(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 433 584**

(51) Int. CI.:

H04W 8/20 (2009.01)
H04L 29/08 (2006.01)
H04W 88/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.10.2010 E 10774257 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2013 EP 2491732**

(54) Título: **Punto de acceso inalámbrico**

(30) Prioridad:

19.10.2009 GB 0918217

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2013

(73) Titular/es:

UBIQUISYS LIMITED (100.0%)
The Stella Building, Windmill Hill Business Park, Whitehill Way, Swindon
SN5 6NX, GB

(72) Inventor/es:

WALKER, MARK y
HAILEY, IAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Punto de acceso inalámbrico

Esta invención se relaciona con un punto de acceso, y en particular con un punto de acceso inalámbrico para proporcionar servicios con base en ubicación y servicios con base en usuario a los dispositivos inalámbricos conectados.

En una red celular que comprende dispositivos de internet móviles (teléfonos y ordenadores con módems compatibles, en adelante MID) y baja energía, punto de accesos de la estación base interna (femtoceldas, en adelante AP), los MID y AP cada uno contiene una credencial de identidad inmutable y única. Esta identidad frecuentemente toma la forma de un SIM, pero puede ser un software certificado instalado antes de primer uso (es decir durante fabricación). La identidad se utiliza como una credencial de autorización durante el establecimiento de las capas inferiores de conectividad de red.

Para servicios de telefonía celular, esta identidad del MID también se utiliza comúnmente en la capa de aplicación, en donde tiene una asociación una a una con la identidad del llamante.

Para servicios de datos las identidades no se propagan a la capa de aplicación para por lo menos dos razones. En primer lugar, las redes IP se diseñan independientemente de la red celular con el fin de que la identidad del llamante no volátil no sea parte necesaria o esencial para establecer el servicio (solo se requiere una dirección de remitente para la sesión). En segundo lugar, las identidades se consideran sensibles por el operador de red debido a su función en autorizar acceso de red, y no es deseable propagarlas más allá de la red de telefonía en internet.

La presente invención describe cómo se pueden utilizar las credenciales de identidad dentro del MID y AP para proporcionar una "identidad del llamante" y "etiqueta de ubicación" respectivamente cuando el MID tiene acceso a servicios de datos por medio del AP.

Como el uso de internet se ha vuelto común, le permite a los usuarios tener acceso a contenidos que se puede almacenar en servidores alrededor del mundo, han habido intentos correspondientes para proporcionar servicios que son importantes en alguna forma para la ubicación del usuario.

Por ejemplo, cuando un usuario tiene acceso a internet, se puede utilizar su dirección IP para inferir alguna información acerca de la ubicación del usuario, y se pueden visualizar anuncios importantes para esta ubicación al usuario. Por ejemplo, el documento WO2006/031379 describe un sistema en el que se almacenan las ubicaciones geográficas en diversos puntos de acceso inalámbricos. Cuando un usuario tiene acceso a la red a través del punto de acceso inalámbrico, se puede utilizar la dirección IP para identificar el punto de acceso inalámbrico, y el sistema puede seleccionar visualizar los anuncios de usuario que se relacionan geográficamente con el punto de acceso inalámbrico. Durante la operación de red IP normal la red IP reasignará direcciones periódicamente, y pueden agrupar efectivamente direcciones (un proceso conocido como Traducción de Dirección de Red), las cuales limitan la resolución de los sistemas de ubicación con base en IP.

La publicación de patente de la técnica anterior WO 03/050743 A1, describe un servidor proxy que intercepta las solicitudes HTTP de una terminal móvil y los insertos y cabecera adicional con la identificación del usuario en una red celular que se utiliza por el proveedor de contenidos para determinar la identidad del usuario y para personalizar la prestación del servicio.

La publicación de patente de la técnica anterior US 2007/0099634 A1 describe un nodo de acceso en una red de nodos de acceso de red inalámbrica, que solicitan proxies HTTP al interceptarlos y agregar una etiqueta de ubicación para el servidor de destino.

Sin embargo, ninguno de los documentos de la técnica anterior mencionados propone realizar la inserción de los datos de identidad en un nodo (es decir una estación base celular) que tiene acceso directo para identificar tokens para autorización para acceder a la red celular.

La presente invención utiliza un único identificador inmutable asociado con cada punto de acceso inalámbrico de rango corto individual para proporcionar una etiqueta de ubicación que se puede utilizar para inferir la ubicación para la resolución de este radio cubrimiento de punto de acceso. Cuando el usuario tiene acceso a la red a través del punto de acceso el punto de acceso agrega automáticamente su etiqueta de ubicación a los datos enviados a través de la red. Luego, dependiendo de qué se ha almacenado según se asocia con la etiqueta de ubicación, la ubicación geográfica o el contexto (es decir "hogar, "oficina", "café") se pueden utilizar para seleccionar o modificar los datos regresados.

De forma similar, muchos servicios de internet le permiten al usuario crear una cuenta para personalizar el servicio. Esto requiere usualmente que los usuarios se identifiquen por sí mismos cuando acceden al servicio, tal como al ingresar un nombre de usuario, lo que puede ser incómodo en un dispositivo móvil con una interfaz limitada de usuario. La presente invención utiliza un único identificador inmutable asociado con cada dispositivo móvil para proporcionar una identidad para el propietario. Esta identidad es conocida por el punto de acceso debido a su uso en establecer la conexión de red, cuando el usuario tiene acceso a la red a través del punto de acceso, este agrega automáticamente la identidad del propietario a los datos enviados a través de la red, de tal manera que el usuario no necesita identificarlos por sí mismos utilizando la interfaz de usuario.

