(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 474**

(51) Int. CI.:

H04L 29/14 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.03.2010 PCT/US2010/027973**

(87) Fecha y número de publicación internacional: **21.10.2010 WO10120432**

(96) Fecha de presentación y número de la solicitud europea: **19.03.2010 E 10764806 (5)**

(97) Fecha y número de publicación de la concesión europea: **08.02.2017 EP 2601612**

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

(30) Prioridad:

13.04.2009 US 168798 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.07.2017

(73) Titular/es:

BLACKBERRY LIMITED (100.0%)
295 Phillip Street
Waterloo, ON N2L 3W8, CA

(72) Inventor/es:

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

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método para determinar la confianza de los mensajes SIP

Antecedentes

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

Como se usa aquí, los términos “agente de usuario” y “UA” podrían referirse en algunos casos a dispositivos móviles tales como teléfonos móviles, asistentes digitales personales, dispositivos portátiles u ordenadores portátiles, y dispositivos similares que tienen capacidades de telecomunicaciones. Dicho UA podría ser parte de un UE (Equipo de Usuario). Un UE puede tener múltiples UA. Un UE puede tener módulos de memoria extraíbles asociados, tales como pero no limitados a una Tarjeta de Circuito Integrado Universal (UICC) que incluye una aplicación de Módulo de Identificación de Abonado (SIM), una aplicación de Módulo de Identificación de Abonado Universal (USIM), una aplicación de Módulo de Identificación de Servicios Multimedia IP (ISIM), o una aplicación de Módulo de Identificación de Usuario Extraíble (R-UIM), etc. Ejemplos de dichos módulos podrían incluir, pero no están limitados a, Tarjetas de PC, Compact Flash I, Compact Flash II, SmartMedia, Memory Stick, Memory Stick Duo, Memory Stick PRO Duo, Memory Stick PRO-HG Duo, Memory Stick Micro M2, Tarjeta Multimedia, Tarjeta Multimedia de Tamaño Reducido, Tarjeta microMMC, tarjeta Secure Digital, SxS, Almacenamiento Flash Universal, tarjeta miniSD, tarjeta microSD, tarjeta xD-Picture, Intelligent Stick, Módulo Serial Flash, 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 en sí sin dichos módulos. En otros casos, el término “UA” podría referirse a dispositivos que tienen capacidades similares pero que no son transportables, tales como teléfonos de línea fija, ordenadores de sobremesa, decodificadores de televisión, o nodos de red. Cuando uno o más UA son parte de un nodo de red, el nodo de red podría actuar en beneficio de otra función tal como un UA o un dispositivo de línea fija y simular o emular el UA o el dispositivo de línea fija. Por ejemplo, para algunos UA, el cliente SIP IMS que normalmente residiría en el dispositivo realmente reside en la red y transmite la información del mensaje SIP al dispositivo usando protocolos optimizados. En otras palabras, algunas funciones que tradicionalmente eran llevadas a cabo por un UA pueden ser distribuidas en forma de un UA remoto, donde el UA remoto representa el UA en la red. El término “UA” puede también referirse a cualquier componente de hardware o software que pueda terminar una sesión de comunicación que podría incluir, pero no está limitada a, una sesión SIP. También, los términos “agente de usuario”, “UA”, “equipo de usuario”, “UE”, y “nodo” podrían usarse como sinónimos aquí. También, los términos “cabecera” y “campo de cabecera” podrían usarse como sinónimos aquí. También, un mensaje SIP es una solicitud SIP o una respuesta SIP.

Un UA podría conectarse a una red basada en SIP que incluya una pluralidad de otros componentes tales como una P-CSCF (Función de Control de Sesión de Llamada Proxy), un S-CSCF (CSCF servidora), un IBCF (Función de Control de Frontera de Interconexión), un Servidor de Aplicación (AS), y otros componentes, cualquiera de los cuales podría ser referido como nodos de red. Podría existir una relación de confianza entre los nodos en una red SIP. Esto es, un grupo de nodos dentro de una red podrían considerar todos los mensajes recibidos desde otros nodos en el grupo como legítimos. Dicho grupo se puede decir que forma un dominio de confianza o una o más redes de confianza. La RFC 3325 IETF titulada “Extensiones Privadas al Protocolo de Inicio de Sesiones (SIP) para la Identidad Declarada dentro de Redes de Confianza” discute más este tema. La TS 24.229 V8.7.0 3GPP, subcláusula 5.2.6.3.2A describe una P-CSCF enviando una respuesta 504 a un UE.

Breve descripción de los dibujos

Para una comprensión más completa de esta descripción, se hace ahora referencia a la siguiente breve descripción, tomada en relación con los dibujos adjuntos y la descripción detallada, en donde los mismos números de referencia representan las mismas partes.

La Figura 1 es un diagrama de un sistema de comunicaciones que incluye una pluralidad de nodos de red según una realización de la descripción.

La Figura 2 es un diagrama de flujo de una llamada que ilustra un método para un UA para recuperar la información de confianza según una realización de la descripción.

La Figura 3 ilustra un método para determinar si un nodo fuera de un dominio de confianza en una red IMS puede ser de confianza según una realización de la descripción.

La Figura 4 ilustra un método para determinar si un nodo fuera de un dominio de confianza en una red IMS puede ser de confianza según una realización alternativa de la descripción.

La Figura 5 ilustra un procesador y los componentes relacionados adecuados para implementar las varias realizaciones de la presente descripción.

Descripción detallada

La invención se define en las reivindicaciones independientes 1 y 7. Debería ser entendido desde el inicio que aunque más adelante se proporcionan las implementaciones ilustrativas de una o más realizaciones de la presente descripción, los sistemas y/o los métodos descritos se pueden implementar usando cualquier número de técnicas, ya sean actualmente conocidas o en existencia. La descripción no debería limitarse de modo alguno a las implementaciones ilustrativas, los dibujos, y las técnicas ilustradas más adelante, que incluyen los diseños y las implementaciones ejemplares ilustradas y descritas aquí, pero se puede modificar 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 IMS podría recibir un mensaje desde un nodo fuera del dominio de confianza. En algunos casos, dicho mensaje podría mandar al nodo en el dominio de confianza a realizar una o más acciones que pueden no ser deseables para que las realice ese nodo. Por ejemplo, un mensaje podría ser enviado maliciosamente a una pluralidad de UA informando falsamente a los UA de que se ha superado un tiempo de espera del servidor. Un UA que recibe dicho mensaje podría intentar volver a registrarse con un registrador SIP incluso aunque el nuevo registro no es realmente necesario. Si un gran número de UA intentan volver a registrarse, el registrador podría sobrecargarse y fallar. Esto podría llevar a problemas mayores en la red ya que otros UA podrían entonces ser incapaces de registrarse.

En una realización, un mensaje enviado a un nodo de red desde fuera del dominio de confianza de los nodos de la red puede incluir un indicador de confianza que indica la fiabilidad del mensaje. Un indicador de confianza puede ser también un elemento de confianza, un identificador de confianza o una bandera de confianza. Los indicadores de confianza pueden ser de uno 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 envía el mensaje. El destinatario del 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, se verifica el indicador de confianza, 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 se asocian normalmente con la recepción del mensaje o del mensaje y su contenido. Si el indicador de confianza no está presente o si el indicador de confianza no se verifica, el nodo de red que recibe el mensaje podría no realizar una o más de las acciones que se asocian normalmente con la recepción del mensaje o del mensaje y su contenido.

