(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 346 435**

(51) Int. Cl.:
H04W 12/06 (2006.01)
H04L 9/32 (2006.01)
H04W 12/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04075767 .6**
(96) Fecha de presentación : **23.01.2001**
(97) Número de publicación de la solicitud: **1432271**
(97) Fecha de publicación de la solicitud: **23.06.2004**

(54) Título: **Comprobación de integridad en un sistema de comunicación.**

(30) Prioridad: **22.02.2000 GB 0004178**

(45) Fecha de publicación de la mención BOPI:
15.10.2010

(45) Fecha de la publicación del folleto de la patente:
15.10.2010

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Vialen, Jukka y**
Niemi, Valtteri

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

Comprobación de integridad en un sistema de comunicación.

La presente invención se refiere a un procedimiento para comprobar la integridad de las comunicaciones entre un primer nodo y un segundo nodo. En particular, pero no exclusivamente, la invención se refiere a un procedimiento para comprobar la integridad de las comunicaciones entre una estación móvil y una red celular.

Se conocen diversas redes distintas de telecomunicación. Una red de telecomunicación es una red de telecomunicación celular, en la cual el área cubierta por la red se divide en una pluralidad de células. Cada célula está dotada de una estación base, que sirve a estaciones móviles en la célula asociada a la estación base. El equipo de usuario, tal como las estaciones móviles, recibe así señales desde, y transmite señales a, la estación base y, por ello, puede comunicarse a través de las estaciones base. El sistema celular también comprende habitualmente un controlador de estación base que controla el funcionamiento de una o más estaciones base. Al menos algunos de los equipos de usuario en el sistema pueden ser capaces de comunicarse simultáneamente por uno o más canales de comunicación.

Las telecomunicaciones están expuestas al problema de asegurar que la información recibida es enviada por un remitente autorizado, y no por un participante no autorizado que está intentando pasar por el remitente. El problema es especialmente relevante para los sistemas de telecomunicación celular, donde la interfaz aérea presenta una oportunidad potencial para que un participante espíe y reemplace el contenido de una transmisión. El documento US 4.393.269 expone un procedimiento y aparato que incorporan una secuencia de vía única para la verificación de transacciones e identidades.

Una solución para este problema es la autenticación de los participantes en la comunicación. Un proceso de autenticación intenta descubrir y comprobar la identidad de ambos participantes en la comunicación, de forma tal que cada participante reciba información acerca de la identidad del otro participante, y pueda fiarse de la identidad. La autenticación se efectúa habitualmente en un procedimiento específico al principio de una conexión. Sin embargo, este procedimiento deja espacio para la manipulación, inserción y borrado no autorizados de los mensajes subsiguientes. Hay una necesidad de una autenticación por separado de cada mensaje transmitido. Esto puede hacerse adosando un código de autenticación de mensaje (MAC-I) al mensaje en el extremo transmisor, y comprobando el valor del código MAC-I de autenticación de mensaje en el extremo receptor.

Un código MAC-I de autenticación de mensaje es habitualmente una cadena relativamente breve de bits, que depende del mensaje que protege y de una clave secreta conocida tanto por el remitente como por el destinatario del mensaje. La clave secreta se genera y acuerda durante el procedimiento de autenticación al comienzo de la conexión. En algunos casos, el algoritmo (que se usa para calcular el código MAC-I de autenticación de mensaje sobre la base de la clave secreta y el mensaje) también es secreto, pero este no es el caso normalmente.

El proceso de autenticación de mensajes individuales se llama a menudo protección de integridad. Para proteger la integridad de un mensaje, el participante transmisor calcula un valor de autenticación del mensaje sobre la base del mensaje a enviar y de la clave secreta, utilizando el algoritmo especificado, y envía el mensaje con el valor del código MAC-I de autenticación de mensaje. El participante receptor recalcula un valor del código MAC-I de autenticación de mensaje sobre la base del mensaje y la clave secreta según el algoritmo especificado, y compara el código MAC-I de autenticación de mensaje recibido con el código MAC-I de autenticación de mensaje calculado. Si los dos valores del código MAC-I de autenticación de mensaje coinciden, el destinatario puede confiar en que el mensaje está intacto y enviado por el supuesto participante.

Los esquemas de protección de integridad pueden ser atacados. Hay dos procedimientos que un participante no autorizado puede usar para falsificar un valor del código MAC-I de autenticación de mensaje, para mensajes modificados o nuevos. El primer procedimiento implica obtener la clave secreta y el segundo procedimiento implica proporcionar mensajes modificados o nuevos sin conocimiento de la clave secreta.

La clave secreta puede ser obtenida por terceros de dos maneras:

- calculando todas las claves posibles hasta que se halla una clave que coincide con datos de pares observados de códigos MAC-I de autenticación de mensaje, o bien forzando el algoritmo para producir valores de códigos MAC-I de autenticación de mensajes; o bien
- capturando directamente una clave secreta almacenada o transmitida.

Los participantes originales en la comunicación pueden impedir que un tercero obtenga la clave secreta usando un algoritmo que sea criptográficamente fuerte, usando una clave secreta lo bastante larga para impedir la búsqueda exhaustiva de todas las claves y usando un procedimiento seguro para la transmisión y almacenamiento de claves secretas.

Un tercero puede intentar perturbar el intercambio de mensajes entre los dos participantes sin una clave secreta, adivinando el valor correcto del código MAC-I de autenticación de mensaje, o bien reproduciendo algún mensaje anterior transmitido entre los dos participantes. En este último caso, el código MAC-I correcto de autenticación de mensaje para el mensaje se conoce a partir de la transmisión original. Este ataque puede ser muy útil para un tercero no autorizado. Por ejemplo, puede multiplicar el número de acciones adicionales que son favorables al intruso. Incluso las transacciones monetarias pueden repetirse de esta manera.

La correcta adivinación del valor del código MAC-I de autenticación de mensaje puede impedirse usando valores largos del código MAC-I de autenticación de mensaje. El valor MAC-I de autenticación de mensaje debería ser lo bastante largo como para reducir la probabilidad de adivinar correctamente a un nivel lo suficientemente bajo en comparación con el beneficio obtenido por una falsificación exitosa. Por ejemplo, el uso de un valor de 32 bits del código MAC-I de autenticación de mensaje reduce la probabilidad de una adivinación correcta a 1/4294967296.

Esto es lo bastante pequeño para la mayoría de las aplicaciones.

La obtención de un valor correcto del código MAC-I de autenticación de mensaje, usando el ataque por reproducción, es decir, reproduciendo un mensaje anterior, puede impedirse introduciendo un parámetro que varía con el tiempo al cálculo de los valores MAC-I de autenticación de mensaje. Por ejemplo, puede usarse un valor de sello temporal o un número de secuencia como entrada adicional al algoritmo del código MAC-I de autenticación de mensaje, además de la clave secreta de integridad y el mensaje.

En el caso en que se usa una secuencia de números como parámetros que varían con el tiempo, se usa un mecanismo que impide la posibilidad de usar el mismo número de secuencia más de una vez con la misma clave secreta. Habitualmente, ambos participantes en la comunicación mantienen un registro de los números de secuencia usados.

Si hay varios canales de comunicación en uso, todos los cuales utilizan la misma clave secreta, surge el siguiente problema. Un mensaje en un canal de comunicación asociado a un número de secuencia dado, por ejemplo n, puede repetirse en otro canal de comunicación en un momento adecuado, es decir, toda vez que el número n de secuencia es aceptable en el otro canal.

Se ha propuesto aplicar el cifrado y la protección de integridad en el sistema UMTS para el estándar de tercera generación. Sin embargo, el procedimiento que se ha propuesto permite que el mensaje idéntico se envíe por dos distintos portadores de radio de señalización en distintos momentos. Esto hace que el sistema sea vulnerable a ataques del hombre de la calle. En particular, tal sistema puede ser vulnerable al "ataque por reproducción" descrito anteriormente.

Habitualmente, un único mensaje de señalización repetido no brinda una ventaja significativa al tercero no autorizado, pero es posible que el tercero pudiera intentar repetir un diálogo más largo, por ejemplo, a fin de establecer una llamada adicional y, así, robar partes de una conexión.

El documento ETSI: "Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3GPP TS 33, 102 version 3.3.1 Release 1999)" ["Sistema Universal de Telecomunicaciones Móviles (UMTS); Seguridad 3G; Arquitectura de Seguridad (3GPP TS 33, 102 versión 3.3.1 Edición 1999"], ETSI TS 133 102 V3.3.1, de Enero de 2000 (2000-01), páginas 1-64, XP002225628, describe en detalle un procedimiento de seguridad para su uso en un sistema de telecomunicaciones 3G.

Es un objetivo de las realizaciones de la presente invención abordar uno o más de los problemas anteriormente expuestos.

Según un aspecto de la presente invención, se proporciona un nodo para su uso en un sistema que comprende dicho nodo y un nodo adicional, proporcionándose una pluralidad de distintos canales de comunicación entre dichos nodos, y teniendo cada canal de comunicación una identidad distinta. Este nodo está caracterizado por comprender medios para calcular un código de autenticación a partir de una pluralidad de valores, siendo algunos de esos valores los mismos para dicha pluralidad de distintos canales de comunicación, estando dispuesto al menos uno de dichos valores para comprender información relacionada con la identidad de un canal de comunicación de dicha pluralidad de canales de comunicación, medios para recibir información con respecto a un código de autenticación calculado por dicho nodo adicional, y medios para comparar información relacionada con un código de autenticación calculado por dicho nodo con información relacionada con un código de autenticación calculado por el nodo adicional.

Según otro aspecto de la presente invención, se proporciona un procedimiento para llevar a cabo una comprobación de integridad en un sistema que comprende un nodo y un nodo adicional, proporcionándose una pluralidad de canales de comunicación entre dicho nodo y dicho nodo adicional, teniendo cada canal de comunicación una identidad distinta. El procedimiento se caracteriza por las etapas de recibir en el nodo información relacionada con un código de autenticación desde el nodo adicional, calcular un código de autenticación adicional usando una pluralidad de valores, siendo algunos de dichos valores los mismos para dicha pluralidad de distintos canales de comunicación, estando al menos uno de dichos valores dispuesto para comprender información relacionada con la identidad de un canal de comunicación de dicha pluralidad de canales, y comparar el código de autenticación adicional con dicha información relacionada con un código de autenticación recibido desde el nodo adicional.

