(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 818**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.05.2013 E 13167508 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.12.2014 EP 2665224**

(54) Título: **Procedimiento de distribución de una clave digital de cifrado hacia terminales de telecomunicaciones**

(30) Prioridad:

15.05.2012 FR 1254466

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.04.2015

(73) Titular/es:

AIRBUS DS SAS (50.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR y
CASSIDIAN FINLAND OY (50.0%)

(72) Inventor/es:

PRAT, JULIEN;
MOUFFRON, MARC;
RINNE, SIMO y
KAUHANEN, LARI-MIKKO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de distribución de una clave digital de cifrado hacia terminales de telecomunicaciones

Campo

La presente invención se refiere al campo técnico de las comunicaciones cifradas que precisan de una clave de cifrado para la identificación de terminales y de cifrado de los datos, de voz y de direcciones.

Más en particular, el campo de la invención concierne a un procedimiento de distribución de clave que permite la cohabitación de dos sistemas de criptografía que se basan en diferentes concepciones de claves de cifrado. El campo de la invención se refiere a las problemáticas de migraciones de arquitecturas diferentes de sistemas de comunicación que cohabitan antes de un despliegue completo.

Estado de la técnica anterior

Actualmente existen soluciones, para ciertas redes de comunicación, para cifrar las transmisiones de datos y/o de voz. Determinadas redes cifradas precisan del cifrado de las direcciones de los terminales para asegurar una máxima confidencialidad.

Es típicamente el caso, generalmente, de una infraestructura de red profesional de radiocomunicación de tipo PMR.

Las redes profesionales de comunicación PMR (“Professional Mobile Radiocommunications” en inglés) de tipo TETRA (“Trans European Trunked Radio”) o TETRAPOL, definido por el foro industrial TETRAPOL (http://www.tetrapol.com), o también de tipo P25, definido por la “Telecommunications Industry Association (TIA)” para la “Association of Public-Safety Communications Officers (APCO)” son redes independientes de comunicación móvil especializadas para uso de las empresas o de las administraciones, en particular para procurar la seguridad pública, la seguridad industrial o en las actividades de transporte. Las redes PMR son utilizadas ampliamente por los servicios de seguridad pública (Guardia Civil y policía nacional, por ejemplo) y de emergencias, y también por otras muchas categorías de usuarios (transportes públicos, aeropuertos,...). Son redes privadas que presentan un elevado nivel de seguridad.

La estructura de las redes profesionales de comunicación está normalizada. Estas últimas estriban en una arquitectura en malla común para todo tipo de redes de comunicación. Los terminales móviles se conectan a la red a través de puntos de acceso inalámbrico, denominados estaciones base y denotados por BS en la continuación de este documento.

Las redes de comunicación cifradas precisan de una arquitectura en la que un servidor de gestión de claves permite gestionar diferentes funciones. En particular, realiza diferentes funciones tales como la renovación de las claves o su adquisición desde un sistema tercero. Adicionalmente, el servidor de gestión de claves asume la tarea de la distribución de las claves a los equipos de la red.

Generalmente, se distribuyen claves comunes y claves individuales que permiten la gestión de diferentes calidades de servicios de comunicación para los usuarios de la red.

Las claves comunes pueden ser utilizadas para servicios de difusión de datos desde un terminal de origen o una estación base. Generalmente se utilizan para comunicaciones de tipo difusión hacia una pluralidad de usuarios, tales como comunicaciones de tipo “radioaficionado cifradas”, con un usuario que difunde voz o datos hacia otros usuarios.

Las claves comunes pueden también ser utilizadas en las comunicaciones entre usuarios, especialmente para el descifrado de las direcciones de los terminales. Las direcciones pueden ser tanto direcciones individuales como direcciones colectivas, designando entonces a un grupo de al menos dos usuarios.

Las claves individuales pueden ser utilizadas para enlaces punto a punto entre dos terminales. Adicionalmente, pueden ser utilizadas complementariamente a claves comunes cuando estas últimas cifran las direcciones de los terminales.

Generalmente se asume que el nivel de seguridad depende especialmente de la complejidad de una clave, por una parte y, por otra, del algoritmo de cifrado / descifrado.

En orden a aumentar los niveles de seguridad, es también práctica común en tales redes cambiar las claves regularmente. Según las arquitecturas de red, las claves pueden ser cambiadas mensualmente, semanalmente, diariamente o incluso cada hora, por ejemplo para sistemas con un alto grado de confidencialidad.

Las claves, entonces, son distribuidas por el servidor de gestión de claves. Estas últimas pueden comprender claves individuales y claves comunes. Las claves comunes son generalmente de igual tipo y de igual longitud y permiten una homogeneidad de funcionamiento en el seno de todos los terminales de la red y una interoperabilidad entre los

diferentes equipos de esa propia red.

En cambio, existe una problemática cuando, para aumentar la seguridad de la red, se modifica la propia estructura de las claves comunes de cifrado aumentando su tamaño. Así, para el correcto funcionamiento de una red existente, es necesario que todos los equipos dispongan de esas nuevas claves.

Un inconveniente está en que es necesario entonces requerir el retorno de todos los terminales para modificar el soporte físico o el soporte lógico de procesamiento de las nuevas claves de cifrado. Ello requiere una interrupción de servicio para cada usuario y puede traer consigo un cuantioso coste suplementario de mantenimiento según el número de terminales afectados por la migración.

Otra solución es la de mantener dos tipos de claves comunes y, por tanto, dos conjuntos de terminales operando juntos. Un primer conjunto de terminales ya desplegados opera con claves de cifrado antiguas (de tamaño relativamente pequeño). Un segundo conjunto de terminales en despliegue opera con un nuevo tipo de clave de cifrado (de tamaño relativamente grande).

Un primer inconveniente está en que la interoperabilidad entre los terminales de los dos conjuntos no queda asegurada y en que esta gestión de claves eleva la complejidad del mantenimiento de la red.

Un segundo inconveniente está en el pirateo de los terminales que tienen un tipo de claves que ofrecen menos seguridad por parte de un tercero, el cual representa una amenaza para todos los usuarios de la red, incluyendo los usuarios de nuevos terminales que tienen un tipo de claves que brindan una seguridad añadida.

Un tercer inconveniente está en que ya no son posibles las comunicaciones de un usuario hacia una pluralidad de terminales mediante la utilización de una única clave común que fuera diferente según que los terminales pertenezcan a un conjunto de terminales que, ya desplegados, operan con claves antiguas, o a un conjunto de terminales que, en despliegue, operan con un nuevo tipo de clave de cifrado.

Finalmente, un gran inconveniente está en que, cuando la clave común es utilizada para el cifrado de direcciones de terminales y, para el cifrado de dichas direcciones, se utilizan dos tipos de claves, cuando, por ejemplo, se instancia una comunicación entre dos terminales, ya no le es posible a un terminal saber con qué claves se ha cifrado la dirección de otro terminal.

La consecuencia de esta duplicación simple de la clave común para el grupo de nuevos terminales es la de, bajo una célula, no poder ya discriminar los terminales por su dirección cifrada. En efecto, cabe entonces la posibilidad de que la dirección cifrada de un primer terminal y la de otro terminal sean iguales aunque sus direcciones en claro sean diferentes.

