(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 732 548**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.02.2010 PCT/SE2010/050167**

(87) Fecha y número de publicación internacional: **18.08.2011 WO11099904**

(96) Fecha de presentación y número de la solicitud europea: **12.02.2010 E 10845885 (2)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2534809**

(54) Título: **Descubrimiento de confianza en una red de comunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.11.2019

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm , SE

(72) Inventor/es:

HADDAD, WASSIM;
BLOM, ROLF y
NÄSLUND, MATS

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Descubrimiento de confianza en una red de comunicaciones

Campo técnico

La invención se refiere al campo del descubrimiento de confianza en una red de comunicaciones.

Antecedentes

Una red inalámbrica ad hoc es, en cierta medida, una red inalámbrica descentralizada. Los terminales en la red se comunican entre sí usando la misma interfaz de radio o similar a la que usarían para comunicarse con una estación base. Esto se conoce a veces como comunicación de "modo directo". Una red inalámbrica totalmente ad hoc no necesita depender de la infraestructura existente de la red, como las estaciones base, etc. En su lugar, cada nodo participa en el enrutamiento reenviando datos para otros nodos, por lo que la determinación de qué nodos reenvían los datos se realiza de forma dinámica basándose en la conectividad de la red. En una red ad hoc ligeramente más controlada, los terminales se pueden comunicar directamente entre sí y/o usar la infraestructura de red existente. Esto podría verse como una red ad hoc con algún apoyo de una infraestructura. Típicamente, una red inalámbrica ad hoc tiene un rango limitado cuando se usa el modo directo, por ejemplo, decenas o cientos de metros. Es posible un rango más largo, pero puede causar problemas de interferencia cuando los nodos tanto ad hoc (en movimiento) como basados en infraestructura (fijos) usan el mismo espectro.

La figura 1 muestra tres ejemplos de escenarios de red ad hoc. La figura 1a muestra un desglose local controlado por la red, en el que el terminal 1 contacta con la infraestructura 2 de red para iniciar la comunicación con el terminal 3. La figura 1b muestra un escenario de "relé" en el que los terminales 1, 3 establecen comunicación entre sí, pero solo el terminal 1 está en comunicación con la red 2. La figura 1c muestra un verdadero escenario de red ad-hoc en el que tres terminales 1, 3, 4 se comunican directamente entre sí sin estar en comunicación con la infraestructura 2 de red. Este escenario está precedido típicamente por uno de los dos primeros escenarios. La siguiente descripción supone una red de evolución a largo plazo (LTE), pero se apreciará que los conceptos se aplican a otros tipos de red celular.

Se requiere un grado de confianza para que los terminales establezcan una red ad hoc. Esto se logra típicamente mediante una autenticación sólida y un intercambio de claves, pero antes de tomar este paso, se requiere un "descubrimiento de confianza del vecino" rápido y mutuo. Un terminal (el nodo de anuncio) anunciará típicamente su presencia y otro terminal (el nodo de respuesta) puede responder. En ausencia de una fase de autenticación previa liviana para el descubrimiento rápido de confianza del vecino, los dos terminales están expuestos a ataques de denegación de servicio (DoS), por ejemplo, vaciar innecesariamente la potencia de la batería, al establecer asociaciones de seguridad.

Un terminal LTE se conoce como equipo de usuario (UE). En este ejemplo, una red inalámbrica ad-hoc es un derivado de una infraestructura LTE desplegada. La red inalámbrica ad-hoc permite que un conjunto de UE habilitados detecte la presencia de otros y/o anuncien diferentes tipos de servicios públicos y privados sin usar la infraestructura LTE. Además, estos UE habilitados pueden detectar constantemente el entorno que los rodea, y así pueden recibir anuncios de servicios basados en proximidad, como menús/ofertas de restaurantes, horarios de transporte público, etc. Además de las actividades sociales, estos servicios pueden incluir actividades comerciales, multimedia, anuncios basados en proximidad, presencia de amigos, etc.

Considérese el escenario en el que un usuario (Bob) que usa el UE 1 es la voluntad de anuncio de jugar una partida de ajedrez, y un usuario interesado (Alice) que usa el UE 3 detecta el anuncio de Bob y decide participar con él en una partida de ajedrez. Alice y Bob pueden ser completos desconocidos y no existe una relación de confianza entre ellos o sus UE. El primer paso es que Alice inicie un protocolo de "descubrimiento de confianza del vecino", que permite a Alice y Bob verificar mutuamente la legitimidad del otro. Una vez que esto se haya completado, se puede llevar a cabo una autenticación más segura, incluido un intercambio de claves.

En este tipo de entorno, no es fácil para Alicia verificar la legitimidad de Bob. Además, dicho intercambio significaría que ambos UE están expuestos a un ataque DoS en forma de mensajes de protocolo de intercambio de claves falsificados enviados por nodos maliciosos cercanos. Tampoco hay forma de asegurar que los dos nodos que iniciaron el intercambio de claves sean los mismos que los que lo completaron.

Una solución al problema del descubrimiento de confianza del vecino es que la infraestructura de red proporcione a cada usuario un certificado de clave pública convencional. Por razones de privacidad, estos certificados deben ser de corta duración, con un "seudónimo" en lugar de una identidad a largo plazo. Esto causaría una gran sobrecarga en la red ya que la red necesita certificar todas las claves públicas. También implicaría una sobrecarga en los terminales, ya que cada terminal potencialmente necesitaría almacenar (o adquirir, cuando sea necesario) los certificados de todos los demás nodos, o todos los otros nodos con los cuales el terminal puede establecer una red ad hoc.

La siguiente literatura se considera que representa la técnica anterior relevante:

"Diversidad de canal de nivelación para el establecimiento de clave en redes de sensor inalámbricas" (XP31072299), de M. J. Miller y N. H. Vaidya, en INFOCOM 2006, 25ª conferencia internacional IEEE en comunicaciones informáticas, páginas 1-12, 2006, se divulga un protocolo nuevo para la distribución de claves simétricas que usa múltiples canales disponibles en el hardware del sensor. Esta diversidad de canales, junto con la diversidad espacial de las ubicaciones del dispositivo, permite sensores vecinos para establecer claves de enlace seguras a partir de claves de texto llano que se emiten mediante sensores en la vecindad.

"Autenticación de emisión de multiusuario en redes de sensor inalámbricas" (XP011268124) de K. Ren, S. Yu, W. Lou, y Y. Zhang, en transacciones IEEE en tecnología vehicular, vol. 58, páginas 4554-4564, 2009, divulga esquemas eficientes basados en claves públicas para logar autenticación de emisión inmediata en redes de sensor inalámbricas (WSN) y así evitar la vulnerabilidad de seguridad que es intrínseca a esquemas tipo TESLA μ que se basan en soluciones basadas en claves simétricas.

La publicación de la patente US 20060072759-A1 titulada "Métodos y aparato para arrancar claves de autenticación extranjeras y extranjeras móviles en IP móvil" de S. Gundavelli et. al. como se publicó el 6 de abril de 2006.

Sumario

Los inventores se han dado cuenta de los problemas asociados con el descubrimiento de confianza del vecino, y han ideado una forma segura y eficiente para permitir que los nodos realicen el descubrimiento de confianza del vecino antes del establecimiento de la conexión y el intercambio de claves, al tiempo que minimizan el riesgo de un ataque DoS.

De acuerdo con un primer aspecto de la invención, se proporciona un método para establecer la confianza entre dos nodos en una red de comunicaciones. Un primer nodo recibe de un nodo de red datos de autenticación exclusivos del primer nodo. Los datos de autenticación se pueden usar para obtener una representación compacta de los datos de verificación para el primer nodo. El primer nodo también recibe una representación compacta certificada de los datos de verificación de todos los nodos en la red. Cuando el primer nodo desea configurar una red ad hoc con un segundo nodo, obtiene información de confianza de los datos de autenticación para el nodo y envía al segundo nodo un mensaje que incluye la información de confianza y al menos una parte de los datos de autenticación El segundo nodo tiene su propia copia de la representación compacta certificada de los datos de verificación de todos los nodos en la red, y verifica la autenticidad del mensaje desde el primer nodo usando la representación compacta de los datos de verificación de todos los nodos en la red y la información de confianza recibida y los datos de autenticación. Dado que ambos nodos han recibido la representación compacta certificada de los datos de verificación de la red, pueden establecer un grado de confianza antes de un intercambio de claves sin tener que seguir comunicándose con la red.

Como una opción, la representación compacta de los datos de verificación del primer nodo comprende una raíz de un árbol de Merkle que se ha derivado de los datos de autenticación exclusivos del primer nodo y una pluralidad de tiempos de referencia relativos a un tiempo de referencia base dentro de un periodo de tiempo predeterminado. Al usar los tiempos de referencia, el segundo nodo también puede usar los tiempos para ayudar a verificar la autenticidad del mensaje.

Como una opción adicional, la representación compacta de los datos de verificación de todos los nodos en la red comprende uno de un filtro de Bloom y una raíz de un árbol de Merkle derivados de los datos de verificación de todos los nodos en las redes.

El método comprende opcionalmente, en el primer nodo, derivar una hoja de un árbol de Merkle de los datos de autenticación exclusivos del primer nodo y un solo tiempo de referencia derivado de la información obtenida de un reloj en el primer nodo, en el que la información de confianza se deriva de la hoja derivada. Esto permite que el segundo nodo verifique la autenticidad del mensaje usando información derivada de un reloj en el segundo nodo. El segundo nodo verifica opcionalmente la autenticidad del mensaje del primer nodo derivando una hoja de un árbol de Merkle de los datos de autenticación y un tiempo de referencia derivado de la información obtenida de un reloj en el segundo nodo, verificando la información de confianza, derivando una segunda representación compacta de los datos de verificación del primer nodo, y verificación de que la segunda representación compacta de los datos de verificación del primer nodo concuerda con la representación compacta de los datos de verificación de todos los nodos en la red.

