de acceso objetivo (74); y
en donde calcular la clave criptográfica comprende calcular la clave criptográfica en respuesta a la recepción del mensaje de conmutación de trayectoria.

3. El método de la reivindicación 2, en el que:

recibir un mensaje de conmutación de trayectoria comprende además recibir un mensaje de conmutación de trayectoria que comprende una indicación de una identificación de célula; y en donde
calcular la clave criptográfica comprende calcular la clave criptográfica por medio de la primera función usando al menos la identificación de célula y el primer valor intermedio anteriormente almacenado como sus parámetros.

4. El método de la reivindicación 2, en el que:

recibir un mensaje de conmutación de trayectoria comprende además recibir un mensaje de conmutación de trayectoria que ha sido protegido por el punto de acceso objetivo (74) por medio de la primera función usando al menos el primer valor intermedio; y comprendiendo además:
verificar el mensaje de conmutación de trayectoria basándose al menos en parte en el primer valor intermedio antes de calcular la clave criptográfica.

5. El método de cualquiera de las reivindicaciones 1-4, en el que calcular el segundo valor intermedio comprende calcular el segundo valor intermedio por medio de la segunda función usando al menos la clave criptográfica calculada, el primer valor intermedio y K_{ASME}, en donde el K_{ASME} es parte de un contexto de seguridad.

6. El método de cualquiera de las reivindicaciones 1-5, en el que calcular una clave criptográfica comprende calcular la clave criptográfica tras traspaso de enlace de radio del dispositivo de equipo de usuario (70).

7. El método de cualquiera de las reivindicaciones 1-6, en el que calcular el segundo valor intermedio comprende una entidad de gestión de movilidad que calcula el segundo valor intermedio.

8. Un método implementado en un equipo de usuario (70), comprendiendo el método:

recibir, en respuesta a un traspaso de dispositivo de equipo de usuario (70) desde un punto de acceso fuente (72) a un punto de acceso objetivo (74), una orden de traspaso desde un punto de acceso fuente (72);
calcular (418), en respuesta a la recepción de la orden de traspaso, una clave criptográfica por medio de una primera función usando al menos un primer valor intermedio como su parámetro; y
calcular (418) un segundo valor intermedio por medio de una segunda función usando al menos la clave criptográfica como su parámetro, en donde el segundo valor intermedio tiene que usarse para el cálculo de una o más claves criptográficas en un traspaso posterior.

9. El método de la reivindicación 8, en el que la orden de traspaso comprende además una indicación de una identificación de célula; y en el que
calcular la clave criptográfica comprende calcular la clave criptográfica por medio de la primera función usando al menos la identificación de célula y el primer valor intermedio como su parámetro.

10. El método de cualquiera de las reivindicaciones 8-9, en el que calcular el segundo valor intermedio comprende calcular el segundo valor intermedio por medio de la segunda función usando al menos la clave criptográfica calculada, el primer valor intermedio y K_{ASME}, en donde el K_{ASME} es parte de un contexto de seguridad.

11. El método de cualquiera de las reivindicaciones 8-10, en el que la orden de traspaso indica un traspaso de un dispositivo de equipo de usuario desde el punto de acceso fuente a un punto de acceso objetivo.

12. El método de cualquiera de las reivindicaciones 8-11, en el que la clave criptográfica calculada se usa para facilitar comunicaciones con un punto de acceso objetivo tras el traspaso.

13. El método de cualquiera de las reivindicaciones 8-12, que comprende además almacenar el segundo valor intermedio en una memoria.

14. El método de cualquiera de las reivindicaciones 8-13, en el que calcular el segundo valor intermedio comprende calcular el segundo valor intermedio con un gestor de traspaso.

15. Un producto de programa informático incorporado en un medio de almacenamiento y que comprende instrucciones que, cuando son ejecutadas por al menos un procesador de datos, dan como resultado las operaciones de acuerdo con cualquiera de las reivindicaciones 1 a 7.

16. Un producto de programa informático incorporado en un medio tangible y que comprende instrucciones que, cuando son ejecutadas por al menos un procesador de datos, dan como resultado las operaciones de acuerdo con cualquiera de las reivindicaciones 8 a 14.

