(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 354**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.08.2007 E 07801546 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.04.2016 EP 2070290**

(54) Título: **Encriptación en telecomunicaciones inalámbricas**

(30) Prioridad:

03.10.2006 GB 0619499

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.09.2016

(73) Titular/es:

ALCATEL LUCENT (100.0%)
148/152 route de la Reine
92100 Boulogne-Billancourt, FR

(72) Inventor/es:

CASATI, ALESSIO;
PALAT, SUDEEP, KUMAR y
TATESH, SAID

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Encriptación en telecomunicaciones inalámbricas

Campo de la invención

La presente invención se refiere a telecomunicaciones, en particular a comunicaciones inalámbricas.

Descripción de la técnica relacionada

En sistemas del Sistema Universal de Telecomunicaciones Móviles (UMTS), algunos mensajes están encriptados. La encriptación se inicia mediante un comando de modo de seguridad que se envía desde la red principal mediante la red de acceso de radio terrestre de UMTS (UTRAN) para recibirse mediante el terminal móvil. Esto es seguido por una respuesta de modo de seguridad que se envía desde el terminal móvil y se recibe mediante la red principal.

Por ejemplo, como se muestra en la Figura 1, tras recibir una solicitud 1 de establecimiento de sesión, o portadora la red 2 principal (CN) envía un comando 4 de modo de seguridad a la UTRAN 6. Esto provoca que la UTRAN 6 reenvíe el comando 4 de modo de seguridad al terminal móvil (Equipo de Usuario, UE 8). El terminal 8 móvil reacciona inicializando sus algoritmos de encriptación usando valores de parámetros específicos, en ocasiones denominados como un contexto de seguridad, y a continuación realiza acuse de recibo enviando una respuesta 10 de modo de seguridad a la UTRAN 6 que pasa la respuesta 10 a la red principal 2. Posteriormente se envía un mensaje de Estrato de No Acceso (NAS) encriptado, tal como una respuesta 12 de establecimiento de sesión desde la red principal 2 al terminal 8 móvil mediante la UTRAN 6.

En este enfoque conocido, los mensajes de modo de seguridad están desencriptados puesto que proporcionan la información de encriptación necesaria para encriptar los mensajes que siguen.

La Especificación Técnica del Proyecto Común de Tecnologías Inalámbricas de la Tercera Generación 3GPP TS 25.331 proporciona algún antecedente sobre redes de UMTS.

Otra área de antecedentes son las redes de Evolución a Largo Plazo, LTE. A partir de las redes UMTS, se están desarrollando ahora las denominadas redes de Evolución a Largo Plazo, LTE. Para antecedentes sobre las redes de Evolución a Largo Plazo, se hace referencia al lector a la Especificación Técnica del Proyecto Común de Tecnologías Inalámbricas de la Tercera Generación 3GPP TS23.882.

Se conoce a partir de la Publicación de Patente de Estados Unidos US-A-2004/024012 proporcionar un procedimiento de transmisión de datos de usuario encriptados a un terminal móvil en una red de telecomunicaciones inalámbrica, comprendiendo el procedimiento enviar al terminal móvil un paquete de datos, comprendiendo el paquete de datos tanto un identificador de información de encriptación a usarse al recuperar datos de usuario encriptados, como datos de usuario encriptados usando dicha información de encriptación.

Sumario de la invención

Se hace referencia al lector a las reivindicaciones independientes adjuntas. Algunas características preferidas se exponen en las reivindicaciones dependientes.

Los inventores se han dado cuenta de que en el enfoque conocido el comando de modo de seguridad y la señalización de respuesta provocan retardo en los procedimientos de establecimiento de sesión. Por ejemplo, cuando el terminal móvil se mueve al área de cobertura de otra estación base, puede haber un cambio en la clave de encriptación usada. Esto requiere el comando de modo de seguridad y la señalización de respuesta para informar al terminal móvil de la nueva clave antes de que se envíen datos encriptados usando la nueva clave. Esta señalización adicional puede dar lugar a un retardo adicional. Un retardo de este tipo puede ser molesto para el abonado, y puede provocar problemas con aplicaciones que son sensibles a retardo de establecimiento de llamada, tales como pulsar para hablar.

En algunas realizaciones de la invención pueden reducirse tales retardos.

Breve descripción de los dibujos

Las realizaciones de la presente invención se describirán ahora a modo de ejemplo y con referencia a los dibujos, en los que:

La Figura 1 es un diagrama que ilustra el enfoque conocido para fomentar la encriptación como parte del establecimiento de sesión (TÉCNICA ANTERIOR),
La Figura 2 es un diagrama que ilustra una red de Evolución a Largo Plazo, LTE, de acuerdo con una primera realización de la presente invención,
La Figura 3 es un diagrama que ilustra un enfoque para fomentar la encriptación como parte del establecimiento de sesión en la red mostrada en la Figura 2,
La Figura 4 es un diagrama que ilustra la estructura de un mensaje de NAS enviado en establecimiento de

sesión,
La Figura 5 es un diagrama que ilustra cómo se encriptan los mensajes de señalización de NAS,
La Figura 6 es un diagrama que ilustra traspaso entre nodos de red principal CN en la red de LTE,
La Figura 7 es un diagrama que ilustra fomentar la encriptación como parte del establecimiento de conexión de control de recursos de radio, RRC, en la red de LTE,
La Figura 8 es un diagrama que ilustra una red de Sistema Universal de Telecomunicaciones Móviles (UMTS) de acuerdo con una segunda realización de la presente invención, y
La Figura 9 es un diagrama que ilustra un enfoque para fomentar la encriptación como parte del establecimiento de sesión en la red mostrada en la Figura 8.

Descripción detallada

Se describirá en primer lugar una red de LTE de ejemplo, seguido por explicaciones de cómo se inicia la encriptación en establecimiento de sesión usando un mensaje combinado. Esto es seguido por una explicación de cómo se maneja la encriptación tras traspaso de un terminal móvil desde conexión con un nodo de red principal a otro.

