(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 659 387**

(51) Int. CI.:

H04W 12/10 (2009.01)
H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/12 (2009.01)
H04W 76/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.10.2001 PCT/FI2001/00870**

(87) Fecha y número de publicación internacional: **06.06.2002 WO02045453**

(96) Fecha de presentación y número de la solicitud europea: **09.10.2001 E 01976329 (1)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2017 EP 1338164**

(54) Título: **Un sistema para asegurar la comunicación encriptada después de traspaso**

(30) Prioridad:

28.11.2000 FI 20002613
14.02.2001 FI 20010282

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.03.2018

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

VIALEN, JUKKA y
NIEMI, VALTTERI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Un sistema para asegurar la comunicación encriptada después de traspaso

Campo de la invención

La presente invención se refiere en general a una protección de integridad en una red de telecomunicaciones.

Antecedentes de la invención

Un sistema de comunicaciones móviles de la tercera generación se denomina en Europa UMTS (Sistema de Telecomunicaciones Móviles Universal). Es una parte del sistema IMT-200 de la Unión Internacional de las Telecomunicaciones. UMTS/IMT-2000 es el sistema multimedia inalámbrico global que proporciona velocidad de transmisión más alta (2 Mbit/s) que las redes móviles existentes.

La Figura **1** muestra con un diagrama de bloques simplificado una red de GSM (Sistema Global para Comunicaciones Móviles) y una red de UMTS. Las partes principales de la red son los terminales de usuario **100** y una parte red que comprende el subsistema de estación base BSS de GSM **105** y la red de acceso de radio terrestre UTRAN de UMTS **101** (que es una red de radio de acceso múltiple de banda ancha que se está especificando actualmente en el 3GPP (Proyecto Común de Tecnologías Inalámbricas de la Tercera Generación)) y una red principal CN **104**. La interfaz de radio entre un terminal de usuario y la UTRAN se denomina Uu y la interfaz entre la UTRAN y la red principal de 3G se denomina *Iu*. La interfaz entre el subsistema de estación base BSS de GSM y la red principal del servicio general de paquetes de radio GPRS se denomina Gb y la interfaz entre el subsistema de estación base BSS de GSM y las redes principales de GSM se denomina A. Los terminales de usuario pueden ser terminales multi-modo, que pueden operar usando al menos dos tecnologías de acceso de radio, en este ejemplo UMTS y GSM. La UTRAN consiste en unos subsistemas de red de radio RNS **102** que consisten adicionalmente en el controlador de red de radio RNC **103** y uno o más nodos B (no mostrados en la Figura 1). Una interfaz entre dos RNS se denomina Iur. La interfaz entre el terminal de usuario y el subsistema de estación base BSS de GSM se denomina simplemente "Interfaz de radio". El subsistema de estación base BSS de GSM consiste en los controladores de estación base BSC **106** y las estaciones base transceptoras BTS **107**. Los nodos de red principal, por ejemplo el Centro de Conmutación Móvil MSC (GSM) y el nodo de soporte de servidor SGSN (GPRS), pueden controlar ambos tipos de redes de acceso de radio - UTRAN y BSS. Otra posible configuración de red es de manera que cada red de acceso de radio (UTRAN y BSS) tiene su propio nodo de red principal de control, MSC y SGSN, respectivamente - 2G MSC, 2G SGSN y 3G MSC, 3G SGSN - pero todos estos elementos de red principales están conectados a uno y el mismo registro de localización doméstico HLR (no mostrado en la Figura 1), que contiene toda la información estática de usuario, por ejemplo la facturación de los usuarios puede controlarse desde una localización incluso cuando los terminales de usuario pueden operar mediante varias diferentes redes de acceso de radio.

Los protocolos de interfaz de radio que son necesarios para establecer, reconfigurar y liberar los servicios de operadora de radio se analizan brevemente a continuación. La arquitectura de protocolo de interfaz de radio en el estrato de acceso consiste en tres diferentes capas de protocolo que son desde la parte superior a la parte inferior: la capa de red de radio (L3), la capa de enlace de datos (L2), y la capa física (L1). Las entidades de protocolo en estas capas son las siguientes. La capa de red de radio consiste en únicamente un protocolo, que en la interfaz de radio de UMTS se denomina RRC (Control de Recurso de Radio) y en la interfaz de radio 2G de GSM se denomina RR (protocolo de Recursos de Radio). La capa de enlace de datos consiste en varios protocolos en la interfaz de radio de UMTS denominados PDCP (Protocolo de Convergencia de Datos de Paquetes), BMC (protocolo de Control de Multidifusión de Difusión), RLC (protocolo de Control de Enlace de Radio), y MAC (protocolo de Control de Acceso al Medio). En la interfaz de radio de GSM/GPRS, los protocolos de capa 2 son LLC (Control de Enlace Lógico), LAPDm (Protocolo de Acceso de Enlace en el canal de Dm), RLC (Control de Enlace de Radio), y MAC (protocolo de Control de Acceso al Medio). La capa física es únicamente de un ‘protocolo’, que no tiene nombre específico. Todos los protocolos de interfaz de radio mencionados son específicos para cada técnica de acceso de radio, que significa que son diferentes para la interfaz de radio de GSM y la interfaz de UMTS Uu, por ejemplo.

En el UMTS, la capa de RRC ofrece servicios a capas superiores, es decir, a un estrato de no acceso NAS mediante puntos de acceso servicio que se usan por los protocolos superiores en el lado del terminal de usuario y por el protocolo de RANAP (Parte de Aplicación de Red de Acceso de Radio) de Iu en el lado de la UTRAN. Toda la señalización de capa superior (gestión de movilidad, control de llamada, gestión de sesión, etc.) se encapsula en mensajes de RRC para transmisión a través de la interfaz de radio.

Toda la telecomunicación se somete al problema de cómo asegurar que la información recibida se ha enviado por un emisor autorizado y no por alguien que está intentando enmascararse como el emisor. El problema es particularmente evidente en sistemas de telecomunicaciones celulares, donde la interfaz aérea presenta una plataforma excelente para escucha clandestina y sustitución de los contenidos de una transmisión usando niveles de transmisión superiores, incluso a distancia. Una solución básica a este problema es la autenticación de las partes de la comunicación. Un proceso de autenticación tiene como objetivo descubrir y comprobar la identidad de ambas de

las partes de la comunicación, de modo que cada parte recibe información acerca de la identidad de la otra parte y puede basarse en la identificación hasta un grado suficiente. La autenticación se realiza normalmente en un procedimiento específico en el comienzo de la conexión. Sin embargo, esto no protege adecuadamente mensajes posteriores de manipulación no autorizada, inserción y borrado. Por lo tanto, existe una necesidad de la autenticación separada de cada mensaje transmitido. La última tarea puede llevarse a cabo anexando un código de autenticación de mensaje (MAC-I) al mensaje en el extremo de transmisión y comprobar el valor de MAC-I en el extremo de recepción.

Un MAC-I es normalmente una cadena de bits relativamente corta basándose en alguna manera especificada en el mensaje que protege y en una clave secreta conocida tanto por el emisor como por el receptor del mensaje. La clave secreta se genera y acuerda normalmente en relación con el procedimiento de autenticación en el comienzo de la conexión. En algunos casos el algoritmo que se usa para calcular el MAC-I basándose en la clave secreta y en el mensaje también es secreto, pero este no es el caso habitual.

El proceso de autenticación de mensajes únicos se denomina en ocasiones protección de integridad. Para proteger la integridad de la señalización, la parte de transmisión calcula un valor de MAC-I basándose en el mensaje a enviarse y la clave secreta usando el algoritmo especificado, y envía el mensaje con el valor de MAC-I. La parte de recepción recalcula un valor de MAC-I basándose en el mensaje y la clave secreta de acuerdo con el algoritmo especificado, y compara el MAC-I recibido y el MAC-I calculado. Si los dos valores de MAC-I coinciden, el receptor puede confiar que el mensaje se encuentra intacto y se ha enviado por la parte autorizada.

La Figura **2** ilustra el cálculo de un código de autenticación de mensaje en la UTRAN. La longitud del MAC-I usado en UTRAN son 32 bits.

El algoritmo de integridad de UMTS usado en el bloque **200** es una función criptográfica unidireccional para calcular el código de autenticación de mensaje (MAC-I) basándose en los parámetros de entrada mostrados en la Figura **2**. La función unidireccional significa que es imposible derivar los parámetros de entrada desconocidos a partir de un MAC-I, incluso si se conocieran todos menos un parámetro de entrada.

Los parámetros de entrada para calcular el MAC-I son el mensaje de señalización real (después de codificar) a enviarse, una clave de integridad secreta, un número de secuencia COUNT-I para el mensaje a protegerse en integridad, un valor que indica la dirección de transmisión, es decir si el mensaje se envía en dirección de enlace ascendente (desde el terminal de usuario a la red) o de enlace descendente (desde la red al terminal de usuario), y un número aleatorio (FRESH) generado por la red. COUNT-I está compuesto de un número de secuencia corta SN y un número de secuencia larga denominado número de híper trama HFN. Únicamente se envía normalmente el número de secuencia corta con el mensaje; el HFN se actualiza localmente en cada parte de la comunicación.

El bloque de cálculo **200** calcula el código de autenticación de mensaje aplicando los parámetros anteriormente mencionados al algoritmo de integridad, que se denomina algoritmo f9 en las especificaciones de 3GPP Versión'99. Es posible que estén disponibles más algoritmos en versiones futuras de nuevas especificaciones. Antes de que se inicie la protección de integridad, el terminal de usuario informa a la red, qué algoritmos de integridad soporta, y la red a continuación selecciona uno de estos algoritmos para usarse para la conexión. Un mecanismo similar con respecto a los algoritmos soportados se usa también para el cifrado.

La Figura **3** ilustra un mensaje a enviarse a través de, por ejemplo, una interfaz de radio. El mensaje es una unidad de datos de protocolo (PDU) de capa N **300**, que se transfiere como una carga útil en la PDU de capa N-1 **301**. En el presente ejemplo, la capa N representa el protocolo de control de recursos de radio (RRC) en la interfaz de radio y la capa N-1 representa la capa de control de enlace de radio (RLC). La PDU de capa N-1 normalmente tiene un tamaño fijo, que depende del tipo de canal de capa física (la capa más inferior, no visible en la Figura 2) usado y de los parámetros, por ejemplo modulación, codificación de canal, intercalación. Si las PDU de capa N no tienen exactamente el tamaño de la carga útil diferida por la capa N-1 como es normalmente el caso, la capa N-1 puede utilizar funciones como segmentación, concatenación y relleno para hacer las PDU de capa N-1 siempre de un tamaño fijo. En la presente solicitud nos concentramos en una PDU de capa N que consiste en los datos de señalización real y la información de comprobación de integridad. La información de comprobación de integridad consiste en el MAC-I y el número de secuencia de mensaje SN necesario en el extremo de par para el recálculo de MAC-I. La longitud total del mensaje es entonces una combinación de los bits de datos de señalización y los bits de información de comprobación de integridad.

La Figura **4** ilustra traspaso intersistema desde una red de acceso de radio a un subsistema de estación base de GSM. Por simplicidad únicamente se muestra un centro de conmutación móvil en la Figura **4**. Realmente consiste en un centro de conmutación móvil MSC de GSM (2G o segunda generación) y un centro de conmutación móvil de UMTS (3G o tercera generación), que pueden ser físicamente uno cualquiera o dos MSC separados. La interacción entre estos dos centros de conmutación móviles (si fueran dos entidades separadas) no es esencial en vista de la invención real y por lo tanto no se describe a continuación.