Como una opción adicional, la representación compacta de los datos de verificación de todos los nodos en la red comprende un filtro de Bloom, y la segunda representación compacta de los datos de verificación del primer nodo concuerda con la representación compacta de los datos de verificación de todos los nodos en la red si la segunda representación compacta de los datos de verificación se indica como miembro del filtro de Bloom. Alternativamente, la representación compacta de los datos de verificación de todos los nodos en la red comprende una raíz de árbol de

Merkle derivada de los datos de verificación de todos los nodos en la red, y la segunda representación compacta de los datos de verificación del primer nodo concuerda con la representación compacta de los datos de verificación de todos los nodos en la red si la raíz del árbol de Merkle puede derivarse de la segunda representación compacta de los datos de verificación del primer nodo.

Para mejorar aún más la seguridad, el método opcionalmente comprende además el primer nodo que recibe del nodo de red una clave de grupo disponible para todos los nodos de red que pertenecen a un grupo, y el primer nodo que cifra al menos parte del mensaje usando la clave de grupo antes de enviarlo al segundo nodo. De esta manera, parte del mensaje se puede cifrar y solo otros miembros del grupo pueden acceder a él.

El mensaje se envía opcionalmente en respuesta a una consulta desde el segundo nodo, habiéndose enviado la consulta desde el segundo nodo en respuesta a un mensaje de anuncio enviado por el primer nodo.

De acuerdo con un segundo aspecto de la invención, se proporciona un nodo de comunicaciones móvil para su uso en una red de comunicaciones. El nodo comprende un receptor para recibir desde un nodo de red datos de autenticación exclusivos del nodo del cual se puede derivar una representación compacta de los datos de verificación para el nodo, y una representación compacta de los datos de verificación de todos los nodos en la red, siendo certificada la representación compacta de los datos de verificación de todos los nodos en la red por el nodo de red. El nodo también cuenta con un procesador para derivar información de confianza de los datos de autenticación y un transmisor para enviar a un segundo nodo la información de confianza y al menos una parte de los datos de autenticación. La información de confianza puede ser usada por el segundo nodo para verificar la autenticidad del mensaje mediante la representación compacta de los datos de verificación de todos los nodos en la red y la información de confianza y los datos de autenticación recibidos.

El nodo de comunicaciones móvil comprende opcionalmente además un reloj, en el que el procesador está dispuesto para derivar una hoja de un árbol de Merkle de los datos de autenticación exclusivos del nodo y un solo tiempo de referencia derivado de la información obtenida del reloj, en el que se deriva la información de confianza de la hoja derivada.

Como opción, el nodo de comunicaciones móvil comprende además una memoria para almacenar una clave de grupo, en la que el procesador está dispuesto para cifrar al menos parte del mensaje usando la clave de grupo antes de enviarlo al segundo nodo.

La representación compacta de los datos de verificación comprende opcionalmente una raíz de un árbol de Merkle, siendo derivado el árbol de Merkle de los datos de autenticación exclusivos del nodo y una pluralidad de tiempos de referencia relativos a un tiempo de referencia base dentro de un período de tiempo predeterminado. Como una opción adicional, la representación compacta de los datos de verificación de todos los nodos en la red comprende uno de un filtro de Bloom y una raíz de un árbol de Merkle derivados de los datos de autenticación de todos los nodos en las redes.

De acuerdo con un tercer aspecto de la invención, se proporciona un nodo de comunicaciones móvil para su uso en una red de comunicaciones. El nodo cuenta con un receptor para recibir desde un nodo de red una representación compacta de los datos de verificación de todos los nodos en la red certificados por el nodo de red. Se proporciona una memoria para almacenar la representación compacta recibida de los datos de verificación de todos los nodos en la red certificados por el nodo de red. El receptor está dispuesto además para recibir desde un nodo de anuncio un mensaje, el mensaje incluye los datos de autenticación y la información de confianza derivados de datos de autenticación para el nodo de anuncio. Se proporciona un procesador para verificar la autenticidad del mensaje usando la representación compacta de los datos de verificación de todos los nodos en la red, la información de confianza recibida y los datos de autenticación recibidos para el nodo de anuncio.

El nodo de comunicaciones móvil cuenta opcionalmente con un reloj, en el que el procesador está dispuesto para verificar la información de confianza comparándola con la información derivada de una hoja de un árbol de Merkle, siendo derivada la hoja de los datos de autenticación y la información derivada de un tiempo obtenido desde el reloj, estando dispuesto el procesador además para derivar una segunda representación compacta de los datos de verificación de todos los nodos en la red y verificar si dicha segunda representación compacta de los datos de verificación de todos los nodos concuerda con la representación compacta almacenada de los datos de verificación de todos los nodos en la red.

De acuerdo con un cuarto aspecto de la invención, se proporciona un nodo de red para su uso en una red de comunicaciones. El nodo de red comprende un procesador para derivar, para cada uno de una pluralidad de nodos asociados con la red de comunicaciones, datos de autenticación exclusivos de cada nodo, y una representación compacta certificada de los datos de verificación de todos los nodos en la red. También se proporciona un transmisor para enviar a cada uno de la pluralidad de nodos los datos de autenticación exclusivos de cada nodo, y la representación compacta certificada de los datos de verificación de todos los nodos en la red.

De acuerdo con un quinto aspecto de la invención, se proporciona un programa informático que comprende un código legible por ordenador que, cuando se ejecuta en un nodo de comunicaciones móvil, hace que el nodo de comunicaciones móvil se comporte como un nodo de comunicaciones móvil como se describe anteriormente en cualquiera de los segundos o terceros aspectos de la invención.

De acuerdo con un sexto aspecto de la invención, se proporciona un programa informático, que comprende un código legible por ordenador que, cuando se ejecuta en un nodo de red, hace que el nodo de red se comporte como un nodo de red como se describe anteriormente en el cuarto aspecto de la invención.

De acuerdo con un séptimo aspecto de la invención, se proporciona un producto de programa informático que comprende un medio legible por ordenador y un programa informático como se describe anteriormente en los aspectos quinto o sexto de la invención, en el que el programa informático se almacena en el medio legible por ordenador.

Breve descripción de los dibujos

La figura 1 ilustra esquemáticamente en escenarios de red de ejemplo de diagrama de bloques;

la figura 2 ilustra esquemáticamente un árbol de Merkle generado a partir de claves hash;

la figura 3 es un diagrama de señalización que ilustra la señalización de acuerdo con una realización de la invención;

la figura 4 es un diagrama de flujo que ilustra los pasos de una primera realización de la invención;

la figura 5 ilustra esquemáticamente en un diagrama de bloques un terminal de anuncio de acuerdo con una realización de la invención;

la figura 6 ilustra esquemáticamente en un diagrama de bloques un terminal de recepción de acuerdo con una realización de la invención; y

la figura 7 ilustra esquemáticamente en un diagrama de bloques un nodo de red de acuerdo con una realización de la invención.

Descripción detallada

La siguiente descripción supone que cada nodo en una red puede comunicarse con los nodos de la red central o entre sí sin comunicarse a través de la red (para crear una red ad hoc). Se supone una infraestructura LTE, aunque se apreciará que se podría usar un método similar en cualquier tipo de red de comunicaciones. La infraestructura LTE puede llegar a cualquier nodo habilitado ad-hoc en cualquier momento y en cualquier lugar mediante un canal de unidifusión y/o multidifusión, por ejemplo, "paginación" o difusión celular. También se supone que cada nodo tiene un reloj interno y que todos están sincronizados en el tiempo. Esta sincronización de tiempo no necesita ser exacta si se usa un mecanismo de ventana.

Cuando un nodo desea formar una red ad hoc con otro nodo, envía un anuncio. Se consideran las siguientes tres categorías de anuncio:

- Anuncios "públicos" que se refieren principalmente a anuncios orientados a negocios (por ejemplo, transporte público/privado, etc.)

- Anuncios "privados" que se refieren principalmente a anuncios de presencia y proximidad a un conjunto especial de nodos (por ejemplo, entre mis amigos y yo)

- Anuncios "semipúblicos" que se refieren a anuncios sociales y orientados a la seguridad (por ejemplo, juegos, servicios médicos, sociales, mensajes vehiculares, etc.)

Un UE 1 que se conecta a una red LTE 2 obtiene de forma segura un conjunto de "parámetros de seguridad", generados por la infraestructura LTE, por ejemplo la entidad de gestión de movilidad (MME), que se envían al UE 1. La seguridad para esta transmisión sería proporcionada típicamente por los protocolos de señalización existentes de UE a red. En una primera realización, los parámetros de seguridad se implementan usando árboles de Merkle. Estos parámetros se pueden dividir en dos categorías: un conjunto de parámetros usados para autenticar anuncios salientes y un (único) parámetro usado para verificar los entrantes. Esto significa que la infraestructura LTE puede rastrear cualquier comportamiento malicioso, como un ataque DoS, de vuelta al remitente y tomar las medidas necesarias (por ejemplo, prohibir a ese usuario en la red).

Se envía una representación compacta de los parámetros de seguridad a cada UE en la red. De acuerdo con una primera realización de la invención, la representación compacta se basa en árboles de Merkle, y de acuerdo con una

segunda realización de la invención, una representación compacta se basa en filtros de Bloom. Esta representación compacta es necesaria, ya que un UE puede necesitar verificar anuncios de cualquier otro UE. Puede haber miles de otros UE en la red, por lo que un enfoque directo para enviar una representación no compacta consumiría tanto ancho de banda que no sería práctico.

