(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 714 751**

(51) Int. CI.:

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: **26.07.2011 PCT/US2011/045304**

(87) Fecha y número de publicación internacional: **23.02.2012 WO12024065**

(96) Fecha de presentación y número de la solicitud europea: **26.07.2011 E 11748791 (8)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2018 EP 2606624**

(54) Título: **Método y aparato de descubrimiento automatizado en una red de comunicaciones**

(30) Prioridad:

19.08.2010 US 859503

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2019

(73) Titular/es:

ALCATEL LUCENT (100.0%)
Site Nokia Paris Saclay, Route de Villejust
91620 Nozay, FR

(72) Inventor/es:

SUNDARAM, GANAPATHY;
MIZIKOVSKY, SEMYON, B. y
BROUSTIS, IOANNIS

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y aparato de descubrimiento automatizado en una red de comunicaciones

Campo de la invención

La invención se refiere a métodos por los cuales las entidades en una red de comunicaciones se dan a conocer unas a otras.

Antecedentes de la técnica

A medida que la comunicación automatizada entre dispositivos en redes se vuelve cada vez más ubicua, crece la necesidad de automatizar transacciones de una complejidad cada vez mayor. Esto, a su vez, requiere la solución de cada vez más problemas en el campo de los protocolos de comunicación de red.

Una de estas clases de problemas se relaciona con el establecimiento de asociaciones de reconocimiento y seguridad recíprocas entre entidades que inicialmente desconocen la presencia de las otras en una red. Se hace referencia a un problema generalizado de esta clase como el “problema de descubrimiento de hoteles” debido a la siguiente analogía:
un visitante que llega al aeropuerto pretende llegar a su hotel de destino en la ciudad de llegada. Aunque se supone que el visitante llega a un destino específico, y aunque el hotel de destino le está esperando, el visitante ignora la identidad del hotel de destino. El hotel, por supuesto, debe tratar con muchos visitantes. El visitante puede visitar uno o más destinos y presentarse con la esperanza de que uno de los hoteles visitados sea su destino y lo reconozca. Sin embargo, tal proceso puede no ser factible si hay muchos hoteles candidatos. Por lo tanto, el problema es encontrar un método eficiente para encontrar el hotel correcto con una asistencia mínima o sin asistencia de terceros. La solución deseada debe garantizar la seguridad del visitante encontrándole el hotel correcto, y debe garantizar la seguridad del hotel admitiendo solo a los visitantes que se espera.

Sorprendentemente, el problema descrito anteriormente, con diversas modificaciones, puede aplicarse a múltiples entornos de comunicaciones automatizados que implican entidades o dispositivos cliente (con o sin interfaces humanas) y redes de destino o entidades servidor. Por ejemplo, un propietario de una vivienda compra un medidor de servicios legible a distancia en un centro comercial y lo instala en su casa. El medidor de servicios necesita descubrir el sitio web de la compañía de servicios a la que informará, y la compañía de servicios debe descubrir que el medidor se ha conectado. Para garantizar la privacidad del propietario y evitar los abusos, es necesario establecer una asociación de seguridad entre el medidor de servicios y el sitio web de la compañía de servicios. Convencionalmente, estas operaciones se realizarían a través de la intervención de terceros.

El documento US 2006/259602 A1 desvela un método y un aparato para la publicidad y el descubrimiento de un servidor a nivel de transporte. La primera información se recibe en una pila de protocolos de transporte. La pila de protocolos de transporte reconoce que la primera información representa uno o más servicios proporcionados por un servidor. Basándose en la primera información, la pila de protocolos de transporte determina si debe usarse uno o más de los servicios. Además, el documento US 2009/287766 A1 desvela un método de descubrimiento de servicios web móvil que permite al proveedor equilibrar las relaciones de coste/rendimiento y utilizar el ancho de banda de red de manera más eficaz, al mismo tiempo que lograr los niveles de calidad esperados por el cliente.

Lo que ha faltado hasta ahora es un método automatizado que pueda realizar el descubrimiento y la autenticación necesarios con poca o ninguna asistencia en línea de terceros.

Sumario de la invención

La invención proporciona un método de este tipo, como se define en la reivindicación independiente 1. Las realizaciones específicas se definen en las reivindicaciones dependientes.

Breve descripción de los dibujos

La figura 1 es un dibujo esquemático de un entorno de comunicaciones automatizado representativo. El problema de descubrimiento de hoteles puede aplicarse a entornos como los representados en la figura, entre otros.
La figura 2 es un diagrama esquemático de las diversas relaciones transaccionales entre entidades en un ecosistema máquina a máquina (M2M) complejo.
La figura 3 es un diagrama esquemático que proporciona una visión de conjunto funcional de alto nivel de la arquitectura de capas de servicio en un ecosistema máquina a máquina (M2M).
Las figuras 4-6 son diagramas de flujo de mensajes que ilustran el descubrimiento del operador máquina a máquina (M2MO) de acuerdo con diversas realizaciones de la invención.
La figura 7 es un diagrama de flujo de mensajes que ilustra un procedimiento para el establecimiento de una suscripción entre un M2MO y un dispositivo M2M de acuerdo con una realización de la invención.

Las figuras 8-10 son estructuras de datagramas a modo de ejemplo para mensajes de señalización útiles para poner en práctica la invención en algunas realizaciones.

Descripción detallada

ENTORNO DE COMUNICACIONES AUTOMATIZADO GENÉRICO

El problema de descubrimiento de hoteles puede aplicarse directamente a entornos de comunicaciones automatizados, tales como el representado en la figura 1. En esta configuración genérica, se considera un conjunto de N entidades cliente 10 y un conjunto de M entidades servidor 20 que intentan conectarse entre sí de manera segura.

Se define el siguiente *problema de descubrimiento de hoteles automatizado*: cada entidad cliente quiere conectarse exactamente con una entidad servidor, pero una entidad servidor puede servir a muchas entidades cliente. El cliente no sabe por adelantado a qué servidor necesita conectarse, aunque cada servidor puede conocer la identidad del cliente con el que espera comunicarse. El objetivo es conectar cada entidad cliente con su entidad servidor correspondiente de manera segura, es decir, de una manera que evite que una entidad servidor falsa secuestre una entidad cliente, y que, a la inversa, garantice que cada entidad servidor solo hablará con aquellas entidades cliente con las que espera hablar. En el problema planteado en este caso, se supone que las entidades cliente y servidor establecen enlaces a través de una red de comunicaciones, que incluye unas pasarelas 30 y unos servidores de servicios de gestión 40, por ejemplo, portales web que se conectan a bases de datos.

REALIZACIONES DEL PROBLEMA DE DESCUBRIMIENTO DE HOTELES

Realización del problema de descubrimiento de hoteles en redes de comunicaciones móviles. En un ejemplo de una realización actual del problema de descubrimiento de hoteles, un teléfono móvil (en el papel de “visitante” en el problema que se ha planteado anteriormente), al activarse, necesita descubrir con qué operador de red de acceso (en el papel de “hotel”) se supone que va a asociarse. Más específicamente, el problema se aplica si, cuando un usuario enciende un teléfono móvil, el teléfono no conoce *a priori* la identidad de red del operador con el que se supone que está registrado (un problema análogo puede aplicarse al acceso WiFi en puntos de acceso públicos).

El crecimiento de los dispositivos inalámbricos no tradicionales, tales como los lectores electrónicos, que operan en los denominados entornos de dispositivos abiertos, ha hecho que el problema sea más urgente. Por ejemplo, los lectores electrónicos vienen equipados con interfaces inalámbricas y, en mayor medida, soportan múltiples tecnologías inalámbricas con el fin de ampliar la audiencia objetivo. Este enfoque también permite que los fabricantes de lectores electrónicos aprovechen las estrategias de distribución minorista abiertas pero fiables en lugar de centrarse en un solo operador a la vez para distribuir sus dispositivos.