En el comienzo, existe una conexión entre el terminal de usuario y la red de acceso de radio, que en este ejemplo

particular es una UTRAN. Basándose en diversos parámetros, por ejemplo la información de carga de célula vecina, las mediciones desde el terminal de usuario, y la existencia de células de GSM en el área geográfica cercana, así como la existencia de las capacidades del terminal de usuario (para soportar también el modo GSM), la red de acceso de radio puede iniciar un traspaso intersistema al subsistema de estación base BSS. En primer lugar, la UTRAN solicita el terminal de usuario que inicie mediciones intersistema en operadoras de GSM enviando un mensaje de CONTROL DE MEDICIÓN **400** que contiene parámetros específicos intersistema. Cuando se satisfacen los criterios (como se describe en el mensaje CONTROL DE MEDICIÓN) para enviar un informe de medición, el terminal de usuario envía un informe o informes de medición **401**. A continuación se toma la decisión de traspaso inter-sistema en la UTRAN. Después de la decisión un controlador de red de radio servidor SRNC, que está situado en la UTRAN, envía un mensaje RELOCALIZACIÓN REQUERIDA **402** a través de la interfaz Iu al centro de conmutación móvil (3G MSC). Una vez después de recibir el mensaje, el centro de conmutación móvil (2G MSC) envía un mensaje de solicitud de traspaso **403** a un subsistema de estación base objetivo, que comprende información, tal como el algoritmo de cifrado y la clave de cifrado para usarse para la conexión, y la información de marca de clase de MS, que indica, por ejemplo, qué algoritmos de cifrado se soportan por el terminal de usuario. Por lo tanto, es posible que el centro de conmutación móvil MSC seleccione el algoritmo de cifrado e indique únicamente el algoritmo seleccionado al subsistema de estación base BSS, o que el centro de conmutación móvil MSC envíe una lista de posibles algoritmos de cifrado al subsistema de estación base BSS, que a continuación toma la selección final. La información de marca de clase de MS se envía por el terminal de usuario al centro de conmutación móvil MSC en el comienzo de la conexión (UMTS). También es posible que se envíe la información de marca de clase de MS desde el terminal de usuario a la red de acceso de radio de UMTS (UTRAN) en el comienzo de la conexión (UMTS). Cuando se activa un traspaso inter-sistema desde UMTS a GSM, la información de marca de clase de MS se reenvía desde la UTRAN al MSC. Cuando un controlador de estación base de GSM recibe el mensaje, realiza la reserva desde la célula de GSM indicada y responde enviando de vuelta un mensaje de ACK de solicitud de traspaso **404** que indica que el traspaso solicitado en el subsistema de estación base BSS puede soportarse y también a qué canal o canales de radio debería dirigirse el terminal de usuario. La solicitud de traspaso ACK **404** también indica que el algoritmo de traspaso solicitado se ha aceptado, o, si la solicitud de traspaso **403** contiene varios algoritmos, qué algoritmo de traspaso se ha seleccionado. Si el subsistema de estación base BSS no puede soportar ninguno de los algoritmos de cifrado indicados, devuelve un mensaje FALLO DE TRASPASO (en lugar de **404**) y el centro de conmutación móvil MSC indica fallo del traspaso a la UTRAN. En la etapa **405**, el centro de conmutación móvil (3G MSC) responde con un mensaje de COMANDO DE RELOCALIZACIÓN a través de la interfaz Iu al mensaje enviado en la etapa **402** desde el controlador de red de radio servidor situado en la UTRAN. El COMANDO DE RELOCALIZACIÓN lleva en una carga útil, por ejemplo, la información acerca de los canales de GSM objetivo junto con la información de modo de cifrado. La UTRAN ordena que el terminal de usuario ejecute el traspaso enviando un COMANDO DE MENSAJE DE TRASPASO INTERSISTEMA **406** que incluye información de canal para el GSM objetivo. Además, puede incluirse otra información, tal como la información de ajuste de modo de cifrado de GSM, que indica al menos el algoritmo de cifrado a usarse en la conexión de GSM. Después de haberse conmutado a los canales de GSM asignados, la estación móvil normalmente envía cuatro veces el mensaje ACCESO DE TRASPASO **407** en cuatro tramas de capa 1 sucesivas en el DCCH principal. Estos mensajes se envían en ráfagas de acceso de GSM, que no están cifradas. En algunas situaciones puede no ser necesario enviar estos mensajes de ACCESO DE TRASPASO, si se indica así en el COMANDO DE TRASPASO INTERSISTEMA **406**. El terminal puede recibir un mensaje de INFORMACIÓN FÍSICA **408** como una respuesta a los mensajes de ACCESO DE TRASPASO. El mensaje de INFORMACIÓN FÍSICA contiene únicamente la información de avance de temporización de GSM. La recepción de un mensaje de INFORMACIÓN FÍSICA provoca que el terminal detenga el envío de ráfagas de acceso. Los mensajes de ACCESO DE TRASPASO, si se usan, activan el controlador de estación base en el sistema de estación base de GSM para informar acerca de la situación al centro de conmutación móvil (2G) con un mensaje DETECTAR TRASPASO **409**.

Después de que se establezcan satisfactoriamente las conexiones de capa inferior, la estación móvil devuelve un mensaje de TRASPASO COMPLETO **410** al subsistema de estación base de GSM en el DCCH principal. Cuando se recibe el mensaje de TRASPASO COMPLETO **410**, la red libera los canales antiguos, en este ejemplo los canales de UTRAN. En la Figura **4**, se muestran tres mensajes de este procedimiento de liberación, aunque en realidad serían necesarios muchos otros mensajes entre elementos de red, que no se muestran en la Figura **4**. Estos tres mensajes son en primer lugar el mensaje de TRASPASO COMPLETO **411** desde el subsistema de estación base de GSM al centro de conmutación móvil, a continuación un COMANDO DE LIBERACIÓN DE IU **412** a través de la interfaz Iu a la UTRAN o más precisamente al controlador de red de radio servidor. El tercer mensaje es el mensaje de LIBERACIÓN DE IU COMPLETA **413**.

La clave de cifrado a usarse después del traspaso intersistema se deriva con una función de conversión a partir de la clave de cifrado usada en UTRAN antes del traspaso. Esta función de conversión existe tanto en la estación móvil como en el centro de conmutación móvil, por lo tanto no son necesarios procedimientos adicionales a través de la interfaz de radio. Como se ha descrito anteriormente, el algoritmo de cifrado de GSM a usarse después del traspaso intersistema se selecciona por el MSC o por el BSS y se informa a la estación móvil (en los mensajes **405** y **406**). La capacidad de algoritmo de cifrado de GSM (incluido en los elementos de información de marca de clase de MS de GSM) es en las especificaciones actuales transparente para la UTRAN. Sin embargo, los elementos de información de marca de clase de MS de GSM se envían desde la estación móvil a la UTRAN durante el procedimiento de establecimiento de conexión de RRC, para que se reenvíe más tarde a la red principal durante el traspaso inter-

sistema a GSM.

La Figura **5** es un diagrama de señalización que muestra el procedimiento de configuración de conexión básica y configuración de modo de seguridad usado en la UTRAN de 3GPP. La Figura 5 muestra únicamente la señalización más importante entre una estación móvil y un controlador de red de radio servidor que reside en la red de acceso de radio por una parte y el controlador de red de radio servidor y un centro de conmutación móvil o un nodo de soporte de GPRS de servicio por la otra.

El establecimiento de una conexión de control de recursos de radio (RRC) entre la estación móvil y el controlador de red de radio servidor se realiza a través de la interfaz Uu **500**. Durante el establecimiento de conexión de RRC, la estación móvil puede transferir información tal como la capacidad de seguridad de equipo de usuario y los valores de INICIO, que se requieren para los algoritmos de protección de cifrado e integridad. La capacidad de seguridad de equipo de usuario incluye información acerca de los algoritmos de cifrado (UMTS) y algoritmos de integridad (UMTS) soportados. Todos los valores anteriormente mencionados se almacenan para uso posterior en el controlador de red de radio servidor en la etapa **501**. También la información de marca de clase de GSM (Marca de clase de MS 2 y Marca de clase de MS 3) se transmite desde la estación móvil a la UTRAN durante el establecimiento de conexión de RRC, y puede almacenarse para uso posterior en el controlador de red de radio servidor.

A continuación la estación móvil envía un mensaje de capa superior inicial **502** (que puede ser, por ejemplo, SOLICITUD DE SERVICIO DE CM, SOLICITUD DE ACTUALIZACIÓN DE LOCALIZACIÓN o SOLICITUD DE RE-ESTABLECIMIENTO DE CM) mediante el controlador de red de radio servidor a través de la interfaz Iu al centro de conmutación móvil, que incluye, por ejemplo, la identidad de usuario, un identificador de ajuste de clave KSI y la marca de clase de MS que indica, por ejemplo, los algoritmos de cifrado de GSM soportados cuando se inicializa el traspaso intersistema al GSM. La red inicia el procedimiento de autenticación que también conduce a la generación de nuevas claves de seguridad **503**. A continuación, la red decide el ajuste de los algoritmos de integridad de UMTS UIA y algoritmos de encriptación de UMTS UEA a partir de los cuales tiene que seleccionarse el UIA y UEA para esta conexión **504**. A continuación, en la etapa **505**, el centro de conmutación móvil envía un mensaje de COMANDO DE MODO DE SEGURIDAD al controlador de red de radio servidor, en el que informa la clave de cifrado usada CK, clave de integridad IK, y el conjunto de UIA y UEA permisibles.

Basándose en las capacidades de seguridad del equipo de usuario almacenadas en la etapa **501** y la lista de posibles UIA y UEA recibidos desde el centro de conmutación móvil en la etapa **505**, el controlador de red de radio servidor selecciona los algoritmos a usarse durante la conexión. También genera un valor aleatorio FRESH para usarse como el parámetro de entrada para el algoritmo de integridad (Figura 2) y para el algoritmo de cifrado. También inicia el descifrado y la protección de integridad **506**.

Un primer mensaje de integridad protegida COMANDO DE MODO DE SEGURIDAD **507** se envía a través de la interfaz de radio desde el controlador de red de radio servidor a la estación móvil. El mensaje incluye los UIA y UEA seleccionados junto con el parámetro FRESH de UE a usarse. Además, el COMANDO DE MODO DE SEGURIDAD contiene la misma capacidad de seguridad del UE que se recibió desde el equipo de usuario durante el establecimiento de conexión de RRC **500**. La razón para la reproducción de esta información de vuelta al UE es proporcionar al equipo de usuario una posibilidad de comprobar que la red ha recibido esta información correctamente. Este mecanismo es necesario, puesto que los mensajes enviados durante el establecimiento de conexión de RRC **500** no están cifrados ni protegidos en integridad. Un código de autenticación de mensaje MAC-I, usado para la protección de integridad, se anexa al mensaje de COMANDO DE MODO DE SEGURIDAD **507**.

En la etapa **508** la estación móvil compara si la capacidad de seguridad de UE recibida es la misma que la que se ha enviado durante el procedimiento de establecimiento de conexión de RRC **500**. Si las dos capacidades de seguridad de UE coinciden, la estación móvil puede confiar que la red ha recibido la capacidad de seguridad correctamente. De otra manera, el UE libera la conexión de RRC entra en modo en reposo.

Si la comparación es satisfactoria la estación móvil responde con un mensaje de MODO DE SEGURIDAD COMPLETO **509**. Este es también un mensaje de integridad protegida; por lo tanto antes de enviar este mensaje la estación móvil genera el MAC-I para el mensaje.

Cuando el controlador de red de radio servidor recibe el mensaje lo verifica, en la etapa **510**, calculando en primer lugar el código de autenticación de mensaje XMAC-I esperado y a continuación comparando el XMAC-I calculado con el MAC-I recibido. Si los valores coinciden, el controlador de red de radio servidor envía un mensaje MODO DE SEGURIDAD COMPLETO **511** al centro de conmutación móvil que incluye, por ejemplo, información del UIA y UEA seleccionados.

En la interfaz de radio de UTRAN la protección de integridad es una función del protocolo de control de recursos de radio entre el terminal de usuario y el controlador de red de radio. Toda la señalización de capa superior está protegida en integridad por la capa de protocolo de control de recursos de radio puesto que toda la señalización de capa superior se lleva como una carga útil en mensajes de control de recursos de radio específicos (por ejemplo TRANSFERENCIA DIRECTA INICIAL, TRANSFERENCIA DIRECTA DE ENLACE ASCENDENTE,

TRANSFERENCIA DIRECTA DE ENLACE DESCENDENTE). El problema es que no puede realizarse autenticación antes de que se envíe el primer mensaje de capa superior, que se lleva en la TRANSFERENCIA DIRECTA INICIAL. Esto conduce a una situación donde la primera capa más superior, es decir, el mensaje de estrado de no acceso **502** no puede estar protegido en integridad.

