(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 546**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 29/14 (2006.01)
H04L 29/12 (2006.01)
H04W 12/10 (2009.01)
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.03.2010 E 16173001 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 3086532**

(54) Título: **Sistema y método para determinar la confianza para mensajes de SIP**

(30) Prioridad:

13.04.2009 US 168798 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2020

(73) Titular/es:

BLACKBERRY LIMITED (100.0%)
2200 University Avenue East
Waterloo, ON N2K 0A7, CA

(72) Inventor/es:

BAKKER, JAN HENDRIK LUCAS;
BUCKLEY, ADRIAN y
ALLEN, ANDREW

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema y método para determinar la confianza para mensajes de SIP

Antecedentes

El Subsistema Multimedia del IP (Protocolo de Internet) (IMS) es una arquitectura estandarizada para proporcionar servicios multimedia y llamadas de voz sobre IP para tanto agentes de usuarios (UA) móviles como fijos. El Protocolo de Inicio de Sesión (SIP) ha sido estandarizado y regido principalmente por el Grupo de Trabajo de Ingeniería de Internet (IETF) como un protocolo de señalización para crear, modificar y finalizar llamadas o sesiones basadas en IMS.

Como se utiliza en este documento, los términos “agente de usuario” y “UA” se pueden referir en algunos casos a dispositivos móviles tales como teléfonos móviles, asistentes digitales personales, ordenadores de mano o portátiles, y dispositivos similares que tienen capacidades de telecomunicaciones. Dicha UA podría ser parte de un UE (Equipo de Usuario). Un UE puede tener múltiples UA. Un UE puede tener un módulo de memoria extraíble asociado, tal como, pero no limitado a, una Tarjeta de Circuito Integrado Universal (UICC) que incluye una aplicación de Módulo de Identidad de Suscriptor (SIM), una aplicación del Módulo de Identidad del Suscriptor Universal (USIM), una aplicación del Módulo de Identidad de Servicios Multimedia de IP (ISIM), o una aplicación de Módulo de Identidad de Usuario Extraíble (R-UIM), etc. Ejemplos de dichos módulos pueden incluir, entre otros, Tarjeta de PC, CompactFlash I, CompactFlash II, SmartMedia, Tarjeta de Memoria, Tarjeta de Memoria Duo, Tarjeta de Memoria PRO Duo, Tarjeta de Memoria PRO-HG Duo, Tarjeta de Memoria Micro M2, Tarjeta Multimedia, Tarjeta Multimedia de Tamaño Reducido, Tarjeta MMCmicro, tarjeta de Seguro Digital, SxS, Almacenamiento Flash Universal, tarjeta miniSD, tarjeta microSD, Tarjeta xD-Picture, Memoria Inteligente, Módulo de Flash en Serie, tarjeta µ y Tarjeta NT. Cuando la información se almacena en un módulo de memoria extraíble, los contenidos del módulo se pueden visualizar en el UE.

Alternativamente, dicho UA podría consistir en el dispositivo mismo sin dicho módulo. En otros casos, el término “UA” se podría referir a dispositivos que tienen capacidades similares pero que no son transportables, tales como teléfonos de línea fija, ordenadores de escritorio, decodificadores o nodos de red. Cuando uno o más UA forman parte de un nodo de red, el nodo de red podría actuar a nombre de otra función, tal como un UA o un dispositivo de línea fija, y simular o emular el UA o dispositivo de línea fija. Por ejemplo, para algunos UA, el cliente de SIP de IMS que normalmente residiría en el dispositivo realmente reside en la red y transmite la información del mensaje de SIP al dispositivo utilizando protocolos optimizados. En otras palabras, algunas funciones que tradicionalmente se llevaban a cabo por un UA se pueden distribuir en forma de un UA remoto, en el que el UA remoto representa al UA en la red. El término “UA” también puede referirse a cualquier componente de hardware o software que pueda terminar una sesión de comunicación que podría incluir, pero no se limita a, una sesión de SIP. También, los términos “agente de usuario”, “UA”, “equipo de usuario”, “UE” y “nodo” se pueden utilizar como sinónimos en el presente documento. También, los términos “encabezado” y “campo de encabezado” se pueden utilizar como sinónimos en este documento. También, un mensaje de SIP es una solicitud de SIP o una respuesta de SIP.

Un UA se puede conectar a una red basada en SIP que incluye una pluralidad de otros componentes tales como una P-CSCF (Función de Control de Sesión de Llamada de Proxy), una S-CSCF (CSCF de Servicio), una IBCF (Función de Control en la Frontera de Interconexión)), un Servidor de Aplicaciones (AS) y otros componentes, cualquiera de los cuales se podría denominar nodos de red. Puede existir una relación de confianza entre los nodos en una red de SIP. Es decir, un grupo de nodos dentro de una red puede considerar todos los mensajes recibidos de otros nodos en el grupo como legítimos. Se puede decir que dicho grupo forma un dominio de confianza o una o más redes de confianza. IETF RFC 3325 titulado “Extensiones privadas al Protocolo de Inicio de Sesión (SIP) para la Asserted-Identity dentro de las Redes de Confianza” discute este tema más a fondo.

Los documentos WO 2009/033504 A1 y US 2009/077616 A1 divulgan un método para manejar la confianza en una red de Subsistema Multimedia de IP. Un nodo en la red del Subsistema Multimedia de IP recibe un mensaje del Protocolo de Inicio de Sesión desde un nodo remoto. El mensaje incluye un indicador que indica el nivel de confianza de una comunicación enviada desde el nodo remoto hasta el nodo del Subsistema Multimedia de IP. Teniendo como base el indicador, el nodo aplica una política de seguridad al mensaje.

El documento US 2005/068935 A1 divulga un método de comunicación entre una parte que llama en una primera red y una parte llamada en una segunda red. El método comprende determinar en la primera red una dirección asociada con la parte llamada. El método también comprende determinar, en función de la dirección, si la parte llamada está en una red confiable, y controlar la comunicación entre la parte llamada y la parte que llama en función de si la parte llamada está en una red confiable.

El documento WO 2008/049455 A1 divulga un método para transportar información de estado de conectividad de señalización en un Subsistema multimedia de IP.

Breve descripción de los dibujos

Para una comprensión más completa de esta divulgación, se hace referencia ahora a la siguiente breve descripción, tomada en relación con los dibujos acompañantes y la descripción detallada, en la que los números de referencia similares representan partes similares.

La Figura 1 es un diagrama de un sistema de comunicaciones que incluye una pluralidad de nodos de red de acuerdo con una realización de la divulgación.

La Figura 2 es un diagrama de flujo de llamadas que ilustra un método para que un UA recupere información de confianza de acuerdo con una realización de la divulgación.

La Figura 3 ilustra un método para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS de acuerdo con una realización de la divulgación.

La Figura 4 ilustra un método para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS de acuerdo con una realización alternativa de la divulgación.

La Figura 5 ilustra un procesador y componentes relacionados adecuados para implementar las diversas realizaciones de la presente divulgación.

Descripción detallada

La invención se define en las reivindicaciones independientes. Las realizaciones preferidas se definen en las reivindicaciones dependientes. Se debe entender desde el principio que, aunque a continuación se proporcionan implementaciones ilustrativas de una o más realizaciones de la presente divulgación, los sistemas y/o métodos divulgados se pueden implementar utilizando cualquier número de técnicas, ya sean actualmente conocidas o existentes. La divulgación no debe limitarse de ninguna manera a las implementaciones ilustrativas, dibujos y técnicas ilustradas a continuación, que incluyen los diseños e implementaciones de ejemplo ilustrados y descritos en este documento, sino que puede modificarse dentro del alcance de las reivindicaciones adjuntas junto con su alcance completo de equivalentes.

Un nodo dentro de un dominio de confianza en una red de IMS podría recibir un mensaje de un nodo fuera del dominio de confianza. En algunos casos, dicho mensaje podría dirigir al nodo en el dominio de confianza a realizar una o más acciones que pueden no ser deseables para ese nodo. Por ejemplo, un mensaje se puede enviar maliciosamente a una pluralidad de UA informando falsamente a los UA que se ha producido un Tiempo de Espera del Servidor. Una UA que reciba dicho mensaje podría intentar volver a registrarse con un registrador de SIP, aunque en realidad no sea necesario volver a registrarse. Si una gran cantidad de UA intentan volver a registrarse, el registrador podría sobrecargarse y fallar. Esto podría ocasionar problemas importantes en la red, ya que otras UA podrían no poder registrarse.