Por lo tanto, parece que la gestión del cifrado de las direcciones por medio de dos claves de cifrado constituye una regresión importante desde el punto de vista del funcionamiento de la red y del mantenimiento de su seguridad y de la interoperabilidad.

I. RAY et al., "Using Compatible Keys for Secure Multicasting in E-Commerce ", en "Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02)", expone un procedimiento de distribución de claves compatibles en el seno de un sistema de grabación.

M. BAUGHER et al., "Multicast Security (MSEC) Group Key Management Architecture", en "Request for Comments 4046, Network Working Group" expone protocolos de gestión de clave en el seno de una arquitectura con soporte Multicast Security (MSEC).

Resumen de la invención

La invención permite solucionar los citados inconvenientes.

El objeto de la invención concierne a un procedimiento de distribución de claves de cifrado a dos conjuntos de terminales a través de una red de comunicación desde un servidor de datos. Un primer conjunto de terminales utiliza un primer tipo de clave de un tamaño dado, un segundo conjunto de terminales utiliza un segundo tipo de clave de tamaño estrictamente superior al tamaño dado, siendo conocidas las claves de cada uno de los tipos por el servidor en un instante dado, comprendiendo cada terminal una dirección de identificación.

Adicionalmente, el procedimiento comprende, en el servidor:

- una recepción de un primer mensaje de datos desde un primer terminal, comprendiendo el primer mensaje la dirección del primer terminal;
- una identificación de dicho primer terminal mediante una comparación de la dirección del terminal con direcciones de los dos conjuntos de terminales para establecer la pertenencia del primer terminal a uno de los dos conjuntos;

- una selección de una primera clave del segundo tipo de clave;
- cuando el primer terminal pertenece al primer conjunto, un procesamiento por parte del servidor de la primera clave mediante una primera función para definir una segunda clave de tamaño igual a N y compatible con claves del primer tipo;
- una transmisión al primer terminal de la primera clave o de la segunda clave según la pertenencia del primer terminal al primer o al segundo conjunto.

El procedimiento de distribución permite una facilidad de distribución que no precisa de procesamiento en los terminales que ya están en servicio. El procedimiento de la invención permite un ahorro de tiempo en lo referente al mantenimiento de los terminales de la red, especialmente de los ya desplegados.

Una ventaja de la invención está en permitir aumentar el grado de seguridad del conjunto de las comunicaciones de los terminales de la red, al propio tiempo que brinda una interoperabilidad entre diferentes generaciones de terminales operativos.

Ventajosamente, el procedimiento de distribución comprende una recepción de la clave transmitida por el primer terminal.

La ventaja está en permitir un envío y una recepción de una clave que será compatible con todos los terminales de cada uno de los dos conjuntos.

Ventajosamente, las claves del primer tipo de claves y del segundo tipo de claves son claves comunes. La ventaja de esta característica está en facilitar la emisión de una clave común a cada terminal para cada uno de los dos conjuntos.

Adicionalmente, esto permite que todos los terminales posean una clave común para al menos el descifrado de las direcciones.

Ventajosamente, de acuerdo con una forma de realización, las direcciones son individuales y definen un identificador único para cada terminal. En otra realización, las direcciones son colectivas y definen identificadores para grupos de al menos dos terminales.

Ventajosamente, el procedimiento comprende un procesamiento por parte del primer terminal, cuando el primer terminal pertenece al segundo conjunto, de la primera clave mediante una primera función que permite definir una segunda clave de tamaño igual a N y compatible con claves del primer tipo.

Esta característica permite hacer compatibles entre los terminales de los dos conjuntos unas claves comunes.

Ventajosamente, la primera función es una función llamada de sentido único. La primera función puede ser, por ejemplo, una función resumen. Esta última posibilidad permite una implementación simple de funciones conocidas y que cuentan con interesantes características para evitar reconstruir una clave del segundo tipo a partir de una clave del primer tipo generada mediante tal función resumen. La elección de la primera función permite un correcto compromiso entre el nivel de seguridad requerido y la facilidad de implementación de tal función en un servidor o en un terminal, como también en una estación base.

Ventajosamente, el segundo tipo de claves comprende claves de un tamaño superior a 100 bits.

Ventajosamente, los intercambios de datos entre el servidor y al menos un terminal se realizan por medio de una estación base que permite establecer la conexión y el encaminamiento de los datos transmitidos.

Ventajosamente, la red de comunicación es una red de tipo PMR, que designa “Professional Mobile Radiocommunications” de tipo TETRA, que designa “Trans European Trunked Radio”.

Otro objeto de la invención concierne a un procedimiento de cifrado de datos en una transferencia de datos desde un terminal, habiendo recibido dicho terminal una clave de cifrado según el procedimiento de distribución de la invención.

Cuando dicho terminal pertenece al segundo conjunto, el procedimiento comprende

- un cifrado de una dirección de dicho terminal, con ayuda de la segunda clave, por parte del terminal,
- un cifrado de los datos, con ayuda de una tercera clave de cifrado de los datos, por parte del terminal,
- una transmisión de la dirección cifrada y de los datos cifrados a una estación base.

Otro objeto de la invención concierne a un procedimiento de descifrado de datos en una transferencia de datos desde un terminal hacia una estación base, habiendo recibido el terminal una clave de cifrado según el

procedimiento de distribución de la invención.

Cuando el terminal pertenece al segundo conjunto, el procedimiento de descifrado comprende:

- un descifrado de la dirección del terminal, con ayuda de la segunda clave, por parte de la estación base,
- una comparación de la dirección descifrada con las direcciones de los dos conjuntos de terminales para obtener una clave de cifrado de los datos por parte de la estación base,
- un descifrado de los datos, con ayuda de la clave de cifrado de los datos, por parte de la estación base.

La invención concierne a un procedimiento de cifrado de datos desde una estación base hacia un terminal, habiendo recibido dicho terminal una clave de cifrado según el procedimiento de distribución de la invención.

Cuando el terminal pertenece al segundo conjunto, el procedimiento de cifrado comprende:

- un cifrado de una dirección del terminal, con ayuda de la segunda clave, por parte de la estación base,
- un cifrado de los datos, con ayuda de una tercera clave de cifrado de los datos, por parte de la estación base,
- una transmisión de la dirección cifrada y de los datos cifrados al terminal.

La invención concierne a un procedimiento de descifrado de datos por parte de un terminal en una transferencia de datos desde una estación base hacia dicho terminal, habiendo recibido el terminal una clave de cifrado según el procedimiento de distribución de la invención.

Cuando el terminal pertenece al segundo conjunto, el procedimiento de descifrado de la invención comprende:

- un descifrado de la dirección del terminal, con ayuda de la segunda clave, por parte del terminal,
- una comparación de la dirección descifrada con las direcciones del terminal para obtener la clave de cifrado de los datos por parte del terminal,
- un descifrado de los datos, con ayuda de la clave de cifrado de los datos, por parte del terminal.

Ventajosamente, la tercera clave de cifrado de datos es una primera clave común para el primer conjunto de terminales. En una alternativa, la tercera clave de cifrado de datos es una clave individual de cifrado del terminal.

Adicionalmente, otro objeto de la invención concierne a un terminal móvil para la transmisión de datos en el seno de una red de comunicación.

