(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 429 133**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.09.2002 E 02767632 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2013 EP 1428403**

(54) Título: **Métodos, sistemas y terminales de comunicaciones**

(30) Prioridad:

11.09.2001 GB 0121979

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2013

(73) Titular/es:

MOTOROLA SOLUTIONS, INC. (100.0%)
1303 East Algonquin Road
Schaumburg IL 60196, US

(72) Inventor/es:

CHATER-LEA, DAVID J. y
SHAHAF, MARK

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Métodos, sistemas y terminales de comunicaciones

Campo de la invención

Esta invención se refiere a métodos, a sistemas y a terminales de comunicaciones. En particular, se refiere al uso de encriptación en tales métodos, sistemas y terminales de comunicaciones, especialmente para comunicaciones móviles.

Antecedentes de la invención

Los sistemas de comunicaciones de radio móviles, por ejemplo telefonía celular o sistemas de comunicaciones de radio móviles privados, proporcionan normalmente enlaces de telecomunicación de radio para su disposición entre una pluralidad de unidades de abonado, a menudo referidos en la técnica como estaciones móviles (MS). El término estación móvil (MS) incluye generalmente unidades de radio tanto portátiles como montadas en vehículos, radioteléfonos y unidades de comunicaciones de radio similares.

Los sistemas de comunicaciones de radio móviles se distinguen de los sistemas de comunicaciones fijos, tales como las redes telefónicas públicas conmutadas (PSTN), principalmente porque las estaciones móviles pueden moverse en una ubicación geográfica para acompañar a su usuario y así encontrar diversos entornos de propagación de radio. Los sistemas de comunicaciones de radio móviles y las estaciones móviles usadas en los mismos pueden operar en uno de dos modos principales, concretamente el modo de operación troncal (TMO) y el modo de operación directo (DMO). Las comunicaciones de TMO usan la infraestructura suministrada por el operador del sistema, por ejemplo estaciones transceptoras base (BTS), para entregar comunicaciones desde un terminal, por ejemplo la MS de un usuario u operador, a la de uno u otros terminales, por ejemplo la MS de uno u otros usuarios. En cambio, el DMO es un método que proporciona la capacidad de una comunicación directa entre dos o más MS sin ninguna infraestructura del operador asociado. Algunas MS pueden ser de operación en modo dual usando o bien TMO o bien DMO según sea apropiado.

En un sistema de comunicaciones de radio de TMO, cada BTS tiene asociada con la misma un área (o célula) de cobertura geográfica particular. La célula define un alcance particular en el que la BTS puede mantener comunicaciones aceptables con MS que operan dentro de la célula. A menudo se combinan células para producir un área de cobertura de sistema expandida. Además, las células se agrupan a menudo en áreas de ubicación para fines de seguimiento de una MS dentro del área de cobertura mientras se minimiza la señalización de actualización de ubicación. En un sistema de TMO, la información, que es información de usuario, se conoce como información considerada como contenida en el “plano de U” (o plano de usuario) de la pila de protocolos de sistema, y es independiente de la información de control usada por el sistema considerada como contenida en el “plano de C” (o plano de control) de la pila de protocolos de sistema.

En el campo de esta invención se conoce que sistemas tales como los que operan según las normas TETRA (radio truncada terrestre), emplean tecnología de encriptación de interfaz aérea (AI). Las normas TETRA son procedimientos o protocolos de operación que se han definido por el Instituto Europeo de Normas de Telecomunicaciones (ETSI). Además, tales sistemas que son sistemas de TMO pueden soportar una capa de encriptación adicional que se denomina encriptación de extremo a extremo. El proceso se conoce como “de extremo a extremo” puesto que sólo puede aplicarse por el remitente (fuente) de la información y eliminarse por el receptor (destino) de la información. Para conseguir este proceso de encriptación de extremo a extremo, las claves de encriptación usadas por el terminal de transmisión y el terminal de recepción deben ser las mismas.

Una comunicación encriptada de extremo a extremo entre MS en TMO se lleva a cabo de manera transparente (sin modificación) a través de la infraestructura y a través de las interfaces aéreas del sistema, y la desencriptación se lleva a cabo sólo mediante la MS del receptor de la información. En otras palabras, la red de sistema y sus instalaciones de componentes que intervienen, tales como BTS, BSC, etc. (descritas más adelante), a través de las que pasan las transmisiones encriptadas, no poseen las claves de encriptación. Por tanto, estas instalaciones no pueden desencriptar ni recuperar la información que se transmite.

La encriptación y desencriptación también se conoce en sistemas de DMO y en este caso el método de comunicación segura usa encriptación de extremo a extremo y de interfaz aérea.

Una clave de encriptación se define generalmente como información, normalmente una secuencia de dígitos binarios aleatorios o pseudoaleatorios, usada inicialmente para configurar y cambiar periódicamente las operaciones realizadas en equipo criptográfico. Tales claves se usan para encriptar o desencriptar señales electrónicas, o para determinar patrones contra contramedidas electrónicas, por ejemplo salto de frecuencia o espectro ensanchado, o para producir otras claves. En la técnica, el término “clave” se usa a menudo para abarcar los términos “clave

variable", "inserción de claves variable" y "criptografía variable."

Cuando dos o más usuarios en un sistema de TMO o DMO emplean encriptación de extremo a extremo para una comunicación entre sí, deben usar la misma clave de encriptación que usará el remitente para encriptar la información, y el/los receptor(es) usará(n) la misma clave para desencriptar la información. Las claves idénticas usadas por el remitente y el receptor se conocen como clave compartida. En la práctica, la clave compartida se almacena en una memoria segura de cada MS que será miembro de un grupo de charla seguro. La encriptación de clave compartida es un proceso operativo conocido que es apropiado para emplearse, por ejemplo, en un sistema de comunicaciones de TETRA.

Con el fin de mantener la seguridad de las comunicaciones encriptadas, puede ser deseable cambiar la clave de encriptación de manera regular (y la frecuencia de cambio viene dictada por una política de seguridad de sistema). Esto sirve para impedir que un adversario descubra una clave de encriptación, o bien mediante análisis del material encriptado con esa clave, o bien mediante algunos otros medios de descubrimiento, tales como robar la clave de uno de sus usuarios.

Las normas de TETRA en TMO soportan el uso de diversos protocolos para controlar y entregar comunicaciones entre una infraestructura de conmutación y gestión (SwMI) y las estaciones móviles (MS). Los protocolos tienen capas diferentes, de una manera similar a las capas separadas descritas anteriormente. La capa de control de acceso al medio (MAC), que es la parte inferior de la capa 2 del plano de C de la pila de protocolos, usa un direccionamiento para distinguir una MS de otra. A cada MS se le da un código de identificación o dirección de MAC de capa 2 única. La dirección de MAC no proporciona ninguna confidencialidad, pero permite que se distingan las transmisiones tanto hacia como desde MS diferentes.

Un sistema de encriptación que usa claves de encriptación tal como se describió anteriormente proporciona confidencialidad de información comunicada. También impide que un adversario proporcione información falsa a las MS de comunicación, puesto que el adversario no tiene la clave para encriptar la información correctamente. Sin embargo, puesto que la información tiene que pasar por canales no seguros tanto en TMO como en DMO, podría ser susceptible de un mal uso. Por ejemplo, un adversario podría grabar una transmisión encriptada y reproducirla más tarde frente a los mismos usuarios (mientras que la clave de encriptación todavía es válida) o a diferentes usuarios que también están usando la misma clave.

Un mecanismo conocido para los expertos en la técnica para impedir este tipo de ataque de seguridad es proporcionar una señal de sincronismo, que se confía a cada una de las partes que comparten una clave de encriptación. La MS de cada usuario de este tipo combina la señal de sincronismo con la clave compartida acordada previamente para generar una clave de encriptación compartida nueva, y la clave nueva se usa para encriptar la información. Si una transmisión se intercepta y reproduce en un momento posterior, la señal de sincronismo no coincidirá con la señal de sincronismo actual en uso mediante MS de recepción, y entonces la información ya no puede desencriptarse correctamente.

Un ataque de seguridad alternativo que podría intentarse por un adversario es la redirección de mensajes. Si el adversario puede interceptar un mensaje encriptado de extremo a extremo en la transmisión, o bien en la SwMI (en un sistema de TMO) o bien por la interfaz aérea, podría redireccionarlo de manera que parezca que se ha originado de una parte de transmisión diferente. Aunque el adversario no pueda cambiar el contenido del mensaje, podría provocar confusión si el mensaje, cuando se recibe, parece haberse originado de la MS incorrecta.