17. Una entidad de gestión de movilidad (80) que comprende:

medios para calcular, en respuesta a un traspaso de un dispositivo de equipo de usuario (70) desde un punto de acceso fuente (72) a un punto de acceso objetivo (74), una clave criptográfica por medio de una primera función usando al menos un primer valor intermedio anteriormente almacenado como su parámetro;
medios para calcular un segundo valor intermedio por medio de una segunda función usando al menos la clave criptográfica calculada como su parámetro; y
medios para enviar un mensaje de acuse de recibo de conmutación de trayectoria, que incluye el segundo valor intermedio, al punto de acceso objetivo (74) para uso en un traspaso posterior del dispositivo de equipo de usuario.

18. La entidad de gestión de movilidad (80) de la reivindicación 17, configurada adicionalmente para realizar el método de acuerdo con cualquiera de las reivindicaciones 2 a 7.

19. Un equipo de usuario (70) que comprende:

medios para recibir, en respuesta a un traspaso de dispositivo de equipo de usuario (70) desde un punto de acceso fuente (72) a un punto de acceso objetivo (74), una orden de traspaso desde un punto de acceso fuente (72);
medios para calcular, en respuesta a la recepción de la orden de traspaso, una clave criptográfica por medio de una primera función usando al menos un primer valor intermedio como su parámetro; y
medios para calcular un segundo valor intermedio por medio de una segunda función usando al menos la clave criptográfica como su parámetro, en donde el segundo valor intermedio tiene que usarse para el cálculo de una o más claves criptográficas en un traspaso posterior.

20. El equipo de usuario (70) de la reivindicación 19, configurado adicionalmente para realizar el método de acuerdo con cualquiera de las reivindicaciones 9 a 14.

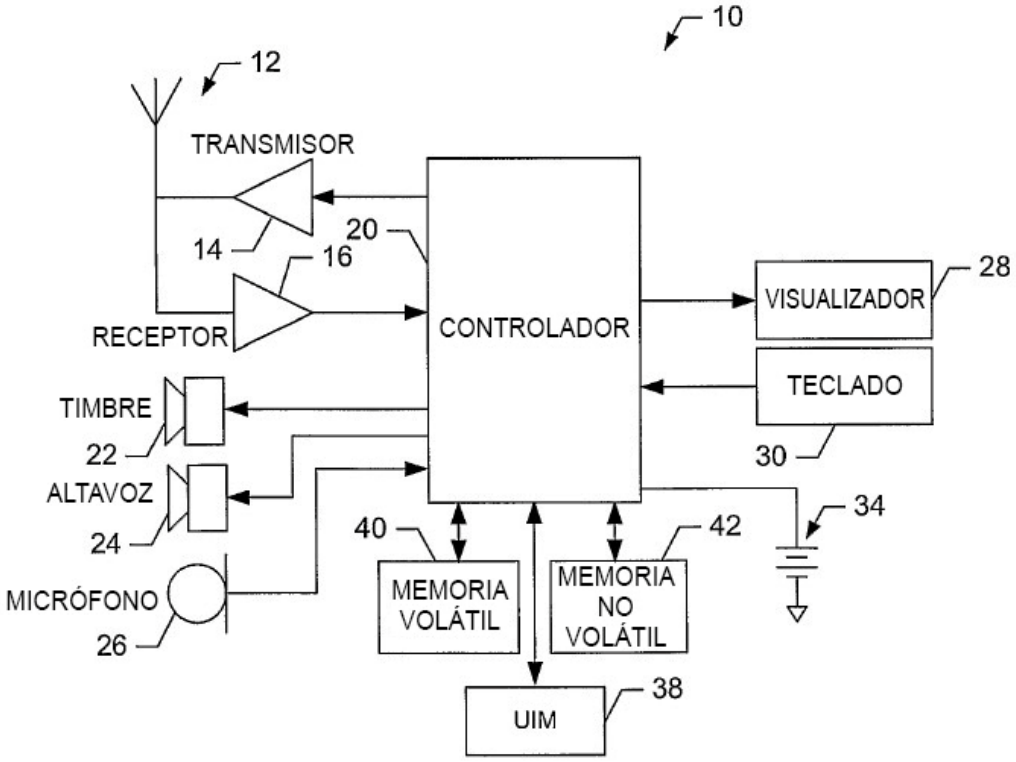
10
12
TRANSMISOR
14
16
20
RECEPTOR
CONTROLADOR
VISUALIZADOR
28
TECLADO
30
TIMBRE
22
ALTAVOZ
24
MICRÓFONO
26
34
40
42
MEMORIA VOLÁTIL
MEMORIA NO VOLÁTIL
UIM
38

FIG. 1.

