(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 913 538**

(51) Int. CI.:

H04W 12/80 (2011.01)
H04W 8/26 (2009.01)
H04W 12/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.05.2018 E 18173821 (2)**

(97) Fecha y número de publicación de la concesión europea: **23.03.2022 EP 3573304**

(54) Título: **Método y disposición de detección de identidad de abonado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2022

(73) Titular/es:

EXFO OY (100.0%)
Elektroniikkatie 2
90590 Oulu, FI

(72) Inventor/es:

AINALI, TIMO;
IKÄHEIMO, JORMA;
MÄKELÄ, TUURE y
NIIRANEN, TAISTO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y disposición de detección de identidad de abonado

Campo

La invención se refiere a un método y a una disposición que comprende una estación base falsa y una entidad dentro de una infraestructura de un sistema de telefonía móvil.

Antecedentes

Se usa una estación falsa para detectar una identidad de abonado. Este procedimiento se puede denominar captación de IMSI. Sin embargo, en los sistemas de telefonía móvil recientes, la identidad de abonado está cifrada, de modo que los métodos de detección tradicionales no funcionan.

Breve descripción

La presente invención busca proporcionar un método mejorado y una disposición mejorada.

De acuerdo con un aspecto de la presente invención, se proporciona un método como se especifica en la reivindicación 1.

De acuerdo con otro aspecto de la presente invención, se proporciona una disposición como se especifica en la reivindicación 8.

Lista de dibujos

A continuación se describen realizaciones ilustrativas de la presente invención, solo a modo de ejemplo, con referencia a los dibujos adjuntos, en los que

la figura 1 ilustra realizaciones ilustrativas de un método;
la figura 2 ilustra realizaciones ilustrativas de una disposición;
la figura 3 ilustra realizaciones ilustrativas en una arquitectura medular basada en servicios del sistema de telefonía móvil; y
la figura 4 ilustra realizaciones ilustrativas de un protocolo de comunicación.

Descripción de realizaciones

Las realizaciones siguientes son solo ejemplos. Aunque la memoria descriptiva puede hacer referencia a "una" realización en varias ubicaciones, esto no significa necesariamente que cada referencia de este tipo sea a la misma realización o realizaciones, o que la característica solo sea de aplicación a una única realización. También se pueden combinar características únicas de diferentes realizaciones para proporcionar otras realizaciones. Además, se debería entender que las expresiones "comprendiendo/que comprende" e "incluyendo/que incluye" no limitan las realizaciones descritas a consistir solo en aquellas características que se han mencionado y tales realizaciones también pueden contener características/estructuras que no se han mencionado específicamente.

Estúdiese en primer lugar la figura 1, que ilustra realizaciones ilustrativas de un método.

El método empieza en 100.

En 102, al menos un mensaje inalámbrico transmitido desde un aparato de abonado móvil interoperable con un sistema de telefonía móvil es capturado en una estación base falsa.

En 104, se detecta una identidad de abonado cifrada a partir del al menos un mensaje inalámbrico capturado.

En 106, se recupera una identidad de abonado no cifrada desde una entidad dentro de una infraestructura del sistema de telefonía móvil basándose en la identidad de abonado cifrada.

El método termina en 110 después de que se haya finalizado el procesamiento, o el método puede realizar un bucle 108 de vuelta a la operación 102 para recibir mensajes adicionales desde el mismo aparato de abonado móvil que antes, o desde algún otro aparato móvil.

Estúdiese a continuación la figura 2, que ilustra realizaciones ilustrativas de una disposición con la que se puede implementar el método.

La disposición comprende la estación base falsa 200 y la entidad 210 dentro de la infraestructura del sistema de

telefonía móvil 220.

La estación base falsa 200 comprende una o más unidades de procesamiento 204 y uno o más transceptores de radio 202. Estas partes 202, 204 están configuradas para implementar una comunicación y un procesamiento requeridos por el método. En consecuencia, las partes 202, 204 están configuradas para capturar 102 el al menos un mensaje inalámbrico 260 a partir del aparato de abonado móvil 250, para detectar 104 la identidad de abonado cifrada a partir del al menos un mensaje inalámbrico 260 capturado y para transmitir la identidad de abonado cifrada 262 a la entidad 210.

