(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 537**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 12/56 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.03.2008 E 08736787 (6)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2012 EP 2127198**

(54) Título: **Protocolo de autenticación y cifrado en sistemas de comunicaciones inalámbricas**

(30) Prioridad:

28.03.2007 FI 20075201

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2013

(73) Titular/es:

TELIASONERA AB (100.0%)
Stureplan 8
106 63 Stockholm, SE

(72) Inventor/es:

KORHONEN, JOUNI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Protocolo de autenticación y cifrado en sistemas de comunicaciones inalámbricas

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un protocolo de autenticación y cifrado en un sistema de comunicaciones.

ANTECEDENTES DE LA INVENCIÓN

El protocolo de identidad del servidor (HIP) proporciona una solución para separar los roles de identificador y localizador en el punto extremo de las direcciones IP (protocolo de internet). La arquitectura del HIP introduce nuevos espacio de nombres, identidad del servidor (HI) basados en criptografía, y una nueva capa entre la capa de red y la capa de transporte. La nueva capa, que transporta la identidad del servidor, se denomina capa del servidor. El espacio de nombres de identidad del servidor se basa en claves públicas que de manera típica, pero no necesaria, se autogeneran.

La Internet actual tiene dos espacios de nombres globales, los nombres de dominio y las direcciones IP. Las direcciones IP se usan tanto como localizadores topológicos y como identidades de interfaz de red. Este rol doble de las direcciones IP limita la flexibilidad de la arquitectura de Internet y hace difícil la movilidad y la reenumeración de las direcciones IP. En particular, los protocolos de transporte, tal como UDP (protocolo de datagrama de usuario) o TCP (protocolo de control de transmisión), están unidos a las direcciones IP y se desconectan cuando cambian las direcciones. La arquitectura del protocolo de identidad del servidor define un nuevo espacio global de nombres de Internet. El espacio de nombres de identidad del servidor separa los roles de nombre y localizador en la actualidad cubiertos por las direcciones IP. De acuerdo con HIP, la capa de transporte usa identidades del servidor en lugar de direcciones IP como nombres en punto extremo. Al mismo tiempo, la capa de red usa direcciones IP como localizadores puros.

La capa de identidad del servidor se añade como una unión entre la capa de transporte y la capa de red de la pila del protocolo. Cada servidor habilitado con HIP tiene uno o más identificadores del servidor (HI). El identificador del servidor es una clave pública. El identificador del servidor se representa por un identificador de 128 bits de largo, una etiqueta de identidad del servidor (HIT). La etiqueta de identidad del servidor se construye aplicando una función hash criptográfica sobre una clave pública. En HIP, los zócalos se ligan a los HI en lugar de a las direcciones IP. Las direcciones IP se usan para enrutar paquetes. Un procedimiento de inicio de sesión en una red basado en HIP se describe en GB2424154.

El HIP permite movilidad, multiorientación de multidirecciones, resistencia y seguridad de extremo a extremo a ataques de denegación de servicio (DoS) en un sistema de comunicaciones. Por lo tanto, pudiera desearse usar HIP como un protocolo de gestión de claves y autenticación genérico común. Sin embargo, un problema asociado al mismo es que los sistemas actuales sólo permiten usar HIP para autenticar y cifrar el tráfico de conexiones punto a punto. Esto es porque en un sistema más grande, cada nodo de red debería conocer todas las etiquetas de identidad del servidor e identidades del servidor necesarias. La única solución disponible sería, por lo tanto, usar tablas estáticas almacenadas en los nodos de red con el objetivo de asociar las HIT a los dominios de seguridad correspondientes (REALM). Esto no sería muy práctico.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

Un objeto de la presente invención es por lo tanto proporcionar un método y un aparato para implementar el método a fin de resolver el problema anterior. El objeto de la invención se logra mediante un método, un sistema, autenticador y servidor que se caracterizan por lo que se establece en las reivindicaciones independientes. Las modalidades preferidas de la invención se describen en las reivindicaciones dependientes.

La invención se refiere a la autenticación de usuarios en una red de acceso inalámbrico. La invención además se refiere a utilizar el protocolo de identidad del servidor HIP. La red de acceso comprende un nodo autenticador que recibe un paquete de datos, que incluye una etiqueta de identidad del servidor de un terminal de usuario. Sobre la base de la etiqueta de identidad del servidor, el nodo autenticador solicita información sobre una red propia del terminal de usuario desde un servidor de nombres. Ya que el servidor de nombres proporciona información sobre la red propia del terminal de usuario, el autenticador es capaz de transmitir una solicitud de autenticación, que incluye la etiqueta de identidad del servidor, hacia un servidor de autenticación de la red propia. El servidor recibe la solicitud de autenticación, comprueba la etiqueta de identidad del servidor, y si la etiqueta de identidad del servidor puede admitirse por el servidor, se transmite una respuesta de autenticación hacia el nodo autenticador. Después, una etiqueta de identidad del servidor del nodo autenticador se proporciona hacia el terminal de usuario.