En consecuencia, existe una necesidad de un método automatizado mediante el cual el teléfono móvil, el lector electrónico, u otro aparato de usuario, pueda reconocer al menos algunas redes de acceso candidatas y seleccionar de manera segura la adecuada, y mediante el cual la red de acceso pueda restringir la admisión solo a aquellos dispositivos legítimos de los que ya tenga conocimiento o que ya esté esperando.

Realización del problema de descubrimiento de hoteles en las comunicaciones M2M. Las comunicaciones máquina a máquina (M2M) están experimentando un crecimiento generalizado debido a la aparición y al potencial sin precedentes de las aplicaciones M2M. Se espera que se desplieguen varios miles de millones de dispositivos M2M de bajo coste con miles de aplicaciones proporcionadas por una pluralidad de operadores M2M (M2MO) que aprovechan una combinación de redes de acceso. Las implementaciones tempranas M2M se han caracterizado por su fuerte dependencia de, y confianza en, un solo operador de red de acceso vinculado, que habitualmente gestiona la mayoría de las operaciones M2M y proporciona una serie de servicios esenciales.

Uno de los servicios disponibles en la actualidad es el descubrimiento de servicios M2M, que permite que un dispositivo M2M disponible en el mercado proporcione, a través de procedimientos de red de acceso adecuados, la identidad de su M2MO vinculado, y permite conectarlo a ese M2MO. Por ejemplo, el dispositivo M2M podría preconfigurarse (por ejemplo, en la fábrica) para operar con un proveedor de red de acceso específico, mientras que el proveedor de red de acceso tiene un acuerdo exclusivo con el M2MO específico en un área en particular. Cuando el dispositivo M2M se conecta a la red de acceso por primera vez, la red de acceso comunica al dispositivo la identidad del operador M2M, incluyendo su dirección y parámetros de comunicación. Posteriormente, el dispositivo M2M se comunica con este M2MO específico.

Sin embargo, un modelo de arquitectura de este tipo no puede dar cabida (como era de esperar) a ecosistemas M2M complejos compuestos por despliegues M2M a gran escala en los que el M2MO se desacopla del operador de red de acceso y debe gestionar muchos, posiblemente incluso miles de millones, de dispositivos independientemente como un proveedor de servicios M2M.

La figura 2 representa esquemáticamente las relaciones transaccionales que habitualmente conectan las diversas entidades que participan en un ecosistema M2M complejo, o bien como operadores de entidades de red o como partes interesadas de otro tipo. Estas incluyen los fabricantes 50, los proveedores de aplicaciones 60, los operadores M2M 70, los operadores de red de acceso 80 y los clientes 90 que poseen o controlan los dispositivos 100.

En estos ecosistemas M2M complejos, el M2MO no puede depender de la capa de red de acceso para gestionar las operaciones de descubrimiento de servicios M2M. Es decir, puede que falten relaciones comerciales entre el M2MO y el operador de red de acceso, o la infraestructura de la red de acceso puede ser inherentemente incapaz de proporcionar dicho soporte (por ejemplo, la red de acceso disponible a menudo no será más que un simple medio de transporte sin capacidades especiales).

Además, los dispositivos M2M a menudo se fabrican y distribuyen para su disponibilidad comercial antes de tomar cualquier decisión con respecto a las asociaciones específicas entre los operadores M2M y los dispositivos M2M. Una consecuencia es que un gran número de dispositivos M2M disponibles en el mercado que no tienen interfaz de usuario para la configuración posterior desconocen la activación inicial de la identidad del M2MO con el que deben establecer una asociación, y no tendrán ningún medio automático para obtener esa información sobre la activación inicial. Dada la gran cantidad de dispositivos M2M que un M2MO puede necesitar soportar, se entenderá que pueden no ser factibles las soluciones no escalables, tales como el aprovisionamiento previo manual de información relacionada con M2MO.

En consecuencia, existe una necesidad de técnicas escalables para abordar el problema de permitir que los dispositivos M2M descubran y se asocien con el M2MO adecuado. A continuación, con fines ilustrativos, se describirán las técnicas relacionadas con los *dispositivos M2M*. Sin embargo, debe tenerse en cuenta que las mismas técnicas también pueden aplicarse a las *pasarelas M2M*, como se entiende, por ejemplo, a partir de la definición de “pasarela M2M” en la especificación técnica ETSI TS 102 690: Machine-to-Machine Communications (M2M); Functional Architecture.

Una realización del problema de descubrimiento de hoteles en la publicidad. El objetivo de la publicidad es atraer la atención de los clientes hacia nuevos productos. En una realización del problema de descubrimiento de hoteles aplicado a la publicidad, el cliente desempeña el papel de visitante, mientras que la empresa que anuncia un nuevo producto desempeña el papel de hotel. En consecuencia, el objetivo de la empresa es informar al cliente sobre la existencia y el valor del producto. En respuesta, se espera que el cliente establezca una relación con la empresa que vende el producto, como posible comprador del producto.

Las modernas metodologías de extracción de datos han permitido a los anunciantes identificar a los consumidores que son los objetivos publicitarios preferidos.

En consecuencia, existe una necesidad de un método automatizado mediante el cual se permita de manera segura que el anunciante alcance sus objetivos preferidos, y, por el contrario, que los clientes solo reciban el anuncio que prefieran.

DESCRIPCIÓN DE ALTO NIVEL DE LAS SOLUCIONES AL PROBLEMA DE DESCUBRIMIENTO DE HOTELES

A continuación, se describirán tres métodos que, como se mostrará, pueden automatizarse, y que son soluciones a modo de ejemplo al problema de descubrimiento de hoteles. Con cualquiera de estos métodos, el visitante puede identificar y alcanzar el destino adecuado aunque no conozca, *a priori*, la identidad de su destino, y aunque los terceros no puedan asesorarlo de manera continua. En resumen, las soluciones son:

1. El hotel es consciente del hecho de que el visitante quiere llegar al mismo y, en consecuencia, envía un representante al aeropuerto para reunirse con el visitante y recogerlo. Esto se aplica en casos limitados, cuando se conoce la hora exacta de llegada y puede confirmarse la seguridad del visitante y del hotel.
2. Un grupo de hoteles envía una furgoneta de recogida al aeropuerto para recoger a diversas personas; sin embargo, el visitante específico no está explícitamente invitado o avisado. El visitante acepta el viaje y se dirige al hotel, donde, a través de un proceso de negociación seguro, determina si este hotel es el destino previsto o no. Si no lo es, entonces el visitante regresa a la furgoneta y se dirige a otro destino candidato (en variaciones de este escenario, cada hotel ofrece su propia furgoneta).
3. El visitante avisa de su llegada usando los medios. El hotel que espera al visitante se entera de su llegada y envía un representante al aeropuerto para que lo encuentre y lo lleve al hotel después de una verificación por parte del visitante y del representante.

A continuación, se explicará cómo pueden implementarse estas soluciones para su aplicación a entornos de comunicaciones específicos en configuraciones automatizadas. En particular, se describirá un protocolo que es eficaz para garantizar la seguridad y la eficiencia, y una arquitectura de sistemas que hace que estas soluciones sean factibles.

INFRAESTRUCTURA Y SOLUCIONES EN ENTORNOS DE COMUNICACIONES AUTOMATIZADOS

Solución al problema genérico. Con referencia a la figura 1, se considera un entorno de comunicaciones automatizado en el que un conjunto de N entidades cliente 10 y un conjunto de M entidades servidor 20 intentan conectarse entre sí de manera segura. Se supone que las entidades cliente y servidor establecen enlaces a través de una red de comunicaciones que incluye unas pasarelas 30 y unos servidores de servicios de gestión 40 (por "servidor de servicios de gestión" se entiende un portal web u otra entidad similar, que está conectado a una base de datos y a la red).