Los uno o más transceptores de radio 202 se pueden implementar con una tecnología de radio definida por software (SDR). Con la tecnología de SDR, los uno o más transceptores de radio 202 contienen las partes de radiofrecuencia requeridas (por ejemplo: una antena, un amplificador de ruido bajo, filtros de paso de banda, un convertidor de analógico a digital), pero al menos algunos de los componentes de hardware tradicionales, especialmente los usados para el procesamiento de señales digitales, se implementan con un software de interfaz de radio que se ejecuta en una unidad de procesamiento. Las una o más unidades de procesamiento 204 descritas pueden ejecutar el software de interfaz de radio o, como alternativa, puede haber procesadores dedicados (no ilustrados en la figura 1) acoplados con los uno o más transceptores de radio 204 para ejecutar el software de interfaz de radio.

Las una o más unidades de procesamiento 204 se pueden implementar con uno o más procesadores (tales como un microprocesador) y un código de programa informático (software), o como un circuito integrado específico de la aplicación (ASIC), o como cualquier otra forma de implementar un dispositivo que es capaz de procesar datos.

La entidad 210 comprende una o más unidades de procesamiento 214 y una o más interfaces de comunicación 212. Estas partes 212, 214 están configuradas para implementar una comunicación y un procesamiento requeridos por el método. En consecuencia, las partes 212, 214 están configuradas para recibir la identidad de abonado cifrada 262 desde la estación base falsa 200, para recuperar 106 la identidad de abonado no cifrada 266 desde un elemento de red 230 del sistema de telefonía móvil 220 basándose en la identidad de abonado cifrada 264, y para transmitir la identidad de abonado no cifrada 268 a la estación base falsa 200.

La entidad 210 se puede implementar como un aparato de servidor en red. La estación base falsa 200 y el aparato de servidor en red 210 pueden operar de acuerdo con una arquitectura de cliente-servidor, una arquitectura de computación en la nube, un sistema de igual a igual u otra arquitectura de computación aplicable. Las una o más interfaces de comunicación 212 se pueden implementar con protocolos normalizados/de propiedad exclusiva y tecnologías de comunicación cableadas/inalámbricas apropiadas.

La estación base falsa 200 también se puede denominar estación base falsa o aparato de control autónomo fuera del sistema de telefonía móvil 220. 'Falsa' se refiere al hecho de que la estación base falsa 200 no es parte del sistema de telefonía móvil (real) 220 y no proporciona un servicio continuo para los aparatos de abonado móvil 250 y sus usuarios. El fin de la estación base falsa 200 es realizar funciones de interfaz de radio requeridas para descubrir la identidad de abonado asociada con el aparato de abonado móvil 250. La figura 2 también ilustra que el aparato de abonado móvil 250 es interoperable con el sistema de telefonía móvil real 220, es decir, el aparato de abonado móvil 250 podría conseguir el servicio 280 a partir del sistema de telefonía móvil real 220 (pero la estación base falsa 200 invalida esto, al menos momentáneamente, de tal modo que se pueden capturar 102 uno o mensajes).

Debido a que la identidad de abonado está cifrada, la estación base falsa 200 por sí sola no puede descubrir su identidad real. Por lo tanto, se requiere ayuda del sistema de telefonía móvil 220. Pero, debido a que el sistema de telefonía móvil 220 está protegido fuertemente, se requiere una interfaz adecuada. Se permite que la entidad 210 opere dentro de la infraestructura del sistema de telefonía móvil 220, de modo que esta puede acceder al elemento de red 230 del sistema de telefonía móvil 220.

Naturalmente, la entidad 210 también está protegida fuertemente: la estación base falsa 200 solo puede acceder a la entidad 210 a través de un sistema de control de acceso (con un identificador de usuario, una contraseña y un túnel de comunicación con un cifrado fuerte, por ejemplo).

La identidad de abonado puede estar vinculada a un módulo de identidad de abonado (SIM), que puede ser un circuito integrado colocado en un lector del aparato de abonado móvil 250, o puede ser una SIM integrada, o incluso se prevé una SIM de software.

En una realización ilustrativa, la identidad de abonado cifrada 262, 264 comprende un Identificador Ocultado de Abono (a veces conocido como SUCI).

En una realización ilustrativa, la identidad de abonado no cifrada 266, 268 comprende un Identificador permanente de abono (a veces conocido como SUPI).