Una ventaja de la invención es que permite que el protocolo de identidad del servidor (HIP) se use para autenticar y cifrar otras conexiones además de las conexiones punto a punto. Esto permite que HIP se use como un protocolo de autenticación y gestión de claves común en una red de comunicaciones, por ejemplo, en una red inalámbrica de

área local WLAN. La invención permite el mapeo de una etiqueta iniciadora de identidad del servidor en la información a la que son capaces de responder las arquitecturas de red actuales.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En lo que sigue la invención se describirá con mayor detalle por medio de modalidades preferidas con referencia a los dibujos adjuntos, en los cuales:

La Figura 1 ilustra un sistema de comunicaciones de acuerdo con la presente solución;

La Figura 2 ilustra una señalización de acuerdo con la presente solución;

La Figura 3 es un diagrama de flujo que ilustra el funcionamiento de un autenticador de red de acuerdo con la presente solución;

La Figura 4 es un diagrama de flujo que ilustra el funcionamiento de un servidor de autenticación, autorización y estadísticas de acuerdo con la presente solución.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

En lo que sigue, las modalidades de la invención se describirán con referencia a un sistema de comunicaciones inalámbricas, tal como una WLAN. Esta invención, sin embargo, no pretende limitarse a estas modalidades. En consecuencia, la invención puede aplicarse a cualquier sistema de comunicaciones inalámbricas o móviles, tal como UMTS capaz de proporcionar un servicio de radio de paquetes conmutados. De manera especial las especificaciones de los sistemas de comunicaciones móviles WLAN y de tercera generación (3G) avanzan con rapidez. Esto puede requerir cambios adicionales a la invención. Por esta razón, la terminología y las expresiones usadas deberían interpretarse en su más amplio sentido dado que pretenden ilustrar la invención y no restringirla. El aspecto relevante de la invención es la funcionalidad en cuestión, no el elemento o equipo de la red donde se ejecuta.

Un identificador del servidor HI se refiere a una clave criptográfica. Este es una clave pública de un par de claves asimétricas. Un servidor tiene al menos una única identidad del servidor. La identidad del servidor, y el correspondiente identificador del servidor, pueden ser ya sea públicos (por ejemplo publicados en el DNS) o no publicados. Cuando se usa HIP el tráfico de carga útil real entre dos anfitriones de HIP se protege de manera típica utilizando un IP seguro (IPsec). Las identidades del servidor se usan para crear asociaciones de seguridad IPsec SA y para autenticar los anfitriones. La identidad del servidor permite separar las capas de interconexión de redes y de transporte. Esto permite una evolución independiente de las dos capas. Otra característica es la autenticación de servidor. Debido a que el identificador del servidor es una clave pública, puede usarse para la autenticación en protocolos de seguridad como IPsec.

Una etiqueta de identidad del servidor (HIT) es una representación de 128 bits para una identidad del servidor. Esta se crea tomando un hash criptográfico sobre el correspondiente identificador del servidor. En los paquetes de HIP, las HIT identifican el remitente y el destinatario de un paquete. Una HIT es única en todo el universo IP mientras esté en uso. En la arquitectura de HIP, los identificadores del servidor toman el rol de identificadores en punto extremo.

El protocolo de identidad del servidor HIP proporciona una unión de los protocolos de la capa de transporte, en el cual las asociaciones de la capa de transporte, es decir las conexiones TCP y las asociaciones UDP, ya no están unidas a las direcciones IP sino a las identidades del servidor.

Un puntero de autoridad de denominación (NAPTR) es un registro DNS, que soporta reescritura basada en expresiones regulares. Varios registros NAPTR pueden encadenarse juntos creando reglas de reescritura de URI. Un registro puede ir a través de cualquier número de reescrituras antes de alcanzar una condición terminal. Por ejemplo, después de traducir un número de teléfono +1 770 555 1212 en un URI 2.1.2.1.5.5.5.0.7.7.1.e164.arpa, éste se transforma usando reglas de reescritura que se encuentran en los registros NAPTR. Una configuración de unión para los registros devueltos de una consulta para 2.1.2.1.5.5.5.0.7.7.1.e164.arpa pudiera después aparecer como sigue:

$ORIGEN 2.1.2.1.5.5.5.0.7.7.1.e164.arpa.

EN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:información@pbx.ejemplo.com!i".

EN NAPTR 102 10 "u" "smtp+E2U" "!^.*$!mailto:información@ejemplo.com!i".

El mapeo de números de teléfono (ENUM) es una serie de protocolos para unificar el sistema de numeración de teléfonos E.164 con el sistema de direccionamiento de Internet DNS usando un método de búsqueda indirecta para obtener los registros NAPTR. Los registros se almacenan en una base de datos de DNS. ENUM se basa en un

sistema de servidores de nombres públicos que ofrece accesibilidad global. Por medio de ENUM, los usuarios finales y las compañías pueden ellos mismos gestionar su comunicación, y, por ejemplo, recibir llamadas telefónicas mediante Internet, las llamadas que se hacen con números de teléfono.

Un registro de recursos RR se refiere a un registro de recursos de DNS, que es una unidad de datos en el sistema de nombres de dominio, que define los atributos para un nombre de dominio. El atributo puede ser, por ejemplo, una dirección IP, una cadena de texto, o una ruta de correo.

La Figura 1 ilustra un sistema de comunicaciones S de acuerdo con una modalidad de la presente solución. La Figura 1 muestra una versión simplificada de la arquitectura de red, que ilustra solo componentes que son esenciales para la invención, aún cuando los expertos en la materia naturalmente conocen que un sistema de comunicaciones inalámbricas o móviles general comprende además otras funciones y estructuras, las cuales no tienen que describirse con más detalle en la presente.

En la Figura 1, el sistema de comunicaciones S comprende una red de acceso inalámbrico WLAN y un núcleo de red CN. La red de acceso WLAN es, por ejemplo, una red inalámbrica de área local, y comprende un autenticador de red HIP-R (es decir un contestador de HIP) con el cual puede comunicarse un terminal de usuario UE a través de un punto de acceso AP cuando el UE está en el área de cobertura de AP. El punto de acceso AP puede además referirse como una estación base. El terminal de usuario UE puede además referirse como un iniciador de HIP (HIP-I), y puede comprender cualquier dispositivo de usuario portátil inalámbrico, tal como una computadora portátil o una estación móvil, capaz de comunicarse con el AP. El núcleo de red CN ilustra una "red propia" del terminal de usuario UE, y comprende un servidor de autenticación, autorización y estadísticas AAAH con el cual puede comunicarse el contestador de HIP. El contestador de HIP puede además comunicarse con un servidor de nombres ENUM. Un enlace de radio entre el AP y el UE se implementa utilizando una tecnología de radio, tal como WLAN.