El método descrito a continuación se refiere principalmente a la categoría de anuncios semipúblicos, ya que la categoría privada exige su propia privacidad y seguridad. Sin embargo, el método también puede aplicarse a la categoría de anuncios públicos, ya que puede optimizar significativamente el uso del ancho de banda LTE al eliminar la necesidad de consultar la infraestructura para cada anuncio público.

El método para establecer una relación de confianza en una red ad hoc, como se describe a continuación, se considera que actúa como un mecanismo de confianza "temprano", y pretende ser un precursor de un protocolo de intercambio de claves. La habilitación de un descubrimiento de confianza rápido entre un anuncio y un UE que responde asegura que ambos nodos estén protegidos de un posible ataque DoS que, de lo contrario, podría iniciarse durante el procedimiento de emparejamiento.

Si los UE deciden interactuar, típicamente también tendrá lugar un establecimiento de clave por pares, por ejemplo, basándose en Diffie-Hellman, después del descubrimiento. Sin embargo, esto está fuera del alcance de la invención. Téngase en cuenta que la invención sería aplicable para autenticar los parámetros de Diffie-Hellman transmitidos.

Con el fin de describir mejor la primera realización de la invención, y con referencia a la figura 2, sigue una descripción de un árbol de Merkle:

Un árbol de Merkle es un árbol binario etiquetado. Las etiquetas de las hojas son de forma, L1 = H (R1), L2 = H (R2),…, Ln = H (Rn) donde H es una función hash criptográfica (unidireccional) (por ejemplo, implementada usando las funciones hash SHA-256 o Whirlpool) y Rj: s puede tener cualquier valor. La etiqueta de un vértice interno, v, se define de manera recursiva a partir de las etiquetas de los "hijos", es decir,

Etiqueta (v) = H (Etiqueta (izquierda (v)) || Etiqueta (derecha (v)))

donde izquierda (v) y derecha (v) corresponden al hijo izquierdo/derecho de v y || indica la concatenación. El árbol puede estar asociado/identificado por la etiqueta de la raíz.

Las funciones hash, como H, se pueden usar para autenticar o "señalar" mensajes individuales. El usuario publica el mensaje, m, y H(H(R) || m), donde R es un valor aleatorio. Para permitir la verificación, el usuario revela R. El verificador comprueba que R, cuando se realiza hash con el mensaje de acuerdo con la fórmula anterior, produce el mismo resultado. El inconveniente es que solo un único mensaje puede señalarse de forma segura ya que R se consume en el instante en que se divulga.

En el ejemplo de la figura 2, se genera un valor raíz Hash 0 a partir de los valores clave Clave 000 a Clave 003. Cada valor clave es una hoja del árbol de Merkle.

Los árboles de Merkle permiten la autenticación de varios mensajes. Cada hoja puede considerarse como la "clave pública" para un mensaje, lo que proporciona medios para autenticar un número de mensajes exponencial (en la profundidad del árbol). Téngase en cuenta que al usar árboles de Merkle, el usuario no solo debe revelar la hoja, sino también los hermanos "fuera de ruta" a lo largo de la ruta desde la hoja hasta la raíz. Hay un número logarítmico (en el tamaño del árbol) de dichos hermanos.

Para describir mejor la segunda realización de la invención, un filtro de Bloom es un vector de bits de una longitud predeterminada, m, junto con un conjunto de funciones hash k h1, h2, …, hk, mapeando en el conjunto {1, 2, .., m}. Para insertar un elemento de datos, x, en el filtro de Bloom, las posiciones de bits h1(x), h2(x), ... hk (x) del vector de bits están configuradas en "1". A la inversa, para determinar si un determinado elemento de datos candidato, y, es un miembro de un conjunto de datos codificado por el filtro de Bloom, las posiciones de bit h1(y), h2(y), ... hk (y) se verifican, y si todas estas posiciones de bit son "1", se puede suponer que y es un miembro del conjunto de datos. Como resultado, los filtros de Bloom pueden dar los llamados "falsos positivos", ya que las posiciones de los bits pueden haberse establecido en "1" por algún otro elemento o elementos, diferente de y. Sin embargo, la tasa de falsos positivos se puede controlar seleccionando valores apropiados de m y k. Por ejemplo, un filtro de Bloom con una tasa de falsos positivos 2 ^(-t) puede construirse siempre que el tamaño del filtro de Bloom sea al menos m = 1,44 x t x N, donde N es el número de elementos insertados.

Volviendo ahora a la primera realización de la invención, la MME determina una pluralidad de periodos de tiempo con referencia a un periodo de tiempo base. Por ejemplo, suponiendo que el período de tiempo mínimo es de 6 segundos si el período de tiempo base es medianoche, cada período de tiempo de la pluralidad de períodos de tiempo es medianoche + 6 segundos, medianoche + 12 segundos, media noche + 18 segundos y así sucesivamente. Cada período de tiempo puede ser usado por un nodo para enviar un anuncio. A cada anuncio se le asignan dos parámetros especiales llamados datos de autenticación e información de confianza que, al menos en

parte, están previamente almacenados en el nodo de anuncio. De ello se deduce que un período de 24 horas requiere 14400 parámetros de confianza diferentes con la granularidad anterior. El número de parámetros se conoce como n (n = 14400 es el valor predeterminado en este ejemplo).

La MME también determina un número máximo, N, de usuarios servidos. Para cada usuario, u = 1, 2, ... N, y cada período de tiempo, j = 1, 2, … n la red asigna un (pseudo) valor aleatorio Suj que sirve como datos de autenticación para el período de tiempo correspondiente, Tj.

La MME calcula un árbol de Merkle y lo certifica para cada usuario /UE legítimo (por ejemplo, en la conexión de red). Cada hoja del árbol de Merkle se calcula mediante la realización de hash de los datos de autenticación aleatorios Suj asociados con ese UE con cada uno de los 14400 períodos de tiempo. Esto significa que hoja (j) o Lj = Primero [128, H (Suj | Tj)], donde Suj es el secreto anterior asociado con Tj, elegido por la red y que también es conocido por el usuario y Tj corresponde a un período de tiempo específico. Para simplificar, se supone que todos los Tj tienen la misma duración, aunque es posible tener Tj de diferentes duraciones. Esto puede tener en cuenta el tráfico pico en la red donde se permiten más Tj en un período de tiempo determinado.

Téngase en cuenta que en un caso típico como una red LTE, cada Suj podría generarse a partir de una clave, Su, compartida entre la red y el UE de acuerdo con, por ejemplo, Suj = H(Su, j). Por lo tanto, solo debe ponerse a disposición del UE y la red, y no debe revelarse a otros UE.

LTE genera y almacena un árbol de Merkle específico para cada UE que cubre las siguientes 24 horas. Por lo tanto, la red LTE calcula previamente R(u), la raíz del árbol de Merkle del usuario u (antes de que el usuario se conecte). Esto se repite para todos los N usuarios. Téngase en cuenta que solo es necesario almacenar Su, TO, n y R(u), en lugar de los árboles completos: cualquier vértice interno se puede reconstruir, si es necesario, desde TO, n y Su. Esto implica O(N * n) cálculos hash.

En algún momento, el UE 1 se conecta a un ecosistema social ad-hoc a través de la autenticación y autorización de LTE, durante el cual recibe de forma segura los datos de autenticación Suj (o Su) y n de la red. El UE 1 puede crear los parámetros principales de su propio árbol hash, lo que significa que el UE 1 y la red LTE no necesitan intercambiar ninguna hoja específica porque ambos pueden generar cualquiera de ellas siempre que se requieran usando T1, n, el Su compartido y un hash unidireccional, H. El UE 1 también recibe un único certificado de sistema que representa un conjunto de al menos todos los usuarios conectados actualmente. (El certificado también puede representar a usuarios aún no conectados como se describe a continuación). Este certificado del sistema es una representación compacta y verificable de todas las raíces del árbol de Merkle de los usuarios, que se explica a continuación.

Cuando el UE 1 desea formar una red ad hoc con otro UE 3 sin involucrar más a la red 2, el UE 1 envía un anuncio que incluye los datos de autenticación Suj y la información de confianza basándose en la hoja correspondiente, Lj, asociada con el intervalo de tiempo actual, Tj, de la transacción. Por ejemplo, Lj puede usarse como una clave para calcular un código de autenticación de mensaje (MAC), por ejemplo, Hash(Lj, mensaje).

Al enviar Suj, (y posiblemente hermanos, según sea necesario), el UE 3 de recepción puede calcular la raíz y verificar su validez a través de una copia local del certificado del sistema que el UE 3 ha recibido previamente de la red. El receptor no necesita verificar si la hoja es parte del árbol. En su lugar, verifica si el conjunto de parámetros conduciría a una raíz, que es un parámetro válido, en otras palabras está certificado por el certificado del sistema.

El certificado del sistema debe permitir que el nodo de recepción verifique cualquier nodo en la red. Como se describió anteriormente, no es deseable distribuir una raíz asociada con cada UE registrado en la red, ya que puede haber un número muy alto de ellos. Por lo tanto, la red crea un segundo árbol de Merkle usando las raíces de cada UE registrado: R(1), R(2), ... R(N) como hojas de entrada. La raíz del árbol de todo el sistema se denomina R. La red señaliza R usando un mecanismo de señal convencional, por ejemplo, criptografía de clave pública RSA, y la distribuye. Para cada usuario u, la red envía información que comprende los hermanos "fuera de ruta" de la ruta de R(u) a la raíz R. Por lo tanto, suponiendo que el número de usuarios es N = 2^t, cada usuario obtiene valores adicionales O(registro N) = O(t). Este conjunto se denomina Sib (u). Téngase en cuenta que como esta distribución es unidifusión de la red a cada UE, las claves (compartidas) LTE preexistentes se pueden usar alternativamente para "señalar" R y esta información, en lugar de usar RSA.