Según otro aspecto de la presente invención, se proporciona un sistema de comunicación que comprende un nodo según lo anteriormente descrito, y dispuesto para funcionar según el procedimiento anteriormente descrito.

Pueden lograrse varias ventajas por las realizaciones de la invención. En la solución de la presente invención, el ataque por reproducción puede impedirse también en el caso en que se usan varios canales de comunicación paralelos. Una ventaja es que las realizaciones pueden aplicarse flexiblemente a cualquier sistema que utiliza canales de comunicación paralelos dentro de una conexión. La realización de la presente invención puede mejorar la seguridad del usuario en sistemas de comunicación, especialmente en sistemas de comunicación inalámbrica. Las realizaciones pueden garantizar que los canales de comunicación paralelos dentro de una conexión nunca usarán el mismo conjunto de parámetros de entrada para calcular el código MAC-I de autenticación de mensaje.

Para una mejor comprensión de la presente invención, y de cómo la misma puede llevarse a cabo, se hará ahora referencia, a modo de ejemplo, a los dibujos adjuntos, en los cuales:

La Figura 1 muestra elementos de una red celular con la cual pueden usarse realizaciones de la presente invención;

La Figura 2 muestra la arquitectura del protocolo Uu de interfaz de radio entre el equipo UE de usuario y el Nodo B, y entre el equipo UE de usuario y el controlador RNC de red de radio de la Figura 1;

La Figura 3 ilustra esquemáticamente la función de protección de integridad;

La Figura 4 muestra la función de protección de integridad modificada de acuerdo a realizaciones de la presente invención;

La Figura 5 muestra la función de protección de integridad modificada de acuerdo a una realización adicional de la invención;

La Figura 6 muestra una realización adicional de la presente invención;

La Figura 7 muestra un procedimiento de autenticación y acuerdo de claves;

La Figura 8 muestra la generación de vectores de autenticación; y

La Figura 9 muestra un ejemplo de función de autenticación de usuario en un USIM (Módulo de Identidad de Servicios de Usuario), de acuerdo a una realización de la presente invención.

Con referencia a la Figura 1, se describirá una típica estructura de sistema de telefonía móvil. Las partes principales del sistema de telefonía móvil son: una red central CN 2, una red de acceso terrestre por radio del UMTS (UTRAN) 4, y un equipo UE 6 de usuario. La red central CN 2 puede estar conectada con redes externas 8, que pueden bien ser redes 81 Conmutadas por Circuitos (CS) (p. ej., PLMN, PSTN, ISDN) o redes 82 Conmutadas por Paquetes (PS) (p. ej., Internet). La interfaz entre la red central CN2 y la red de acceso terrestre por radio del UMTS, UTRAN 4, se llama la interfaz Iu, y la interfaz entre la red de acceso terrestre por radio del UMTS, UTRAN 4, y el equipo UE 6 de usuario se llama la interfaz Uu. Como se muestra en la Figura 1, el RNC está conectado con dos nodos de la CN (MSC/VLR y SGSN). En algunas topologías de red puede ser posible que un RNC esté conectado con un nodo de la CN o con más de dos nodos de la CN.

La red central CN 2 se compone de un Registro de Ubicación Local HLR 10, un Centro de Conmutación de Servicios Móviles/Registro de Ubicación de Visitante, MSC/VLR 12, un MSC de Pasarela, GMSC 14, un Nodo Servidor de Soporte del GPRS (Servicio General de Radio en Paquetes), SGSN 16, y un Nodo de Pasarela de Soporte del GPRS, GGSN 18.

La UTRAN 14 se compone de los subsistemas de red de radio RNS 20 y 22. La interfaz entre dos subsistemas RNS de red de radio se llama la interfaz Iur. Los subsistemas de red de radio RNS 20 y 22 se componen de un controlador de red de radio, RNC 24, y uno más nodos B 26. La interfaz entre el controlador de red de radio, RNC 24, y el nodo B 26 se llama la interfaz Iub.

El Controlador de Red de Radio, RNC 24, es el elemento de red responsable del control de los recursos de radio de la UTRAN 4. El RNC 24 mantiene una interfaz con la red central CN 2 (normalmente, con un MSC 12 y un SGSN 16) y también termina el protocolo de Control de Recursos de Radio, RRC, que define los mensajes y procedimientos entre el equipo UE 6 de usuario y la UTRAN 4. El RNC 24 corresponde lógicamente al controlador de estación base del estándar GSM (sistema global para comunicaciones móviles).

La función principal del Nodo B 26 es efectuar el procesamiento de la interfaz aérea L1 (codificación e intercalación de canal, adaptación de velocidad, expansión, etc.). También efectúa alguna operación básica de Gestión de Recursos de Radio, tal como el control de potencia del bucle interno. Corresponde lógicamente a la Estación Transceptora Base del estándar GSM.

El equipo UE 6 de usuario consiste en dos partes: el Equipo Móvil ME 30 y el Módulo de Identidad de Abonado del UMTS, USIM 32. El equipo móvil ME es el terminal de radio usado para la comunicación de radio por la interfaz Uu entre el equipo UE 6 de usuario y la UTRAN 4. El USIM 32 es una tarjeta inteligente que guarda la identidad del abonado, realiza algoritmos de autenticación y almacena claves de autenticación y cifrado y alguna información de abonado que se necesita en el terminal.

Con referencia a la Figura 2, se describirá la arquitectura del protocolo de interfaz de radio según las especificaciones 3GPP. Las entidades de protocolo descritas funcionan entre:

el equipo UE 6 de usuario y el Nodo B 26, y/o

el equipo UE 6 de usuario y el RNC 24.

La división de capas de protocolo entre el Nodo B 26 y el RNC 24 no se describe aquí adicionalmente.

Los protocolos de interfaz de radio pueden dividirse entre un plano 50 de control y un plano 52 de usuario. El plano 50 de control se usa para toda señalización entre el UE 6 y el RNC 24, y también entre el equipo UE 6 de usuario y la red central CN 2. El plano de usuario lleva los datos de usuario efectivos. Algunos de los protocolos de interfaz de radio funcionan sólo en un plano, mientras que algunos protocolos funcionan en ambos planos.

Los protocolos de interfaz de radio pueden dividirse en capas, que son la capa 1 L1 54 (también llamada la capa física), la capa 2 L2 56 (también llamada la capa del enlace de datos) y la capa 3 L3 58 (también llamada la capa de red). Algunas capas contienen sólo un protocolo, mientras que algunas capas contienen varios protocolos distintos.

La capa física L1 54 ofrece servicios a la capa 60 de Control de Acceso al Medio (MAC), mediante canales de transporte que se caracterizan por cómo y con qué características se transfieren los datos.

La capa 60 de Control de Acceso al Medio (MAC), a su vez, ofrece servicios a la capa 62 de control del enlace de radio, RLC, por medio de canales lógicos. Los canales lógicos se caracterizan por el tipo de datos que se transmiten. En la capa 60 de control de acceso al medio, MAC, los canales lógicos se asocian a los canales de transporte.

La capa 62 de Control del Enlace de Radio, RLC, ofrece servicios a las capas superiores mediante los puntos SAP de acceso a servicios, que describen cómo la capa 62 de control del enlace de radio, RLC, gestiona los paquetes de datos y, por ejemplo, si se usa una función de solicitud de repetición automática (ARQ). En el plano 50 de control, los servicios de control del enlace de radio, RLC, son usados por la capa 64 de control de recursos de radio, RRC, para el transporte de señalización. Normalmente, un mínimo de tres entidades de control del enlace de radio, RLC 62, se involucran para el transporte de señalización - una entidad en modalidad transparente, una en modalidad sin acuse de recibo y una en modalidad con acuse de recibo. En el plano 52 de usuario, los servicios de RLC son usados bien por las capas de protocolo específicas del servicio - el protocolo PDCP 66 de convergencia de datos en paquetes o el control de difusión-multidifusión BMC 68 - o bien por otras funciones del plano de usuario de capas superiores (p. ej., códecs de voz). Los servicios del RLC se llaman Portadores de Radio de Señalización en el plano de control y Portadores de Radio en el plano de usuario, para servicios que no utilizan los protocolos PDCP o BMC.

El Protocolo de Convergencia de Datos en Paquetes (PCDP) existe sólo para los servicios del dominio conmutado por paquetes, PS (servicios encaminados

mediante el SGSN) y su principal función es la compresión de cabeceras, lo que significa compresión de información redundante de control del protocolo (p. ej., cabeceras de TCP/IP y RTP/UDP/IP) en la entidad transmisora y descompresión en la entidad receptora. Los servicios ofrecidos por el PDCP se llaman Portadores de Radio.

El protocolo de Control de Difusión-Multidifusión (BMC) existe sólo para el servicio de Difusión Celular del servicio de mensajes breves, SMS, que deriva del GSM. El servicio ofrecido por el protocolo BMC también se llama un Portador de Radio.

La capa 64 del RRC ofrece servicios a las capas superiores (al Estrato No de Acceso) mediante puntos de acceso al servicio. Toda la señalización de capas superiores entre el equipo UE 6 de usuario y la red central CN 2 (gestión de movilidad, control de llamadas, gestión de sesiones, etc.) se encapsula en mensajes del RRC para su transmisión por la interfaz de radio.

Las interfaces de control entre el RRC 64 y todos los protocolos de capas inferiores son usadas por la capa 64 del RRC para configurar características de las entidades de protocolos de capas inferiores, incluyendo parámetros para los canales físicos, de transporte y lógicos. Las mismas interfaces de control son usadas por la capa 64 del RRC, p. ej., para ordenar a las capas inferiores que realicen ciertos tipos de mediciones, y por las capas inferiores para informar de resultados y errores de medición al RRC.

