(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 510 715**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.12.2006 E 06841195 (8)**

(97) Fecha y número de publicación de la concesión europea: **06.08.2014 EP 2095595**

(54) Título: **Proxy IP móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.10.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
126 25 Stockholm, SE

(72) Inventor/es:

ROMMER, STEFAN y
TURÁNYI, ZOLTÁN RICHÁRD

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Proxy IP móvil

Campo técnico

La presente invención se refiere a una solución IP Móvil y en particular a una solución para manejar una red intermediaria en un entorno IP Móvil.

Antecedentes de la invención

Un tema "caliente" en la evolución de las comunicaciones fijas y móviles es el múltiple acceso, es decir, la capacidad de acceder al mismo conjunto de servicios a través de múltiples tecnologías de acceso. Las tecnologías de acceso posibles incluyen ambos accesos definidos por 3GPP (2G, 3G, LTE) y tecnologías no definidas por 3GPP (por ejemplo, WLAN, WiMAX, DSL). Un aspecto particular de acceso múltiple es la continuidad de la sesión, es decir, la capacidad para que el usuario se mueva entre diferentes tecnologías de accesos sin interrumpir una sesión de servicio en curso.

Una tecnología importante para permitir la continuidad de sesión es IP Móvil (MIP). MIP permite que el terminal utilice una dirección IP estable (llamada Dirección de origen), independientemente de su punto de conexión actual (PoA) a Internet. El terminal también utilizará direcciones IP locales (así denominadas las direcciones implícitas) que representa el PoA actual del terminal. IP Móvil oculta estas direcciones locales de las aplicaciones que funcionan en el terminal.

El caso típico con accesos 3GPP es que el Operador Móvil (MO) es propietario de los accesos (red de radio) y tiene relación con los clientes finales (suscriptores). Con los accesos distintos de 3GPP como por ejemplo WLAN y WiMAX, es probable que el Operador Móvil no sea dueño de todas las redes de acceso. En cambio, el MO hará acuerdos comerciales con los proveedores de red de acceso (por ejemplo. Operadores de hotspot (sitios de conexión) de WLAN) que permiten que los suscriptores del MO accedan a los servicios de MO también por accesos distintos de 3GPP.

Estos aspectos comerciales también tienen consecuencias en el escenario de itinerancia. En un escenario de itinerancia 3GPP, como se muestra en la Fig. 1, sólo dos operadores están involucrados; un operador visitado 2 y un operador de origen 3. En la itinerancia en acceso distinto de 3GPP, tres entidades comerciales pueden estar involucradas; proveedor de acceso distinto de 3GPP 1, operador visitado 2 y operador de origen 3. En este caso, existen acuerdos comerciales 7 entre el operador visitado y de origen, así como Entre el operador visitado y proveedor de acceso distinto de 3GPP, pero no entre el operador de origen y el proveedor de acceso distinto de 3GPP.

El término " Proxy IP Móvil " se ha utilizado antes en diferentes contextos:

- Proxy MIP como un medio para apoyar MIPv4 trasversal a través de puertas VPN. El Proxy MIP está aquí siempre que se utiliza junto con una puerta VPN.

- Un protocolo para extender MIPv6 para eliminar sus dependencias de capa de enlace en el Enlace de origen y distribuir las Has en el nivel IP. Un proxy MIP se introduce para la Gestión de Movilidad Local y Optimización de Ruta.

El Proxy MIP está en las referencias mencionadas utilizadas para otros fines y con diferentes procedimientos que el Proxy MIP propuso en esta invención. En consecuencia, las referencias citadas no serán tomadas como técnica anterior.

En el modelo de tres redes, la señalización del plano de control 4 tal como una señalización de autenticación de usuario será retransmitida típicamente (con proxy) por la red visitada (VN) 2. Esto es, en muchos casos requerido ya que la red de acceso distinto de 3GPP 1 no podrá saber cómo encontrar la red de origen 3 y viceversa. Esto es consecuencia de que no existe un acuerdo mutuo o configuración de interconexión entre las dos redes

Sin embargo, no está claro si y cómo el Plano de usuario (UP) 5 será retransmitido por la red visitada (intermediaria) 2. Las razones para retransmitir el tráfico a través de la VN es permitir que el operador de VN tenga control sobre el tráfico de usuarios, por ejemplo, para la carga, aplicación de políticas, intercepción legal, etc. El plano de usuario puede ser derivado entre la red de acceso 1 y la red de origen 3 sin la participación de la red visitada 2. En este escenario es imposible que el operador de red visitada controle el tráfico y maneje los servicios antes mencionados.

El protocolo de IP Móvil controla la movilidad y enrutamiento UP entre el terminal y la red de origen, pero no ayuda aquí. IP Móvil en su forma básica sólo tiene soporte para dos niveles de red:

1. Red de acceso (con Router de Acceso, Agente foráneo)

2. Red de origen (con Agente de origen)

IP Móvil establece un túnel UP entre la MN o agente externo en la red de acceso y el agente de origen en la red de origen. En MIP de ese modo no hay noción de una red visitada. En cambio, el tráfico de UP será enrutado utilizando mecanismos de enrutamiento IP regulares entre la red de acceso y la red de origen.

Hay diferentes posibilidades existentes (o futuras) para forzar el tráfico UP a través de VN. Se debaten brevemente a continuación:

Enfoques basados en el terminal.

IP Móvil Jerárquica (HMIP) es una extensión del MIP que se puede utilizar para introducir un nivel intermedio, por ejemplo, en la NW visitada. Un problema con HMIP es sin embargo que se requiere la funcionalidad HMIP en el terminal. Esto aumentará la complejidad y posiblemente el costo del terminal.

Un MN túnel IPSec entre MN y VN se puede utilizar como una alternativa. También esta solución tiene un impacto significativo en el terminal.

Enfoques de Túnel / ruta estática.

Otras alternativas para forzar el tráfico a través de la VN son configurar rutas estáticas o túneles estáticos entre la red de acceso y VN, así como entre VN y HN. Un inconveniente de estas alternativas es que ponen requerimientos sobre la red de acceso distinta de 3GPP. Debido a que el MO no posee y opera el acceso distinto de 3GPP, esto es beneficioso si se evitan los requerimientos específicos de MO en el acceso distinto de 3GPP. El proveedor de acceso distinto de 3GPP puede ser además una entidad muy "pobre" (por ejemplo, proveedor de hotspot de WLAN en una cafetería), lo que lo hace técnica y financieramente difícil requerir características específicas de MO.