Comprendiendo el terminal una dirección. Al menos un computador permite realizar:

- una función de instanciación que permite declararse frente a un servidor de gestión de claves de cifrado;
- una función de recepción y de descifrado de una primera clave común de cifrado recibida después de haberse declarado el terminal frente a dicho servidor;
- una función de grabación de la primera clave común recibida en una memoria;
- una función de generación de una segunda clave cuyo tamaño es estrictamente inferior al tamaño de la primera clave;
- una primera función de cifrado de su dirección en emisión y de descifrado de una dirección en recepción a partir de la segunda clave de cifrado;
- una segunda función de cifrado de los datos emitidos desde el terminal y de descifrado de los datos recibidos a partir de una tercera clave de cifrado de datos.

Una ventaja de un terminal de este tipo está en que es fácilmente desplegable en una red de comunicaciones, permitiendo funciones de cifrado de alto grado de seguridad, al propio tiempo que brinda una interoperabilidad con terminales de una antigua generación.

Otra ventaja está en poder adaptar la tercera clave en función del caso de aplicación, del tipo de comunicación o del tipo de terminal, como también del grado de seguridad o de confidencialidad.

Otro objeto de la invención concierne a un servidor de datos para la gestión y la distribución de claves de cifrado hacia terminales de una red de comunicación. Al menos un computador permite llevar a la práctica el procedimiento de distribución de claves de la invención.

Finalmente, la invención concierne a una estación base para la transferencia de datos en el seno de una red de comunicación hacia un terminal que ha recibido una clave de cifrado según el procedimiento de distribución de la invención.

La estación base comprende al menos un computador que permite realizar:

- una primera función de cifrado de una dirección (ADD) del terminal en emisión y de descifrado de una dirección del terminal en recepción, a partir de la segunda clave de cifrado (CCK_{S2});
- una segunda función de cifrado de los datos emitidos hacia el terminal y de descifrado de los datos recibidos desde el terminal a partir de una tercera clave de cifrado de datos.

La tercera clave puede ser de acuerdo con la configuración o el caso de aplicación: una clave definida con relación al tipo de comunicación o al tipo de terminal, como también al grado deseado de seguridad o de confidencialidad.

Puede ser bien una clave común, o bien una clave individual.

Breve descripción de las figuras

Otras características y ventajas de la invención se desprenderán de la lectura de la descripción detallada que sigue, con referencia a las figuras que se acompañan, las cuales ilustran:

figura 1: una arquitectura de red que comprende terminales, estaciones base y un servidor de gestión de claves;

figura 2: una función que permite la generación de una clave de cifrado de acuerdo con la invención;

figura 3: un sistema de equipo de una red de comunicación que permite llevar a la práctica los procedimientos de la invención;

la figura 4: una comunicación entre un terminal del conjunto que tiene un tipo de clave de tamaño mayor que los terminales ya desplegados y una estación base; y

la figura 5: una comunicación entre una estación base y un terminal del conjunto que tiene un tipo de clave de tamaño mayor que los terminales ya desplegados.

Descripción

Más adelante en la descripción, se denomina una función “de sentido único” a una función que puede ser calculada con facilidad, pero que es difícil de invertir. Es decir, supuesta una imagen, es difícil hallarle un antecedente. Las funciones de sentido único se utilizan especialmente en criptografía asimétrica y en las funciones resumen criptográficas.

Más adelante en la descripción, se denomina indistintamente una “clave de cifrado” y una “clave de cifrado” a una clave que permite cifrar datos o voz transmitidos a través de una red de comunicación entre diferentes terminales.

Se denomina una “clave individual” a una clave vinculada a un primer terminal que permite a un equipo, tal como un servidor u otro terminal, como también una estación base, descifrar comunicaciones provenientes del primer terminal a partir del momento en que dicho equipo está en conocimiento de la clave individual.

Se denomina clave común a una misma clave que, transmitida a diferentes terminales, permite cifrar y descifrar las comunicaciones de voz y de datos y cifrar y descifrar las direcciones de los terminales. El hecho de que la clave de cifrado de las direcciones sea común para todos los terminales garantiza una correspondencia única entre cada dirección en claro y una dirección cifrada y recíprocamente.

Se define un “tipo de clave” para designar claves que permiten ser compatibles con un algoritmo de cifrado o de descifrado de direcciones, de datos o de voz. Se pueden renovar claves en un sistema sin dejar de ser compatibles, es decir, permiten ser asociadas a un algoritmo invariante.

Decimos que una clave común de tamaño N es compatible con un primer tipo de claves cuando es compatible con el algoritmo de cifrado o de descifrado asociado al primer tipo de clave.

Un primer tipo de clave queda definido por la notación CCK_S cuando es clave común de tamaño N. Un segundo tipo de clave queda definido por la notación CCK_B cuando es clave común de tamaño N_{sup}.

Se puede denotar por clave CCK_{Bi} una clave común del segundo tipo de clave, por ejemplo distribuida en el instante ti y válida durante un tiempo Di.

Se puede denotar por clave CCK_{Si} una clave común del primer tipo de clave, por ejemplo distribuida en el instante ti y válida durante un tiempo Di.

Más adelante en la descripción, por comodidad del lenguaje, se podrá señalar indistintamente un tipo de clave CCK_B o una clave común CCK_B de ese tipo.

La figura 1 representa un servidor de gestión de claves, denotado por SERV, que permite, en una fase de inicialización, distribuir las claves a al menos un terminal. El servidor distribuye especialmente las claves comunes CCK_B y CCK_S.

En la figura 1 se representa una posible arquitectura de red de una configuración de la invención. El servidor SERV se comunica:

- a través de un primer enlace de datos L1 con una primera estación base, denotada por BS1, que define una primera célula en la que está declarada una primera pluralidad de terminales TS y TB;
- a través de un segundo enlace de datos L2 con una segunda estación base, denotada por BS2, que define una segunda célula en la que está declarada una segunda pluralidad de terminales TB, TS.

Cada estación base, BS1, BS2, comprende un computador que puede ser un servidor o un PC y medios de emisión / recepción respectivamente denotados por E/R1 y E/R2. Los medios de emisión / recepción pueden ser repetidores para la cobertura de telecomunicaciones inalámbricas.

Según otras configuraciones, puede haber una sola o una pluralidad de estaciones base que permite(n) definir una célula de comunicación en la que está declarado al menos un terminal.

Decimos que un terminal está declarado en la célula cuando una estación base ha referenciado su presencia en un área de cobertura dada.

La invención se refiere a dos tipos de terminales. Hay, por tanto, dos conjuntos de terminales, que comprenden los terminales de tipo TB y los terminales de tipo TS.

El primer conjunto, denotado por ENS^B, comprende los terminales TB de nueva introducción en la red de comunicación. Estos terminales disponen de medios que permiten descifrar datos a partir de una clave común de cifrado CCK_B de mayor tamaño, denotado por N_{sup}, que las claves comunes de cifrado TS de los terminales ya desplegados en la red, cuyo tamaño se denota por N más adelante en la descripción.

El segundo conjunto, denotado por ENS^S, comprende los terminales TS que ya están desplegados en la red de comunicación. Estos terminales disponen de medios que permiten descifrar datos a partir de una clave de cifrado CCK_S de menor tamaño N que las claves de cifrado CCK_B de los nuevos terminales TB del conjunto ENS^B.