En una realización, un mensaje enviado a un nodo de red desde fuera del dominio de confianza del nodo de red puede incluir un indicador de confianza que indica la confiabilidad del mensaje. Un indicador de confianza también puede ser una credencial de confianza, una guía de confianza o un indicador de confianza. Los indicadores de confianza pueden ser de dos tipos. La presencia de un tipo de indicador de confianza en un mensaje indica que se puede confiar en el nodo de red que envió el mensaje. El destinatario de un mensaje que contiene dicho indicador de confianza no necesita realizar ninguna verificación del indicador de confianza. Cuando el otro tipo de indicador de confianza está presente en un mensaje, el destinatario del mensaje compara el indicador de confianza con la información/base de datos de confianza almacenada internamente. Si el indicador de confianza coincide con la información de confianza almacenada, el indicador de confianza se verifica y el destinatario/receptor sabe que se puede confiar en el nodo de red que envió el mensaje.

Si el primer tipo de indicador de confianza está presente en un mensaje o si el segundo tipo está presente y se verifica, el nodo de red que recibe el mensaje realiza las acciones que normalmente están asociadas con la recepción del mensaje o el mensaje y su contenido. Si no hay un indicador de confianza presente o si el indicador de confianza no está verificado, el nodo de red que recibe el mensaje podría no realizar una o más de las acciones que normalmente están asociadas con la recepción del mensaje o el mensaje y su contenido.

En una realización, el nodo de red que recibe el mensaje es un UA que mantiene información de confianza relacionada con los nodos de red fuera del dominio de confianza del UA. Al recibir un mensaje desde fuera de su dominio de confianza, el UA puede comparar el indicador de confianza que podría incluirse con el mensaje con la información de confianza que mantiene el UA. Si el UA verifica que el indicador de confianza coincide con la información de confianza que mantiene, el UA realiza las acciones que normalmente están asociadas con la recepción del mensaje o el mensaje y su contenido. Si el UA no puede verificar que el indicador de confianza coincida con la información de confianza que mantiene, el UA no realiza al menos una acción que normalmente está asociada con la recepción del mensaje o el mensaje y su contenido.

Estas realizaciones se ilustran en la Figura 1, en el que un UA 110 es capaz de comunicarse con un nodo B 130 de red, que es capaz de comunicarse con un nodo A 120 de red. El UA 110, el nodo A 120 de red y el nodo B 130 de red podrían ser componentes en una red basada en IMS, y el nodo A 120 de red y el nodo B 130 de red podrían

estar fuera del dominio de confianza de la UA. Si bien solo se muestran otros dos nodos de red, otros números podrían estar presentes. En esta realización, el nodo A 120 de red genera un mensaje A 140 e incluye un indicador A 145 de confianza en el mensaje A 140. El nodo 120 de red luego envía el mensaje A 140 al nodo B 130 de red. La recepción del mensaje A 140 provoca que el nodo B 130 de red genere un mensaje B 150 que contiene un indicador B 155 de confianza, y luego se envía el mensaje B 150 al UA 110. El mensaje A 140 puede o no ser el mismo que el mensaje B 150, y el indicador A 145 de confianza puede o no ser lo mismo que el indicador B 155 de confianza. En otras palabras, el nodo B 130 de red podría simplemente pasar el indicador A 145 de confianza que se recibe del nodo A 120 de red, o el nodo B 130 de red podría generar un nuevo indicador B 155 de confianza basado en el indicador A 145 de confianza u otra información recibida del nodo A 120 de red y/u otros nodos de red.

En otras realizaciones, el nodo A 120 de red no incluye el indicador A 145 de confianza en el mensaje A 140. En cambio, el nodo B 130 de red genera el indicador B 155 de confianza sin tener en cuenta ninguna información incluida en el mensaje A 140, y la red el nodo B 130 incluye el indicador B 155 de confianza en el mensaje B 150 enviado al UA 110. En otras palabras, el indicador de confianza que recibe el UA 110 podría haber sido generado por el nodo de red con el que el UA 110 está en comunicación directa, podría haber sido generado por otro nodo de red y luego transmitido sin modificación por el nodo de red con el que el UA 110 está en comunicación directa, o podría haber sido generado por otro nodo de red y luego transmitido con modificación por el nodo de red en el que el UA 110 está en comunicación directa.

En algunas realizaciones, al recibir un mensaje que contiene un indicador de confianza, el UA 110 realiza las acciones que están normalmente asociadas con la recepción del mensaje. En otras realizaciones, al recibir un mensaje que contiene un indicador de confianza, el UA 110 compara el indicador de confianza con la información 115 de confianza que el UA 110 ha recibido y almacenado previamente. Cuando se encuentra una coincidencia entre el indicador de confianza en el mensaje y la información 115 de confianza almacenada, el UA 110 realiza las acciones que normalmente están asociadas con la recepción del mensaje. Cuando no se encuentra una coincidencia entre el indicador de confianza y la información 115 de confianza almacenada, el UA 110 no realiza al menos una acción que normalmente está asociada con la recepción del mensaje.

En una realización, el indicador de confianza y/o la información 115 de confianza podría ser un Identificador de Recursos Uniforme (URI), o algún otro tipo de identificador, de un nodo de red confiable. Un nodo de red podría incluir su URI en un mensaje enviado al UA 110. El UA 110 podría haber recibido previamente información 115 de confianza en forma de una lista de URI confiables. Al recibir un mensaje con un indicador de confianza en forma de URI, el UA 110 podría comparar el URI en el mensaje con los URI en la lista de URI. Si se encuentra una coincidencia, el UA 110 podría confiar en el nodo de red que envió el mensaje.

El UA 110 podría no ser capaz de identificar si un URI pertenece a una P-CSCF, una S-SCSF, una IBCF o algún otro tipo de nodo de red. Algunos nodos de la red (tales como una IBCF) pueden incluir o no su información de URI. Por lo tanto, el UA puede no estar seguro de qué URI representa qué nodo de red. Para determinar esto, se pueden seguir algunas convenciones o se puede agregar un indicador adicional. Una solicitud REGISTER de SIP y su respuesta (y los valores de campo de encabezado incluidos en la respuesta o solicitud) generalmente no deben abandonar el dominio de confianza. Una solicitud REGISTER de un tercero activada por la solicitud REGISTER original puede abandonar el dominio de confianza. En una realización, se establecen medidas para evitar la contaminación de la información en las respuestas al REGISTER en tal caso. Por ejemplo, el hecho de que un URI representa un nodo de red conocido se podría indicar mediante un parámetro de URI a un mensaje de SIP. Por ejemplo, para una S-CSCF, se podría agregar el parámetro de URI scscf. Alternativamente, un parámetro de URI tal como “fe” se podría establecer en un valor o una lista de valores tales como fe = “scscf” o fe = “pcscf, scscf”. En este documento, un nodo de red se conoce como un elemento funcional, o “fe”. Cuando se utiliza el encabezado Service-Route de SIP, el mensaje puede adoptar una forma como la siguiente:

Service-Route: sip: orig@scscf1.home1.com; lr; scscf

o

Service-Route: sip: orig@pcscf1.home1.com; lr; fe = “pcscf, scscf”

en implementaciones en las que los elementos funcionales P-CSCF y S-CSCF (y posiblemente otros) se colocan sobre un equipo físico.

Como alternativa, después de recibir la información 115 de confianza en forma de una lista de URIs, el UA 110 podría consultar una base de datos u otro depósito de datos para determinar los nodos de la red y/o el indicador de confianza y/o la información de confianza que corresponde a los URI listados. La base de datos podría ser un nodo de red en la red o una base de datos en el dispositivo almacenada en la memoria interna o en un módulo de memoria extraíble.

En otra realización, el Marco de Configuración de SIP, el Marco de Política de SIP, un mecanismo de recuperación de política basado en EAP, un servidor basado en XCAP/HTTP o un objeto de gestión de dispositivos (DM) de Open Mobile Alliance (OMA) se podrían utilizar para transmitir indicadores de confianza y/o la información de confianza y/o los nodos de red que corresponden a los URIs enumerados al UA 110.