Se describe a continuación un mensaje combinado alternativo.

Se describe a continuación una red alternativa, que es una red de UMTS, seguido por una explicación de cómo se inicia la encriptación en esa red.

Red de Evolución a Largo Plazo

La red 14 de LTE, que está basada en una red del Sistema Universal de Telecomunicaciones Móviles (UMTS), es básicamente como se muestra en la Figura 2. La red principal incluye las Entidades de Gestión Móviles (MME). Cada MME 16 incluye una etapa 26 de encriptación de mensaje de NAS. En la Figura 2, únicamente se muestra una Entidad 16 de Gestión Móvil (MME) de la red 18 principal y una estación 20 base de la red 14 de LTE por simplicidad. La red de LTE incluye múltiples estaciones base. En la Figura, la estación base se denomina también "eNodo B" de acuerdo con terminología de la LTE. Una célula, también denominada como un sector, es el área de cobertura de radio servida por una antena correspondiente de una estación base. Cada estación 20 base típicamente tiene tres células 22, cada una cubierta mediante una de tres antenas 24 direccionales en ángulo a 120 grados entre sí en azimut.

En uso, un terminal 28 de usuario móvil (a menudo denominado como Equipo de Usuario (UE) en terminología de LTE/UMTS) comunica con una entidad 16 de gestión móvil mediante al menos una célula 22 de al menos una estación 20 base. De esta manera, el terminal de usuario móvil comunica con la red 2 de UTRAN.

Fomentar la encriptación en el establecimiento de sesión

Los inventores se han dado cuenta de que es posible combinar el comando de modo de seguridad y el mensaje de Estrato de No Acceso (NAS) (tal como una respuesta de establecimiento de sesión) en un único mensaje combinado. La primera parte del mensaje es el comando de modo de seguridad y esta parte está desencriptada. La segunda parte del mensaje es un mensaje de NAS y esta parte está encriptada.

Como se muestra en la Figura 3, tras recibir una solicitud 30 de establecimiento de sesión, la entidad 16 de gestión móvil envía el mensaje 32 combinado que consiste en el comando de modo de seguridad desencriptado y en el mensaje de señalización de NAS encriptado a la estación 20 base. Esto provoca que la estación 20 base reenvíe el mensaje 32 combinado al terminal móvil (Equipo de Usuario, UE 28). El terminal 28 móvil efectúa la inicialización de su contexto de seguridad y a continuación realiza acuse de recibo enviando una respuesta 34 de modo de seguridad a la estación 20 base desde donde se reenvía la respuesta 34 a la entidad 16 de gestión móvil. Posteriormente se envía un mensaje de Estrato de No Acceso (NAS) encriptado, tal como una respuesta 36 de establecimiento de sesión desde la MME 16 al terminal 28 móvil mediante la estación 20 base.

El mensaje 32 combinado como se ha hecho referencia anteriormente es como se muestra en la Figura 4, y consiste en un comando 38 de seguridad desencriptado y un mensaje 40 de NAS encriptado. El comando 38 de seguridad consiste en elementos de información que definen información de contexto de seguridad tal como un identificador de la clave de encriptación a usarse, y por ejemplo, un identificador de tiempo de inicio para la encriptación. El mensaje 40 de NAS consiste en elementos de información que constituyen una respuesta de Establecimiento de Sesión.

Producción del mensaje combinado

En la red 14 de LTE la encriptación de mensajes de NAS se realiza mediante las etapas 26 de encriptación en los respectivos nodos de la red 18 principal. La encriptación de los mensajes de NAS es independiente de la encriptación de los datos de usuario.

Como se muestra en la Figura 5, el mensaje de NAS para encriptación junto con la información para efectuar la encriptación tal como las claves de encriptación se introducen en la etapa 26 de encriptación desde la que se

proporciona el mensaje 40 de NAS encriptado. El mensaje 40 de NAS encriptado está concatenado con la información 38 de encabezamiento desencriptada. Esto es posible puesto que la MME 16 generalmente permite la encriptación de al menos parte de un mensaje de NAS antes de la concatenación con otra porción de mensaje desencriptado.

Manejar la encriptación tras traspaso

El traspaso es el procedimiento para transferir el terminal 28 móvil desde la conexión con una estación 20 base y por lo tanto el nodo 18 de red principal a otra estación base (no mostrada) y por lo tanto a otro nodo de red principal (no mostrado). El traspaso en ocasiones se conoce como transferencia.

Un ejemplo de procedimiento de traspaso se muestra en la Figura 6. Inicialmente la conexión es a la estación 20 base e implica usar una primera clave de encriptación. El nodo 18 de red principal envía un comando 42 de traspaso mediante la estación 20 base al terminal 28 móvil, después de lo cual se efectúa el traspaso 44 de la conexión de llamada a una estación 20' base adicional y por lo tanto al nodo 20' de red principal. A continuación se envía un mensaje 46 de "traspaso completo" desde el terminal 28 móvil a la nueva estación 18' base y por lo tanto al nodo 18' de red principal. Posteriormente el nodo de red principal envía un mensaje 48 combinado, que consiste en un comando 50 de modo de seguridad desencriptado que incluye identificadores de clave de encriptación como se ha analizado anteriormente, seguido por una porción 52 encriptada de datos de usuario tal como mensajes de señalización de NAS. Por lo que, por ejemplo, cuando el nodo de la red principal hace cambios de encriptación, el primer mensaje 50 combinado desde el nuevo nodo 18' de red principal indica en el comando de modo de seguridad los nuevos valores de parámetros de seguridad a usarse, e incluye en forma encriptada, nuevos mensajes de señalización de NAS.

En una realización similar de otra manera, si se hace en su lugar la encriptación y la configuración de encriptación en el plano de usuario, el paquete combinado en el plano de usuario consiste en el comando de modo de seguridad desencriptado concatenado con datos de usuario.