Por lo tanto, la invención aborda una problemática de despliegue de una pluralidad de terminales que comprenden nuevas funcionalidades en el seno de un conjunto de terminales que siguen siendo empleados. Los dos conjuntos de terminales deben, pues, cohabitar y ser interoperantes.

Tenemos la relación $N < N_{sup}$. Cuanto mayor sea el tamaño de la clave, más elevado será el grado de seguridad referente a la confidencialidad de los intercambios digitales. Por lo tanto, es importante aumentar la seguridad de la red frente a intrusiones de terceros, al propio tiempo que se garantiza una máxima interoperabilidad entre todos los equipos de la red.

La figura 2 representa una función F1 que puede ser realizada por el servidor SERV de acuerdo con la invención.

La función F1 permite, a partir de una clave común de cifrado CCK_B que tiene un tamaño N_{sup} dado, generar una clave de cifrado CCK_S de menor tamaño N que sea compatible con algoritmos de cifrado ya existentes. La función F1 está construida, por tanto, basándose en requisitos de compatibilidad de las claves generadas con un algoritmo existente de los terminales del conjunto ENS^S.

La función F1 es preferiblemente una función de sentido único. En una forma de realización, se trata de una función resumen criptográfica.

El carácter no invertible de la función F1 de sentido único garantiza que, aun si un tercero averigua la clave CCK_S, este no podría sacar provecho de ella para averiguar la clave CCK_B, cuyo uso es el de mejorar la seguridad de las comunicaciones que protege.

La función F1 es capaz de generar una clave de menor tamaño $F1(CCK_B) = CCK_S$ compatible con antiguos terminales TS y compatible con nuevos terminales TB para el descifrado de las direcciones. La función F1 es una función no invertible.

Una ventaja de la función F1 está en permitir conservar un cifrado y un descifrado de las direcciones de los terminales a partir de una clave común de tamaño único para todos los terminales de cada uno de los dos conjuntos ENS^B y ENS^S.

Las claves de cifrado son enviadas a los terminales en una etapa de inicialización. Pueden comprender claves comunes y claves individuales.

La figura 3 representa un servidor de gestión de claves e ilustra un procedimiento de distribución de las claves con la inicialización de un terminal. Por “inicialización de un terminal” se entiende el momento en el que el terminal se declara frente al servidor de gestión de las claves SERV para obtener las claves de cifrado. Esta operación puede ser reeditada a repetición y de manera regular por uno o varios terminales.

En esta etapa de inicialización, un terminal T1 del conjunto ENS^B (o ENS^S) se declara frente a un servidor de gestión de las claves a través de la red. El SERV puede igualmente iniciar la comunicación a partir de un procedimiento previo de búsqueda de un terminal dado, tal como una exploración de una dirección.

El terminal T1 envía al menos una primera trama de datos que comprende su dirección a través de la red de comunicación.

En una primera realización, el servidor SERV, por medio de un comparador C, compara la dirección recibida desde el terminal con una lista de direcciones conocidas y accesibles. La lista de las direcciones de los terminales de la red puede estar referenciada, por ejemplo, por medio de una memoria M que indica si la dirección de un terminal está asociada al conjunto ENS^B o al conjunto ENS^S.

Si el terminal pertenece al conjunto ENS^B, entonces el terminal es un terminal TB que acaba de ser desplegado en la red. Entonces es capaz de recibir claves de tamaño N_{sup}, especialmente para cifrar y descifrar tramas de direcciones, de voz y de datos. El servidor SERV, al haber determinado el conjunto de pertenencia del terminal TB, procede a la emisión al terminal TB, a través de la red, de una clave común CCK_B de un tamaño N_{sup}.

Si el terminal pertenece al conjunto ENS^S, entonces el terminal es un terminal TS que ya está desplegado en la red. Este terminal no es capaz de recibir claves de tamaño N_{sup} especialmente para cifrar y descifrar tramas de direcciones, de voz y de datos. El terminal TS tan sólo puede gestionar claves más pequeñas de tamaño N. El servidor SERV, al haber determinado el conjunto de pertenencia del terminal TS por medio del comparador C, procede a un procesamiento de una clave común CCK_B de tamaño N_{sup} mediante la función F1 que permite ajustar a formato la clave para que sea compatible con el cifrado y descifrado por parte de los terminales del conjunto ENS^S.

La función F1 genera, por tanto, una clave CCK_S de tamaño N compatible con algoritmos de los terminales del conjunto ENS^S y procede a su emisión a través de la red hacia el terminal TS.

Una alternativa de realización puede comprender, en la inicialización de un terminal, un cifrado de los datos entre un terminal y el servidor. En particular, esta alternativa permite transmitir direcciones cifradas, claves cifradas y datos cifrados. En este caso, se trata de una clave individual de tipo DCK y no una clave común de tipo CCK.

La figura 3 representa una función de descifrado DCH de los datos recibidos por el servidor por medio de una clave individual y una función de cifrado CH de datos que comprende al menos una clave enviada al terminal. La etapa de cifrado puede realizarse a continuación del procesamiento de clave común CCK_B por la función F1, para generar una clave CCK_S, o directamente a partir de una clave común CCK_B de tamaño N_{sup}.

En una comunicación, por ejemplo, entre al menos dos terminales, estos últimos cifran su dirección en el momento de la transmisión de datos.

Las direcciones son cifradas:

- ya sea directamente a partir de una clave de cifrado común CCK_S de un terminal del conjunto ENS^S,
- o bien a partir de una clave generada por la función F1 de un terminal TB del conjunto ENS^B, también denotada por CCK_S.

La figura 2 ilustra este último escenario en el que la clave común CCK_S generada permite cifrar una dirección ADD mediante un algoritmo de cifrado CH1 para generar una dirección cifrada E(ADD), denotada asimismo en las figuras 4 y 5 por: E1(ADD).

Una ventaja está en que no es necesario introducir modificaciones en los terminales del conjunto ENS^S que reciben una clave CCK_S ya ajustada a formato para los algoritmos implementados en los terminales del conjunto ENS^S. No es, pues, necesario actualizar los terminales ya desplegados del conjunto ENS^S, ni realizar modificaciones o acciones de retroadaptación.

Cuando se descifra una dirección con una clave común CCK_S, un terminal, o un servidor de datos, o una estación base puede intentar descifrar los datos de una comunicación con una clave adecuada según la dirección descifrada.

Por lo tanto, un terminal puede comprender varias claves de cifrado. Es un caso de realización práctica, por ejemplo, el hecho de que, en la fase de inicialización, el terminal puede recibir, en la misma fase o en sucesivas fases,

diferentes claves de cifrado.

Una clave principal K, una primera clave individual DCK y una primera clave común CCK pueden transmitirse a al menos un terminal de una célula por intermedio de la estación base SB. Las claves pueden asimismo ser enviadas simultáneamente a una pluralidad de terminales de una misma célula.

La clave principal K o la primera clave individual DCK puede utilizarse para transmitir de manera segura otras claves individuales o comunes. Tal es particularmente el caso del ejemplo representado en la figura 3, donde las funciones de cifrado CH y de descifrado DCH de la clave común CCK_S y CCK_B se realizan tras la recepción de los datos desde un terminal y antes de la emisión de datos hacia un terminal. Las funciones de cifrado CH y de descifrado DCH se realizan por medio de una clave individual DCK_S o DCK_B según la pertenencia del terminal a los conjuntos ENS_S y ENS_B.