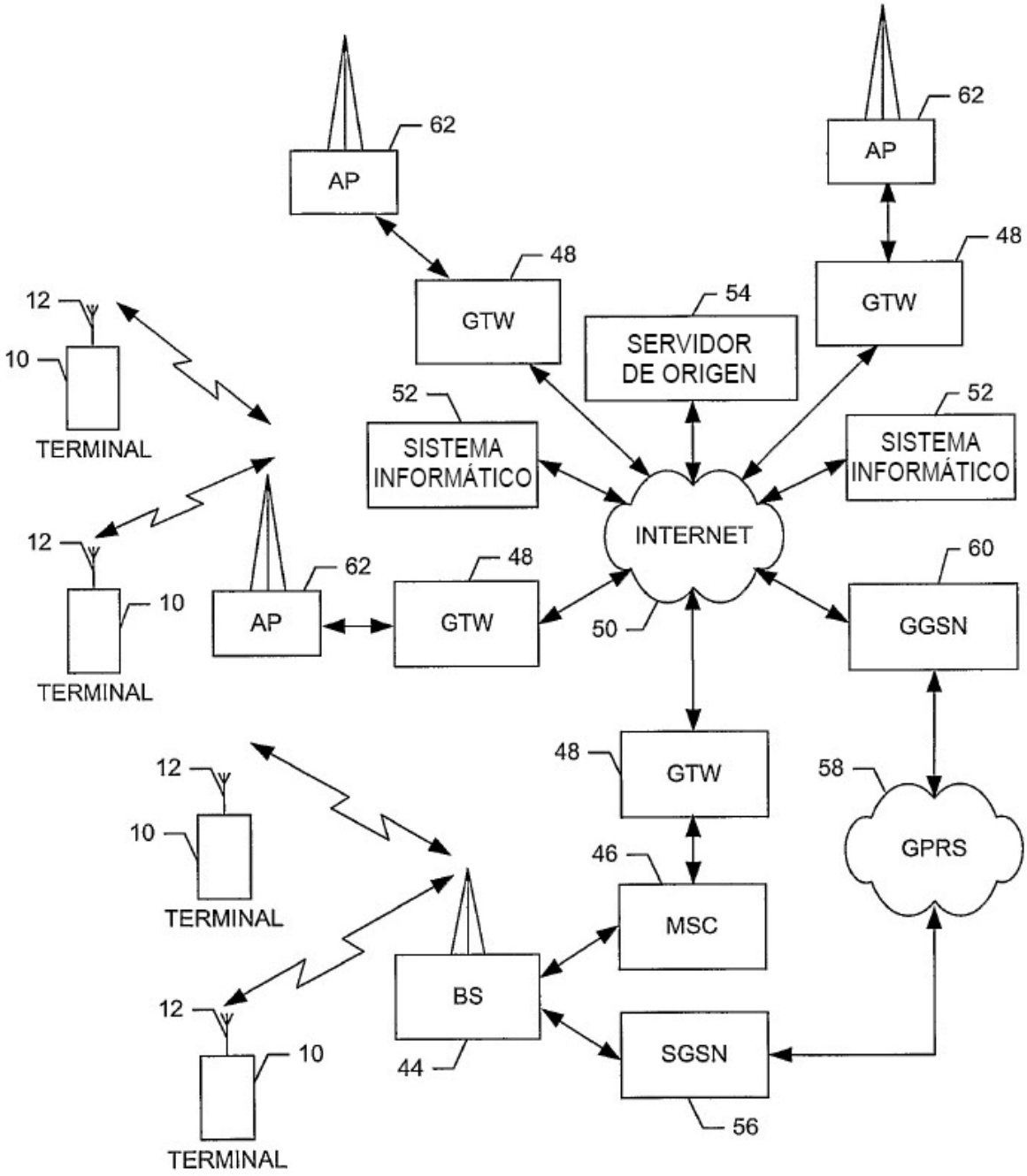
62
AP
62
AP
48
GTW
48
GTW
54
SERVIDOR DE ORIGEN
12
10
TERMINAL
52
SISTEMA INFORMÁTICO
52
SISTEMA INFORMÁTICO
INTERNET
12
10
TERMINAL
62
AP
48
GTW
50
60
GGSN
48
GTW
58
GPRS
12
10
TERMINAL
46
MSC
BS
12
10
TERMINAL
44
SGSN
56