En una realización, el nodo de red que recibe el mensaje es un UA que mantiene la información de confianza relacionada con los nodos de red fuera del dominio de confianza del UA. Tras recibir un mensaje desde fuera del dominio de confianza, el UA puede comparar el indicador de confianza que debería estar incluido en el mensaje con la información de confianza que el UA mantiene. Si el UA verifica que el indicador de confianza coincide con la información de confianza que este mantiene, el UA realiza las acciones que se asocian normalmente con la recepción del mensaje o del mensaje y su contenido. Si el UA no puede verificar que el indicador de confianza coincide con la información de confianza que mantiene, el UA no realiza al menos una acción de las que se asocian normalmente con la recepción del mensaje o del mensaje y su contenido.

Estas realizaciones se ilustran en la Figura 1, donde 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 del UA. Aunque sólo se muestran dos nodos de red, se podría presentar otro número. En esta realización, el nodo A 120 de red genera un mensaje A 140 que incluye un indicador A 145 de confianza en el mensaje A 140. El nodo 120 de red entonces envía el mensaje A 140 al nodo B 130 de red. La recepción del mensaje A 140 provoca que el nodo B 130 genere un mensaje B 150 que contiene un indicador de confianza B 155, y el mensaje B 150 se envía después al UA 110. El Mensaje A 140 puede ser o no el mismo que el mensaje B 150, y el indicador de confianza A 145 puede ser o no el 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 desde el nodo A 120 de red, o el nodo B 130 de red podría generar un nuevo indicador B 155 de confianza basándose en el indicador de confianza A 145 u otra información recibida desde el nodo A 120 de red y/u otros nodos de red.

En otras realizaciones, el nodo A 120 de red no incluye un 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 considerar ninguna información incluida en el mensaje A 140, y el nodo B 130 de red entonces incluye el indicador B 155 de confianza en el mensaje B 150 enviado al UA 110. En otras palabras, el indicador de confianza que el UA 110 recibe podría haber sido generado por el nodo de red con el cual el UA 110 está en comunicación directa, podría haber sido generado por otro nodo de red y después transmitido sin modificación por el nodo de red con el cual el UA 110 está en comunicación directa, o

podría haber sido generado por otro nodo de red y después transmitido con modificación por el nodo de red con el cual el UA 110 está en comunicación directa.

En algunas realizaciones, tras recibir un mensaje que contiene un indicador de confianza, el UA 110 realiza las acciones que se asocian normalmente con la recepción del mensaje. En otras realizaciones, tras recibir un mensaje que contiene un indicador de confianza, el UA 110 compara el indicador de confianza a 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 se asocian 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 de las acciones que normalmente se asocia 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 de confianza. Un nodo de red podría incluir su URI en un mensaje enviado al UA 110. EL UA 110 podría haber recibido previamente la información 115 de confianza en forma de una lista de URI de confianza. Tras 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, a una S_CSCF, a una OBCF, o a algún otro tipo de nodo de red. Algunos nodos de red (tales como una IBCF) pueden incluir o no su información URI. Por lo tanto, el UA puede no estar seguro de que URI representa qué nodo de red. Para determinar esto, se podrían seguir algunas convenciones o se puede añadir un indicador adicional. Una solicitud de REGISTRO SIP y su respuesta (y los valores del campo de cabecera incluidos en la respuesta o la solicitud) normalmente no debería abandonar el dominio de confianza. Una solicitud de registro de un tercero desencadenada por la solicitud de REGISTRO original puede abandonar el dominio de confianza. En una realización, se establecen medidas para evitar la contaminación de la información en las respuestas al REGISTRO en tal caso. Por ejemplo, el hecho de que un URI representa un nodo de red conocido podría ser indicado por un parámetro URI a un mensaje SIP. Por ejemplo, para una S-CSCF, se podría añadir el parámetro URI scscf. Alternativamente, un parámetro URI tale como “fe” se podría establecer a un valor o a una lista de valores tales como fe = “scscf” o fe=”pcscf, scscf”. Aquí, un nodo de red es referido como un elemento funcional, o “fe”. Cuando se usa la cabecera de Ruta de Servicio SIP, el mensaje podría tomar una forma como la siguiente:

Ruta de Servicio: sip:orig@scscf1.home1.com;lr;scscf

o

Ruta de Servicio: sip:orig@scscf1.home1.com;lr;fe=”pcscf, scscf”

en despliegues donde la P-CSCF y la S-CSCF (y posiblemente otros) elementos funcionales son colocados en un equipo físico.

Como alternativa, después de recibir la información 115 de confianza en forma de una lista de URI, el UA 110 podría consultar una base de datos u otro repositorio de datos para determinar los nodos de 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 en la red o una base de datos en el dispositivo almacenada en una memoria que es bien interna o un módulo de memoria extraíble.

En otra realización, el Marco de Configuración de SIP, el Marco de Política SIP, un mecanismo de recuperación de políticas basado en EAP, un servidor basado en XCAP/HTTP o un objeto de gestión de dispositivos (DM) de la Alianza Móvil Abierta (OMA) podrían ser utilizados para transportar los indicadores de confianza y/o la información de confianza y/o los nodos de red que corresponden a los URI listados para el UA 110.

El UA 110 podría recibir la información 115 de confianza de una o más de entre varias maneras diferentes. En algunas realizaciones, la información 115 de confianza se podría proporcionar al UA 110 en respuesta a una solicitud de REGISTRO SIP enviada por el UA 110. En algunas variaciones de estas realizaciones, la respuesta podría ser una respuesta 200 OK SIP, y la información 115 de confianza podría estar incluida directamente en la respuesta 200 OK. La información 115 podría estar incluida en la respuesta 200 OK por un nodo de red, tal como un servidor de aplicación, que recibió la solicitud de REGISTRO ya que la solicitud fue enrutada a través de este. Alternativamente, el servidor de aplicación podría haber recibido una solicitud de registro de una tercera parte como configurada por los Criterios de Filtro iniciales en un S-CSCF.

En otras variaciones de estar realizaciones, la respuesta 200 OK que el UA 110 recibe en respuesta a una solicitud de REGISTRO podría contener información que informa al UA 110 de cómo se puede obtener la información 115 de confianza. Tal realización se ilustra en la Figura 2. En el evento 210, el UA 110 se registra en una red IMS mediante el envío de una solicitud de REGISTRO al nodo B 130 de red, el cual podría ser un S-CSCF. Como parte del procedimiento 220 de registro, un servidor 200 de abonado local (HSS), o un componente similar, podría descargar al nodo B 130 de red la información 115 de confianza que ha de ser usada por el UA 110. En el evento 230, el

registro está completo, y el nodo B 130 de 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 donde 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 SIP, el UA 110 podría abonarse al paquete de Eventos de Registro de SIP, el cual puede entregar información de vuelta al UA 110. En respuesta al mensaje de abono en el evento 240, el nodo B 130 de red, en el evento 250, podría devolver un mensaje tal como un mensaje de Notificación. El mensaje de Notificación podría contener la ubicación de la información 115 de confianza que fue descargada desde el HSS 200 como se describió anteriormente.