La realización de la invención se describe en el contexto de un UMTS (Sistema Universal de Telecomunicaciones Móviles). La presente invención es aplicable a todos los tipos de comunicación, p. ej., señalización, servicios en tiempo real y servicios no en tiempo real. Sin embargo, debería apreciarse que las realizaciones de la presente invención son aplicables a cualquier otro sistema.

En la propuesta para el estándar del UMTS para la tercera generación, el SGSN 16, y el equipo UE 6 de usuario, por ejemplo, una estación móvil, tienen una capa superior L3 que brinda soporte a la gestión de movilidad, MM (a veces llamada GMM) y a la gestión de sesiones, SM. Esta capa superior también brinda soporte al servicio de mensajes breves SMS. Estos protocolos L3 de capas superiores derivan del sistema GPRS de segunda generación. El SMS brinda soporte al servicio de mensajes breves, originado en móviles y terminado en móviles, descrito en la especificación de tercera generación 3GPP TS 23.040. La función de gestión de movilidad gestiona la ubicación de la estación móvil, es decir, la anexión de la estación móvil a la red, y la autenticación. Así, la MM brinda soporte a funcionalidad de gestión de movilidad tal como la anexión, desconexión, seguridad (p. ej., autenticación) y actualizaciones de encaminamiento. De acuerdo a una realización, las claves de integridad pueden calcularse durante el procedimiento de autenticación de la MM. Una realización ejemplificadora de este aspecto de la presente invención se explicará en más detalle más adelante.

El SGSN 16 y el RNS 20 tienen una capa del Protocolo de Aplicación de Red de Acceso por Radio (RANAP). Este protocolo se usa para controlar los portadores de interfaces Iu, pero también encapsula y transporta señalización de capas superiores. RANAP gestiona la señalización entre el SGSN 16 y el RNS 20. RANAP se especifica en la especificación de tercera generación 3GPP TS 25.413. Tanto la estación móvil 6 como el RNS 20 tienen un protocolo de control de recursos de radio, RRC, que proporciona control de portadores de radio por la interfaz de radio, por ejemplo, para la transmisión de mensajes de señalización de capas superiores y mensajes del SMS. Esta capa gestiona la mayor parte de la comunicación entre la estación móvil 6 y el RNC 24. Un RRC está especificado, por ejemplo, en la especificación de tercera generación 3GPP TS 25.331.

Los mensajes de MM, SM y SMS se envían desde el SGSN 16 al RNS 20, encapsulados en un mensaje del protocolo RANAP (el mensaje se llama Transferencia Directa en las especificaciones 3GPP). El paquete es remitido por la capa RANAP del RNC 24 a la capa RRC del RNC 24. La función de retransmisión en el RNS 20 arranca efectivamente las cabeceras del RANAP y remite la carga útil al protocolo del RRC, usando una primitiva adecuada, de forma tal que la capa RRC sepa que este es un mensaje de capas superiores que debe ser remitido a la estación móvil 6. El RNC 24 inserta una suma de control de integridad al mensaje (RRC) que lleva el mensaje de capas superiores, en la carga útil (el mensaje del RRC se llama Transferencia Directa en las especificaciones 3GPP). El RNC 24 también puede cifrar el mensaje. Esto se describirá en más detalle más adelante en el presente documento. El RNS 20 remite el paquete, mediante la interfaz aérea, a la estación móvil 6.

En la dirección originada en el móvil, la capa de RRC de la estación móvil 6 recibe el mensaje de capas superiores, lo encapsula en un mensaje de Transferencia Directa del RRC y le añade un código de autenticación de mensaje ante de enviarlo al RNS 20. El mensaje es retransmitido desde la capa del RRC a la capa RANAP del RNS 20. El RNS 20 comprueba la información asociada al mensaje, para ver si la integridad del paquete ha sido comprobada.

El procedimiento de comprobación de integridad se describirá ahora. La mayoría de los elementos de información del control de recursos de radio, RRC, la gestión de movilidad, MM, y la gestión de sesiones, SM (así como otros protocolos de capas superiores 3) se consideran sensibles y su integridad debe protegerse. Debido a esto, una función de integridad puede aplicarse sobre la mayoría de los mensajes de señalización del RRC transmitidos entre la estación móvil y el RNS 20. Sin embargo, esos mensajes del RRC que se envían antes de que se conozca la clave de integridad pueden ignorarse. Esta función de integridad usa un algoritmo de integridad con la clave IK de integridad para calcular un código de autenticación de mensaje para un mensaje dado. Esto se lleva a cabo en la estación móvil y el RNS, que tienen ambos la clave IK de integridad y el algoritmo de integridad.

Se hace referencia a la Figura 3, que ilustra el uso del algoritmo de integridad para calcular el código MAC-I de autenticación de mensaje.

Los parámetros de entrada al algoritmo son la clave IK de integridad, una entrada CONTADOR-I dependiente de la hora o del número de mensaje, un valor aleatorio generado por la red, REFRESCO, el bit DIRECCIÓN de dirección y el MENSAJE de datos de señalización. La última entrada es el mensaje o paquete de datos. Sobre la base de estos parámetros de entrada, un código de autenticación de mensaje para la integridad de datos (MAC-I) es calculado por el algoritmo UIA de integridad. Este código MAC-I se

adosa luego al mensaje antes de enviarlo por la interfaz aérea, bien a o desde la estación móvil.

El receptor de ese código y mensaje también calcula un código de autenticación de mensaje para la integridad, XMAC-I, sobre el mensaje recibido, utilizando el mismo algoritmo UIA. El algoritmo UIA tiene las mismas entradas que en el extremo remitente del mensaje. Los códigos calculados por el algoritmo en el extremo remitente (MAC-I) y en el extremo receptor (XMAC-I) deberían ser el mismo si ha de verificarse la integridad de datos del mensaje.

El parámetro CONTADOR-I de entrada es un valor incrementado en uno para cada mensaje de integridad protegida. CONTADOR-I consiste en dos partes: el número de hipertrama (HFN) como la parte más significativa y un número de secuencia de mensaje como la parte menos significativa. El valor inicial del número de hipertrama es enviado por la estación móvil a la red durante un establecimiento de conexión. Al liberarse la conexión, la estación móvil almacena el mayor número usado de hipertrama de la conexión y lo incrementa en uno. Este valor se usa luego como el valor inicial de HFN para la próxima conexión. De esta manera, el usuario se asegura de que ningún valor de CONTADOR-I sea reutilizado (por la red) con la misma clave de integridad para distintas conexiones. Después de un procedimiento de (re-)autenticación, cuando una nueva IK se genera y se pone en uso, el valor de HFN puede reiniciarse en cero.

El parámetro REFRESCO de entrada protege a la red contra la reproducción de mensajes de señalización por parte de la estación móvil. En el establecimiento de conexión, la red genera un valor aleatorio de REFRESCO y lo envía al usuario. El valor de REFRESCO es usado a continuación tanto por la red como por la estación móvil, a lo largo de la duración de una conexión individual. Este mecanismo garantiza a la red que la estación móvil no está reproduciendo algún antiguo código MAC-I de autenticación de mensaje de una conexión previa.

La configuración de la clave IK de integridad es como se ha descrito en el presente documento. La clave puede cambiarse con tanta frecuencia como desee el operador de la red. La configuración de clave puede tener lugar en cuanto se conoce la identidad del abonado móvil. La clave IK se almacena en el registro de ubicación de visitante y se transfiere al RNC cuando se necesita. La clave IK también se almacena en la estación móvil hasta que se actualiza en la próxima autenticación.

Un identificador de conjunto de claves, KSI, es un número que está asociado con las claves de cifrado e integridad derivadas durante el procedimiento de autenticación. Se almacena junto con las claves de cifrado e integridad en la estación móvil, MS, y en la red. El identificador de conjunto de claves se usa para permitir la reutilización de claves durante establecimientos subsiguientes de conexión. El KSI se usa para verificar si la MS y la red han de usar las mismas claves de cifrado y claves de integridad.

Se proporciona un mecanismo para garantizar que una clave de integridad específica no se use durante un periodo ilimitado de tiempo, para evitar ataques utilizando claves comprometidas. La autenticación que genera claves de integridad no es obligatoria en el establecimiento de conexión.

La estación móvil está dispuesta para activar la generación de una nueva clave de cifrado y una clave de integridad si el contador alcanza un máximo valor fijado por el operador, y almacenado en la estación móvil, en el próximo mensaje despachado de solicitud de conexión del RRC. Este mecanismo garantizará que una clave de integridad y una clave de cifrado no puedan reutilizarse más veces que el límite fijado por el operador.

Debería apreciarse que puede haber más de un algoritmo de integridad, y que la información se intercambia entre la estación móvil y los controladores de red de radio que definen el algoritmo. Debería observarse que el mismo algoritmo debería ser usado por el remitente y el receptor de los mensajes.

Cuando una estación móvil desea establecer una conexión con la red, la estación móvil indicará a la red qué versión, o versiones, del algoritmo, cuentan con soporte de la MS. Este mismo mensaje debe tener su integridad protegida, y se transmite al RNC después de que el procedimiento de autenticación esté completado.

La red comparará sus capacidades y preferencias de protección de integridad, y cualquier requisito especial del abono de la estación móvil, con aquellas indicadas por la estación móvil, y actuará según las siguientes reglas:

1) Si la estación móvil y la red no tienen en común ninguna versión del algoritmo, entonces la conexión se liberará.

2) Si la estación móvil y la red tienen al menos una versión del algoritmo en común, entonces la red seleccionará una de las versiones mutuamente aceptables del algoritmo para su uso sobre esa conexión.

La protección de integridad se efectúa adosando el código MAC-I de autenticación de mensaje al mensaje cuya integridad ha de protegerse. La estación móvil puede adosar el MAC-I a los mensajes en cuanto haya recibido un valor de REFRESCO específico para la conexión desde el RNC.

Si el valor del número HFN de hipertrama es mayor o igual al máximo valor almacenado en la estación móvil, la estación móvil indica a la red, en el establecimiento de conexión del RRC, que se requiere inicializar una nueva autenticación y acuerdo de clave.