Habitualmente, el cliente será un dispositivo que tiene una interfaz de usuario muy limitada, o incluso ninguna en absoluto, y que está diseñado para ser capaz de comunicarse con el servidor en la red, con poca o ninguna intervención humana. Las técnicas de comunicaciones M2M, por ejemplo, pueden ayudar al dispositivo cliente a comunicarse con otra máquina en la red, tal como un servidor de red, automáticamente y sin intervención humana.

Algunos ejemplos de sistemas M2M son: medidores de servicios que informan periódicamente al servidor de proveedor de servicios, monitores médicos que suministran los datos del paciente recogidos al servidor de un hospital, módulos de vehículos automatizados controlados por un sistema informático de vehículo central, y dispositivos de control climático que informan a, y se controlan por, un ordenador central de planta física.

En una realización, las entidades servidor y las entidades cliente pueden compartir una *contraseña temporal*. La contraseña temporal puede proporcionarse previamente al cliente durante la fabricación, o, como alternativa (pero solo si una interfaz de usuario adecuada, tal como un teclado, está disponible), el usuario del cliente puede elegir una contraseña temporal e introducirla en el cliente.

Además, la información sobre cada cliente se comparte con el servidor de servicios de gestión. La información compartida incluirá habitualmente la contraseña temporal y una identidad para el cliente. Esta identidad debe identificar de manera única al cliente en el servidor específico. La información compartida también puede incluir, entre otras cosas, la identidad del servidor al que el cliente necesita conectarse y las primitivas criptográficas relacionadas con la identidad. El servidor de servicios de gestión compartirá habitualmente esta información con un servidor de autenticación (expuesto a continuación, pero no mostrado, en la figura 1).

Con referencia adicional al problema de descubrimiento de hoteles, la entidad servidor en un entorno de comunicaciones, como se ha descrito anteriormente, desempeña el papel del *hotel*, mientras que la entidad cliente desempeña el papel de *visitante*. Con el fin de que un cliente y un servidor se identifiquen entre sí y establezcan una asociación de servicio, uno o más de los siguientes enfoques a modo de ejemplo, cada uno de los cuales es una solución al problema de descubrimiento de hoteles, puede ser ventajoso:

(1) La entidad servidor obtiene la identidad cliente del servidor de servicios de gestión. Esta información puede anunciarse a la entidad servidor por el servidor de servicios de gestión, es decir, "impulsarse" hacia la misma. Como alternativa, la entidad servidor puede solicitar periódicamente esta información al servidor de servicios de gestión asociado, y recibirla como respuesta, es decir, "extraerla".
A continuación, la entidad servidor se comunica enviando un mensaje publicitario al cliente que tiene esa identidad específica. Al recibir el anuncio, el cliente participa en una sesión de autenticación recíproca con la entidad servidor. Habitualmente, esto se hará a través de una pasarela en la red de comunicaciones. Después de una autenticación exitosa, las entidades cliente y servidor ejecutan un protocolo de seguridad más permanente y se descubren entre sí de manera permanente.
Algunos protocolos de seguridad conocidos que pueden ser útiles a este respecto son IBAKE y PAK. Véase, por ejemplo, el borrador de internet de IETF http://tools.ietf.org/html/draft-cakulev-ibake-01, *IBAKE*: *Identity-Based Authenticated Key Agreement*, e IETF RFC 5683, *Password-Authenticated Key (PAK) Diffie-Hellman Exchange*, http://tools.ietf.org/html/rfc5683.
(2) Los anuncios de la entidad servidor toman la forma de un mensaje de difusión (una "oferta de servicio") destinado a cualquier entidad cliente "interesada". Como se ha indicado anteriormente, tan pronto como un cliente recibe un mensaje de difusión (una oferta), comienza el proceso de descubrimiento. Sin embargo, recibir un mensaje de difusión no necesariamente resulta exitoso. Por ejemplo, el cliente podría recibir la oferta de una entidad de servicio incorrecta o un cliente inesperado podría intentar conectarse a la entidad de servicio. En cualquier caso, el resultado será un fallo de un proceso de descubrimiento recíprocamente autenticado. En caso de fallo, la entidad cliente reanuda la escucha de los mensajes de difusión e intenta conectarse a otras entidades servidor de manera sucesiva, hasta que el proceso de descubrimiento se autentique recíprocamente y tenga éxito.
(3) La entidad cliente inicia el proceso solicitando un anuncio. Esta solicitud puede comunicarse al servidor de servicios de gestión a través de, por ejemplo, un acceso a la página web. A continuación, el servidor de servicios de gestión puede comunicar esta solicitud a la entidad de servicio. Tan pronto como la entidad de servicio recibe una solicitud de este tipo, envía un anuncio al cliente, tal como se ha descrito, por ejemplo, con respecto al primero de estos enfoques a modo de ejemplo. Tras la recepción del anuncio por parte del cliente, el cliente y el servidor se autentican recíprocamente y, posteriormente, establecen unas credenciales permanentes, pertinentes para la suscripción.

Cada uno de los tres enfoques a modo de ejemplo anteriores se describe con mayor detalle a continuación.

Solución al problema de la realización en entornos de dispositivos abiertos

Cada uno de los tres enfoques anteriores puede implementarse en un entorno de dispositivo abierto. Se entiende bien que los dispositivos genéricos que no están asociados *a priori* con un proveedor de servicios específico, es decir, que no están preconfigurados para funcionar solo y exclusivamente con una entidad de servicios específica, se consideran *dispositivos abiertos*. La infraestructura que se define para dar cabida a *dispositivos abiertos* e integrarlos en un sistema operativo se define como "*entorno de dispositivo abierto*". Los ejemplos de dispositivos abiertos incluyen un medidor de agua genérico que puede funcionar con cualquier compañía suministradora de agua, o un sensor de alarma que puede integrarse con cualquier sistema de alarma y al que pueden ofrecerse las credenciales específicas de sistema. De manera similar, se consideran dispositivos abiertos los lectores electrónicos que no están vinculados a una red prescrita específica.

De acuerdo con el primer enfoque, el usuario del *dispositivo abierto* puede establecer credenciales temporales (por ejemplo, una contraseña temporal) con una red de acceso de su elección. En otras palabras, el usuario configura una relación comercial temporal con el operador de red correspondiente. Por ejemplo, en un procedimiento a menudo denominado "aprovisionamiento previo sin conexión", el usuario se comunica con un servidor de servicios de gestión, establece una suscripción de servicio, proporciona la identidad del dispositivo, etc. El servidor de servicios de gestión, a su vez, proporciona la identidad del dispositivo al operador de servicios.

Cabe señalar a este respecto que la comunicación entre el usuario y la red elegida podría no implicar el dispositivo abierto específico que sea de interés. En particular, es posible que el dispositivo abierto no conozca las credenciales temporales y que el usuario tenga que proporcionarlas a través de una interfaz estándar, tal como un teclado. El operador, sin embargo, conoce la existencia del dispositivo.

Después del aprovisionamiento previo, el dispositivo (en el papel de *visitante*) recibe un mensaje de aviso explícito del operador (en el papel de *hotel*), que proporciona una información que identifica al operador de red y el tipo de servicios ofrecidos. A continuación, el dispositivo podría enviar una solicitud de suscripción al operador. Si el dispositivo y el operador se autentican recíprocamente con éxito, continúan con el establecimiento de la suscripción de servicio que permitirá configurar una sesión segura para comunicaciones posteriores, incluidas aquellas que comunican datos de servicio.