Surge un problema principal a partir del hecho de que la protección de integridad no está aún efectuándose cuando se envían los primeros mensajes durante el establecimiento de conexión de RRC (etapa **500** en la Figura **5**). Sin protección de integridad hay siempre un riesgo de que un intruso cambie la información de algoritmo de encriptación incluida en los mensajes en la etapa **500** en el valor "algoritmos de encriptación de GSM no disponibles". En el caso de GSM, la red principal recibe esta información con los elementos de información de CM de marca de clase de estación móvil (CM2 y CM3) que se incluyen en el mensaje de RELOCALIZACIÓN REQUERIDA (mensaje 402 en la Figura 4). Cuando el equipo de usuario lleva a cabo un traspaso intersistema, por ejemplo desde la UTRAN al subsistema de estación base BSS de GSM (Figura 4) el centro de conmutación móvil reconoce que el UE no soporta ningún algoritmo de cifrado de GSM y debe establecer la conexión en el BSS de GSM sin cifrado. Ahora es fácil para el intruso iniciar la escucha clandestina de la llamada.

El documento WO99/26420 A2 se refiere a una técnica para establecer encriptación para una conexión en un sistema combinado de la RAN del sistema IMT-2000 y la red principal (MSC) del sistema de GSM.

Sumario de la invención

Un objetivo de la presente invención es idear un sistema de telecomunicaciones móviles que revela un intento de un intruso fraudulento para eliminar información acerca de un algoritmo de encriptación cuando una estación móvil multi-modo envía un mensaje de señalización no protegido que contiene esta información a través de la interfaz de radio al sistema de telecomunicaciones móviles. De acuerdo con las especificaciones existentes, el mensaje de señalización es CONFIGURACIÓN DE CONEXIÓN DE RRC COMPLETA.

La presente invención proporciona el aparato de acuerdo con la reivindicación 1 y la reivindicación 9, y los métodos de acuerdo con la reivindicación 18 y la reivindicación 21.

En una realización; el sistema comprende al menos dos redes de acceso de radio que proporcionan estaciones móviles con acceso a al menos una red principal, una estación móvil multi-modo, y al menos una red principal. La estación móvil multi-modo envía, durante el establecimiento de la conexión con una primera red de acceso de radio, al menos un mensaje de señalización no protegido, que incluye información acerca de algoritmos de encriptación soportados por la estación móvil multi-modo en una segunda red de acceso de radio. La red principal recibe información acerca de los algoritmos de encriptación mediante la primera red de acceso de radio cuando se activa un traspaso a la segunda red de acceso de radio (mensaje 402 en la Figura 4). En la recepción de un mensaje de comando desde la red principal que ordena a la estación móvil multi-modo que cifre la comunicación adicional en la primera red de acceso de radio, la primera red de acceso de radio compone un mensaje de comando de integridad protegida que incluye información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en la segunda red de acceso de radio.

El mensaje de comando protegido comprende una carga útil y un código de autenticación de mensaje. La información acerca de los algoritmos soportados en la segunda red de acceso de radio está localizada en la carga útil o la información se usa como un parámetro cuando se calcula el código de autenticación de mensaje.

En ambos casos la estación móvil multi-modo puede concluir a partir del mensaje protegido recibido si la información embebida en el mensaje corresponde a la información enviada por la estación móvil multi-modo en el mensaje de señalización anterior. Si se envía la información y la información recibida por la estación móvil multi-modo difiere una con respecto a la otra, es probable que un intruso fraudulento haya cambiado la información de encriptación. A continuación la estación móvil multi-modo inicia la liberación de la conexión.

Breve descripción de los dibujos

La invención se describe más estrechamente con referencia a los dibujos adjuntos, en los que

La Figura **1** ilustra con un diagrama de bloques simplificado unas redes de acceso de radio de GSM y UMTS, conectadas a la misma red principal;
La Figura **2** representa el cálculo de un código de autenticación de mensaje;
La Figura **3** muestra los contenidos de un mensaje;
La Figura **4** es un diagrama de señalización que ilustra traspaso intersistema desde la red de UMTS a la red de GSM;
La Figura **5** es un gráfico de señalización que muestra el procedimiento de configuración de conexión básica y configuración de modo de seguridad en la UTRAN de 3GPP;
La Figura **6** muestra como un diagrama de flujo del primer ejemplo de la implementación del método de acuerdo con la invención;

La Figura **7** muestra como un diagrama de flujo de un segundo ejemplo de la implementación del método de acuerdo con la invención;
La Figura **8** muestra como un diagrama de flujo de un tercer ejemplo de la implementación del método de acuerdo con la invención;
La Figura **9** muestra como un diagrama de flujo de un cuarto ejemplo de la implementación del método de acuerdo con la invención;
La Figura **10** muestra un quinto ejemplo de la implementación del método de acuerdo con la invención;
La Figura **11** muestra un sexto ejemplo de la implementación del método de acuerdo con la invención.

Descripción detallada de la realización preferida

La idea del método descrita a continuación es aumentar la seguridad en redes de telecomunicaciones, especialmente la seguridad que pertenece a la señalización a través de la interfaz de radio.

Se ha de observar que todas las expresiones "terminal", "terminal de usuario", "estación móvil" y "equipo de usuario" hacen referencia al mismo equipo.

La mayoría de los mensajes de señalización enviados entre un terminal de usuario y la red, por ejemplo, deben estar protegidos en integridad. Ejemplos de tales mensajes son mensajes RRC, MM, CC, GMM y SM. La protección de integridad se aplica en la capa de RRC, tanto en el terminal de usuario como en la red.

La protección de integridad se realiza normalmente para todos los mensajes de RRC (Control de Recurso de Radio), con algunas excepciones. Estas excepciones pueden ser:

1. mensajes asignados a más de un receptor,
2. mensajes enviados antes de que se crearan las claves de integridad para la conexión, y
3. mensajes frecuentemente repetidos, que incluye información que no necesita protección de integridad.

Debido a la seguridad, es especialmente importante proteger en integridad los mensajes iniciales mencionados en la alternativa 2, o al menos elementos de información críticos en ellos. Como ya se ha mencionado, sin protección de integridad hay siempre un riesgo de que un intruso cambie la información de algoritmo de encriptación incluida en el mensaje **500** al valor "algoritmo de encriptación no está disponible".

Hay varias diferentes maneras de implementar la funcionalidad requerida para aumentar la seguridad pero únicamente se muestran algunas de las soluciones.

La invención se describe ahora en detalle con cuatro ejemplos haciendo referencia a las Figuras **6 - 9**.

En el comienzo se establece una conexión entre un terminal de usuario y una red de UMTS. Posteriormente se lleva a cabo un traspaso desde la red de UMTS a una red de GSM.

La Figura **6** muestra como un diagrama de flujo de una implementación del método de acuerdo con la invención. Se supone que la señalización corresponde a la situación mostrada en la Figura **5** hasta que la red principal recibe el mensaje **503**.

Además se supone que el terminal de usuario es un terminal de modo dual (UMTS/GSM), que en el modo de UMTS envía el primer mensaje de estrato de no acceso a través de la interfaz de radio en un mensaje de TRANSFERENCIA DIRECTA INICIAL de control de recursos de radio (que corresponde a **502** en la Figura **5**). Se supone adicionalmente que el establecimiento de conexión de RRC (500) se ha realizado, por lo tanto el terminal de usuario estaba en un estado en reposo y no tenía conexión de RRC existente cuando llegó una solicitud para establecer una conexión con la red principal.

La red principal recibe información de marca de clase de GSM en el mensaje inicial **502** desde el terminal de usuario, en este punto la estación móvil. Esta información indica características de estación móvil generales en el modo de GSM que incluyen información acerca de qué algoritmos de cifrado de GSM se soportan en el terminal cuando se encuentra en el modo de GSM. La expresión “marca de clase” tiene que entenderse como específica de GSM; puede usarse otro término en otros sistemas. El centro de conmutación móvil en la red principal añade información acerca de algoritmos de encriptación soportados por la estación móvil en el mensaje de COMANDO DE MODO DE SEGURIDAD **600**. El mensaje se envía al controlador de red de radio servidor a través de la interfaz Iu. El controlador de red de radio servidor añade esta información acerca de algoritmos de encriptación soportados por la estación móvil, que incluye información acerca de algoritmos de encriptación soportados, a un mensaje de COMANDO DE SEGURIDAD antes de la codificación **601**. Se calcula un código de autenticación de mensaje de 32 bits MAC-I y se añade al mensaje codificado.

Además del mensaje codificado, el código de MAC-I también está basado en varios otros parámetros. Los siguientes parámetros de entrada son necesarios para el cálculo del algoritmo de integridad: el mensaje codificado, el número

de secuencia de SN de 4 bits, el número de híper-trama HFN de 28 bits, el número aleatorio FRESH de 32 bits, el identificador de dirección DIR de 1 bit, y el parámetro más importante - la clave de integridad IK de 128 bits. El número de secuencia corta SN y el número de secuencia larga HFN juntos componen el número de secuencia de integridad en serie COUNT-I.

Cuando se calcula el código de autenticación de mensaje usando el algoritmo de integridad y los parámetros anteriores, se garantiza que ningún otro distinto al emisor real pueda añadir el código de MAC-I correcto al mensaje de señalización. COUNT-I, por ejemplo, evita que el mismo mensaje se envíe repetitivamente. Sin embargo, si el mismo mensaje de señalización por alguna razón u otra se ha de enviar repetitivamente, el código de MAC-I se diferencia del código de MAC-I que estaba en el mensaje de señalización previamente enviado. El objetivo de esto es proteger el mensaje tan fuerte como sea posible contra escuchadores clandestinos y otros usuarios fraudulentos. Por lo tanto, para esta invención particular, es importante observar también que la información de GSM acerca de algoritmos de encriptación soportados por la estación móvil que se añade al mensaje de COMANDO DE MODO DE SEGURIDAD **507**, está protegida en integridad, de modo que la estación móvil puede estar segura de que esta información no se ha cambiado por un intruso.

A continuación, en la etapa **602**, cuando la estación móvil recibe el mensaje de COMANDO DE MODO DE SEGURIDAD, la información acerca de algoritmos de encriptación soportados por la estación móvil recibidos con este mensaje se compara con la información acerca de algoritmos de encriptación soportados por la estación móvil enviados anteriormente desde la estación móvil a la red en el mensaje inicial **502**. En correspondencia, de acuerdo con la técnica anterior, el parámetro de capacidad de seguridad del UE recibido (UMTS) se compara con el parámetro de capacidad de seguridad del UE. Si ambas comparaciones son satisfactorias la estación móvil acepta la conexión **604**, de otra manera la conexión se libera **603**.

La Figura **7** muestra como un diagrama de flujo de la segunda implementación del método.

En la etapa **700** la estación móvil envía un mensaje de TRANSFERENCIA DIRECTA INICIAL (que corresponde al mensaje **502** en la Figura 5) a la red principal mediante el controlador de red de radio servidor en la red de acceso de radio. El mensaje consiste en dos partes principales: una parte de RRC y una parte de estrato de no acceso, que se observa por el RRC como una carga útil transparente. Además, la parte de carga útil incluye uno de los siguientes mensajes: SOLICITUD DE SERVICIO DE CM, SOLICITUD DE ACTUALIZACIÓN DE LOCALIZACIÓN, SOLICITUD DE RE-ESTABLECIMIENTO DE CM o RESPUESTA DE RADIOBÚSQUEDA.

Cuando el controlador de red de radio servidor recibe el mensaje, almacena el mensaje **701** y reenvía la parte de carga útil o la parte de NAS a través de la interfaz Iu a la red principal **702**. La red principal responde con el mensaje de COMANDO DE MODO DE SEGURIDAD normal **703**. Como en el ejemplo anterior, el código de autenticación de mensaje MAC-I se calcula para proteger el mensaje a transmitirse a la estación móvil. El código se añade a continuación al mensaje. El código de autenticación de mensaje depende de una manera especificada en el mensaje que está protegiendo. En este punto el cálculo se lleva a cabo usando la siguiente cadena de bits concatenada como un parámetro de MENSAJE:

> MENSAJE = COMANDO DE MODO DE SEGURIDAD + SOLICITUD DE CONEXIÓN DE RRC + TRANSFERENCIA DIRECTA INICIAL DE RRC.

Posteriormente, el mensaje de COMANDO DE MODO DE SEGURIDAD de integridad protegida se envía a la estación móvil **704**.

Debería observarse que en esta solución es innecesario incluir el parámetro de capacidad de seguridad del UE (UMTS) en el mensaje anterior. Sin embargo, ambos parámetros relacionados con seguridad, es decir el parámetro de capacidad de seguridad de UE y el parámetro de marca de clase de GSM eran parámetros de entrada cuando se calculó el código de MAC-I.