La Figura 2 ilustra la señalización de acuerdo con una modalidad de la presente solución. Primero, un primer paquete iniciador I1 que comprende una etiqueta de identidad del servidor HIT-I del UE iniciador de HIP se transmite 2-1 desde el terminal de usuario UE (es decir un iniciador de HIP) hacia un punto de acceso AP de la WLAN. El paquete I1 se reenvía 2-2 por el punto de acceso AP hacia un contestador de HIP HIP-R (es decir el autenticador de WLAN). Sobre la base de I1, el contestador de HIP solicita información sobre una red propia del terminal de usuario transmitiendo, en una solicitud de mapeo (solicitud de DNS) 2-3, la etiqueta de identidad del servidor HIT-I hacia un servidor de nombres global ENUM. En una respuesta de mapeo 2-4, la información sobre la red propia (por ejemplo la REALM) CN se transmite desde ENUM hacia HIP-R. Sobre la base de la respuesta de mapeo, una primera solicitud de autenticación 2-5 se transmite desde HIP-R hacia un servidor de autenticación, autorización y estadísticas AAAH de la red propia, la solicitud 2-5 que indica la HIT-I. La solicitud 2-5 puede además incluir una etiqueta de identidad del servidor del contestador de HIP, es decir el HIT-R. Cuando la primera solicitud de autenticación se recibe 2-6 en el AAAH, el AAAH se dispone para comprobar 2-6 si la HIT-I es válida o no. Si se encuentra que la HIT-I es válida, se transmite una demanda de autenticación 2-7 desde el AAAH hacia el HIP-R. Sobre la base de la demanda de autenticación, el HIP-R genera 2-8 un primer paquete contestador R1 y lo transmite 2-9, 2-10, a través del AP, hacia el terminal de usuario UE. El primer paquete contestador R1 puede incluir información sobre la etiqueta de identidad del servidor del contestador HIT-R. Después de recibir el mensaje 2-10 en el UE, el UE crea y transmite 2-11 un segundo paquete iniciador I2, a través del AP, hacia el HIP-R. Sobre la base de I2, una segunda solicitud de autenticación 2-13 se transmite desde el HIP-R hacia el AAAH, la solicitud 2-13 que indica HIT-I. La solicitud 2-13 puede además incluir la etiqueta de identidad del servidor del contestador HIT-R. Cuando la segunda solicitud de autenticación se recibe 2-14 en el AAAH, el AAAH se dispone para comprobar 2-14 si la HIT-I es válida o no. Si se encuentra que la HIT-I es válida, se transmite una respuesta de autenticación 2-15 desde el AAAH hacia el HIP-R. Sobre la base de la respuesta de autenticación, el HIP-R genera 2-16 un segundo paquete contestador R2 y lo transmite 2-17 hacia el AP. El segundo paquete contestador R2 incluye información sobre la etiqueta de identidad del servidor del contestador HIT-R. Sobre la base de R2, se derivan claves criptográficas de capa-2 (L2) en el AP en la etapa 2-18. En este punto, se ha negociado así una conexión entre el UE y el HIP-R. En el mensaje 2-19, el segundo paquete contestador R2 se transmite hacia el UE. Sobre la base de R2, se derivan las claves criptográficas de L2 en el UE en la etapa 2-20. Después de eso, se asegura la conexión 2-21 entre el UE y el HIP-R.

La Figura 3 ilustra el funcionamiento de un autenticador de red (es decir un contestador de HIP HIP-R) de acuerdo con una modalidad de la presente solución. En la etapa 3-1, un primer paquete iniciador I1 que comprende una etiqueta de identidad del servidor HIT-I del iniciador de HIP UE se recibe desde un punto de acceso AP de WLAN. Sobre la base de I1, el contestador de HIP solicita 3-2 información sobre una red propia del terminal de usuario UE transmitiendo, en una solicitud de mapeo (solicitud de DNS), la etiqueta de identidad del servidor HIT-I hacia un servidor de nombres global ENUM. Una respuesta de mapeo que incluye información sobre la red propia (por ejemplo la REALM) se recibe 3-3 desde ENUM. Sobre la base de la respuesta de mapeo, una primera solicitud de autenticación se transmite 3-4 hacia un servidor de autenticación, autorización y estadísticas AAAH de la red propia CN, la solicitud que indica HIT-I. La solicitud puede además incluir una etiqueta de identidad del servidor del contestador de HIP, es decir HIT-R. Después de eso, se recibe 3-5 una demanda de autenticación desde el AAAH. Sobre la base de la demanda de autenticación, el HIP-R genera 3-6 un primer paquete contestador R1 y lo transmite 3-7 hacia el AP. El primer paquete contestador R1 puede incluir información sobre la etiqueta de identidad del

servidor del contestador HIT-R. En la etapa 3-8, un segundo paquete iniciador I2 se recibe desde AP. Sobre la base de I2, una segunda solicitud de autenticación se transmite 3-9 desde el HIP-R hacia el AAAH, la solicitud que indica HIT-I. La solicitud puede además incluir la etiqueta de identidad del servidor del contestador HIT-R. Después de eso, se recibe 3-10 una respuesta de autenticación desde el AAAH. Sobre la base de la respuesta de autenticación, el HIP-R genera 3-11 un segundo paquete contestador R2 y lo transmite 3-12 hacia el AP. El segundo paquete contestador R2 incluye información sobre la etiqueta de identidad del servidor del contestador HIT-R.