El RNC puede disponerse para detectar que se necesitan nuevos parámetros de seguridad. Esto puede activarse por el fallo (repetido) de comprobaciones de integridad (p. ej., CONTADOR-I se ha desincronizado), o porque el traspaso a un nuevo RNC no da soporte a un algoritmo seleccionado por el viejo RNC, etc.

Se establece una nueva clave de cifrado, CK, cada vez que se ejecuta un procedimiento de autenticación entre la estación móvil y el SGSN.

La clave IK de integridad puede cambiarse si hay un traspaso de la estación móvil desde una estación base a una estación base distinta.

Debería apreciarse que en las realizaciones de la invención la comprobación de integridad sólo puede iniciarse en cualquier punto después de que la conexión ha sido establecida, así como en la anexión.

Debería apreciarse que, con las conexiones de datos, la conexión puede estar abierta por periodos de tiempo relativamente largos, o incluso puede estar permanentemente abierta.

Se ha acordado que puede establecerse más de un

portador de radio de señalización, es decir, un portador de radio en el plano de control que es un servicio ofrecido por el RLC, entre una estación móvil u otro equipo 6 de usuario, y el RNS 20. La actual especificación 3GPP propone que puedan proporcionarse hasta cuatro portadores de radio de señalización.

En la especificación 3GPP actual, dos o más de los portadores de radio de señalización, SRB, pueden tener los mismos parámetros de entrada al algoritmo de integridad ilustrado en la Figura 3. Si todos los parámetros de entrada al algoritmo de integridad son los mismos, entonces la salida es la misma.

Esta propuesta actual, como se ha mencionado anteriormente, deja abierta la posibilidad de que un intruso, o un "hombre de la calle", repita un mensaje de señalización, desde un portador de radio de señalización, sobre otro portador de radio de señalización. El valor de CONTADOR-I es específico para cada portador de radio de señalización, y puede ser distinto en distintos portadores de señalización. Consideremos el siguiente escenario. Se ha enviado un mensaje por un primer portador SRB1 de radio de señalización, con un valor del CONTADOR de 77. Cuando el valor del contador para un segundo portador SRB2 de radio de señalización llega a 77, el participante no autorizado puede simplemente repetir el mensaje enviado anteriormente por el SRB1, utilizando el SRB2.

Habitualmente, un único mensaje de señalización desde un portador de radio de señalización, repetido en el segundo portador de radio de señalización, no da una ventaja significativa al "hombre de la calle", pero puede ser posible que el participante no autorizado repita también un diálogo más largo, por ejemplo, a fin de establecer una llamada adicional que el "hombre de la calle" pueda utilizar y, así, robar partes de la conexión. Un caso más sencillo de "repetición-de-ataque" sería que el participante no autorizado, p. ej., pudiera repetir un diálogo realizado mediante SMS, siendo el diálogo, p. ej., una transacción monetaria.

Con las actuales propuestas de tercera generación, este problema puede sólo surgir en un número limitado de circunstancias. Esto se debe al hecho de que el empleo de los cuatro portadores de radio de señalización (SRB) está limitado. Sólo ciertos mensajes del RRC pueden enviarse por ciertos portadores de radio de señalización. El escenario de "repetición de ataque" sería posible para un mensaje de Estrato No de Acceso (NAS) (mensajes CM/MM/SMS, etc., llevados en Transferencia Directa del RRC) o un diálogo de mensajes NAS entre el UE y el SGSN/MSC. La Transferencia Directa del RRC es un mensaje del RRC que lleva en carga útil todos los mensajes NAS por la interfaz aérea. Sin embargo, este problema podría dañar a un usuario móvil ya que, por ejemplo, los mensajes del SMS podrían verse adversamente afectados.

Hay dos soluciones básicas para el problema del "ataque de reproducción". En primer lugar, distintos canales de comunicación, que usan la misma clave secreta, pueden coordinar el uso de números CONTADOR-I de secuencia, de tal forma que cada número de secuencia se use a lo sumo una vez en cualquiera de los canales. Esta coordinación puede ser muy engorrosa, o incluso imposible en algunas situaciones. Debería apreciarse que, cuando las realizaciones se aplican a la interfaz de radio de la red celular UMTS de 3ª generación, los canales de comunicación pueden llamarse portadores de radio.

Como se expondrá en más detalle, las realizaciones de la presente invención usan una solución donde se usa un parámetro adicional como una entrada al cálculo del código MAC-I de autenticación de mensaje. El valor de este parámetro es único, al menos para cada canal de comunicación que usa la misma clave secreta. El valor también puede ser único para todos los canales de comunicación dentro de una conexión entre el equipo UE 6 de usuario y el RNS 20.

En una realización adicional de la presente invención, el problema se evita garantizando que la misma clave de integridad nunca se use para distintos canales de comunicación paralelos.

Con referencia a la Figura 4, se describen las modificaciones de la conocida función de protección de integridad que realiza la presente invención. Estas modificaciones no causan ningún cambio en el algoritmo UIA de integridad efectivo.

Se añade un parámetro específico del canal de comunicación como entrada al algoritmo de protección de integridad. En las especificaciones 3GPP, este parámetro específico del canal de comunicación es la identificación del portador de radio (RB ID). En un ejemplo de una aplicación de la presente invención, la identificación del portador de radio representa la identidad del portador de radio de señalización en el propuesto sistema WCDMA de tercera generación, y puede ser un número entre 0 y 3. Debería observarse que el parámetro usado, específico para el canal de comunicación, depende de la capa de protocolo donde se calcula el código de autenticación de mensaje. Usando aún la especificación 3GPP como un ejemplo, si el código de autenticación de mensaje se añadiese en el protocolo del RLC, el parámetro sería una identidad de canal lógico (véase la Figura 2). Como otro posible ejemplo, si la protección de integridad se realizara en la capa del protocolo PDCP o en la capa del protocolo del RRC, el parámetro adicional sería una identidad de portador de radio (véase la Figura 2). Debería apreciarse que, al exponer la parte del plano de control de la pila de protocolos, los términos "identidad de portador de radio de señalización" e "identidad de portador de radio" son equivalentes.

Como la identidad del portador de radio de señalización es conocida tanto por el remitente como por el receptor, es decir, el equipo UE 6 de usuario y el RNS 20, no es necesario enviar la información de identidad explícitamente por la interfaz de radio.

La Figura 4 ilustra los posibles lugares donde puede incluirse el nuevo parámetro sin modificar el algoritmo UIA de integridad. Dado que el remitente y el receptor son similares cuando se ven desde el punto de vista del parámetro de entrada (véase la Figura 3), sólo un lado se muestra en la Figura 4. Debería apreciarse que las partes receptora y transmisora realizarán el mismo algoritmo. Como puede verse en la Figura 4, las realizaciones preferidas incluyen el nuevo parámetro adosándolo (como una cadena) a uno o más de los parámetros de entrada existentes del algoritmo.

En una realización, la identificación del portador de radio de señalización, RB ID, se hace parte de los parámetros de entrada REFRESCO o CONTADOR-I. Esto se ilustra con los números "1" y "2" en la Figura 4, respectivamente. En la práctica, los parámetros REFRESCO y CONTADOR-I incorporarían tanto la información de REFRESCO y CONTADOR-I como la información de identificación. Por ejemplo,

si el valor de REFRESCO tiene n bits, la información de REFRESCO se representaría con "a" bits, y la información de identificación con "b" bits, donde a+b = n. Esto significaría, en efecto, acortar el parámetro REFRESCO. La misma modificación puede hacerse al parámetro CONTADOR-I. En una modificación, parte de la identificación del portador de radio de señalización puede ser proporcionada por el parámetro CONTADOR-I, y parte por el parámetro REFRESCO. Sin embargo, si el CONTADOR-I se acorta, puede llevarle un tiempo más breve "dar toda la vuelta", es decir, alcanzar el máximo valor y volver al cero. Si se acorta el parámetro REFRESCO, puede ser que aumente la probabilidad de repetir el valor por accidente (se escoge aleatoriamente).

En una realización adicional, el identificador del portador de radio de señalización se hace parte de la clave IK de integridad. Esto se ilustra con el número "4" en la Figura 4. Por ejemplo, si el valor de IK tiene n bits, la información de IK se representaría con "a" bits, y la información de identificación con "b" bits, donde a+b=n. Sin embargo, si la clave IK es más corta, hay mayor probabilidad de adivinar simplemente la clave.

En una realización adicional de la presente invención, la identidad del portador de radio de señalización puede incorporarse al MENSAJE que se ingresa en el algoritmo de integridad. Esto se ilustra con el número "3" en la Figura 4. Como la identidad del portador de radio de señalización es conocida tanto por el remitente como por el receptor, es decir, la estación móvil y el RNS 20, no es necesario enviar la información de identidad por la interfaz de radio con el MENSAJE efectivo. Por ejemplo, si el MENSAJE tiene n bits y el identificador RB ID tiene "i" bits, el "MENSAJE" efectivo que ingresaría al algoritmo de integridad tendría n+i bits. Así, en lugar de ingresar sólo el MENSAJE al algoritmo de integridad, la cadena de bits ingresada al algoritmo de integridad se convertiría en la identidad del portador de radio de señalización y en el MENSAJE. Esta solución no tiene ningún impacto sobre cuestiones de seguridad (p. ej., longitudes de contador) relacionadas con el algoritmo de integridad. Esto significa que no se acorta ningún parámetro que se ingresa al algoritmo.

En algunas realizaciones, es posible dividir la información de identificación entre más de una entrada.

La Figura 5 ilustra una realización adicional de la invención, teniendo esta realización efecto sobre el algoritmo UIA de integridad efectivo. En esta realización se proporciona al algoritmo de integridad un parámetro adicional, según se muestra en la Figura 5. En este ejemplo, cuando se efectúa la protección de integridad en la capa del protocolo del RRC, el parámetro adicional es un identificador de portador de radio (de señalización), RB ID, que es único para el portador de radio (de señalización). Este parámetro se ingresa por separado y se usa en el cálculo efectuado por el algoritmo UIA de integridad.