Por supuesto, en algunas realizaciones, puede hacerse el cambio a una nueva clave de encriptación, enviando un mensaje combinado que consiste en un comando de modo de seguridad desencriptado que incluye identificadores de clave de encriptación seguido por una porción encriptada de datos de usuario encriptados usando esa clave de encriptación, en otros momentos distintos del traspaso entre células. Por ejemplo, en otra realización, la célula antigua y la célula nueva pueden ser la misma célula.

En este ejemplo, inicialmente la célula comunica con el terminal móvil usando los parámetros de encriptación antiguos. A medio camino a través de la sesión la célula envía un paquete que contiene los nuevos parámetros de encriptación y datos de usuario adicionales. El terminal móvil recibe los nuevos parámetros de encriptación. El terminal móvil usa los nuevos parámetros de encriptación para desencriptar la parte encriptada del paquete. El terminal móvil también almacena los nuevos parámetros de encriptación para uso posterior en la desencriptación de paquetes posteriores que están encriptados usando los nuevos parámetros de encriptación.

Control de recursos de radio

Como se muestra en la Figura 7, puede enviarse de manera similar un mensaje combinado que consiste en un comando de modo de seguridad desencriptado y una porción de datos de usuario encriptada, donde la porción de datos de usuario consiste en un mensaje de Control de Recursos de Radio (RRC). Como se muestra en la Figura 7, se envía una Solicitud 54 de Conexión de RRC a una estación 20" base y el mensaje 56 combinado, que comprende más específicamente el comando de Modo de Seguridad desencriptado seguido por la Respuesta de Conexión de RRC encriptada (con la nueva clave), mediante la estación base al terminal 28' móvil en contestación. Se envía a continuación una respuesta de modo de seguridad desde el terminal 28' de usuario.

Otro sistema de ejemplo: UMTS

La red es una red de acceso terrestre (UTRAN) del Sistema Universal de Telecomunicaciones Móviles (UMTS), que es un tipo de red de acceso múltiple por división de código de banda ancha (CDMA) para telecomunicaciones móviles. La red UTRAN es básicamente como se muestra en la Figura 8. Únicamente se muestra un controlador de red de radio y dos estaciones base de la red 62 de UTRAN por simplicidad. Como se muestra en esta Figura, la red 62 de UTRAN incluye las estaciones 64 base. En la Figura, cada una de las estaciones 64 base se denomina también "Nodo B" de acuerdo con terminología de UMTS. Una célula, también denominada como un sector, es el área de cobertura de radio servida mediante una antena correspondiente de una estación base. Cada estación base típicamente tiene tres células 66, cada una cubierta mediante una de las tres antenas 67 direccionales en ángulo a 120 grados entre sí en azimut. Cada controlador 68 de red de radio (RNC) típicamente controla varias estaciones 64 base y por lo tanto un número de células 66. Una estación 64 base está conectada a su controlador 68 de red de radio (RNC) mediante una interfaz 69 respectiva conocida como una interfaz IuB. En uso, un terminal 70 de usuario móvil (a menudo denominado como Equipo de Usuario (UE) en terminología de UMTS) comunica con un controlador 68 de red de radio (RCN) servidor mediante al menos una célula 66 de al menos una estación 64 base. De esta manera, el terminal de usuario móvil comunica con la red 62 de UTRAN.

El RNC está conectado a un Nodo 72 de Soporte de Pasarela Servidor, SGSN, de la red 74 principal. El SGSN 72 incluye una etapa 76 de encriptación de mensaje de NAS como se describe en más detalle a continuación.

Fomentar la encriptación en establecimiento de sesión: ejemplo de UMTS

Los inventores se han dado cuenta de que es posible combinar el comando de modo de seguridad y el mensaje de Estrato de No Acceso (NAS) (tal como una respuesta de establecimiento de sesión) en un único mensaje combinado. La primera parte del mensaje es el comando de modo de seguridad y esta parte está desencriptada. La segunda parte del mensaje es un mensaje de NAS y esta parte está encriptada.

Como se muestra en la Figura 9, tras recibir una solicitud 78 de establecimiento de sesión, el SGSN 72 envía el mensaje 80 combinado que consiste en el comando de modo de seguridad desencriptado y el mensaje de señalización de NAS encriptado al RNC 68 y por lo tanto a la estación 64 base. Esto provoca que la estación 64 base reenvíe el mensaje 80 combinado al terminal móvil (Equipo de Usuario, UE 70).

El mensaje 80 combinado consiste en un comando de seguridad desencriptado y un mensaje de NAS encriptado. El comando de seguridad consiste en elementos de información que definen información de contexto de seguridad tal como un identificador de la clave de encriptación a usarse, y por ejemplo, un identificador de tiempo de inicio para la encriptación. La porción de mensaje de NAS encriptado del mensaje 80 consiste en elementos de información que constituyen una respuesta de Establecimiento de Sesión.

El terminal 70 móvil efectúa la inicialización de su contexto de seguridad y a continuación realiza acuse de recibo enviando una respuesta 82 de modo de seguridad a la estación 64 base y por lo tanto al RNC 68 desde donde la respuesta 82 se reenvía en el SGSN 72.

General

La presente invención puede realizarse en otras formas específicas sin alejarse de sus características esenciales. Las realizaciones descritas se han de considerar en todos los aspectos únicamente como ilustrativas y no restrictivas. El alcance de la invención se indica, por lo tanto, mediante las reivindicaciones adjuntas en lugar de mediante la anterior descripción. Todos los cambios que entren dentro del significado y alcance de equivalencia de las reivindicaciones se han de abarcar dentro de su alcance.

Algunas abreviaturas

CN: Red principal
UMTS: Sistema Universal de Telecomunicaciones Móviles
UE: equipo de usuario
NAS: Estrato de No Acceso (también conocido como el protocolo de red principal)
MME: Entidad de Gestión de Movilidad
LTE: Evolución a Largo Plazo, un término usado en 3GPP para el sistema que se está estandarizando después de UMTS
IE: Elemento de Información
RRC: Control de Recursos de Radio (la parte de radio del protocolo de control denominada de otra manera parte de Estrato de Acceso del protocolo de control).
SGSN: Nodo de Soporte de Pasarela de Señalización.