El UA 110 podría recibir la información 115 de confianza de una o más de varias maneras diferentes. En algunas realizaciones, la información 115 de confianza se podría proporcionar al UA 110 en respuesta a una solicitud REGISTER SIP presentada por el UA 110. En algunas variaciones de estas realizaciones, la respuesta podría ser una respuesta de SIP 200 OK, y la información 115 de confianza podría incluirse directamente en la respuesta 200 OK. La información 115 de confianza se podría incluir en la respuesta 200 OK de un nodo de red, como un servidor de aplicaciones, que recibió la solicitud REGISTER porque la solicitud fue enrutada a través de ella. Alternativamente, el servidor de aplicaciones podría haber recibido una solicitud de registro de un tercero según lo configurado por los Criterios de Filtro iniciales en una S-CSCF.

En otras variaciones de estas realizaciones, la respuesta 200 OK que recibe el UA 110 en respuesta a una solicitud REGISTER podría contener información que informa al UA 110 cómo se puede obtener la información 115 de confianza. Dicha realización se ilustra en la Figura 2. En el evento 210, el UA 110 se registra con una red de IMS al enviar una solicitud REGISTER al nodo B 130 de red, que podría ser una S-CSCF. Como parte del procedimiento 220 de registro, un servidor 200 de suscriptor doméstico (HSS), o un componente similar, puede descargar en el nodo B 130 de red la información 115 de confianza que utilizará el UA 110. En el evento 230, se completa el registro, y el nodo B 130 de red envía al UA 110 una respuesta 200 OK. En la realización de la Figura 2, la respuesta 200 OK podría contener un URI, o algún otro tipo de identificador, que identifique una ubicación en el que se pueda obtener la información 115 de confianza. En otras realizaciones, como se mencionó anteriormente, la respuesta 200 OK podría incluir directamente la información 115 de confianza.

Alternativamente, como se muestra en el evento 240, como parte del registro de SIP, el UA 110 se podría suscribir al paquete de Eventos Reg de SIP, que puede entregar información al UA 110. En respuesta al mensaje de Suscripción en el evento 240, el nodo B 130 de red, en el evento 250, podría devolver un mensaje como un mensaje de Notificación. El mensaje de Notificación puede contener la ubicación de la información 115 de confianza que se descargó del HSS 200 como se describió anteriormente.

Cuando el UA 110 ha recibido la ubicación de la información 115 de confianza, ya sea a través del mensaje 200 OK en el evento 230, a través del mensaje de Notificación en el evento 250, o mediante otro método de SIP, el UA 110 puede recuperar la información 115 de confianza desde la ubicación especificada. En este caso, la ubicación especificada es el nodo A 120 de red, pero en otros casos, la información 115 de confianza se podría recuperar de otros nodos de red. En el evento 260, el UA 110 envía un mensaje, tal como un mensaje HTTP GET, para recuperar la información 115 de confianza desde el nodo A 120 de red. En el evento 270, el nodo A 120 de red envía la información 115 de confianza al UA 110. El UA 110 puede almacenar la información 115 de confianza en la memoria interna o extraíble, en la que la información 115 de confianza estará disponible para uso futuro por el UA 110 para determinar si un nodo de red es de confianza.

En una realización alternativa, la información 115 de confianza se podría proporcionar durante el registro del UA 110 en uno o más campos en el encabezado Path de SIP o el encabezado Service-Route de SIP. Por ejemplo, una solicitud REGISTER de SIP originada por el UA 110 se podría enrutar a través de al menos una P-CSCF y una S-CSCF, en la que la S-CSCF desempeña la función REGISTRAR. La respuesta (tal como una respuesta 200 OK) que el UA 110 recibe a su solicitud REGISTER puede incluir un indicador (tal como un nuevo encabezado P, un encabezado existente o XML incorporado) que transmite información acerca de los nodos de la red (tales como una P-CSCF y una S-SCSF) sobre la ruta por la que se enrutó la solicitud REGISTER. Adicionalmente, uno o más campos en el encabezado Service-Route de SIP pueden contener al menos las direcciones de la P-CSCF o S-CSCF que realmente realizan cualquier servicio. La dirección de S-CSCF en el campo de encabezado Service-Route y la S-CSCF en el campo de encabezado Path no son necesariamente las mismas.

En algunos casos, una S-CSCF que actúa como REGISTRAR puede no ser la S-CSCF que responde a otras solicitudes del UA 110. Más generalmente, no se pueden incluir todos los nodos de red que son capaces de transmitir un mensaje confiable sobre la ruta por la cual se enruta la solicitud REGISTER o su respuesta. Sin embargo, si un nodo de red transmite un mensaje confiable, puede ser ventajoso llenar un campo de encabezado (tal como un campo de encabezado de Asserted-Identity P de SIP) o un parámetro de URI o una parte del cuerpo de SIP con un valor representativo del originador. Existen varios medios para permitir que el UA 110 determine que algún valor representativo del originador solo puede ser conocido o solo insertado por el originador. Por ejemplo, un valor en el campo de encabezado de Asserted-Identity P de SIP se podría comparar con un valor en el campo de encabezado Service-Route.

Cuando un indicador de confianza no está presente en un mensaje recibido por el UA 110 desde un nodo de red fuera del dominio de confianza del UA, o cuando está presente un indicador de confianza, pero no coincide con la información 115 de confianza almacenada del UA, el UA 110 podría reaccionar de varias maneras diferentes. En algunos casos, el UA 110 puede negar, descartar o finalizar el mensaje. En otros casos, el UA 110 podría devolver un mensaje de error al nodo de red que envió el mensaje. En todavía otros casos, el UA 110 podría eliminar porciones del mensaje que podrían provocar acciones indeseables y procesar el resto del mensaje. En algunos casos, se pueden tomar varias combinaciones de estas acciones.

La Figura 3 ilustra una realización de un método 300 para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS. En el bloque 310, un UA recibe del nodo de red un mensaje que contiene

un indicador de confianza. En el bloque 320, el UA determina si el indicador de confianza coincide con la información de confianza almacenada en el UA. En el bloque 330, cuando el indicador de confianza coincide con la información de confianza almacenada en el UA, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje. En el bloque 340, cuando el indicador de confianza no coincide con la información de confianza almacenada en el UA, el UA se abstiene de realizar al menos una acción normalmente asociada con la recepción del mensaje.

La Figura 4 ilustra una realización alternativa de un método 400 para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS. En el bloque 410, un UA recibe un mensaje del nodo de red. En el bloque 420, el UA determina si un indicador de confianza está presente en el mensaje. En el bloque 430, cuando el indicador de confianza está presente en el mensaje, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje. En el bloque 440, cuando el indicador de confianza no está presente en el mensaje, el UA se abstiene de realizar al menos una acción normalmente asociada con la recepción del mensaje.

Volviendo al ejemplo mencionado anteriormente en el que se envía un mensaje malicioso a una pluralidad de UA que informa falsamente a los UA que se ha producido un Tiempo de Espera del Servidor, las realizaciones descritas en este documento podrían evitar que los UA intenten volver a registrarse innecesariamente en la red. Cuando uno de los UA recibe el mensaje malicioso, el UA puede utilizar una técnica descrita en este documento para determinar si se puede confiar en el remitente del mensaje. Dado que, en este caso, no se confiará en el remitente, el UA no realizará una o más acciones normalmente asociadas con la recepción del mensaje. En este caso, la UA no se volvería a registrar.

Una posible reflexión para el UE podría ser la siguiente en 3GPP TS 24.229, subcláusula 5.1.2A.1.6, titulada “Casos anormales”:

En el evento de que el UE reciba una respuesta 504 (Tiempo de Espera del Servidor) que contiene:

- un campo de encabezado P-Asserted-Identity establecido en:

- un valor igual a un valor en el campo de encabezado Service-Route o Path recibido durante el registro; o

- un campo de encabezado Content-Type establecido de acuerdo con la subcláusula 7.6 (es decir, “aplication/3gpp-ims+xml”), independiente del valor o la presencia del campo de encabezado Content-Disposition, independiente del valor o la presencia de parámetros de Content-Disposition, luego la disposición de contenido predeterminada, identificada como “3gpp-alternative-service”, se aplica de la siguiente manera:

- si la respuesta 504 (Tiempo de Espera del Servidor) incluye un cuerpo XML del subsistema CN de IM como se describe en la subcláusula 7.6 con el elemento de tipo establecido en “restauración” y el elemento de acción establecido en “registro inicial”, entonces el UE:

- iniciará los procedimientos de restauración al realizar un registro inicial como se especifica en la subcláusula 5.1.1.2; y

- puede proporcionar una indicación al usuario basada en la cadena de texto contenida en el elemento de razón.