La Figura 6 ilustra una realización adicional de la invención, teniendo esta realización efecto sobre el algoritmo UIA de integridad efectivo. En esta realización, el nuevo parámetro identificador de portador (RB ID) se combina con el parámetro DIRECCIÓN. Esta realización alargaría efectivamente el "viejo" parámetro existente DIRECCIÓN y, así, tendría efecto sobre el algoritmo UIA de integridad efectivo.

En una realización alternativa, se produce una única clave de integridad, IK, para cada portador de radio. Esto puede lograrse modificando el procedimiento de autenticación de una capa superior L3 que brinda soporte a la gestión de movilidad, MM, y a la gestión de sesiones, SM, en las especificaciones propuestas del UMTS. Como se ha explicado en breve anteriormente, la función de gestión de movilidad gestiona la ubicación de la estación móvil, es decir, la anexión de la estación móvil a la red, y la autenticación. El algoritmo de integridad realizado en cada uno de los portadores de radio de señalización durante un procedimiento de autenticación modificado puede brindar resultados únicos, impidiendo el tipo de ataque anteriormente esbozado.

Se hará ahora referencia a las Figuras 7 a 9, mostrando posibles procedimientos de autenticación y acuerdo de claves. Los mecanismos descritos logran la autenticación mutua, mostrando el usuario y la red conocimiento de una clave secreta K, que está compartida entre, y disponible sólo para, el Módulo de Identidad de Servicios de Usuario, USIM, y el Centro de Autenticación, AuC, en el Entorno Local HE del usuario. Además, el USIM y el HE mantienen registro de los contadores SEQ_{MS} y SEQ_{HE}, respectivamente, para prestar soporte a la autenticación de red.

El procedimiento puede diseñarse de forma tal que sea compatible, p. ej., con la arquitectura actual de seguridad del GSM, y facilite la migración desde el GSM al UMTS. El procedimiento se compone de un protocolo de reto/respuesta, idéntico al protocolo de autenticación y establecimiento de claves de abonado del GSM, combinado con un protocolo de un paso basado en números de secuencia para la autenticación de red, derivado del estándar ISO/IEC 9798-4 de la ISO. Antes de explicar la formación de las claves de integridad, se expondrá un mecanismo de autenticación y acuerdo de claves. Un panorama general de un posible mecanismo de autenticación y acuerdo de claves se muestra en la Figura 7. La Figura 8 muestra un posible procedimiento para la generación de vectores de autenticación.

Al recibir una solicitud del VLR/SGSN, el HE/AuC envía una formación ordenada de vectores de autenticación (el equivalente de un "trío" del GSM) al VLR/SGSN. Cada vector de autenticación consiste en los siguientes componentes: un número aleatorio RAND, una respuesta esperada XRES, una clave cifrada CK, una clave IK de integridad y un testigo AUTN de autenticación. Cada vector de autenticación es bueno para una autenticación y acuerdo de claves entre el VLR/SGSN y el USIM.

Cuando el VLR/SGSN inicia una autenticación y acuerdo de claves, selecciona el próximo vector de autenticación de la formación y envía los parámetros RAND y AUTN al usuario. El USIM comprueba si AUTN puede aceptarse y, en ese caso, produce una respuesta RES que se devuelve al VLR/SGSN. El USIM también calcula CK e IK. El VLR/SGSN compara la RES recibida con XRES. Si coinciden, el VLR/SGSN considera que el intercambio de autenticación y acuerdo de claves se ha completado con éxito. Las claves establecidas CK e IK serán transferidas luego por el USIM y el VLR/SGSN a las entidades que realizan funciones de cifrado e integridad. En el propuesto sistema UMTS, estas entidades pueden, preferiblemente, ser algunos de los protocolos de interfaz de radio descritos en la Figura 2. Las entidades

se sitúan, preferiblemente, en el Equipo UE de Usuario y en el Controlador de Red de Radio, RNC.

Los VLR/SGSN pueden ofrecer servicio seguro incluso cuando no se dispone de enlaces HE/AuC, dejándoles usar claves de cifrado e integridad derivadas previamente para un usuario, de forma tal que aún pueda establecerse una conexión segura sin necesidad de una autenticación y un acuerdo de clave. La autenticación, en ese caso, se basa en una clave de integridad compartida, por medio de la protección de la integridad de datos de mensajes de señalización.

Los participantes autenticadores serán el AuC del HE del usuario (HE/AuC) y el USIM en la estación móvil del usuario. El mecanismo puede consistir en los siguientes procedimientos:

Distribución de información de autenticación desde el HE/AuC al VLR/SGSN. Se supone que el VLR/SGSN es fiable para el HE del usuario, a fin de gestionar con seguridad información de autenticación. También se supone que los enlaces intra-sistemas entre el VLR/SGSN y el HE/AuC son adecuadamente seguros. Se supone adicionalmente que el usuario confía en el HE.

- Autenticación mutua y establecimiento de nuevas claves de cifrado e integridad entre el VLR/SGSN y la MS.
- Distribución de datos de autenticación desde un VLR anteriormente visitado al VLR recién visitado. Se supone que los enlaces entre los VLR/SGSN son adecuadamente seguros.

El fin de la distribución de datos de autenticación de HE a SN es proporcionar al VLR/SGSN una formación de vectores de autenticación refrescados del HE del usuario, para llevar a cabo un cierto número de autenticaciones de usuario. El VLR/SGSN invoca los procedimientos solicitando vectores de autenticación al HE/AuC. La solicitud de datos de autenticación incluirá una identidad de usuario. Si el usuario es conocido en el VLR/SGSN por medio de la IMUI (Identidad Internacional de Usuario Móvil), la solicitud de datos de autenticación incluirá la IMUI. Si el usuario está identificado por medio de una identidad permanente cifrada, puede incluirse en cambio el mensaje del HLR desde el cual el HE puede obtener la IMUI. En ese caso, este procedimiento, y el procedimiento de solicitud de identidad de usuario al HLR, están preferiblemente integrados.

Al recibir la solicitud de datos de autenticación desde el VLR/SGSN, el HE puede haber precalculado el número requerido de vectores de autenticación, y haberlos extraído de la base de datos del HLR, o puede calcularlos a pedido. El HE/AuC devuelve una respuesta de autenticación al VLR/SGSN que contiene una formación ordenada de n vectores de autenticación AV(1..n). El HE/AuC genera un nuevo número SQN de secuencia y un reto RAND impredecible. Para cada usuario, el HE/AuC también mantiene un registro de un contador que es SQN_{HE}.

Los mecanismos para verificar la renovación de los números de secuencia en el USIM permitirán, en cierto grado, el uso fuera de orden de los números de secuencia. Esto es para garantizar que la tasa de fallos de autenticación debidos a fallos de sincronización sea suficientemente baja. Esto requiere la capacidad del USIM para almacenar información sobre sucesos pasados de autenticación exitosa (p. ej., números de secuencia o partes relevantes de los mismos). El mecanismo garantizará que un número de secuencia aún pueda aceptarse si está entre los últimos x = 50 números de secuencia generados. Esto no impedirá que un número de secuencia sea rechazado por otros motivos, tales como un límite en la edad para números de secuencia basados en el tiempo.

Se necesita usar el mismo número mínimo x entre los sistemas, para garantizar que la tasa de fallos de sincronización sea suficientemente baja en diversos escenarios de utilización, en particular, el registro simultáneo en los dominios de servicios CS y PS, el movimiento de usuarios entre los VLR/SGSN que no intercambian información de autenticación y redes sobrecargadas.

El uso de SEQ_{HE} puede ser específico para el procedimiento de generación de números de secuencia. Un campo AMF de autenticación y gestión de claves puede incluirse en el testigo de autenticación de cada vector de autenticación.

A continuación pueden calcularse los siguientes valores:

- un código de autenticación de mensaje MAC = $f1_K$ (SQN || RAND || AMF), donde f1 es una función de autenticación de mensajes;
- una respuesta esperada XRES = $f2_K$ (RAND), donde f2 es una función de autenticación de mensaje (posiblemente truncado);
- una clave de cifrado CK = $f3_K$ (RAND), donde f3 es una función generadora de claves;
- una clave de integridad IK = $f4_K$ (RAND), donde f4 es una función generadora de claves;
- una clave de anonimato AK = $f5_K$ (RAND), donde f5 es una función generadora de claves, o f5 ≡ 0.

Según las realizaciones de la presente invención, se genera más de una IK. Esto puede lograrse, por ejemplo, modificando la función f4 de forma tal que produzca el número deseado de IK (p. ej., 4: véase la Figura 9). Una posibilidad es especificar que la función f4 debe activarse varias veces durante la generación de un vector de autenticación. Esto puede implementarse, p. ej., ingresando, en la segunda ronda, la primera IK[1] producida como entrada a la función f4, en lugar de un nuevo RAND. En la tercera "ronda", la IK[2] producida en la segunda ronda se introduciría en la función f4 para obtener la tercera clave IK[3] de integridad. Una posibilidad es también ingresar un número deseado de valores de RAND a la función f4. Así es posible producir tantas IK como sea necesario para el sistema en cuestión. Por ejemplo, en el sistema UMTS según las especificaciones de la Versión '99 de 3GPP, se necesitarían cuatro claves de integridad.

El testigo de autenticación AUTN = SQN (+) AK || AMF || MAC puede construirse luego. La AK es una clave de anonimato usada para ocultar el número de secuencia, ya que este último puede exponer la identidad y ubicación del usuario. La ocultación del número de secuencia es para proteger sólo contra ataques pasivos. Si no se necesita ninguna ocultación, entonces f5 ≡ 0.