El procedimiento de distribución de claves de la invención permite utilizar para el cifrado de las direcciones tan sólo una clave común CCK_S para todos los terminales, sea cual sea su pertenencia al conjunto ENS^S o ENS^B.

Esto permite conservar una fase de distribución de clave rigurosamente idéntica para los terminales ya desplegados, con el fin de no cargar la interfaz aérea con intercambios suplementarios.

Y esto permite enviar claves comunes nuevas CCK_B a los nuevos terminales, los cuales son capaces de generar una clave común CCK_S, dado que la función F1 se halla presente en los terminales TB del conjunto ENS^B.

Para ello, la clave de cifrado de las direcciones pasa a ser:

$CCK_S = F1(CCK_B)$.

Este cálculo se lleva a cabo en el servidor SERV de gestión de las claves y en los terminales TB del conjunto ENS^B que reciben la clave CCK_B. Los terminales TS pertenecientes al conjunto ENS^S siguen recibiendo una clave CCK_S con el formato que esos terminales conocen.

La figura 4 ilustra una configuración de un intercambio desde un terminal TB1 del conjunto ENS^B que tiene una clave común de tamaño N_{sup} hacia una estación base BS.

La configuración es la siguiente: el terminal TB1 trata de establecer una comunicación cifrada según el procedimiento de cifrado de la invención con la estación base. La estación base descifra las tramas recibidas, de acuerdo con el procedimiento de descifrado de la invención, a través de la red.

En esta configuración, se parte del supuesto de que la clave común permite cifrar las direcciones de los terminales y los datos de las comunicaciones.

El terminal TB1, que posee una clave común CCK_B de tamaño N_{sup}, puede generar una clave común CCK_S de tamaño N por medio de la función F1 que está implementada en cada terminal TB del conjunto ENS^B. La clave común CCK_S así generada permite cifrar la dirección ADD del terminal TB1 por medio de un algoritmo de cifrado CH1 utilizando la clave común CCK_S de tamaño N. La dirección cifrada se denota por E1(ADD). La dirección cifrada es enviada a la estación base BS.

Los datos DATA son cifrados, preferentemente, con la clave individual DCK_B por medio de un algoritmo de cifrado CH2 para obtener los datos cifrados E2(DATA). Como variante, los datos DATA pueden ser cifrados con la clave común CCK_B.

Las tramas de datos cifradas E2(DATA) pueden ser enviadas simultánea o sucesivamente a las tramas que comprenden la dirección cifrada E1(ADD).

La estación base BS recibe la trama que comprende la dirección cifrada E1(ADD) y descifra por medio de un algoritmo de descifrado DCH1, utilizando una clave CCK_S obtenida con anterioridad para obtener una dirección descifrada ADD.

Cuando se descifra la dirección ADD del terminal TB1, una función C permite comparar si la dirección descifrada se corresponde con una dirección individual o colectiva del terminal TB1 para determinar la clave de descifrado de los datos E2(DATA). Estas direcciones se memorizan en una memoria M de la estación base, asociándose cada dirección a una clave de descifrado individual o común. Si la dirección ADD es individual, la clave será una clave individual DCK_B de un terminal del conjunto ENS^B o una clave individual DCK_S de un terminal del conjunto ENS^S. Si la dirección ADD es colectiva, la clave será una clave común CCK_B para los terminales del conjunto ENS^B o una clave común CCK_S para los terminales del conjunto ENS^S.

Si la comparación es positiva, la estación base BS puede utilizar la clave CCK_B o DCK_B asociada al terminal TB1 para descifrar, por medio de un algoritmo de descifrado DCH2, las tramas de datos DATA.

Si la comparación no es positiva, la estación base BS no procesa los datos.

La figura 5 ilustra una configuración de un intercambio desde una estación base BS hacia un terminal TB2 del conjunto ENS^B que tiene una clave común de tamaño N_{sup}.

La configuración es la siguiente: la estación base BS trata de establecer una comunicación cifrada según el procedimiento de cifrado de la invención con el terminal TB2 que está inscrito bajo la célula de esa estación base. El terminal TB2 descifra las tramas recibidas de acuerdo con el procedimiento de descifrado de la invención.

En esta configuración, se parte del supuesto de que la clave común permite cifrar las direcciones de los terminales y los datos DATA de las comunicaciones.

La estación base BS, que posee una clave común CCK_B de tamaño N_{sup}, puede generar una clave común CCK_S de tamaño N por medio de la función F1 que está implementada en la estación base BS. En una variante de realización, la estación base BS puede recibir del servidor directamente la clave común CCK_S de tamaño N. La clave común CCK_S así obtenida permite cifrar la dirección ADD (individual o colectiva) del terminal TB2 por medio de un algoritmo de cifrado CH1, utilizando la clave común CCK_S de tamaño N. La dirección cifrada se denota por E1(ADD). La dirección cifrada es enviada al terminal destinatario TB2.

La estación base cifra las tramas DATA mediante aplicación de la clave CCK_B a un algoritmo de cifrado CH2 para obtener las tramas cifradas E2(DATA). Las tramas de datos E2(DATA) pueden ser enviadas simultánea o sucesivamente a las tramas E1(ADD).

El terminal TB2 recibe la trama que comprende la dirección cifrada E1(ADD) y descifra por medio de un algoritmo de descifrado DCH1, utilizando una clave CCK_S que ha sido generada con anterioridad por una función F1 del terminal TB2 a partir de una clave CCK_B.

Cuando se descifra la dirección ADD del terminal TB2, una función D permite comparar si la dirección descifrada se corresponde con una dirección individual o colectiva del terminal TB2, para determinar la clave de descifrado de los datos E2(DATA). Estas direcciones se memorizan en una memoria M del terminal TB2, asociándose cada dirección a una clave de descifrado individual o común. Si la dirección ADD es individual, la clave es una clave individual DCK_B. Si la dirección ADD es colectiva, la clave es una clave común CCK_B.

Si la comparación es positiva, el terminal TB2 puede utilizar la clave CCK_B o DCK_B para descifrar, por medio de un algoritmo de descifrado DCH2, las tramas de datos DATA.

Si la comparación no es positiva, el terminal TB2 no procesa los datos.

Es posible, en una alternativa de realización de la invención, que las funciones de descifrado DCH1 de la dirección ADD y de comparación C también sean soportadas por los terminales TB1 y TB2 en una comunicación directa entre los terminales o una comunicación de extremo a extremo, es decir, sin procesamiento intermedio entre esos terminales.

En este último caso, cada terminal comprende la lista de las direcciones de los demás terminales y, ocasionalmente, su pertenencia a los dos conjuntos ENS^S y ENS^B.

En este último caso, la función de comparación C que permite comparar una dirección de un terminal dado con las direcciones de dos conjuntos de terminales, para determinar la pertenencia de los terminales a los dos conjuntos, la realiza directamente el terminal.

La invención permite, por tanto, aumentar el nivel de seguridad y de confidencialidad de los terminales del conjunto ENS^B, al propio tiempo que brinda una compatibilidad con los terminales del conjunto ENS^S que precisan de claves de menor tamaño.