Una posible reflexión para la P-CSCF podría ser la siguiente en 3GPP TS 24.229, subcláusula 5.2.6.3.2A, titulada “Casos anormales”:

Cuando la P-CSCF no puede reenviar una solicitud inicial para un diálogo o una solicitud de una transacción independiente al siguiente salto en el encabezado Service-Route, según lo determinado por uno de los siguientes:

- no hay respuesta a la solicitud de servicio y sus retransmisiones por la P-CSCF;

- se recibe una respuesta 3xx o 480 (temporalmente no disponible) para la solicitud; o

- por medios no especificados disponibles para la P-CSCF;

y:

- la P-CSCF admite procedimientos de restauración;

entonces la P-CSCF:

1) rechazará la solicitud al devolver una respuesta 504 (Tiempo de Espera del Servidor) al UE;

2) supondrá que el UE admite la versión 1 del Esquema XML para el cuerpo XML del subsistema CN de IM 3GPP si el soporte del cuerpo XML del subsistema CN de IM 3GPP como se describe en la subcláusula 7.6 en el campo de encabezado Accept no está indicado; y

3) incluirá en la respuesta 504 (Tiempo de Espera del Servidor):

a) un campo de encabezado Content-Type con el valor establecido en el tipo MIME asociado del cuerpo XML del subsistema CN de IM 3GPP como se describe en la subcláusula 7.6.1;

b) un campo de encabezado P-Asserted-Identity establecido en el valor del URI de SIP de la P-CSCF incluido en el campo de encabezado Path durante el registro del usuario cuyo UE envió la solicitud que provoca esta respuesta; y

c) un cuerpo XML del subsistema CN de IM 3GPP que contiene:

i) un elemento <alternative-service>, configurado con los parámetros del servicio alternativo;

ii) un elemento secundario <type>, establecido en “restauración” para indicar que se admiten los procedimientos de restauración;

iii) un elemento secundario <reason>, establecido en un motivo configurable por el operador; y

iv) un elemento secundario <action>, establecido en “registro inicial”

NOTA: Estos procedimientos no impiden el uso de confiabilidad no especificada o técnicas de recuperación superiores a las especificadas en esta subcláusula.

Una posible reflexión para la S-CSCF podría ser la siguiente en 3GPP TS 24.229, subcláusula 5.4.3.2, titulada “Solicitudes iniciadas por el usuario servido”:

Cuando la S-CSCF recibe una solicitud iniciada por el usuario servido para el cual la S-CSCF no tiene el perfil de usuario o no confía en los datos que tiene (por ejemplo, debido al reinicio), la S-CSCF intentará recuperar el perfil de usuario del HSS. Si la S-CSCF no puede recuperar el perfil de usuario y la S-CSCF admite procedimientos de restauración, entonces la S-CSCF deberá:

1) rechazar la solicitud al devolver una respuesta 504 (Tiempo de Espera del Servidor) al UE;

2) asumir que el UE admite la versión 1 del Esquema XML para el cuerpo XML del subsistema CN de IM 3GPP si el soporte para el cuerpo XML del subsistema CN de IM 3GPP como se describe en la subcláusula 7.6 en el campo de encabezado Aceppt no está indicado; y

3) un campo de encabezado P-Asserted-Identity establecido en el valor del SIP URI de la S-CSCF incluido en el campo de encabezado Service-Route durante el registro del usuario cuyo UE envió la solicitud que provoca esta respuesta;

4) incluirá en la respuesta 504 (Tiempo de Espera del Servidor):

a) un campo de encabezado Content-Type con el valor establecido en el tipo MIME asociado del cuerpo XML del subsistema CN de IM 3GPP como se describe en la subcláusula 7.6.1; y

b) un cuerpo XML del subsistema CN de IM 3GPP:

i) un elemento <alternative-service>, ajustado a los parámetros del servicio alternativo;

ii) un elemento secundario <type>, establecido en “restauración” para indicar que se admiten los procedimientos de restauración;

iii) un elemento secundario <reason>, establecido en un motivo configurable por el operador; y

iv) un elemento secundario <action>, establecido en “registro inicial”

Adicionalmente, las siguientes modificaciones se podrían realizar en 3GPP TS 24.229, subcláusula 5.10.4.1, titulada “General”:

NOTA 1: La funcionalidad THIG se realiza en I-CSCF en la Versión-5 y la Versión-6 y es compatible con Los procedimientos especificados en esta subcláusula.

Los siguientes procedimientos solo se aplicarán si la red requiere el ocultamiento de la topología de la red. La red que requiere el ocultamiento de la topología de red se denomina red oculta.

NOTA 2: Las solicitudes y respuestas se manejan de manera independiente, por lo tanto, no se necesita información del estado red de ocultación para ese propósito dentro de una IBCF.

La IBCF aplicará la topología de red oculta a todos los campos de encabezado que revelen información de topología, tal como Via, Route, Record-Route, Service-Route, y Path.

Al recibir una solicitud REGISTER entrante para la cual se debe aplicar el ocultamiento de topología de red y que incluye un campo de encabezado Path, la IBCF agregará el URI de SIP enrutable de la IBCF a la parte superior del campo de encabezado Path. La IBCF puede incluir en el URI de SIP insertado un indicador que identifica la dirección de las solicitudes posteriores recibidas por la IBCF, es decir, desde la S-CSCF hacia la P-CSCF, para identificar el caso de terminación de UE. La IBCF puede codificar este indicador de diferentes maneras, tales como, por ejemplo, un parámetro único en el URI, una cadena de caracteres en la parte del nombre de usuario del URI o un número de puerto dedicado en el URI.

NOTA 3: Cualquier solicitud posterior que incluya el indicador de dirección (en el campo de encabezado Route) o llegue al número de puerto dedicado, indica que la solicitud se envió por la S-CSCF hacia la P-CSCF.

Al recibir una solicitud inicial entrante para la cual se debe aplicar el ocultamiento de topología de red, una solicitud de SIP o respuesta de SIP con un campo de encabezado P-Asserted-Identity establece el URI de SIP de un elemento funcional dentro de su dominio de confianza, la IBCF aplicará el ocultamiento de topología de red al campo de encabezado P-Asserted-Identity.

Al recibir una solicitud inicial entrante para la cual se debe aplicar el ocultamiento de la topología de red y que incluye un campo de encabezado Record-Route, la IBCF agregará su propio URI de SIP enrutable en la parte superior del campo de encabezado Record-Route.

El UE puede recibir un valor diferente al valor almacenado por el nodo de red, ya que la IBCF puede ocultar la ubicación y reemplazar los URI en el mensaje de SIP (tal como los campos de encabezado Path o Service-Route) con, por ejemplo, al menos uno de los valores del SIP URI de la IBCF. La IBCF tendría que realizar consistentemente esta ubicación ocultando o reemplazando los URI para no romper la confianza que se indica.

Cuando el UA de SIP recibe un mensaje de SIP, analizará una tabla dentro de la función para ver si es necesario realizar alguna acción para ese mensaje de SIP, por ejemplo, una solicitud INVITE. La tabla o estructura de datos identifica los indicadores. Estos indicadores podrían ser, pero no se limitan a, campos de encabezado de SIP, valores específicos de SIP para buscar, etc. Para cada campo, también podría haber una acción o grupo de acciones que podrían realizarse, pero no se limitan a:

Eliminar	Eliminar el elemento si no es de confianza
Ignorar	Ignorar el elemento
Terminar	Terminar el diálogo o rechazar el diálogo para continuar
Confiable	Marque el campo como confiable
No confiable	Marque el campo como no confiable
Confianza	Marque el mensaje como confiable
Desconfianza	Marque el mensaje como no confiable

Para los dos últimos elementos, “Confianza” y “Desconfianza”, todos los elementos en el método SIP tienen que ser confiables. El método para identificar el mensaje como confiable podría transmitirse como:

A) Nueva Etiqueta de Función: Aquí agregará una etiqueta de función al encabezado del contacto con un valor que indica la confiabilidad del mensaje.