REIVINDICACIONES

1. Un procedimiento de transmisión de datos (40) de usuario encriptados a un terminal (28) móvil en una red (14) de telecomunicaciones inalámbrica, comprendiendo el procedimiento enviar al terminal móvil un paquete (32, 48) de datos, comprendiendo el paquete de datos tanto un identificador (38, 50) de información de encriptación para ser usado al recuperar datos de usuario encriptados, como datos (40,52) de usuario encriptados usando dicha información de encriptación, en el que
en respuesta a la recepción del paquete de datos el terminal móvil inicializa (70) su contexto de seguridad usando la información de encriptación identificada, y
la red comprende una red de UMTS o de LTE.

2. Un procedimiento de acuerdo con la reivindicación 1, en el que la información de encriptación comprende un algoritmo de encriptación.

3. Un procedimiento de acuerdo con la reivindicación 1 o la reivindicación 2, en el que la información de encriptación comprende una clave de encriptación.

4. Un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que los datos de usuario comprenden datos de señalización de usuario.

5. Un procedimiento de acuerdo con la reivindicación 4, en el que los datos de señalización de usuario comprenden un mensaje de NAS o mensaje de RRC.

6. Un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que los datos de usuario comprenden datos de tráfico de usuario.

7. Un procedimiento de acuerdo con cualquier reivindicación anterior, que comprende además la etapa de usar el terminal (28) móvil la información de encriptación identificada para recuperar los datos de usuario.

8. Un procedimiento de acuerdo con la reivindicación 7, que comprende además almacenar el terminal (28) móvil la información de encriptación identificada para su uso al recuperar datos de usuario encriptados en un paquete de datos recibido posteriormente.

9. Un procedimiento de acuerdo con la reivindicación 1, en el que el paquete de datos comprende un comando (38) de modo de seguridad, comprendiendo el comando de modo de seguridad el identificador de la información de encriptación.

10. Una estación (20, 64) base de telecomunicaciones inalámbricas de UMTS o LTE configurada para transmitir datos de usuario encriptados en un paquete (32, 48) de datos, comprendiendo el paquete de datos tanto un identificador (38, 50) de nueva información de encriptación, estando adaptada dicha nueva información de encriptación para ser usada en en un receptor para recuperar datos de usuario encriptados, como datos (40, 52) de usuario encriptados usando dicha nueva información de encriptación.

11. Una estación base de telecomunicaciones inalámbricas de UMTS o LTE de acuerdo con la reivindicación 10, configurada, después de la transmisión de datos de usuario encriptados usando información de encriptación antigua, para transmitir dichos datos de usuario encriptados en dicho paquete (32, 48) de datos.

12. Un terminal (28) de telecomunicaciones inalámbricas que comprende un receptor y un procesador,
estando configurado el receptor para recibir un paquete (32, 48) de datos, comprendiendo el paquete de datos tanto un identificador (38, 50) de información de encriptación para ser usado al recuperar datos de usuario encriptados, como datos (40, 52) de usuario encriptados usando dicha información de encriptación, en el que
en respuesta a la recepción del paquete de datos el terminal (28) móvil inicializa su contexto de seguridad usando la información de encriptación identificada, y
el procesador está configurado para usar dicha información de encriptación para recuperar los datos de usuario encriptados usando dicha información de encriptación, estando configurado el terminal móvil para almacenar dicha información de encriptación para uso posterior, y
el terminal es un terminal de telecomunicaciones inalámbricas de UMTS o LTE.

13. Un terminal de telecomunicaciones inalámbricas de acuerdo con la reivindicación 12, en el que
el paquete de datos comprende un comando (38) de modo de seguridad, comprendiendo el comando de modo de seguridad el identificador de información de encriptación.

14. Un procedimiento de un terminal (28) móvil en una red de telecomunicaciones inalámbrica que recibe datos de usuario encriptados, comprendiendo el procedimiento:

que el terminal móvil reciba un primer paquete de datos, comprendiendo el primer paquete de datos datos de usuario encriptados usando primera información de encriptación;
recuperar los datos de usuario en el terminal móvil usando primera información de encriptación almacenada en el terminal móvil;

recibir el terminal móvil un siguiente paquete (32, 48) de datos, comprendiendo el paquete de datos tanto un identificador (38, 50) de información de encriptación actualizada para ser usado al recuperar datos de usuario encriptados, como datos (40, 52) de usuario encriptados usando dicha información de encriptación actualizada, en el que

en respuesta a la recepción de dicho siguiente paquete de datos el terminal móvil inicializa su contexto de seguridad usando la información de encriptación actualizada identificada;

usar el terminal móvil dicha información de encriptación para recuperar los datos de usuario encriptados usando dicha información de encriptación actualizada y almacenar dicha información de encriptación actualizada para posterior uso al desencriptar paquetes posteriores.