De acuerdo con la materia objeto reivindicada de la presente invención, se proporciona una estación base celular, configurada para permitir que un dispositivo se conecte a esta sobre a interfaz inalámbrica, en donde la estación base celular sea capaz de establecer una conexión a una red celular de tal manera que la red celular requiere un token de identidad para autorización, y en donde la estación base celular tiene una conexión a una Red de Área Extendida, de tal manera que puede enrutar el tráfico de datos de los dispositivos conectados a un servicio remoto sobre la Red de Área Extensa y, en el evento en que el tráfico de datos desde un dispositivo conectado está destinado al servicio remoto, el punto de acceso se adapta para insertar información derivada del token de identidad tomada en el tráfico de datos, y reenviar el tráfico de datos modificado al servicio remoto.

Sin embargo, un token de identidad con un uso existente en la red celular se puede reutilizar para proporcionar información de identidad al servicio remoto accesado sobre la Red de Área Extendida. El servicio remoto luego es capaz de proporcionar información que es relevante para esa identidad.

Para una mejor compresión de la presente invención, ahora se hará referencia, por vía de ejemplo, a los dibujos que acompañan, en los que:

La Figura 1 es un diagrama esquemático, que ilustra una parte de una red de comunicaciones de acuerdo con la presente invención.

La Figura 2 ilustra un esquema de flujo de mensajes en un método de acuerdo con la presente invención.

La Figura 3 ilustra ligeramente en más detalle el flujo de mensajes del método de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA

La Figura 1 muestra una parte de una red de comunicaciones móvil que opera de acuerdo con la presente invención.

Específicamente, la Figura 1 muestra un dispositivo de internet móvil 10, que es capaz de conectarse a una Red de Área Extensa 12 tal como internet a través de un punto de acceso 14.

La invención se describirá en más detalle con referencia específica al caso en donde el punto de acceso 14 es una estación base de femtocelda, y el dispositivo de internet móvil 10 puede ser un teléfono móvil u ordenador personal, que es capaz de comunicar utilizando un estándar de comunicaciones celular, tal como uno de los estándares de interfaz de aire asociado con el Sistema de Telecomunicaciones Móviles Universal (UMTS). Dichos dispositivos de internet móviles se conocen bien, y no se describirán adicionalmente aquí, excepto cuando sea necesario para una compresión de la presente invención.

La estación base de femtocelda es de un tipo que se conoce, y tiene una antena 16 para transmisión y recepción sobre la interfaz de aire apropiada, conectada el circuito de interfaz RF 18. Las señales recibidas se pasan a intercepción y los circuitos de enrutamiento 20, que operan bajo el control de un procesador 22: Como se conoce, la estación base de femtocelda 14 se conecta normalmente a internet 12 sobre una conexión de banda ancha existente 24 que sirve a las instalaciones en las que se ubica, y se puede conectar sobre internet 12 a la red núcleo 26 de la red de comunicaciones celular, administrada por el operador de red móvil.

La Figura 1 también muestra una estación base celular de macrocelda 28 conectada a la red núcleo 26. Se apreciará que la red celular contendrá normalmente muchas estaciones base celulares de macrocelda, que cubren un área extensa.

Cada estación base de femtocelda 14, por contraste, proporcionará el cubrimiento solo en un área pequeña, por ejemplo dentro de las instalaciones de un cliente. Sin embargo, dentro de aquellas instalaciones, la estación base de femtocelda 14 debe ser capaz de proporcionar cubrimiento más fuerte que la estación base de macrocelda de servicio. Un dispositivo móvil, tal como el dispositivo de internet móvil 10, que es activo en la red de comunicaciones celulares, es por lo tanto capaz de moverse entre las celdas de la red de macrocelda, y cualquier femtocelda que permita dicho acceso. Por ejemplo, una estación base de femtocelda que se ubica dentro de las instalaciones pequeñas o domésticas del cliente se puede configurar de tal manera que solo los dispositivos que se registran

específicamente por este cliente pueden obtener dicho acceso, aunque otros clientes pueden permitir a cualquier usuario de la red de comunicaciones celular obtener acceso.

El acceso a la red se controla con base en una credencial de identidad única e inmutable incorporada dentro del dispositivo de conexión. Esta credencial de identidad toma frecuentemente la forma de un Módulo de Identidad de Suscriptor (SIM), pero puede ser un software certificado instalado antes de primer uso (es decir durante fabricación). El dispositivo de internet móvil 10 contiene una identidad 30 (Identidad "A") en la que la red núcleo verifica contra su sistema de Autenticación, Autorización y Contabilización (AAA) 34 antes de otorgar acceso de red del punto de acceso 14 o la macrocelda 28. El punto de acceso de femtocelda contiene una identidad 32 (Identidad "B") que la red núcleo verifica contra su sistema AAA 34 antes de permitir al punto de acceso proporcionar conectividad a los dispositivos de internet móviles.

Como se mencionó anteriormente, la estación base de femtocelda 14 contiene circuitos de enrutamiento e intercepción 20, permitiéndole interrogar y modificar los mensajes enviados a y desde los dispositivos móviles que se conectan a este. Por ejemplo, la estación base de femtocelda 14 puede contener pilas de software dispuestas como se describe en el documento WO2008/102099, permitiéndole interceptar los mensajes enviados desde los dispositivos móviles conectados a este sobre un protocolo de comunicación inalámbrico celular, y luego le permite enrutar el tráfico según se requiera.

Los circuitos de enrutamiento e intercepción 20 así pueden interceptar sesiones de datos que implican el dispositivo móvil 10, y pueden determinar el mejor enrutamiento para dichas sesiones de datos. Por ejemplo, se puede enrutar una llamada de teléfono de vos sobre internet 12 en la red núcleo 26 en un punto adecuado, que permite conexión al teléfono llamado. Una solicitud para acceder a un sitio web se puede en su lugar enrutar directamente sobre el internet a un servidor 36 que aloja un sitio web, sin involucramiento de la red núcleo 26.