Cuando el UA 110 ha recibido la ubicación de la información 115 de confianza, bien a través del mensaje 200 OK en el evento 230, a través del mensaje de Notificación en el evento 250, o a través de otro método SIP, el UA 110 puede recuperar la información 115 de confianza de la ubicación especificada. En este caso, la ubicación especificada es un nodo A 120 de red, pero en otros casos, la información 115 de confianza podría ser recuperada 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 del 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 entonces almacenar la información 115 de confianza en la memoria interna o extraíble, donde la información 115 de confianza estará disponible para su uso futuro por el UA 110 en la determinación de si un nodo de red es de confianza.

En una realización alternativa, la información 115 de confianza podría ser proporcionada durante el registro del UA 110 en uno o más campos en la cabecera de Camino SIP o en la cabecera de Ruta de Servicio SIP. Por ejemplo, una solicitud de REGISTRO SIP originada por el UA 110 podría ser enrutada a través de al menos un P-CSCF y un S-CSCF, donde el S-CSCF realiza el rol del REGISTRADOR. La respuesta (tal como una respuesta 200 OK) que recibe el UA 110 a su solicitud de REGISTRO podría incluir un indicador (tal como una nueva cabecera P, una cabecera existente, o un XML incrustado) que transporta la información sobre los nodos de red (tales como un P-CSCF y un S-CSCF) en el camino sobre el cual fue enrutada la solicitud de REGISTRO. Además, uno o más campos en la cabecera de la Ruta de Servicio SIP podrían contener al menos las direcciones del P-CSCF o S-CSCF que realmente realizan cualquier servicio. La dirección del S-CSCF en el campo cabecera de la Ruta de Servicio y del S-CSCF en el campo cabecera de Camino no es necesariamente la misma.

En algunos casos, un S-CSCF que actúa como un REGISTRADOR puede no ser el S-CSCF que responda a otras solicitudes del UA 110. Más generalmente, no todos los nodos de red que son capaces de transmitir un mensaje de confianza se puede incluir en el camino sobre el cual se enruta la solicitud de REGISTRO o su respuesta. Sin embargo, si un nodo de red transmite un mensaje de confianza, puede ser ventajoso completar un campo de cabecera (tal como un campo de cabecera de la Identidad Afirmada P SIP) o un parámetro URI o una parte del cuerpo SIP con un valor representativo del iniciador. Existen varios medios para permitir al UA 110 determinar que algún valor representativo del iniciador podría sólo ser conocido o sólo ser insertado por el iniciador. Por ejemplo, un valor en el campo de cabecera de la Identidad Afirmada P SIP podría ser comparado con un valor en el campo de cabecera de la Ruta de Servicio.

Cuando un indicador de confianza no esté presente en un mensaje recibido por el UA 110 de un nodo de red fuera del dominio de confianza del UA, o cuando un indicador de confianza está presente 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 podría denegar, descartar, o terminar el mensaje. En otros casos, el UA 110 podría devolver un mensaje de error al nodo de red que envió el mensaje. En otros casos, el UA 110 podría eliminar porciones del mensaje que pudieran causar que se tomen acciones indeseables y podría procesar el resto del mensaje. En algunos casos, podrían ser tomadas varias combinaciones de estas acciones.

La Figura 3 ilustra una realización de un método 300 para determinar si un nodo fuera del dominio de confianza en una red IMS puede ser de confianza. En el bloque 310, un UA recibe desde el 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 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 almacenada en el UA, el UA se abstiene de realizar al menos una acción de las normalmente asociadas con la recepción del mensaje.

La Figura 4 ilustra una realización alternativa de un método 400 para determinar si un nodo fuera de un dominio de confianza en una red IMS puede ser de confianza. En el bloque 410, un UA recibe un mensaje desde el 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 de las normalmente asociadas con la recepción del mensaje.

Volviendo al ejemplo mencionada anteriormente donde un mensaje malicioso enviado a una pluralidad de UA informando falsamente a los UA de que se ha superado un tiempo de espera del servidor, las realizaciones descritas aquí podrían prevenir a los UA de innecesarios intentos de volver a registrarse en la red. Cuando uno de los UA recibe el mensaje malicioso, el UA podría usar una técnica descrita aquí para determinar si el emisor del mensaje puede ser de confianza. Ya que, en este caso, el emisor no sería de confianza, el UA no realizaría una o más acciones de las normalmente asociadas con la recepción del mensaje, En este caso, el UA no se volvería a registrar.

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

En el evento el UE recibe una respuesta 504 (tiempo de espera del Servidor) que contiene:

- un campo de cabecera de la Identidad Afirmada P establecido a:

  - un valor igual a un valor en campo cabecera de la Ruta de Servicio o del camino recibido durante el registro; o

- un campo de cabecera del Tipo de Contenido establecido según a la subcláusula 7.6 (esto es "aplicación/3gpp-ims+xml"), independiente del valor o la presencia del campo de cabecera de la Disposición de Contenido, independiente del valor o la presencia de los parámetros de la Disposición de Contenido, entonces la disposición de contenido predeterminada, identificada como "3gpp-servicio-alternativo", se aplica como sigue:

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

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

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

Una posible reflexión para la P-CSCF podría ser como sigue en la TS 24.229 3GPP, subcláusula 5.2.6.3.2A, titulada "Casos anormales":

Cuando la P-CSCF es incapaz de enviar una solicitud inicial para un diálogo o una solicitud para una transacción autónoma al siguiente salto en la cabecera de la Ruta de Servicio, como se determina por uno de los siguientes:

- no hay respuesta a la solicitud de servicio y su retransmisión por la P-CSCF;

- se recibe una respuesta 3xx o una respuesta 480 (Temporalmente No Disponible) para la solicitud; o

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

y:

- la P-CSCF soporta procedimientos de restauración;

entonces la P-CSCF:

1) rechazará la solicitud mediante la devolución de una respuesta 504 (tiempo de espera del servidor) al UE;

2) asumirá que el UE soporta la versión 1 del esquema XML para el cuerpo XML del subsistema CN IM 3GPP si no se indica el soporte para el cuerpo XML del subsistema CN IM 3GPP como se describe en la subcláusula 7.6 en el campo de cabecera de Aceptación; e

3) incluirá en la respuesta 504 (tiempo de espera del servidor):

a) un campo de cabecera del Tipo de Contenido con el valor establecido al tipo MIME asociado del cuerpo XML del subsistema CN IM 3GPP como se describe en la subcláusula 7.6.1;

b) un campo de cabecera de la Identidad Afirmada P establecido al valor del URI SIP de la P-CSCF incluido en el campo de cabecera de Camino durante el registro del usuario cuyo UE envía la solicitud que causa esta respuesta; y

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

i. un elemento <servicio alternativo>, establecido a los parámetros del servicio alternativo

ii. un elemento hijo <tipo>, establecido a “restauración” para indicar que se soportan procedimientos de restauración;

iii. una elemento hijo <razón>, establecido a una razón configurable del operador; y

iv. un elemento hijo <acción>, establecido a un “registro inicial”

NOTA: estos procedimientos no impiden el uso de técnicas de fiabilidad o de recuperación no especificadas anteriormente y que estén más allá de las especificadas en esta subcláusula.