El extremo de recepción, es decir la estación móvil, tiene el algoritmo idéntico para calcular el código de autenticación de mensaje para verificar que el código de autenticación de mensaje recibido es el mismo que el código calculado **705**. Por lo tanto, la estación móvil ha grabado los mensajes anteriormente enviados, el mensaje de SOLICITUD DE CONEXIÓN DE RRC (**500**) y el mensaje de TRANSFERENCIA DIRECTA INICIAL DE RRC (**502**) para calcular XMAC-I para el mensaje de COMANDO DE MODO DE SEGURIDAD recibido. Cuando el valor de MAC-I recibido y el valor de XMAC-I calculado coinciden, la estación móvil supone que la red ha recibido información correcta para la capacidad de seguridad y las marcas de clase de GSM, y la conexión se acepta **707**. De otra manera la conexión se libera **706**.

Existe una desventaja de esta solución, que es que los mensajes codificados SOLICITUD DE CONEXIÓN DE RRC y TRANSFERENCIA DIRECTA INICIAL DE RRC deben almacenarse en la memoria de tanto el controlador de red de radio servidor como la estación móvil hasta que se haya enviado/recibido el mensaje de COMANDO DE MODO DE SEGURIDAD. Pero por otra parte, esta solución hace posible omitir la capacidad de seguridad del UE del mensaje de COMANDO DE MODO DE SEGURIDAD de la técnica anterior y de esta manera ahorrar 32 bits de

espacio en el mensaje.

La Figura **8** muestra como un diagrama de flujo de la tercera implementación del método.

Esta solución se diferencia ligeramente de la segunda solución, es decir únicamente los bloques **801**, **804** y **805** se diferencian de los bloques en la Figura. 7. Por lo tanto, estos dos bloques se describen ahora en detalle.

En la etapa **801**, en lugar de almacenar la totalidad del mensaje, el controlador de red de radio servidor únicamente almacena la parte del mensaje de carga útil para uso posterior. En otras palabras, almacena uno de los siguientes mensajes: SOLICITUD DE SERVICIO DE CM, SOLICITUD DE ACTUALIZACIÓN DE LOCALIZACIÓN, SOLICITUD DE RE-ESTABLECIMIENTO DE CM o SOLICITUD DE RADIOBÚSQUEDA. Por lo tanto, esta solución ahorra espacio de memoria en comparación con la segunda solución.

En la etapa **804**, para proteger el mensaje, se calcula el código de autenticación de mensaje MAC-I usando la carga útil previamente almacenada. El mensaje se forma en este caso como sigue:

> MENSAJE = COMANDO DE MODO DE SEGURIDAD + CAPACIDAD DE SEGURIDAD DE UE + parte de mensaje de NAS del mensaje de TRANSFERENCIA DIRECTA INICIAL

Únicamente se envía el mensaje COMANDO DE MODO DE SEGURIDAD a través de la interfaz Uu a la estación móvil. Esto significa que tanto los parámetros de seguridad para la capacidad de seguridad del UE como las marcas de clase de MS de GSM se usan al calcular el código de autenticación de mensaje MAC-I, pero no hay necesidad de incluirlos en el mensaje. Sin embargo, esto no reduce de ninguna manera la seguridad.

En la etapa **805** la estación móvil calcula el XMAC-I usando el mismo parámetro de MENSAJE que el que usó la red en la etapa **804**, es decir los parámetros, que se grabaron anteriormente de la capacidad de seguridad de UE y el mensaje de NAS de la parte del mensaje de TRANSFERENCIA DIRECTA INICIAL.

La Figura **9** muestra como un diagrama de flujo la cuarta implementación del método. Esta solución es una combinación de la primera y la tercera soluciones.

Durante el establecimiento de la conexión entre la estación móvil y el controlador de red de radio servidor en la red de acceso de radio, el último recibe y almacena la información de capacidad del equipo de usuario UEC en su memoria para uso posterior **900**. Después de eso la estación móvil envía el primer mensaje de estrato de no acceso que contiene por ejemplo información acerca de algoritmos de encriptación soportados por la estación móvil, como una carga útil en un mensaje de TRANSFERENCIA DIRECTA INICIAL DE RRC a la red de acceso de radio, que reenvía el mensaje de NAS a la red principal **901**. El centro de conmutación móvil en la red principal añade la información acerca de algoritmos de encriptación soportados por el parámetro de estación móvil al mensaje de COMANDO DE MODO DE SEGURIDAD y envía el mensaje a través de la interfaz Iu al controlador de red de radio servidor en la red de acceso de radio, en la etapa **902** y **903**.

En la etapa **904** el controlador de red de radio servidor calcula el código MAC-I de la manera anteriormente descrita, añadiendo a los parámetros anteriormente descritos el parámetro de mensaje, que se forma como sigue:

> MENSAJE = COMANDO DE MODO DE SEGURIDAD + CAPACIDAD DE SEGURIDAD DE UE + MARCAS DE CLASE DE GSM

De la misma manera que en el ejemplo anterior, tanto la capacidad de seguridad de UE de parámetros de seguridad y la marca de clase de GSM se usan para calcular el código de autenticación de mensaje MAC-I, pero no hay necesidad de incluirlos en el mensaje. La ventaja de esta solución es que no es necesaria memoria adicional en la estación móvil o en el controlador de red de radio.

Es esencial que en las soluciones anteriormente descritas la red principal sea un elemento de red de 3G, controlando por lo tanto al menos una red de acceso de radio de UMTS y opcionalmente también el subsistema de estación base de GSM.

La implementación y realización de la presente invención se ha explicado anteriormente con algunos ejemplos. Sin embargo, se ha de entender que la invención no está restringida a los detalles de la realización anterior y que pueden realizarse numerosos cambios y modificaciones por los expertos en la materia sin alejarse de los rasgos característicos de la invención. La realización descrita se ha de considerar ilustrativa pero no restrictiva. Por lo tanto, la invención debería limitarse por las reivindicaciones adjuntas. Por lo tanto, se incluyen implementaciones alternativas definidas mediante las reivindicaciones, así como implementaciones equivalentes, en el alcance de la invención.

Por ejemplo, la red de acceso de radio de origen puede ser, por ejemplo, la UTRAN, el subsistema de estación base de GSM, el sistema de GPRS (Servicio General de Paquetes de Radio), GSM Edge, GSM 1800, o algún otro

sistema. En correspondencia, la red de acceso de radio objetivo puede ser, por ejemplo, la UTRAN, el subsistema de estación base de GSM, el GPRS (Servicio General de Paquetes de Radio), GSM Edge, GSM 1800, o algún otro sistema.

Adicionalmente, la información acerca de los algoritmos de seguridad de GSM (A5/1, A5/2, A5/3, etc.) que se soportan por el terminal móvil multi-modo puede añadirse como una parte de la “Capacidad de Acceso de Radio de UE” de UMTS. Como alternativa, la información puede ser un elemento de información separado o incluso una parte del parámetro de capacidad de seguridad de UE. En la práctica esta información debe añadirse al procedimiento de establecimiento de conexión de RRC (véase la etapa **500** en la Figura **5**), así como al mensaje de COMANDO DE MODO DE SEGURIDAD (véase la etapa **507** en la Figura 5). Como en las otras posibles implementaciones anteriormente descritas, también en este caso añadiendo el elemento de información “Capacidad de Acceso de Radio Inter-RAT” real (que incluye información acerca de algoritmos de seguridad de GSM soportados) al mensaje de COMANDO DE MODO DE SEGURIDAD DE RRC es solamente una alternativa e introduce alguna carga a la señalización, puesto que el móvil no necesita necesariamente este elemento de información, sino únicamente una confirmación de que la red lo ha recibido correctamente. Se describen a continuación tres soluciones alternativas, es decir la quinta, sexta y séptima implementaciones de ejemplo del método.

En el quinto ejemplo de la implementación del método, se define un nuevo elemento de información de RRC, que incluye únicamente la capacidad de algoritmo de cifrado de GSM. Esto requiere 7 bits. Este elemento de información se añade a continuación al mensaje de COMANDO DE MODO DE SEGURIDAD DE RRC. La desventaja de esta solución es que para codificar este nuevo elemento de información en dicho mensaje, el protocolo de RRC de UTRAN tiene que decodificar en primer lugar los elementos de información de marca de clase 2 y marca de clase 3 de GSM, cuyas reglas de codificación/decodificación no son parte del protocolo de RRC de UTRAN.

La Figura **10** ilustra el sexto ejemplo de la implementación del método. En el lado de la UTRAN, la información de marca de clase 2 y marca de clase 3 de GSM recibida (elemento de información de RRC "capacidad de acceso de radio de UE Inter-RAT" **1001**), junto con la "Capacidad de Seguridad de UE" **1002** (que contiene información acerca de los algoritmos de seguridad de UTRAN soportados), se usa para calcular MAC-I (y XMAC-I) para el mensaje de COMANDO DE MODO DE SEGURIDAD DE RRC **1000**. Esta es esencialmente la misma solución que en la Figura 9 con la excepción de que la información de marca de clase de GSM (de la estación móvil y no de la red principal (902)) ya se ha recibido y almacenado en el controlador de red de radio servidor durante la fase de establecimiento de conexión de RRC (900). El COMANDO DE MODO DE SEGURIDAD a enviarse a la estación móvil no contiene la “capacidad de seguridad de UE" ni la "capacidad de acceso de radio de UE Inter-RAT"; estos elementos de información se usan únicamente cuando se calcula el MAC-I para este mensaje.

La desventaja de la sexta implementación es que la codificación de los elementos de información adicionales ("capacidad de seguridad de UE" y "capacidad de acceso de radio de UE Inter-RAT") usados para el cálculo de MAC-I tiene que definirse explícitamente. Si esto no es aceptable, se muestra una implementación más directa en la Figura **11** (una séptima implementación del método). En este punto todo el mensaje ESTABLECIMIENTO_CONEXIÓN_RRC_COMPLETO codificado se usa cuando se calcula MAC-I (y XMAC-I) para el mensaje COMANDO_MODO_SEGURIDAD_RRC **1000** (en lugar de los dos elementos de información únicamente como en la sexta implementación). En la práctica esto significa que durante el procedimiento de establecimiento de conexión de RRC (véase la etapa **500** en la Figura 5), cuando se envía el mensaje de ESTABLECIMIENTO_CONEXIÓN_RRC_COMPLETO la estación móvil debe grabar una copia del mensaje codificado en su memoria hasta que recibe el mensaje COMANDO_MODO_SEGURIDAD y ha comprobado su suma de comprobación de integridad. En el lado de la red (en el caso de UTRAN en el controlador de red de radio servidor) una copia del mensaje ESTABLECIMIENTO_CONEXIÓN_RRC_COMPLETO (no decodificado) recibido debe mantenerse en la memoria hasta que se haya calculado el código MAC-I para el mensaje COMANDO_MODO_SEGURIDAD. Desde el punto de vista de la implementación, probablemente es bastante fácil grabar el mensaje codificado completo en la memoria antes de que se envíe (lado del UE) o justo después de recibirlo y antes de que se pase al decodificador (lado de UTRAN). Por lo tanto, MAC-I para COMANDO_MODO_SEGURIDAD se calcularía estableciendo el parámetro de entrada de mensaje para el algoritmo de integridad como:

MENSAJE = COMANDO_MODO_SEGURIDAD + CONFIGURACIÓN_CONEXIÓN_RRC_COMPLETA

La desventaja en este punto, en comparación con el sexto ejemplo de la implementación del método, es que esta solución requiere un poco más memoria, tanto en la estación móvil y en el lado de la red. La información de marca de clase de GSM incluye los algoritmos de encriptación soportados por la estación móvil.

REIVINDICACIONES

1. Aparato situado en una red de acceso de radio, adaptado para:

- recibir un mensaje de comando desde una red principal que ordena a una estación móvil multi-modo cifrar la comunicación;
- componer (601, 704, 804, 904) un mensaje de comando de integridad protegida para enviar desde la red de acceso de radio (101) a la estación móvil multi-modo (100), incluyendo dicho mensaje de comando de identidad protegida información relacionada con los algoritmos de encriptación soportados por dicha estación móvil multi-modo en una red de acceso de radio (105) adicional, y que comprende una carga útil y un código de autenticación de mensaje.

2. Aparato como se define en la reivindicación 1, adaptado para grabar (701) un mensaje de señalización no protegido recibido desde la estación móvil multi-modo, y que incluye información acerca de algoritmos de encriptación soportados por la estación móvil multi-modo en la red de acceso de radio adicional, y para usar el mensaje de señalización no protegido en un algoritmo que calcula dicho código de autenticación de mensaje.