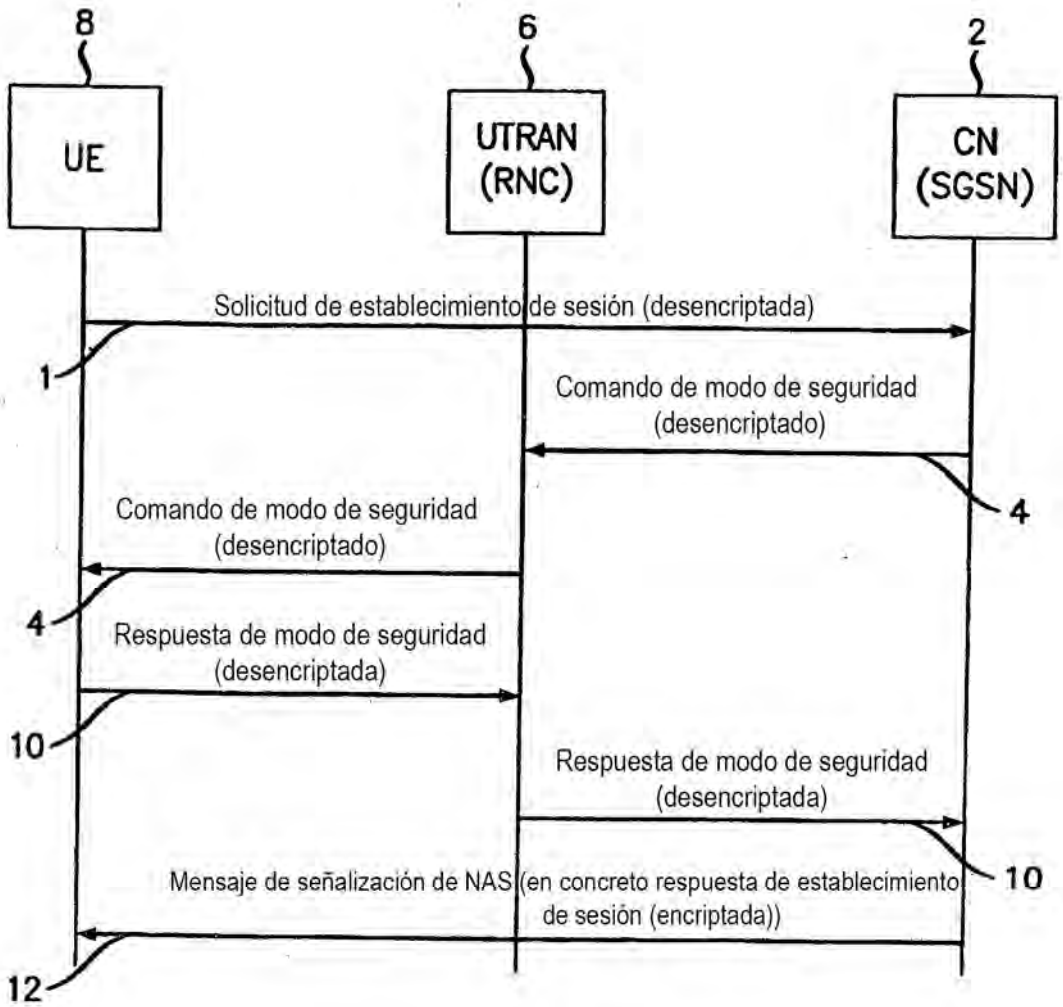

FIG. 1

TÉCNICA ANTERIOR

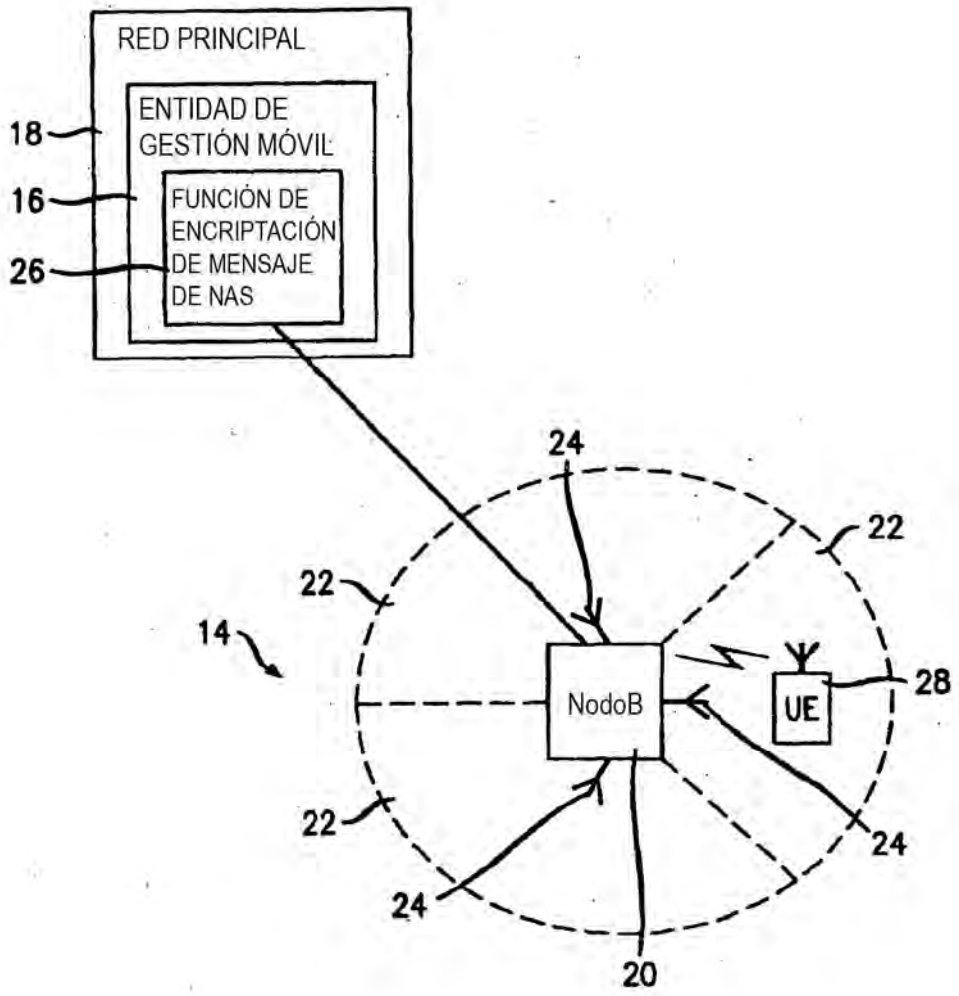
RED PRINCIPAL
ENTIDAD DE GESTIÓN MÓVIL
FUNCIÓN DE ENCRIPTACIÓN DE MENSAJE DE NAS
18
16
26
24
22
22
14
NodoB
UE
28
22
24
24
20