El fin del procedimiento de autenticación y acuerdo de clave es autenticar al usuario y establecer un nuevo par de claves de cifrado e integridad entre el

VLR/SGSN y la MS. Durante la autenticación, el usuario verifica la renovación del vector de autenticación que se usa. El VLR/SGSN invoca el procedimiento seleccionando el próximo vector de autenticación sin usar entre la formación ordenada de vectores de autenticación en la base de datos del VLR. El VLR/SGSN envía al usuario el reto aleatorio RAND y un testigo de autenticación AUTN para autenticación de red, a partir del vector de autenticación seleccionado. Al recibirlos, el usuario procede según se muestra en la Figura 9.

Al recibir RAND y AUTN, el usuario calcula primero la clave de anonimato AK = $f5_K$ (RAND) y extrae el número de secuencia SQN = (SQN (+) AK) (+) AK. Luego, el usuario calcula XMAC = $f1_K$ (SQN || RAND || AMF) y compara esto con MAC, que está incluido en AUTN. Si son distintos, el usuario devuelve un rechazo de autenticación de usuario al VLR/SGSN, con una indicación de la causa, y el usuario abandona el procedimiento. A continuación, el USIM verifica que el número SQN de secuencia recibido esté en la gama correcta.

Según una realización de la presente invención, el USIM genera más de una IK, en lugar de generar sólo una IK. Como se ha explicado anteriormente, esto puede lograrse, por ejemplo, modificando la función f4, especificando que la función f4 debe activarse varias veces durante la generación de un vector de autenticación, o por el ingreso de un número deseado de valores de RAND en la función f4. Esto puede requerir que la red (SN/VLR) envíe el número requerido de valores de RAND y AUTN al UE, y que el UE pueda necesitar producir también una RES para cada RAND y devolver todas las RES producidas a la red, como se describió anteriormente para el caso de un valor RAND+AUTN.

Las realizaciones de la presente invención pueden usarse en cualquier sistema que permite la señalización no cifrada y la utilización de sumas de control de integridad en al menos dos portadores de radio paralelos.

Las realizaciones de la presente invención se han descrito en el contexto de una red de telecomunicaciones celulares inalámbricas. Sin embargo, pueden usarse realizaciones alternativas de la presente invención con cualquier otro tipo de red de comunicaciones, inalámbrica o no. Las realizaciones de la presente invención pueden usarse con cualquier forma de comunicación donde se proporcionen comprobaciones de integridad, o similares, con una pluralidad de portadores de radio, o similares, en paralelo.

REIVINDICACIONES

1. Un nodo para su uso en un sistema que comprende dicho nodo (6, 20) y un nodo adicional (20, 6), proporcionándose una pluralidad de distintos canales de comunicación entre dichos nodos, teniendo cada canal de comunicación una identidad distinta, comprendiendo dicho nodo:

medios para calcular un código (XMAC-I) de autenticación a partir de una pluralidad de valores, siendo algunos de dichos valores los mismos para dicha pluralidad de distintos canales de comunicación, medios para recibir información relacionada con un código (MAC-I) de autenticación calculado por dicho nodo adicional; y

medios para comparar información relacionada con un código (XMAC-I) de autenticación calculado por dicho nodo con información relacionada con un código (MAC-I) de autenticación calculado por el nodo adicional; y **caracterizado** por

estar al menos uno de dichos valores dispuesto para comprender información relacionada con la identidad (RB ID) de un canal de comunicación de dicha pluralidad de canales de comunicación.

2. Un nodo según la reivindicación 1, que comprende un controlador (24) de red de radio.

3. Un nodo según la reivindicación 1, que comprende un equipo (6) de usuario.

4. Un nodo según cualquier reivindicación precedente, que comprende medios para la comunicación mediante una conexión inalámbrica.

5. Un sistema de comunicación que comprende un nodo según cualquier reivindicación precedente.

6. Un procedimiento para llevar a cabo una comprobación de integridad en un sistema que comprende un nodo y un nodo adicional (6, 20), proporcionándose una pluralidad de canales de comunicación entre dicho nodo y dicho nodo adicional, teniendo cada canal de comunicación una identidad (RB ID) distinta, comprendiendo dicho procedimiento las etapas de:

recibir en el nodo información relacionada con un código (MAC-I) de autenticación del nodo adicional;

calcular un código (XMAC-I) adicional de autenticación usando una pluralidad de valores, siendo algunos de dichos valores los mismos para dicha pluralidad de distintos canales de comunicación, comparar el código (XMAC-I) adicional de autenticación con dicha información relacionada con un código (MAC-I) de autenticación recibido desde el nodo adicional, y **caracterizado** por estar al menos uno de dichos valores dispuesto para comprender información relacionada con la identidad (RB ID) de un canal de comunicación de dicha pluralidad de canales.

7. Un procedimiento según la reivindicación 6, que comprende ingresar información relacionada con la identidad (RB ID) del canal de comunicación de dicha pluralidad de canales de comunicación, como un valor de entrada por separado, en un algoritmo (UIA) de integridad para calcular el código (XMAC-I) de autenticación.

8. Un procedimiento según la reivindicación 6, que comprende proporcionar un valor de entrada combinado, combinando información relacionada con la identidad (RB ID) del canal de comunicación de dicha pluralidad de canales de comunicación, con al menos otro valor de entrada, e ingresar el valor de entrada combinado en un algoritmo (UIA) de integridad para calcular el código (XMAC-I) de autenticación.

9. Un procedimiento según cualquiera de las reivindicaciones 6 a 8, en el cual dichos valores para calcular el código (XMAC-I) de autenticación de mensaje comprenden uno o más de los siguientes valores de la arquitectura de seguridad del Sistema Universal de Telecomunicaciones Móviles (UMTS) del Proyecto de Asociación de 3ª Generación (3GPP); una clave (IK) de integridad; un valor (DIRECCIÓN) de dirección, un valor (REFRESCO) de refresco, un valor (MENSAJE) de mensaje y un valor (CONTADOR-I) de contador.

10. Un procedimiento según cualquiera de las reivindicaciones 6 a 9, en el cual dichos canales de comunicación comprenden un portador de radio.

11. Un procedimiento según la reivindicación 10, en el cual dicho portador de radio es un portador de radio de señalización.

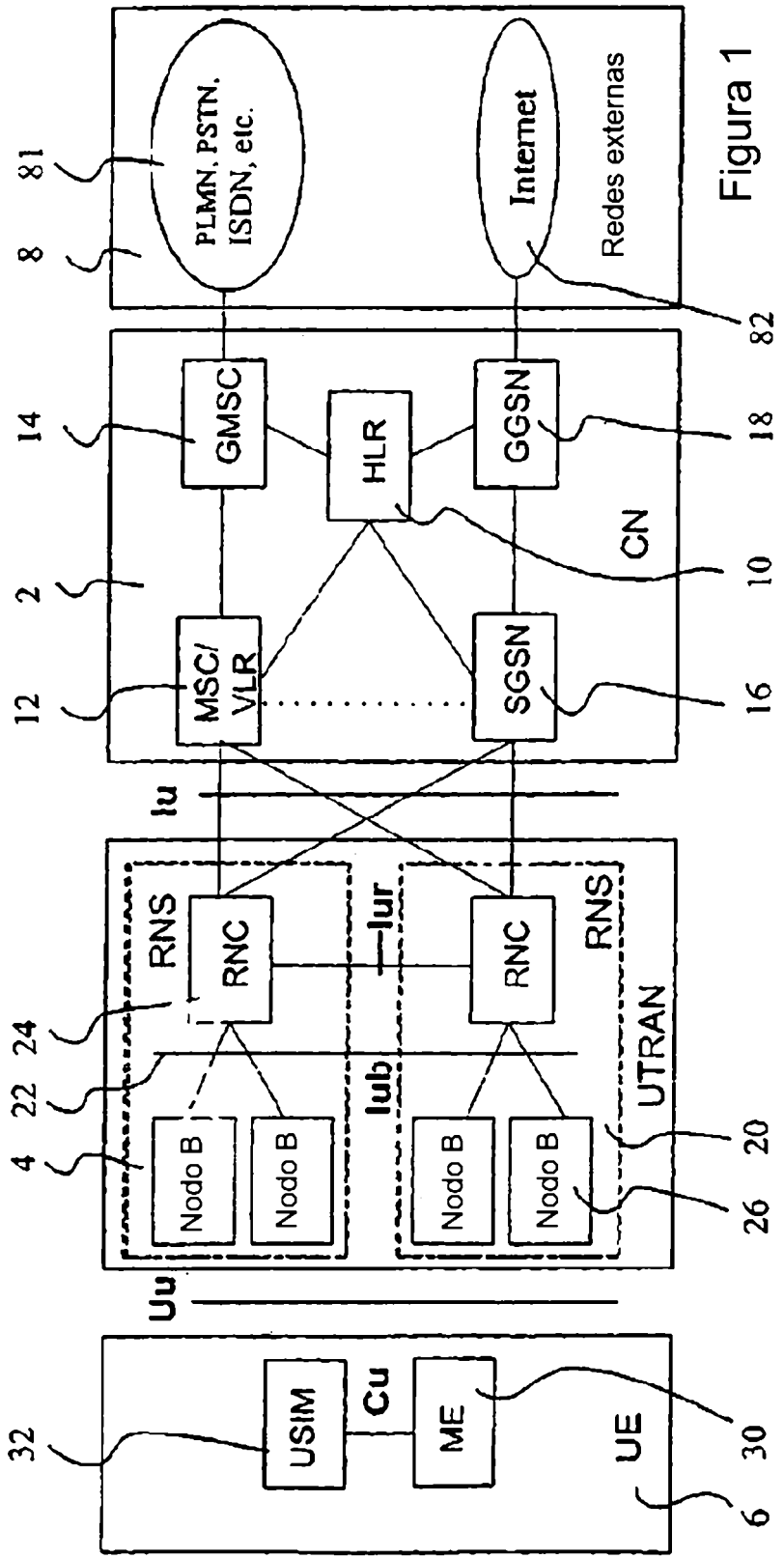
PLMN, PSTN, ISDN, etc.
Internet
Redes externas
8
81
82
GMSC
HLR
GGSN
14
18
CN
2
10
MSC/ VLR
SGSN
12
16
Iu
RNS
RNC
Iur
RNC
RNS
24
22
Iub
UTRAN
4
Nodo B
Nodo B
Nodo B
Nodo B
20
26
Uu
USIM
Cu
ME
UE
32
30
6