En una realización ilustrativa, la identidad de abonado cifrada se ha cifrado con una criptografía de clave pública, también conocida como criptografía asimétrica, que usa un par de claves: una clave pública 252, que es conocida por

el aparato de abonado móvil 250, y una clave privada 232, que solo es conocida por el elemento de red 230.

El al menos un mensaje inalámbrico, que se transmite desde el aparato de abonado móvil y es capturado por la estación base falsa 200, contiene la identidad de abonado cifrada con la clave pública 252. Solo el titular de la clave privada emparejada, es decir, el elemento de red 230, es capaz de descifrar la identidad de abonado cifrada con la clave privada 232.

En consecuencia, la estación base falsa 200, ayudada por la entidad 210, está configurada para comunicarse con el elemento de sistema 230 del sistema de telefonía móvil 220 que posee la clave privada 232 de la criptografía de clave pública para descifrar la identidad de abonado cifrada 264.

En una realización ilustrativa, la identidad de abonado cifrada se obtiene 102 a partir de los uno o mensajes (Solicitud de registro, aceptación, Solicitud de anulación de registro, Solicitud de servicio, Orden de actualización de configuración, Respuesta de identidad), que pueden ser conformes con la norma de 3GPP TS de 3GPP 24.501 (Proyecto de Asociación de 3ª Generación; *Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS)*),

En algunos casos, la estación base falsa 200 está configurada para recibir, en primer lugar, uno o más mensajes 260 desde el aparato de abonado móvil 250, que contienen GUTI de 5G (Identidad Temporal Única Global de 5G) o su versión abreviada TMSI-S de 5G (Identidad de Abonado Móvil Temporal-S de 5G). Pero, debido a que esta es una identidad temporal, se requieren operaciones adicionales. En consecuencia, la estación base falsa 200 está configurada para responder con una Solicitud de Identidad (SUCI), que hace que el aparato de abonado móvil 250 responda 260 con una Respuesta de identidad (SUCI), que contiene la Identidad Ocultada de Abonado (SUCI). Después de que la identidad se haya resuelto como Identidad Permanente de Abonado (SUPI) como se describe, la estación base falsa 200 está configurada para responder 260 con una respuesta adecuada que no requiere una protección de integridad (véase 4.4.4.2, *Integrity checking of NAS signalling messages in the UE* - Comprobación de integridad de mensajes de señalización de NAS en el UE - de TS de 3GPP 24.501), con un Rechazo de registro con un código de causa adecuado como se explica en 5.5.1.2.5 *Initial registration not accepted by the network* (Registro inicial no aceptado por la red) de TS de 3GPP 24.501, por ejemplo. Obsérvese que la Solicitud de identidad (SUCI) se puede enviar sin la protección de integridad (4.4.4.2 *Integrity checking* - Comprobación de integridad - de TS de 3GPP 24.501), por lo que la identidad se puede solicitar para cada operación.

En una realización ilustrativa ilustrada en la figura 3, el elemento de red 230, 318 pertenece a una arquitectura medular basada en servicios del sistema de telefonía móvil 220.

La figura 3 ilustra una red de acceso (AN) (de radio) 300, una función de plano de usuario (UPF) 302 y una red de datos (DN) 304 y también las interfaces N1, N2, N3, N4 y N6.

En la arquitectura basada en servicios, cada función de red (NF) ofrece una interfaz basada en servicios (SBI):

- Función de servidor de autenticación (AUSF) 306 con una interfaz Nausf;
- Función de gestión de acceso y de movilidad (AMF) 308 con una interfaz Namf;
- Función de gestión de sesión (SMF) 310 con una interfaz Nsmf;
- Función de exposición de red (NEF) 312 con una interfaz Nnef;
- Función de repositorio de red (NRF) 314 con una interfaz Nnrf;
- Función de control de política (PCF) 316 con una interfaz Npcf;
- Función de gestión de datos unificada (UDM) 318 con una interfaz Nudm; y
- Función de aplicación (AF) 320 con una interfaz Naf.

Como se muestra en la figura 3, la función de UDM 318 puede ofrecer el servicio requerido como el elemento de red 230 a través de la interfaz Nudm, que se puede acoplar comunicativamente con la entidad 210. La figura 3 ilustra la cadena de comunicación 262, 264, 266, 268 entre la estación base falsa 200, la entidad 210 y el elemento de red 230, 318.