Una posible reflexión para la S-CSCF podría ser como sigue en la TS 24.229 3GPP, 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 la cual la S-CSCF no tiene el perfil de usuario o no confía en los datos que este tiene (por ejemplo debido a un reinicio), el S-CSCF intentará recuperar el perfil de usuario del HSS. Si la S-CSCF falla al recuperar el perfil de usuario y la S-CSCF soporta los procedimientos de restauración, entonces la S-CSCF:

1) rechazará la solicitud mediante la devolución de una respuesta 504 (Tiempo límite del Servidor) al UE;

2) asumirá que el UE soporta la versión 1 del esquema XML para el cuerpo XML del subsistema CN IM 3GPP si no se indica el soporte para el cuerpo XML del subsistema CN IM 3GPP como se describe en la subcláusula 7.6 en el campo de cabecera de Aceptación; y

3) un campo de cabecera de la Identidad Afirmada P establecido al valor del URI SIP de la S-CSCF incluido en el campo de cabecera de Ruta de Servicio durante el registro del usuario cuyo UE envía la solicitud que causa esta respuesta; e

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

a) un campo de cabecera del Tipo de Contenido con el valor establecido al tipo de MIME asociado del cuerpo XML del subsistema CN IM 3GPP como se describe en la subcláusula 7.6.1; y

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

i. un elemento <servicio alternativo>, establecido a los parámetros del servicio alternativo

ii. un elemento hijo <tipo>, establecido a “restauración” para indicar que se soportan procedimientos de restauración;

iii. una elemento hijo <razón>, establecido a una razón configurable del operador; y

iv. un elemento hijo <acción>, establecido a un “registro inicial”

Además, se podrían hacer las siguientes modificaciones a la TS 24.229 3GPP, subcláusula 5.10.4.1, titulada “General”:

NOTA 1: la funcionalidad THIG se realiza en la versión 5 y la versión 6 de la I-CSCF y es compatible con los procedimientos especificados en esta subcláusula.

Los siguientes procedimientos sólo se aplicarán si la ocultación de la topología de red es requerida por la red. La red que requiere la ocultación de la topología de red es llamada red de ocultación.

NOTA 2: Las solicitudes y respuestas se manejan independientemente por lo tanto no se necesita información de estado para tal propósito dentro de una IBCF.

La IBCF aplicará la topología de red ocultándola a todos los campos de la cabecera que revelan información de la topología, tales como Vía, Ruta, Ruta de Registro, Ruta de Servicio, y Camino.

Tras recibir una solicitud de REGISTRO entrante para la cual se ha de aplicar la ocultación de la topología de red y la cual incluye un campo de cabecera de Camino, la IBCF añadirá el URI SIP enrutable de la IBCF a la parte superior del campo de cabecera de Camino. La IBCF puede incluir en la URI SIP insertada un indicador que identifica la dirección de las posteriores solicitudes recibidas por la IBCF esto es, desde la S-CSCF hacia la P-CSCF, para identificar el caso de terminación del UE. La IBCF puede codificar este indicador de diferentes maneras, tales

como, por ejemplo, un parámetro único en la 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 cabecera de Ruta) o llegue por el número de puerto dedicado, indica que la solicitud fue enviada por la S-CSCF hacia la P-CSCF.

Tras recibir una solicitud inicial entrante para la cual se ha de aplicar la ocultación de la topología de red una solicitud SIP o una respuesta SIP con un campo de cabecera de la Identidad Afirmada P establece el URI SIP de un elemento funcional dentro de su dominio de confianza, la IBCF aplicará la ocultación de la topología de red al campo de cabecera de la Identidad Afirmada P

Tras recibir una solicitud inicial entrante para la cual se ha de aplicar la ocultación de la topología de red y la cual incluye un campo de cabecera de Ruta de Registro, la IBCF añadirá su propio URI SIP enrutable a la parte superior del campo de cabecera de Ruta de Registro.

El UE puede recibir un valor diferente del valor almacenado por el nodo de red como la IBCF puede realizar la ocultación de la ubicación y reemplazo de los URI en el mensaje SIP (tales como los campos de cabecera de Ruta de Servicio o Camino) con, por ejemplo, al menos uno de los valores del URI SIP de la IBCF. Consecuentemente la IBCF tendría que realizar esta ocultación de la ubicación o el reemplazo de estos URI para no romper la confianza que se indica.

Cuando el UA SIP recibe un mensaje SIP, éste analizará una tabla dentro de la función para ver si se necesita realizar algunas acciones para ese mensaje SIP, por ejemplo, una solicitud de INVITACIÓN. La tabla o la estructura de datos identifican los indicadores. Estos indicadores podrían ser, pero no están limitados a, campos de la cabecera SIP, valores específicos de SIP a buscar, etc. Para cada campo, podría haber también una acción o un grupo de acciones que podrían ser realizadas pero que no están limitados a:

Eliminar	Elimina el elemento si no es de confianza
Ignorar	Ignora el elemento
Terminar	Termina el diálogo o rechaza el diálogo para continuar
Confianza	Marca el campo como de confianza
No confianza	Marca el campo como de no confianza
Mensaje de confianza	Marca el mensaje como de confianza
Mensaje de no confianza	Marca el mensaje como de no confianza

Para los últimos dos elementos, “Mensaje de confianza” y “Mensaje de no confianza”, todos los elementos en el método SIP tienen que ser de confianza. El método para identificar el mensaje como de confianza podría ser transportado como:

A. Etiqueta de nueva característica Aquí se añadirá una etiqueta de característica a la cabecera de contacto con un valor que indica la fiabilidad del mensaje.

B. Nuevo parámetro URI

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

D. Nuevo campo de cabecera

Una realización de ejemplo de la estructura de datos es la siguiente.

Método SIP

|

|> INVITACIÓN

| |

| |> Campo 1: Valor X

| | |>Acción: Eliminar, ignorar, terminar, dialogar etc

| |> Campo 2: Valor k, c

|

|>200 OK

| |

| |>Campo 3: Valor.....

El UA 110 y otros componentes descritos anteriormente podrían incluir un componente de procesamiento que sea capaz de ejecutar las 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 descritas aquí. Además del procesador 1310 (el cual puede ser referido como una unidad central de procesamiento o CPU), el sistema 1300 podría incluir dispositivos 1320 de conectividad de red, memoria de acceso aleatoria (RAM) 1330, memoria de sólo lectura (ROM) 1340, un almacenamiento secundario 1350, y dispositivos 1360 de entrada/salida (I/O). Estos componentes podrían comunicarse los unos con los otros a través de un bus 1370. En algunos casos, algunos de estos componentes pueden no estar presentes o pueden estar combinados los unos con los otros o con otros componentes no mostrados en varias combinaciones. Estos componentes se podrían ubicar en una entidad física única o en más de una entidad física. Cualquier acción descrita aquí como que es tomada por el procesador 1310 podría ser tomada por el procesador 1310 sólo o por el procesador 1310 en conjunción con uno o más componentes mostrados o no mostrados en los dibujos, tales como un procesador digital de la señal (DSP) 1380. Aunque el DSP 1380 se muestra como un componente separado, el DSP 1380 podría ser incorporado en el procesador 1310.