B) Nuevo parámetro de URI

C) Parte del cuerpo (por ejemplo, en XML)

D) Nuevo campo de encabezado

Una realización de ejemplo de la estructura de datos está a continuación.

```
SIP Method
|
|> INVITE
| |
| |> Field 1 : Value X
] | |> Action: Remove, ignore, terminate dialogue etc
| |> Field 2: Value k, c
|
|>200 OK
| |
| |>Field 3: Value.....
```

El UA 110 y otros componentes descritos anteriormente podrían incluir un componente de procesamiento que sea capaz de ejecutar instrucciones relacionadas con las acciones descritas anteriormente. La Figura 5 ilustra un ejemplo de un sistema 1300 que incluye un componente 1310 de procesamiento adecuado para implementar una o más realizaciones divulgadas en este documento. Además del procesador 1310 (que se puede denominar unidad de procesador central o CPU), el sistema 1300 puede incluir dispositivos 1320 de conectividad de red, memoria 1330 de acceso aleatorio (RAM), memoria 1340 de solo lectura (ROM), almacenamiento 1350 secundario y dispositivos 1360 de entrada/salida (I/O). Estos componentes pueden comunicarse entre sí a través de un bus 1370. En algunos casos, algunos de estos componentes pueden no estar presentes o se pueden combinar en varias combinaciones entre sí o con otros componentes no mostrados. Estos componentes pueden estar ubicados en una sola entidad física o en más de una entidad física. Cualquier acción descrita en este documento como tomada por el procesador 1310 podría ser tomada por el procesador 1310 solo o por el procesador 1310 junto con uno o más componentes mostrados o no mostrados en el dibujo, como un procesador 1380 de señal digital (DSP). Aunque el DSP 1380 se muestra como un componente separado, el DSP 1380 se podría incorporar al procesador 1310.

El procesador 1310 ejecuta instrucciones, códigos, programas de ordenador o scripts a los que puede acceder desde los dispositivos 1320 de conectividad de red, RAM 1330, ROM 1340 o almacenamiento 1350 secundario (que puede incluir varios sistemas basados en disco tal como el disco duro, disquete o disco óptico). Si bien solo se muestra una CPU 1310, pueden estar presentes múltiples procesadores. Por lo tanto, aunque las instrucciones pueden ser discutidas como ejecutadas por un procesador, las instrucciones pueden ejecutarse simultáneamente, en serie o de otro modo por uno o múltiples procesadores. El procesador 1310 puede implementarse como uno o más chips de CPU.

Los dispositivos 1320 de conectividad de red pueden tomar la forma de módems, bancos de módems, dispositivos Ethernet, dispositivos de interfaz de bus serie universal (USB), interfaces en serie, dispositivos de anillo de credencial, dispositivos de interfaz de datos distribuidos por fibra (FDDI), dispositivos de red de área local inalámbrica (WLAN), dispositivos de transceptor de radio tales como dispositivos de acceso múltiple por división de código (CDMA), sistema global para dispositivos de transceptor de radio de comunicaciones móviles (GSM), dispositivos de interoperabilidad mundial para dispositivos de acceso de microondas (WiMAX) y/u otros dispositivos bien conocidos para conectarse a redes. Estos dispositivos 1320 de conectividad de red pueden permitir que el procesador 1310 se comunique con Internet o una o más redes de telecomunicaciones u otras redes desde las cuales el procesador 1310 podría recibir información o hacia las cuales el procesador 1310 podría enviar información. Los dispositivos 1320 de conectividad de red también pueden incluir uno o más componentes 1325 transceptores capaces de transmitir y/o recibir datos de forma inalámbrica.

La RAM 1330 podría utilizarse para almacenar datos volátiles y tal vez para almacenar instrucciones que se ejecutan por el procesador 1310. La ROM 1340 es un dispositivo de memoria no volátil que normalmente tiene una capacidad de memoria menor que la capacidad de memoria del almacenamiento 1350 secundario. La ROM 1340 se podría utilizar para almacenar instrucciones y tal vez datos que se leen durante la ejecución de las instrucciones. El acceso tanto a la RAM 1330 como a la ROM 1340 es normalmente más rápido que al almacenamiento 1350 secundario. El almacenamiento 1350 secundario normalmente está compuesto por una o más unidades de disco o cintas y se puede utilizar para el almacenamiento no volátil de datos o como un desbordamiento dispositivo de almacenamiento de datos si la RAM 1330 no es lo suficientemente grande como para contener todos los datos de trabajo. El almacenamiento 1350 secundario se puede utilizar para almacenar programas que se cargan en la RAM 1330 cuando dichos programas se seleccionan para su ejecución.

Los dispositivos 1360 de I/O pueden incluir pantallas de cristal líquido (LCD), pantallas táctiles, teclados, teclados, interruptores, diales, ratones, bolas de seguimiento, reconocedores de voz, lectores de tarjetas, lectores de cinta de papel, impresoras, monitores de video, u otros dispositivos de entrada o salida conocidos. Adicionalmente, el transceptor 1325 se podría considerar como un componente de los dispositivos 1360 de I/O en lugar de ser o además de un componente de los dispositivos 1320 de conectividad de red.

En una realización, se proporciona un método para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS. El método incluye un UA que recibe del nodo de red un mensaje que contiene un

indicador de confianza. El método incluye adicionalmente el UA que determina si el indicador de confianza coincide con la información de confianza almacenada en el UA. El método incluye adicionalmente, cuando el indicador de confianza coincide con la información de confianza almacenada en el UA, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje. El método incluye adicionalmente, cuando el indicador de confianza no coincide con la información de confianza almacenada en el UA, el UA se abstiene de realizar al menos una acción normalmente asociada con la recepción del mensaje.

En otra realización, se proporciona un UA. El UA incluye un procesador configurado para recibir de un nodo fuera de un dominio de confianza en una red de IMS un mensaje que contiene un indicador de confianza. El procesador está configurado adicionalmente para determinar si el indicador de confianza coincide con la información de confianza almacenada en el UA. El procesador se configura adicionalmente, cuando el indicador de confianza coincide con la información de confianza almacenada en el UA, para realizar todas las acciones normalmente asociadas con la recepción del mensaje. El procesador se configura adicionalmente, cuando el indicador de confianza no coincide con la información de confianza almacenada en el UA, para abstenerse de realizar al menos una acción normalmente asociada con la recepción del mensaje.

En otra realización, se proporciona un método alternativo para determinar si se puede confiar en un nodo fuera de un dominio de confianza en una red de IMS. El método incluye un UA que recibe un mensaje del nodo de red. El método incluye adicionalmente el UA que determina si un indicador de confianza está presente en el mensaje. El método incluye adicionalmente, cuando el indicador de confianza está presente en el mensaje, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje. El método incluye adicionalmente, cuando el indicador de confianza no está presente en el mensaje, el UA se abstiene de realizar al menos una acción normalmente asociada con la recepción del mensaje.

En otra realización, se proporciona un UA. El UA incluye un procesador configurado para recibir un mensaje de un nodo fuera de un dominio de confianza en una red de IMS. El procesador está configurado adicionalmente para determinar si hay un indicador de confianza en el mensaje. El procesador está configurado adicionalmente, cuando el indicador de confianza está presente en el mensaje, para realizar todas las acciones normalmente asociadas con la recepción del mensaje. El procesador está configurado adicionalmente, cuando el indicador de confianza no está presente en el mensaje, para abstenerse de realizar al menos una acción normalmente asociada con la recepción del mensaje.

En otra realización, se proporciona un método para realizar el registro. El método incluye recibir un mensaje de Tiempo de Espera del Servidor, el mensaje de tiempo de espera del servidor incluye al menos un primer campo establecido en un valor igual a un valor recibido en un segundo campo durante un primer registro. El método incluye adicionalmente iniciar procedimientos de restauración al realizar un segundo registro en respuesta a la recepción del mensaje de tiempo de espera del servidor.

En otra realización, se proporciona un UA. El UA incluye uno o más procesadores configurados de manera tal que el UA recibe un mensaje de tiempo de espera del servidor que incluye al menos un primer campo establecido en un valor igual a un valor recibido en un segundo campo durante un primer registro, y configurado de tal manera que el UA inicia procedimientos de restauración al realizar un segundo registro en respuesta a la recepción del mensaje de tiempo de espera del servidor.