FIG. 2

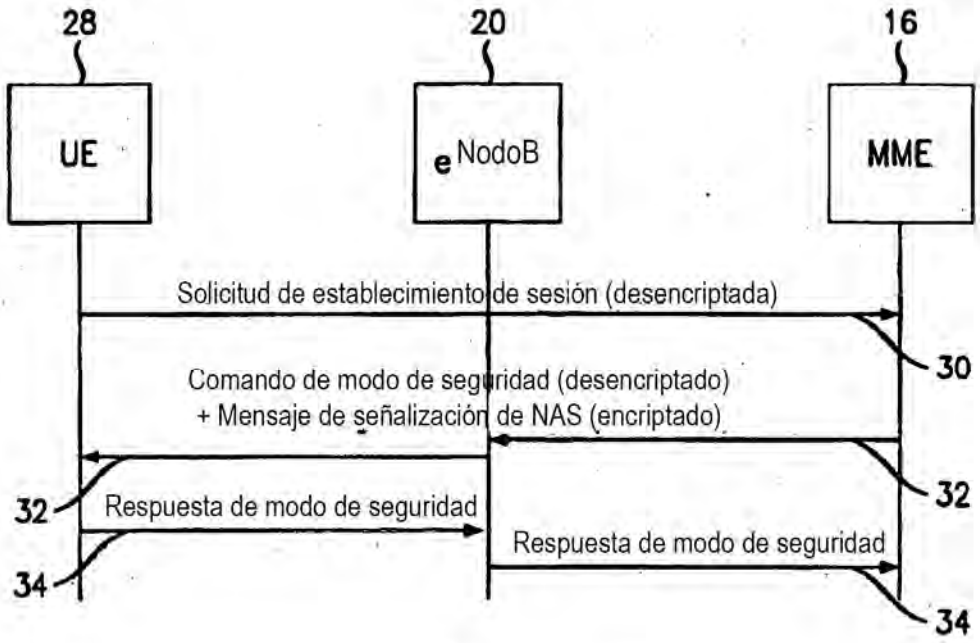
28
20
16
UE
eNodoB
MME
Solicitud de establecimiento de sesión (desencriptada)
30
Comando de modo de seguridad (desencriptado)
+ Mensaje de señalización de NAS (encriptado)
32
32
Respuesta de modo de seguridad
Respuesta de modo de seguridad
34
34

FIG. 3

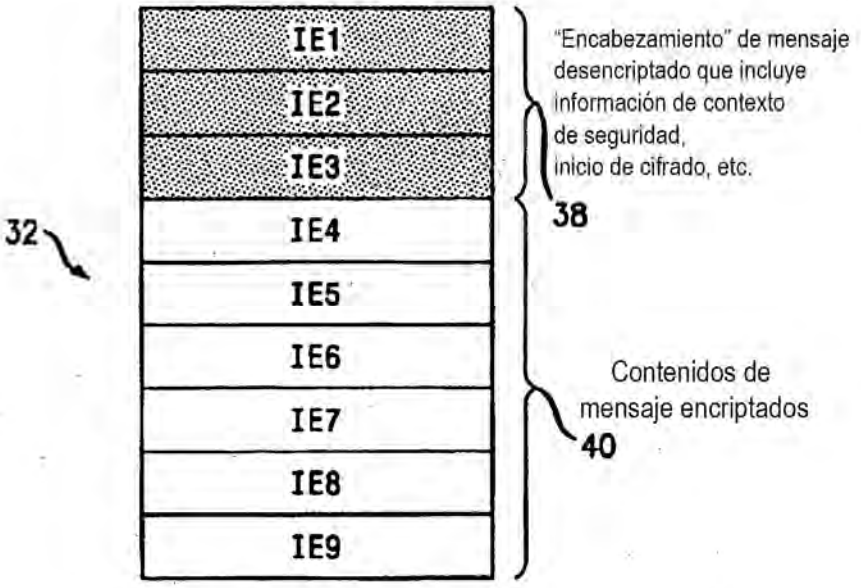
IE1
IE2
IE3
IE4
IE5
IE6
IE7
IE8
IE9
32
"Encabezamiento" de mensaje desencriptado que incluye información de contexto de seguridad, inicio de cifrado, etc.
38
Contenidos de mensaje encriptados
40

FIG. 4

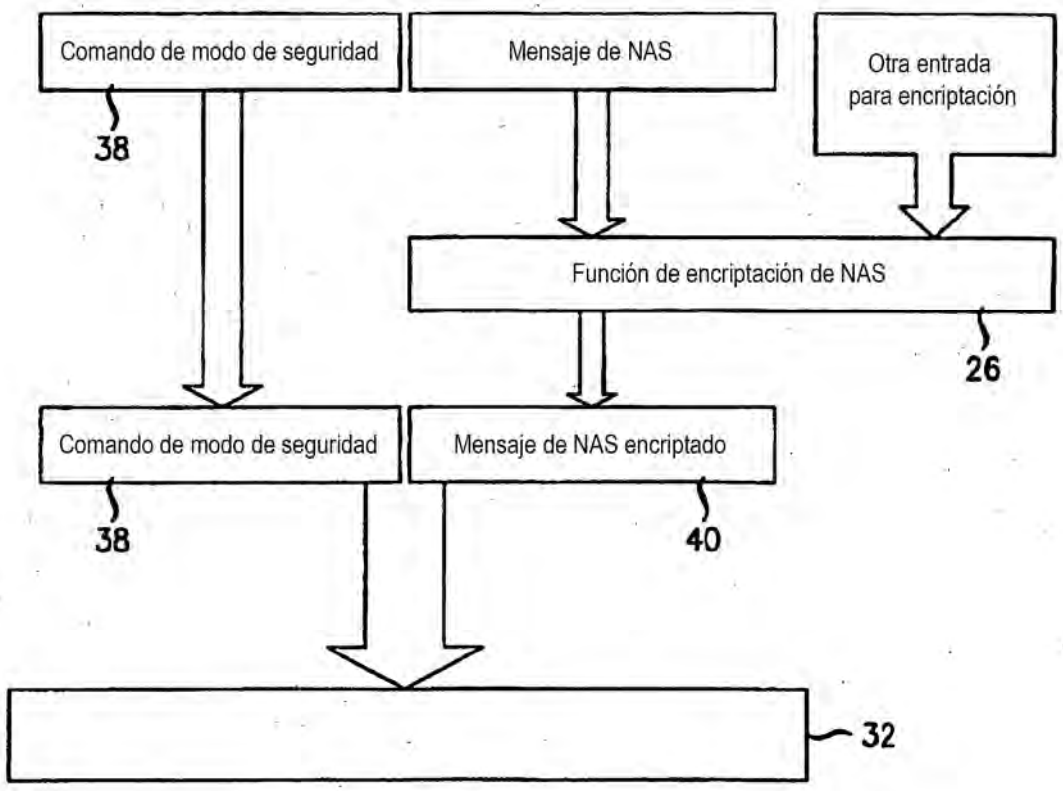
Comando de modo de seguridad
Mensaje de NAS
Otra entrada para encriptación
38
Función de encriptación de NAS
26
Comando de modo de seguridad
Mensaje de NAS encriptado
38
40
32