Esquemas de movilidad en base a la red

Podrían utilizarse esquemas de movilidad basados en NW tal como proxy MIP (PMIP) y NETLMM. Esta alternativa pone incluso requisitos más exigentes en la NW de acceso distinto de 3GPP ya que debe tener soporte para el protocolo de movilidad basado en NW. También será difícil usar esta alternativa para tecnologías de acceso que ya utilizan por ejemplo, PMIP para la movilidad entre accesos. Los dos usos de los esquemas de movilidad entonces deben estar alineados (si es posible).

El documento US 2003/0224788 A1 divulga un procedimiento y un aparato para el registro de un nodo móvil en un agente de origen. Un proxy IP Móvil se utiliza para informar al nodo móvil si el nodo móvil es una red interna o una red remota. El nodo móvil envía un pedido de registro. Desde el pedido de registro, el proxy IP Móvil determina si el nodo móvil se encuentra en la red interna o en una red remota. Si el nodo móvil está en una red remota, el proxy IP Móvil actúa como intermediario, creando túneles a la dirección implícita y el agente de origen. De lo contrario, el proxy IP Móvil puede permitir que el nodo móvil y el agente de origen se comuniquen entre sí sin utilizar el proxy IP Móvil como intermediario

Compendio de la invención

La función de un "Proxy IP Móvil" se introduce en la red visitada (intermedia). El Proxy MIP introduce un nivel intermedio en la jerarquía que permite que el tráfico de UP sea siempre retransmitido a través de la red visitada. La señalización IP Móvil es modificada de tal manera que el túnel MIP UP es dividido en dos partes;

1) Entre MN / FA y MIP Proxy, y

2) Entre MIP Proxy y HA

El objetivo del Proxy MIP es asegurar que el tráfico en túnel con MIP siempre esté tunelizado a través de la red visitada. Esto le dará al operador visitado un aumentó en el control de la UP, por ejemplo, para la carga, control de políticas e intercepción legal. La invención se puede aplicar tanto a IP Móvilv4 como a IP Móvilv6

La invención se realiza en una serie de aspectos.

Un sistema de acuerdo a la reivindicación 1.

Otro aspecto de la presente invención es un procedimiento de acuerdo a la reivindicación 6.

Las realizaciones se definen en las reivindicaciones dependientes.

Las ventajas de la invención en comparación con las soluciones existentes incluyen

- Ningún impacto en el terminal.
    - La alternativa HMIP requiere soporte del terminal.
- No hay impactos sobre las redes de acceso distintas de 3GPP.

- La configuración que utiliza túneles y/o configuraciones de enrutamiento específicas entre el acceso NW y VN requiere funcionalidad en la red de acceso.

- Fácil de activar dinámicamente.

  - El uso del MIP Proxy puede ser controlado dinámicamente por la VN y/o HN en función de cada sesión en la configuración de la sesión.

  - Las alternativas de túnel estático y HMIP son difíciles (¿imposibles?) de utilizar en función de cada sesión.

- Ningún overhead de plano de usuario

  - Los enfoques de túneles estáticos y HMIP proporcionan overhead de tunelación UP

Estos y otros aspectos de la invención serán evidentes a partir de y se deducirán con referencia a las realizaciones descritas a continuación.

Breve descripción de los dibujos

A continuación, la invención se describirá de una manera no limitativa y con más detalle con referencia a las realizaciones ejemplares ilustradas en los dibujos adjuntos, en los cuales:

La Fig. 1 ilustra esquemáticamente una situación de red típica de acuerdo a tecnología conocida;

La Fig. 2 ilustra esquemáticamente una arquitectura de red de acuerdo a la presente invención;

La Fig. 3 ilustra esquemáticamente una situación de red de acuerdo a la presente invención;

La Fig. 4 ilustra esquemáticamente un esquema de señalización de acuerdo a una realización de la presente invención;

La Fig. 5a y b ilustra esquemáticamente esquemas de señalización de acuerdo a otras dos realizaciones de la presente invención para IP Móvilv4;

La Fig. 6 ilustra esquemáticamente un esquema de señalización de acuerdo a otra realización de la presente invención para IP Móvilv6;

La Fig. 7 ilustra esquemáticamente un dispositivo de infraestructura de acuerdo a la presente invención.

Descripción detallada de las realizaciones preferentes

En la Fig. 2, el número de referencia 200 en general indica una red de telecomunicaciones de acuerdo a la presente invención. La red comprende en este caso tres partes diferentes de la red: red de origen 201 (HN), red visitada 202 (VN), y red de acceso 203 (AN). Un nodo de visita, se refiere a menudo como un nodo móvil (MN), por ejemplo, una estación móvil 209 o laptop 210 o algún otro equipo de usuario (UE) se comunica con la red de acceso 203 a través de alguna de las interfaces inalámbricas, por ejemplo, GPRS, UMTS, WCDMA o interfaz similar compatible con los protocolos de comunicación basada en paquetes. En la presente invención una puerta de acceso (por ejemplo, un router de acceso o punto de acceso) 208 (AR), ubicado en una red de acceso 203 conecta el UE a la red 200. La puerta de acceso 208 a su vez está conectada a un proxy de IP Móvil (MIP) a su vez conectado a un agente de origen 205 (HA) en la red de origen 201. El proxy MIP tiene comunicación con un Servidor AAA 206 (vAAA) en la red visitada 202 para manejar los servicios de autenticación, autorización y cómputo dentro de la red 200 en relación con la sesión de comunicación. Además, el agente de origen tiene comunicación con un Servidor AAA 204 (HAAA) dentro de la red de origen para los mismos fines. Estos Servidores AAA se utilizan por ejemplo para la autenticación del usuario, manejo de asuntos de facturación, comunicarse cuyos servicios están disponibles para un usuario determinado y así sucesivamente como lo aprecia la persona experta en la técnica. En MIP versión 4, el UE puede comunicarse con un agente foráneo (FA), que en este caso sería, por ejemplo, la puerta de acceso 208; sin embargo, debe entenderse que otras partes (no mostradas) de la red de acceso pueden actuar como agentes foráneos. El concepto de FA no se utiliza para redes versión 6 de MIP.