En el contexto de la presente invención, se puede hacer una distinción entre la función que la identidad 30 cumple cuando el dispositivo de internet móvil participa en servicios de telefonía y cuando participa en las sesiones de datos. En las redes móviles GSM y UMTS la identidad 30 es un SIM y la identidad primaria contiene, en la que se basa el control de acceso, el IMSI (Identidad de Suscriptor Móvil Internacional). La identidad 32 también puede ser un SIM, aunque puede ser un certificado suave o cualquier token de identidad de seguro similar.

La red núcleo mantiene una única relación entre el IMSI y el MSISDN (Números de Red Digital de Servicios Integrados de Suscriptor Móvil), que es el número de teléfono público que el SIM asocia con el dispositivo. Cuando el dispositivo móvil hace una llamada telefónica, o utiliza otros servicios de telefonía tal como SMS (Servicio de Mensaje Corto), el MSISDN se envía usualmente con una “identidad de llamante” de tal manera que receptor conde de donde se origina el mensaje o llamada. Específicamente identidad de llamante MSISDN identificará el mismo originador sobre una franja de tiempo larga y muchas llamadas, independiente de donde y cuando se conectan a la red. Para las sesiones de datos ninguno de los dispositivos de internet móvil, macrocelda o red núcleo inserta una identidad similar que deja el servidor 36 conocido desde donde se origina la sesión de datos. A todo el servidor se le da una dirección IP de retorno para enrutar una repuesta, pero esta dirección es transitoria y puede ser diferente para cada sesión del dispositivo de internet móvil que inicia con el servidor. Si el servidor necesita reconocer el mismo retorno de dispositivo entre las sesiones, alguna credencial de identidad independiente con significado para el servidor, tal como un nombre de usuario o cookie, se puede ingresar en el dispositivo.

La presente invención describe cómo el punto de acceso 14, utilizando la intersección y función de enrutamiento 20, puede insertar identidades en una sesión de datos entre el dispositivo de internet móvil 10 y el servidor 36. En algunas realizaciones, estas identidades son las identidades inmutables y únicas 30 y 32, y ya que la información que se inserta en la sesión de datos se deriva directamente del token de identidad relevante. En otras realizaciones, cuando estas identidades frecuentemente se consideran sensibles, la información insertada en la sesión de datos en su lugar se relaciona estadísticamente con la identidad en una forma equivalente a la relación entre IMSI y MSISDN. La relación de mapeo de identidad se mantiene en un registro de identidad de servicio 38 que se puede acceder por medio de la red núcleo o por medio de internet dependiendo de las consideraciones comerciales. El servidor 36 almacenará normalmente y aplicará datos específicos de servicio 40 en sus interacciones con el usuario, y seleccionará estos datos utilizando las identidades insertadas en la sesión de datos. Cuando una identidad asociada con el dispositivo de internet móvil se inserta en la sesión de datos, permite que el servidor reconozca el dispositivo (e infiera el propietario/usuario). Cuando una identidad asociada con el punto de acceso se inserta en la sesión de datos permite que el servidor infiera la ubicación del dispositivo de internet móvil (a una resolución del cubrimiento del punto de acceso).

La Figura 2 ilustra un primer proceso de acuerdo con la presente invención, en términos del flujo de mensajes entre el dispositivo de internet móvil (MID) 10, el punto de acceso (AP) 14, la red núcleo 26 y un servidor remoto (RS) 36. Específicamente, el servidor remoto 36 acoge un servicio remoto, por ejemplo en la forma de un sitio web. En el ejemplo ilustrado, el servicio remoto es un portal de reconocimiento de ubicación. Por ejemplo, puede ser un sitio web del hogar del operador móvil para uso por los clientes del operador móvil. Sin embargo, puede ser igualmente cualquier otro servicio, por ejemplo proporcionar una búsqueda o servicio de publicidad.

En esta realización ilustrada, el servicio reconoce la ubicación, en el sentido que puede modificar el contenido sirve, con base en la ubicación del usuario. Sin embargo, en otras realizaciones, el servidor puede adaptar su contenido con base en otros aspectos del contexto, tal como la identidad del usuario.

En primer lugar, en la etapa 50, cuando arranca el AP, utiliza su identidad de acceso de red 32 para solicitar conexión a la red núcleo (etapa 50) y se autoriza (etapa 52). El punto de acceso está listo para proporcionar servicio (etapa 54) a los dispositivos de internet móviles.

Finalmente, cuando el MID 10 llega en la cubierta AP intenta conectar (etapa 60) utilizando su identidad de acceso de red 30. La intercepción y función de enrutamiento 20 tiene la oportunidad de rechazar el acceso automáticamente (por ejemplo una estación base de femtocelda que se ubica dentro de las instalaciones del cliente pequeñas o domésticas se pueden configurar con un "grupo de usuario cerrado" de tal manera que solo los dispositivos específicamente registrados por este cliente pueden obtener mucho acceso) pero enrutarán normalmente la solicitud a la red núcleo (etapa 62). Asumiendo que esto se autoriza (etapa 64) por la red núcleo, el AP 14 transmite (etapa 66) la respuesta al MID. Si se garantiza acceso, el MID se considera acampado en el AP 70 de tal manera que el AP proporcionará acceso de red al MID como y cuando se requiera.

En la fase de uso, como se muestra en la etapa 80 de la Figura 2, un dispositivo móvil unido al punto de acceso intenta acceder el servicio remoto. Al inspeccionar el tráfico de datos que se pasa a través de este, el punto de acceso es capaz en la etapa 82 de reconocer una sesión de datos objetivo e intercepta los datos. En este flujo de mensajes básicos una sesión de datos objetivo es cualquier sesión de datos que utiliza un protocolo de capa de aplicación que se puede manipular. Un ejemplo de dicha sesión de datos es una sesión web HTTP, en la que el protocolo tiene una franja predefinida en la que se pueden insertar las cookies. También, los protocolos con base en XML tal como XMPP y SIMPLE son inherentemente extensibles, y pueden tener los identificadores relevantes inyectados en la sesión de datos.