REIVINDICACIONES

1. Procedimiento de distribución de claves de cifrado a dos conjuntos (ENS^B, ENS^S) de terminales (TBi, TSi) a través de una red de comunicación desde un servidor de datos (SERV), utilizando un primer conjunto (ENS^S) de terminales (TSi) un primer tipo de clave (CCK_S) de tamaño dado (N), utilizando un segundo conjunto (ENS^B) de terminales (TBi) un segundo tipo de clave (CCK_B) de tamaño estrictamente superior al tamaño dado (N_{sup}), siendo conocidas por el servidor (SERV) las claves de cada uno de los tipos en un instante dado, comprendiendo cada terminal (TBi, TSi) una dirección de identificación (ADDi), comprendiendo el procedimiento, en el servidor:

- una recepción de un primer mensaje de datos desde un primer terminal, comprendiendo el primer mensaje la dirección del primer terminal;
- una identificación de dicho primer terminal (T1) mediante una comparación de la dirección (ADDi) del terminal (T1) con direcciones de los dos conjuntos de terminales para establecer la pertenencia del primer terminal a uno de los dos conjuntos;
- una selección de una primera clave del segundo tipo de clave (CCK_B);
- cuando el primer terminal (T1) pertenece al primer conjunto (ENS^S), un procesamiento, por parte del servidor (SERV), de la primera clave (CCK_{B1}) mediante una primera función (F1) para definir una segunda clave (CCK_{S2}) de tamaño igual a N y compatible con claves del primer tipo (CCK_S);
- una transmisión al primer terminal (T1) de la primera clave (CCK_{B1}) o de la segunda clave (CCK_{S2}) según la pertenencia del primer terminal al primer o al segundo conjunto.

2. Procedimiento de distribución de claves de cifrado según la reivindicación 1, caracterizado por que comprende una recepción de la clave transmitida por el primer terminal (T1).

3. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 2, caracterizado por que las claves del primer tipo de claves y del segundo tipo de claves son claves comunes para todos los terminales.

4. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que las direcciones son individuales, definiendo un identificador único para cada terminal.

5. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que las direcciones son colectivas, definiendo identificadores para grupos de al menos dos terminales.

6. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que el procedimiento comprende un procesamiento por parte del primer terminal (T1), cuando el primer terminal (T1) pertenece al segundo conjunto (ENS^B), de la primera clave (CCK_{B1}) mediante una primera función (F1) que permite definir una segunda clave (CCK_{S2}) de tamaño igual a N y compatible con claves del primer tipo (CCK_S).

7. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que la primera función (F1) es una función llamada de sentido único.

8. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que la primera función (F1) es una función resumen.

9. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que el segundo tipo de claves (CCK_{B1}) comprende claves de un tamaño superior a 100 bits.

10. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 9, caracterizado por que los intercambios de datos entre el servidor (SERV) y al menos un terminal se realizan por medio de una estación base que permite establecer la conexión y el encaminamiento de los datos transmitidos.

11. Procedimiento de distribución de claves de cifrado según una cualquiera de las reivindicaciones 1 a 10, caracterizado por que la red de comunicación es una red de tipo PMR, que designa “Professional Mobile Radiocommunications”, de tipo TETRA, que designa “Trans European Trunked Radio”.

12. Procedimiento de cifrado de datos en una transferencia de datos desde un terminal (TB1) que comprende las etapas del procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, caracterizado por que comprende, cuando el terminal (TB1) pertenece al segundo conjunto (ENS^B):

- un cifrado de una dirección (ADD) del terminal (TB1), con ayuda de la segunda clave (CCK_{S2}), por parte del terminal,

- un cifrado de los datos (DATA), con ayuda de una tercera clave (CCK_B, DCK_B) de cifrado de los datos, por parte del terminal,
- una transmisión de la dirección cifrada (E1(ADD)) y de los datos cifrados (E2(DATA)) a una estación base (BS).

13. Procedimiento de descifrado de datos en una transferencia de datos desde un terminal (TB1) hacia una estación base (BS), que comprende las etapas del procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, caracterizado por que comprende, cuando el terminal (TB1) pertenece al segundo conjunto (ENS^B):

- un descifrado de la dirección (ADD) del terminal (TB1), con ayuda de la segunda clave (CCK_{S2}), por parte de la estación base (BS),
- una comparación (C) de la dirección (ADD) descifrada con las direcciones de los dos conjuntos de terminales para obtener una clave de cifrado de los datos por parte de la estación base (BS),
- un descifrado de los datos, con ayuda de la clave de cifrado de los datos, por parte de la estación base (BS).

14. Procedimiento de cifrado de datos desde una estación base (BS) hacia un terminal (TB2), que comprende las etapas del procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, caracterizado por que comprende, cuando el terminal (TB2) pertenece al segundo conjunto (ENS^B):

- un cifrado de una dirección (ADD) del terminal (TB2), con ayuda de la segunda clave (CCK_{S2}), por parte de la estación base (BS),
- un cifrado de los datos (DATA), con ayuda de una tercera clave de cifrado de los datos, por parte de la estación base,
- una transmisión de la dirección cifrada (E1(ADD)) y de los datos cifrados (E2(DATA)) al terminal (TB2).

15. Procedimiento de descifrado de datos por parte de un terminal (TB2) en una transferencia de datos desde una estación base (BS) hacia dicho terminal (TB2), que comprende las etapas del procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, caracterizado por que comprende, cuando el terminal (TB2) pertenece al segundo conjunto (ENS^B):

- un descifrado de la dirección (ADD) del terminal (TB2), con ayuda de la segunda clave (CCK_{S2}), por parte del terminal,
- una comparación (D) de la dirección descifrada con las direcciones del terminal para obtener la clave de cifrado de los datos por parte del terminal,
- un descifrado de los datos, con ayuda de la clave de cifrado de los datos, por parte del terminal.

16. Procedimiento de cifrado y de descifrado según una de las reivindicaciones 12 a 15, caracterizado por que la tercera clave de cifrado de datos es una primera clave común (CCK_B) para el primer conjunto de terminales.

17. Procedimiento de cifrado y de descifrado según una de las reivindicaciones 12 a 15, caracterizado por que la tercera clave de cifrado de datos es una clave individual de cifrado (DCK_B) del terminal.

18. Terminal móvil para la transmisión de datos en el seno de una red de comunicación, comprendiendo el terminal una dirección, caracterizado por que comprende al menos un computador que permite realizar:

- una función de instanciación que permite declararse frente a un servidor de gestión de claves de cifrado (SERV);
- una función de recepción y de descifrado de una primera clave común (CCK_{B1}) de cifrado recibida después de haberse declarado el terminal frente a dicho servidor (SERV);
- una función de grabación de la primera clave común (CCK_{B1}) recibida en una memoria (M);
- una función de generación de una segunda clave (CCK_{S2}) cuyo tamaño es estrictamente inferior al tamaño de la primera clave (CCK_{B1});
- una primera función de cifrado de su dirección (ADD) en emisión y de descifrado de una dirección en recepción a partir de la segunda clave de cifrado (CCK_{S2});
- una segunda función de cifrado de los datos emitidos desde el terminal y de descifrado de los datos

recibidos a partir de una tercera clave (CCK_B, DCK_B) de cifrado de datos.