Con el fin de garantizar que el tráfico UP sea enrutado a través de la VN, el MIP Proxy se introduce en el VN.

El MIP Proxy 207 es un control de plano (CP) y el proxy de plano de usuario (UP) para la señalización relacionada con MIP y túneles UP. Este esencialmente actúa como un HA con respecto al UE 209, 210 y un UE con respecto al HA 205. Un objetivo de la solución de proxy MIP es hacer que sea transparente para el UE 209, 210. Dependiendo de la aplicación alternativa, el MIP Proxy también podría ser transparente para el HA. Cabe sin embargo tener en cuenta que el operador de origen puede querer saber si un MIP Proxy se utiliza en el VN y por ello la transparencia con respecto al HN puede no desearse.

La Fig. 3 muestra un ejemplo de red de acuerdo a la presente invención con un nodo móvil (MN) 306 que se

comunica con una red de acceso 301 y un primer router de conexión intermedia 307. La red de acceso está en contacto con una red de origen 303 con un agente de origen (HA) 309 directamente o a través de una red visitada 302 con un proxy MIP 308 que actúa como nodo intermediario. Dos situaciones son plausibles en este escenario: dos diferentes túneles MIP de plano de usuario (UP) se pueden establecer: un túnel 305 directamente al HA 309 si no hay proxy MIP 308 en la red visitada y un túnel 304 al HA 309 a través del proxy MIP 308 si este está instalado en la red visitada 302.

Para que el UP con túnel a MIP sea retransmitido a través del proxy MIP 308, el MN 306, el MIP Proxy 308 y el HA 309 necesitan ser configurados con los valores apropiados para la dirección de origen, dirección IP HA, y la dirección implícita (CoA).

La dirección IP HA necesita ser configurada de la siguiente manera:

- El MN tendrá dirección IP HA establecida en la dirección IP MIP Proxy
- El MIP Proxy tendrá dirección IP HA establecida en la dirección IP HA real.

Con el fin de registrar la CoA correcta en el MIP Proxy y HA, un MIP RRQ/BU (Pedido de Registro / Actualización de Vinculación) se envía primero desde el MN al MIP Proxy. El valor CoA en este RRQ / BU es

- CoA = Dirección IP local de UE o dirección IP FA.

El MIP Proxy modifica el RRQ / BU de la siguiente manera

- CoA = dirección IP MIP Proxy

El MIP Proxy realiza funciones de seguridad de acuerdo con una alternativa como se debatirá más adelante en este documento y después reenvía el RRQ / BU al HA.

La MN y MIP Proxy necesitan ser configurados con la dirección IP HA adecuada y un flujo de mensajes de señalización ilustrativo se muestra en la Fig. 4. Una posibilidad de resolver esto es utilizar la señalización AAA durante la autenticación de acceso para asignar HA, por ejemplo, la señalización de AAA a través de un protocolo de radio o diámetro. La HN asignará la dirección IP HA en la respuesta de AAA enviada a la MN. Debido a que la señalización AAA para la autenticación de acceso típicamente es retransmitida a través de la VN, la VN puede extraer la dirección IP HA del mensaje AAA y reemplazarla por la dirección IP MIP Proxy. El mensaje AAA se envía entonces a la red de acceso. Debe tenerse en cuenta que la solución bootstrapping debatida anteriormente no es la única solución posible. También otros procedimientos de bootstrapping son posibles, por ejemplo, utilizando registros de servicio DNS.

La idea básica con el MIP Proxy es que el túnel UP entre MN/FA y HA sea enrutado a través del MIP Proxy. El MIP Proxy necesita modificar la dirección IP de origen y destino de la cabecera IP del túnel de cada paquete IP.

IP Móvil requiere una Asociación de Seguridad en Movilidad (MSA) entre MN y HA. La MSA se utiliza para proteger los mensajes de señalización MIP que se envían entre MN y HA. El MIP Proxy se introduce en el paso entre MN y HA y las consecuencias que esto tiene para la seguridad deben ser tratadas. Diferentes soluciones alternativas son posibles dependiendo de la versión IP Móvil (v4 o v6) que se use y qué tipo de solución de seguridad se utiliza para esa versión MIP. Tres escenarios diferentes se debaten a continuación.

MIPv4 utiliza campos de autenticación en los mensajes de señalización MIP para proteger el contenido. Los campos de autenticación se calculan sobre la base de una clave que se comparte entre MN y HA. El MIP Proxy no puede modificar el mensaje de señalización sin también recalcular la extensión de autenticación.

Dos opciones son posibles:

1a) Autenticación delegada con claves fijas

Esta situación se ilustra esquemáticamente en la Fig. 5a donde se muestra un ejemplo de flujo de mensajes. El cálculo de las extensiones de autenticación por HA es delegado a MIP Proxy. El MIP proxy recibe las claves necesarias de la HN, por ejemplo, utilizando señalización AAA. El MIP proxy puede, en base a las claves recibidas, comprobar las extensiones de autenticación recibidas de la MN y HA. El MIP Proxy también puede calcular nuevas extensiones de autenticación para los mensajes que reenvía hacia el MN o HA. Esta alternativa es transparente para el MN, es decir, el MN no ve el MIP proxy; lo percibirá como es comunicándose con HA directamente.

La señalización entre MN y MIP Proxy es así protegida en la forma regular utilizando extensiones de autenticación MIP. La señalización entre MIP Proxy y HA o bien se puede proteger utilizando extensiones regulares de autenticación MIP, y/o por ejemplo, mediante túneles IPSec entre VN y HN.

1b) Autenticación delegada con claves temporales

Esta situación se ilustra esquemáticamente en la Fig. 5b donde se muestra un ejemplo de flujo de mensajes. El HN

puede no querer enviar las claves fijas compartidas entre MN y HN a la VN. En lugar de ello, puede ser mejor crear claves temporales MN-HA y MN-AAA en forma dinámica que se envían a la VN. Esta alternativa requiere que tanto el MN como la HN puedan derivar las mismas claves temporales. El algoritmo exacto para derivar las claves no se aborda aquí. Las claves temporales MN-HA y MN-AAA se envían al MIP Proxy durante el proceso de registro.

Además de utilizar claves temporales en esta alternativa, la protección real de los mensajes se realiza en la misma manera que en la alternativa 1 a.