La Figura 4 ilustra el funcionamiento de un servidor de autenticación, autorización y estadísticas AAAH de una red propia CN de un terminal de usuario UE, de acuerdo con una modalidad de la presente solución. Primero, una primera solicitud de autenticación se recibe desde el HIP-R, la solicitud que indica una etiqueta de identidad del servidor HIT-I del terminal de usuario. La solicitud puede además incluir una etiqueta de identidad del servidor HIT-R del contestador de HIP. Cuando la primera solicitud de autenticación se recibe en el AAAH, el AAAH se dispone para comprobar 4-2 si la HIT-I es válida o no. Si se encuentra que la HIT-I es válida, se transmite 4-3 una demanda de autenticación desde el AAAH hacia el HIP-R. Si se encuentra que la HIT-I no es válida, el proceso puede terminar o puede transmitirse un mensaje (no mostrado) hacia el HIP-R, informando al HIP-R de una HIT-I inválida. En la etapa 4-4, una segunda solicitud de autenticación se recibe desde el HIP-R, la solicitud que indica la HIT-I. La solicitud puede además incluir la etiqueta de identidad del servidor del contestador HIT-R. Cuando la segunda solicitud de autenticación se recibe 4-4 en el AAAH, el AAAH se dispone para comprobar 4-5 si la HIT-I es válida o no. Si se encuentra que la HIT-I es válida, se transmite 4-6 una respuesta de autenticación desde el AAAH hacia el HIP-R.

La presente invención permite que un nodo de red (por ejemplo un contestador de HIP) adquiera información sobre las etiquetas de identidad del servidor y las identidades del servidor, sin que el nodo de red tenga que mantener información sobre todas las etiquetas de identidad del servidor y/o las identidades del servidor. La presente invención permite así una asociación dinámica de las etiquetas de identidad del servidor (HIT) a las REALM correspondientes utilizando el HIP. Por medio del dominio de seguridad (REALM), puede localizarse una red propia de un terminal del usuario que llama, dado que la red propia es capaz de reconocer la etiqueta de identidad del servidor y el identificador del servidor usados. Por medio de la invención, un contestador de HIP es capaz de asociar la etiqueta de identidad del servidor a una REALM. La información sobre la etiqueta de identidad del servidor y la identidad del servidor del terminal de usuario se almacena en la red propia. Por ejemplo, si el HIP se usa en una WLAN para sustituir un protocolo 802.1X, el contestador de HIP tiene que ser capaz de encontrar, sobre la base de la HIT del contestador, la red propia del iniciador de HIP (es decir el cliente) y el servidor AAA desde donde el contestador de HIP puede recuperar la información necesaria para realizar un intercambio de base de acuerdo con el protocolo HIP. La HIT puede ser un identificador de 128 bits no enrutado como el Ipv6 de acuerdo con las definiciones Orchid. La presente invención define una solución que se puede escalar para un ambiente itinerante para asociar la HIT a la REALM y de esta manera a cualquier servidor/servicio. En la presente solución, los roles de HIP se mapean encima de la arquitectura de la WLAN de manera que un iniciador de HIP se corresponde con una estación de WLAN/solicitante, una estación base de WLAN se corresponde con cualquier punto de acceso de paso a través de la WLAN, un contestador de HIP se corresponde con un autenticador de WLAN y un AAA (autenticación, autorización y estadística) se corresponde, por ejemplo, con un servidor AAA&EAP (protocolo de autenticación extensible).

La idea de la invención es proporcionar una configuración de contestador de HIP dinámica para asociar la HIT a la REALM. En la invención, en relación con un paquete I1, el contestador HIP es capaz de encontrar la REALM correcta, con el objetivo de encontrar el AAAH. En lo que sigue, la REALM se representa por "@aaah". En la invención, el contestador de HIP utiliza DNS. Cada HIT se provee en el ENUM-DNS, y la asociación HIT->REALM se realiza por medio de una consulta de ENUM-DNS. La consulta devuelve un NAPTR-RR con un indicador terminal "s" y una dirección por medio de la cual un SRV-RR puede interrogarse con el objetivo de encontrar un AAAH. Un ejemplo de una solución de NAPTR puede ser como sigue:

$ORIGEN 0.1.2.3.4.5.6.7.8.9.0.1.2.3.4.5.6.7.8.9.0.a.b.c.d.e.f.0.1.2.3.4.5.e164.arpa.						
;;	orden	pref	indicadores	servicio	expreg	sustituto
EN NAPTR	100	10	"s"	"AAA+D2T"	""	aaa.operador.com.

El ejemplo anterior define los siguientes aspectos para la HIT 0x543210fedcba98765432109876543210: se interroga SRV-RR en el dominio aaa.operador.com, se solicita el servidor AAA, el servicio está sobre diameter-TCP.

Sin embargo, el hecho de que el dominio de nivel superior (TLD) .e164.arpa. ya está en uso puede provocar colisiones en el sistema. Por lo tanto, puede usarse un dominio de nivel superior (TLD) diferente a e164.arpa. Por ejemplo, pudiera usarse un TLD ficticio de .hit.arpa.

En otro ejemplo, el sistema se configura para utilizar el TLD existente .e164.arpa. de manera que sea compatible en

la dirección contraria. Esto requiere que, para el HIP, se reserve un "código de país" propio a partir del espacio E.164. El código de país pudiera ser por ejemplo +668. Así, con el TLD .e164.arpa., se obtiene un TLD de .8.6.6.e164.arpa. reservado para el HIP.
El NAPTR-ORIGEN pudiera además ser de un tipo diferente del usado por ENUM. El servicio de NAPTR pudiera además ser diferente de "AAA+D2T" y "AAA+D2S" definidos por la RFC3588 del protocolo diameter. Pudiera ser, por ejemplo, "AAA+R2T" y "AAA+R2S", si se desea usar un protocolo RADIUS en lugar de diameter.