Un procedimiento conocido en la técnica para impedir este tipo ataque es confirmar la identidad del remitente de un mensaje acordando claves de encriptación únicas para cada par originador/destino posible para un mensaje. Por tanto, si un mensaje se ha direccionado incorrectamente, se encriptará con la clave incorrecta para la comunicación, y no podrá recuperarse. Este enfoque tiene la desventaja de que es necesario un par de claves diferentes para cada par de usuarios. Esto supone un gran problema de gestión de claves que es necesario resolver. Además, no puede usarse en comunicaciones de grupo en las que el mismo mensaje se envía simultáneamente a un grupo de (tres o más) receptores. Para comunicaciones de grupo, cada usuario podría usar una clave única para su transmisión, permitiendo así que los receptores del mensaje confirmen la identidad del remitente mediante la clave que está usando. Sin embargo, todos los miembros del grupo tendrían que tener un conjunto completo de claves para todos los demás miembros del grupo, lo que a su vez supondría un gran problema de gestión de claves que resolver.

En segundo lugar, es posible confirmar una identidad del remitente de un mensaje usando una firma electrónica codificada con el mensaje. Un enfoque de este tipo puede ser aceptable para mensajes de datos, pero no para una comunicación de voz. Es muy difícil emplear firmas electrónicas de manera satisfactoria en un sistema de comunicación de voz en tiempo real y "de longitud ilimitada". Todo el mensaje debe firmarse si es posible, lo que significa que los receptores no recibirían confirmación de la identidad del remitente hasta que el receptor procese el final del mensaje y luego pueda comprobar la firma electrónica. En cualquier caso, a menudo no es posible recibir el mensaje completo en un sistema de radio móvil en el que un desvanecimiento de la señal puede hacer que se pierdan partes de una comunicación.

En un enfoque alternativo, podrían confirmarse segmentos de voz menores. Sin embargo, una confirmación de mensajes más frecuente requiere una sobrecarga de ancho de banda (y de procesamiento) adicional para enviar, codificar/encriptar y decodificar/desencriptar los mensajes.

Además, se requeriría un sistema de TMO de radio móvil privado que emplee claves de encriptación únicas mientras se soportan cientos de MS individuales para gestionar muchas claves individuales y compartidas.

En el documento US 5.357.571 se describe un método en el que se permite que un grupo de usuarios compartan una clave común para la encriptación de comunicaciones entre el grupo. El objetivo del método descrito es proporcionar comunicaciones privadas adicionales además de las disponibles entre el grupo. Se permite adicionalmente que pares de individuos del grupo obtengan privacidad de otros miembros del mismo grupo, que poseen la clave común, cuando se tienen comunicaciones individuales. Se usa una función predeterminada como modificador de clave de encriptación. La función predeterminada es un secreto acordado entre las dos partes antes de las comunicaciones. Alternativamente, si la función predeterminada es conocida, las identidades se mantienen en secreto. Un ejemplo de la función especificada para su uso como modificador de claves es un código único secreto introducido por un operador del terminal de transmisión y recibido por un operador del terminal de recepción.

Por tanto existe la necesidad de un sistema y un método y un terminal de comunicaciones encriptadas de extremo a extremo mejorados para su uso en el mismo, en los que puedan reducirse las desventajas mencionadas anteriormente y se aumente la probabilidad de seguridad de las comunicaciones resultantes.

Sumario de invención

Según la presente invención en un primer aspecto se proporciona un método de encriptación según la reivindicación 1 de las reivindicaciones adjuntas.

Según la presente invención en un segundo aspecto se proporciona un método para desencriptar según la reivindicación 2 de las reivindicaciones adjuntas.

En el método del primer o segundo aspecto la etapa de combinar puede incluir aplicar una o más de las funciones de combinación de señales siguientes para combinar el código de identificador con la clave compartida: función OR exclusiva (XOR), adición, multiplicación.

La etapa de combinar dicho identificador definida en la reivindicación 1 o la reivindicación 2 con la clave compartida puede ser una de una pluralidad de modificaciones de la clave compartida para proporcionar la clave de encriptación. Otra etapa de modificación puede aplicarse antes y/o durante y/o después de la combinación del identificador con la clave compartida. La(s) etapa(s) de modificación adicional(es) puede(n) incluir, por ejemplo, una o más de las etapas de modificación de claves conocidas en la técnica. Un ejemplo de otro modificador para su uso en el procedimiento de modificación es el número de portadora o frecuencia en uso. Alternativamente, el procedimiento de encriptación puede ser diferente para transmisiones en frecuencias diferentes tal como se conoce en la técnica.

Según la presente invención en un tercer aspecto, se proporciona un método de comunicación entre un terminal de transmisión y uno o más terminales de recepción remotos, siendo el método tal como se define en la reivindicación 3 de las reivindicaciones adjuntas.

En el método según el tercer aspecto, las comunicaciones enviadas entre los terminales que incluyen el terminal de transmisión y el uno o más terminales de recepción pueden ser comunicaciones inalámbricas. Los terminales pueden operarse en un sistema de comunicaciones móviles y uno o más de los terminales puede(n) ser, por tanto, estaciones móviles. El terminal de transmisión y/o uno o más de los terminales de recepción puede(n) ser una estación móvil. El terminal de transmisión o el terminal de recepción o uno de los terminales de recepción puede(n) ser un terminal fijo, por ejemplo usado u operado por un gestor de uso de sistema.

En el método según el tercer aspecto de la invención, preferiblemente la clave compartida se recibe y se almacena por los terminales antes del inicio de la etapa de combinación del método de encriptación o desencriptación. La clave compartida puede emitirse por separado mediante o bajo el control de un gestor de sistema. Éste puede ser un gestor del sistema de comunicaciones, o alguien encargado de gestionar la encriptación dentro del sistema de comunicaciones. Las claves requeridas por los miembros de un grupo seguro definido particular pueden dispensarse de manera manual y usarse de manera manual, por ejemplo programando de manera manual el terminal con la clave, o pueden entregarse mediante comunicación segura, por ejemplo comunicación inalámbrica que usa un mecanismo de recodificación por el aire (ambos métodos son bastante conocidos en sí en la técnica). Cuando cada terminal en el grupo va a programarse de manera manual con la información de clave compartida, por ejemplo en forma de código que comprende dígitos binarios que representan números, letras u otros símbolos o una combinación de éstos, la información puede introducirse en el terminal por un usuario u operador del terminal

usando una interfaz conocida tal como un conjunto de claves proporcionadas en un teclado en el terminal.

La clave compartida puede almacenarse por un terminal, por ejemplo una estación móvil o fija, de una manera conocida. La clave puede almacenarse o bien en una memoria segura en el terminal (una memoria que normalmente no es accesible para el mundo exterior), o en una memoria segura en un módulo de encriptación especial. Para la encriptación de interfaz aérea (y la SCK en DMO tal como se describe más adelante), se prefiere su uso en una estación móvil de una memoria segura. Para una encriptación de extremo a extremo, se prefiere el uso de un módulo de encriptación. En cualquier caso, la clave compartida puede almacenarse en un dispositivo asociado, por ejemplo una tarjeta inteligente (por ejemplo un SIM o módulo de identidad de abonado) en cambio.

En el método según el tercer aspecto de la invención, el identificador del terminal de transmisión ("ID de transmisor") puede transmitirse por el terminal de transmisión mediante comunicación inalámbrica al uno o más terminales de recepción. El ID de transmisor puede almacenarse en una memoria no volátil del terminal de transmisión, que puede ser o no una memoria segura. El ID de transmisor puede transmitirse como parte de una señalización de control de sistema por el aire normal. Esta comunicación de ID está normalmente fuera de la parte encriptada del mensaje, al menos la parte que implica usar la clave modificada proporcionada mediante modificación de la clave compartida por el ID de transmisor según la invención. De ese modo, cada terminal de recepción puede reconocer y extraer el ID de transmisor. El ID de transmisor puede ser, según el protocolo usado, por ejemplo el protocolo de TETRA, incluido en una posición definida previamente en la estructura de la señalización de control. El ID podría estar en los mismos o diferentes lugares en diferentes tramas de señalización, dependiendo del mensaje, pero el ID siempre puede incluirse en algún lugar en la señalización de control y el terminal de recepción siempre puede saber, según el protocolo usado, dónde buscar el ID de transmisor. El terminal de recepción puede almacenar el ID de transmisor recibido en su propia memoria antes de su uso en el procedimiento de desencriptación.

Alternativamente, el ID de transmisor puede transmitirse en un mensaje encriptado separado. Un mensaje de este tipo debe ser por un medio que no requiera que se use el ID individual en el proceso de desencriptación. En TMO, un sistema de encriptación de extremo a extremo podría presentar el ID al terminal de recepción encriptado con una encriptación de interfaz aérea, de modo que el receptor podría usar una encriptación-desencriptación de interfaz aérea para decodificar el ID, luego usar el ID para generar la clave final que va a usarse en la encriptación de extremo a extremo tal como se describió anteriormente.