En la etapa 84, el punto de acceso modifica los datos enviados desde el dispositivo móvil, insertando el identificador 30 para el MID y/o el identificador 32 para el AP. Por ejemplo, cuando el servicio remoto es un sitio web, el punto de acceso puede modificar los datos al agregar una línea a la cabecera HTTP con cookies que contienen las identidades.

Después de esto, el punto de acceso 14 continúa con la transmisión de los datos modificados para el servicio remoto en la etapa 86.

En la etapa 88, el servicio remoto es capaz de hacer modificaciones dependientes del contexto a los datos que se proporcionan en respuesta a una solicitud de acceso. El identificador MID 30 se puede utilizar por el servicio remoto para identificar un usuario particular, aunque el identificador AP 32 se puede utilizar por el servicio remoto para inferir una ubicación particular (ya sea la ubicación geográfica o el contexto es decir "hogar, "oficina", "café"). Por ejemplo, un sitio web reconoce la ubicación utilizará el identificador AP 32 para decidir las modificaciones dependientes del contexto.

En la etapa 90, el servidor remoto 36 regresa los datos a través del punto de acceso 14 al dispositivo móvil 10.

La Figura 2 ilustra el método de inserción de identidad básica de acuerdo con una realización de la invención. El método como se describe con referencia a la Figura 2 es suficiente para permitir que la invención se ponga en efecto, y puede ser adecuada para uso en algunas situaciones de implementación. Sin embargo, se presentan otras situaciones en las que el método descrito previamente es improbable que sea comercialmente aceptable.

En primer lugar, las identidades de acceso de redes 30 y 32 se consideran sensibles por los operadores comerciales de redes núcleo, no es deseable transmitirlas al servicio remoto 36. En segundo lugar, insertar indiscriminadamente los identificadores de usuarios y sus ubicaciones en el tráfico de internet incrementa los problemas de privacidad. En tercer lugar, la provisión del usuario y ubicación de información dentro de una solicitud de servicio puede generar valor significativo para el proveedor del servicio, y el punto de acceso y el operador de red núcleo puede desear controlar la disponibilidad de la información con el fin de adquirir una parte del valor generado.

La Figura 3 ilustra una realización adicional del método de acuerdo con la presente invención, que aborda seguridad, privacidad y consideraciones comerciales. Específicamente, la Figura 3 ilustra el flujo de mensajes entre el dispositivo de internet móvil (MID) 10, el punto de acceso (AP) 14, el registro de identidad (IR) 38 y un servidor remoto (RS) 36.

El método mostrado en la Figura 3 tiene diversas etapas en común con el método mostrado en la Figura 2. En donde las etapas del método mostradas en la Figura 3 son iguales que las etapas del método mostrado en la Figura 2 y descritas anteriormente, estas no se describirán en detalle adicional.

Cuando el AP arranca, utiliza su identidad de acceso de red 32 para solicitar conexión a la red núcleo, y se autoriza, como se describe con referencia a la Figura 2. El punto de acceso luego está listo para proporcionar servicio (etapa 54) a los dispositivos de internet móviles.

La Figura 3 ilustra el uso del registro de identidad 38. El registro de identidad es una base de datos que mapea las identidades de acceso de redes 30 y 32 (que son privadas y sensible al operador de red) a las identidades de servicio que se pueden compartir con el servidor remoto 36.

En primer lugar, después que el AP proporciona servicio (etapa 54), realiza una búsqueda (etapa 100) contra el registro de identidad 38, en donde su identidad de acceso 32 se pasa como un parámetro. El registro de identidad regresa al AP su identidad de servicio (etapa 102). En la recepción de la identidad de servicio regresada, el AP 14 en la etapa 104 almacena la identidad de servicio en un caché que se mantiene, que contiene un subgrupo pequeño de identidades de servicio desde el registro de identidad con el cual se relaciona. Manteniendo este caché evita la latencia y la carga de red que resultaría de consulta del registro de identidad 38 cada vez que el AP requiere una identidad de servicio.

En segundo lugar, tiene lugar una fase de registro, en la que, en la etapa 110, el servicio remoto (RS) envía un mensaje de registro al punto de acceso (AP). Esto puede tener lugar cuando el servicio remoto determina que puede utilizar las identidades de este punto de acceso, por ejemplo cuando el servicio remoto se despliega primero.

El mensaje de registro incluye un identificador de servicio, que describe la forma en la que un dispositivo móvil accederá, normalmente en la forma del Identificador de Recurso Uniforme (URI). El mensaje de registro también especificará qué identidades de usuario (asociadas con MID) o de ubicación (asociadas a AP) se desean insertar en cualquier sesión de datos cuando un dispositivo móvil accede posteriormente al servicio. El mensaje de registro también puede incluir identificadores sustitutos específicos de servicio que se utilizan en lugar del identificador de servicio genérico para el AP que se va a obtener desde el IR en la etapa 102, y en el lugar del identificador de servicio genérico para el MID que se va a obtener desde el IR en la etapa 74.

La fase de registro incluye un intercambio de credencial 112 entre el punto de acceso y el servicio remoto para establecer la confianza mediante autenticación mutua entre las entidades, y para establecer qué servicio remoto se autoriza para hacer la solicitud de registro.

En el caso en que el servicio remoto 36 sea un sitio web, la URI sería una dirección Uniforme de Localización de Recursos (URL) y el identificador de inserción sería una cookie.