El procesador 1310 ejecuta las instrucciones, códigos, programas de ordenador, o scripts que se podrían acceder desde los dispositivos 1320 de conectividad de red, la RAM 1330, la ROM 1340 o el almacenamiento secundario 1350 (el cual podría incluir varios sistemas basados en disco tales como un disco duro, un disco flexible o un disco óptico). Aunque sólo se muestra una CPU 1310, pueden estar presentes múltiples procesadores. Así, aunque las instrucciones pueden ser discutidas como que son ejecutadas por un procesador, las instrucciones pueden ser ejecutadas simultáneamente, en serie, o de otra manera por uno o múltiples procesadores. El procesador 1310 se puede implementar como uno o más chips CPU.

Los dispositivos 1320 de conectividad de red pueden tomar la forma de módems, bancos de módems, dispositivos de Ethernet, dispositivos de interfaz de bus serie universal (USB), interfaces seriales, dispositivos token ring, dispositivos de la interfaz de datos distribuida por fibra (FDDI), dispositivos de red de área local inalámbrica (WLAN), dispositivos transceptores de radio tales como los dispositivos de acceso múltiple por división de código (CDMA), dispositivos transceptores de radio para las comunicaciones móviles (GSM), dispositivos de interoperabilidad mundial para el acceso por microondas (WiMAX), y/u otros dispositivos bien conocidos para conectarse a las redes. Estos dispositivos 1320 de conectividad de red pueden permitir al procesador 1310 comunicarse con Internet o una o más redes de telecomunicaciones u otras redes desde las cuales el procesador 1310 podría recibir información o a las cuales el procesador 1310 podría emitir información. Los dispositivos 1320 de conectividad de red podrían también incluir uno o más componentes 1325 transceptores capaces de transmitir y/o recibir datos inalámbricamente.

La RAM 1330 se podría usar para almacenar datos volátiles y quizás para almacenar instrucciones que son ejecutadas por el procesador 1310. La ROM 1340 es un dispositivo de memoria no volátil que normalmente tiene una menor capacidad de memoria que la capacidad de memoria del almacenamiento secundario 1350. La ROM 1340 se podría usar para almacenar instrucciones y quizás datos que sean leídos 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 secundario 1350. El almacenamiento secundario 1350 está comprendido normalmente de una o más unidades de disco o unidades de cinta y podría ser usado por el almacenamiento no volátil de datos o como un dispositivo de almacenamiento de datos de desbordamiento si la RAM 1330 no es suficientemente grande para mantener todos los datos de trabajo. El almacenamiento secundario 1350 se puede usar para almacenar programas que se cargan en la RAM 1330 cuando dichos programas son seleccionados para su ejecución.

Los dispositivos 1360 de I/O pueden incluir elementos de presentación de cristal líquido (LCD), pantallas táctiles, teclados, teclados numéricos, conmutadores, diales, ratones, ruedas de desplazamiento, reconocedores de voz, lectores de tarjetas, lectores de cinta de papel, impresoras, monitores de video, u otros dispositivos de entrada o salida bien conocidos. También, el transceptor 1325 podría ser considerado ser un componente de los dispositivos 1360 de I/O en lugar de o además de ser un componente de los dispositivos 1320 de conectividad de red.

En una realización, se proporciona un método para determinar si un nodo fuera de un dominio de confianza en una red IMS puede ser de confianza. El método incluye un UA que recibe un mensaje del nodo de red que contiene un indicador de confianza. El método además incluye al UA determinando si el indicador de confianza coincide con la información de confianza almacenada en el UA. El método además incluye, cuando el indicador de confianza coincide con la información de confianza almacenada en el UA, al UA realizando todas las acciones normalmente asociadas con la recepción del mensaje. El método además incluye, cuando el indicador de confianza no coincide

con la información de confianza almacenada en el UA, al UA absteniéndose de realizar al menos una acción de las normalmente asociadas con la recepción del mensaje.

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

En otra realización, se proporciona un método alternativo para determinar si un nodo fuera del dominio de confianza en una red IMS puede ser de confianza. El método incluye un UA que recibe un mensaje del nodo de red. El método además incluye al UA determinando si un indicador de confianza está presente en el mensaje. El método además incluye, cuando el indicador de confianza está presente en el mensaje, al UA realizando todas las acciones normalmente asociadas con la recepción del mensaje. El método además incluye, cuando el indicador de confianza no está presente en el mensaje, al UA absteniéndose de realizar al menos una acción de las normalmente asociadas 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 del dominio de confianza en una red IMS. El procesador se configura además para determinar si un indicador de confianza está presente en el mensaje. El procesador se configura además, cuando el indicador de confianza está presente en el mensaje, para realizar todas las acciones normalmente asociadas con la recepción del mensaje. El procesador se configura además, cuando el indicador de confianza no está presente en el mensaje, para abstenerse de realizar al menos una acción de las normalmente asociadas con la recepción del mensaje.

En otra realización, se proporciona un método para realizar el registro. El método incluye la recepción de un mensaje de tiempo de espera del servidor, incluyendo el mensaje de tiempo de espera del servidor al menos un primer campo establecido a un valor igual al valor recibido en un segundo campo durante un primer registro. El método además incluye el inicio de los procedimientos de restauración mediante la realización de 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 tales que el UA reciba un mensaje de tiempo de espera del servidor que incluye al menos un primer campo establecido a un valor igual al valor recibido en un segundo campo durante un primer registro, y configurado tal que el UA inicie los procedimientos de restauración mediante la realización de 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 3ª Generación (3GPP) se incorpora aquí por la referencia: TS 24.229

Los presentes ejemplos han de ser considerados como ilustrativos y no restrictivos, y la intención no es estar limitado a los detalles dados aquí. Por ejemplo, los diversos elementos o componentes se pueden combinar o integrar en otro sistema o ciertas características se pueden omitir, o no implementar.

También, las técnicas, los sistemas, los subsistemas y los 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 salir del alcance de la presente descripción. Otros elementos mostrados o discutidos como acoplados o acoplados o que se comunican directamente los unos con los otros se pueden acoplar indirectamente o comunicarse a través de alguna interfaz, dispositivo, o componente intermedio, bien eléctricamente, mecánicamente, o de otra manera. Otros ejemplos de cambios, sustituciones, y alteraciones son comprobables por alguien experto en la técnica y podrían ser hechos sin salir del alcance aquí descrito.

REIVINDICACIONES

1. Un método realizado por un agente de usuario para realizar el registro, comprendiendo el método:

recibir un mensaje de tiempo de espera del servidor, en el UA, incluyendo el mensaje de tiempo de espera del servidor al menos un primer campo establecido a un valor igual al valor recibido en un segundo campo durante un primer registro del UA, en donde el segundo campo es un campo de cabecera de Ruta de Servicio y el primer campo comprende un campo de cabecera de la Identidad Afirmada P; e

iniciar los procedimientos de restauración, en el UA, mediante la realización de un segundo registro en respuesta a la recepción del mensaje de tiempo de espera del servidor.

2. El método como se reivindica en la reivindicación 1, en donde el valor recibido en el mensaje de tiempo de espera del servidor es un protocolo de inicio de sesiones, SIP, un identificador de recurso uniforme, URI, de una Función de control de sesión de llamada servidora, S-CSCF.

3. El método como se reivindica en la reivindicación 1, en donde, cuando el valor del mensaje de tiempo de espera del servidor incluye el primer campo establecido a un valor no igual al valor recibido durante el primer registro, no se realiza la restauración.