FIG. 5

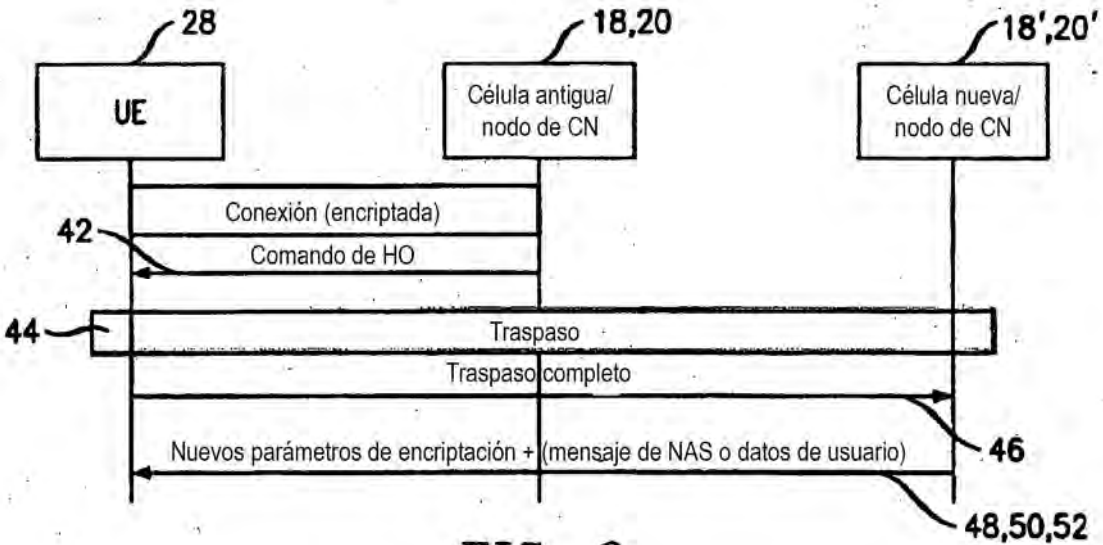
28
18,20
18',20'
UE
Célula antigua/ nodo de CN
Célula nueva/ nodo de CN
Conexión (encriptada)
42
Comando de HO
44
Traspaso
Traspaso completo
46
Nuevos parámetros de encriptación + (mensaje de NAS o datos de usuario)
48,50,52

FIG. 6

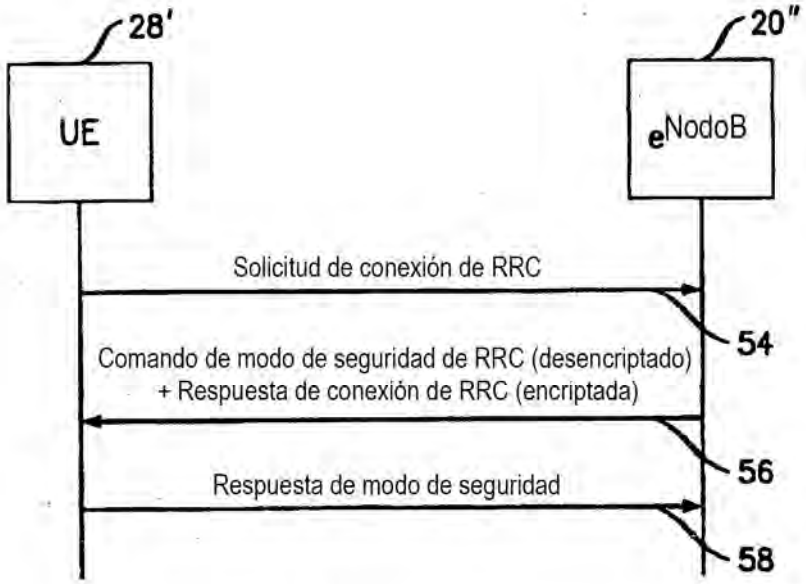
28'
UE
20"
eNodoB
Solicitud de conexión de RRC
54
Comando de modo de seguridad de RRC (desencriptado)
+ Respuesta de conexión de RRC (encriptada)
56
Respuesta de modo de seguridad
58