En una realización ilustrativa, la función de UDM 318 implementa una desocultación de identidad de abonado de UDM con la que se obtiene la identidad de abonado no cifrada basándose en la identidad de abonado cifrada como se describe en las normas de 3GPP TS de 3GPP 29.500 (Proyecto de Asociación de 3ª generación; *Technical Specification Group Core Network and Terminals; 5G System; Technical Realization of Service Based Architecture*) y TS de 3GPP 33.501 (Proyecto de Asociación de 3ª Generación; *Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system*, véase especialmente el capítulo 6.1.3 *Authentication procedures of 3GPP TS 33.501 for UDM subscriber identity deconcealing* (Procedimientos de autenticación de TS de 3GPP 33.501 para desocultación de identidad de abonado de UDM).

En una realización ilustrativa ilustrada en la figura 4, el protocolo de comunicación entre la entidad 210 y el elemento de red 230, 318 se puede implementar como sigue:

- la capa física/de enlace/de interfaz de red 400 se implementa según se requiera (de forma cableada o inalámbrica);
- se adopta HTTP/2 (Protocolo de Transferencia de Hipertexto) 412 como el protocolo de capa de aplicación para la interfaz basada en servicios;
- se adopta TCP (Protocolo de Control de Transmisión) 408 como el protocolo de capa de transporte 404;
- se adopta TLS (Seguridad de Capa de Transporte) 406 como el protocolo de privacidad y de integridad de datos;
- se adopta IP (Protocolo de Internet) 402 como el protocolo de capa de red;
- el uso de QUIC (Conexiones de Internet de UDP Rápidas) 410, codificación binaria (Representación de Objetos Binarios Concisa, CBOR, por ejemplo) se puede implementar según se requiera;
- se adopta JSON (Notación de Objetos de JavaScript) 414 como el protocolo de serialización; y
- diseño de servicios de estilo REST (Transferencia de Estado Representacional) siempre que sea posible y, en caso contrario, métodos personalizados (de Llamada a Procedimiento Remoto, basados en RPC).

En una realización ilustrativa, el sistema de telefonía móvil 220 comprende un sistema inalámbrico de quinta generación (5G), aunque las realizaciones ilustrativas no se limitan a un sistema de este tipo, sino que también son aplicables con otros sistemas inalámbricos que posean características similares para la protección de la identidad de abonado.

Será evidente para un experto en la materia que, a medida que la tecnología avanza, el concepto inventivo se puede implementar de diversas formas. La invención y sus realizaciones no están limitadas a las realizaciones ilustrativas descritas anteriormente, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método que comprende:
capturar (102) en una estación base falsa (200) al menos un mensaje inalámbrico transmitido desde un aparato de abonado móvil (250) interoperable con un sistema de telefonía móvil (220), en donde el sistema de telefonía móvil (220) proporciona un servicio continuo para aparatos de abonado móvil;
detectar (104) a partir del al menos un mensaje inalámbrico capturado, por la estación base falsa (200), una identidad de abonado cifrada, SUCI, (262) asociada con el aparato de abonado móvil (250) y cifrada con una clave pública (252), en donde la estación base falsa (200) no es parte del sistema de telefonía móvil (220), y en donde la estación base falsa (200) invalida el servicio continuo (280) desde el sistema de telefonía móvil (220) con el fin de capturar el al menos un mensaje inalámbrico; y
recuperar (106), por la estación base falsa (200), a través de un sistema de control de acceso, una identidad de abonado no cifrada, SUPI, (268) desde una entidad (210) dentro de una infraestructura del sistema de telefonía móvil (220) basándose en la identidad de abonado cifrada (262), en donde se permite que la entidad (210) opere dentro de la infraestructura del sistema de telefonía móvil (220), y la entidad (210) accede a un elemento de red (230) del sistema de telefonía móvil (220) con la identidad de abonado cifrada (264), el elemento de red (230) descifra la identidad de abonado cifrada (264) con una clave privada (232) emparejada con la clave pública (252) y conocida solo por el elemento de red (230) para obtener una identidad de abonado no cifrada (266), el elemento de red (230) devuelve la identidad de abonado no cifrada (266) a la entidad (210), y la entidad (210) transmite la identidad de abonado no cifrada (268) a la estación base falsa (200).

2. El método de la reivindicación 1, en donde la identidad de abonado cifrada (262, 264) se ha cifrado con una criptografía de clave pública.

3. El método de la reivindicación 2, en donde la entidad (210) se comunica con el elemento de red (230) del sistema de telefonía móvil (220) que posee la clave privada (232) de la criptografía de clave pública para descifrar la identidad de abonado cifrada (264).