La siguiente Especificación Técnica (TS) del Proyecto de Asociación de 3ra Generación (3GPP) se incorpora en este documento como referencia: TS 24.229.

Si bien se han proporcionado varias realizaciones en la presente divulgación, se debe entender que los sistemas y métodos divulgados se pueden realizar de muchas otras formas específicas sin apartarse del espíritu o alcance de la presente divulgación. Los presentes ejemplos deben considerarse como ilustrativos y no restrictivos, y la intención no debe limitarse a los detalles proporcionados en este documento. Por ejemplo, los diversos elementos o componentes se pueden combinar o integrar en otro sistema o se pueden omitir o no implementar ciertas características.

También, las técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diversas realizaciones como discretos o separados se pueden combinar o integrar con otros sistemas, módulos, técnicas o métodos sin apartarse del alcance de la presente divulgación. Otros elementos mostrados o discutidos como acoplados o directamente acoplados o comunicados entre sí pueden estar indirectamente acoplados o comunicarse a través de alguna interfaz, dispositivo o componente intermedio, ya sea eléctricamente, mecánicamente o de otro modo. Un experto en la técnica puede determinar otros ejemplos de cambios, sustituciones y alteraciones y podrían realizarse sin apartarse del alcance en este documento divulgado.

REIVINDICACIONES

1. Un método realizado por un primer nodo (130) de red de un Subsistema Multimedia de Protocolo de Internet, IMS, Red, el método comprende:

recibir en el primer nodo de red, un Identificador de Recursos Uniforme, URI, en un campo de encabezado en un primer Protocolo de Inicio de Sesión, SIP, mensaje (140);

recibir en el primer nodo de red, una credencial en el campo de encabezado en el primer mensaje (140) de SIP, la credencial indicadora de un tipo de un nodo (120) de red en una ruta del primer mensaje (140) de SIP, en el que el primer mensaje de SIP es una solicitud de REGISTER de SIP presentada por un agente de usuario, UA;

con base en la credencial recibida, enviar mediante el primer nodo de red, un segundo mensaje (150) de SIP que incluye el URI recibido, el segundo mensaje (150) que transmite información acerca del primer nodo (130) de red; y

recibir un tercer mensaje de SIP activado por el primer mensaje de SIP, en el que el tercer mensaje de SIP activado por el primer mensaje de SIP es una solicitud de registro de un tercero que se configura por Criterio de Filtro inicial sobre una Función de Control de Sesión de Llamada en Servicio, S-CSCF.

2. El método como se reivindica en la Reivindicación 1, en el que la credencial es un parámetro asociado con el URI recibido.

3. El método como se reivindica en la Reivindicación 1, en el que un segundo nodo (110) de red está en una ruta del primer mensaje (140) de SIP.

4. El método como se reivindica en la Reivindicación 1, en el que el segundo mensaje (150) de SIP es respuesta SIP 200 OK.

5. Un sistema, que comprende:

un primer nodo (130) de red de un Subsistema Multimedia de Protocolo de Internet, IMS, Red, el primer nodo (130) de red configurado para:

recibir un Identificador de Recursos Uniforme, URI, en un campo de encabezado en un primer Protocolo de Inicio de Sesión, SIP, mensaje (140)

recibir una credencial en el campo de encabezado en el primer mensaje (140) de SIP, la credencial indicadora de un tipo de un nodo de red en una ruta del primer mensaje (140) de SIP, en el que el primer mensaje de SIP es una solicitud de REGISTER de SIP presentada por un agente de usuario, UA;

con base en la credencial recibida, enviar un segundo mensaje (150) de SIP que incluye el URI recibido, el segundo mensaje (150) que transmite información acerca del primer nodo (130) de red; y

recibir un tercer mensaje de SIP activado por el primer mensaje de SIP, en el que el tercer mensaje de SIP activado por el primer mensaje de SIP es una solicitud de registro de un tercero que se configura por Criterio de Filtro inicial sobre una Función de Control de Sesión de Llamada en Servicio, S-CSCF.

6. Un producto de programa de ordenador que comprende un medio tangible de almacenamiento legible por ordenador que tiene instrucciones almacenadas en el mismo que, cuando se ejecuta por un dispositivo de procesamiento, implementan un método realizado por un primer nodo de red de un Subsistema Multimedia de Protocolo de Internet, IMS, Red, el método comprende:

recibir en el primer nodo de red, un Identificador de Recursos Uniforme URI, en un campo de encabezado en un primer Protocolo de Inicio de Sesión, SIP, mensaje (140), en el que el primer mensaje de SIP es una solicitud de REGISTER de SIP presentada por un agente de usuario, UA;

recibir en el primer nodo de red, una credencial en el campo de encabezado en el primer mensaje (140) de SIP, la credencial indicadora de un tipo de un nodo de red en una ruta del primer mensaje (140) de SIP; y

con base en la credencial recibida, enviar mediante el primer nodo de red, un segundo mensaje (150) de SIP que incluye el URI recibido, el segundo mensaje (150) que transmite información acerca del primer nodo (130) de red; y

recibir un tercer mensaje de SIP activado por el primer mensaje de SIP, en el que el tercer mensaje de SIP activado por el primer mensaje de SIP es una solicitud de registro de un tercero que se configura por Criterio de Filtro inicial en una Función de Control de Sesión de Llamada en Servicio, S-CSCF.

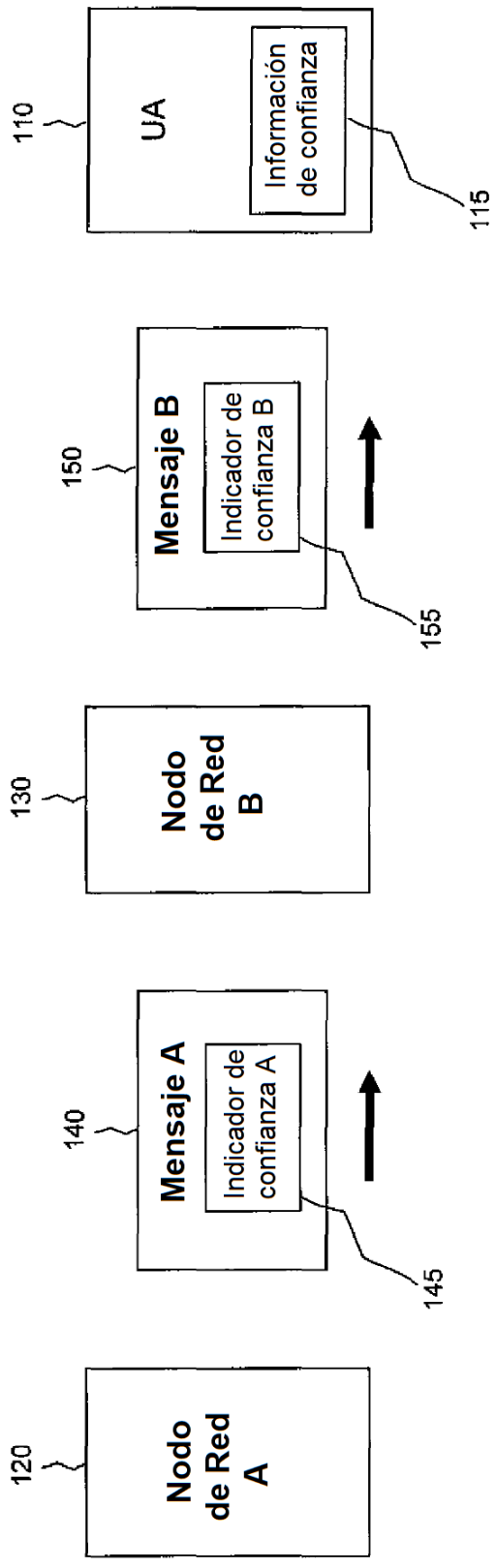
110
UA
Información de confianza
115
150
Mensaje B
Indicador de confianza B
155
130
Nodo de Red B
140
Mensaje A
Indicador de confianza A
145
120
Nodo de Red A