De acuerdo con el segundo enfoque, el operador de red obtiene la identidad del dispositivo, como se ha descrito anteriormente. Sin embargo, en lugar de enviar un mensaje de aviso explícito, el operador difunde una trama de señalización genérica. Esta señalización transmitida genérica avisará de la presencia de la entidad de servicio del operador a todos los dispositivos interesados en la región. A este respecto, no se dirige a un dispositivo específico, sino que se recibe y se comprende por todos los dispositivos que esperan tales avisos en el área de difusión. Con esta señalización, la red de acceso activa múltiples dispositivos para intentar establecer de manera segura una sesión de servicio de red.

Lo que se desea es conectar el dispositivo abierto dado a la red adecuada. Habitualmente, esto ocurrirá después de que el dispositivo dado examine una o más de las señalizaciones e intente asociarse con cada uno de varios operadores diferentes. Finalmente, el dispositivo se encontrará con el operador de red adecuado y se autenticará recíprocamente con el mismo. Después de esto, el dispositivo y la red pueden proceder a establecer la suscripción de servicio y, si se desea, una sesión de servicio.

De acuerdo con el tercer enfoque, el dispositivo abierto transmite un aviso de que ha comenzado un esfuerzo para identificar el operador de red adecuado. Al recibir dicho aviso, una o más redes disponibles en el área pueden enviar invitaciones explícitas al dispositivo. Mediante el uso de credenciales de seguridad aprovisionadas previamente, el dispositivo abierto identificará la red adecuada a través de una autenticación recíproca y, posteriormente, se conectará a ese operador para establecer la suscripción de servicio o la sesión de servicio.

Aplicación de los tres enfoques mencionados anteriormente para resolver el problema de descubrimiento de hoteles para el M2M. En esta sección, se describirán aplicaciones a modo de ejemplo de las tres estrategias de asociación mencionadas anteriormente al problema del descubrimiento M2MO para comunicaciones máquina a máquina. Se supone que el dispositivo M2M se registra exitosamente con una red de acceso tras la activación, antes de adoptar acciones adicionales con respecto al descubrimiento y asociación M2MO. En los ejemplos que se describen a continuación, el M2MO desempeña el papel del *destino deseado*, mientras que el dispositivo M2M asume el papel del *visitante* en relación con el problema de descubrimiento de hoteles.

En general, la red de acceso realizará un papel de soporte como una red de transporte para llegar al M2MO deseado o el dispositivo M2M deseado. Sin embargo, también puede haber escenarios en los que la red de acceso no solo proporciona transporte, sino que también asume las funciones del M2MO como se describe en este caso. Por ejemplo, en un escenario simple de este tipo, el dispositivo cliente (abierto) es un lector electrónico, que puede descargar libros usando los servicios de cualquiera de los diversos proveedores de servicios de telecomunicaciones

(TSP). El servidor de servicios de gestión selecciona un TSP específico, que a partir de entonces no solo sirve como red de servicio, sino también como operador M2M para efectuar la descarga del texto de la librería en línea.

De acuerdo con el primer enfoque, el M2MO envía una invitación de capa de servicio M2M explícita al dispositivo M2M después de aprovisionarse con la identidad de dispositivo M2M y un conjunto de parámetros relacionados. El dispositivo M2M recibe la invitación y se autentica recíprocamente con el M2MO. A continuación, el dispositivo M2M y el M2MO continúan con el establecimiento de la suscripción de servicio M2M.

De acuerdo con el segundo enfoque, los anuncios se difunden desde el M2MO. El fin de estos anuncios es atraer dispositivos que buscan sus M2MO designados. Al recibir tal anuncio, el dispositivo M2M envía una solicitud de suscripción al M2MO. Esto puede iniciar una autenticación recíproca que, si es exitosa, puede seguirse del establecimiento de una suscripción de servicio entre el M2MO y el dispositivo M2M.

De acuerdo con el tercer enfoque, el dispositivo M2M avisa de su intención de identificar un M2MO a través de un mensaje de difusión. El M2MO recibe el aviso y responde enviando una invitación explícita al dispositivo M2M. La invitación incluye información que indica al dispositivo M2M cómo proceder con el establecimiento de una suscripción de servicio. El dispositivo M2MO y el dispositivo M2M establecen la suscripción tras una autenticación recíproca exitosa.

Soluciones a la realización de problemas en publicidad

Ejemplos de motivación. De acuerdo con el primer enfoque, se asume que la empresa que vende el producto tiene conocimiento de los clientes específicos que estarán muy interesados en comprar el producto. Por ejemplo, la información de este tipo puede recopilarse aplicando métodos estadísticos a los datos transaccionales y demográficos de los clientes. Por ejemplo, un folleto de un concesionario de automóviles local que promociona automóviles de lujo podría dirigirse a clientes potenciales que son dueños de casas caras en un área suburbana cara muy conocida.

De acuerdo con el segundo enfoque, la empresa no se ocupa de clientes específicos; en cambio, anuncia el producto usando medios de difusión. Por ejemplo, podría informarse a un gran número de clientes que estarían interesados en un nuevo refresco a través de anuncios de televisión.

De acuerdo con el tercer enfoque, un cliente interesado en comprar un producto específico (ofrecido por una o más empresas) avisa de este interés, de tal manera que se notifican las empresas candidatas (un ejemplo es publicar el interés en periódicos, sitios web públicos, páginas amarillas y similares). De hecho, tal aviso puede estar implícito, ya que puede inferirse de otros comportamientos, tales como la compra de un artículo como una casa cara.

Aplicaciones a entornos automatizados. Considérese el caso de la publicidad en línea, donde los anuncios electrónicos aparecen en banners que están integrados dentro de las páginas web. Cada vez que un usuario en línea hace clic en ciertos enlaces o busca cadenas específicas usando motores de búsqueda en línea, dichas acciones y los datos relacionados se monitorizan y comparten entre los operadores de red y las entidades de publicidad. Un software inteligente puede registrar los hábitos y preferencias del usuario, y puede procesar esta información para usarla al proporcionar anuncios personalizados para el usuario específico.

De acuerdo con el primero de los enfoques descritos anteriormente, la empresa que está interesada en la venta de un producto anuncia el producto al cliente o usuario específico mediante la visualización de un anuncio que coincide con los hábitos y preferencias de ese cliente o usuario.

De acuerdo con el segundo enfoque, la empresa difunde un anuncio en línea a todos los clientes o usuarios potenciales.

De acuerdo con el tercer enfoque, el usuario en línea puede hacer clic intencionadamente en ciertos enlaces para activar mecanismos de software que responden proporcionando anuncios para un tipo específico de producto. Cabe señalar que este es un escenario en el que el comportamiento del usuario, es decir, hacer clic en enlaces específicos, puede constituir un aviso explícito de sus intereses y necesidades de productos.

UNA ARQUITECTURA DE SISTEMAS A MODO DE EJEMPLO

Antes de proceder con el análisis de cómo cada uno de los tres enfoques mencionados anteriormente para resolver el problema de descubrimiento de hoteles puede aplicarse en el caso M2M, se proporcionará una visión general de una arquitectura de capa de servicios ilustrativa. La arquitectura está representada pictóricamente en la figura 3, a la que ahora se dirige la atención. Se entenderá que, si bien la arquitectura de sistemas descrita en este caso se ilustra en el contexto específico de los entornos M2M, los expertos en la materia pueden ampliar fácilmente las ideas descritas en este caso a otros entornos.

Como se muestra en la figura 3, el M2MO 110 incluye tres entidades funcionales básicas: un servidor de autenticación M2M y una base de datos 120 (por ejemplo, un servidor AAA) que almacena las identidades de dispositivo y las credenciales de seguridad de los dispositivos M2M y también almacena una lista de dispositivos registrados, un agente de servicio M2MO 130 para comunicar información entre los dispositivos y el M2MO, y una entidad servidor de aplicaciones 140 que puede tener varios papeles diferentes. Por ejemplo, el servidor de aplicaciones puede realizar las operaciones de arranque con los dispositivos M2M 150 que generan parámetros para las claves de seguridad permanentes, y puede comunicar esos parámetros al servidor de autenticación. Una entidad de aprovisionamiento fiable (TPE) 160 proporciona credenciales de dispositivo M2M al servidor de autenticación. El M2MO usa dichas credenciales para enviar invitaciones a los dispositivos, así como para aceptar solicitudes de suscripción de manera segura. A este respecto, cabe señalar que cualquier intercambio de información entre un dispositivo y el M2MO pasa por el agente de servicio M2MO.