La Fig. 6 ilustra esquemáticamente una realización de la presente invención para MIP versión 6 en la que se muestra un ejemplo de flujo de mensajes. IP Móvilv6 utiliza en su especificación original IPSec para proteger la señalización. Una posibilidad en este caso es dejar que la protección IPSec específica de MIP sólo cubra los mensajes enviados entre MN y MIP Proxy. La señalización entre VN y HN podría ser protegida de acuerdo a cierto acuerdo entre operadores. Además esta protección podría, por supuesto, utilizar IPSec

Las credenciales de seguridad (llaves, etc.) necesarias para establecer la Asociación de Seguridad IP entre MN y proxy MIP se envían desde la HN a la VN utilizando por ejemplo protocolos AAA.

RFC 4285 (es decir, IETF, la Fuerza de Tareas de Ingeniería de Internet, Solicitud de Comentario No. 4285: Protocolo de autenticación pata IP Móvilv6) proporciona un procedimiento de Autenticación alternativo para MIPv6. Este procedimiento es similar al Procedimiento de Autenticación MIPv4. El mismo tipo de alternativas de seguridad como se describe para la alternativa 1 (A y B) es por lo tanto posible también aquí. Tenga en cuenta que la terminología para los parámetros de autenticación, campos, claves, etc. difiere entre MIPv4 y MIPv6 utilizando RFC 4285.

Se supone que se utiliza un túnel inverso con MIPv4. El MIP Proxy no será capaz de asegurar que el tráfico de enlace ascendente sea enrutado a través de la VN si se utiliza enrutamiento triangular. Esto sin embargo no debe considerarse una limitación en los escenarios relevantes, ya que un Operador Móvil (MO) lo más probable es que requiera túnel inverso para ser utilizado, por ejemplo para permitir la carga, aplicación de políticas y intercepción legal en la red de origen. }

Para MIPv6 se supone que todo el tráfico es tunelizado a través del Agente de origen. El MIP Proxy no será capaz de asegurarse de que el tráfico sea enrutado a través de la VN si se utiliza la optimización de rutas MIPv6. Por otro lado, el MIP proxy puede iniciar la optimización de ruta en nombre del MN utilizando su dirección como dirección implícita.

La solución mencionada anteriormente se puede implementar en una serie de nodos de infraestructura como conjuntos de instrucciones en el software. La Fig. 7 ilustra en un diagrama de bloques esquemático un nodo de infraestructura (por ejemplo, un nodo de soporte, por ejemplo un GGSN o SGSN) de acuerdo a la presente invención, en el que una unidad de procesamiento 701 maneja datos de comunicación e información de control de comunicación. El nodo de infraestructura 700 además comprende una unidad de memoria volátil (por ejemplo RAM) 702 y/o no volátil (por ejemplo un disco duro o un disco flash) 703, y una unidad de interfaz 704 para la conexión de los comandos de control de un administrador del nodo. El nodo de infraestructura 700 puede comprender además una unidad de comunicación corriente abajo 705 y una unidad de comunicación corriente arriba 706, cada una con una interfaz de conexión respectiva. Todas las unidades en el nodo de la infraestructura pueden comunicarse entre sí directamente o indirectamente a través de la unidad de procesamiento 701. Software para manejar la comunicación hacia y desde los nodos móviles conectados a la red se ejecuta al menos en parte en este nodo y puede ser almacenado en el nodo, sin embargo, el software también puede cargarse dinámicamente en el arranque del nodo o en una etapa posterior, por ejemplo, durante un intervalo de servicio. El software se puede implementar como un producto de programa de computadora y puede ser distribuido y/o almacenado en medios legibles por computadora, por ejemplo disquete, CD (disco compacto), DVD (disco de vídeo digital), medio flash o medios de memoria removible similar (por ejemplo, CompactFlash, SD Secure Digital, Memory Stick, miniSD, tarjeta de multimedia MMC, SmartMedia, TransFlash, XD), HD-DVD (DVD de alta definición), o DVD Bluray, medios de memoria extraíble basados en USB (Conductor Universal en Serie) , medios de cinta magnética, medios de almacenamiento óptico, medios magneto-ópticos, memoria burbuja, o distribuidos como una señal propagada a través de una red (por ejemplo, Ethernet, ATM, ISDN, PSTN, X.25, Internet, red de área local (LAN) o redes similares capaces de transportar paquetes de datos al nodo de infraestructura).

Cabe señalar que la palabra "comprende" no excluye la presencia de otros elementos o etapas distintas de las enumeradas y las palabras "un" o "una" precediendo a un elemento no excluyen la presencia de una pluralidad de tales elementos. La invención puede al menos en parte ser implementada en software o hardware. Además, debe tenerse en cuenta que cualquier signo de referencia no limita el alcance de las reivindicaciones, y que varios "medios", "dispositivos", y "unidades" pueden estar representadas por el mismo artículo de hardware.

Las realizaciones anteriormente mencionadas y descritas sólo se dan como ejemplos y no deberían limitar la presente invención. Otras soluciones, usos, objetivos y funciones dentro del alcance de la invención según lo reivindicado en las reivindicaciones de patente que se describen a continuación deben ser evidentes para la persona experta en la técnica.

Definiciones

BA	Reconocimiento de vinculación (MIPv6)
BU	Actualización de vinculación (MIPv6)
CP	Plano de control
HA	Agente de origen
HMIP	IP Móvil Jerárquico
HN	Red de origen
IP	Protocolo de Internet
MIP	IP Móvil
MN	Nodo móvil (utilizado como sinónimo de UE)
MO	Operador móvil
RRP	Respuesta de registro (MIPv4)
RRQ	Pedido de registro (MIPv4)
UE	Equipo de usuario (utilizado como sinónimo de MN)
UP	Plano de usuario
VN	Red visitada

REIVINDICACIONES

1. Un sistema para su uso en una red visitada intermedia (202, 302) en una red de telecomunicaciones (200, 300) para controlar el tráfico de comunicación en la red visitada intermedia, comprendiendo el sistema un IP Móvil, MIP, proxy (207, 308, 700) para la comunicación entre una red de origen (201, 303) y un nodo de visita (209, 210, 306) que se comunica con una red de acceso (203; 301), comprendiendo además el sistema una autenticación, autorización, y cómputo, Servidor AAA (206), en el que:

- el servidor AAA (206) está dispuesto para modificar la señalización IP Móvil enviando, en un mensaje de respuesta AAA, como dirección temporaria de agente de origen una dirección IP del proxy MIP (207,308,700) al nodo de visita (209, 210, 306), y el proxy MIP (207,308,700) esta dispuesto para configurar una dirección de agente de origen del nodo de visita (209, 210, 306) a una dirección de un agente de origen actual (309) y configurar una Dirección implícita, CoA, del nodo de visita (209, 210, 306) a la dirección IP del proxy MIP (207,308,700), por lo que un túnel plano de usuario de IP Móvil (304) es dividido en dos partes, un túnel entre la red de acceso (203; 301) y el proxy MIP (207; 308), y otro túnel entre el proxy MIP (207; 308) y la red de origen (201; 303),

- el proxy MIP (207,308,700) además está dispuesto para comunicarse con el servidor AAA (206) para manejar los servicios de autenticación, autorización, y cómputo y para manejar asuntos de facturación relacionados con la comunicación en el túnel plano de usuario de IP Móvil (304) entre la red de origen (201, 303) y el nodo de visita (209, 210, 306), y el proxy MIP (207,308,700) además está dispuesto para retransmitir los paquetes del plano de usuario entre la red de origen (201, 303) y el nodo de visita (209, 210, 306) a través de la red de acceso (203, 301).

2. El sistema de acuerdo a la reivindicación 1, que además comprende medios para configurar la tabla de traducción utilizando una autenticación, autorización, y cómputo, AAA, señalización de protocolo.

3. El sistema de acuerdo a la reivindicación 1, en el que la función de traducción de dirección comprende una asignación de dirección implícita.

4. El sistema de acuerdo a la reivindicación 1, además dispuesto para obtener un nuevo código de autenticación y reemplazar con el código de autenticación obtenido, siendo retransmitidos los códigos de autenticación en los paquetes de plano de usuario que son retransmitidos.

5. El sistema de acuerdo a la reivindicación 4, además dispuesto para obtener un nuevo código mediante el cálculo de un nuevo código utilizando una de las claves fijas delegadas y claves temporarias delegadas obtenidas de la red de origen del nodo móvil.

6. Un procedimiento para controlar flujos de tráfico en una red de telecomunicaciones (200, 300), comprendiendo la red de telecomunicaciones (200, 300) una red visitada intermedia (202, 302) que comprende una IP Móvil, MIP, proxy (207, 308, 700) y una autenticación, autorización, y cómputo, Servidor AAA (206), comprendiendo el procedimiento:

- en el Servidor AAA (206), modificar la señalización IP Móvil enviando, en un mensaje de respuesta AAA, como dirección de agente de origen temporaria una dirección IP del proxy MIP (207,308,700) a un nodo de visita (209, 210, 306) que se comunica con una red de acceso (203, 301), y configurar, en el proxy MIP (207,308,700), una dirección de agente de origen del nodo de visita (209, 210, 306) a una dirección de un agente de origen actual (309) y configurar una dirección implícita, CoA, del nodo de visita (209, 210, 306) a la dirección IP del proxy MIP (207,308,700), por lo que un túnel plano de usuario de IP Móvil (304) es dividido en dos partes, un túnel entre la red de acceso (203 ; 301) y el proxy MIP (207, 308, 700) , y otro túnel entre el proxy MIP (207; 308) y una red de origen (201; 303),

- comunicación entre el proxy MIP (207, 308, 700) y el Servidor AAA (206) para manejar los servicios de autenticación, autorización, y cómputo y para manejar asuntos de facturación relacionados con la comunicación en el túnel plano de usuario de IP Móvil (304) entre la red de origen (201, 303) y el nodo de visita (209, 210, 306), y

- en el proxy MIP (207, 308, 700), retransmitir el tráfico del plano de usuario a través del proxy MIP entre la red de origen (201, 303) y el nodo de visita (209, 210, 306) a través de la red de acceso (203, 301).

7. El procedimiento de acuerdo a la reivindicación 6, que además comprende operar funciones de seguridad para la autenticación del nodo móvil.

8. El procedimiento de acuerdo a la reivindicación 7, en el que las funciones de seguridad incluyen una autenticación, autorización, y cómputo, AAA, protocolo, por ejemplo de acuerdo al Radio o Diámetro.

9. El procedimiento de acuerdo a la reivindicación 6, que además comprende: obtener un código de autenticación y reemplazar los códigos de autenticación en los paquetes de información de contenido siendo retransmitidos con el código de autenticación obtenido.

10. El procedimiento de acuerdo a la reivindicación 9, en el que obtener el código de autenticación incluye calcular un nuevo código utilizando una de las claves fijas delegadas y claves temporarias delegadas.