La invención mejora el HIP introduciendo una posibilidad para comprobar la información sobre un usuario. La idea es comprobar si un usuario definido por una etiqueta de identidad del servidor existe en realidad en el sistema, y/o si el usuario tiene un permiso para usar el servicio y/o la red en cuestión. Aquí se asume que la propia red de acceso WLAN es fiable. La invención permite, por ejemplo, a los operadores de red comprobar la seguridad de los datos de sus clientes, usando el HIP. Esto permite que los puntos de extremo intercambien información sobre sus etiquetas de identidad del servidor con el objetivo de permitir la comunicación fiable de datos entre ellos.

De acuerdo con una modalidad, la presente solución no se restringe al uso del HIP, sino también pueden usarse otras tecnologías en lugar o además del HIP.

De acuerdo con una modalidad, la solicitud de mapeo comprende una solicitud de mapeo de números de teléfono - servidor de nombres de dominio ENUM-DNS relacionada con un dominio de nivel superior creado o con un código de país E.164 específico del HIP reservado para el HIP.

Los artículos y etapas mostrados en las Figuras 2, 3 y 4 están simplificados, y sólo ayudan a describir la idea de la invención. Otros artículos pueden usarse y/u otras funciones pueden llevarse a cabo entre las etapas. Los artículos sólo sirven como ejemplos y pueden sólo contener algo de la información antes mencionada. Los artículos pueden además incluir otra información, y los títulos pueden desviarse de los antes dados. En lugar de o además de un autenticador de red o un servidor de autenticación, autorización y estadísticas, las operaciones antes descritas pueden realizarse en cualquier otro elemento de un sistema de comunicaciones.

Además de los medios del arte anterior, un sistema, redes o nodos de red que implementan la funcionalidad de la invención comprenden medios para procesar la información con relación a la autenticación y cifrado de la manera antes descrita. Los nodos de red y terminales de usuario existentes comprenden procesadores y memoria que pueden utilizarse en las operaciones de la invención. Cualesquiera cambios necesarios para implementar la invención pueden llevarse a cabo usando suplementos o actualizaciones de rutinas de software y/o rutinas incluidas en circuitos integrados de aplicación específica (ASIC) y/o circuitos programables, tales como EPLD (dispositivo lógico programable de manera eléctrica) o FPGA (disposición de puertas programables en campo).

Será obvio para un experto en la materia que, a medida que la tecnología avance, el concepto de la invención puede implementarse de varias maneras. La invención y sus modalidades no se limitan a los ejemplos antes descritos sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para autenticar un terminal de usuario (UE) en un sistema de comunicaciones (S), el sistema (S) que comprende un autenticador de red (HIP-R) de una red de acceso inalámbrico (WLAN), en donde

el autenticador de red (HIP-R) recibe al menos un paquete iniciador (2-2, 2-12) transmitido por el terminal de usuario (UE) a través de un punto de acceso (AP), el paquete que incluye una etiqueta de identidad del servidor del terminal de usuario (UE) y **caracterizado por** las etapas siguientes:

transmitir, sobre la base del paquete iniciador, una solicitud de mapeo (2-3) desde el autenticador de red (HIP-R) hacia un servidor de nombres (ENUM);

recibir, en el autenticador de red (HIP-R), una respuesta de mapeo (2-4) desde el servidor de nombres (ENUM), la respuesta de mapeo (2-4) que incluye información sobre un servidor de red propia (AAAH) del terminal de usuario (UE);

transmitir, desde el autenticador de red (HIP-R) hacia el servidor de red propia (AAAH), una solicitud de autenticación (2-5, 2-13) sobre la base de la respuesta de mapeo (2-4), la solicitud de autenticación (2-5, 2-13) que además indica la etiqueta de identidad del servidor del terminal de usuario (UE); y

comprobar (2-6, 2-14), en el servidor de red propia (AAAH), la etiqueta de identidad del servidor del terminal de usuario (UE);
en donde si la etiqueta de identidad del servidor del terminal de usuario (UE) es admisible para el servidor de red propia (AAAH), el método comprende

transmitir una respuesta de autenticación (2-7, 2-15) desde el servidor de red propia (AAAH) hacia el autenticador de red (HIP-R) generar (2-8, 2-16), en el autenticador de red (HIP-R), al menos un paquete contestador sobre la base de la respuesta de autenticación (2-7, 2-15); y

transmitir, hacia el terminal de usuario (UE), el al menos un paquete contestador (2-10, 2-19) que incluye una etiqueta de identidad del servidor del autenticador de red (HIP-R).

2. Un método de acuerdo con la reivindicación 1, **caracterizado por** usar la etiqueta de identidad del servidor del terminal de usuario (UE) y la etiqueta de identidad del servidor del autenticador de red (HIP-R) para autenticar el terminal de usuario (UE).

3. Un método de acuerdo con la reivindicación 1 ó 2, **caracterizado por** utilizar un protocolo HIP para autenticar el terminal de usuario (UE) en una red inalámbrica de área local WLAN.

4. Un método de acuerdo con la reivindicación 1, 2 ó 3, **caracterizado porque** el protocolo de identidad del servidor HIP se aplica entre el terminal de usuario (UE) y el autenticador de red (HIP-R).

5. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** el protocolo de autenticación, autorización y estadística AAA se aplica entre el autenticador de red (HIP-R) y el servidor de red propia (AAAH).

6. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 5, **caracterizado por** incluir un contestador de HIT en el autenticador de red (HIP-R) y/o un iniciador de HIT en el terminal de usuario (UE).

7. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 6, **caracterizado por** la solicitud de mapeo (2-3) que comprende una solicitud de mapeo de números de teléfono - servidor de nombres de dominio ENUM-DNS relacionada con un dominio de nivel superior creado o con un código de país E.164 específico de HIP reservado para el HIP.

8. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 6, **caracterizado por** la solicitud de mapeo (2-3) que incluye una solicitud de registro de recursos de servidor SRV-RR.

9. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 8, **caracterizado por** la respuesta de mapeo (2-4) que incluye un puntero de autoridad de denominación NAPTR.

10. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 9, **caracterizado porque** comprende asociar una etiqueta de identidad del servidor HIT del terminal de usuario (UE) a un dominio de seguridad REALM para encontrar un servidor de autenticación (AAAH) de la red propia (CN) del terminal de usuario (UE).

11. Un sistema de comunicaciones (S) que comprende

un terminal de usuario (UE),

un autenticador de red (HIP-R) de una red de acceso inalámbrico (WLAN), y

un servidor de red propia (AAAH) del terminal de usuario (UE),

en donde el sistema (S) se configura para

transmitir, desde el terminal de usuario (UE) hacia el autenticador de red (HIP-R), al menos un paquete iniciador que incluye una etiqueta de identidad del servidor del terminal de usuario (UE) y **caracterizado porque** se configura para:

transmitir, sobre la base de un primer paquete iniciador transmitido por el terminal de usuario (UE), una solicitud de mapeo desde el autenticador de red (HIP-R) hacia un servidor de nombres (ENUM);

recibir, en el autenticador de red (HIP-R), una respuesta de mapeo desde el servidor de nombres (ENUM), la respuesta de mapeo que incluye información sobre el servidor de red propia (AAAH) del terminal de usuario (UE);

transmitir, desde el autenticador de red (HIP-R) hacia el servidor de red propia (AAAH), al menos una solicitud de autenticación sobre la base de dicha información, la solicitud de autenticación que indica la etiqueta de identidad del servidor del terminal de usuario (UE); y

comprobar, en el servidor de red propia (AAAH), la etiqueta de identidad del servidor del terminal de usuario (UE);

en donde si la etiqueta de identidad del servidor es admisible para el servidor de red propia (AAAH), el sistema (S) se configura para transmitir al menos una respuesta de autenticación desde el servidor de red propia (AAAH) hacia el autenticador de red (HIP-R);

generar, en el autenticador de red (HIP-R), al menos un paquete contestador sobre la base de la respuesta de autenticación, el paquete que incluye una etiqueta de identidad del servidor del autenticador de red (HIP-R); y

transmitir, desde el autenticador de red (HIP-R) hacia el terminal de usuario (UE), el al menos un paquete contestador.

12. Un sistema de comunicaciones (S) de acuerdo con la reivindicación 11, **caracterizado porque** se dispone para usar la etiqueta de identidad del servidor del terminal de usuario (UE) y la etiqueta de identidad del servidor del autenticador de red (HIP-R) para autenticar el terminal de usuario (UE).

13. Un sistema de comunicaciones (S) de acuerdo con la reivindicación 11 ó 12, **caracterizado porque** se dispone para asociar una etiqueta de identidad del servidor HIT a un dominio de seguridad REALM para encontrar un servidor de autenticación (AAAH) de la red propia (CN) del terminal de usuario (UE).