En una forma del método según el primer, segundo o tercer aspecto de la invención, el método incluye además las etapas de (i) notificar una manera cambiada de combinación a terminales de comunicación que operan en dicho sistema de comunicación inalámbrico y que tienen la clave compartida; y (ii) usar la manera cambiada de combinación a comunicaciones de encriptación y/o desencriptación entre los terminales. La notificación puede llevarse a cabo mediante comunicación inalámbrica, una comunicación especialmente segura (encriptada). La notificación puede realizarse por un gestor de sistema y puede enviarse mediante comunicación inalámbrica.

En el método según el tercer aspecto de la invención cada uno de los terminales que tiene la clave compartida puede enviar transmisiones encriptadas mediante el método según el primer aspecto de la invención y desencriptar las comunicaciones encriptadas recibidas mediante el método según el segundo aspecto de la invención realizándose la encriptación y desencriptación mediante procedimientos correspondientes usando la misma clave de encriptación/desencriptación.

El método según el primer, segundo o tercer aspecto de la invención puede aplicarse en un sistema que opera según los procedimientos de normas TETRA.

En el método según la invención en el primer, segundo o tercer aspecto, el sistema de comunicación en cuestión puede operarse en un modo de operación troncal (TMO). En un modo de este tipo el sistema también incluirá y operará usando instalaciones de sistema fijas, por ejemplo una o más estaciones transceptoras base y una infraestructura de conmutación y gestión.

El método según la invención en el primer, segundo o tercer aspecto puede operar en un sistema que usa una encriptación de interfaz aérea, de modo que el procedimiento de encriptación y el ID de transmisor se apliquen en la misma capa en una pila de protocolos de comunicaciones.

Alternativamente, el método según la invención en el primer, segundo o tercer aspecto puede operar en un sistema que usa una encriptación de extremo a extremo, de modo que el ID de transmisor se aplica por el terminal de transmisión en una primera capa de una pila de protocolos de sistema o jerarquía y los protocolos de encriptación están en una segunda capa de la pila de protocolos de sistema o jerarquía de manera que la etapa de combinar el ID de transmisor y la clave compartida en los procedimientos de encriptación y desencriptación une las dos capas de protocolos para comunicaciones encriptadas.

En el método según el primer, segundo o tercer aspecto de la presente invención, el sistema puede operarse en un

modo de operación directo (DMO) en el que los terminales, especialmente estaciones móviles, pueden comunicarse directamente más que a través de un terminal intermedio tal como una BTS. En este caso, la clave compartida puede comprender una clave de cifrado estática (SCK). Clave de cifrado "estática" significa que la clave se carga en el terminal como clave para usar, en lugar de derivarse dinámicamente de algún otro proceso, y que se cambiará sólo por un procedimiento de sustitución de clave relativamente de manera poco frecuente (de 1 mes a 1 año son valores esperados típicos de la vigencia de una clave). Se denomina "estática" para distinguirla de algunas otras claves usadas en sistemas de comunicación tales como los sistemas de TETRA que son mucho más dinámicos, tales como las claves que en la técnica se denominan "clave de cifrado derivada", que es un subproducto del proceso de autenticación, y la "clave de cifrado común" que pretende sustituirse y una clave nueva enviada a terminales (MS) por el sistema de una manera muy frecuente (por ejemplo cada 24 horas). La clave de cifrado estática puede introducirse en un terminal tal como una MS por un usuario del terminal, por ejemplo a través de un teclado en la MS, y puede almacenarse en una memoria de la manera descrita anteriormente.

Cuando el sistema en el que se aplica la invención comprende un sistema de DMO, el sistema y las MS y los métodos para establecer comunicaciones seguras que se usan en el mismo pueden ser tal como se describe en la solicitud de patente inglesa en tramitación junto con la presente del solicitante n.º 0121236.4 presentada el 1 de septiembre de 2001 (número de publicación GB-A-2379361).

Según la presente invención en un cuarto aspecto se proporciona un sistema de comunicación móvil que comprende una pluralidad de terminales de los que al menos uno es una estación móvil, estando cada terminal adaptado para realizar el método según el primer, segundo o tercer aspecto de la invención.

Según la presente invención en un quinto aspecto se proporciona un terminal, por ejemplo una estación móvil, para comunicaciones de radio móviles y que puede operarse para realizar el método según el primer, segundo o tercer aspecto.

El terminal, por ejemplo estación móvil, según el quinto aspecto puede comprender:

un transmisor de radio para transmitir un mensaje encriptado;

medios de memoria para almacenar una clave compartida asociada con un grupo del que es miembro el terminal, y para almacenar un identificador que identifica el terminal, siendo el identificador una dirección de control de acceso al medio (MAC) dada al terminal de transmisión;

un procesador, acoplado de manera operativa a dicho transmisor y dichos medios de memoria, que puede operarse para generar una clave de encriptación modificada desde una combinación de la clave compartida y el identificador; y

medios de encriptación para encriptar dicho mensaje usando dicha clave de encriptación modificada. El terminal, por ejemplo estación móvil, puede comprender alternativamente o además:

un receptor para recibir un mensaje encriptado;

medios de memoria para almacenar una clave compartida asociada con un grupo del que es miembro el terminal y para almacenar un identificador que identifica un terminal que envió el mensaje, siendo el identificador una dirección de control de acceso al medio (MAC) dada al terminal que envió el mensaje;

un procesador, acoplado de manera operativa a dicho receptor y dichos medios de memoria, que puede operarse para generar una clave de encriptación modificada desde una combinación de la clave compartida y el identificador; y

medios de desencriptación para desencriptar el mensaje usando la clave de encriptación modificada.

El terminal, por ejemplo estación móvil, según el quinto aspecto de la invención puede incluir un medio para llevar a cabo una comunicación segura, un procesador para usar la clave de encriptación actual producida como en el método según el primer aspecto descrito anteriormente para convertir señales que representan información de entrada aplicada por un usuario o desde un dispositivo periférico asociado con la unidad de radio, por ejemplo señales que representan voz, datos de texto o información de imagen, en señales encriptadas para su transmisión a uno o más otros terminales designados. El procesador puede operar de una manera conocida, por ejemplo mediante la generación usando la clave de encriptación de entrada, y opcionalmente una señal de un sello de tiempo de entrada, una secuencia criptográfica (transmisión de claves) y aplicando lo mismo a un combinador de señal junto con una señal que representa la información sin formato que va a convertirse por el combinador de señal a una manera encriptada. El combinador de señal puede operar una función OR exclusiva o una multiplicación o una adición de las señales combinadas o una combinación de dos o más de esas funciones. El procesador puede formar

parte de una unidad de procesamiento común de la unidad de comunicaciones, por ejemplo junto con un procesador para aplicar un algoritmo inverso correspondiente para proporcionar la desencriptación de una señal recibida.

Mediante la invención, la unión criptográfica de un mensaje a la identidad de un terminal de transmisión se proporciona de manera beneficiosa. Por ejemplo, en un sistema de TETRA, el método de encriptación de la invención une la transmisión encriptada de extremo a extremo a la identidad usada en el plano de C de dirección de MAC del terminal de transmisión. Esta unión se realiza sin ninguna señalización, procesamiento o sobrecarga de tiempo. Adicionalmente, la invención impide que una parte que interviene interfiera con una transmisión encriptada enviada desde un terminal a otro de manera que el mensaje aparezca en un receptor que se origina de una parte distinta de la parte de origen verdadera.

Otra ventaja de la invención, particularmente relevante en un sistema de DMO, es que cada terminal de transmisión se transmitirá con una clave de encriptación eficaz diferente, puesto que el ID de transmisor se usa en la composición de cada clave de encriptación modificada. Esto aumentará la seguridad del sistema reduciendo la probabilidad de que el procedimiento de encriptación se descubra por una repetición en la transmisión de claves usada.

La presente invención es principalmente adecuada para su uso para proporcionar comunicaciones de voz seguras entre usuarios en un sistema de comunicaciones móviles. Sin embargo, los inventores de la presente invención conciben usos alternativos o adicionales de la invención. Por ejemplo, la invención podría aplicarse en una red de datos de protocolo de Internet (IP), en la que el ID de fuente de capa 3 de un paquete podría usarse como modificador de claves en una transmisión en la que el contenido del paquete está encriptado. Además, aunque la clave compartida usada puede estar relacionada con la identidad de un grupo de llamada para comunicaciones seguras entre terminales en un sistema de comunicación móvil privado o público, está contemplado por la invención que la clave compartida pueda estar relacionada a cualquier tipo de transmisión, tal como una llamada de grupo de emergencia, una llamada de prioridad preferente, una llamada de difusión encriptada o cualquier otra comunicación de radio móvil en la que se usa la encriptación, ya pueda aplicarse a la norma TETRA o a cualquier otra tecnología de comunicación inalámbrica.