El intercambio del mensaje de registro es un ejemplo de un API remoto/llamada de procedimiento remoto alojado en el punto de acceso 10 de tal manera que el servicio remoto 36 puede influenciar y controlar el comportamiento posterior del punto de acceso, como se describe en más detalle en el documento GB-2459107A. El intercambio de credencial 112 para autenticación mutua es parte del procedimiento de registro ya que se puede evitar el uso malicioso o no autorizado del API remoto. Los protocolos de ordenador entre los nodos de red 14 y 36 que proporcionan la seguridad y extensibilidad para las realizaciones incluyen HTTP(S) y XMPP. Dependiendo del protocolo de una realización existirían servidores intermediarios para enrutamiento y autorización de mensajes API entre el punto de acceso 14 y el servidor 36. Estos están implicados como parte de la infraestructura de red 12 en la Figura 1 cuando los detalles son específicos para el protocolo seleccionado y se describen por los estándares de la Fuerza de Tarea de Ingeniería de Internet (IETF), no se describirá adicionalmente aquí.

Luego el registro del punto de acceso almacena en la etapa 114 los detalles del servidor objetivo, cuando se suministran el mensaje de registro. Es posible que el punto de acceso 14 pueda perder energía, o por otras razones se pueda desconectar ocasionalmente y reconectar a la Red de Área Extensa 12. Con el fin de lograr persistencia de los registros del servicio remoto, el punto de acceso puede contener una memoria no volátil asociada con el procesador 22 para almacenamiento persistente de los registros de servicios remotos. En este caso, la operación normal simplemente resume el trabajo después del ciclo de energía.

Como una alternativa, se pueden registrar los registros en una entidad separada, tal como un servidor con almacenamiento no volátil, en la Red de Área Extensa 12, y el punto de acceso se puede programar para solicitar la entidad separada para obtener registros pasados de servicios remotos después de ciclo de energía. Esto sería apropiado para una realización que utiliza HTTP(S) para invocar el API remoto en el punto de acceso.

Como una alternativa adicional, cada servicio remoto puede almacenar la lista de los puntos de acceso con la cual requiere registro, y luego puede emitir un registro renovado en el evento de un punto de acceso de ciclos de energía. Con el fin de ser capaz de implementar esto, el punto de acceso puede emitir un mensaje de notificación de presencia que se enrutará a todos los servicios remotos cuando se vuelve a conectar a la red después de un ciclo de energía. Esto permite que el servicio remoto renueve el registro. Si una realización utiliza XMPP para el API remoto entonces la notificación de presencia con registros almacenados en el servidor hacen parte clave del protocolo.

Cuando un dispositivo de internet móvil (MID) llega a la cobertura del punto de acceso (AP) luego, en la etapa 70, acampará en el AP como un resultado de los procedimientos de autorización de acceso de red descritos previamente. La conclusión de estos procedimientos provoca que el punto de acceso realice una búsqueda (etapa 72) contra el registro de identidad en donde la identidad de acceso de MID 30 se pasa como un parámetro. En la etapa 74, el registro de identidad de servicio 38 regresa al AP de identidad de servicio de MID, que, en la etapa 76, el AP agrega al caché del subgrupo pequeño de identidades de servicio desde el registrador con el que se relaciona.

Como una alternativa, si el AP mantiene una lista fija de identidades de acceso de redes del MID autorizadas (por ejemplo la lista de dispositivos que comprende un "grupo usuario cerrado"), se puede buscar y guardar en caché sus identidades de servicios más tempranas, cuando solicita su propia identidad de servicio 100.

En la fase de uso, como se muestra en la etapa 80 de la Figura 3, un dispositivo móvil unido al punto de acceso intenta acceder al servicio remoto. Al inspeccionar el tráfico de datos se pasa a través de este, el punto de acceso es capaz en la etapa 82 de reconocer una sesión de datos objetivo e intercepta los datos. En este caso, una sesión de datos objetivo es una que utiliza un protocolo que se puede manipular, y se dirige a un servicio que se ha registrado previamente. Es decir, el punto de acceso se desarrolla en la etapa 114, y se almacenan los detalles del servidor objetivo respectivo. En el caso en el que el servicio remoto sea un sitio web, el punto de acceso específicamente inspecciona la cabecera HTTP en el tráfico de datos. Cuando el anfitrión y la fuente en la cabecera HTTP coinciden con el URL registrado por el servicio remoto durante la fase de registro, se reconoce una sesión de datos objetivo.

En la etapa 84, el punto de acceso modifica los datos enviados desde el dispositivo móvil, insertando la identidad de servicio para el MID y/o la identidad de servicio para el AP. Como se describió anteriormente, estas identidades de servicio se obtienen originalmente desde el registro de identidad de servicio 38, pero se pueden haber almacenado en un registro de identidad de servicio caché en el AP. Por ejemplo, en donde el servicio remoto es un sitio web, el punto de acceso puede modificar los datos al agregar una línea a la cabecera HTTP con cookies que contienen las identidades.

Después de esto, el punto de acceso 14 continúa con la transmisión de los datos modificados al servicio remoto en la etapa 86.

En la etapa 88, el servicio remoto es capaz de hacer modificaciones dependientes del contexto a los datos que se proporciona en respuesta a una solicitud de acceso. El identificador MID 30 se pueden utilizar por el servicio remoto para identificar un usuario particular, mientras que el identificador AP 32 se puede utilizar por el servicio remoto para inferir una ubicación particular (ya sea la ubicación geográfica o el contexto es decir "hogar", "oficina", "café"). Por ejemplo, un sitio web que reconoce la ubicación utilizará el identificador AP 32 para decidir las modificaciones dependientes del contexto.

En la etapa 90, el servidor remoto 36 regresa los datos a través del punto de acceso 14 al dispositivo móvil 10.

Por lo tanto se proporciona un punto de acceso que se puede utilizar para proporcionar un servicio mejorado a un dispositivo de internet móvil del usuario.