3. Aparato como se define en la reivindicación 1, adaptado para grabar (801) una carga útil de un mensaje de señalización no protegido recibido desde la estación móvil multi-modo, y que incluye información acerca de algoritmos de encriptación soportados por la estación móvil multi-modo en la red de acceso de radio adicional, y para usar la carga útil del mensaje de señalización no protegido en un algoritmo que calcula dicho código de autenticación de mensaje.

4. Aparato como se define en la reivindicación 1, adaptado para grabar (900) información de capacidad acerca de la capacidad de la estación móvil multi-modo en dicha red de acceso de radio adicional, recibida desde la estación móvil durante el establecimiento de la conexión, y para usar (904) dicha información de capacidad junto con información acerca de un algoritmo de encriptación embebido en un mensaje de comando recibido desde una red principal al calcular dicho código de autenticación de mensaje.

5. Aparato como se define en cualquier reivindicación anterior, adaptado para omitir del mensaje de comando de integridad protegida información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha red de acceso de radio adicional e información acerca de la capacidad de seguridad de dicha estación móvil multi-modo en dicha red de acceso de radio.

6. Aparato como se define en la reivindicación 1, adaptado para incluir (601) en dicho mensaje de comando de identidad protegida información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha red de acceso de radio adicional.

7. Aparato como se define en cualquier reivindicación anterior, adaptado para enviar (702, 802, 901) información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha red de acceso de radio adicional a una red principal (104).

8. Aparato como se define en cualquier reivindicación anterior, en el que dicho mensaje de comando de identidad protegida ordena a la estación móvil multi-modo cifrar comunicaciones adicionales.

9. Aparato situado en una estación móvil multi-modo, adaptado para:

- enviar (700, 800) a una primera red de acceso de radio (101) un mensaje de señalización no protegido que incluye información acerca de algoritmos de encriptación soportados por la estación móvil multi-modo (100) en una segunda red de acceso de radio (105),
- recibir desde la primera red de acceso de radio un mensaje de comando de integridad protegida que incluye información relacionada con dichos algoritmos de encriptación soportados por la estación móvil multi-modo en la segunda red de acceso de radio, comprendiendo dicho mensaje de comando de identidad protegida una carga útil y un código de autenticación de mensaje, y
- concluir (602, 705, 805, 905) si dicha información relacionada con dichos algoritmos de encriptación en dicho mensaje de comando de identidad protegida corresponde a dicha información acerca de dichos algoritmos de encriptación en dicho mensaje de señalización no protegido.

10. Aparato como se define en la reivindicación 9, en el que dicha carga útil comprende información acerca de algoritmos de encriptación, dicha estación móvil multi-modo adaptada para comparar (602) información acerca de los algoritmos de encriptación recibidos en dicha carga útil con información almacenada acerca de dichos algoritmos de encriptación soportados por la estación móvil multi-modo.

11. Aparato como se define en la reivindicación 9, adaptado para grabar el mensaje de señalización no protegido y para usar el mensaje de señalización no protegido en un algoritmo que calcula un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

12. Aparato como se define en la reivindicación 9, adaptado para grabar una carga útil del mensaje de señalización no protegido y para usar la carga útil del mensaje de señalización no protegido en un algoritmo que calcula un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

13. Aparato como se define en la reivindicación 9, adaptado para usar información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio junto con información acerca de algoritmos de encriptación para uso con dicha primera red de acceso de radio al calcular un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

14. Aparato como se define en una cualquiera de las reivindicaciones 9, 11, 12 o 13, en el que dicho mensaje de comando de identidad protegida omite información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio e información acerca de la capacidad de seguridad de dicha estación móvil multi-modo en dicha primera red de acceso de radio.

15. Aparato como se define en la reivindicación 9, en el que dicho mensaje de comando de identidad protegida comprende información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio.

16. Aparato como se define en la reivindicación 9, adaptado para enviar (700, 800) dicha información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio durante el establecimiento de la conexión.

17. Aparato como se define en cualquiera de las reivindicaciones 9 a 16, en el que dicho mensaje de comando de identidad protegida ordena a la estación móvil multi-modo cifrar comunicaciones adicionales.

18. Un método realizado por un aparato situado en una primera red de acceso de radio, que comprende:

- recibir un mensaje de comando desde una red principal que ordena a una estación móvil multi-modo cifrar la comunicación;
- componer (601, 704, 804, 904) un mensaje de comando de integridad protegida para enviar desde la primera red de acceso de radio (101) a la estación móvil multi-modo (100), incluyendo dicho mensaje de comando de identidad protegida información relacionada con los algoritmos de encriptación soportados por la estación móvil multi-modo en una segunda red de acceso de radio (105), y que incluye una carga útil y un código de autenticación de mensaje.

19. Un método como se define en la reivindicación 18, que comprende enviar (702, 802, 901) a una red principal (104) información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio.

20. Un método como se define en la reivindicación 18 o la reivindicación 19, que comprende ordenar a la estación móvil multi-modo cifrar comunicaciones adicionales con dicho mensaje de comando de identidad protegida.

21. Un método realizado por un aparato situado en una estación móvil multi-modo, que comprende:

- enviar (700, 800) desde la estación móvil multi-modo (100) a una primera red de acceso de radio (101) un mensaje de señalización no protegido que incluye información acerca de algoritmos de encriptación soportados por la estación móvil multi-modo en una segunda red de acceso de radio (105),
- recibir en la estación móvil multi-modo desde la primera red de acceso de radio un mensaje de comando de integridad protegida que incluye información relacionada con dichos algoritmos de encriptación soportados por la estación móvil multi-modo en la segunda red de acceso de radio, comprendiendo dicho mensaje de comando de identidad protegida una carga útil y un código de autenticación de mensaje, y
- concluir (602, 705, 805, 905) si dicha información relacionada con dichos algoritmos de encriptación en dicho mensaje de comando de identidad protegida corresponde a dicha información acerca de dichos algoritmos de encriptación en dicho mensaje de señalización no protegido.

22. Un método como se define en la reivindicación 21, en el que dicha carga útil comprende información acerca de algoritmos de encriptación, y que comprende la etapa de comparar (602) información acerca de los algoritmos de encriptación recibidos en dicha carga útil con información almacenada acerca de dichos algoritmos de encriptación soportados por la estación móvil multi-modo.

23. Un método como se define en la reivindicación 21, que comprende grabar el mensaje de señalización no protegido y usar el mensaje de señalización no protegido en un algoritmo que calcula un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

24. Un método como se define en la reivindicación 21, que comprende grabar una carga útil del mensaje de señalización no protegido y usar la carga útil del mensaje de señalización no protegido en un algoritmo que calcula

un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

25. Un método como se define en la reivindicación 21, que comprende usar información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio junto con información acerca de algoritmos de encriptación para uso con dicha primera red de acceso de radio al calcular un código de autenticación de mensaje esperado para el mensaje de comando de integridad protegida.

26. Un método como se define en cualquiera de las reivindicaciones 21 y 23 a 25, en el que dicho mensaje de comando de identidad protegida omite información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio e información acerca de la capacidad de seguridad de dicha estación móvil multi-modo en dicha primera red de acceso de radio.

27. Un método como se define en cualquiera de las reivindicaciones 21 a 25, en el que dicho mensaje de comando de identidad protegida comprende información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio.

28. Un método como se define en cualquiera de las reivindicaciones 21 a 27, que comprende enviar (700, 800) dicha información acerca de los algoritmos de encriptación soportados por la estación móvil multi-modo en dicha segunda red de acceso de radio durante el establecimiento de la conexión.

29. Un método como se define en cualquiera de las reivindicaciones 21 a 28, en el que dicho mensaje de comando de identidad protegida ordena a la estación móvil multi-modo cifrar comunicaciones adicionales.

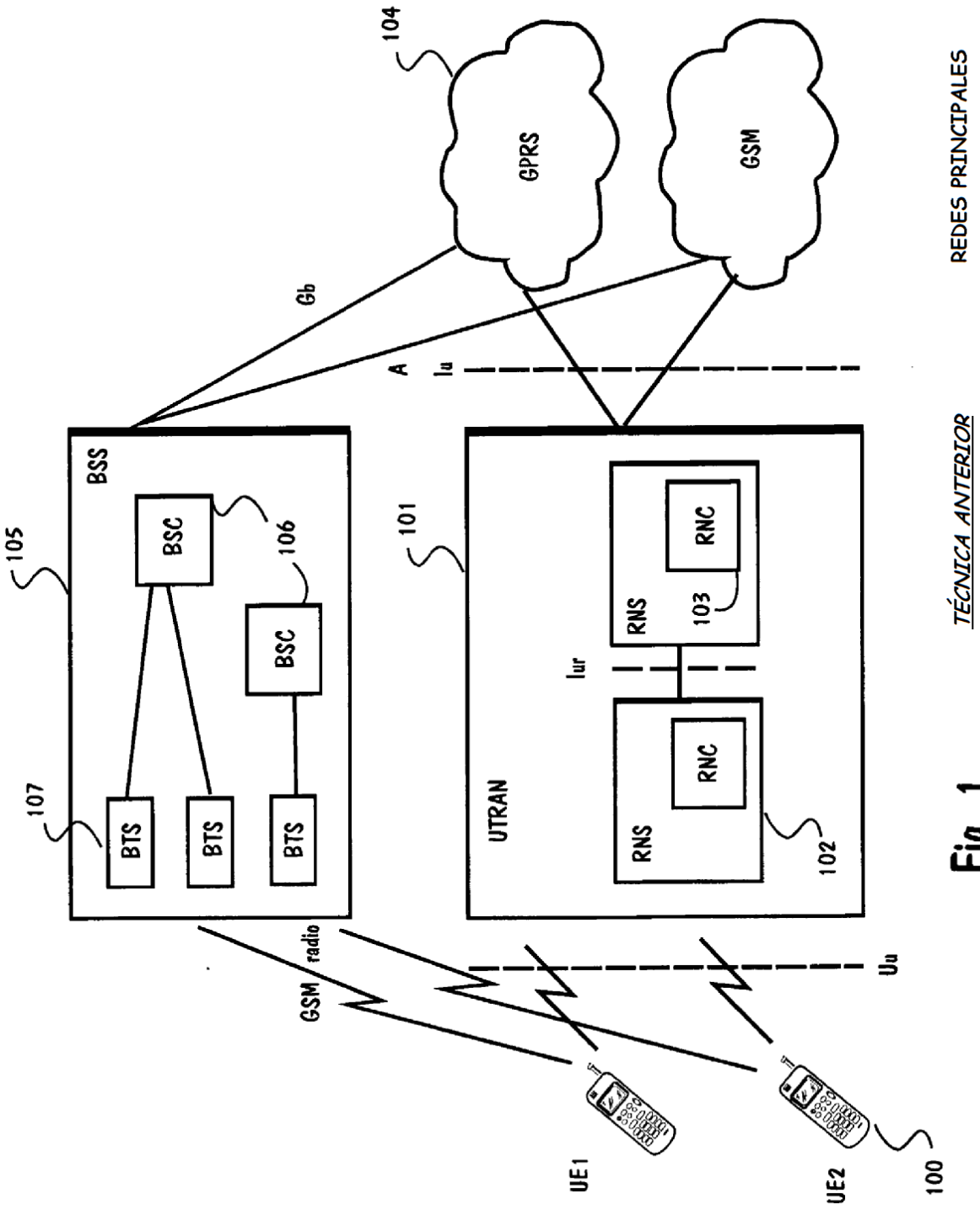
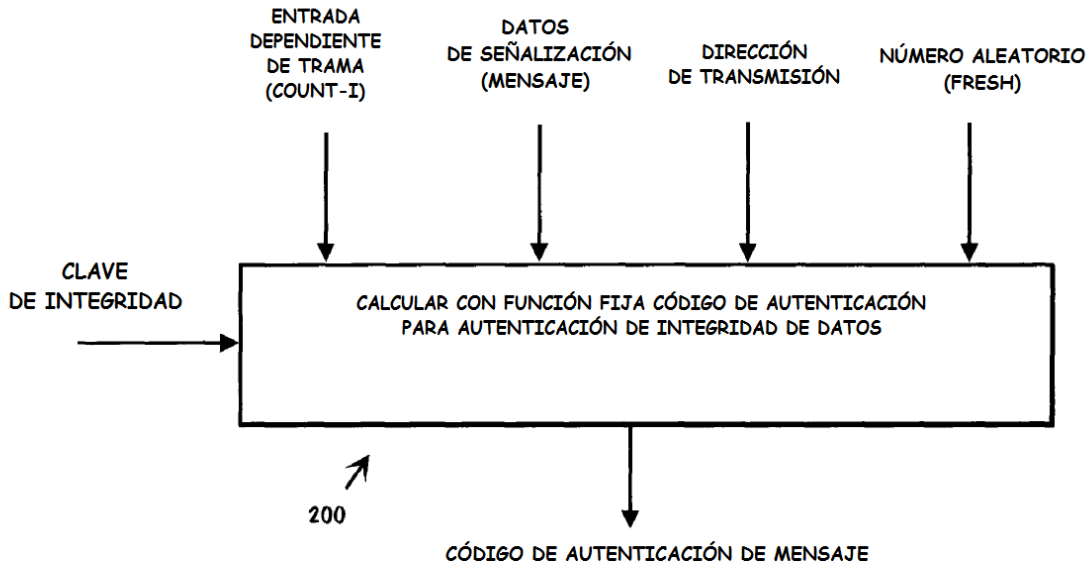
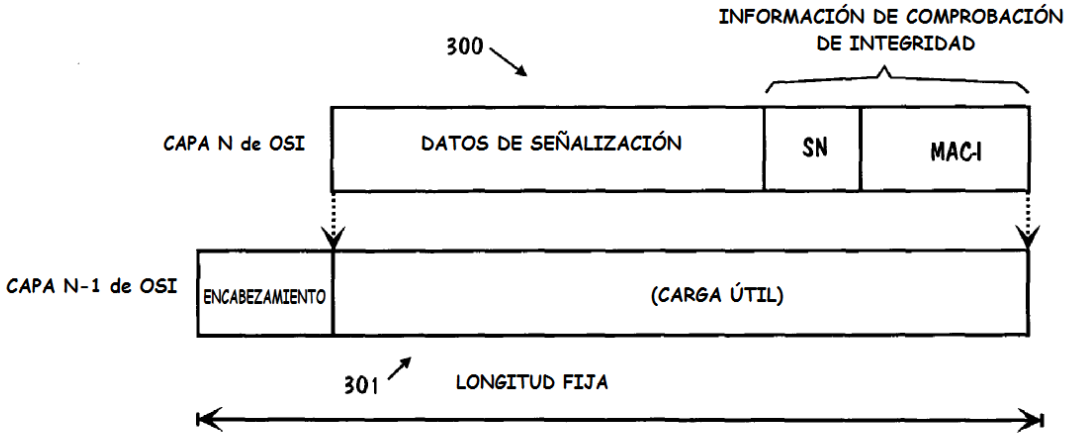