19. Servidor de datos para la gestión y la distribución de claves de cifrado hacia terminales de una red de comunicación, caracterizado por que comprende al menos un computador que permite llevar a la práctica el procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11.

20. Sistema que comprende un servidor adaptado para ejecutar el procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, y una estación base para la transferencia de datos en el seno de una red de comunicación hacia un terminal que ha recibido una clave de cifrado según el procedimiento de distribución de una cualquiera de las reivindicaciones 1 a 11, caracterizado por que comprende al menos un computador que permite realizar:

- una primera función de cifrado de una dirección (ADD) del terminal en emisión y de descifrado de una dirección del terminal en recepción, a partir de la segunda clave de cifrado (CCK_{S2});
- una segunda función de cifrado de los datos emitidos hacia el terminal y de descifrado de los datos recibidos desde el terminal a partir de una tercera clave (CCK_B, DCK_B) de cifrado de datos.

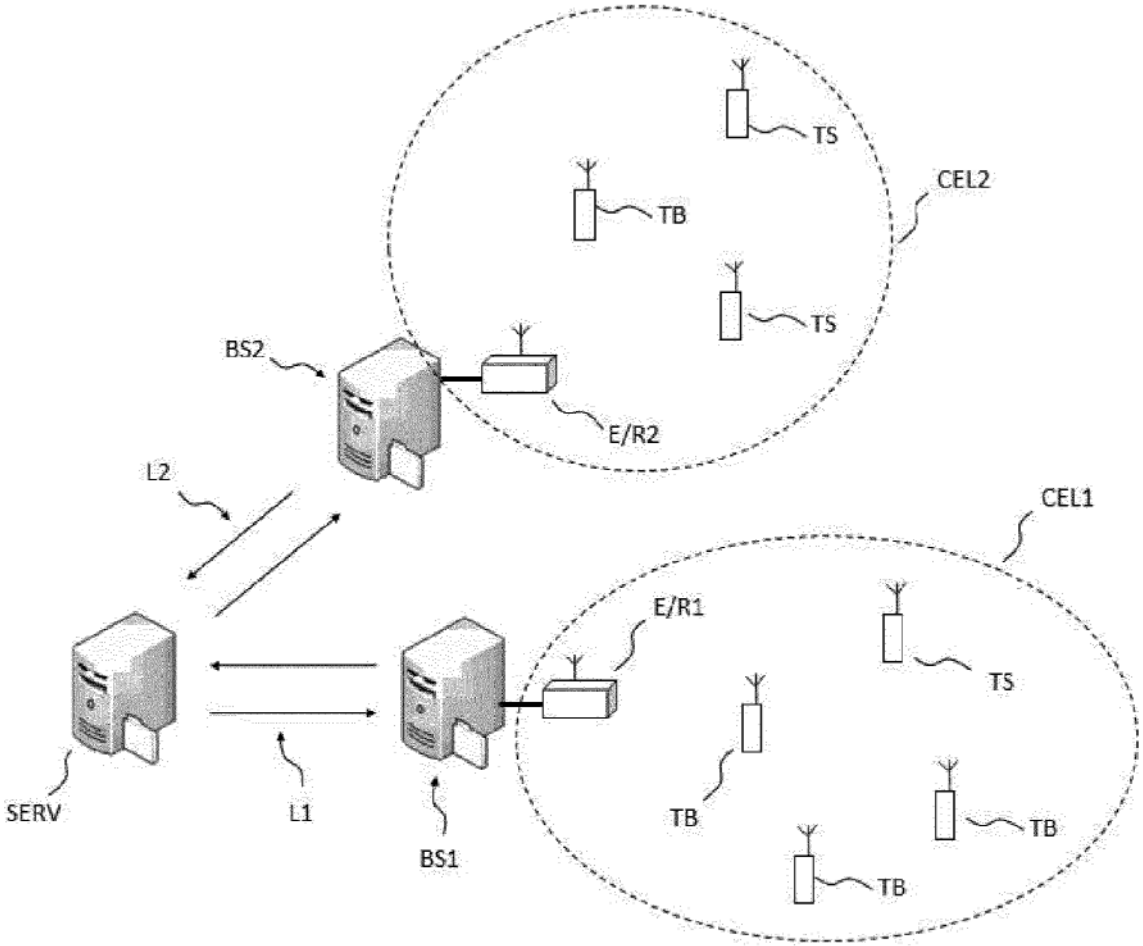

FIG. 1

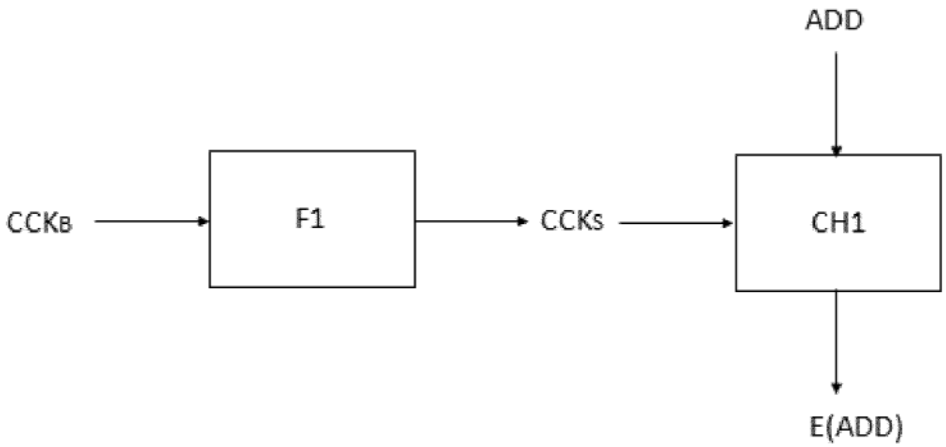

FIG. 2

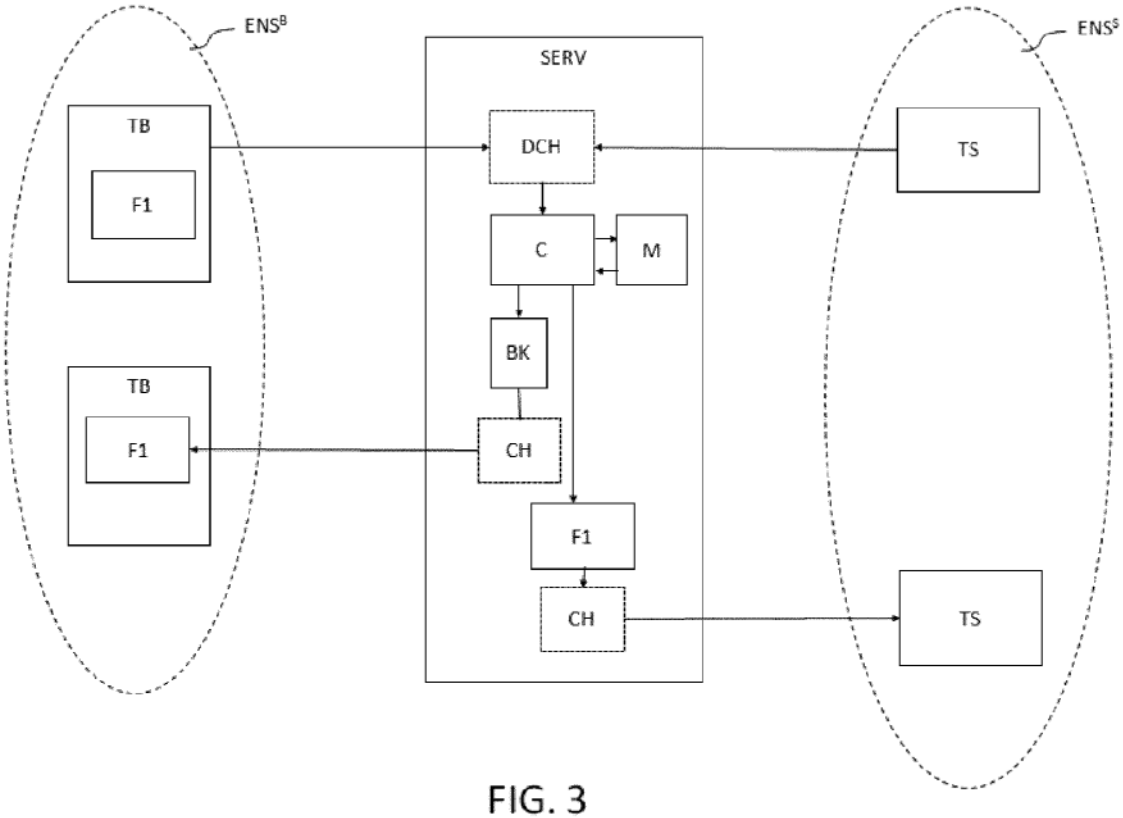

FIG. 3

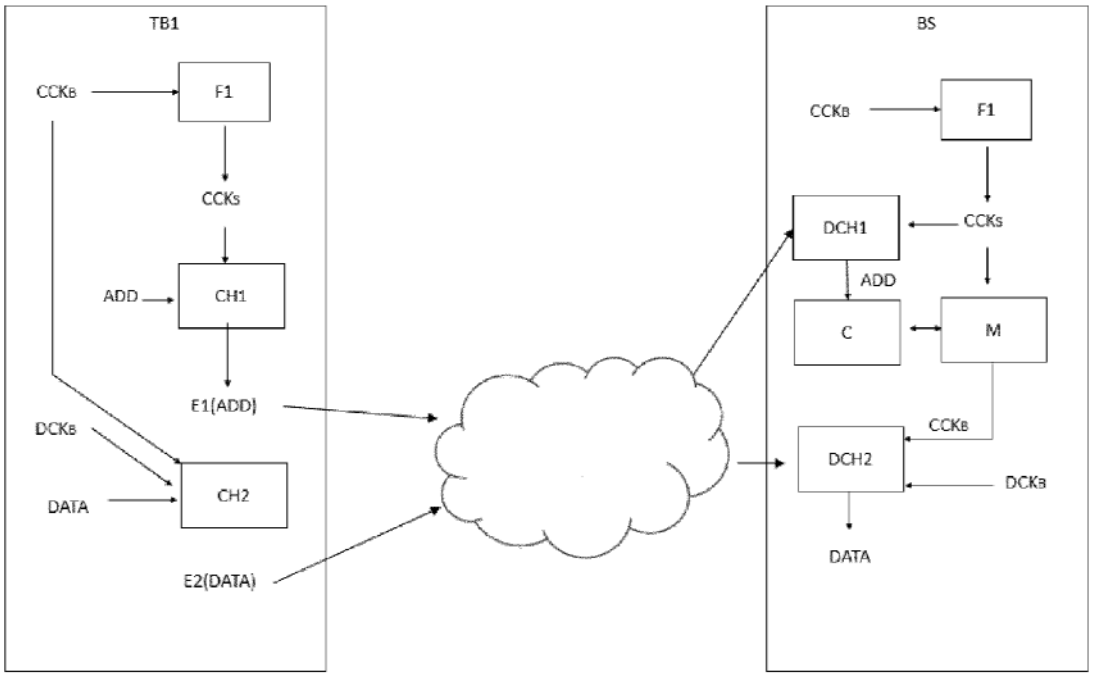
TB1
CCKB
F1
CCKS
ADD
CH1
E1(ADD)
DCKB
DATA
CH2
E2(DATA)
BS
CCKB
F1
DCH1
CCKS
ADD
C
M
CCKB
DCH2
DCKB
DATA

FIG. 4

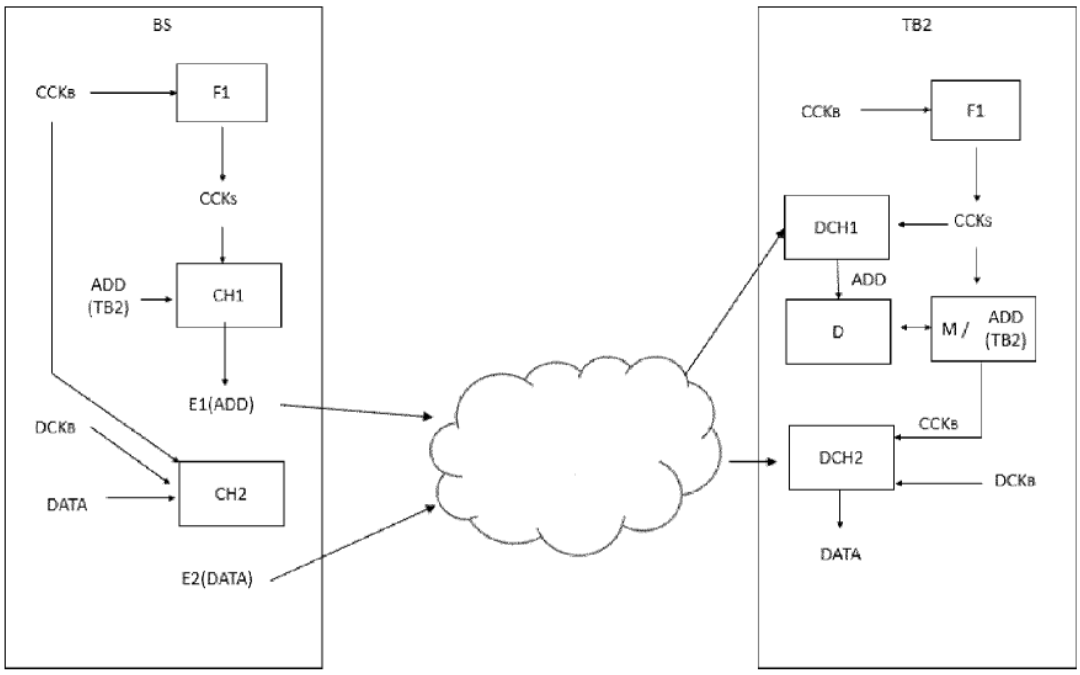
BS
CCKB
F1
CCKS
ADD
(TB2)
CH1
E1(ADD)
DCKB
DATA
CH2
E2(DATA)
TB2
CCKB
F1
DCH1
CCKS
ADD
D
M /
ADD
(TB2)
CCKB
DCH2
DCKB
DATA

FIG. 5