FIG. 2.

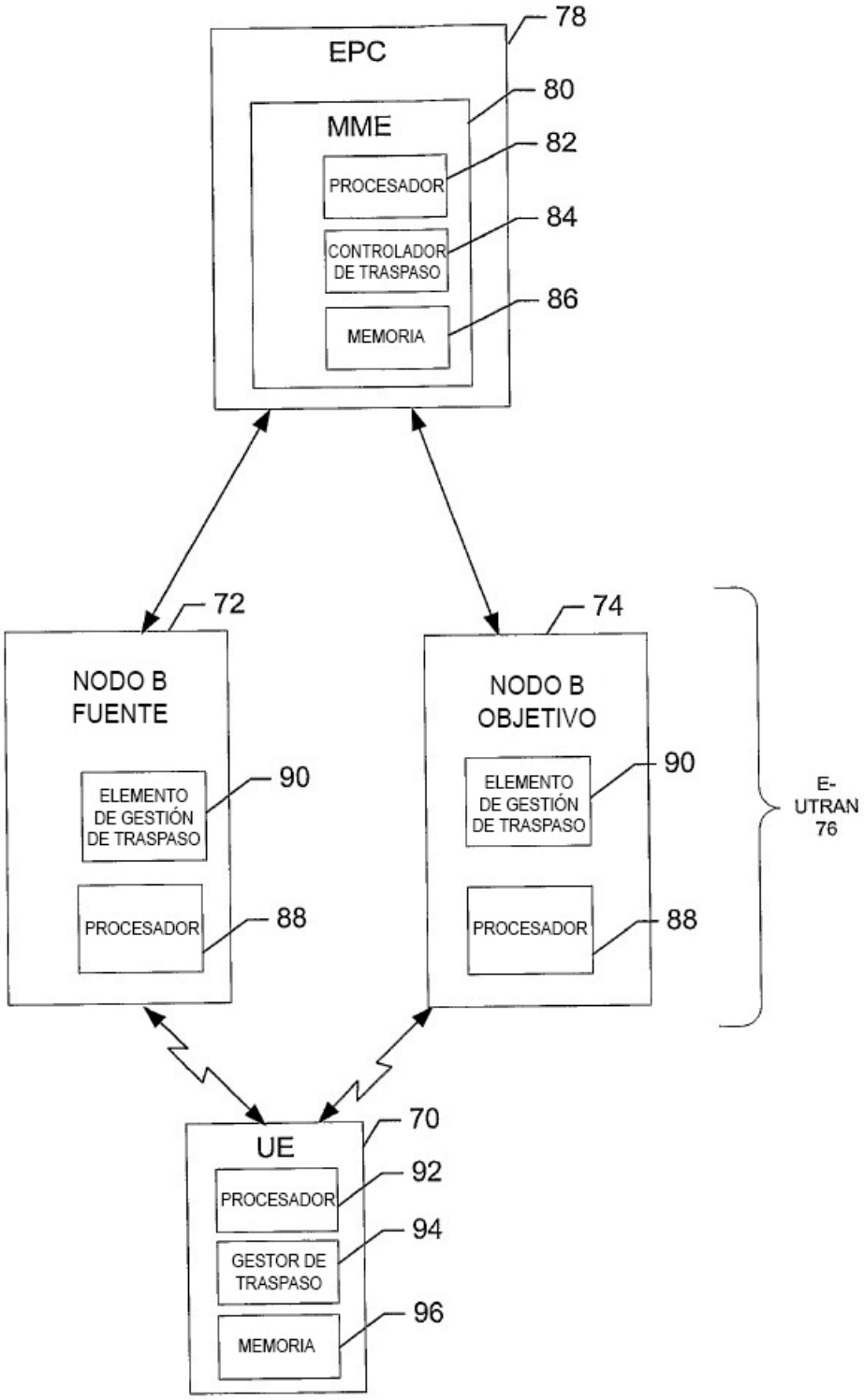
78
EPC
80
MME
82
PROCESADOR
84
CONTROLADOR DE TRASPASO
86
MEMORIA
72
NODO B FUENTE
90
ELEMENTO DE GESTIÓN DE TRASPASO
88
PROCESADOR
74
NODO B OBJETIVO
90
ELEMENTO DE GESTIÓN DE TRASPASO
88
PROCESADOR
E-UTRAN 76
70
UE
92
PROCESADOR
94
GESTOR DE TRASPASO
96
MEMORIA