Téngase en cuenta que el esfuerzo computacional total de la red para construir R es O(N*(n + 1)) evaluaciones de la función hash: O(N*n) para construir todo R(u) y luego O(N) para combinarlos en R.

Durante un intercambio de descubrimiento de confianza del vecino posterior entre dos nodos en una red inalámbrica ad hoc, el nodo de recepción debe validar los datos de autenticación y la información de confianza enviada por el nodo de anuncio sin comunicarse con ningún nodo de red central como MME. Para autenticar un anuncio, un UE 1 de nodo de anuncio libera una hoja en su árbol (asociado con el período de tiempo, Tj obtenido del reloj interno del UE 1) y la información correspondiente fuera de ruta que conduce a la raíz R(u), es decir, valores O(d) donde d = registro n. El usuario de anuncio también envía Sib(u), es decir, valores de O(t). Una "señal" ahora tiene tamaño O(d

+ t). Téngase en cuenta que Sib(u) puede almacenarse en caché para su futuro uso si el espacio de almacenamiento lo permite.

El número de cálculos hash que debe realizar un UE 3 de nodo de recepción para verificar un anuncio también es O(d + t). Esto se hace primero reconstruyendo R(u), luego reconstruyendo R a partir de R(u) y Sib(u).

Se debe tener en cuenta que el nodo de recepción también debería incluir los datos de autenticación y la información de confianza al responder a un mensaje de anuncio para que ambos nodos UE 1 y UE 3 puedan estar mutuamente seguros de que son legítimos.

El protocolo de intercambio de claves entre los dos nodos UE 1 y UE 3 debe abarcar la confianza mostrada durante el protocolo de descubrimiento de confianza del vecino, pero no debe revelar ninguna de las identidades de los nodos. Para este propósito, los primeros dos mensajes requeridos para realizar un intercambio Diffie-Heilman podrían enviarse en modo de multidifusión y deberían llevar parámetros adicionales que se generen a partir de los "parámetros de confianza" intercambiados entre los dos nodos o durante el intercambio de descubrimiento de confianza del vecino.

Con referencia a la figura 3, y con la siguiente numeración correspondiente a la numeración de la figura, los siguientes pasos describen una descripción general de la invención.

S1 y S2. La MME 2 envía a todos los nodos en la red (incluidos los UE 1 y UE 3) los datos de autenticación Su (o Suj) relacionados con cada nodo y el certificado del sistema señalizado. Esto se hace típicamente cuando cada nodo se conecta a la red.

S3. Cuando el UE 1 desea configurar una red ad hoc con otro nodo, determina la información de confianza que comprende la hoja de su árbol de Merkle Lj asociada con la hora actual Tj y los datos de autenticación correspondientes Suj determinados a partir de su reloj interno. La información de confianza y los datos de autenticación se usan para autenticar un anuncio, m.

S4. El UE 1 envía la información de confianza y los datos de autenticación al UE 3 en un anuncio. Por lo tanto, la información transmitida incluye "mensaje", H(Lj, "mensaje"), Suj (es decir, el anuncio en sí, y la información de confianza que comprende el MAC y los datos de autenticación).

S5. El UE 3 verifica el anuncio al calcular Lj = H(Suj | Tj), verificar H (Lj, "mensaje") y luego determinar la raíz del árbol de Merkle para el UE 1, y luego determinar que la raíz R puede derivarse de la raíz para el UE 1 y Sib (u).

La Figura 4 muestra la primera realización específica con más detalle, con la siguiente numeración correspondiente a la numeración de la figura 4:

S6. El UE 1 recibe su información de autenticación (Suj) y el árbol de Merkle certificado derivado de los datos de autenticación de todos los nodos en la red.

S7. El UE 1 deriva una hoja (Lj) de un árbol de Merkle usando sus datos de autenticación (Suj) y una hora (Tj) obtenida indirectamente de su reloj interno. La hoja derivada Lj se usa para derivar el resto de la información de confianza, H(Lj, "mensaje").

S8. El UE 1 envía al UE 2 un mensaje que incluye la información de confianza.

S9. El UE 3 deriva una hoja de árbol de Merkle usando los datos de autenticación y un tiempo de referencia obtenido indirectamente de su propio reloj interno. Se apreciará que los relojes internos del UE 1 y el UE 3 deben estar sincronizados de manera razonablemente estrecha, aunque se pueden permitir algunas diferencias si el UE 3 almacena en caché el mensaje recibido. El resto de la información de confianza H(Lj, "mensaje") también se verifica.

S10. El UE 3 deriva una raíz de un árbol de Merkle para el primer nodo usando la hoja derivada.

S11. El UE 3 determina si la raíz del árbol de Merkle certificado derivado de los datos de verificación de todos los nodos en la red puede derivarse de la raíz del árbol de Merkle para el primer nodo que ha derivado. Si es así, entonces se verifica el mensaje.

Los siguientes ejemplos suponen que se usa una función hash, H, que produce m salidas de bits, por ejemplo, m = 128. El sistema tiene N usuarios y se necesitan n períodos de tiempo (por ejemplo, n = 14400).

Inicialización del sistema:

1. El nodo 2 de red (como una MME) decide los parámetros N y n en el período de tiempo actual T1 (o ligeramente antes).

2. Para cada u = 1, 2, …, N, el nodo 2 de red elige un Su aleatorio (o Suj pseudoaleatorio), construye R(u) a partir de Su y T1, T2, ... Tn, y almacena Su y R(u).

3. R se determina a partir de R(1), R(2), ... R(N), y se almacena.

4. La red señaliza R y lo envía a todos los nodos en la red.

Unión

Esto se ejecuta cuando un nuevo UE, indicado u, se une.

1. Se lleva a cabo la seguridad de acceso normal de LTE.

2. La red envía T1, n, Su y R(u) al UE (alrededor de 2m de bits) protegidos por seguridad de acceso de LTE. Alternativamente, el UE puede seleccionar Su y enviar a la red.

3. En una realización opcional (ya que se supone que la red es de confianza), el UE puede tomar "muestras" para verificar que R(u) se haya creado correctamente, es decir, evaluar algunas rutas (aleatorias) desde las hojas hasta la raíz.

4. La red envía a Sib(u), los hermanos fuera de ruta O(registro N) de R(u) en R a u (un total de O(m * registro N) bits), protegidos por la seguridad de acceso LTE.

5. En una realización opcional, el UE verifica que R es correcto (que requiere cálculos hash O(registro N)).

Autenticar un anuncio

1. El UE 1 deriva la hoja correcta, Lj, correspondiente a Suj y el período de tiempo actual, Tj.

2. El UE 1 hace un anuncio al UE 3, autenticado por Lj (usando Lj como clave para H, por lo que solo se necesita un cálculo de H), los datos de autenticación Suj y los O(registro n) hermanos fuera de ruta de Lj así como los hermanos fuera de ruta O(registro N) de R(u). Como alternativa al paso 2, el UE solo envía el mensaje y el MAC. Un UE 3 de nodo que recibe el anuncio debe solicitar datos de autenticación y los hermanos del UE 1. En cualquier caso, la comunicación total del remitente antes de que alguien más pueda verificar el (primer) anuncio (véase la siguiente sección) es O(m*(1 + registro n + registro N)).

Verificar un anuncio

1. El UE 3 recibe un (primer) anuncio del UE 1 y obtiene los datos de autenticación (correspondientes al UE 1) y los hermanos como se explicó anteriormente, ya sea como parte del anuncio o solicitándolos al UE.

2. El UE 3 verifica que el MAC sea correcto y que Lj junto con los hermanos conduzcan a una raíz R(u), que usa evaluaciones O(1 + registro n) de H.

3. Si es correcto, el UE 3 verifica que R(u) junto con los hermanos del árbol (actual) de todo el sistema, R, conduce a la raíz de R, es decir, evaluaciones O(registro N) de H.

Después del paso 2, el UE de recepción puede almacenar en caché R(u) de modo que si se reciben mensajes posteriores dentro del tiempo de vida de R(u) y R, solo deben realizarse los pasos 1 y 2.

De acuerdo con una segunda realización específica, cada usuario u tiene un árbol de Merkle que se identifica por su raíz, R(u). El principio es el mismo que en la primera realización, ya que el usuario revela las hojas y los hermanos para permitir a otros calcular la ruta a la raíz, autenticando los anuncios. La diferencia en la segunda realización radica en la forma en que se obtiene la "representación compacta" de las claves públicas de todos los usuarios. En la primera realización específica, otro árbol de Merkle para este propósito, mientras que en la segunda realización específica, se usa un filtro de Bloom.

Las raíces de los árboles de Merkle de cada usuario {R(1), R(2), …, R(u), R(N)} se insertan en un filtro de Bloom. La red LTE señaliza el filtro de Bloom, por ejemplo, usando RSA. Cuando el usuario desea autenticar un anuncio, luego después de calcular la raíz (candidata) R(u) del usuario u, el usuario de verificación comprueba si R(u) es miembro del filtro de Bloom señalizado en todo el sistema.