Figura 1

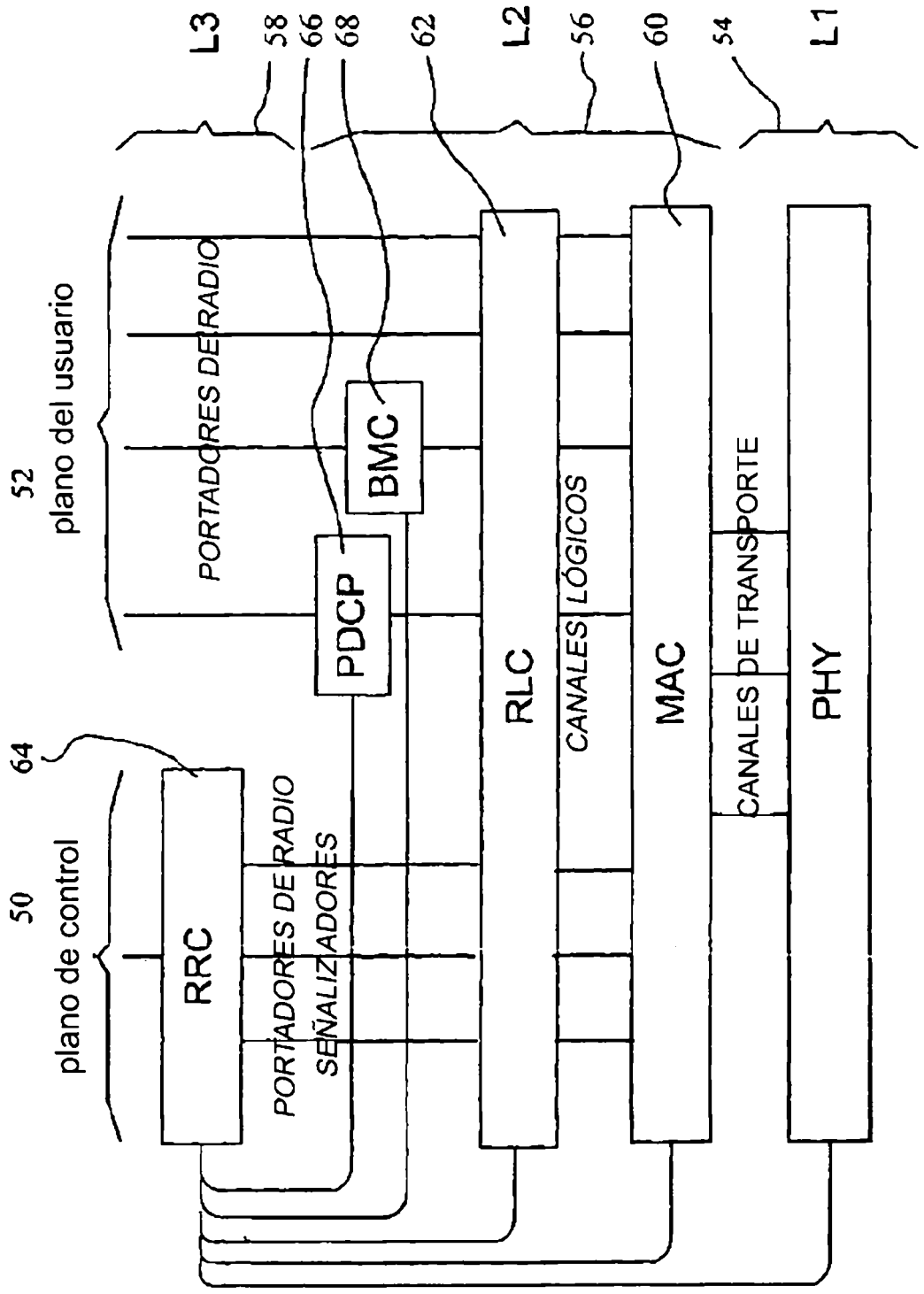
L3
58
66
68
62
L2
56
60
54
L1
52
plano del usuario
PORTADORES DE RADIO
BMC
PDCP
RLC
CANALES LÓGICOS
MAC
CANALES DE TRANSPORTE
PHY
64
50
plano de control
RRC
PORTADORES DE RADIO SEÑALIZADORES