104
GPRS
GSM
REDES PRINCIPALES
Gb
A
Iu
BSS
105
BSC
106
BSC
BTS
BTS
BTS
107
101
UTRAN
RNS
RNC
103
Iur
RNS
RNC
102
TÉCNICA ANTERIOR
GSM radio
Uu
UE1
UE2
100

Fig. 1



TÉCNICA ANTERIOR

Fig. 2



TÉCNICA ANTERIOR

Fig. 3

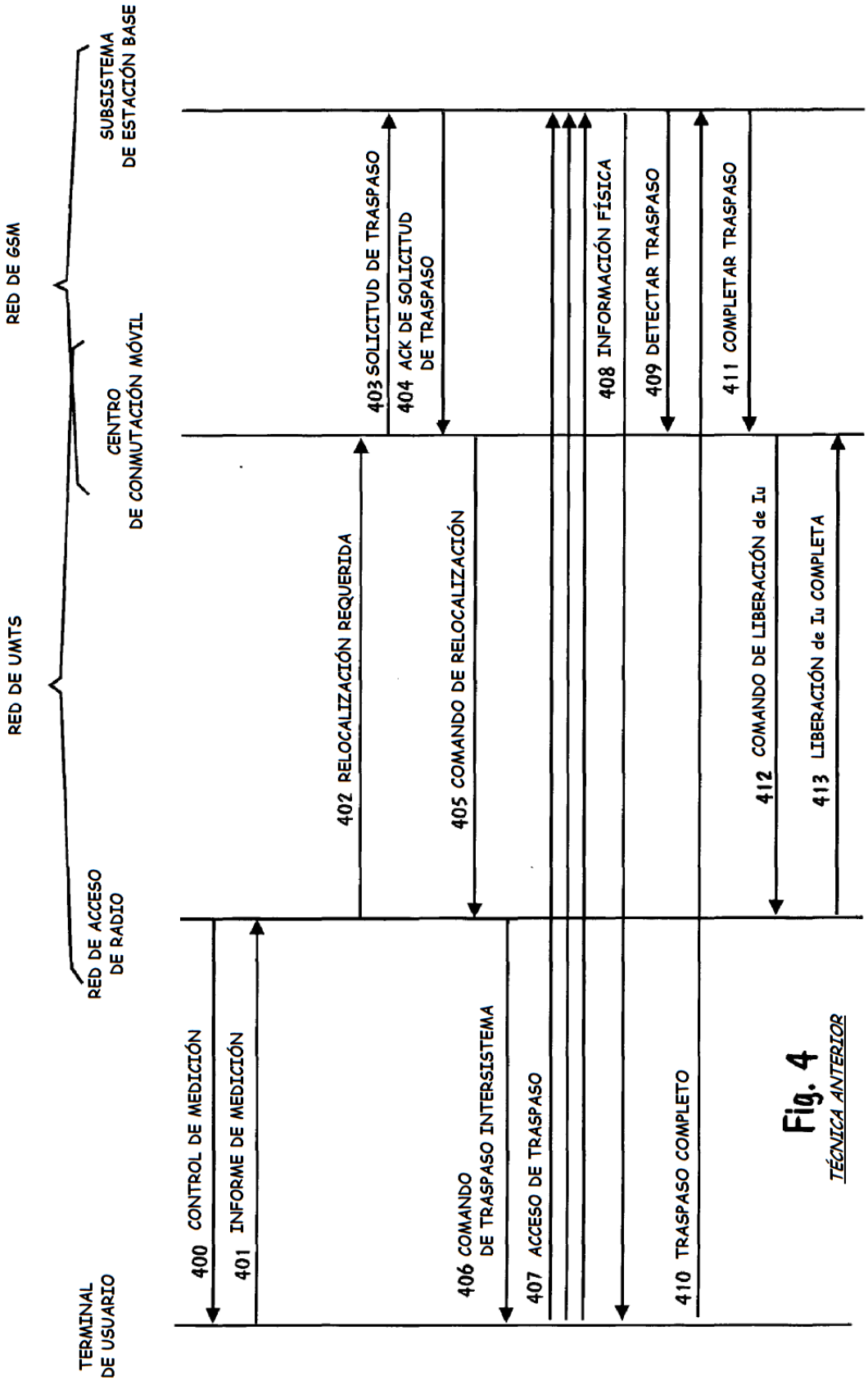


Fig. 4
TÉCNICA ANTERIOR

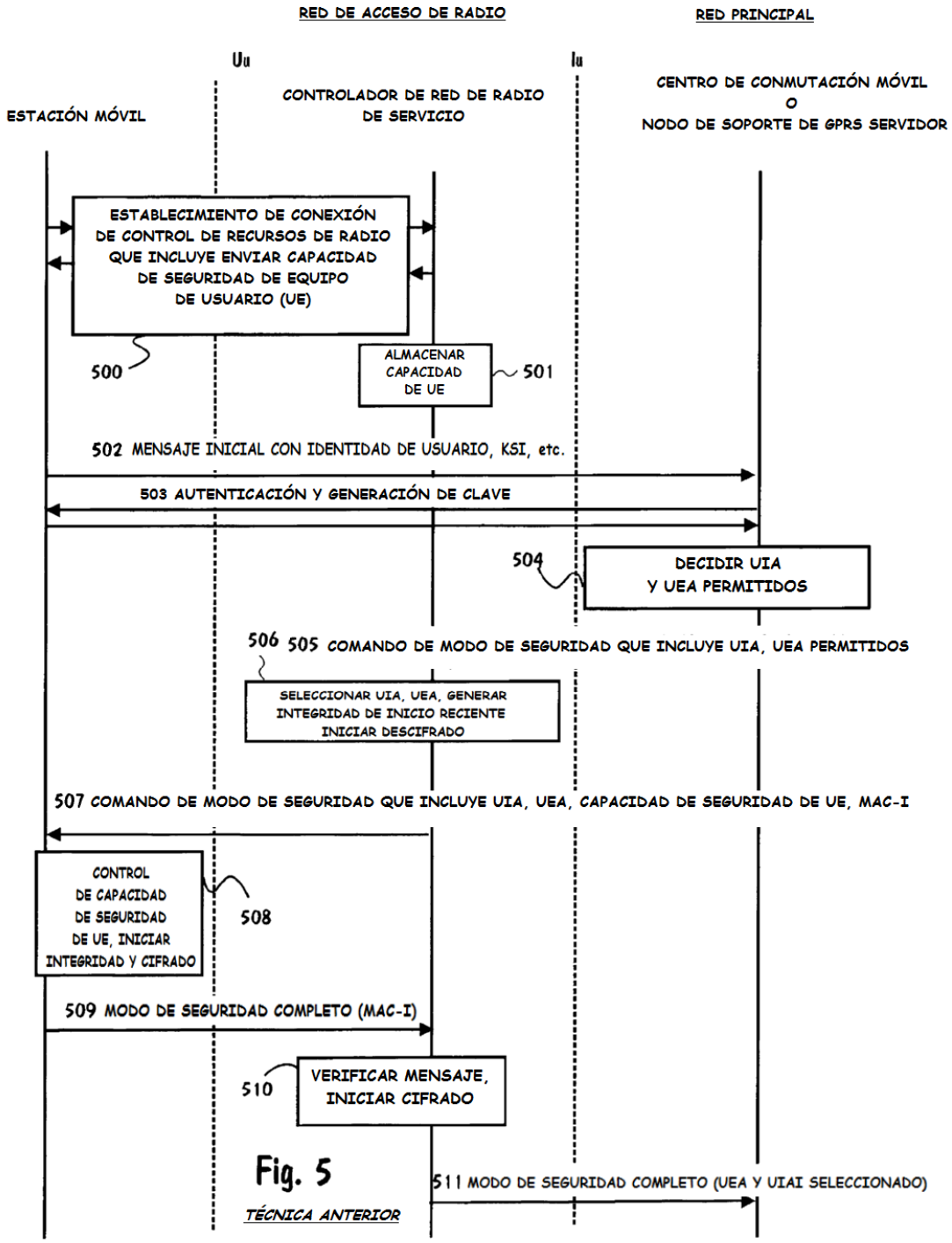
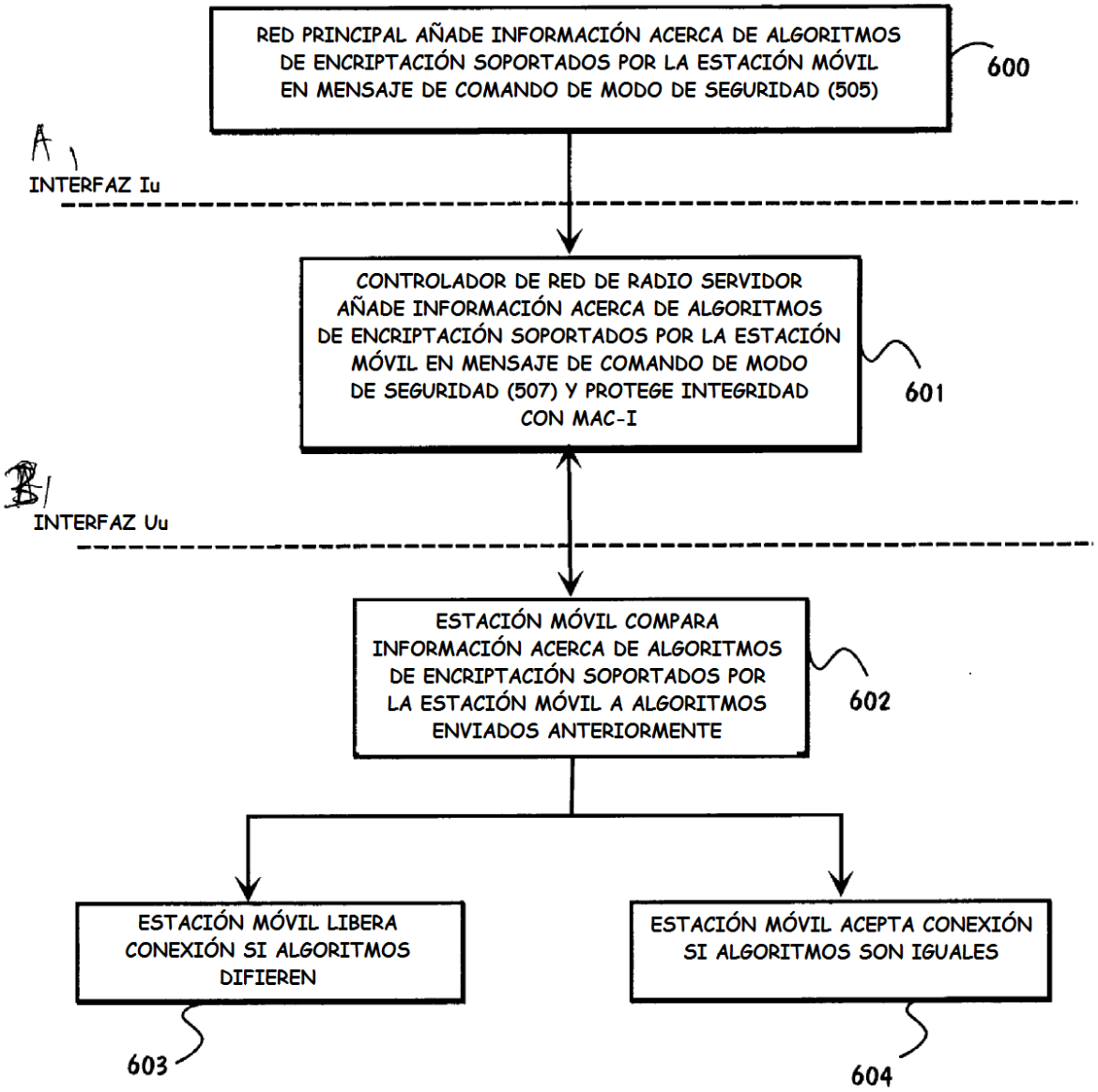