Hay algunas ventajas y desventajas con el uso de un filtro de Bloom. Primero, cuando la red LTE inicializa los parámetros del sistema, no necesita generar árboles de Merkle para los usuarios que aún no se han conectado. Esto se debe a que se pueden insertar elementos arbitrarios en el filtro de Bloom en una etapa posterior. Cuando se

agrega un nuevo usuario, el nodo de red actualiza el filtro de Bloom y lo vuelve a señalar. El árbol de Merkle de todo el sistema no tiene esta propiedad debido a la naturaleza "unidireccional" de la función hash H: las hojas no se pueden agregar "después", el árbol debe generarse de hoja a raíz desde el principio. Además, la verificación del anuncio es más eficiente usando un filtro de Bloom, ya que la profundidad de los árboles involucrados no depende del número total de usuarios en el sistema, sino solo de la cantidad de anuncios realizados por cada usuario. En otras palabras, las realizaciones del árbol de Merkle darían lugar a árboles con una profundidad total de O(registro n + registro N) en lugar de O(registro n) al usar filtros de Bloom. Dada la raíz del árbol de Merkle del usuario u, la verificación del filtro de Bloom es esencialmente instantánea. Específicamente, suponiendo que el filtro de Bloom tenga k funciones hash, verificar que el filtro de Bloom corresponde a los k cálculos hash.

El inconveniente del enfoque del filtro de Bloom es la tasa de falsos positivos de los filtros de Bloom descritos anteriormente. Incluso si una raíz R(u) no está insertada en el filtro de Bloom, puede parecer que lo está. Sin embargo, esto puede controlarse eligiendo los parámetros BF.

Los siguientes ejemplos que usan un filtro de Bloom hacen las mismas suposiciones que los que se hacen al describir la primera realización específica.

Inicialización del sistema

1. El nodo 2 de red determina el parámetro N. Supongamos que el período de tiempo actual es T1 (o ligeramente antes). El sistema elige un filtro de Bloom con un tamaño adecuado y k adecuado (basándose en N y una tasa deseada de falsos positivos). El filtro de Bloom se inicializa para estar vacío.

2. La red señaliza el filtro de Bloom y comienza a enviarlo (por ejemplo, emitir) a todos los nodos en la red.

Unión

Esto se ejecuta cuando un nuevo UE 1, indicado u, se adjunta.

1. Se lleva a cabo la seguridad de acceso LTE normal.

2. El UE 1 elige n hojas y forma un árbol de Merkle, R(u), que se envía al nodo 2 de red protegido por la seguridad de acceso LTE. (Alternativamente, el nodo 2 de red puede elegir el árbol/las hojas, por ejemplo, basándose en los valores de Su/Suj como se describió anteriormente).

3. Opcionalmente, la parte que NO genera el árbol puede tomar muestras para verificar que R(u) se haya creado correctamente, es decir, evaluar algunas rutas (aleatorias) desde las hojas hasta la raíz.

4. La red agrega R(u) al filtro de Bloom, vuelve a señalar el filtro de Bloom y comienza a transmitir el nuevo valor.

Autenticar un anuncio

1. El UE 1 localiza los datos de autenticación correctos Suj (y, por lo tanto, la hoja correspondiente, Lj), correspondiente al período de tiempo actual, Tj.

2. El UE 1 hace un anuncio, autenticado por Lj (por ejemplo, usando Lj como clave para H, por lo que solo se necesita un cálculo de H), los datos de autenticación y los hermanos fuera de ruta O(registro n) de Li.

Como alternativa al paso 2, el UE solo envía el mensaje y el MAC. Un usuario que recibe el anuncio debe solicitar los datos de autenticación y los hermanos. En cualquier caso, la comunicación total del remitente antes de que alguien más pueda verificar el (primer) anuncio (véase más abajo) es O(m*(1 + registro n + registro N)).

Verificar un anuncio

1. Un UE 3 que recibe un (primer) anuncio del UE 1 primero necesita obtener los datos de autenticación y los hermanos como se explicó anteriormente, ya sea como parte del anuncio o por solicitud del UE 1. Se supone que el UE 3 tiene una copia del filtro de Bloom más recientemente emitido (y señalizado).

2. El UE 3 de recepción deriva una raíz R(u) y comprueba que R(u) está en el filtro de Bloom emitido, después de haber verificado que el MAC es correcto y que Lj junto con los hermanos conducen a la raíz R(u), que usa O(1 + registro n) evaluaciones de H.

Después de 2, el UE de recepción puede almacenar en caché R(u) de modo que en los mensajes posteriores enviados dentro del tiempo de vida de R(u) y R, solo deben realizarse los pasos 1 y 2.

Volviendo ahora a la figura 5, se ilustra esquemáticamente en un diagrama de bloques un UE 1 que envía un mensaje de anuncio. El UE 1 cuenta con un receptor 5 para recibir su información de autenticación y el árbol de Merkle certificado (o filtro de Bloom si se usa la segunda realización). Para los propósitos de esta descripción, se hará referencia a un árbol de Merkle aunque la persona experta apreciará que se podría usar un filtro de Bloom como se describió anteriormente). Se proporciona un procesador 6 para derivar una hoja del árbol de Merkle del UE 1 usando los datos de autenticación y el tiempo de referencia y para derivar la información de confianza de la hoja. El tiempo se obtiene directa o indirectamente de un reloj 8. Se proporciona un transmisor 7 para enviar la información de confianza y los datos de autenticación al UE 3. Se proporciona una memoria 9 para almacenar una clave de grupo, en cuyo caso el procesador 6 está dispuesto para cifrar al menos parte del mensaje usando la clave de grupo (como se describe a continuación en la tercera realización específica) antes de enviarla al UE 3. La memoria 9 también se puede usar para almacenar un programa informático 10 que hace que el UE 1 se comporte como se describe anteriormente.

La figura 6 muestra esquemáticamente en un diagrama de bloques un nodo de recepción tal como el UE 3. El UE 3 cuenta con un receptor 11 para recibir el árbol de Merkle certificado. Esto se almacena en una memoria 12. El receptor 11 también está dispuesto para recibir un mensaje del UE 1 que incluye los datos de autenticación y la información de confianza derivada. Se proporciona un procesador 13 para verificar la autenticidad del mensaje usando el árbol de Merkle certificado y los datos de autenticación y la información de confianza recibidos. También se proporciona un reloj 14 para permitir que el procesador 13 verifique la información de confianza como se describe anteriormente. La memoria 12 también se puede usar para almacenar un programa informático 15 que hace que el UE 3 se comporte como se describe anteriormente.

La figura 7 muestra esquemáticamente, en un diagrama de bloques, un nodo 2 de red, tal como una MME. La MME cuenta con un procesador 6 para derivar y certificar un árbol de Merkle (o un filtro de Bloom) a partir de datos de autenticación asociados con cada nodo en la red. Se proporciona un transmisor 17 para enviar el árbol de Merkle certificado (o filtro de Bloom) a cada uno de la pluralidad de nodos en la red, junto con los datos de autenticación exclusivos de cada nodo. También se puede proporcionar una memoria 18 para almacenar datos y un programa informático 9 que hace que la MME se comporte como se describe anteriormente.

La siguiente descripción proporciona un análisis de las ventajas y desventajas de las dos realizaciones.

Desde el punto de vista de la seguridad, se deben considerar dos "ataques".

1. La probabilidad de crear un usuario "falso".

2. La probabilidad de falsificar anuncios en nombre de un usuario legítimo.

En ambas realizaciones, la probabilidad de ataque 2 está determinada por el tamaño de las funciones hash usadas en el árbol de Merkle por usuario y se puede hacer muy pequeña, por ejemplo, 2^(-t) cuando se usan funciones hash de t-bit, por ejemplo, t = 128 o 256.

La probabilidad de ataque 1, sin embargo, depende de si se usan árboles de Merkle o filtros de Bloom para la representación compacta.

Cuando se usan árboles de Merkle, la probabilidad también depende del tamaño de la función hash, es decir, t. Por lo tanto, es fácil asegurar que los ataques 1 y 2 tengan la misma probabilidad (baja) cuando se usan árboles de Merkle.

Sin embargo, cuando se usan filtros de Bloom, la probabilidad de ataque 1 es la misma que la tasa de falsos positivos del filtro de Bloom. Para reducir esto a 2^(-t), como se describió anteriormente, el filtro de Bloom debe tener el tamaño m = 1,44 * t * N, donde N es el número de usuarios. Téngase en cuenta que esto es peor que la realización del árbol de Merkle, que solo necesita t bits para la única raíz de todo el sistema. De hecho, este valor de m es en realidad un 44% más grande que la solución "trivial" de simplemente concatenar las raíces individuales del árbol de Merkle de todos los usuarios N, ya que esto conduciría al tamaño t * N para la representación "compacta". Un filtro de Bloom más pequeño que esta solución trivial podría lograrse a expensas de una tasa de falsos positivos de 2^(- t/1,44). Por ejemplo, con t = 128, la tasa de falsos positivos será aproximadamente 2^(- 88). En general, para lograr una "compresión" plegada en comparación con la solución trivial, necesitaremos aceptar una tasa de falsos positivos de 2^(-t/(1,44*c)).

A pesar de la necesidad de aceptar una mayor probabilidad de ataque 1 al usar filtros de Bloom, la realización de filtro de Bloom todavía tiene la ventaja de que la complejidad de la verificación es independiente del número de usuarios, N, mientras que crece logarítmicamente con N cuando se usa solo los árboles de Merkle. La tasa más alta de falsos positivos también puede ser aceptable si la solución se complementa con una segunda fase de autenticación de usuario (fuerte, mutua) después de la autenticación inicial del anuncio.

Como se describe en las dos primeras realizaciones, el sistema no es totalmente privado ya que se puede rastrear a un usuario mediante la revelación repetida de sus parámetros (por ejemplo, raíz, R(u)). Aunque la identidad del usuario sigue siendo desconocida, este tipo de seguimiento puede no ser deseable.