Por ejemplo, un operador de red móvil puede tener un sitio web de portal, alojado en el servidor 36 que se puede acceder cuando un cliente pulsa un botón específico en su teléfono móvil con capacidad de acceso a Internet, tal como el dispositivo 10. El operador ha desplegado puntos de acceso de femtocelda, tal como el punto de acceso 14, que incorpora un protocolo XMPP para control de servicio, en espacios semipúblicos tal como tiendas. El propietario de la ubicación que aloja cada femtocelda puede registrar con el operador móvil un sitio web que es pertinente para su ubicación. Para cada dicha ubicación, el sitio web de portal (el servicio remoto) registra su propio contenido web con la femtocelda. El sitio web del portal mantiene una tabla de valores relacionada con las identidades de servicio de punto de acceso de los URL de sitio web que el propietario de la ubicación ha suministrado para esa femtocelda.

Ahora, cuando un cliente se conecta a la red por medio de la macrored celular, por ejemplo a través de una estación base de macrocelda 28, y pulsar el botón portal en su teléfono 10, recibirá la página de inicio de portal como usual. Sin embargo, el servicio cambia el comportamiento cuando el cliente está en un local de comida rápida, centro comercial, museo, o ubicación similar que contiene una estación base de femtocelda provisionada de forma adecuada 14, y el cliente se conecta a la red por medio de esta estación base de femtocelda.

Cuando el cliente oprime el botón portal en este caso, la solicitud HTTP recibida por el sitio web portal tiene una cookie adicional insertada por la estación base de femtocelda. El servicio remoto es capaz de realizar una búsqueda interna utilizando la cookie, para obtener los URL del sitio web local.

En este caso, el servicio remoto es capaz de tomar las etapas de tal manera que se modifica el contenido que regresa al cliente. Por ejemplo, se puede emitir un HTTP redirigido al URL del sitio web local como su respuesta en lugar de servir a su página de inicio. El navegador web en el dispositivo de internet móvil del cliente 10 solicitará

automáticamente este sitio web local, con el resultado que el usuario puede recibir un menú, un directorio de almacenamiento o mapa, comprobantes, una guía u otra información local relevante, en lugar de la página de inicio de portal.

Como una alternativa, el servicio remoto puede servir la página de inicio de portal, que lo modifica para incluir o incorporar enlaces o contenido relevante, o específico, para esta ubicación utilizando los URL almacenados para esta ubicación.

Sin embargo, los proveedores del servicio en el mundo físico, tal como locales de comida rápida, centros comerciales o museos, pueden mejorar la experiencia de visitar los clientes al proporcionar información útil, ofertas o servicio más rápido por medio del dispositivo de internet móvil del cliente.

Como se ha descrito hasta ahora, el contenido regresado por el servicio remoto se puede modificar con base en el punto de acceso especifico a través del cual se solicita el servicio. En otras realizaciones de la invención, el contenido se puede modificar con base en la identidad del cliente que hace la solicitud.

Por ejemplo, si es importante la identidad del usuario o dispositivo móvil específico para el servicio remoto, puede disponer para el dispositivo móvil iniciar la sesión de datos para incluir una identidad apropiada, por ejemplo una cookie escrita en los cabezales HTTP por un navegador web que se ejecuta en el dispositivo móvil.

Sin embargo, esto también se puede lograr mediante una variación del proceso mostrado en las Figuras 2 & 3 y descrito anteriormente, con la ventaja que el punto de acceso insertará la cookie que identifica el usuario en cada acceso al servicio incluyendo el primero, mientras que el navegador web se ejecuta en el dispositivo móvil solo puede insertar una cookie que se almacena en un acceso previo del servicio.

REIVINDICACIONES

1. Una estación base celular (14), configurada para permitir que un dispositivo (10) se conecte a esta sobre una interfaz inalámbrica, en donde la estación base celular (14) es capaz de establecer una conexión a una red celular (26) de tal manera que la red celular (26) requiere una identidad tomada para autorización, y en donde la estación base celular (14) tiene una conexión a una Red de Área Extensa (12), de tal manera que puede enrutar el tráfico de datos desde los dispositivos conectados a un servicio remoto (36) sobre la Red de Área Extensa (12) y, en el evento en que el tráfico de datos desde un dispositivo conectado esté destinado para el servicio remoto (36), la estación base celular (14) se adapta para insertar información derivada de la identidad tomada en el tráfico de datos, y para promover el tráfico de datos modificado para el servicio remoto (36).

2. Una estación base celular como se reivindica en la reivindicación 1, en donde la identidad tomada identifica el dispositivo conectado.

3. Una estación base celular como se reivindica en la reivindicación 1, en donde la identidad tomada identifica la estación base celular.

4. Una estación base celular como se reivindica en cualquier reivindicación precedente, en donde la identidad tomada se almacena dentro de un SIM.

5. Una estación base celular como se reivindica en cualquiera de las reivindicaciones 1 a 3, en donde la identidad tomada comprende un certificado.

6. Una estación base celular como se reivindica en cualquier reivindicación precedente, en donde, en el evento en que el tráfico de datos del dispositivo conectado está destinado para el servicio remoto, la estación base celular se adapta para insertar información derivada directamente de la identidad tomada en el tráfico de datos, y para promover el tráfico de datos modificado al servicio remoto.

7. Una estación base celular como se reivindica en cualquier reivindicación precedente, en donde, en el evento en que el tráfico de datos del dispositivo conectado está destinado para el servicio remoto, la estación base celular se adapta para:

obtener desde un registro de identidad de servicio una identidad de servicio que corresponde a la identidad tomada, y para insertar la identidad de servicio en el tráfico de datos, y para promover el tráfico de datos modificado para el servicio remoto.

8. Una estación base celular como se reivindica en cualquier reivindicación precedente, en donde la estación base celular incluye un API, que se puede utilizar mediante el servicio remoto para registrarse a sí mismo con la estación base celular, de tal manera que la estación base celular insertará identidades solo en el tráfico de datos que se enruta en los servicios registrados.

9. Una estación base celular como se reivindica en la reivindicación 8, en donde el API incluido en la estación base celular, utilizado por el servicio remoto para especificar el identificador del servicio, utiliza XMPP para transportar mensajes API entre la estación base celular y el servicio remoto.