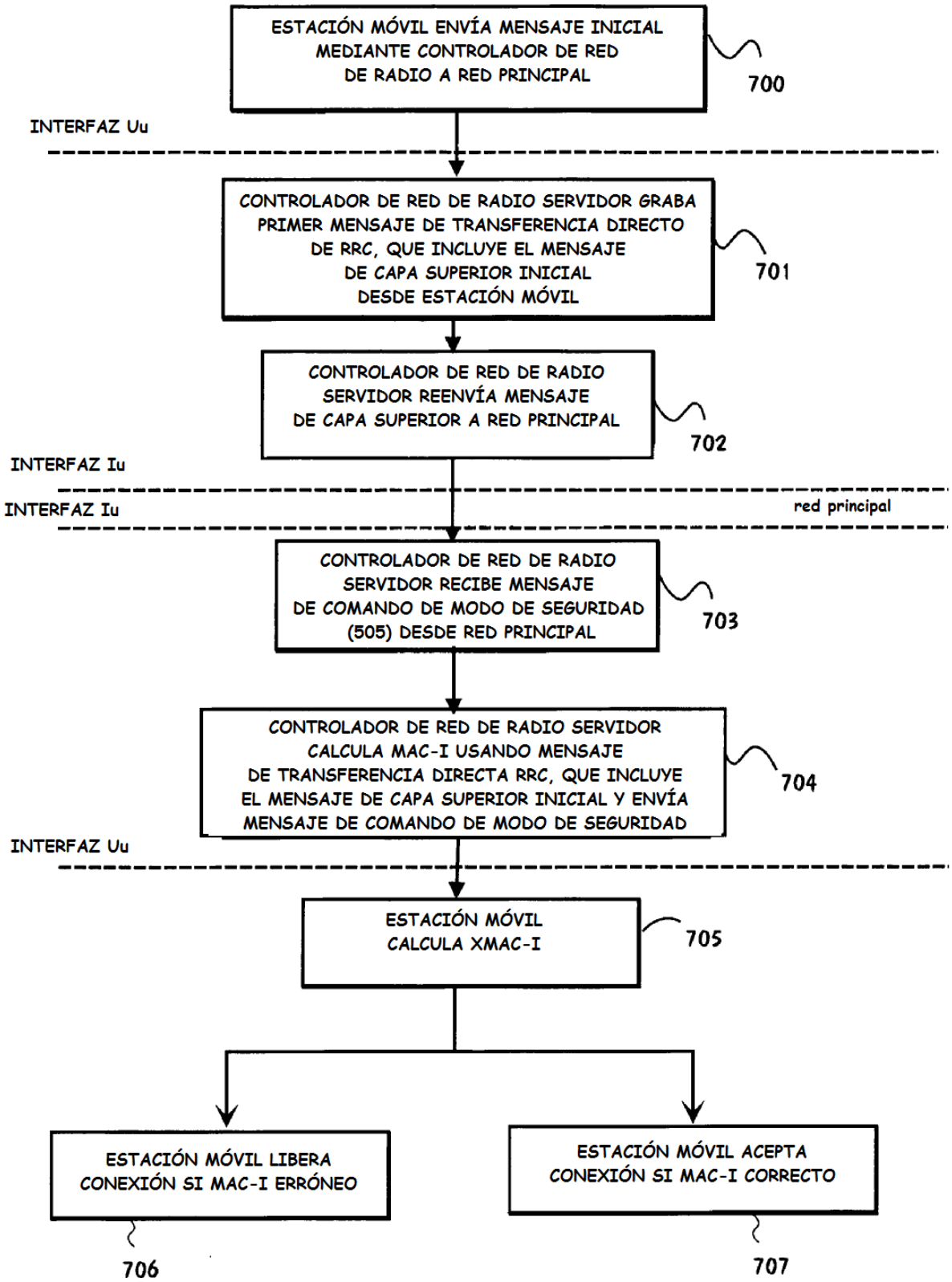
Fig. 5

TÉCNICA ANTERIOR



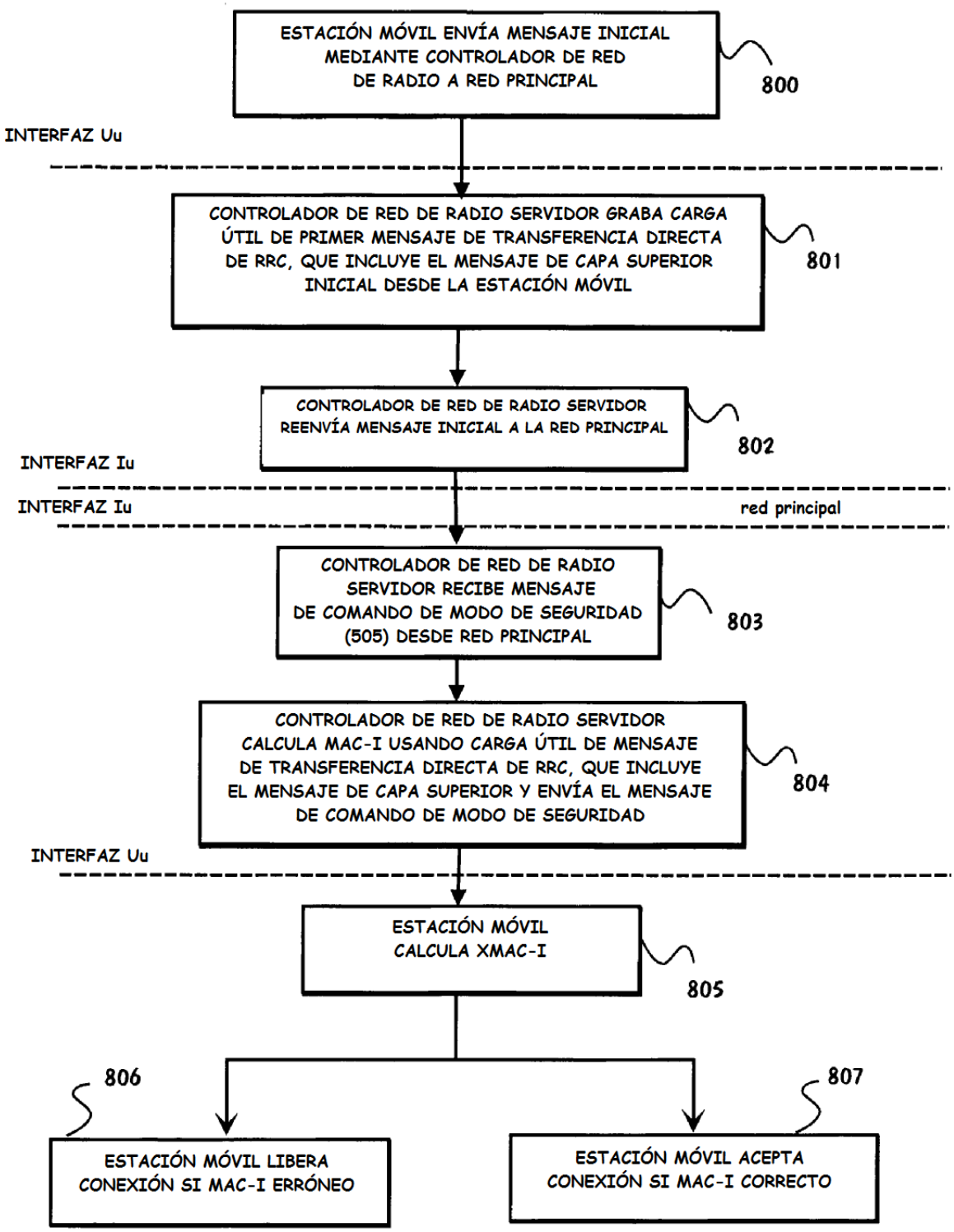
SOLUCIÓN 1

Fig. 6



SOLUCIÓN 2

Fig. 7



SOLUCIÓN 3

Fig. 8

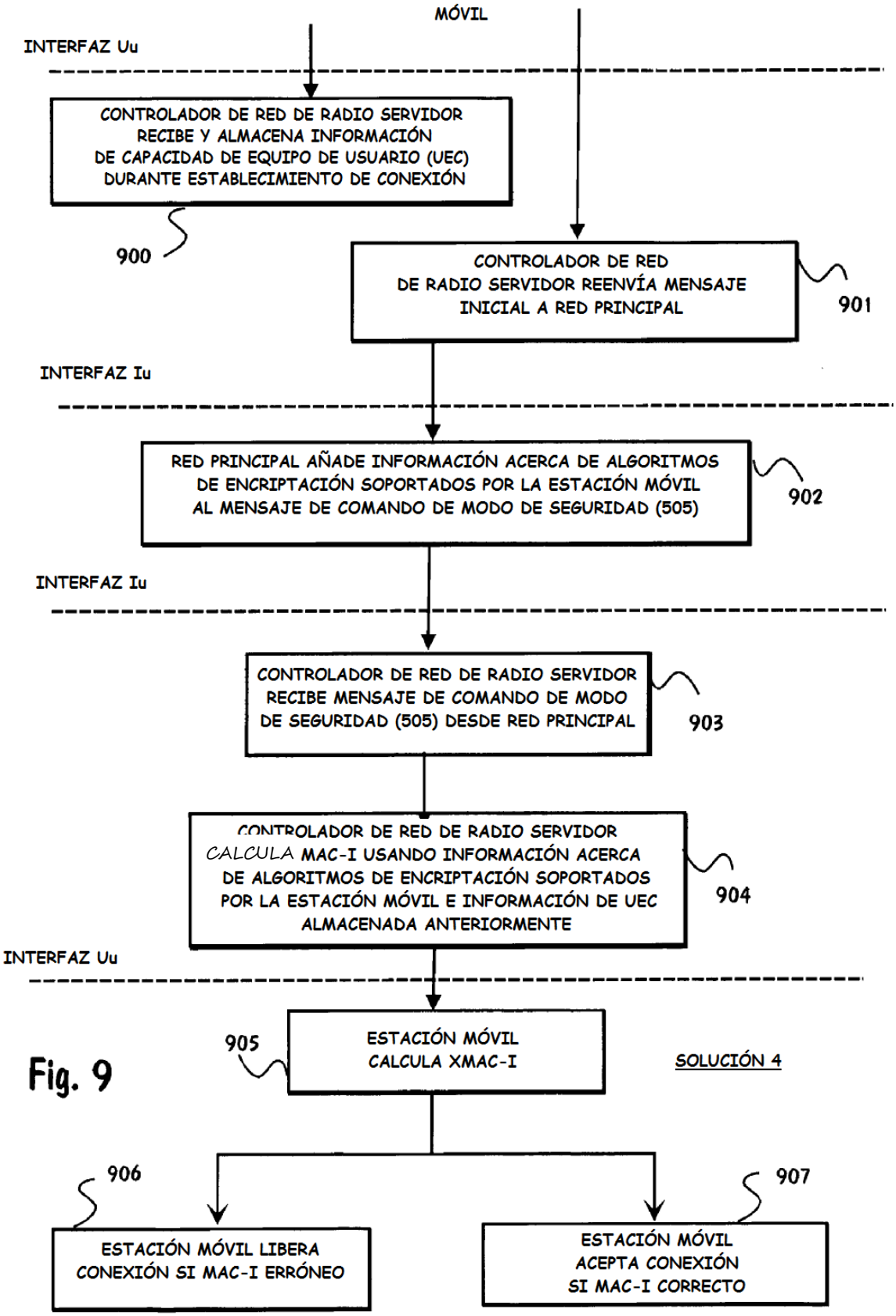

MÓVIL
INTERFAZ Uu
CONTROLADOR DE RED DE RADIO SERVIDOR RECIBE Y ALMACENA INFORMACIÓN DE CAPACIDAD DE EQUIPO DE USUARIO (UEC) DURANTE ESTABLECIMIENTO DE CONEXIÓN
900
CONTROLADOR DE RED DE RADIO SERVIDOR REENVÍA MENSAJE INICIAL A RED PRINCIPAL
901
INTERFAZ Iu
RED PRINCIPAL AÑADE INFORMACIÓN ACERCA DE ALGORITMOS DE ENCRIPTACIÓN SOPORTADOS POR LA ESTACIÓN MÓVIL AL MENSAJE DE COMANDO DE MODO DE SEGURIDAD (505)
902
INTERFAZ Iu
CONTROLADOR DE RED DE RADIO SERVIDOR RECIBE MENSAJE DE COMANDO DE MODO DE SEGURIDAD (505) DESDE RED PRINCIPAL
903
CONTROLADOR DE RED DE RADIO SERVIDOR CALCULA MAC-I USANDO INFORMACIÓN ACERCA DE ALGORITMOS DE ENCRIPTACIÓN SOPORTADOS POR LA ESTACIÓN MÓVIL E INFORMACIÓN DE UEC ALMACENADA ANTERIORMENTE
904
INTERFAZ Uu
905
ESTACIÓN MÓVIL CALCULA XMAC-I
SOLUCIÓN 4
906
ESTACIÓN MÓVIL LIBERA CONEXIÓN SI MAC-I ERRÓNEO