Como se entenderá por los expertos en la materia, los servidores de autenticación habitualmente se ejecutan en los servidores o grupo de servidores 1U estándar. Por supuesto, son posibles muchas alternativas, que incluyen una gama de dispositivos, desde los servidores disponibles en el mercado hasta plataformas de hardware ATCA de alta disponibilidad hechas a la medida (que pueden ser útiles, por ejemplo, para redes en las que existe un alto volumen de transacciones). Habitualmente, los agentes de servicio se implementan en un software que se ejecuta en una plataforma adecuada. La gama de dispositivos que pueden soportar servidores de aplicaciones es similar a la que pueden soportar los servidores de autenticación. Sin embargo, como regla general, se prefiere el hardware del servidor del centro de datos para soportar los servidores de autenticación y de aplicaciones.

A continuación, se expondrá un ejemplo de cómo cada uno de los enfoques genéricos expuestos anteriormente puede aplicarse a las comunicaciones M2M.

Primer enfoque: el M2MO envía una invitación explícita al dispositivo M2M. Este enfoque implica un mensaje de invitación explícito enviado desde el M2MO al dispositivo M2M. Más específicamente, un dispositivo M2M que se compra de manera estándar y se activa por primera vez desconoce con qué M2MO se supone que está asociado. Recuérdese que un dispositivo M2M de bajo coste puede no tener una interfaz de usuario, desde la cual potencialmente podría obtener dicha información.

Tan pronto como se informa al M2MO sobre la existencia del dispositivo M2M y su intención de asociarse con el servicio M2M, el M2MO construirá una invitación M2M y la enviará al dispositivo. Existen varios procedimientos habituales con los que el M2MO puede saber de la existencia del dispositivo. En un ejemplo, el propietario del dispositivo o del proveedor de aplicaciones M2M vinculado se pone en contacto con el M2MO (o bien directamente o a través de terceros) y proporciona la identidad del dispositivo junto con un conjunto opcional de parámetros (que se expondrán a continuación). Con referencia a la arquitectura ilustrativa de la figura 3, a la TPE se le asigna la tarea de proporcionar dicha información al M2MO (y específicamente, a la base de datos del servidor de autenticación).

De acuerdo con este enfoque, el M2MO activará de manera explícita el dispositivo enviando una *invitación M2M* (equivalente al representante enviado al aeropuerto en el planteamiento del problema de descubrimiento de hoteles) que está explícitamente destinada al dispositivo M2M específico. Dicha invitación puede considerarse como un *mensaje de aviso de capa de aplicación*, que indica la identidad del M2MO y la identidad del dispositivo M2M junto con un conjunto de parámetros que se describirán a continuación.

Las etapas del procedimiento anterior se representan en la figura 4 y se describen con mayor detalle a continuación:

1. La TPE conoce la identidad del dispositivo M2M y proporciona la afiliación de la marca y la identidad del dispositivo al M2MO (específicamente, a la base de datos del servidor de autenticación), incluyendo un conjunto de credenciales y parámetros que están relacionados con el proceso de conexión del dispositivo y son específicos para el proceso de conexión específico a seguir. La TPE puede haber obtenido esta información, por ejemplo, del fabricante o de los datos introducidos por el usuario o el propietario del dispositivo M2M a través de una interfaz web. Otros medios posibles para adquirir la información serán fácilmente evidentes para los expertos en la materia. La identidad del dispositivo puede representarse, por ejemplo, por la dirección MAC del dispositivo, por un número de serie electrónico, o por cualquier otro identificador único que se proporcione previamente al dispositivo durante la fabricación.
Se entenderá que así como la información de identificación sobre el dispositivo puede comunicarse a la TPE, también puede comunicarse la localización esperada del dispositivo. Esto puede ser ventajoso debido a que potencialmente permite comunicaciones más centradas y limitadas regionalmente entre el M2MO y el dispositivo.
2. El M2MO ahora sabe que el dispositivo M2M está dispuesto a aceptar invitaciones para la asociación y el registro de servicios adicionales. Si se proporciona al M2MO información (aproximada o explícita) con respecto a la localización lógica de la conexión de la red de acceso, el M2MO puede dirigir el *mensaje de invitación M2M* explícito 170 hacia esa localización. De lo contrario, el M2MO puede difundir la invitación. Dependiendo de si el M2MO recibe o no una respuesta del dispositivo M2M dentro de un intervalo de tiempo predefinido, puede repetir la transmisión de la invitación hasta que se reciba una respuesta. Téngase en cuenta que si el M2MO desea invitar a más de un dispositivo M2M, el mensaje de invitación M2M contiene ventajosamente una lista con las identidades de todos los dispositivos invitados que potencialmente se encuentran en un área específica. En tal

caso, el dispositivo M2M simplemente necesita determinar si su identidad está incluida en la lista antes de enviar una respuesta al M2MO.

3. El dispositivo M2M se activa y se registra en una red de acceso. El dispositivo ahora puede recibir invitaciones para la suscripción del servicio M2M. Si el dispositivo M2M está preconfigurado con la opción de responder solo a invitaciones M2M explícitas, el dispositivo solo responderá al mensaje de invitación M2M que incluya la identidad específica del dispositivo. Tras recibir una invitación de este tipo, el dispositivo responderá al M2MO correspondiente con una *solicitud de suscripción M2M* 180.

4. El M2MO recibe la solicitud de suscripción. Tras una autenticación recíproca exitosa 190 entre el dispositivo M2MO y el dispositivo M2M, el dispositivo M2MO y el dispositivo M2M establecerán recíprocamente la suscripción 200. Ciertos aspectos de este procedimiento se describirán con mayor detalle a continuación.

Cabe señalar que la secuencia de etapas que se ha expuesto anteriormente es meramente ilustrativa y, en particular, que pueden combinarse o subdividirse una o más de las etapas enumeradas.

Segundo enfoque: el M2MO difunde un anuncio a todos los dispositivos M2M interesados. En este caso, el M2MO no envía invitaciones explícitas, aunque sabe qué dispositivos M2M desean identificar el M2MO y asociarse con el mismo. Como alternativa, el M2MO puede difundir periódicamente un aviso genérico (nivel de aplicación) o un mensaje publicitario; este mensaje es equivalente a la “furgoneta de recogida” en el planteamiento del problema de descubrimiento de hoteles. La frecuencia de difusión depende de las políticas del operador. Con este anuncio periódico, el M2MO pretende notificar a los dispositivos su existencia, de manera que los dispositivos puedan conocer el M2MO e intentar asociarse con el mismo. Evidentemente, el M2MO aceptará las solicitudes de suscripción solo de los dispositivos M2M cuyas identidades sean conocidas por el M2MO debido a que ya se ha aprovisionado de las mismas.

Una secuencia de etapas de acuerdo con este enfoque se muestra en la figura 5 y se describe con mayor detalle a continuación.

1. Al igual que en el primer enfoque, la TPE proporciona al M2MO las credenciales del dispositivo y un conjunto de parámetros que están relacionados con el proceso de conexión del dispositivo y son específicos para el proceso de conexión específico a seguir. La TPE puede obtener esta información del fabricante, de los datos introducidos por el usuario o el propietario del dispositivo M2M a través de una interfaz web o de otras fuentes. La identidad puede representarse, por ejemplo, por la dirección MAC del dispositivo, por un número de serie electrónico o por cualquier otro identificador único que se proporcione previamente al dispositivo durante la fabricación.