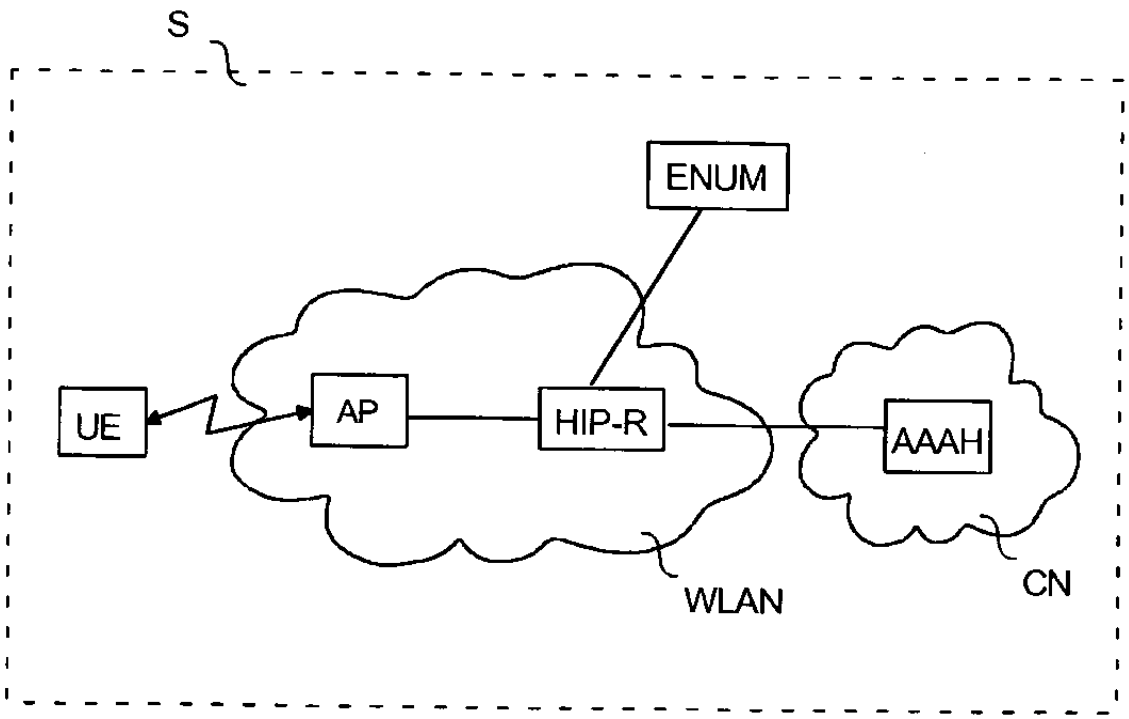

Fig. 1

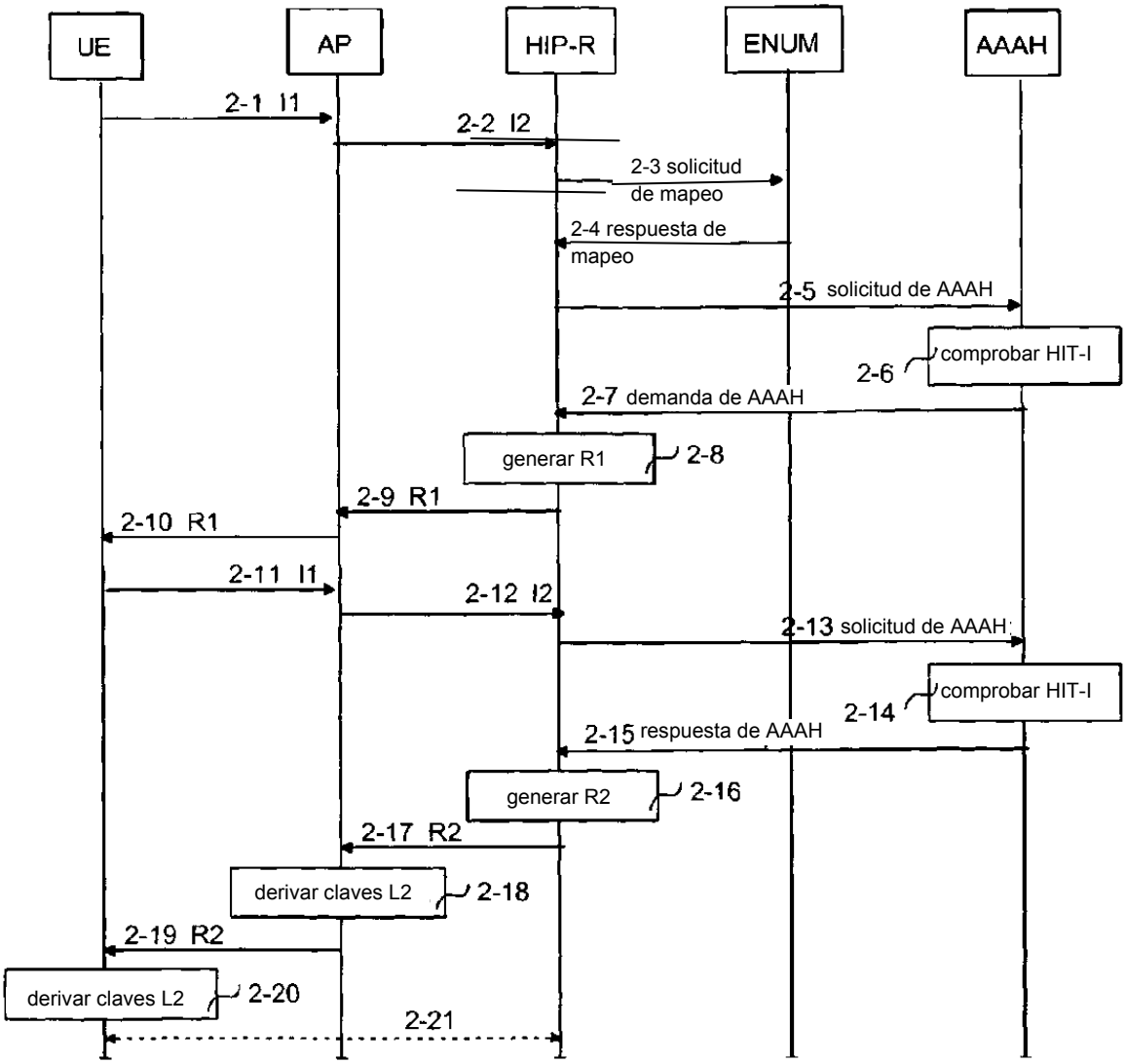
UE
AP
HIP-R
ENUM
AAAH
2-1 I1
2-2 I2
2-3 solicitud de mapeo
2-4 respuesta de mapeo
2-5 solicitud de AAAH
2-6
comprobar HIT-I
2-7 demanda de AAAH
generar R1
2-8
2-9 R1
2-10 R1
2-11 I1
2-12 I2
2-13 solicitud de AAAH
2-14
comprobar HIT-I
2-15 respuesta de AAAH
generar R2
2-16
2-17 R2
derivar claves L2
2-18
2-19 R2
derivar claves L2
2-20
2-21