De acuerdo con una tercera realización específica, que es compatible con cualquiera de la primera o la segunda realización específica, se puede introducir una clave secreta compartida entre todos los usuarios en un "grupo de amigos" para mejorar la privacidad. Esta clave se denomina KB y puede ser elegida por el nodo 2 de red y comunicada a los usuarios a medida que se unen. Se supone que el nodo 2 de la red LTE sabe a qué grupos pertenece un usuario.

Cuando Bob hace un anuncio, todo está cifrado usando KB. Solo los miembros del grupo pueden descifrar, pero téngase en cuenta que no pueden estar seguros de que el anuncio fue dirigido a ellos antes de intentar reconstruir el árbol de Bob. Por lo tanto, Bob cifra no solo la raíz R(u) de su árbol, sino que también la "prefija" mediante un texto (no cifrado) que indica que el mensaje se dirige a este grupo de amigos. Cada miembro del grupo solo necesita descifrar la primera parte del mensaje para verificar si el mensaje está dirigido a ellos, y si tiene algún sentido el intento de reconstruir el árbol.

Se apreciará que cuando se usa la tercera realización con la segunda realización, en lugar de aumentar k, se podrían usar varios filtros de Bloom. En este caso, cada grupo de amigos tiene un certificado en forma de un filtro de Bloom (señalizado), pero que solo contiene los árboles de Merkle de ese grupo de amigos en particular.

La persona experta en la técnica apreciará que pueden realizarse diversas modificaciones a las realizaciones descritas anteriormente sin apartarse del alcance de la presente invención. En particular, la invención puede aplicarse en cualquier tipo de red de comunicaciones. Además, se apreciará que mientras la descripción anterior usa el tiempo obtenido de un reloj para ayudar a verificar de manera independiente la autenticidad de un mensaje enviado desde el primer nodo, se puede usar una variable independiente alternativa.

Las siguientes abreviaturas se usan en la descripción anterior:

DoS	Denegación de servicio
LTE	Evolución a largo plazo
UE	Equipo de usuario
MME	Entidad de gestión de movilidad
CA	Autoridad certificadora

REIVINDICACIONES

1.- Un método para establecer la confianza entre dos nodos (1, 3) de comunicaciones móviles que están unidos a una red (2) de comunicaciones, comprendiendo el método:

en un primer nodo (1) de los dos nodos de comunicaciones móviles, recibir de un nodo (2) de red datos de autenticación exclusivos del primer nodo, cuyos datos de autenticación se aseguran mediante la red de comunicación y desde el cual se puede derivar una representación compacta de los datos de verificación para el primer nodo (1) y una representación compacta adicional de los datos de verificación de todos los nodos de comunicaciones móviles en la red, por lo que la representación compacta adicional de los datos de verificación se asegura mediante la red de comunicaciones y ser certifica mediante el nodo de red;

en el primer nodo (1), derivar información de confianza de los datos de autenticación exclusivos del primer nodo (1); y

enviar desde el primer nodo (1) a un segundo nodo (3) de los dos nodos de comunicación móviles, habiendo recibido también el segundo nodo (3) la representación compacta adicional de los datos de verificación de todos los nodos en la red, un mensaje que se asegura mediante la red de comunicaciones e incluye la información e confianza y al menos una parte de los datos de autenticación exclusivos del primer nodo (1); y

en el segundo nodo (3), verificar la autenticidad del mensaje desde el primer nodo (1) usando la representación compacta adicional de los datos de verificación de todos los nodos en la red, la información de confianza recibida desde el primer nodo (1), y al menos dicha parte de los datos de autenticación recibidos desde el primer nodo (1).

2.- El método de acuerdo con la reivindicación 1, en el que la representación compacta adicional de los datos de verificación del primer nodo (1) comprende una raíz de un árbol de Merkle derivado de los datos de autenticación exclusivos del primer nodo y una pluralidad de tiempos de referencia relativos a un tiempo de referencia base dentro de un período de tiempo predeterminado.

3.- El método de acuerdo con la reivindicación 1 o 2, en el que la representación compacta adicional de los datos de verificación de todos los nodos en la red comprende uno de un filtro de Bloom y una raíz de un árbol de Merkle derivados de los datos de verificación de todos los nodos en las redes.

4.- El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, que comprende además:

en el primer nodo (1), derivar una hoja de un árbol de Merkle de los datos de autenticación exclusivos del primer nodo (1) y un solo tiempo de referencia derivado de la información obtenida de un reloj en el primer nodo (1),

en el que la información de confianza se deriva de la hoja derivada.

5.- El método de acuerdo con la reivindicación 4, en el que el segundo nodo (3) verifica la autenticidad del mensaje desde el primer nodo:

derivando una hoja de un árbol de Merkle de dichos datos de autenticación y un tiempo de referencia derivado de la información obtenida de un reloj en el segundo nodo;

verificando la información de confianza;

derivando una segunda representación compacta de los datos de verificación del primer nodo (1); y

verificando que la segunda representación compacta de los datos de verificación del primer nodo (1) concuerda con la representación compacta de los datos de verificación de todos los nodos en la red.

6.- El método de acuerdo con la reivindicación 5, en el que la representación compacta de los datos de verificación de todos los nodos en la red comprende un filtro de Bloom, y la segunda representación compacta de los datos de verificación del primer nodo (1) concuerda con la representación compacta adicional de los datos de verificación de todos los nodos en la red si la segunda representación compacta de los datos de verificación se indica como un miembro del filtro de Bloom.

7.- El método de acuerdo con la reivindicación 5, en el que la representación compacta adicional de los datos de verificación de todos los nodos en la red comprende una raíz de un árbol de Merkle derivada de los datos de autenticación de todos los nodos en la red, y la segunda representación compacta de los datos de verificación del primer nodo (1) concuerda con la representación compacta de los datos de verificación de todos los nodos en la red si la raíz del árbol de Merkle se deriva de la segunda representación compacta de los datos de verificación del primer nodo (1).

8.- Un primer nodo (1) de comunicaciones móviles para su uso en una red (2) de comunicaciones, comprendiendo el primer nodo:

un transmisor (7), un receptor (5), y un procesador (6), dispuestos para unir el primer nodo a la red de comunicaciones;

estando además dispuesto el receptor para recibir desde un nodo de red datos de autenticación exclusivos del primer nodo, cuyos datos de autenticación se aseguran mediante la red de comunicaciones y desde la cual se deriva una primera representación compacta de los datos de verificación del primer nodo, y una representación compacta adicional de los datos de verificación de todos los nodos en la red, por lo que la representación compacta adicional de los datos de verificación se aseguran mediante la red de comunicaciones y se certifica mediante el nodo (2) de red;

estando además dispuesto el procesador para derivar información de confianza de los datos de autenticación exclusivos del primer nodo (1); estando dicho nodo (1) de comunicación móvil caracterizado por

el transmisor que está además dispuesto para enviar un segundo nodo (3) que está unido a la red de comunicaciones y que ha recibido la representación compacta adicional de los datos de verificación de todos los nodos en la red, un mensaje que se asegura mediante la red de comunicaciones e incluye la información de confianza y al menos una parte de los datos de autenticación exclusivos del primer nodo (1), en el que la información de confianza se aplica mediante el segundo nodo (3) para verificar la autenticidad del mensaje usando la representación compacta adicional de los datos de verificación de todos los nodos en la red, la información de confianza recibida desde el primer nodo (1) y al menos dicha parte de los datos de autenticación recibidos desde el primer nodo (1).

9.- El primer nodo (1) de comunicaciones móvil de acuerdo con la reivindicación 8, que comprende además un reloj, en el que el procesador está dispuesto para derivar una hoja de un árbol de Merkle de los datos de autenticación exclusivos del nodo y un solo tiempo de referencia derivado de la información obtenida del reloj, en el que la información de confianza se deriva de la hoja derivada.

10.- El primer nodo (1) de comunicaciones móvil de acuerdo con la reivindicación 8 o 9, que comprende además una memoria para almacenar una clave de grupo, en la que el procesador está dispuesto para cifrar al menos parte del mensaje usando la clave de grupo antes de enviarlo al segundo nodo (3).

11.- El primer nodo (1) de comunicaciones móvil de acuerdo con cualquiera de las reivindicaciones 8 a 10, en el que la primera representación compacta de los datos de verificación comprende una raíz de un árbol de Merkle derivada de los datos de autenticación exclusivos del primer nodo y una pluralidad de tiempos de referencia relativos a un tiempo de referencia base dentro de un período de tiempo predeterminado.

12.- El primer nodo (1) de comunicaciones móvil de acuerdo con cualquiera de las reivindicaciones 8 a 11, en el que la representación compacta adicional de los datos de verificación de todos los nodos en la red comprende uno de un filtro de Bloom y una raíz de un árbol de Merkle derivados de los datos de autenticación de todos los nodos en las redes.

13.- Un segundo nodo (3) de comunicaciones móvil para su uso en una red (2) de comunicaciones, comprendiendo el segundo nodo:

un transmisor, un receptor (11), y un procesador (13), dispuestos para unir el segundo nodo a la red de comunicaciones;

estando además dispuesto el receptor para recibir desde un nodo (2) de red una representación compacta adicional de los datos de verificación de todos los nodos en la red, por lo que dicha representación compacta adicional de los datos de verificación se asegura mediante la red de comunicaciones y se certifica mediante el nodo de red;

una memoria (12) para almacenar la representación compacta adicional de los datos de verificación de todos los nodos en la red;

estando dicho segundo nodo de comunicación móvil caracterizado por

el receptor que está además dispuesto para recibir desde un primer nodo (1) que está unido a la red de comunicaciones un mensaje que se asegura mediante la red de comunicaciones y que incluye al menos parte de los datos de autenticación exclusivos del primer nodo y la información de confianza derivada a partir de los datos de autenticación exclusivos del primer nodo; y

el procesador siendo además dispuesto para verificar la autenticidad del mensaje recibido desde primer nodo usando la representación compacta de los datos de verificación de todos los nodos en la red, la información de

confianza recibida desde el primer nodo (1), y al menos dicha parte de los datos de autenticación recibidos desde el primer nodo (1).