Por tanto, la invención proporciona medios para encriptar mensajes de manera unívoca en el contexto de un entorno de transmisión de punto a punto o de punto a multipunto para proporcionar comunicaciones, especialmente comunicaciones inalámbricas, entre usuarios u operadores de terminales de comunicación en un grupo o emparejamiento seguro definido previamente. Opera modificando una clave de encriptación de grupo secreta establecida previamente compartida por miembros del grupo establecido previamente combinando con la clave de encriptación compartida un código de identificación que define la identidad del terminal de transmisión para proporcionar una clave de encriptación modificada única para ese terminal de transmisión. Proporciona los siguientes beneficios:

(1) Cualquier terminal de recepción del grupo seguro puede validar la transmisión cuando se origina del terminal de transmisión del miembro de grupo correcto mediante conocimiento de la clave compartida secreta y la identidad de ese terminal. La clave compartida secreta puede haberse grabado previamente por el terminal de recepción. La identidad de ese terminal puede transmitirse en forma de código de identificación en una comunicación desde el terminal de transmisión, que puede comprender una señalización de control de sistema asociada con la transmisión encriptada.

(2) Ninguna parte fuera del grupo puede interceptar las comunicaciones de grupo debido a la falta de conocimiento de la clave compartida secreta.

(2) Ninguna persona fuera del grupo puede hacerse pasar por un miembro del grupo enviando un mensaje afirmando que se ha originado por un miembro del grupo, por ejemplo redireccionando o reproduciendo un mensaje anterior, puesto que no podrán generar la clave única real requerida para encriptar la transmisión desde una parte de origen particular.

Esto supera la debilidad de los sistemas de la técnica anterior, en los que un adversario puede reproducir o redireccionar mensajes que entonces pueden percibirse como válidos por los miembros del grupo, incluso si el adversario no puede entender el contenido del mensaje.

(3) Diferentes capas de la pila de protocolos están unidas entre sí de manera criptográfica, puesto que la identidad en la capa de señalización del terminal de transmisión está unida al contenido de mensaje. Esto dificulta mucho más que un sistema que interviene interfiera con las comunicaciones.

(4) La vigencia de clave de la clave compartida secreta puede extenderse, puesto que no se usa directamente para encriptar las comunicaciones. En la técnica se conoce la modificación de claves para extender la vigencia de la clave, aunque el uso del ID de transmisor en o como parte del procedimiento de modificación de claves con los

beneficios resultantes, tal como se describió anteriormente, no se ha usado o sugerido previamente.

El campo principal de aplicación de la invención es en los sistemas de comunicaciones móviles en los que las comunicaciones son (de radio) inalámbricas. Se observa que los métodos de encriptación de la técnica anterior se han publicado para su uso no en este campo sino en otros campos. Por ejemplo, el documento EP-A-0287720 describe un medio para asegurar mensajes que pasan entre terminales individuales que pertenecen a diferentes grupos. Está destinado a comunicaciones individuales y está dirigido al área de transferencia de fondos electrónicos en un punto de venta (EFTPOS) de la industria bancaria. Esta publicación de patente reivindica una comunicación entre “pares de partes” (en lugar de grupos). El método descrito proporciona un mecanismo para comunicaciones individuales entre miembros de diferentes grupos. Específicamente no se dirige a comunicaciones entre miembros del mismo grupo. En cambio, la presente invención proporciona un mecanismo para las comunicaciones de grupo entre miembros del mismo grupo. El método descrito del documento EP-A-0287720 se dirige específicamente a un entorno en el que los terminales en un grupo confían en terminales del otro grupo, pero no es necesario que haya una confianza entre miembros del mismo grupo. De hecho, es probable que el escenario de EFTPOS proporcione un entorno en el que explícitamente no hay confianza entre los miembros del mismo grupo. En cambio, la invención proporciona un entorno en el que los miembros del mismo grupo confían explícitamente entre sí y no tienen explícitamente confianza en los terminales fuera de este grupo.

Además, el documento EP-A-0287720 requiere que cada parte de comunicación se proporcione por una entidad de emisión de clave separada con una clave única que es una función derivada de la propia identidad de la parte enviada a la parte con una clave diferente. Esta clave única debe proporcionarse de antemano y no puede calcularse por esa parte que se comunica. El método de la invención no requiere un aprovisionamiento previo de este tipo de una clave única, y de hecho dada la dinámica de los sistemas de comunicaciones móviles (en comparación con un sistema que usa terminales fijos en una aplicación bancaria) sería poco probable que un aprovisionamiento previo de este tipo fuera aceptable para los operadores del sistema.

El documento EP-A-0989710 (JP-A-2000-156676) describe un método para proporcionar una prestación para una transmisión segura de contenido entre un *host* que suministra contenido y un terminal que lo solicita. Deriva una clave basándose en una identidad de terminal o frase de contraseña generada por un usuario de terminal, donde la frase de contraseña también se transmite al *host* que suministra de modo que el *host* puede generar la misma clave. Esta clave puede usarse o bien para encriptar contenido directamente, o bien para intercambiar una clave de encriptación de contenido que a su vez encripta el contenido. Puede usarse un valor *hash* de la clave para confirmar la clave en transacciones posteriores.

El método publicado anterior del documento EP-A-0989710 proporciona un medio de protección de la transferencia individual de información entre un *host* fijo y un terminal fijo. A diferencia de la invención, explícitamente no proporciona comunicaciones de grupo entre miembros de un grupo seguro definido previamente en un sistema de comunicaciones móviles. En el método publicado anteriormente, la clave de usuario se deriva directamente de la identidad de usuario o frase de contraseña. No se usa como modificador de claves. Inicialmente no se usa ninguna clave secreta en la generación de la clave de usuario. En cambio, ambas etapas se usan en el método de la invención.

Además, es evidente que el método del documento EP-A-0989710 requiere un algoritmo de generación de clave secreta para generar la clave de usuario a partir de la frase de contraseña o identidad. Por el contrario, una persona que intercepta la transferencia de la frase de contraseña de identidad también podría derivar la clave, haciendo la transferencia insegura. Alternativamente, la red de tránsito debe ofrecer otra capa de seguridad, incluyendo la encriptación, para proteger la frase de contraseña o identidad en el tránsito. El método de la invención requiere cualquiera de los siguientes: utiliza una clave de grupo secreta, que permite de manera conveniente que el algoritmo sea de conocimiento público, y permite que el ID de transmisor se transfiera sin encriptación adicional esencial. Por tanto, la operación de la invención es muy diferente en principio de la del método descrito en el documento EP-A-0989710.

Ahora se describirán realizaciones de la presente invención a modo de ejemplo sólo con referencia a los dibujos adjuntos, en los que:

Breve descripción de los dibujos

La figura 1 muestra un diagrama de bloques esquemático de un sistema de comunicaciones de radio de TMO que puede adaptarse para operar según las realizaciones de la presente invención.

La figura 2 muestra un diagrama de bloques esquemático de una estructura jerárquica de sistema conocida usada en comunicaciones móviles.

La figura 3 muestra un diagrama de bloques esquemático de una estructura jerárquica de sistema de comunicación

adaptada para usarse según una realización de la presente invención.

La figura 4 muestra un diagrama de bloques esquemático de un terminal de comunicaciones móviles que implementa la presente invención.

La figura 5 muestra un diagrama de bloques de un ejemplo de un procesador de encriptación útil en el terminal mostrado en la figura 4.

Descripción de realizaciones de la invención

En referencia en primer lugar a la figura 1, un sistema 100 de comunicaciones de TETRA de radio, que puede estar adaptado para operar según una o más realizaciones de la invención, se muestra a grandes rasgos. Generalmente, el protocolo de interfaz aérea se administra desde estaciones transceptoras base del sistema que están fijas y separadas geográficamente, soportando una estación base una célula (o, por ejemplo, sectores de una célula).

Una pluralidad de MS 112-116 y terminales fijos (no mostrados), se comunican a través de la interfaz 118-120 aérea seleccionada con una pluralidad de estaciones 122-132 transceptoras base (BTS). Con fines de claridad se muestra un número limitado sólo de MS y BTS, concretamente las MS 112-116 y las BTS 122-132.