Figura 1

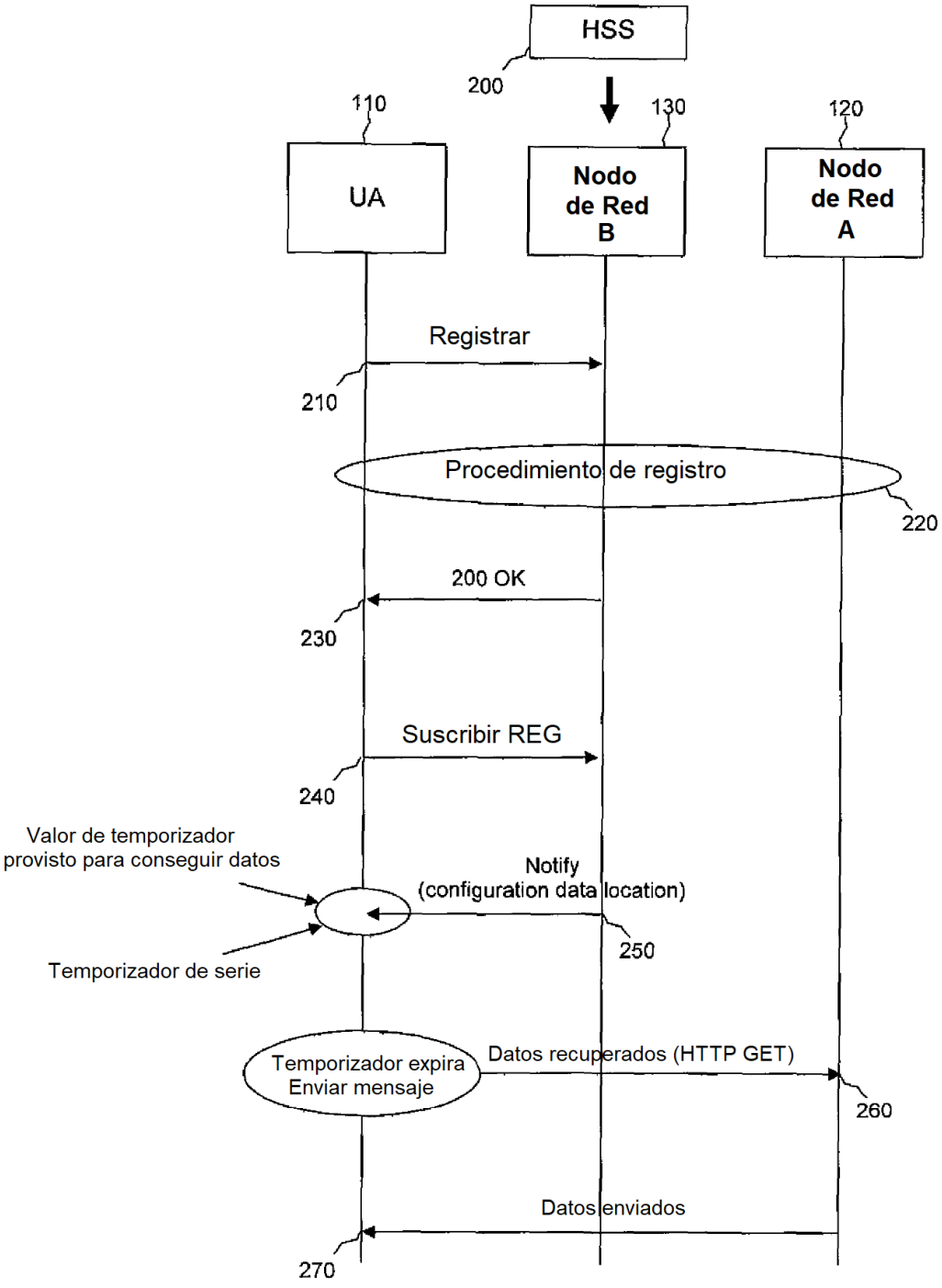
HSS
200
110
130
120
UA
Nodo de Red B
Nodo de Red A
Registrar
210
Procedimiento de registro
220
200 OK
230
Suscribir REG
240
Valor de temporizador provisto para conseguir datos
Notify (configuration data location)
250
Temporizador de serie
Temporizador expira Enviar mensaje
Datos recuperados (HTTP GET)
260
Datos enviados
270

Figura 2

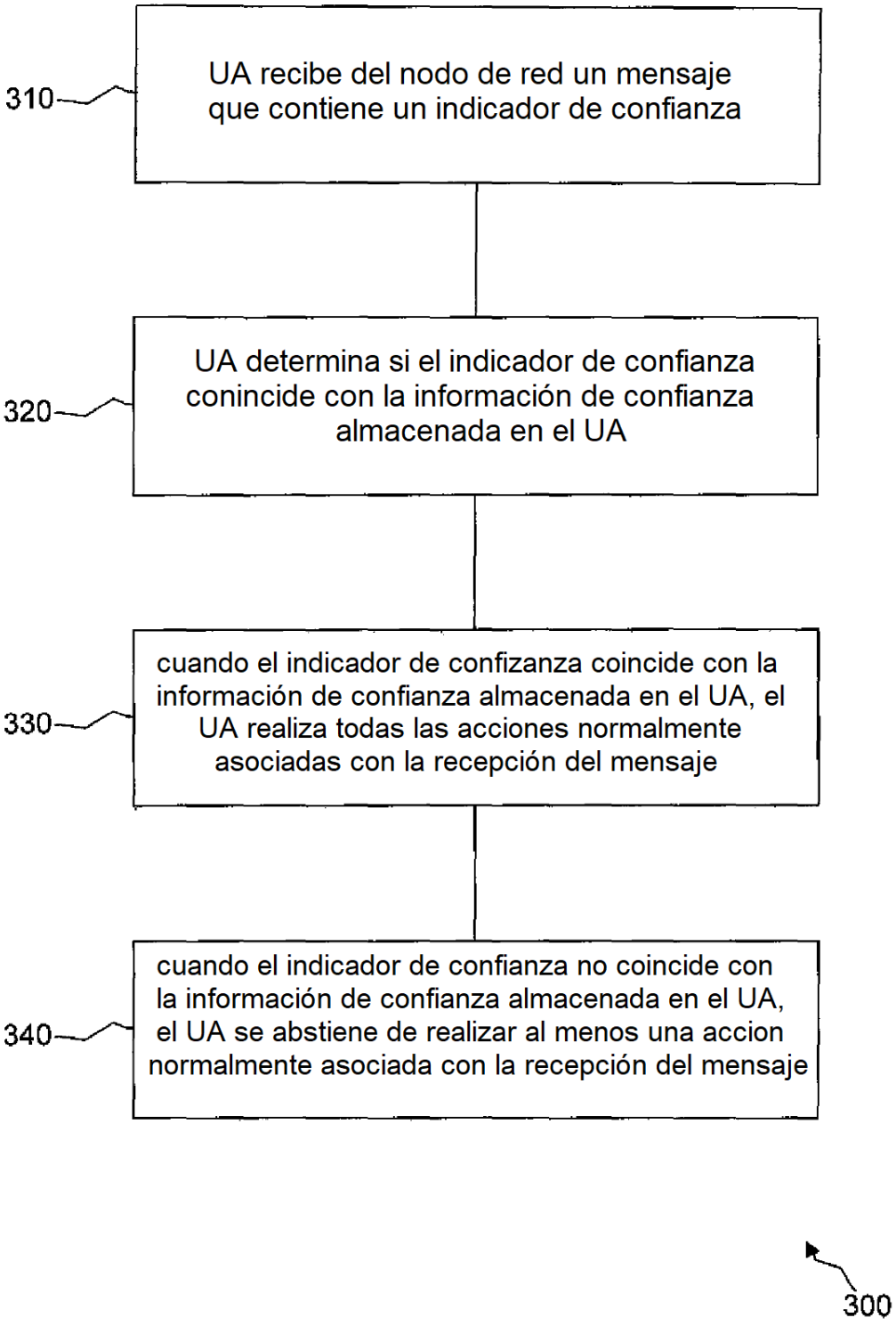
310
UA recibe del nodo de red un mensaje que contiene un indicador de confianza
320
UA determina si el indicador de confianza conincide con la información de confianza almacenada en el UA
330
cuando el indicador de confizanza coincide con la información de confianza almacenada en el UA, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje
340
cuando el indicador de confianza no coincide con la información de confianza almacenada en el UA, el UA se abstiene de realizar al menos una accion normalmente asociada con la recepción del mensaje
300