FIG. 3.

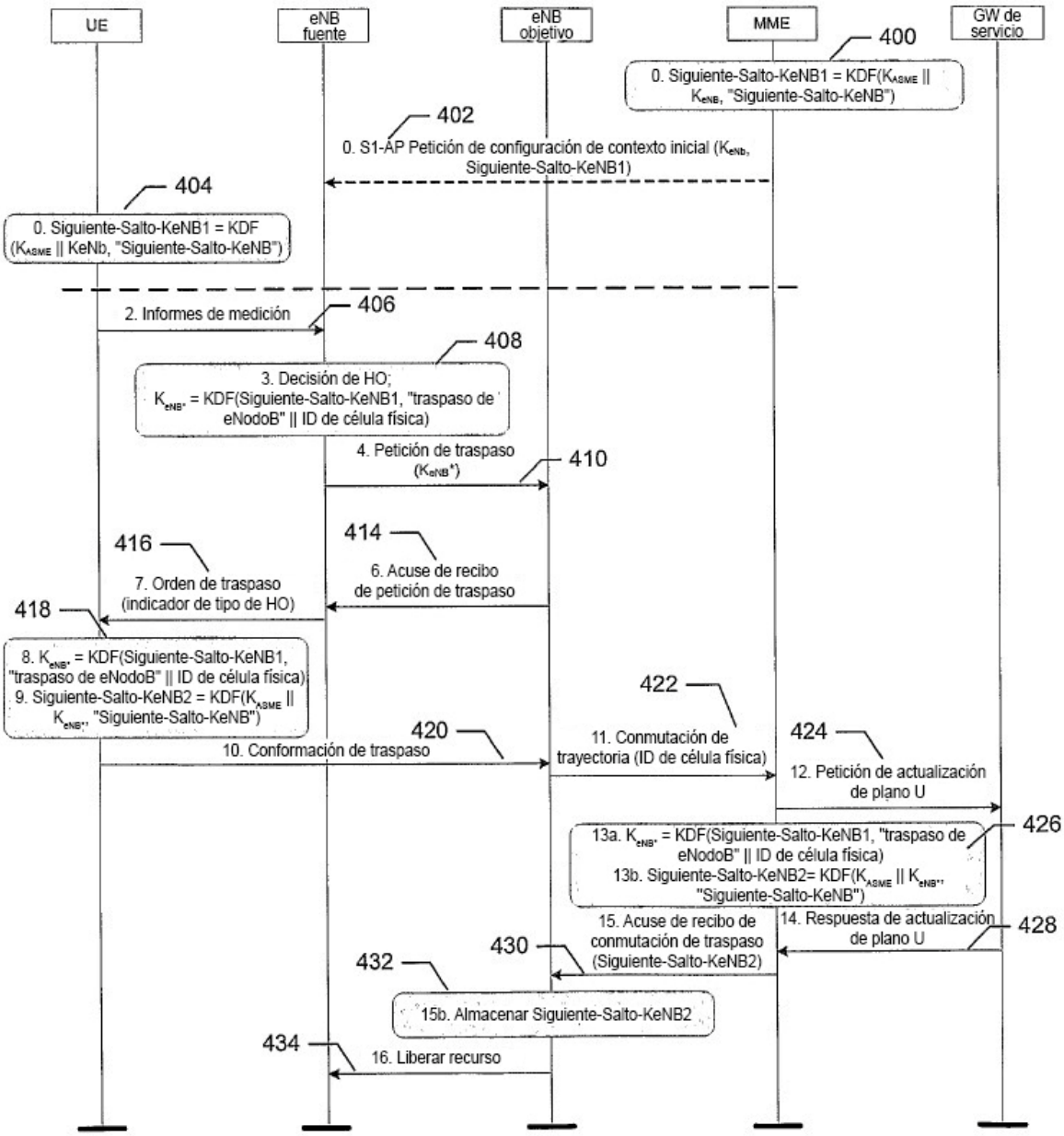
UE
eNB fuente
eNB objetivo
MME
GW de servicio
400
0. Siguiente-Salto-KeNB1 = KDF(KASME || KeNB, "Siguiente-Salto-KeNB")
402
0. S1-AP Petición de configuración de contexto inicial (KeNb, Siguiente-Salto-KeNB1)
404
0. Siguiente-Salto-KeNB1 = KDF (KASME || KeNb, "Siguiente-Salto-KeNB")
2. Informes de medición
406
408
3. Decisión de HO; KeNB* = KDF(Siguiente-Salto-KeNB1, "traspaso de eNodoB" || ID de célula física)
4. Petición de traspaso (KeNB*)
410
414
6. Acuse de recibo de petición de traspaso
416
7. Orden de traspaso (indicador de tipo de HO)
418
8. KeNB* = KDF(Siguiente-Salto-KeNB1, "traspaso de eNodoB" || ID de célula física)
9. Siguiente-Salto-KeNB2 = KDF(KASME || KeNB*, "Siguiente-Salto-KeNB")
422
11. Conmutación de trayectoria (ID de célula física)
420
10. Conformación de traspaso
424
12. Petición de actualización de plano U
426
13a. KeNB* = KDF(Siguiente-Salto-KeNB1, "traspaso de eNodoB" || ID de célula física)
13b. Siguiente-Salto-KeNB2= KDF(KASME || KeNB*, "Siguiente-Salto-KeNB")
15. Acuse de recibo de conmutación de traspaso (Siguiente-Salto-KeNB2)
14. Respuesta de actualización de plano U
428
430
432
15b. Almacenar Siguiente-Salto-KeNB2
434
16. Liberar recurso