14.- El segundo nodo (3) de comunicaciones móvil de acuerdo con la reivindicación 13, que comprende además un reloj, en el que el procesador está dispuesto para verificar la información de confianza comparándola con la información derivada de una hoja de un árbol de Merkle, siendo derivada la hoja de los datos de autenticación y la información derivada de una hora obtenida del reloj, estando dispuesto además el procesador para derivar una segunda representación compacta de los datos de verificación de todos los nodos en la red y verificar si dicha segunda representación compacta de los datos de verificación de todos los nodos concuerda con la representación compacta almacenada de los datos de verificación de todos los nodos en la red.

15.- Un nodo (2) de red para su uso en una red de comunicaciones, comprendiendo el nodo de red:

un procesador (16) para derivar, para cada uno de una pluralidad de nodos (1, 3) de comunicaciones móviles que se han unido a la red de comunicaciones, datos de autenticación exclusivos de cada nodo y una representación compacta certificada de los datos de verificación de todos los nodos en la red; y

un transmisor (17) para enviar a cada uno de la pluralidad de nodos los datos de autenticación exclusivos de cada nodo, y la representación compacta certificada de los datos de verificación de todos los nodos en la red, cuyos datos de autenticación y representación compacta certificada única de los datos de verificación se aseguran mediante la red de comunicaciones, caracterizada porque

dicho nodo (2) de red verifica la autenticidad de un mensaje recibido desde un primer nodo de la pluralidad de los nodos de comunicaciones que se han unido, dicho mensaje se asegura mediante la red de comunicaciones e incluye información de confianza, dicha información de confianza se deriva mediante el primer nodo (1) de los datos de autenticación exclusivos del primer nodo, y al menos una parte de los datos de autenticación exclusivos del primer nodo, usando la representación compacta certificada de los datos de verificación de todos los nodos en la red, la información de confianza recibida desde el primer nodo (1), y al menos dicha parte de los datos de autenticación exclusivos del primer nodo (1) recibido desde el primer nodo (1).

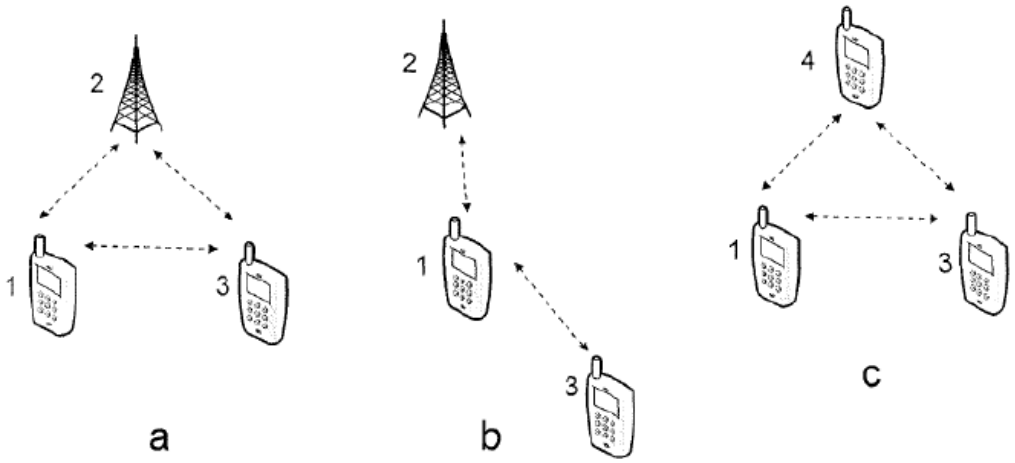

Figura 1

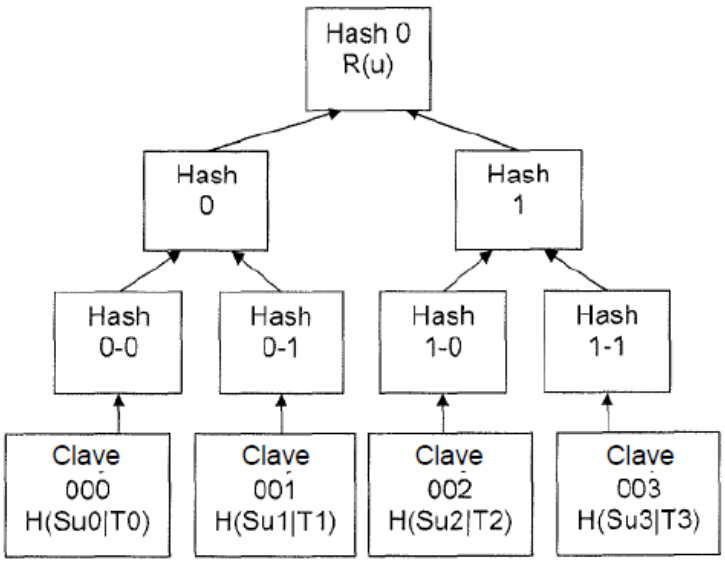

Figura 2

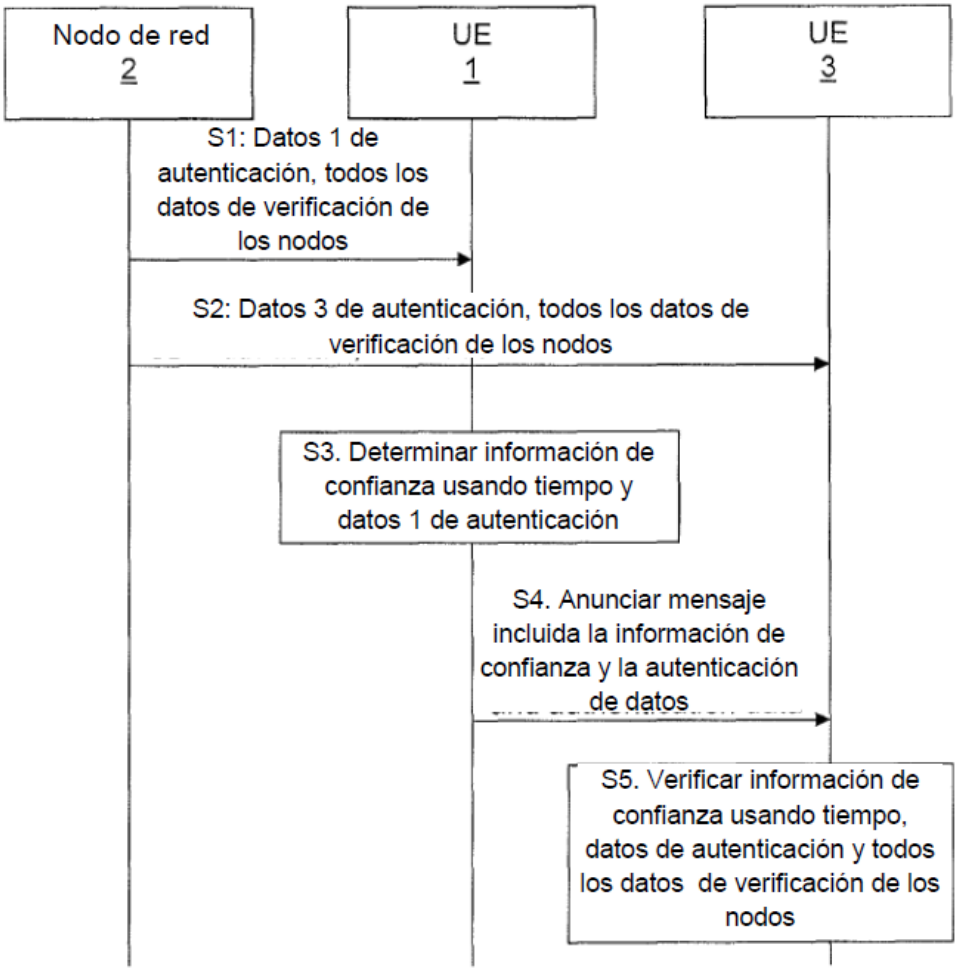
Nodo de red
2
UE
1
UE
3
S1: Datos 1 de autenticación, todos los datos de verificación de los nodos
S2: Datos 3 de autenticación, todos los datos de verificación de los nodos
S3. Determinar información de confianza usando tiempo y datos 1 de autenticación
S4. Anunciar mensaje incluida la información de confianza y la autenticación de datos
S5. Verificar información de confianza usando tiempo, datos de autenticación y todos los datos de verificación de los nodos