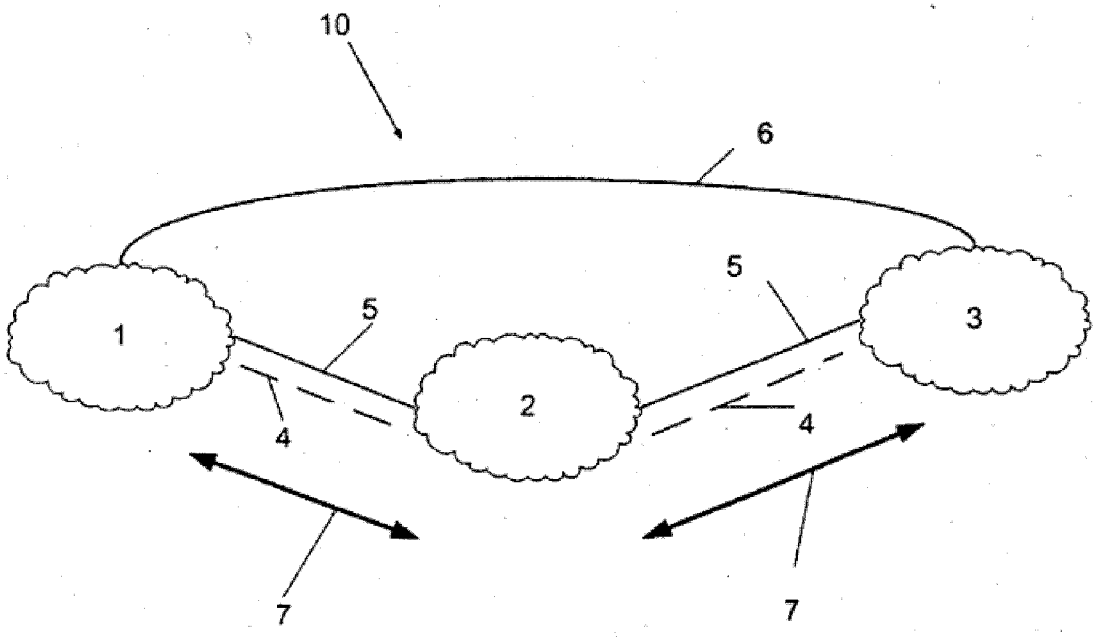

Fig. 1

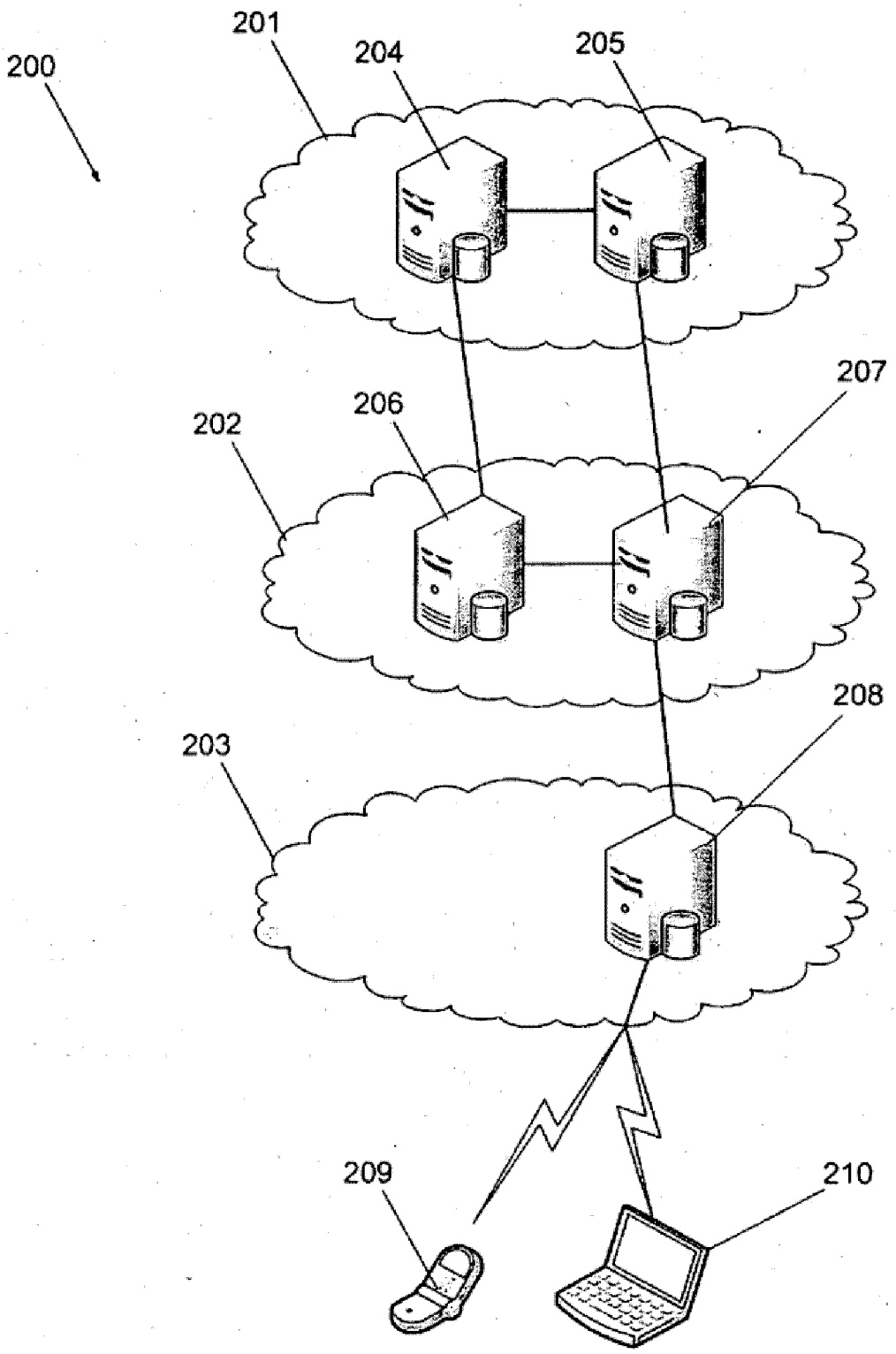

Fig. 2

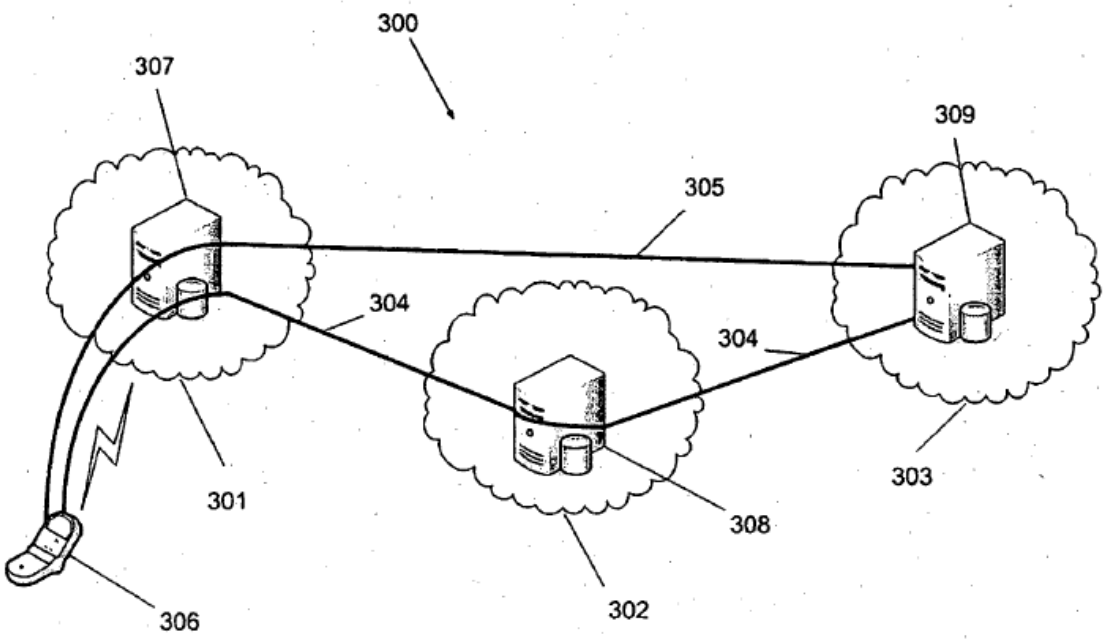

Fig. 3

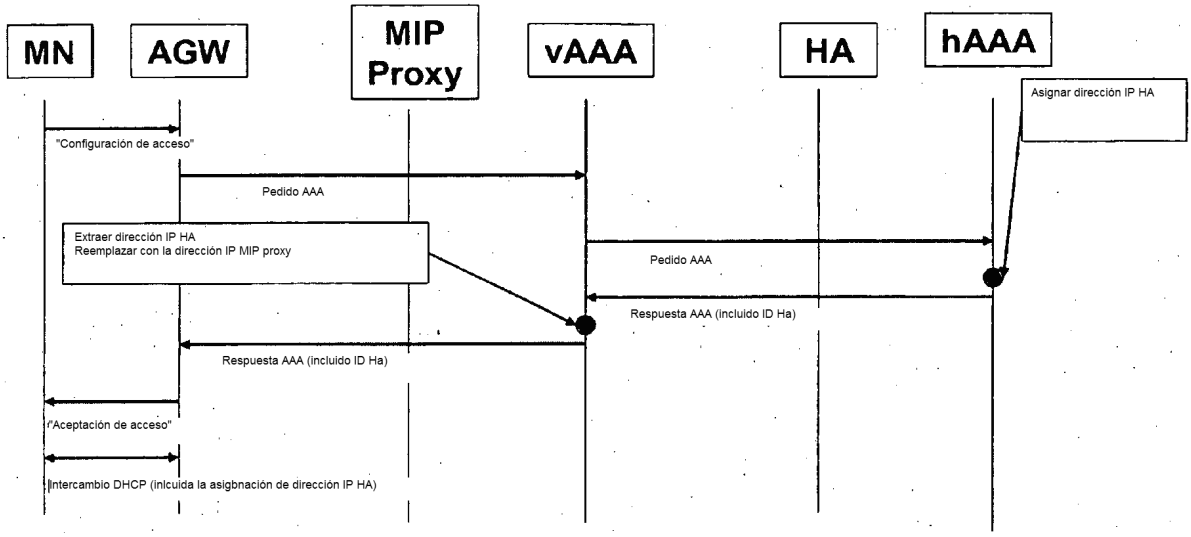
MN
AGW
MIP Proxy
vAAA
HA
hAAA
Asignar dirección IP HA
"Configuración de acceso"
Pedido AAA
Extraer dirección IP HA
Reemplazar con la dirección IP MIP proxy
Pedido AAA
Respuesta AAA (incluido ID Ha)
Respuesta AAA (incluido ID Ha)
"Aceptación de acceso"
Intercambio DHCP (inlcuida la asigbnación de dirección IP HA)