4. El método de la reivindicación 3, en donde el elemento de red (230) pertenece a una arquitectura medular basada en servicios del sistema de telefonía móvil (220).

5. El método de cualquier reivindicación anterior, en donde la identidad de abonado cifrada (262, 264) comprende un Identificador Ocultado de Abono.

6. El método de cualquier reivindicación anterior, en donde la identidad de abonado no cifrada (266, 268) comprende un Identificador Permanente de Abono.

7. El método de cualquier reivindicación anterior, en donde el sistema de telefonía móvil (220) comprende un sistema inalámbrico de quinta generación.

8. Una disposición que comprende una estación base falsa (200) y una entidad (210) dentro de una infraestructura de un sistema de telefonía móvil (220), en donde:
la estación base falsa (200) comprende una o más unidades de procesamiento (204) y uno o más transceptores de radio (202) configurados para capturar al menos un mensaje inalámbrico (260) desde un aparato de abonado móvil (250) interoperable con el sistema de telefonía móvil (220), en donde el sistema de telefonía móvil (220) proporciona un servicio continuo para aparatos de abonado móvil, para detectar a partir del al menos un mensaje inalámbrico (260) capturado una identidad de abonado cifrada, SUCI, (262) asociada con el aparato de abonado móvil (250) y cifrada con una clave pública (252), en donde la estación base falsa (200) no es parte del sistema de telefonía móvil (220), y en donde la estación base falsa (200) invalida el servicio continuo (280) desde el sistema de telefonía móvil (220) con el fin de capturar el al menos un mensaje inalámbrico, y para transmitir la identidad de abonado cifrada (262) a la entidad (210) a través de un sistema de control de acceso; y
la entidad (210) comprende una o más unidades de procesamiento (214) y una o más interfaces de comunicación (212) configuradas para recibir la identidad de abonado cifrada (262) desde la estación base falsa (200), para recuperar una identidad de abonado no cifrada, SUPI, (266) desde un elemento de red (230) del sistema de telefonía móvil (220) basándose en la identidad de abonado cifrada (264), en donde se permite que la entidad (210) opere dentro de la infraestructura del sistema de telefonía móvil (220), y la entidad (210) accede al elemento de red (230) del sistema de telefonía móvil (220) con la identidad de abonado cifrada (264), el elemento de red (230) descifra la identidad de abonado cifrada (264) con una clave privada (232) emparejada con la clave pública (252) y conocida solo por el elemento de red (230) para obtener una identidad de abonado no cifrada (266), y el elemento de red (230) devuelve la identidad de abonado no cifrada (266) a la entidad (210), y para transmitir la identidad de abonado no cifrada (268) a la estación base falsa (200).

9. La disposición de la reivindicación 8, en donde la identidad de abonado cifrada (262, 264) se ha cifrado con una criptografía de clave pública.

10. La disposición de la reivindicación 9, en donde la entidad (210) está configurada para comunicarse con el elemento

de red (230) del sistema de telefonía móvil (220) que posee la clave privada (232) de la criptografía de clave pública para descifrar la identidad de abonado cifrada (264).

11. La disposición de la reivindicación 10, en donde el elemento de red (230, 318) pertenece a una arquitectura medular basada en servicios del sistema de telefonía móvil (220).

12. La disposición de cualquier reivindicación anterior 8-11, en donde la identidad de abonado cifrada (262, 264) comprende un Identificador Ocultado de Abono.

13. La disposición de cualquier reivindicación anterior 8-12, en donde la identidad de abonado no cifrada (266, 268) comprende un Identificador Permanente de Abono.

14. La disposición de cualquier reivindicación anterior 8-13, en donde el sistema de telefonía móvil (220) comprende un sistema inalámbrico de quinta generación.