Figura 2

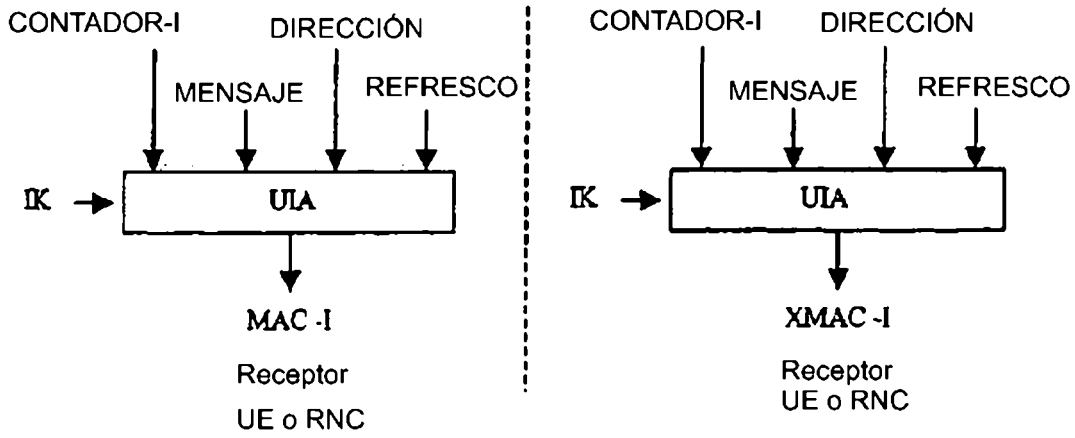

Figura 3

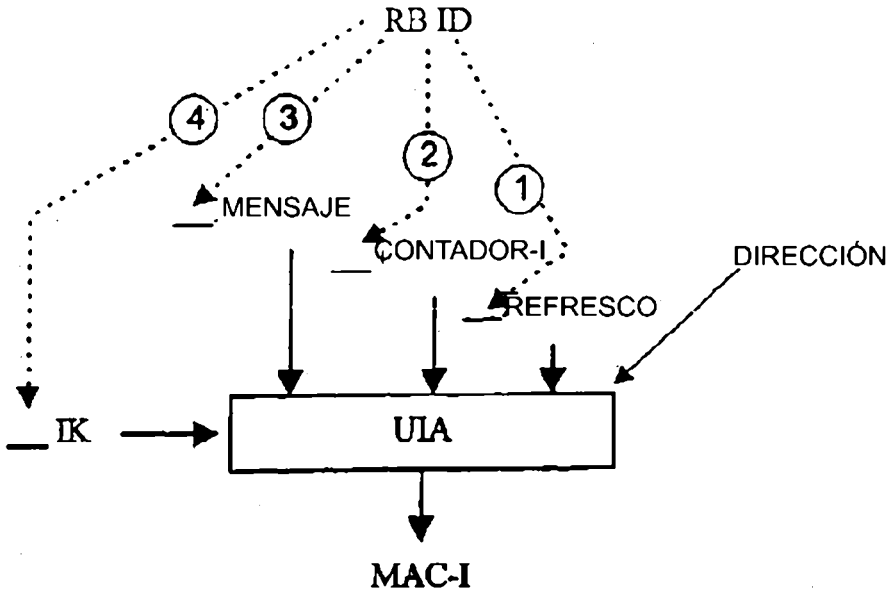

Figura 4

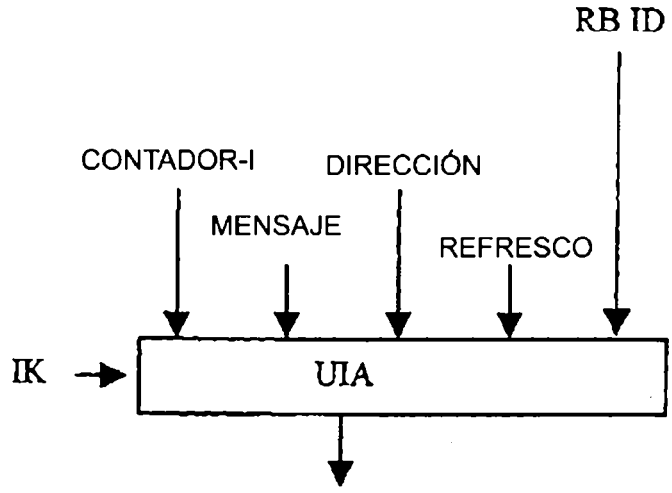

Figura 5

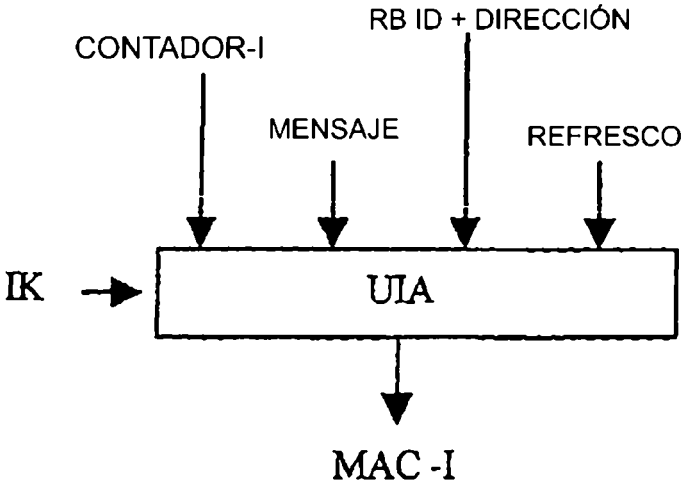

Figura 6

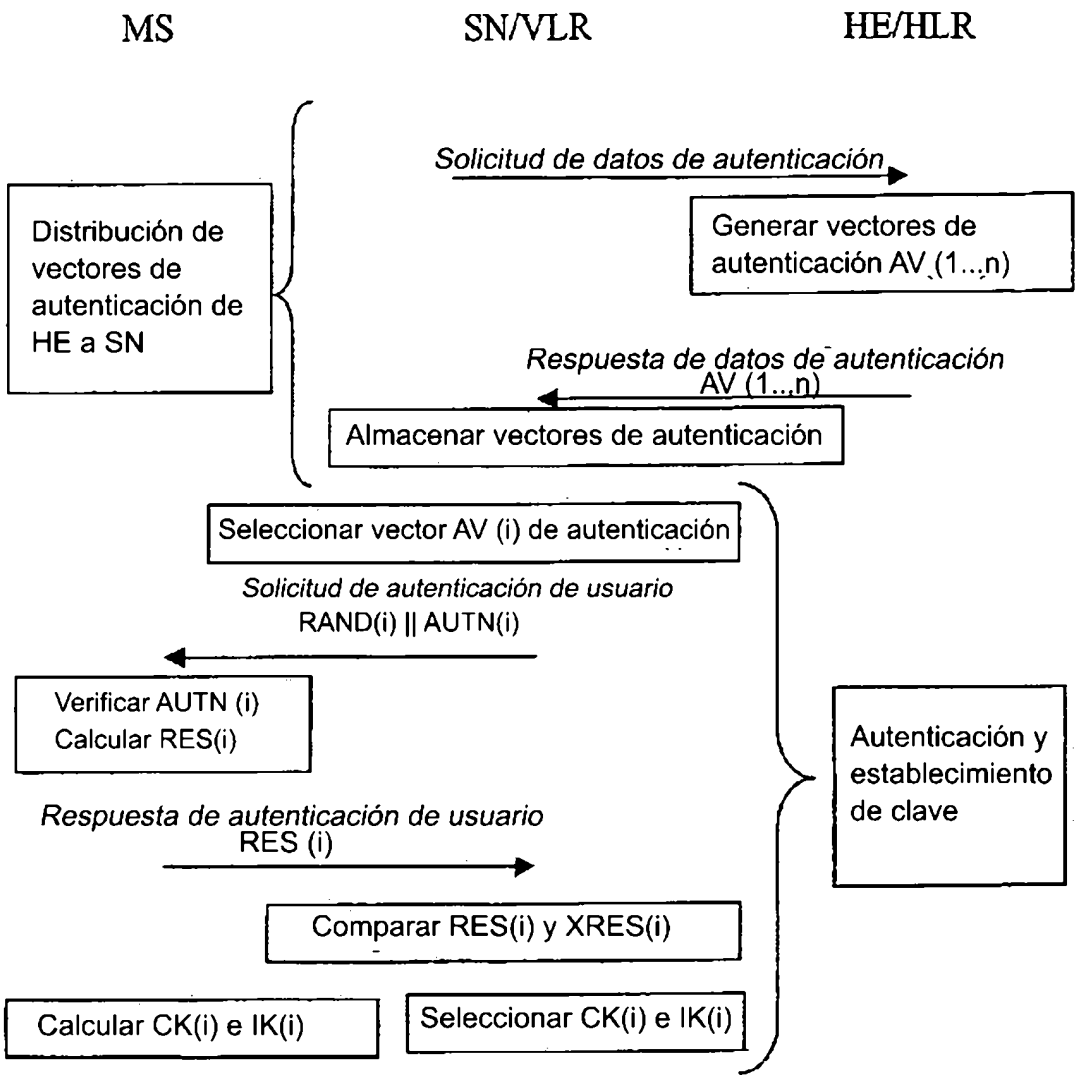
MS
SN/VLR
HE/HLR
Solicitud de datos de autenticación
Distribución de vectores de autenticación de HE a SN
Generar vectores de autenticación AV (1...n)
Respuesta de datos de autenticación AV (1...n)
Almacenar vectores de autenticación
Seleccionar vector AV (i) de autenticación
Solicitud de autenticación de usuario
RAND(i) || AUTN(i)
Verificar AUTN (i)
Calcular RES(i)
Respuesta de autenticación de usuario
RES (i)
Comparar RES(i) y XRES(i)
Calcular CK(i) e IK(i)
Seleccionar CK(i) e IK(i)
Autenticación y establecimiento de clave

Figura 7

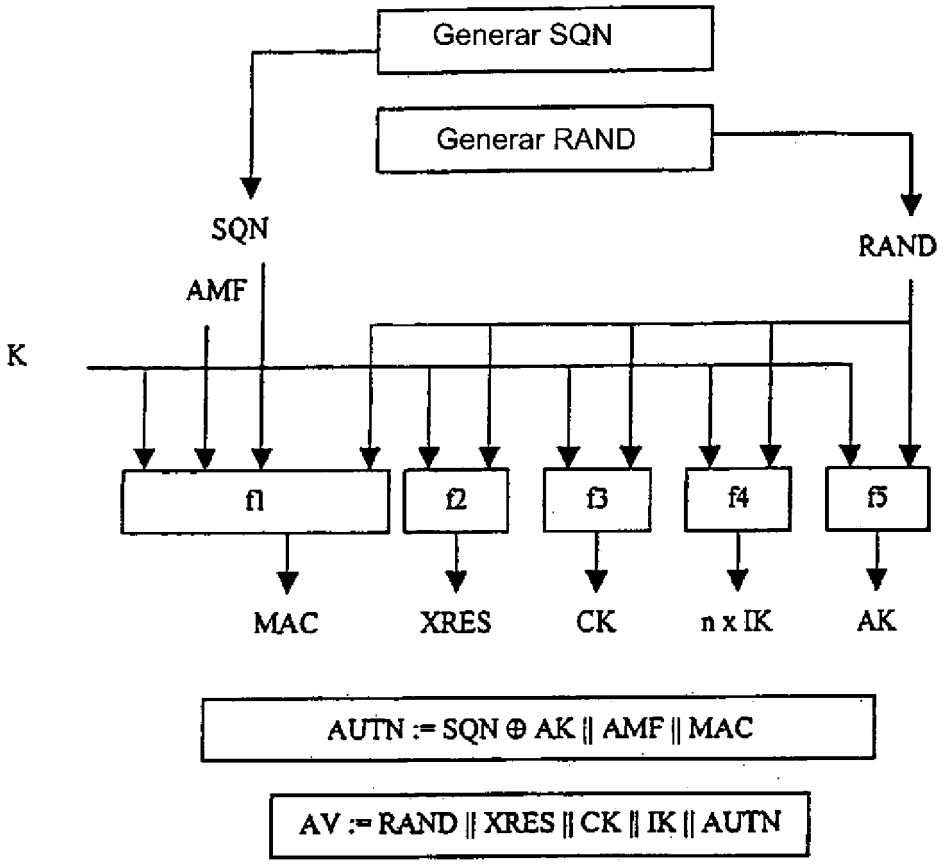
Generar SQN
Generar RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
n x IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figura 8

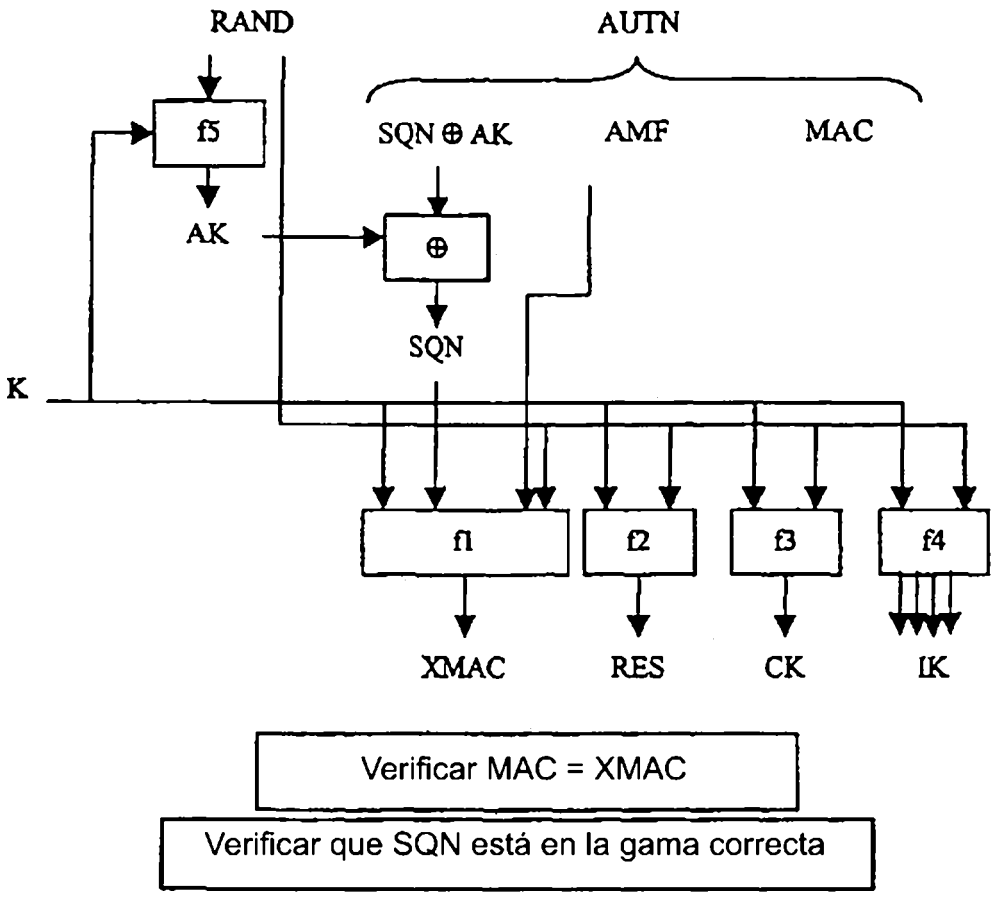
RAND
AUTN
f5
SQN ⊕ AK
AMF
MAC
AK
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verificar MAC = XMAC
Verificar que SQN está en la gama correcta

Figura 9