FIG. 7

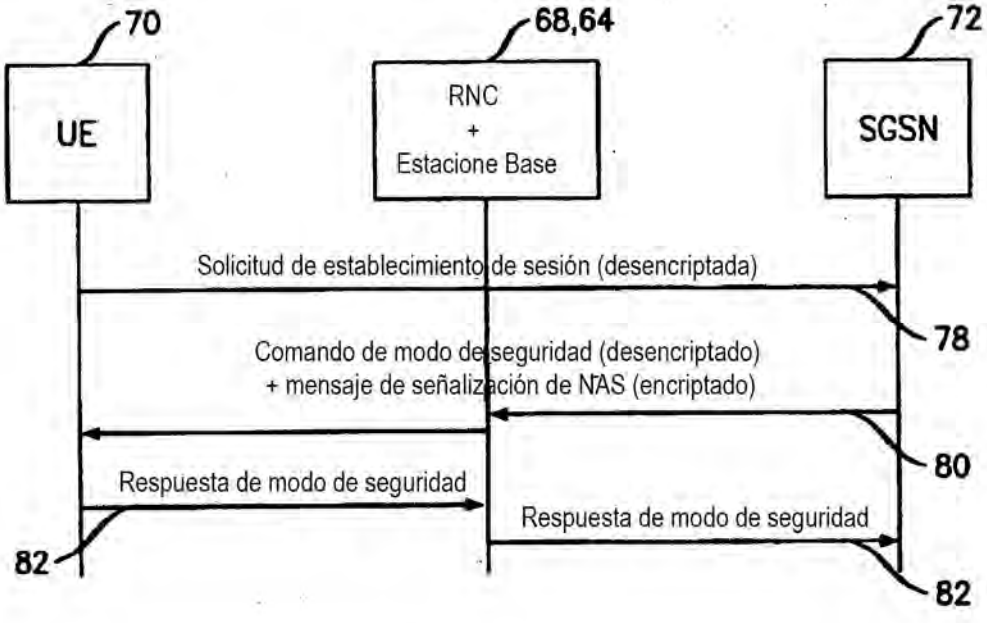
70
UE
68,64
RNC
+
Estacione Base
72
SGSN
Solicitud de establecimiento de sesión (desencriptada)
78
Comando de modo de seguridad (desencriptado)
+ mensaje de señalización de NAS (encriptado)
80
Respuesta de modo de seguridad
Respuesta de modo de seguridad
82
82

FIG. 9

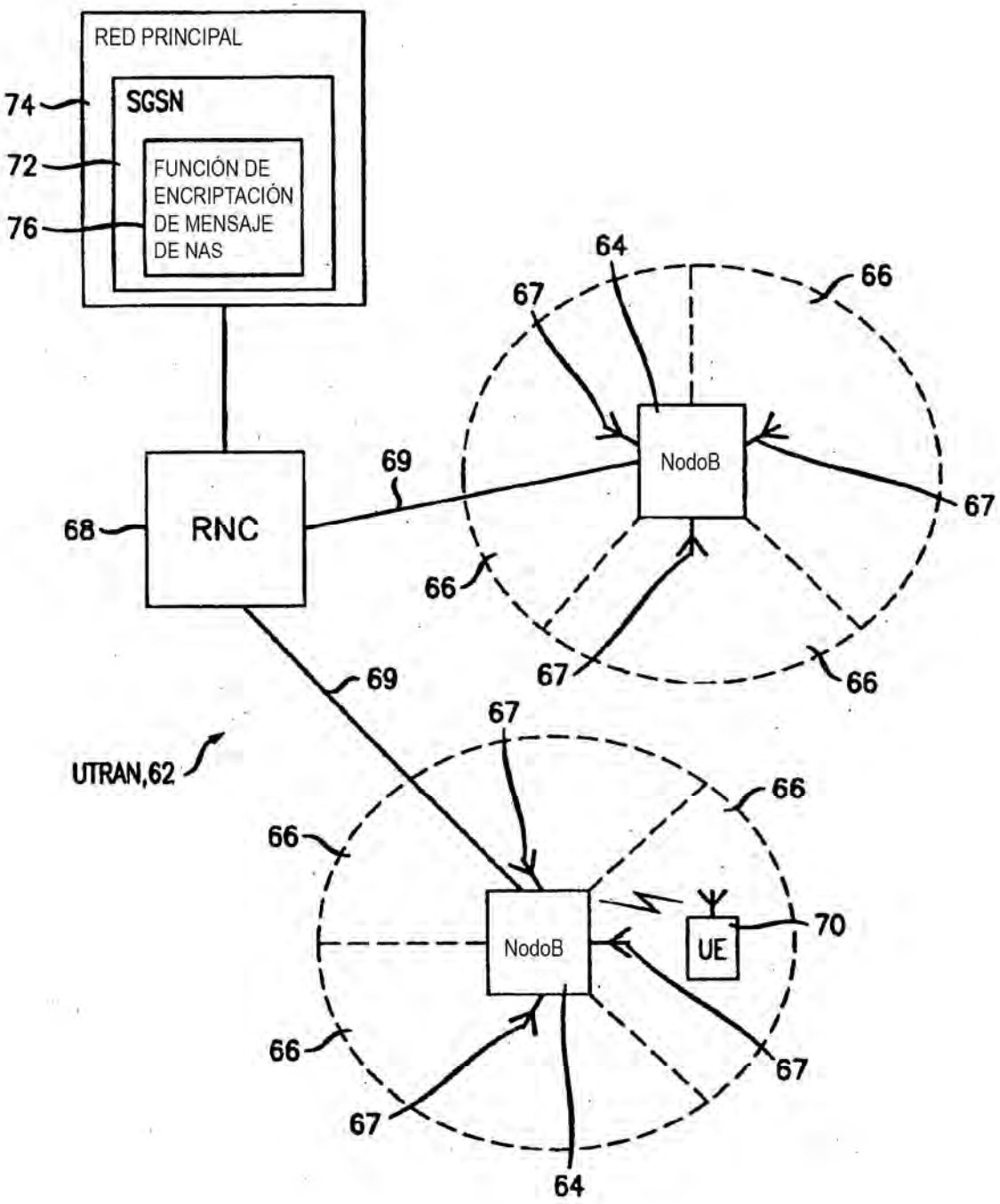
RED PRINCIPAL
SGSN
FUNCIÓN DE ENCRIPTACIÓN DE MENSAJE DE NAS
74
72
76
RNC
68
69
69
UTRAN,62
NodoB
NodoB
UE
64
66
67
70

FIG. 8