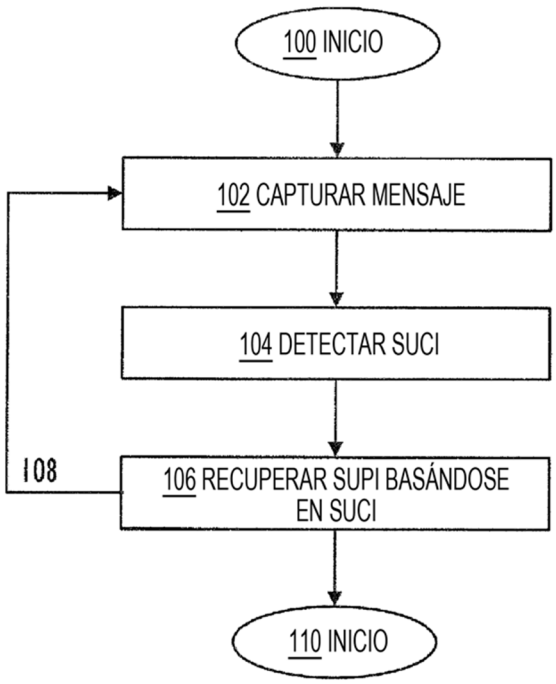
100 INICIO
102 CAPTURAR MENSAJE
104 DETECTAR SUCI
108
106 RECUPERAR SUPI BASÁNDOSE EN SUCI
110 INICIO

FIG. 1

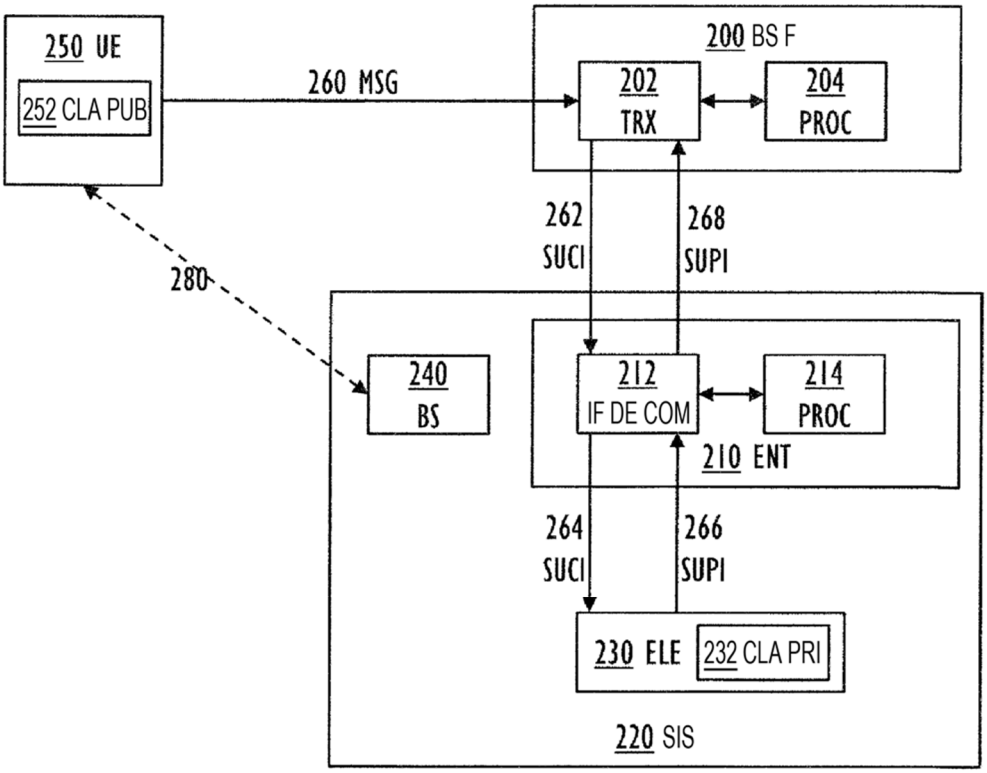
250 UE
252 CLA PUB
260 MSG
200 BS F
202 TRX
204 PROC
262 SUCI
268 SUPI
280
240 BS
212 IF DE COM
214 PROC
210 ENT
264 SUCI
266 SUPI
230 ELE
232 CLA PRI
220 SIS