4. El método de cualquiera de las reivindicaciones precedentes, en donde el mensaje de tiempo de espera del servidor se recibe de un nodo de red dentro de un dominio de confianza.

5. El método de cualquiera de las reivindicaciones precedentes, en donde el mensaje de tiempo de espera del servidor se recibe de un nodo de red que realiza servicios.

6. El método de cualquiera de las reivindicaciones precedentes, que comprende además la recepción del mensaje de tiempo de espera del servidor en respuesta a un mensaje de solicitud.

7. Un agente de usuario, UA, que comprende:

un procesador configurado tal que el UA recibe un mensaje de tiempo de espera del servidor, incluyendo el mensaje de tiempo de espera del servidor al menos un primer campo establecido a un valor igual al valor recibido en un segundo campo durante un primer registro, en donde el segundo campo es un campo de cabecera de Ruta de Servicio y el primer campo comprende un campo de cabecera de la Identidad Afirmada P, y configurado tal que el UA inicia los procedimientos de restauración mediante la realización de un segundo registro en respuesta a la recepción del mensaje de tiempo de espera del servidor.

8. El UA como se reivindica en la reivindicación 7, en donde el valor recibido en el mensaje de tiempo de espera del servidor es un protocolo de inicio de sesión, SIP, un identificador de recurso uniforme, URI, de una función de control de sesión de llamada servidora, S-CSCF.

9. El UA como se reivindica en la reivindicación 7, en donde cuando el valor del mensaje de tiempo de espera del servidor incluye el primer campo establecido a un valor no igual al valor recibido durante el primer registro, no se realiza la restauración.

10. El UA de cualquiera de las reivindicaciones 7 a 9, en donde el mensaje de tiempo de espera del servidor se recibe desde un nodo de red dentro de un dominio de confianza.

11. El UA de cualquiera de las reivindicaciones 7 a 10, en donde el mensaje de tiempo de espera del servidor se recibe de un nodo de red que realiza servicios.

12. El UA de cualquiera de las reivindicaciones 7 a 11, en donde el procesador se configura además para recibir el mensaje de tiempo de espera del servidor en respuesta a un mensaje de solicitud.

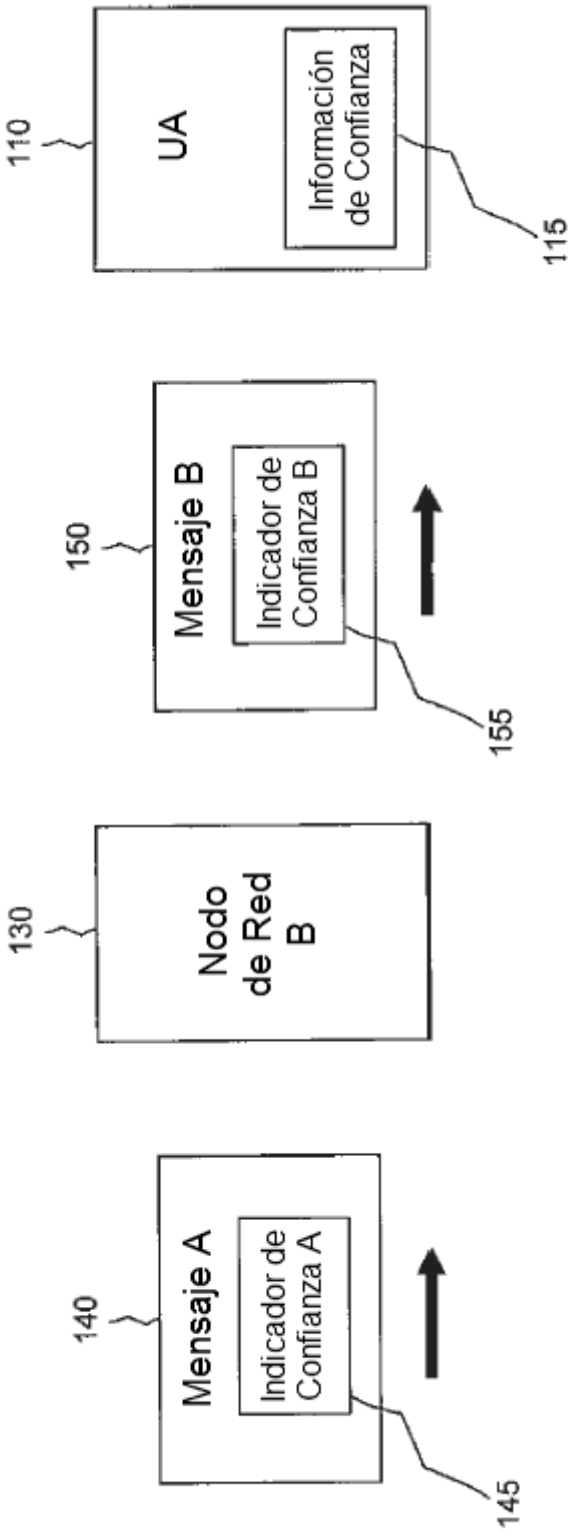
110
UA
Información de Confianza
115
150
Mensaje B
Indicador de Confianza B
155
130
Nodo de Red B
140
Mensaje A
Indicador de Confianza A
145

Figura 1

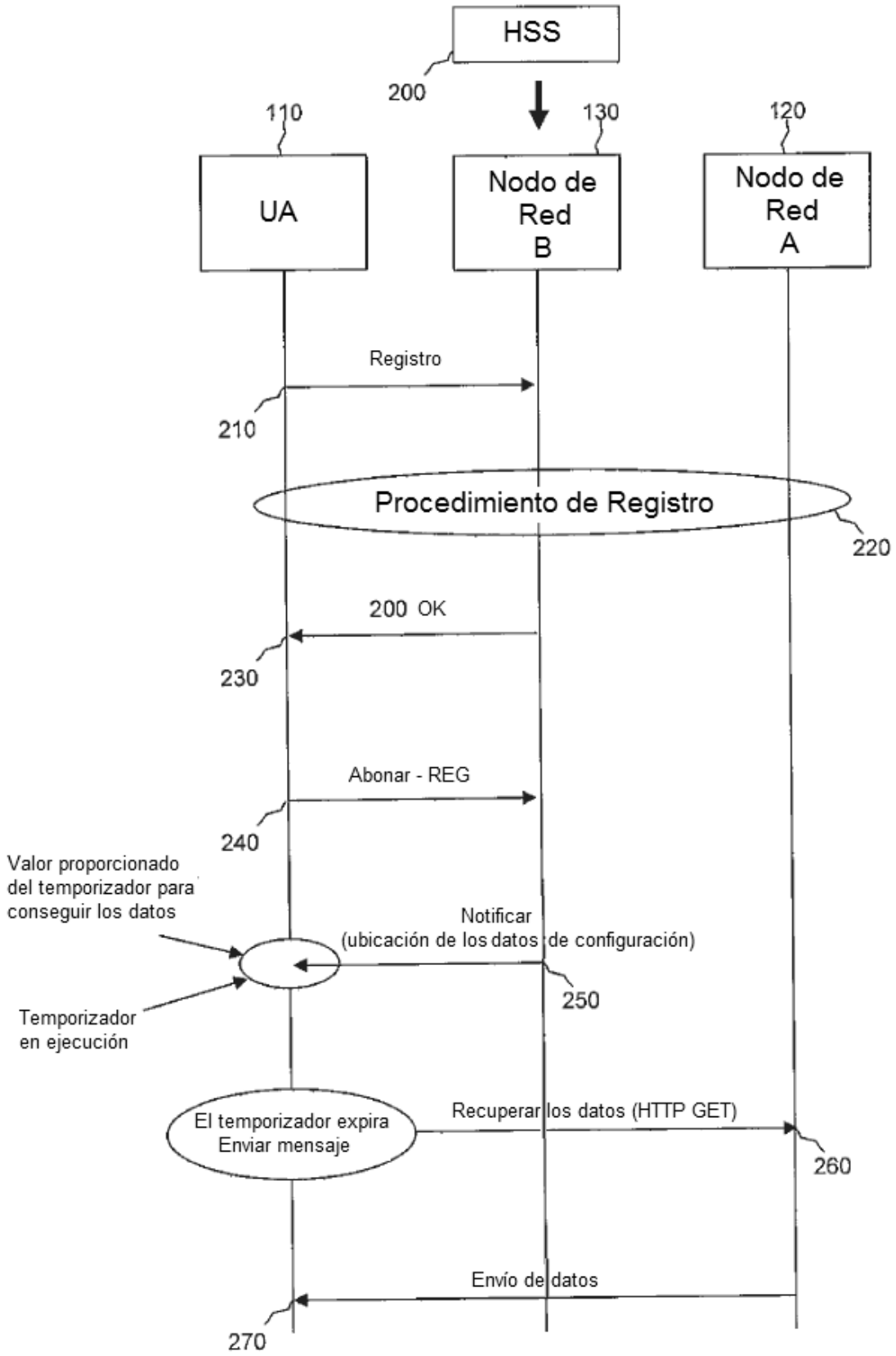
HSS
200
110
130
120
UA
Nodo de Red B
Nodo de Red A
Registro
210
Procedimiento de Registro
220
200 OK
230
Abonar - REG
240
Valor proporcionado del temporizador para conseguir los datos
Notificar (ubicación de los datos de configuración)
250
Temporizador en ejecución
El temporizador expira Enviar mensaje
Recuperar los datos (HTTP GET)
260
Envío de datos
270