Fig. 2

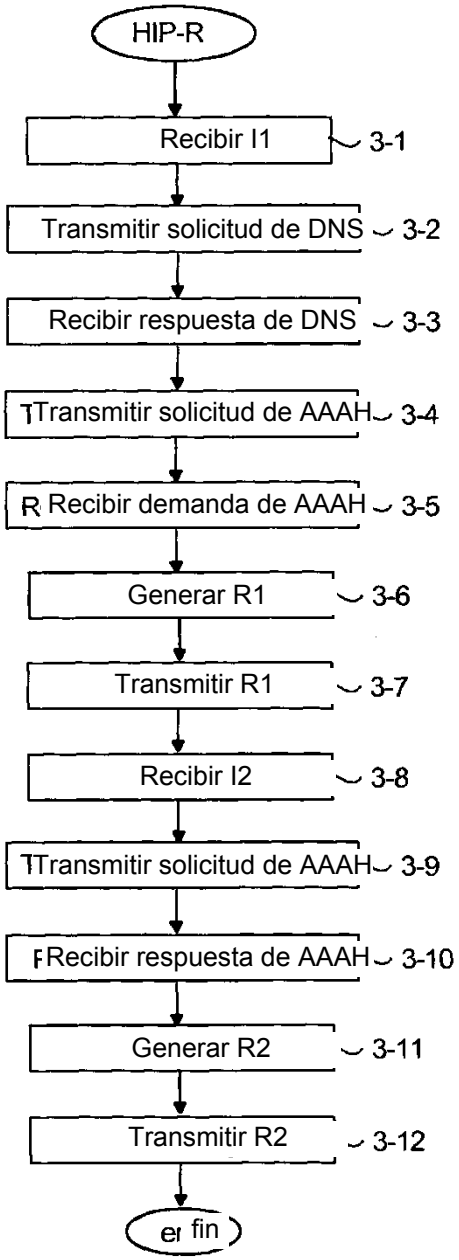
HIP-R
Recibir I1
3-1
Transmitir solicitud de DNS
3-2
Recibir respuesta de DNS
3-3
Transmitir solicitud de AAAH
3-4
Recibir demanda de AAAH
3-5
Generar R1
3-6
Transmitir R1
3-7
Recibir I2
3-8
Transmitir solicitud de AAAH
3-9
Recibir respuesta de AAAH
3-10
Generar R2
3-11
Transmitir R2
3-12
fin

Fig. 3

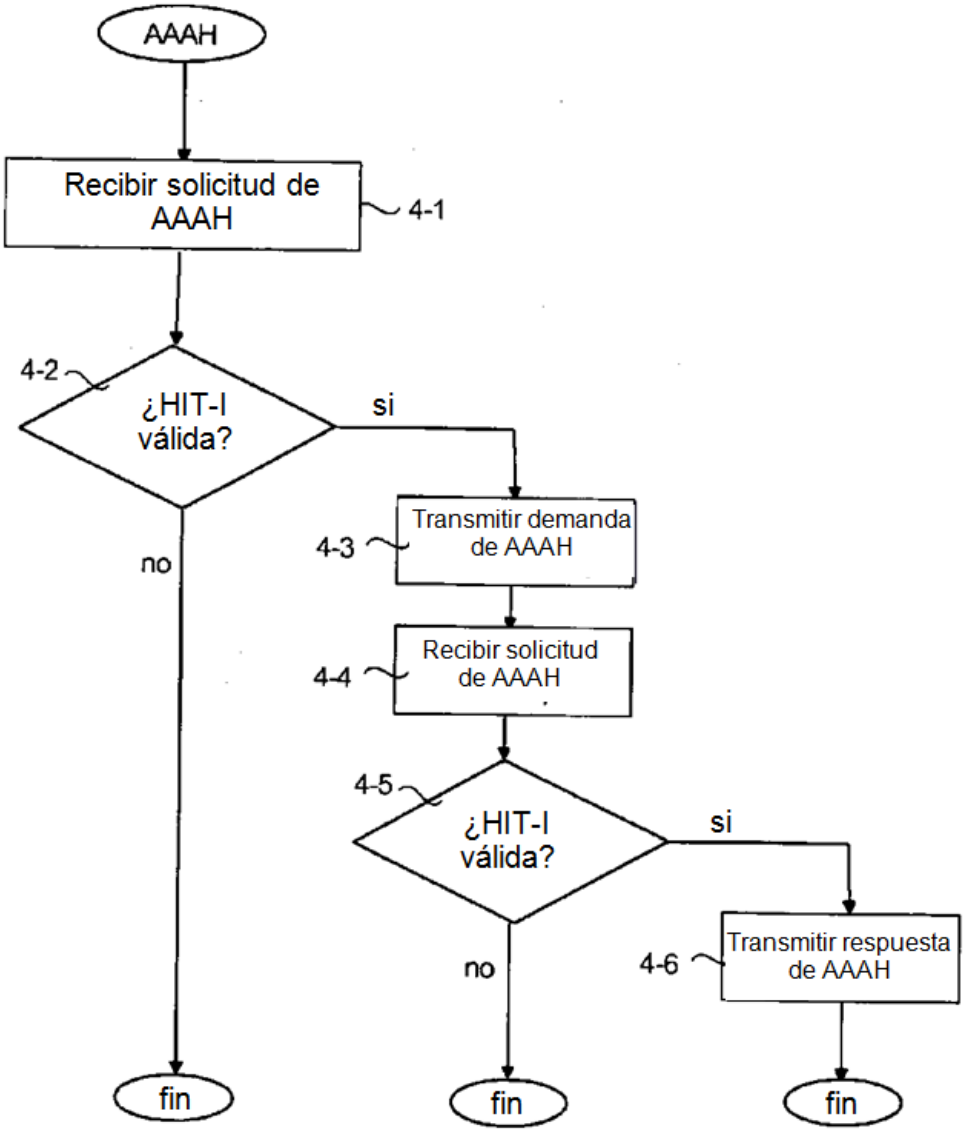
AAAH
Recibir solicitud de AAAH
4-1
4-2
¿HIT-I válida?
si
no
Transmitir demanda de AAAH
4-3
Recibir solicitud de AAAH
4-4
4-5
¿HIT-I válida?
si
no
Transmitir respuesta de AAAH
4-6
fin
fin
fin

Fig. 4