907
ESTACIÓN MÓVIL ACEPTA CONEXIÓN SI MAC-I CORRECTO

Fig. 9

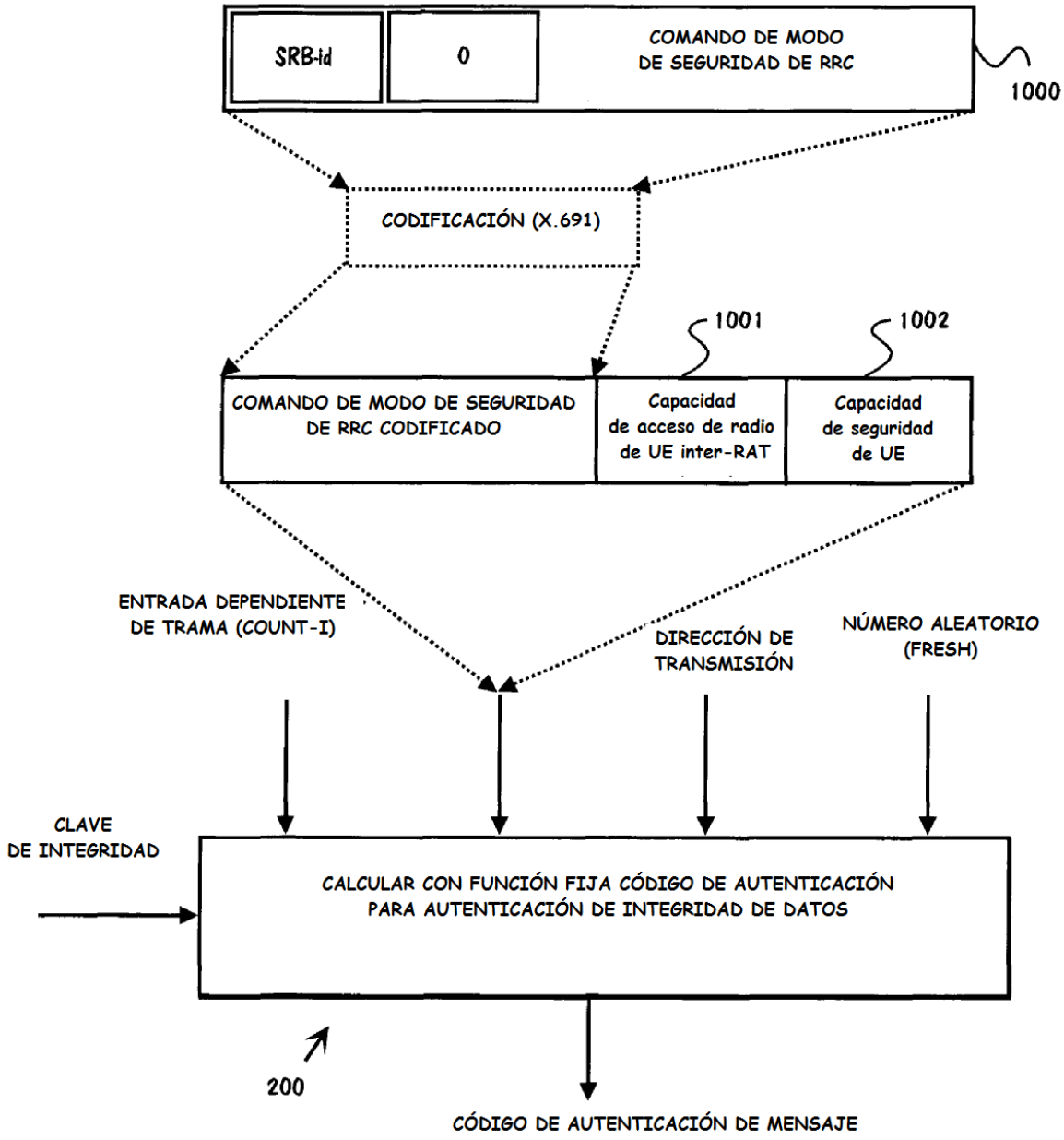

SRB-id
0
COMANDO DE MODO DE SEGURIDAD DE RRC
1000
CODIFICACIÓN (X.691)
1001
1002
COMANDO DE MODO DE SEGURIDAD DE RRC CODIFICADO
Capacidad de acceso de radio de UE inter-RAT
Capacidad de seguridad de UE
ENTRADA DEPENDIENTE DE TRAMA (COUNT-I)
DIRECCIÓN DE TRANSMISIÓN
NÚMERO ALEATORIO (FRESH)
CLAVE DE INTEGRIDAD
CALCULAR CON FUNCIÓN FIJA CÓDIGO DE AUTENTICACIÓN PARA AUTENTICACIÓN DE INTEGRIDAD DE DATOS
200
CÓDIGO DE AUTENTICACIÓN DE MENSAJE
SOLUCIÓN 6

Fig. 10

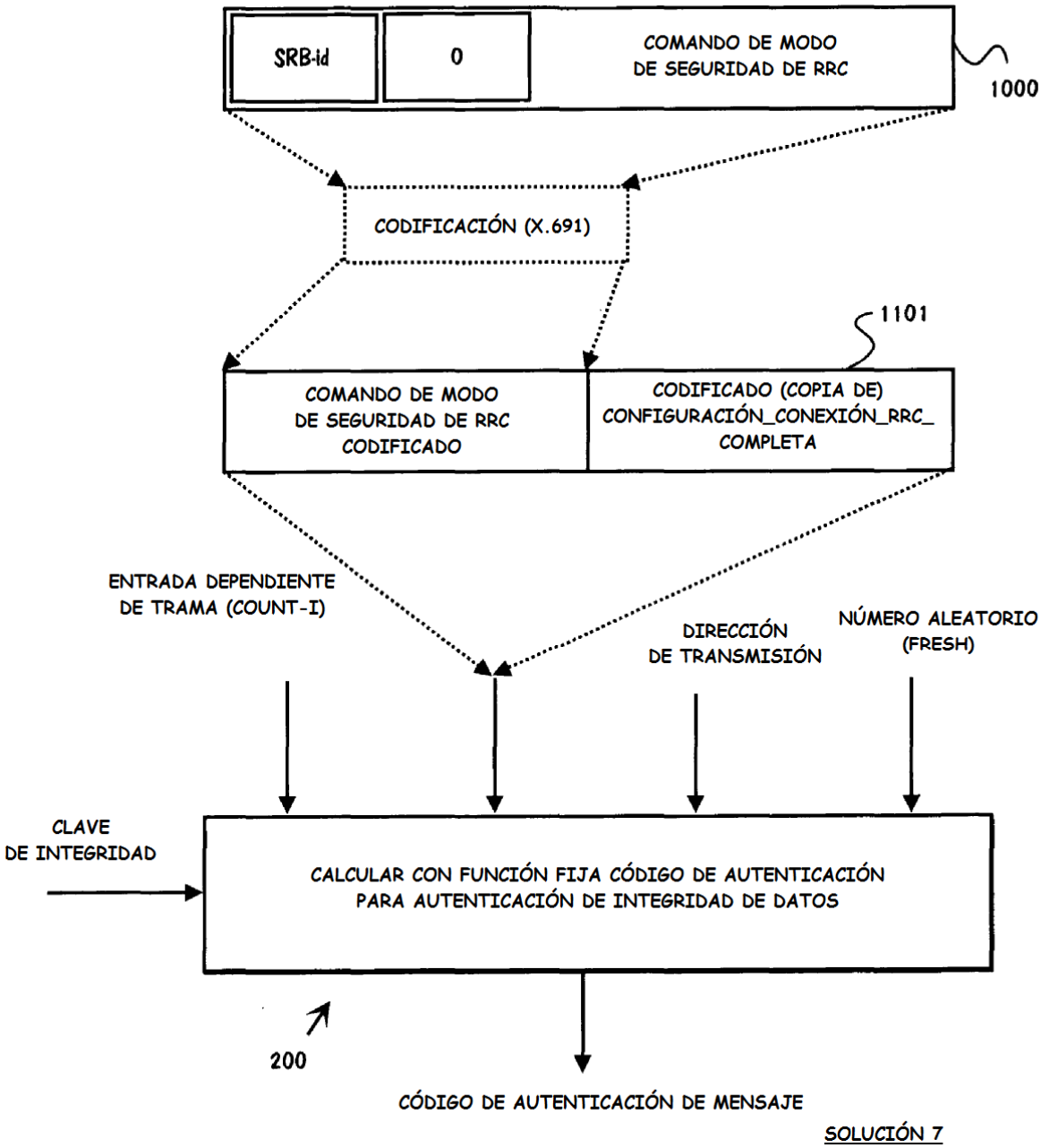

SRB-id
0
COMANDO DE MODO DE SEGURIDAD DE RRC
1000
CODIFICACIÓN (X.691)
1101
COMANDO DE MODO DE SEGURIDAD DE RRC CODIFICADO
CODIFICADO (COPIA DE) CONFIGURACIÓN_CONEXIÓN_RRC_ COMPLETA
ENTRADA DEPENDIENTE DE TRAMA (COUNT-I)
DIRECCIÓN DE TRANSMISIÓN
NÚMERO ALEATORIO (FRESH)
CLAVE DE INTEGRIDAD
CALCULAR CON FUNCIÓN FIJA CÓDIGO DE AUTENTICACIÓN PARA AUTENTICACIÓN DE INTEGRIDAD DE DATOS
200
CÓDIGO DE AUTENTICACIÓN DE MENSAJE
SOLUCIÓN 7

Fig. 11