Figura 3

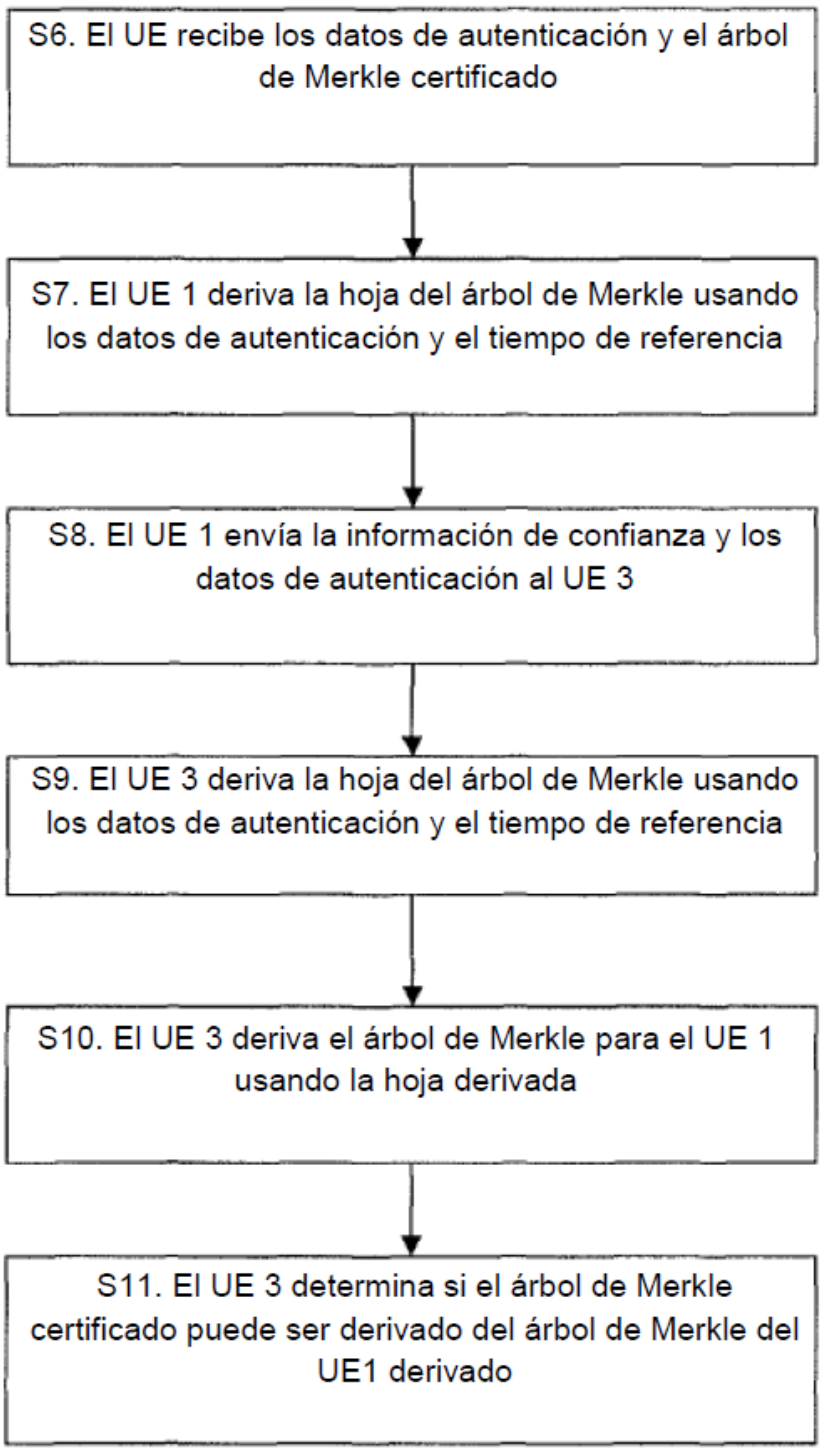
S6. El UE recibe los datos de autenticación y el árbol de Merkle certificado
S7. El UE 1 deriva la hoja del árbol de Merkle usando los datos de autenticación y el tiempo de referencia
S8. El UE 1 envía la información de confianza y los datos de autenticación al UE 3
S9. El UE 3 deriva la hoja del árbol de Merkle usando los datos de autenticación y el tiempo de referencia
S10. El UE 3 deriva el árbol de Merkle para el UE 1 usando la hoja derivada
S11. El UE 3 determina si el árbol de Merkle certificado puede ser derivado del árbol de Merkle del UE1 derivado

Figura 4

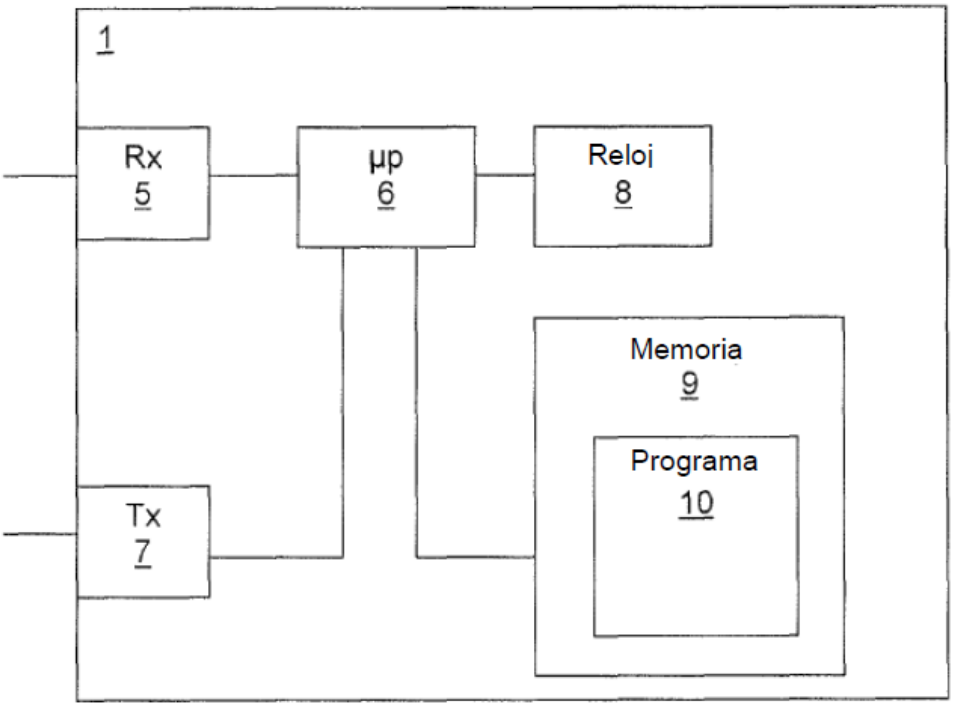

Figura 5

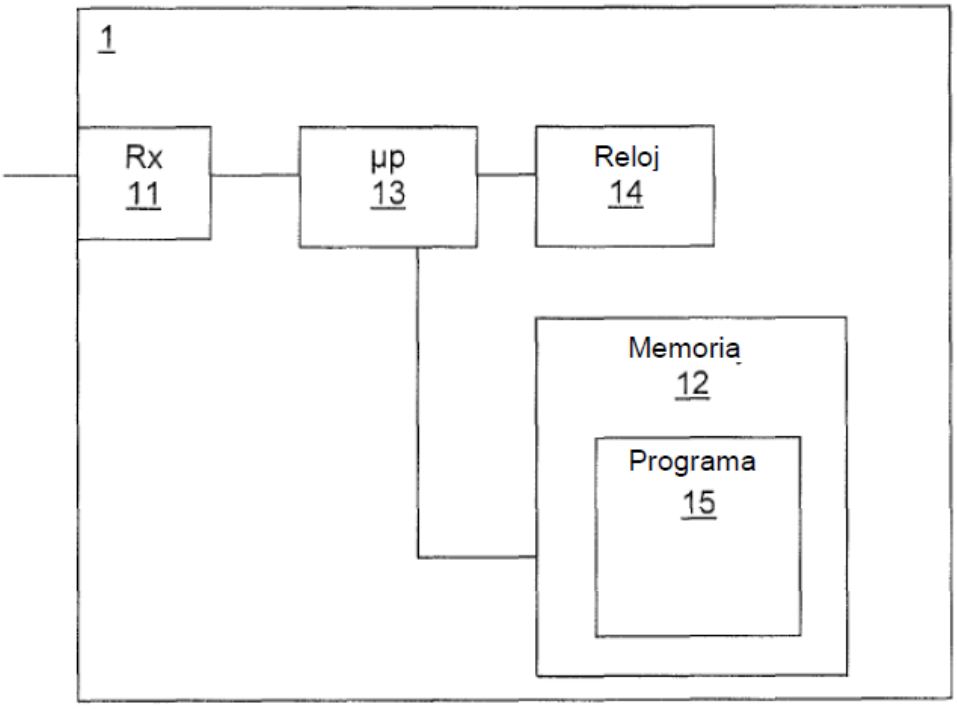

Figura 6

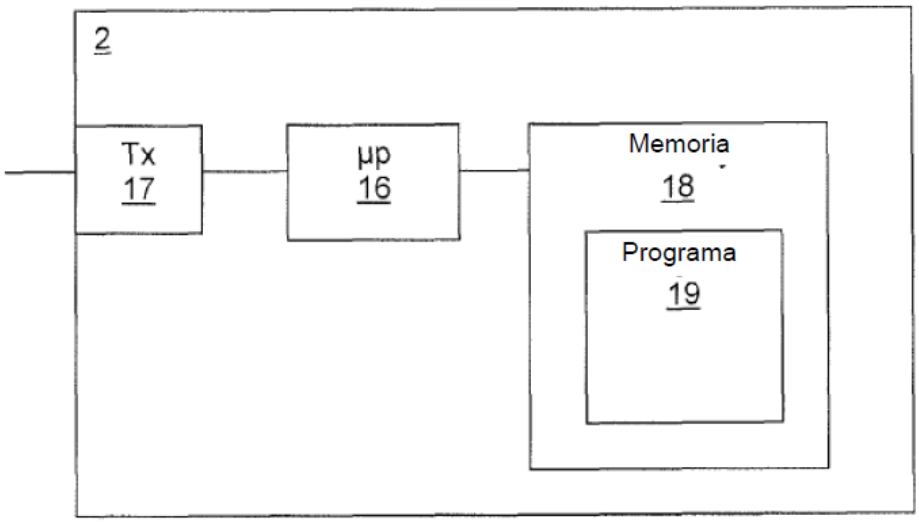

Figura 7