FIG. 4.

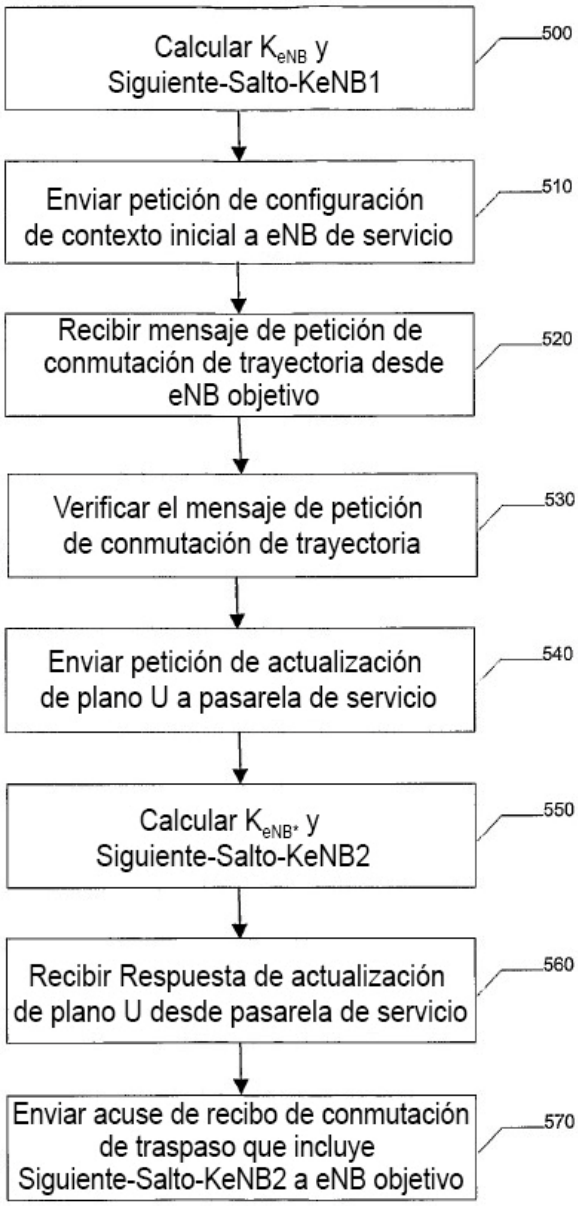
Calcular K_{eNB} y Siguiente-Salto-KeNB1
500
Enviar petición de configuración de contexto inicial a eNB de servicio
510
Recibir mensaje de petición de conmutación de trayectoria desde eNB objetivo
520
Verificar el mensaje de petición de conmutación de trayectoria
530
Enviar petición de actualización de plano U a pasarela de servicio
540
Calcular K_{eNB^*} y Siguiente-Salto-KeNB2
550
Recibir Respuesta de actualización de plano U desde pasarela de servicio
560
Enviar acuse de recibo de conmutación de traspaso que incluye Siguiente-Salto-KeNB2 a eNB objetivo
570

FIG. 5.

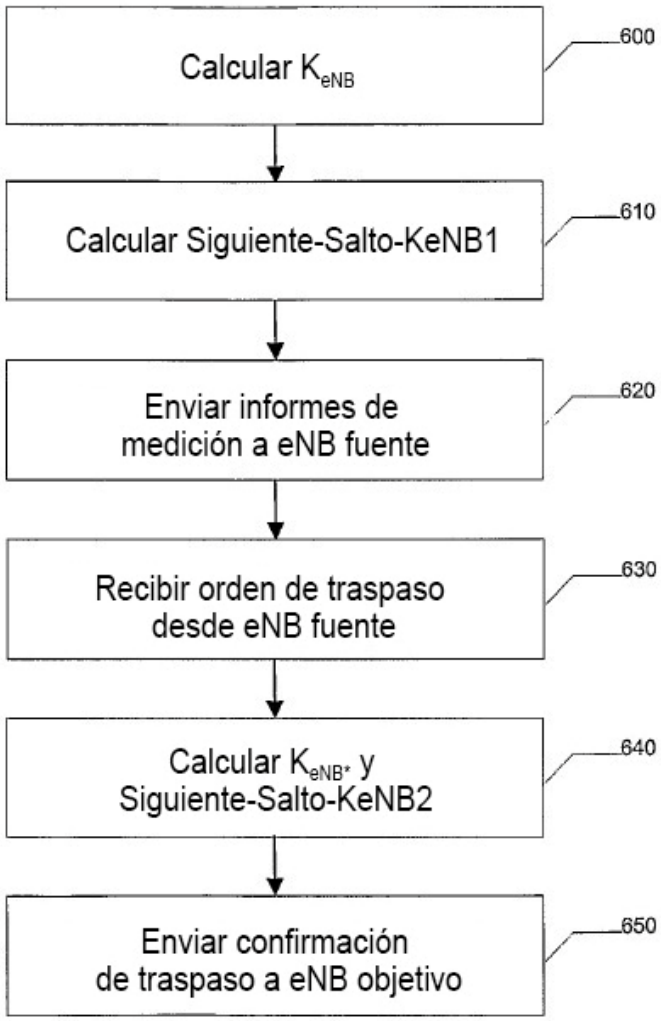
Calcular K_{eNB}
600
Calcular Siguiente-Salto-KeNB1
610
Enviar informes de medición a eNB fuente
620
Recibir orden de traspaso desde eNB fuente
630
Calcular K_{eNB*} y Siguiente-Salto-KeNB2
640
Enviar confirmación de traspaso a eNB objetivo
650

FIG. 6.