La infraestructura del sistema en un sistema de TETRA se denomina generalmente infraestructura de conmutación y gestión (SwMI). En la figura 1, el sistema 100 incluye una SwMI 110, que incluye sustancialmente todos los elementos operativos de sistema aparte de las unidades móviles. Las BTS 122-132 pueden conectarse a una red 134 telefónica conmutada pública (PSTN) convencional a través de controladores 136-140 de estación base (BSC) y centros 142-144 de conmutación móviles (MSC).

Cada BTS 122-132 está diseñada principalmente para dar servicio a su célula primaria, conteniendo cada BTS 122-132 uno o más transceptores. Las BTS 122-132 se comunican 156-166 con el resto de la infraestructura de sistema a través de una interfaz 168 de retransmisión de trama.

Cada BSC 136-140 puede controlar una o más BTS 122-132, estando los BSC 136-140 interconectados generalmente a través de MSC 142-144. Por tanto, los BSC 136-140 pueden comunicarse entre sí, si se desea, para pasar información de control o administración de sistema entre sí, siendo los BSC 136-140 responsables de establecer y mantener un canal de control y canales de tráfico para MS 112-116 a las que puede darse servicio asociadas con los mismos. Por tanto, la interconexión de los BSC 136-140 permite que un sistema de comunicación de radio troncal soporte un traspaso de las MS 112-116 entre células.

Cada MSC 142-144 proporciona una pasarela a la PSTN 134, con los MSC 142-144 interconectados a través de un centro 146 de operaciones y gestión (OMC) que administra el control general del sistema 100 de radio troncal, tal como se entenderá por los expertos en la técnica. Los diversos elementos de sistema, tales como BSC 136-138 y OMC 146, incluirán una lógica 148-152 de control, con los diversos elementos de sistema teniendo habitualmente una memoria 154 asociada (mostrada sólo en relación con el BSC 138 por motivos de claridad). La memoria almacena normalmente datos operativos recopilados históricamente así como datos de llamada entrante, información de sistema y algoritmos de control.

Haciendo referencia ahora a la figura 2, se muestra un diagrama de bloques de una estructura jerárquica de sistema de TMO conocida o pila 200 de protocolos según la estructura de protocolo de OSI bien conocida. La estructura 200 jerárquica está dispuesta en varias capas. Con el fin de describir más adelante los conceptos inventivos de la presente invención, ahora se describirá una capa “2” 210 y una capa “3” y superior 220.

La información que se encamina, que es información 250 de usuario, se conoce como información contenida en un “plano de U” (o plano de usuario) 240 de la estructura 200. La información 250 de usuario es independiente de la información 230 de control de sistema contenida en el “plano de C” (o plano de control) de la estructura 200.

Una capa 260 de control de acceso al medio (MAC) está en la parte inferior de la capa 2 del plano 230 de C y el plano 240 de U. La capa 260 de MAC usa un direccionamiento para distinguir una MS de otra. A cada MS que opera en el sistema se le da una dirección de MAC de capa 2 única. La dirección de MAC no proporciona ninguna confidencialidad, pero permite que se distingan las transmisiones, tanto hacia como desde MS diferentes.

Haciendo referencia ahora a la figura 3, se muestra una estructura 300 jerárquica de sistema de comunicación de TMO adaptada según una realización de la presente invención. Los ítems que tienen los mismos números de referencia que los mostrados en la figura 2 tienen la misma función. Como en la estructura mostrada en la figura 2, la información que se encamina en la estructura 300, que es información 250 de usuario, se conoce como información contenida en el “plano de V” (o plano de usuario) 240 de la estructura. La información 250 de usuario es independiente de la información 230 de control contenida en el “plano de C” (o plano de control) de la estructura 300.

Una identidad 320 de MAC de capa 2 de la MS de cada remitente de una transmisión se pasa a una función 310 de procesamiento de encriptación. La función 310 de procesamiento de encriptación en este caso representa la aplicación de un algoritmo por cada MS u otro terminal que participa en comunicaciones seguras en el sistema para encriptar y desencriptar transmisiones. La función 310 de procesamiento de encriptación usa la identidad 320 de la capa 2, conjuntamente con una clave compartida segura que se almacena en la memoria, por ejemplo de cada MS que participa, en una función de modificación para generar una clave de encriptación de transmisión real que puede usarse para la encriptación y desencriptación de la información 250 de usuario.

Por tanto, cualquier remitente o receptor de una transmisión segura usa la identidad 320 (ID) de capa 2 del remitente junto con la clave compartida, es decir una clave compartida de un grupo particular, por ejemplo un grupo de charla seguro designado, para producir una clave de encriptación para permitir transmisiones entre miembros del grupo que van a encriptarse y/o desencriptarse. De esta manera, si la transmisión se recibiera de manera que pareciera que se ha enviado desde un usuario diferente que no tiene identidad del remitente, la transmisión no podría desencriptarse.

Haciendo referencia ahora a la figura 4, se muestra un diagrama de bloques de una unidad de abonado que es una estación 112 móvil (MS) adaptada para operar usando una realización de la presente invención. La MS 112 puede ser adecuada para operar en un TMO (por ejemplo tal como se ilustra en la figura 1) o un DMO dependiendo del modo seleccionado.

La MS 112 incluye una antena 402 acoplada preferiblemente a un filtro dúplex o circulador 404 que proporciona un aislamiento entre cadenas de recepción y transmisión dentro de la MS 112. La cadena de receptor incluye un circuito 406 frontal de receptor (que de manera eficaz proporciona una recepción, filtrado y conversión de frecuencia de banda base o intermedia). El circuito 406 frontal recibe comunicaciones de señal de otro terminal, tal como otra MS, en su grupo de charla seguro. El circuito 406 frontal está acoplado en serie a un procesador 408 de señal (realizado generalmente por un procesador de señal digital, DSP). El procesador 408 de señal realiza una demodulación de señal, corrección de errores y formateo, y recupera la información encriptada de extremo a extremo desde la señal recibida. Una señal que representa la información recuperada por el procesador 408 de señal se acopla en serie a un procesador 409 de encriptación, cuya operación se describe adicionalmente más adelante con respecto a la figura 5.

Un temporizador 418 puede estar acoplado de manera operativa al procesador 409 de encriptación para proporcionar una protección frente a la reproducción, de una manera conocida mediante modificación de clave u otro medio, al proceso de encriptación además del procedimiento de modificación que utiliza la clave compartida y el código de identificación del transmisor, por ejemplo la identidad de transmisor de MAC de capa 2 tal como se describe con referencia a la figura 4.

Tal como se conoce en la técnica, las señales recibidas que se han desencriptado por el procesador 409 de encriptación se introducen normalmente en un dispositivo 410 de procesamiento de banda base, que toma la información desencriptada recibida desde el procesador 409 de encriptación y la formatea de una manera adecuada para su envío a un dispositivo 411 de salida, tal como un altavoz y/o pantalla de visualización, por ejemplo una unidad de presentación visual (VDU).

En una realización alternativa de la invención, las funciones del procesador 408 de señal y el dispositivo 410 de procesamiento de banda base pueden proporcionarse dentro del mismo dispositivo físico. La función del procesador 409 de encriptación también puede estar previsto dentro del mismo dispositivo físico o bien como procesador 408 de señal o bien como función 410 de procesamiento de banda base, o ambos.

Un controlador 414 controla el flujo de información y el estado operativo de los procesadores dentro de la MS 112.

La MS 112 no podrá desencriptar una transmisión encriptada recibida si la MS 112 no posee la clave compartida, y el ID de transmisor, por ejemplo identificador de capa 2, de la MS de envío, o si la transmisión se ha corrompido para afectar al ID de transmisor de la MS de envío. En este último caso, parecería que la transmisión se ha enviado desde un usuario diferente, y por tanto la transmisión no podría desencriptarse. La MS 112 tampoco podrá desencriptar la transmisión encriptada si no posee el algoritmo de función de combinación correcto.

Con respecto a la cadena de transmisión de la MS 112, ésta incluye esencialmente un dispositivo 420 de entrada, tal como un micrófono, acoplado en serie a través de un procesador 410 de banda base, una función 409 de procesamiento de encriptación, la función 408 de procesamiento de señal, un conjunto 422 de circuitos de transmisor/modulación y un amplificador 424 de potencia. El procesador 408, el conjunto 422 de circuitos de transmisor/modulación y el amplificador 424 de potencia son operativamente sensibles al controlador 414, con una salida del amplificador 424 de potencia acoplado al filtro dúplex o circulador 404, tal como se conoce en la técnica.