2. El M2MO está provisto de una lista de identidades de dispositivos M2M. El M2MO difunde periódicamente un *anuncio M2M* 210 durante el tiempo que uno o más dispositivos M2M permanezcan en esta lista sin haber establecido aún asociaciones de suscripción. Este anuncio a nivel de aplicación incluye la identidad del M2MO y posiblemente un conjunto de parámetros adicionales. Si el M2MO conoce las localizaciones lógicas aproximadas donde los dispositivos M2M pueden conectarse a una red de acceso o acceder a las redes, la transmisión y el reenvío del anuncio M2M pueden estar limitados a ciertas regiones lógicas. Como alternativa, el M2MO puede decidir “inundar” una o más redes de acceso con el anuncio.

3. Un dispositivo M2M recibe el anuncio, lo procesa y decide si debe intentar iniciar el proceso de suscripción al servicio M2M. El dispositivo M2M puede basar esta decisión en ciertos parámetros incluidos en el anuncio, así como en ciertos valores de parámetros que se han proporcionado previamente al dispositivo durante la instalación (un ejemplo de un parámetro que puede proporcionarse previamente es el tipo de servicio ofrecido). Si el dispositivo determina que el M2MO anunciado es un candidato para la suscripción, el dispositivo responde con una solicitud de suscripción M2M 220.

4. El M2MO recibe la solicitud de suscripción. Tras una autenticación recíproca exitosa 230 entre el M2MO y el dispositivo M2M, los dispositivos M2MO y M2M establecen recíprocamente la suscripción 240. Ciertos aspectos de este procedimiento se describen con más detalle a continuación.

Cabe señalar que la secuencia de etapas que se ha expuesto anteriormente es meramente ilustrativa y, en particular, que pueden combinarse o subdividirse una o más de las etapas enumeradas.

Tercer enfoque: el dispositivo M2M avisa de su interés por encontrar un M2MO. El tercer enfoque se realiza al hacer que el dispositivo M2M anuncie su intención de identificar y asociarse con el M2MO adecuado. En este caso, el M2MO espera pasivamente la recepción de anuncios originados en dispositivos M2M. Tras recibir y procesar dichos anuncios, el M2MO se pone en contacto con el dispositivo e intenta establecer una asociación con el mismo.

Una secuencia de etapas de acuerdo con este enfoque se muestra en la figura 6 y se describe con mayor detalle a continuación.

1. La TPE proporciona al M2MO las credenciales del dispositivo y un conjunto de parámetros relacionados con el proceso de conexión del dispositivo y que son específicos del proceso de conexión específico seguido. La TPE puede obtener dicha información del fabricante, de los datos introducidos por el usuario o el propietario del dispositivo M2M a través de una interfaz web o de otras fuentes. La identidad del dispositivo puede

representarse, por ejemplo, por la dirección MAC del dispositivo, por un número de serie electrónico, o por cualquier otro identificador único que se proporcione previamente al dispositivo durante la fabricación.

2. Tan pronto como el dispositivo M2M se active y se registre con una red de acceso, el dispositivo comenzará a difundir periódicamente un *mensaje de presentación de dispositivo M2M* 250, que incluye la identidad del dispositivo.

3. El mensaje de presentación M2M llega a uno o más operadores M2M, que procesan el mensaje y determinan si contactar o no con el dispositivo M2M. En general, un M2MO reconocerá la identidad incluida en el anuncio de presentación M2M como uno del que ya se ha aprovisionado previamente. Ese M2MO envía un *mensaje de invitación M2M explícito* al dispositivo. Este mensaje de invitación es similar al mensaje de invitación M2M expuesto anteriormente en relación con el primer enfoque.

4. Tras recibir el *mensaje de invitación M2M explícito* 260, el dispositivo responde al M2MO correspondiente con una *solicitud de suscripción M2M* 270.

5. El M2MO recibe la solicitud de suscripción. Tras una autenticación recíproca exitosa 280 entre el M2MO y el dispositivo M2M, el M2MO y el dispositivo M2M establecen recíprocamente la suscripción 290. Ciertos aspectos de este procedimiento se exponen con mayor detalle a continuación.

Cabe señalar que la secuencia de etapas que se ha expuesto anteriormente es meramente ilustrativa y, en particular, que pueden combinarse o subdividirse una o más de las etapas enumeradas.

Soporte para los tres enfoques. Dependiendo del software preconfigurado y el modo de funcionamiento de los dispositivos y el equipo M2MO, el M2MO y el dispositivo M2M pueden activar el funcionamiento de acuerdo con cada uno de los tres enfoques descritos anteriormente, o bien individualmente o en combinaciones paralelas. En el caso del funcionamiento en una combinación paralela de enfoques, un dispositivo M2M puede procesar y responder a los mensajes originados a partir de un M2MO de acuerdo con cualquiera de los tres enfoques. De manera similar, el M2MO puede transmitir tanto invitaciones explícitas como anuncios periódicos de acuerdo con cualquiera de los enfoques.

Establecimiento de suscripción de dispositivo. El establecimiento de la suscripción del servicio M2M se inicia después de la transmisión del *mensaje de solicitud de suscripción M2M* desde el dispositivo M2M al M2MO, y después de la autenticación recíproca entre el M2MO y el dispositivo M2M (la autenticación recíproca se logrará habitualmente usando una contraseña temporal, como se describe a continuación). En la figura 7, a la que ahora se dirige la atención, se representa un procedimiento de establecimiento de suscripción.

El proceso de establecimiento de suscripción incluye varios procesos. Un proceso constitutivo es el arranque de las credenciales de seguridad permanentes que se usarán para el registro de servicio. Otro posible proceso constituyente es el establecimiento de los valores acordados para ciertos parámetros relacionados con la suscripción de servicio.

El procedimiento de establecimiento de suscripción se ejecuta entre el dispositivo M2M y una entidad funcional de arranque (por ejemplo, un servidor adecuado) que pertenece al M2MO. Por ejemplo, la entidad funcional de arranque puede ser un servidor de aplicaciones, como se ve, por ejemplo, en la figura 3, que comunica de manera segura las credenciales de seguridad permanentes generadas recíprocamente al servidor de autenticación M2M.

Si el dispositivo M2M y el M2MO deciden continuar con el establecimiento de la suscripción después de la autenticación recíproca 300, el dispositivo M2M envía una *solicitud de arranque de servicio M2M* 310 al M2MO, como se ve en la figura 7. El M2MO responde enviando una *respuesta de arranque de servicio M2M* 320 al dispositivo M2M. Tras la recepción exitosa de este mensaje, el dispositivo M2M envía un *arranque de servicio completado M2M* 330 al M2MO, que finaliza el protocolo de reconocimiento de suscripción. Este protocolo de reconocimiento de tres etapas entre el dispositivo M2M y el M2MO puede facilitar cualquiera de los diversos protocolos para el arranque de las credenciales de seguridad. Los protocolos adecuados incluyen IBAKE, PAK y el establecimiento de suscripción basado en certificados, entre otros.

Después del arranque, el M2MO puede enviar opcionalmente un mensaje de verificación 340 al dispositivo M2M. A continuación, el dispositivo M2M confirma 350 el arranque exitoso de las credenciales de seguridad permanentes. El M2MO puede responder al mensaje de confirmación con un mensaje 360 que incluye los parámetros de registro de servicio.

En general, los parámetros de servicio y suscripción dependen de la aplicación. Tomando, como la aplicación M2M, el ejemplo específico de medición de servicio a modo de ilustración, los parámetros pueden incluir (sin limitación): identidad permanente, identidad de grupo, identidad de servidor anfitrión, intervalos de frecuencia y tiempo para las transmisiones desde el dispositivo y parámetros de difusión para interfaces de gestión.