Figura 2

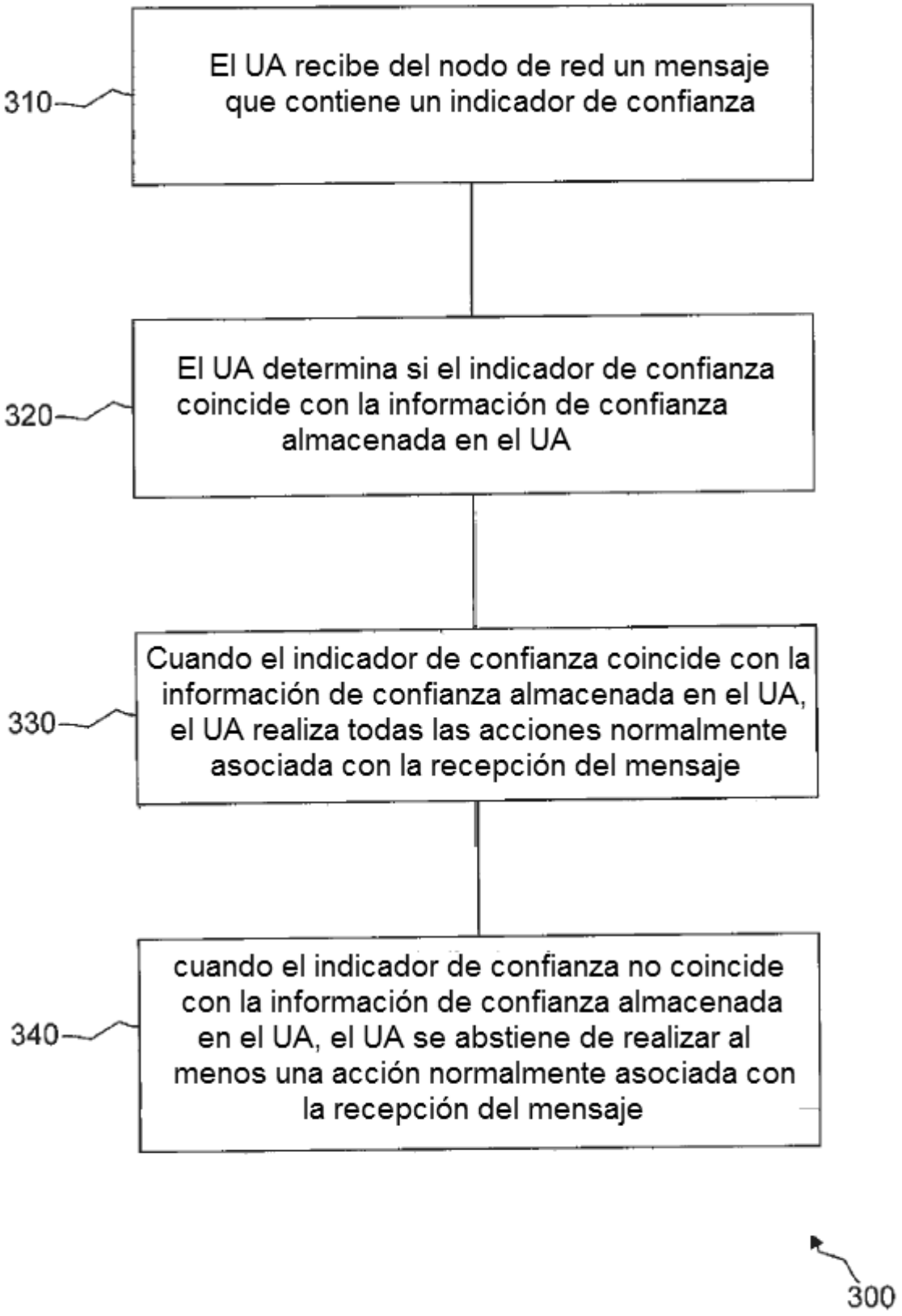
El UA recibe del nodo de red un mensaje que contiene un indicador de confianza
310
El UA determina si el indicador de confianza coincide con la información de confianza almacenada en el UA
320
Cuando el indicador de confianza coincide con la información de confianza almacenada en el UA, el UA realiza todas las acciones normalmente asociada con la recepción del mensaje
330
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
340
300