FIG. 2

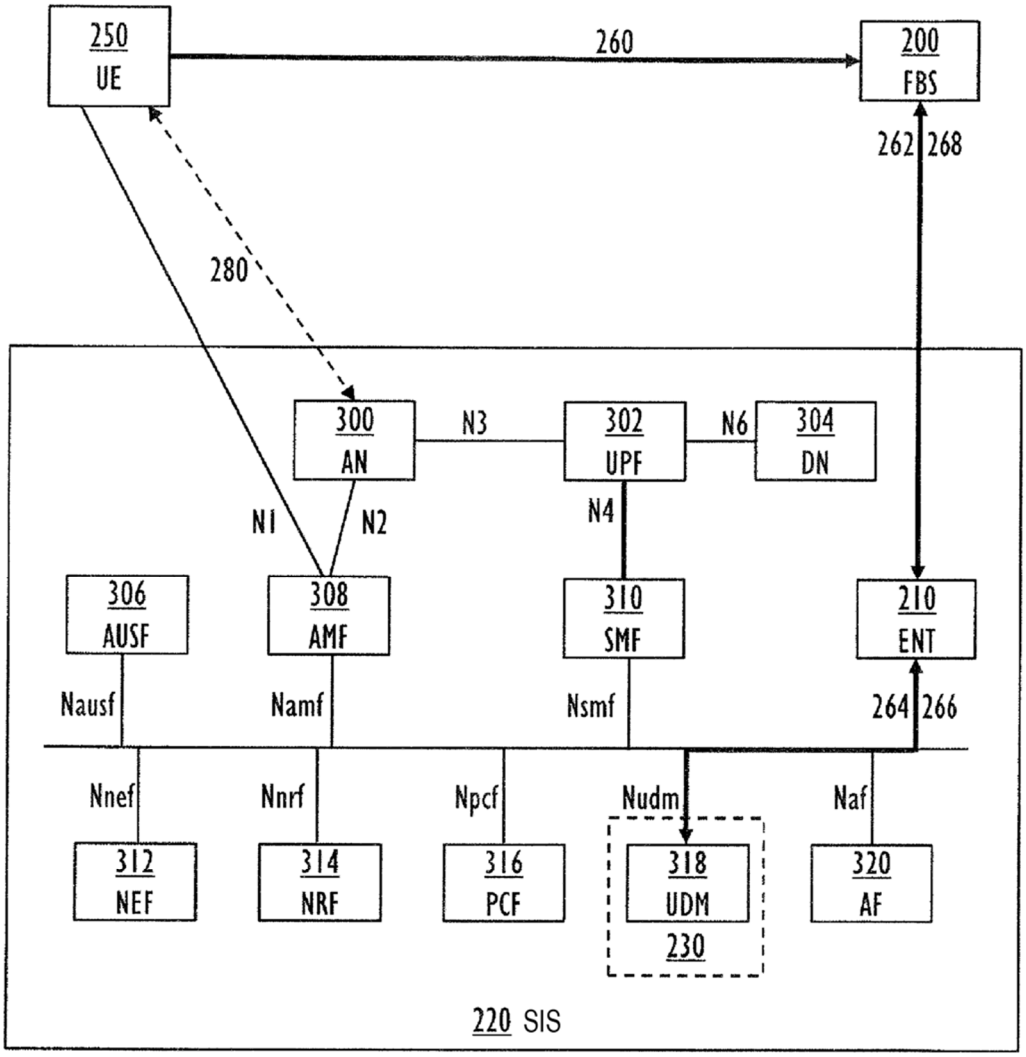
250
UE
260
200
FBS
262
268
280
300
AN
N3
302
UPF
N6
304
DN
N1
N2
N4
306
AUSF
308
AMF
310
SMF
210
ENT
Nausf
Namf
Nsmf
264
266
Nnef
Nnrf
Npcf
Nudm
Naf
312
NEF
314
NRF
316
PCF
318
UDM
230
320
AF
220 SIS

FIG. 3

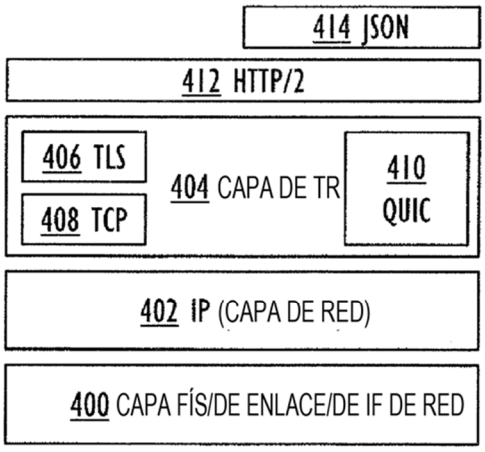
414 JSON
412 HTTP/2
406 TLS
408 TCP
404 CAPA DE TR
410
QUIC
402 IP (CAPA DE RED)
400 CAPA FÍS/DE ENLACE/DE IF DE RED

FIG. 4