10. Una estación base celular como se reivindica en la reivindicación 8 o 9, en donde la estación base celular se adapta para almacenar la información de registro recibida con relación al servicio remoto solo después de autenticar el servicio remoto.

11. Una estación base celular como se reivindica en las reivindicaciones 8, 9 o 10, en donde la estación base celular se adapta para almacenar la información de registro recibida en la memoria no volátil de tal manera que, en el evento de una interrupción de energía, la información de registro recibida almacenada no se pierde.

12. Una estación base celular como se reivindica en la reivindicación 11, en donde e la memoria no volátil está en la estación base celular.

13. Una estación base celular como se reivindica en la reivindicación 11, en donde la memoria no volátil se ubica en forma remota desde la estación base celular, accesible sobre una red.

14. Una estación base celular como se reivindica en una de las reivindicaciones 8 a 10, en donde la estación base celular se adapta, en el evento de una interrupción de energía, para indicar su disponibilidad renovada al servicio remoto luego de la interrupción de energía, de tal manera que el servicio remoto puede renovar su información de registro con la estación base celular.

15. Una estación base celular como se reivindica en la reivindicación 14, en donde la estación base celular se adapta para indicar su disponibilidad renovada al servicio remoto luego de la interrupción de energía utilizando XMPP.

16. Una estación base celular como se reivindica en cualquier reivindicación precedente en donde, cuando el tráfico de datos desde el dispositivo conectado es una solicitud HTTP, la estación base celular se adapta para inspeccionar la cabecera HTTP y modificar la cabecera HTTP al insertar la información derivada de la identidad tomada como un Cookie en la cabecera HTTP.

17. Una estación base celular como se reivindica en la reivindicación 16, en donde, en registro con la estación base celular, los servicios remotos se identifican por sí mismos mediante los URL, y cuando la estación base celular inspecciona la cabecera HTTP solo modifica la cabecera HTTP si la entrada Anfitriona en la cabecera coincide con un URL en la información de registro almacenada.

18. Una estación base celular como se reivindica en la reivindicación 16, en donde, en registro con la estación base celular, los servicios remotos se identifican por sí mismos mediante los URL, y cuando la estación base celular inspecciona la cabecera HTTP solo modifica la cabecera HTTP si la concatenación de la entrada Anfitriona con la entrada URI Solicitada en la cabecera HTTP coincide con un URL en la información de registro almacenada.

19. Una estación base celular como se reivindica en cualquier reivindicación precedente, en donde, en el evento en que el tráfico de datos de un dispositivo conectado está destinado para el servicio remoto, la estación base celular se adapta para insertar información derivada de la identidad tomada en una capa de aplicación del tráfico de datos, y para promover el tráfico de datos modificado para el servicio remoto.

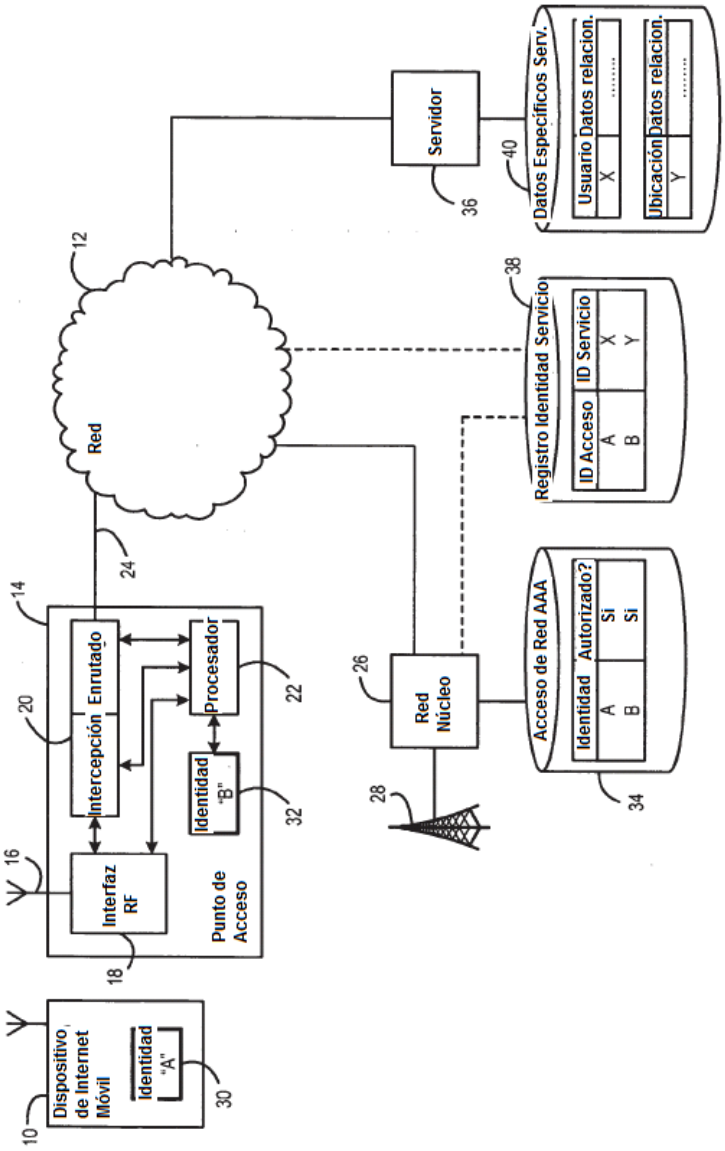
Dispositivo de Internet Móvil
Identidad "A"
10
30
Punto de Acceso
Interfaz RF
16
18
Intercepción Enrutado
Procesador
Identidad "B"
20
22
32
14
24
Red
12
Red Núcleo
26
28
Acceso de Red AAA
Identidad
Autorizado?
A
B
Si
Si
34
Registro Identidad Servicio
ID Acceso
ID Servicio
A
B
X
Y
38
Servidor
36
Datos Específicos Serv.
Usuario Datos relacion.
Ubicación Datos relacion.
X
Y
40