Consideraciones de seguridad. En la exposición anterior sobre las técnicas de establecimiento de identificación y suscripción M2MO, se supone que la identidad del dispositivo M2M se ha proporcionado previamente a un solo M2MO legítimo que, en consecuencia, responde a las solicitudes de suscripción M2M. Además, ciertos procedimientos de seguridad que deben seguirse antes y durante el establecimiento de la suscripción pueden

permitir que el dispositivo M2M determine si un M2MO candidato es legítimo y si es el M2MO adecuado para la suscripción de servicio. Se determina si se trata del M2MO “adecuado” en función de su identidad y el éxito de la autenticación recíproca.

Un dispositivo M2M estará de acuerdo en establecer la suscripción y registrarse para el servicio solo si se verifica la identidad del M2MO, asegurando de este modo que no es un M2MO fraudulento. De manera similar, el M2MO necesita verificar en primer lugar las credenciales del dispositivo M2M antes de continuar con el establecimiento de suscripción.

Una manera de realizar las verificaciones requeridas usa una *contraseña temporal* asociada con la identidad del dispositivo M2M. Esta contraseña se proporciona tanto al dispositivo M2M como al M2MO durante una etapa sin conexión. Más específicamente, la contraseña temporal se proporciona previamente al dispositivo M2M durante la fabricación. Antes de la activación inicial del dispositivo, la contraseña se proporciona (sin conexión) por la TPE al M2MO junto con la identidad del dispositivo M2M (la TPE puede obtener la contraseña y los datos de identificación del fabricante del dispositivo o de otras fuentes).

El M2MO y el dispositivo M2M pueden usar la contraseña temporal para autenticarse recíprocamente *antes del establecimiento de suscripción*. Cualquiera de los diversos procedimientos de autenticación conocidos puede usarse para la operación de autenticación. Uno de estos procedimientos es el protocolo AKA (autenticación y acuerdo de clave), descrito, por ejemplo, en el proyecto de asociación de tercera generación, 3GPP, *especificaciones técnicas 3GPP TS 33.102 V9.0.0*: Technical Specification Group Services and System Aspects; 3G Security; Security Architecture, septiembre de 2009.

Al usar la contraseña temporal con un procedimiento de autenticación adecuado, el dispositivo M2M puede garantizar que el M2MO es el adecuado. El procedimiento de autenticación también desalienta a otros operadores M2M de la práctica abusiva de atraer deliberadamente al dispositivo M2M con el fin de negarle la oportunidad de asociarse con el M2MO adecuado.

Cabe señalar en este sentido que la autenticación basada en una *contraseña temporal* es solo un ejemplo, y que también pueden usarse diversas alternativas.

Por ejemplo, una alternativa es una libreta de un solo uso (OTP) creada por el M2MO y cifrada por IBE con la identidad del dispositivo M2M. El dispositivo M2M descifra la libreta de un solo uso y la devuelve al M2MO, proporcionando de este modo al M2MO su capacidad para descifrar la OTP y, por lo tanto, autenticándose a sí mismo ante el M2MO. Para una exposición de la OTP, véase N. Haller et al., *A One-Time Password System*, RFC2289, http://www.ietf.org/rfc/rfc2289.txt.

En otro procedimiento alternativo, el dispositivo M2M conserva la contraseña y la usa como la huella de CHAP PW para autenticarse a sí mismo ante el M2MO. Para una exposición de CHAP PW, véase W. Simpson, *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994. http://www.faqs.org/rfcs/rfc1994.html.

En las transacciones ideales, un M2MO legítimo y no comprometido responde a las solicitudes de suscripción M2M solo de los dispositivos M2M cuyas identidades ya son conocidas para el M2MO. Debido a que un M2MO legítimo no obtendrá ningún beneficio relacionado con el negocio intentando establecer una suscripción de servicio con un dispositivo desconocido, un M2MO legítimo (idealmente) ignorará o rechazará las solicitudes de suscripción de todos los dispositivos M2M cuyas identidades no se hayan proporcionado *a priori*.

A continuación, se desea señalar la razón por la que es ventajoso recurrir a protocolos de seguridad tales como IBAKE o PAK tras una autenticación recíproca exitosa: estos protocolos garantizan que la clave permanente establecida solo se conocerá por el dispositivo M2M y el M2MO. En particular, la TPE y el fabricante del dispositivo no conocerán la clave de arranque permanente.

CONTENIDOS Y FORMATOS DE MENSAJE

A continuación, se proporcionarán ejemplos de formatos que pueden usarse para los mensajes intercambiados entre el M2MO y el dispositivo M2M en el curso de la fase de descubrimiento M2MO.

(1) **Invitación** M2M**:** este mensaje se envía desde el M2MO al dispositivo M2M en los siguientes dos casos:

(a) El M2MO conoce la identidad del dispositivo y, por lo tanto, envía proactivamente una invitación M2M explícita al dispositivo (o a una lista de dispositivos).
(b) El M2MO recibe un *mensaje de presentación de dispositivo M2M* (véase a continuación) de un dispositivo M2M y responde con una invitación M2M a ese dispositivo (o lista de dispositivos).

Un datagrama de mensaje de *invitación M2M* a modo de ejemplo está estructurado como se muestra en la figura 8. La estructura ilustrada puede integrarse, por ejemplo, como una carga útil en paquetes TCP/UDP/IP. La *invitación*

M2M contiene ventajosamente la siguiente información, entre otros parámetros de comunicación:
Versión: para especificar la versión del protocolo de capa de aplicación de este paquete.

Tipo: para especificar el tipo de este paquete, por ejemplo, “M2M_INVITATION”.

Identidad M2MO: para identificar el operador M2M, como se define en la o las normas específicas que se adopten.

Prioridad: para indicar opcionalmente la prioridad de envío para este mensaje.

Identificadores (ID) de cuenta: para identificar el número de identidades de dispositivos M2M (a las que se destina la invitación) incluidas en este mensaje.

Tipo de autenticación: para indicar el método de autenticación de acuerdo con el cual el o los dispositivos M2M que reciben esta invitación pueden verificar que el M2MO es legítimo. Un paquete con un tipo de autenticación desconocida debería descartarse por los dispositivos M2M.

Intervalo de invitación: para identificar opcionalmente el intervalo de tiempo entre invitaciones. En ciertas ocasiones, con los dispositivos M2M mal configurados, puede necesitarse este valor; también puede usarse como una contramedida contra los ataques de denegación de servicio.

Suma de verificación: para ayudar a los dispositivos receptores en la detección de corrupción de datos en el mensaje de *invitación M2M*. Se encuentra una descripción de las prácticas conocidas relacionadas con la suma de verificación, por ejemplo, en R. Braden et al., RFC 1071, *Computing the Internet Checksum*, http://www.faqs.org/rfcs/rfc1071.html.

Identidad de dispositivo M2M (x): para identificar los receptores de dispositivos M2M previstos que el M2MO pretende atraer. En la invitación M2M puede incluirse una lista de identidades, para todos los dispositivos a los que el M2MO desea llegar a través de este mensaje. Dependiendo de la disponibilidad de la información de localización durante la activación inicial de los dispositivos M2M, diferentes invitaciones M2M (potencialmente simultáneas) (enviadas a diferentes localizaciones) pueden contener diferentes listas de identidades de dispositivos M2M.

Parámetros de servicios M2M: para identificar opcionalmente parámetros preliminares que pueden ser útiles para los dispositivos M2M antes de la suscripción. Como ejemplo, el campo puede incluir información sobre el tipo de servicios M2M ofrecidos, etc.

Datos de autenticación: para contener información relacionada con el campo *tipo de autenticación*, en relación con el método de autenticación y los parámetros con los que un dispositivo M2M puede verificar la identidad del M2MO que envía la invitación.