La cadena de transmisión en la MS 112 toma la señal de banda base desde el dispositivo 420 de entrada y la

convierte en información que puede encriptarse por el procesador 409 de encriptación. El procesador 409 de encriptación la encripta usando una clave de encriptación, que es una función de una clave compartida almacenada dentro del procesador 409 de encriptación y un ID de transmisor, por ejemplo identidad de MAC de capa 2, que puede proporcionarse por el procesador 408, o algún otro dispositivo con capacidad de almacenamiento dentro de la MS 112. La información encriptada se pasa entonces al procesador 408 de señal en el que se codifica para su transmisión mediante el conjunto 422 de circuitos de transmisión/modulación y el amplificador 424 de potencia.

La invención también contempla que la función de combinación usada por el procesador 409 de encriptación puede ser cualquier función de combinación adecuada, tal como una XOR, adición, multiplicación, etc. o cualquier combinación de tales operaciones. Tales combinadores también se conocen bien *per se*. Además, el procesador 409 de encriptación puede modificar la clave compartida mediante uno o más procedimientos de modificación adicionales (además de una combinación con el ID de transmisor) tal como se indicó anteriormente.

El procesador 408 de señal en la cadena de transmisión puede implementarse de manera distinta del procesador en la cadena de recepción. Alternativamente, puede usarse un único procesador 408 para implementar un procesamiento de señales tanto de transmisión como de recepción, tal como se muestra en la figura 4.

Naturalmente, los diversos componentes dentro de la MS 112 pueden realizarse en forma de componentes integrados o discretos, siendo por tanto una última estructura una selección de estas formas.

Haciendo referencia ahora a la figura 5, se muestra un procesador 500 de encriptación, adecuado para su uso como procesador 409 de la figura 4. El procesador 500 de encriptación produce una clave de encriptación que se usa de una manera conocida en una función 550 de encriptación/desencriptación para encriptar y desencriptar información comunicada por el usuario, por ejemplo información contenida dentro del plano de U ilustrado en la figura 3. La clave de encriptación es una clave modificada producida (al menos) por una función 540 de combinación según una realización de la invención.

La función 540 de combinación opera para combinar dos entradas de la siguiente manera. Una primera entrada comprende una señal 520 que representa el ID de transmisor, por ejemplo la identidad de MAC de capa 2 ilustrada en la figura 3, del terminal que envía una transmisión. Para la encriptación de un mensaje que va a transmitirse por la MS 112 que contiene el procesador 500, ésta es la identidad de esa MS, por ejemplo según se obtiene desde un almacenamiento de memoria. Para la desencriptación de un mensaje desde otra MS ésta es la identidad de esa otra MS, por ejemplo según se recupera de la señalización de control enviada por la otra MS tal como se describió anteriormente. Una segunda entrada comprende una clave compartida almacenada proporcionada por un elemento 530 de memoria. La clave compartida almacenada se usa por un grupo de charla seguro particular que incluye la MS 112 que incluye el procesador 500.

La salida de la función 540 de combinación, tal como se indicó anteriormente, es una clave modificada que se introduce en la función 550 de encriptación/desencriptación. La función 550 de encriptación/desencriptación usa la clave modificada de una manera conocida para aplicar un algoritmo de encriptación para encriptar la información 560 de usuario clara para generar información 570 de usuario encriptada o para aplicar un algoritmo de encriptación inverso para desencriptar la información 570 de usuario encriptada para generar la información 560 de usuario clara que permite de ese modo que se recupere la información original.

El procesador 500 de encriptación puede operar de una manera conocida tal como se describió anteriormente para combinar la clave de encriptación producida por la función 540 de combinación que puede estar, por ejemplo, en forma de secuencia criptográfica (transmisión de claves) con la información 560 de usuario clara para producir la información 570 de usuario encriptada.

REIVINDICACIONES

1. Método para proporcionar comunicaciones de grupo seguras en un sistema (100) de comunicación entre una pluralidad de terminales (112, 114, 116) que emplean un protocolo de encriptación que usa una clave de encriptación compartida en cada uno de la pluralidad de terminales en el grupo, incluyendo el método modificar una clave de encriptación compartida asociada con el grupo en un terminal (112) de transmisión para proporcionar una clave de encriptación modificada e información de encriptación que va a transmitirse por el terminal de transmisión usando la clave de encriptación modificada, en el que la clave de encriptación compartida se modifica combinando la clave de encriptación compartida con un identificador (520) que proporciona una identificación única del terminal de transmisión, caracterizado porque:

(i) el identificador (520) es una dirección de control de acceso al medio (MAC) dada al terminal (112) de transmisión; y

(ii) el identificador (520) se transmite en la señalización de control por el terminal (112) de transmisión mediante comunicación inalámbrica a una pluralidad de terminales (114, 116) de recepción, y se extrae y se reconoce mediante la pluralidad de terminales (114, 116) de recepción.

2. Método para desencriptar información en una comunicación de grupo recibida en cada uno de una pluralidad de terminales (114, 116) de recepción desde un terminal (112) de transmisión en un sistema de comunicación que proporciona comunicaciones de grupo seguras entre una pluralidad de terminales (112, 114, 116) en el grupo que emplean un protocolo de encriptación que usa una clave de encriptación compartida asociada con el grupo en cada uno de la pluralidad de terminales (112, 114, 116), incluyendo el método proporcionar en cada uno de la pluralidad de terminales (114, 116) de recepción una clave de desencriptación que corresponde a una clave de encriptación asociada con el mensaje encriptado recibido y desencriptar la información usando la clave de desencriptación, en el que la clave de desencriptación se proporciona combinando con la clave de encriptación compartida un identificador que identifica el terminal (112) de transmisión, caracterizado porque:

(i) el identificador (520) es una dirección de control de acceso al medio (MAC) dada al terminal (112) de transmisión; y

(ii) el identificador se transmite en la señalización de control por el terminal (112) de transmisión mediante comunicación inalámbrica a la pluralidad de terminales (114, 116) de recepción y se extrae y se reconoce mediante la pluralidad de terminales (114, 116) de recepción.

3. Método según la reivindicación 1, que incluye:

(i) transmitir, el terminal (112) de transmisión, una comunicación que incluye información encriptada que se encripta mediante el uso de la clave de encriptación modificada; y

(ii) recibir, los terminales (114, 116) de recepción, la comunicación y desencriptar la información encriptada mediante el uso de una clave de encriptación modificada correspondiente.

4. Método según una cualquiera de las reivindicaciones anteriores y en el que la etapa de combinar incluye aplicar una o más de las funciones de combinación de señales siguientes para combinar el identificador con la clave compartida:

función OR exclusiva (XOR), adición, multiplicación.

5. Método según una cualquiera de las reivindicaciones 1 a 4 y en el que la etapa de combinar dicho identificador con la clave compartida es una de una pluralidad de modificaciones de la clave compartida para proporcionar la clave de encriptación o desencriptación modificada.

6. Método según una cualquiera de las reivindicaciones 3 a 5 y en el que la comunicación enviada entre los terminales que incluyen el terminal (112) de transmisión y los terminales (114, 116) de recepción es una comunicación inalámbrica.

7. Método según la reivindicación 6 y en el que los terminales (112, 114, 116) pueden operarse en un sistema de comunicaciones móviles y uno o más de los terminales (112) es una estación móvil.

8. Método según una cualquiera de las reivindicaciones anteriores 3 a 7 y en el que la clave compartida se recibe y se almacena por los terminales (112, 114, 116) antes de dicha combinación.

9. Método según la reivindicación 6, la reivindicación 7 o la reivindicación 8 y en el que la clave compartida se envía a los terminales (112, 114, 116) mediante una comunicación inalámbrica encriptada.

10. Método según una cualquiera de las reivindicaciones 6 a 9 y en el que la clave compartida comprende un código introducido en cada terminal (112, 114, 116) mediante un usuario o un operador del mismo.

11. Método según una cualquiera de las reivindicaciones anteriores y en el que la clave compartida se almacena en una memoria (530) segura del terminal o en un módulo de encriptación o en un dispositivo asociado con el terminal.

12. Método según una cualquiera de las reivindicaciones anteriores, en el que el identificador se almacena dentro de una memoria del terminal (112) de transmisión y se recupera de la memoria para su transmisión a la pluralidad de terminales (114, 116) de recepción.

13. Método según una cualquiera de las reivindicaciones anteriores y en el que el identificador se transmite como parte de señalización de control de sistema de manera no encriptada.

14. Método según una cualquiera de las reivindicaciones 1 a 12 y en el que el identificador se transmite en un mensaje encriptado.

15. Método según una cualquiera de las reivindicaciones anteriores 6 a 14, incluyendo además el método las etapas de:

(i) notificar una manera cambiada de combinación a terminales de comunicación que operan en dicho sistema de comunicación inalámbrico y que tienen la clave compartida; y

(ii) usar la manera cambiada de combinación a comunicaciones de encriptación y/o desencriptación entre los terminales.