Fig. 4

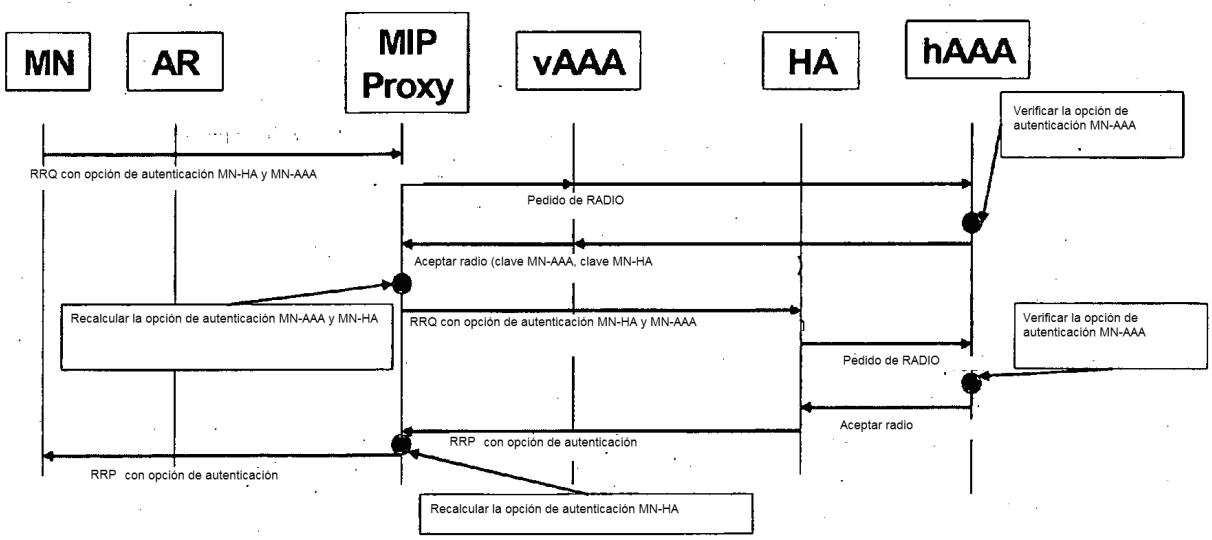
MN
AR
MIP Proxy
vAAA
HA
hAAA
Verificar la opción de autenticación MN-AAA
RRQ con opción de autenticación MN-HA y MN-AAA
Pedido de RADIO
Aceptar radio (clave MN-AAA, clave MN-HA
Recalcular la opción de autenticación MN-AAA y MN-HA
RRQ con opción de autenticación MN-HA y MN-AAA
Verificar la opción de autenticación MN-AAA
Pedido de RADIO
Aceptar radio
RRP con opción de autenticación
RRP con opción de autenticación
Recalcular la opción de autenticación MN-HA