Figura 1

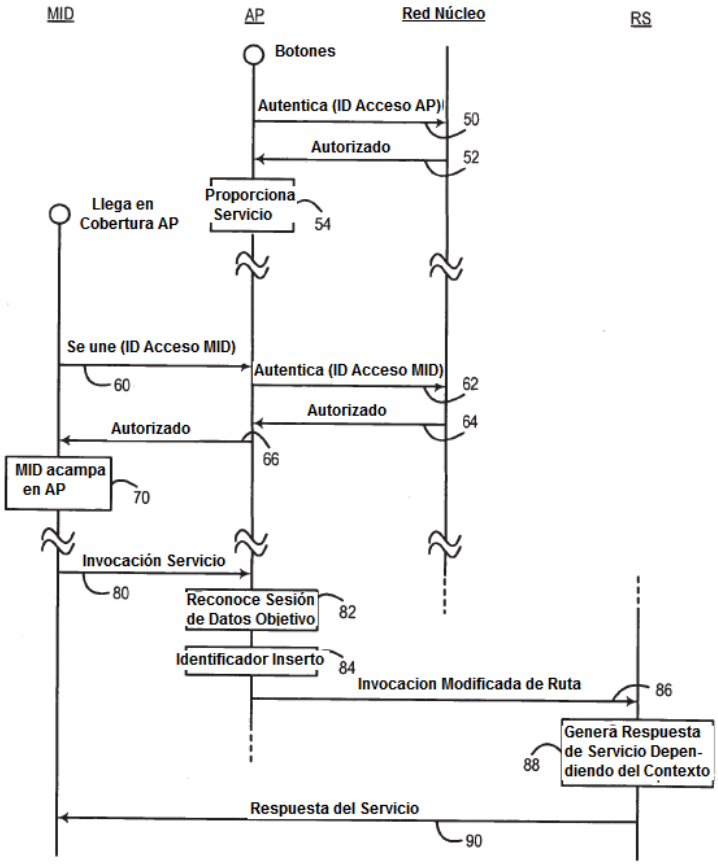
MID
AP
Red Núcleo
RS
Botones
Autentica (ID Acceso AP)
50
Autorizado
52
Proporciona Servicio
54
Llega en Cobertura AP
Se une (ID Acceso MID)
60
Autentica (ID Acceso MID)
62
Autorizado
64
Autorizado
66
MID acampa en AP
70
Invocación Servicio
80
Reconoce Sesión de Datos Objetivo
82
Identificador Inserto
84
Invocacion Modificada de Ruta
86
Genera Respuesta de Servicio Dependiendo del Contexto
88
Respuesta del Servicio
90

Figura 2

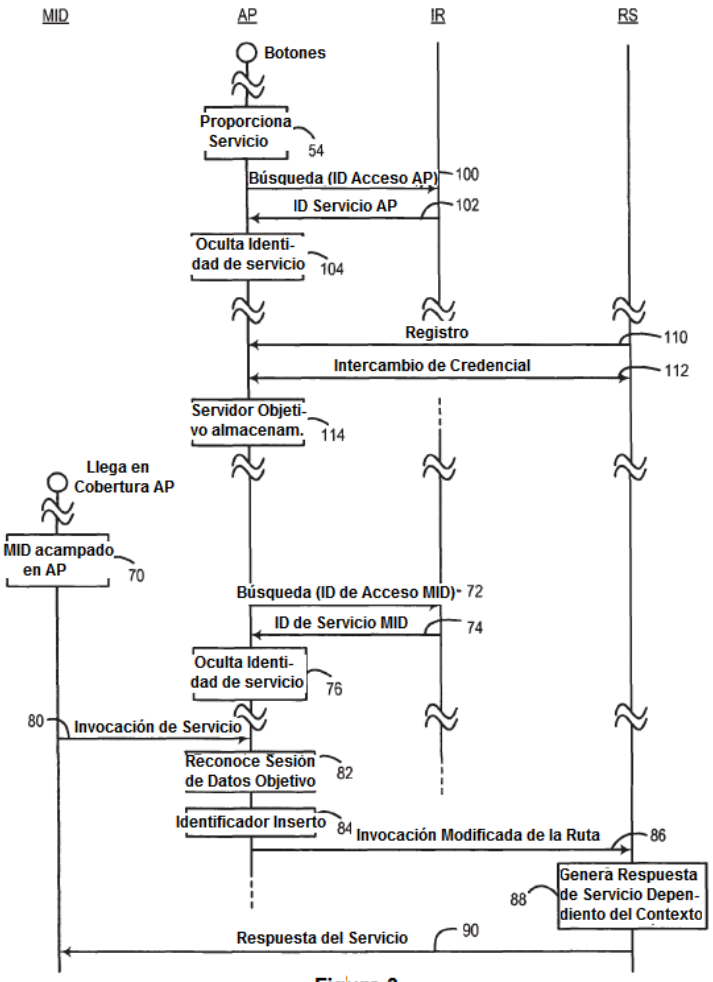
MID
AP
IR
RS
Botones
Proporciona Servicio
54
Búsqueda (ID Acceso AP)
100
ID Servicio AP
102
Oculta Identi-dad de servicio
104
Registro
110
Intercambio de Credencial
112
Servidor Objeti-vo almacenam.
114
Llega en Cobertura AP
MID acampado en AP
70
Búsqueda (ID de Acceso MID)
72
ID de Servicio MID
74
Oculta Identi-dad de servicio
76
80
Invocación de Servicio
Reconoce Sesión de Datos Objetivo
82
Identificador Inserto
84
Invocación Modificada de la Ruta
86
88
Genera Respuesta de Servicio Depen-diento del Contexto
Respuesta del Servicio
90

Figura 3