16. Método según una cualquiera de las reivindicaciones 6 a 15 y en el que cada uno de los terminales que tienen la clave compartida puede enviar transmisiones de grupo encriptadas, encriptadas usando el método según la reivindicación 1 y desencriptando transmisiones de grupo encriptadas recibidas mediante el método según la reivindicación 2.

17. Método según una cualquiera de las reivindicaciones anteriores y en el que el sistema (100) de comunicación puede operarse en un modo de operación troncal (TMO).

18. Método según una cualquiera de las reivindicaciones anteriores y usándose el método en un modo de operación directo (DMO).

19. Método según una cualquiera de las reivindicaciones anteriores y en el que la clave compartida comprende una clave de cifrado estática.

20. Método según una cualquiera de las reivindicaciones anteriores y en el que el sistema (100) usa una encriptación de interfaz aérea, de modo que el procedimiento de encriptación y la identificación de terminal de transmisión operan en la misma capa en una pila de protocolos de comunicaciones.

21. Método según una cualquiera de las reivindicaciones 1 a 20 y en el que el sistema (100) usa una encriptación de extremo a extremo, de modo que la identificación de terminal de transmisión y el procedimiento de encriptación operan en niveles diferentes en la pila de protocolos, mediante lo cual la etapa de combinación une las capas de la pila de protocolos entre sí.

22. Método según una cualquiera de las reivindicaciones anteriores y en el que el sistema (100) en el que se aplica el método opera según procedimientos de normas TETRA.

23. Sistema (100) de comunicación móvil que comprende una pluralidad de terminales (112, 114, 116) adaptado cada uno para realizar el método según una cualquiera de las reivindicaciones anteriores, en el que al menos uno de los terminales es una estación móvil.

24. Sistema según la reivindicación 23 y pudiendo operarse el sistema (100) en un modo de operación troncal (TMO).

25. Sistema (100) según la reivindicación 23 o la reivindicación 24 y pudiendo operarse el sistema en un modo de operación directo (DMO).

26. Sistema (100) según una cualquiera de las reivindicaciones 23 a 25 y en el que la clave compartida comprende una clave de cifrado estática.

27. Sistema (100) según una cualquiera de las reivindicaciones 23 a 26 y usando el sistema una encriptación de interfaz aérea, de modo que el procedimiento de encriptación y la identificación de terminal de transmisión operan en la misma capa en una pila de protocolos de comunicaciones.

28. Sistema (100) según una cualquiera de las reivindicaciones 23 a 27 y usando el sistema una encriptación de extremo a extremo, de modo que la identificación de terminal de transmisión y el procedimiento de encriptación operan en niveles diferentes en la pila de protocolos, mediante lo cual la etapa de combinación une las capas de la pila de protocolos entre sí.

29. Sistema (100) según una cualquiera de las reivindicaciones 23 a 27 y operando el sistema según procedimientos de normas TETRA.

30. Terminal (112) para comunicaciones de radio y que puede operarse para realizar el método según una cualquiera de las reivindicaciones 1 a 22, o adaptado para usarse en un sistema según una cualquiera de las reivindicaciones 23 a 29.

31. Terminal (112) según la reivindicación 30, comprendiendo el terminal:

un transmisor (408, 422, 424, 402) de radio para transmitir un mensaje de grupo encriptado;

medios (530) de memoria para almacenar una clave compartida asociada con un grupo del que es miembro el terminal, y para almacenar un identificador (520) que identifica el terminal, caracterizado porque el identificador es una dirección de control de acceso al medio (MAC) dada al terminal de transmisión;

un procesador (540), acoplado de manera operativa a dicho transmisor y dichos medios de memoria, que puede operarse para generar una clave de encriptación modificada desde una combinación de la clave compartida y el identificador; y

medios (550) de encriptación para encriptar dicho mensaje usando dicha clave de encriptación modificada.

32. Terminal (112) según la reivindicación 30 o la reivindicación 31, y que comprende:

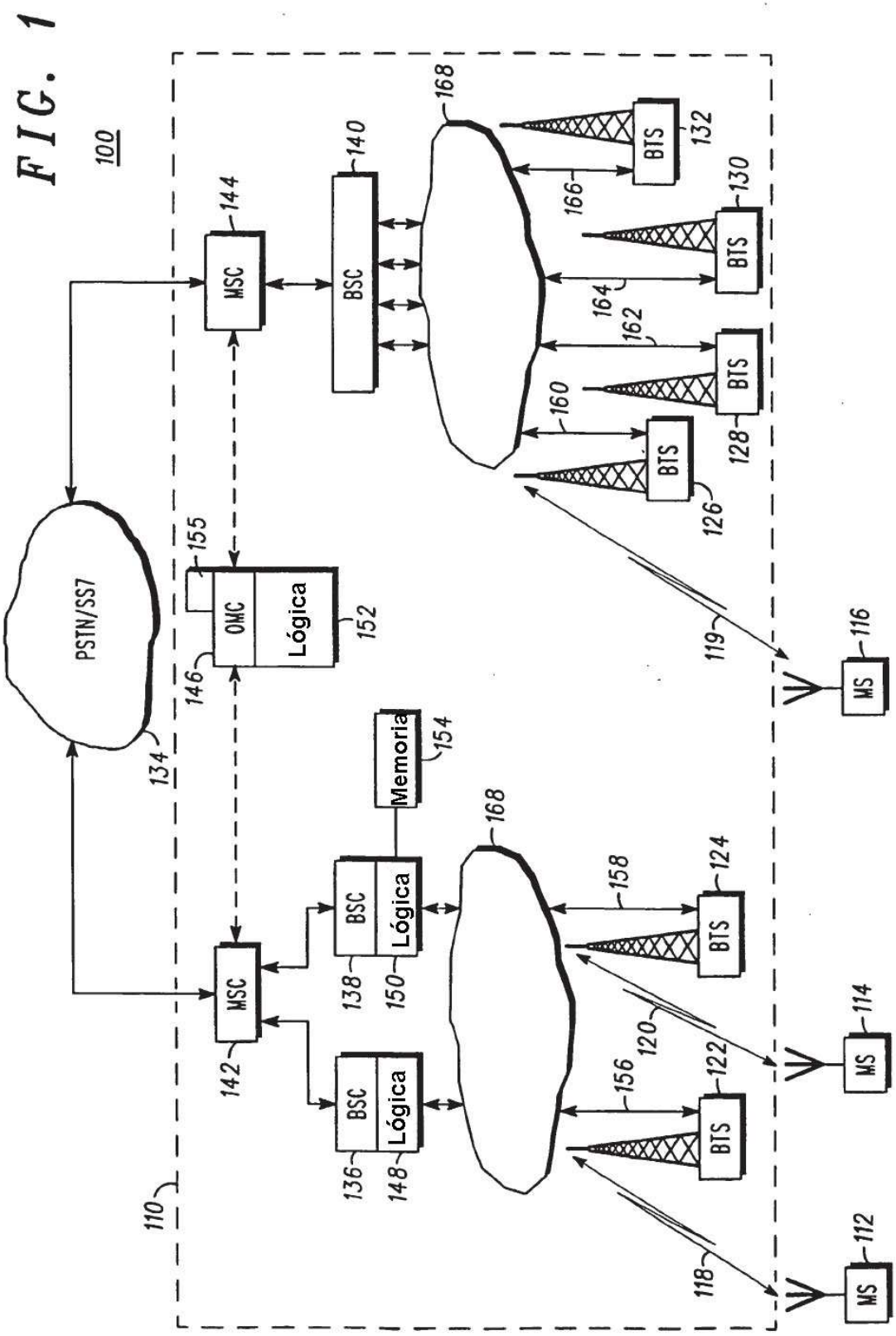
un receptor (402, 406, 408) para recibir un mensaje de grupo encriptado;

medios (530) de memoria para almacenar una clave compartida asociada con un grupo del que es miembro el terminal y para almacenar un identificador que identifica un terminal que envió el mensaje, caracterizado porque el identificador es una dirección de control de acceso al medio (MAC) dada al terminal que envió el mensaje;

un procesador (540), acoplado de manera operativa a dicho receptor y dichos medios de memoria, que puede operarse para generar una clave de encriptación modificada desde una combinación de la clave compartida y el identificador; y medios (550) de desencriptación para desencriptar el mensaje usando la clave de encriptación modificada.