Fig. 5a

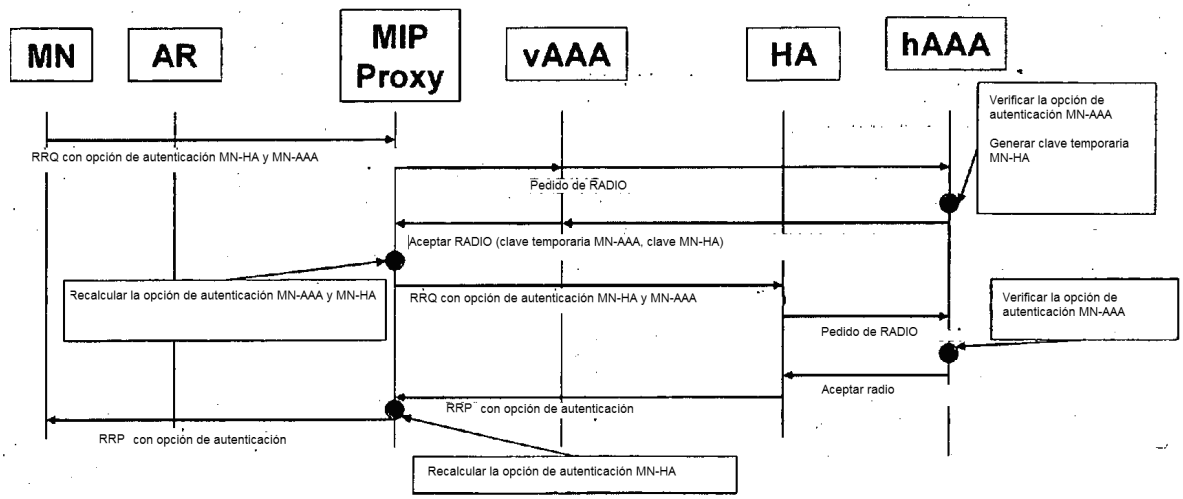
MN
AR
MIP Proxy
vAAA
HA
hAAA
Verificar la opción de autenticación MN-AAA
Generar clave temporaria MN-HA
RRQ con opción de autenticación MN-HA y MN-AAA
Pedido de RADIO
Aceptar RADIO (clave temporaria MN-AAA, clave MN-HA)
Recalcular la opción de autenticación MN-AAA y MN-HA
RRQ con opción de autenticación MN-HA y MN-AAA
Verificar la opción de autenticación MN-AAA
Pedido de RADIO
Aceptar radio
RRP con opción de autenticación
RRP con opción de autenticación
Recalcular la opción de autenticación MN-HA

Fig. 5b

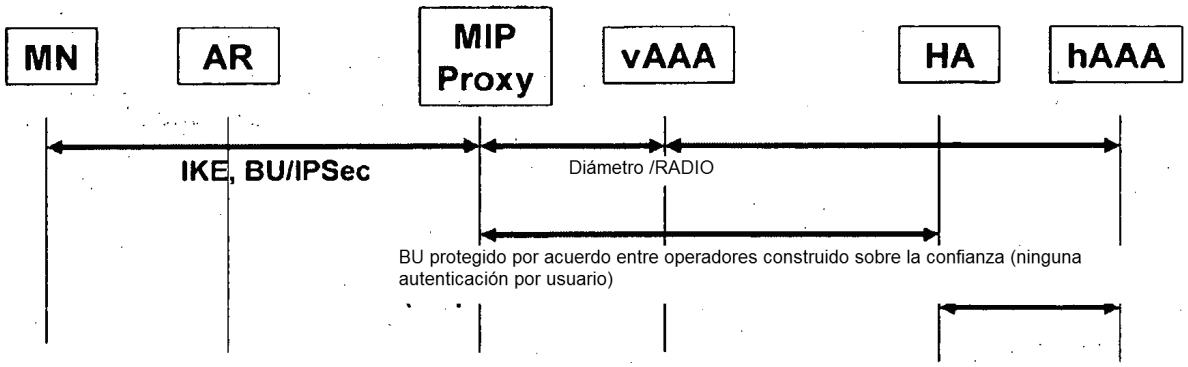
MN
AR
MIP Proxy
vAAA
HA
hAAA
IKE, BU/IPSec
Diámetro /RADIO
BU protegido por acuerdo entre operadores construido sobre la confianza (ninguna autenticación por usuario)

Fig. 6

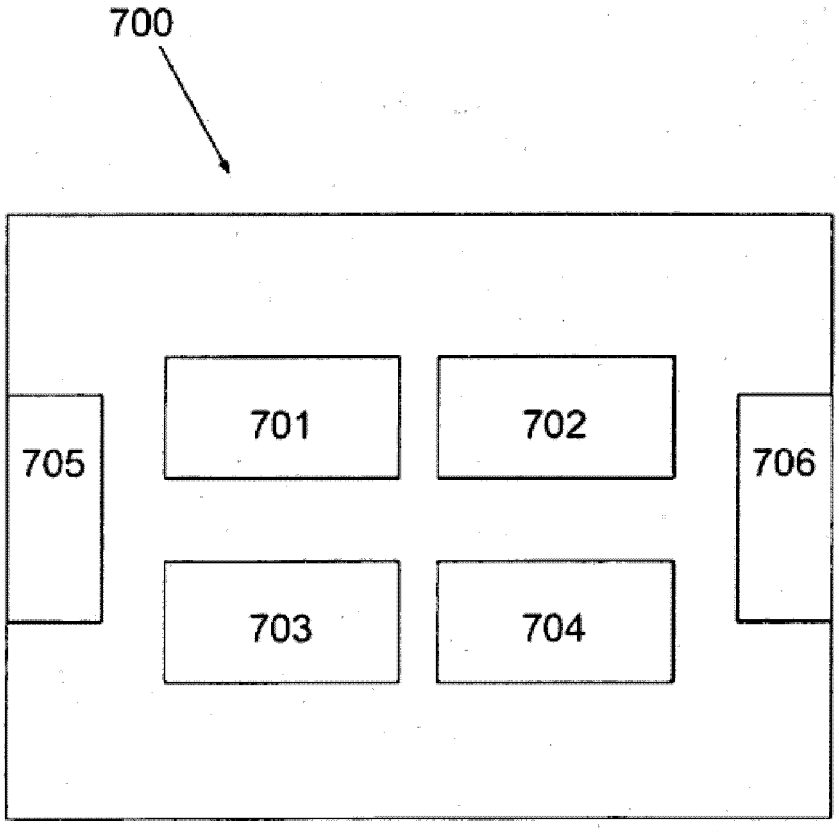

Fig. 7