Figura 3

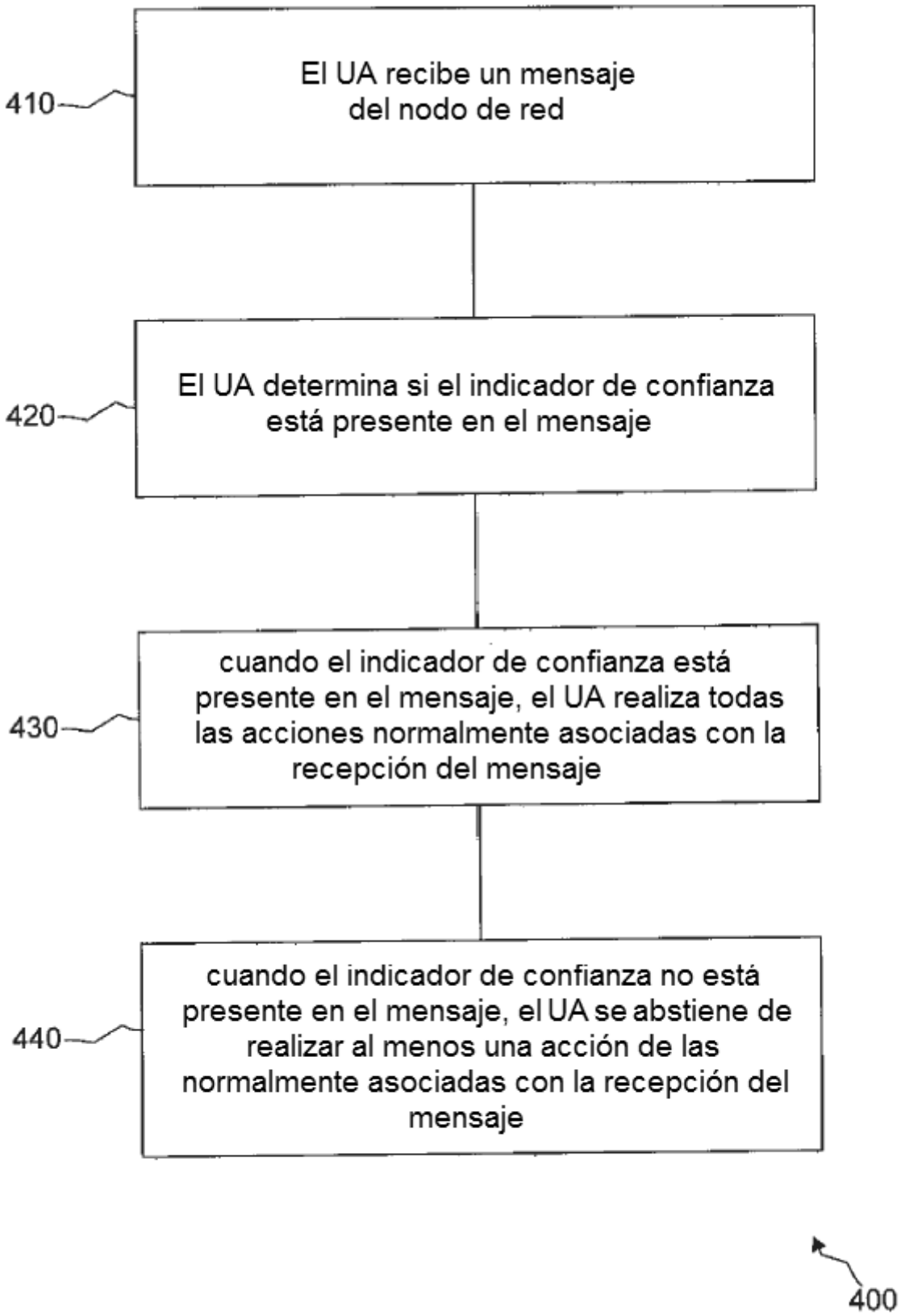
El UA recibe un mensaje del nodo de red
410
El UA determina si el indicador de confianza está presente en el mensaje
420
cuando el indicador de confianza está presente en el mensaje, el UA realiza todas las acciones normalmente asociadas con la recepción del mensaje
430
cuando el indicador de confianza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

Figura 4

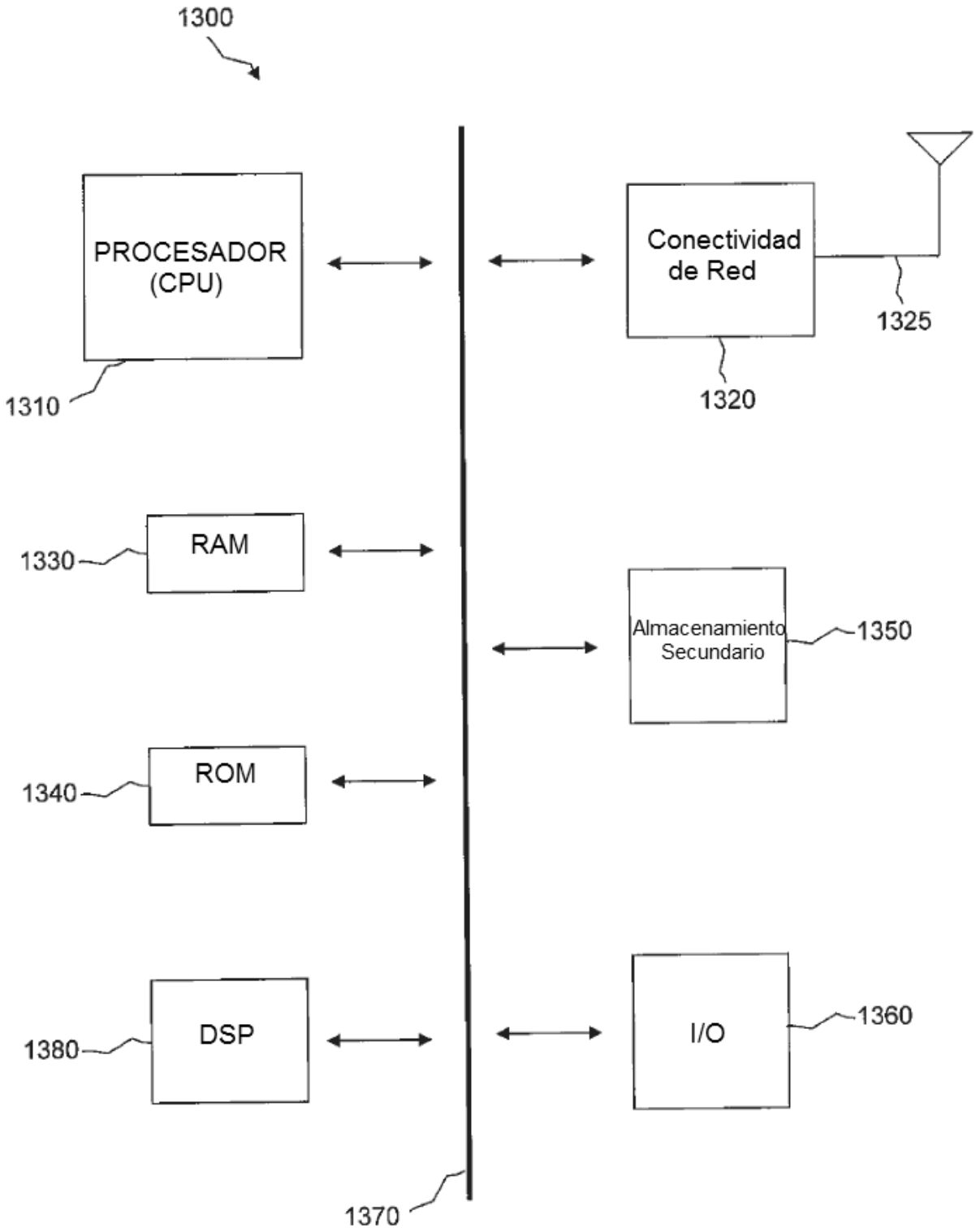
1300
PROCESADOR (CPU)
1310
Conectividad de Red
1320
1325
RAM
1330
Almacenamiento Secundario
1350
ROM
1340
DSP
1380
I/O
1360
1370

Figura 5