33. Terminal (112) según una cualquiera de las reivindicaciones 30 a 32 y que es una estación móvil.

FIG. 1


100
PSTN/SS7
134
MSC
144
BSC
140
OMC
Lógica
155
146
152
Memoria
154
MSC
142
BSC
Lógica
138
150
BSC
Lógica
136
148
110
168
168
168
BTS
132
BTS
130
BTS
128
BTS
126
BTS
124
BTS
122
166
164
162
160
158
156
120
118
119
MS
116
MS
114
MS
112

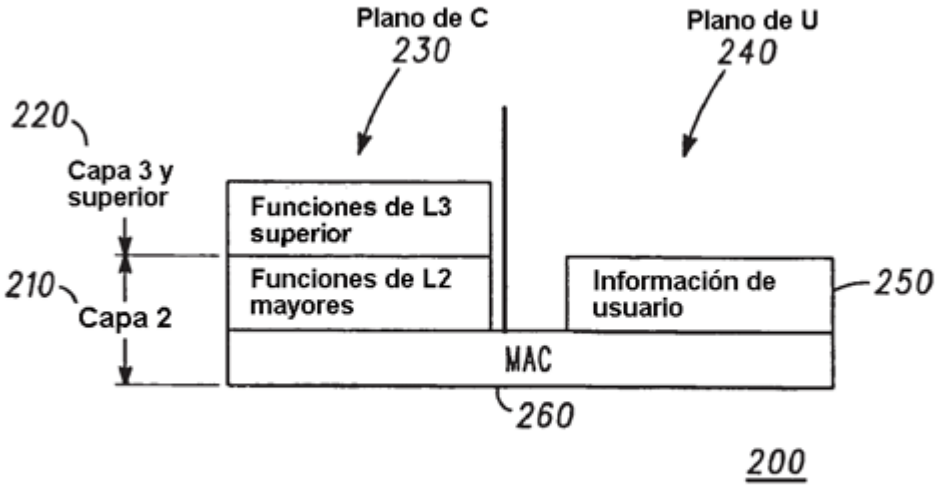

Plano de C
230
Plano de U
240
220
Capa 3 y superior
Funciones de L3 superior
Funciones de L2 mayores
210
Capa 2
Información de usuario
250
MAC
260
200

FIG. 2

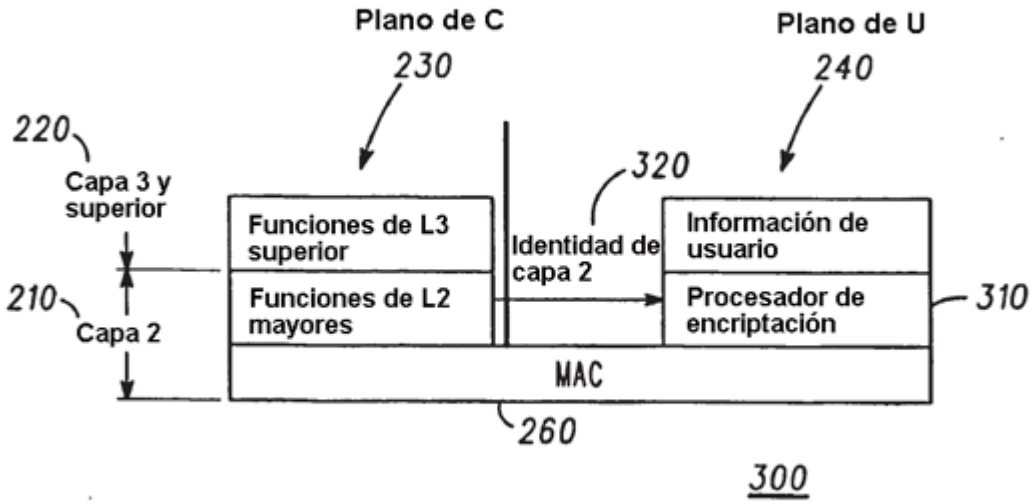

Plano de C
230
Plano de U
240
220
Capa 3 y superior
320
Funciones de L3 superior
Identidad de capa 2
Información de usuario
210
Capa 2
Funciones de L2 mayores
Procesador de encriptación
310
MAC
260
300

FIG. 3

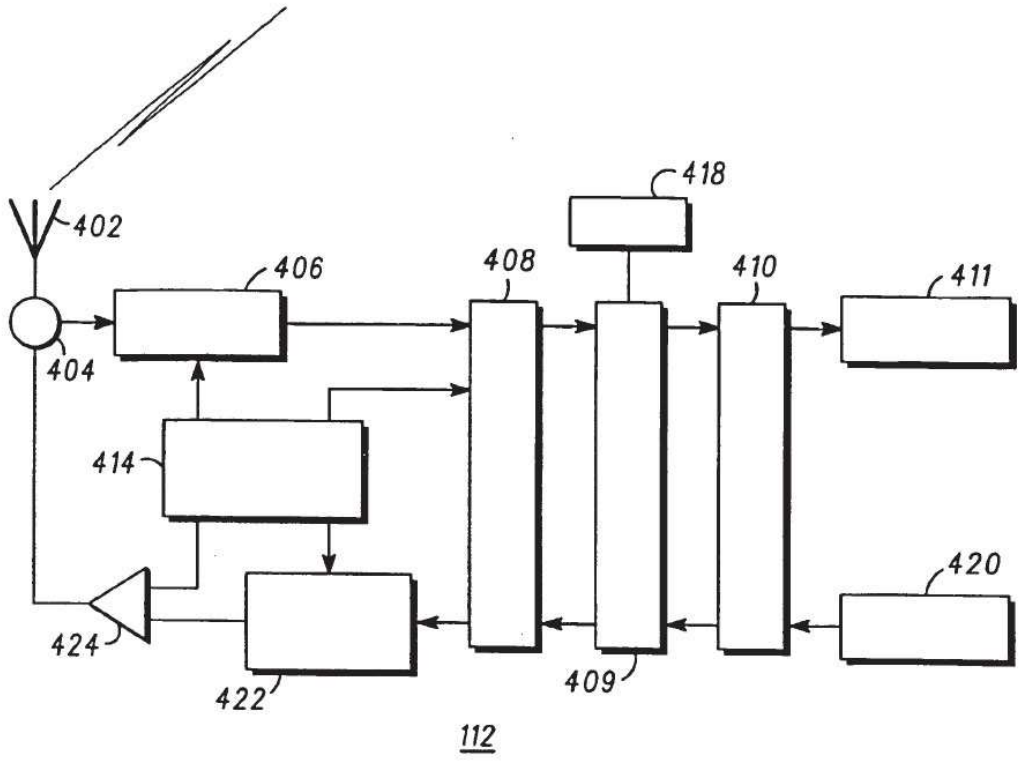

418
402
406
408
410
411
404
414
420
424
422
409
112

FIG. 4

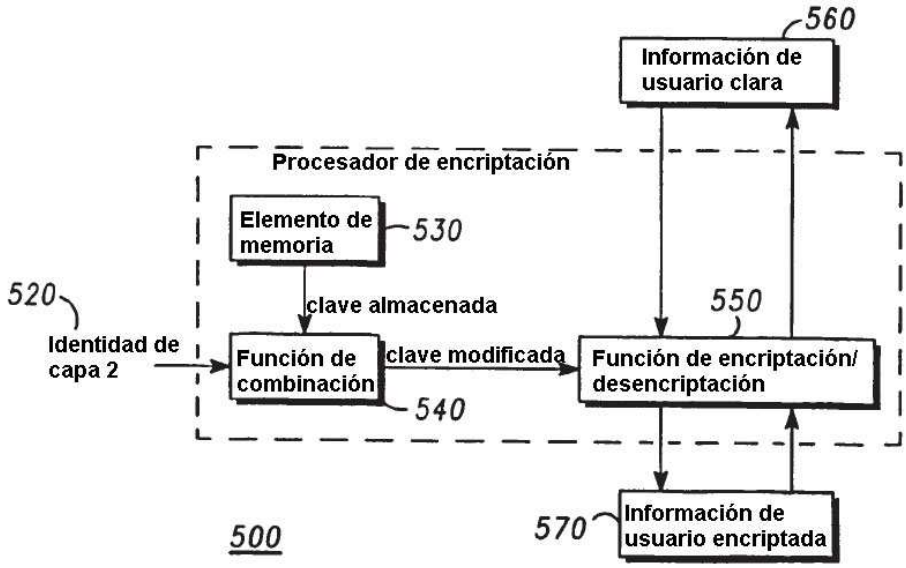

560
Información de usuario clara
Procesador de encriptación
Elemento de memoria
530
clave almacenada
520
550
Identidad de capa 2
Función de combinación
clave modificada
Función de encriptación/ desencriptación
540
570
Información de usuario encriptada
500

FIG. 5