Figura 3

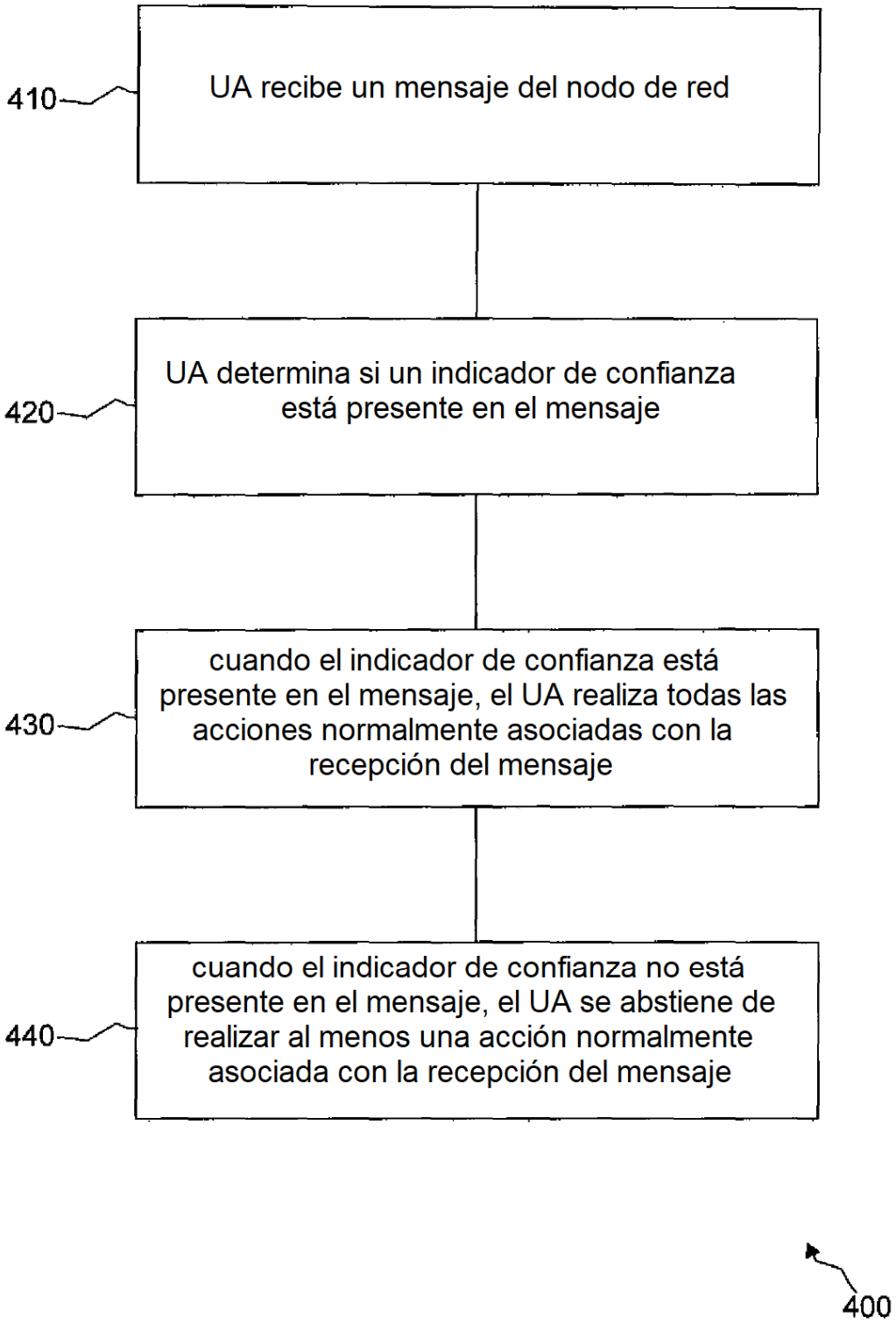
410
UA recibe un mensaje del nodo de red
420
UA determina si un indicador de confianza está presente en el mensaje
430
cuando el indicador de confianza está presente en el mensaje, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje
440
cuando el indicador de confianza no está presente en el mensaje, el UA se abstiene de realizar al menos una acción normalmente asociada con la recepción del mensaje
400

Figura 4

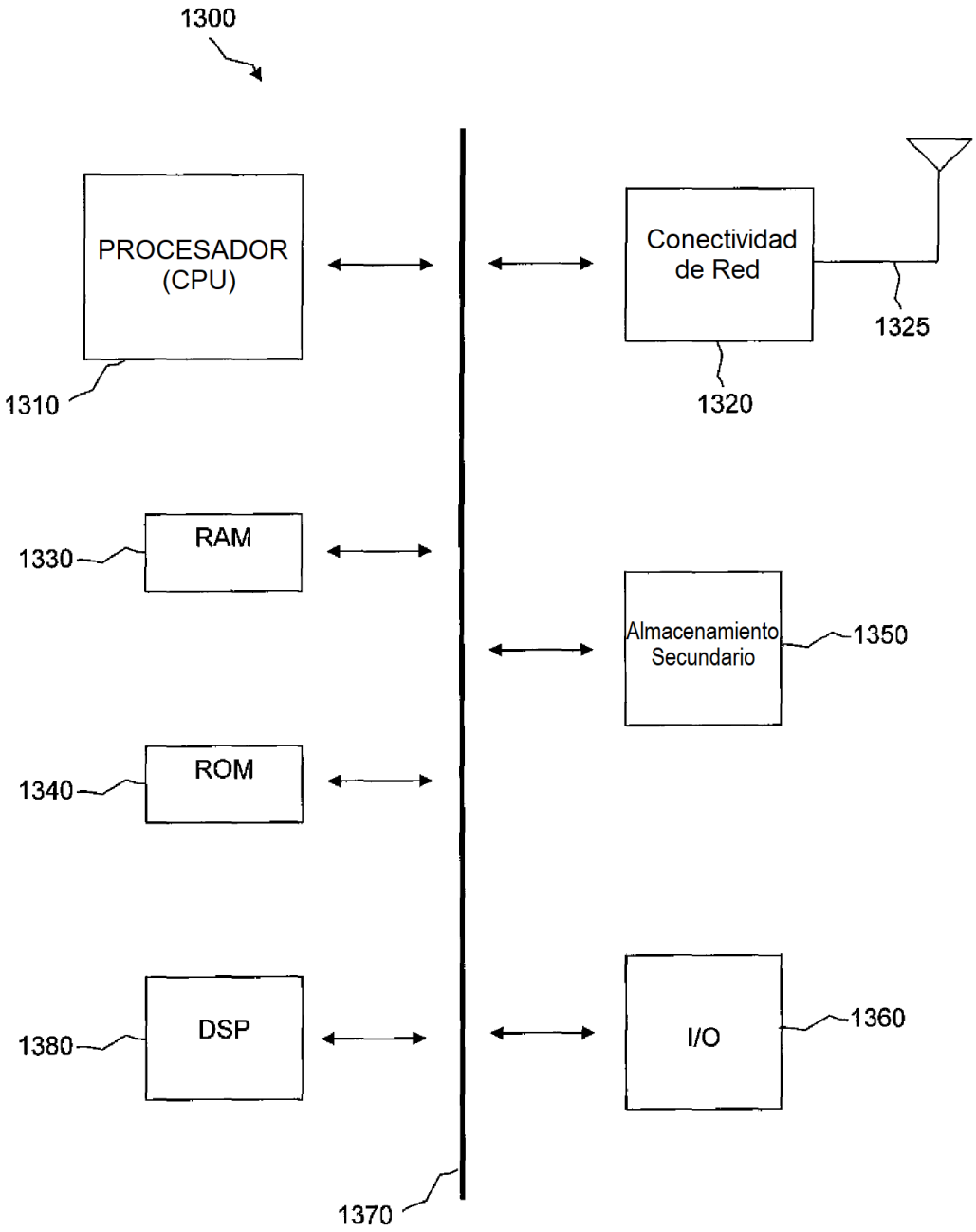
1300
PROCESADOR (CPU)
1310
Conectividad de Red
1320
1325
RAM
1330
Almacenamiento Secundario
1350
ROM
1340
DSP
1380
I/O
1360
1370

Figura 5