(2) ***Anuncio M2M***: este mensaje se envía periódicamente desde el M2MO; es de naturaleza de difusión y no se dirige específicamente a ningún dispositivo M2M en particular.

Un datagrama de mensaje de *anuncio M2M* a modo de ejemplo está estructurado como se ilustra en la figura 9.

El mensaje de *anuncio M2M* puede contener versión, tipo, identidad M2MO, prioridad, tipo de autenticación, intervalo de anuncio, suma de verificación, datos de autenticación, y otros parámetros de servicios M2M.

El mensaje anterior puede integrarse como carga útil en paquetes TCP/UDP/IP. Los campos que constituyen la estructura son similares a los campos del mensaje de *invitación M2M*. Sin embargo, puesto que el anuncio no se destina explícitamente a ningún dispositivo M2M en particular, el mensaje no incluye ninguna identidad de dispositivo M2M ni el campo de *ID de cuenta*. Como alternativa, el formato de datagrama de la *invitación M2M* puede reutilizarse en este caso, en el que el campo *tipo* especificaría que se trata de un *anuncio M2M*, el valor de *ID de cuenta* se establecería en el valor “predeterminado” de cero, mientras que el o los campos de *identidad de dispositivo M2M* también se establecerían como NULOS, lo que indica que este es un mensaje de difusión.

(3) ***Presentación de dispositivo M2M***: la *presentación de dispositivo M2M* es un mensaje de difusión que se origina en un dispositivo M2M tras registrarse en una red de acceso. Este mensaje se usa por el dispositivo M2M en sus intentos por llegar a uno o más operadores M2M candidatos. Un datagrama de mensaje de *presentación de dispositivo M2M* a modo de ejemplo está estructurado como se ilustra en la figura 10.

El mensaje de *presentación de dispositivo M2M* puede contener versión, tipo, identidad de dispositivo M2MO, prioridad, tipo de autenticación, intervalo de transmisión, suma de verificación, datos de autenticación, y otros parámetros de servicios M2M.

El mensaje anterior puede integrarse como carga útil en paquetes TCP/UDP/IP. La estructura es similar a la estructura del mensaje de *anuncio M2M*. La única diferencia es que el campo *identidad de dispositivo M2M* ha

reemplazado al campo *identidad M2MO* (sin embargo, cabe señalar que el mensaje de *presentación de dispositivo M2M* puede incluir diferentes parámetros de servicios M2M, o diferentes valores de parámetros, de los que se usarían en el mensaje de *anuncio M2M*). De nuevo, como alternativa, puede reutilizarse en este caso el formato de datagrama de la *invitación M2M*, en el que el campo *tipo* especificaría que se trata de una *presentación de dispositivo M2M*, la identidad de dispositivo M2M reemplazaría a la identidad M2MO, el valor de *ID de cuenta* se establecería en el valor "predeterminado" de cero, mientras que el o los campos de *identidad de dispositivo M2M* también se establecerían como NULOS, lo que indica que este es un mensaje de difusión.

Se entenderá que los métodos descritos en el presente documento son adecuados para la implementación en cualquier red que soporte un entorno M2M. Dichas redes pueden ser fijas, inalámbricas o una combinación de redes fijas e inalámbricas. Como se describe en el presente documento, los métodos pueden aplicarse, en particular, a las redes que soportan la comunicación de paquetes de acuerdo con el conjunto de protocolos IP, pero los métodos no están limitados en la aplicación a redes de ese tipo. Se entenderá además que un "servidor", tal como este término se usa en el presente documento, es una funcionalidad de software que puede ejecutarse en cualquier máquina informática adecuada que tenga una interfaz de red; dicha máquina puede ser, por ejemplo, un ordenador digital de propósito general o especial o una serie de dichos ordenadores.

REIVINDICACIONES

1. Un método a realizar por una entidad de red (30, 40), que comprende:

recibir de un servidor (20) un identificador de una entidad cliente (10) autorizada para un servicio;
almacenar automáticamente el identificador en un medio de almacenamiento digital para su uso en la identificación de la llegada, en un momento no especificado, de un mensaje desde la entidad cliente (10);
recibir una comunicación digital desde la entidad cliente (10), conteniendo la comunicación de la entidad cliente el identificador e indicando que la entidad cliente (10) se ha conectado a una red de comunicaciones;
antes o después de recibir la comunicación de la entidad cliente, publicitar la entidad de red (30, 40) a la entidad cliente (10) como parte cooperativa para proporcionar el servicio, en donde dicha etapa de publicidad se realiza generando y transmitiendo automáticamente al menos un mensaje en la red de comunicaciones;
después de recibir la comunicación de la entidad cliente, autenticar la entidad cliente (10) a través de una secuencia de etapas automáticas, a condición de que el identificador recibido en la comunicación de la entidad cliente coincida con el identificador recibido en la comunicación del servidor;
establecer una asociación de seguridad permanente con la entidad cliente; e
iniciar el servicio con la entidad cliente (10).

2. El método de la reivindicación 1, en el que la etapa de publicidad se realiza, antes de recibir la comunicación de la entidad cliente, transmitiendo en la red de comunicaciones una pluralidad de mensajes repetidos que contienen información que identifica a la entidad cliente.

3. El método de la reivindicación 2, en el que la pluralidad de mensajes repetidos se transmiten a múltiples entidades cliente.

4. El método de la reivindicación 2, en el que la pluralidad de mensajes repetidos se envían a una única entidad cliente.

5. El método de la reivindicación 1, en el que la etapa de publicidad se realiza en respuesta a la recepción de la comunicación de la entidad cliente.

6. El método de la reivindicación 1, en el que la entidad de red es un operador máquina a máquina y la entidad cliente es un dispositivo máquina a máquina.

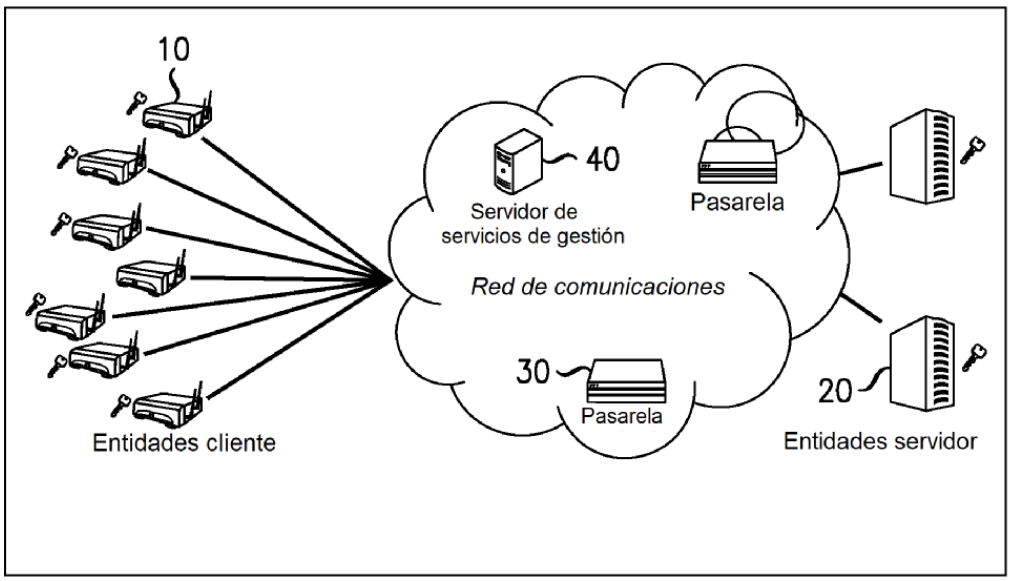
10
40
Servidor de
servicios de gestión
Pasarela
Red de comunicaciones
30
Pasarela
20
Entidades cliente
Entidades servidor

FIG. 1

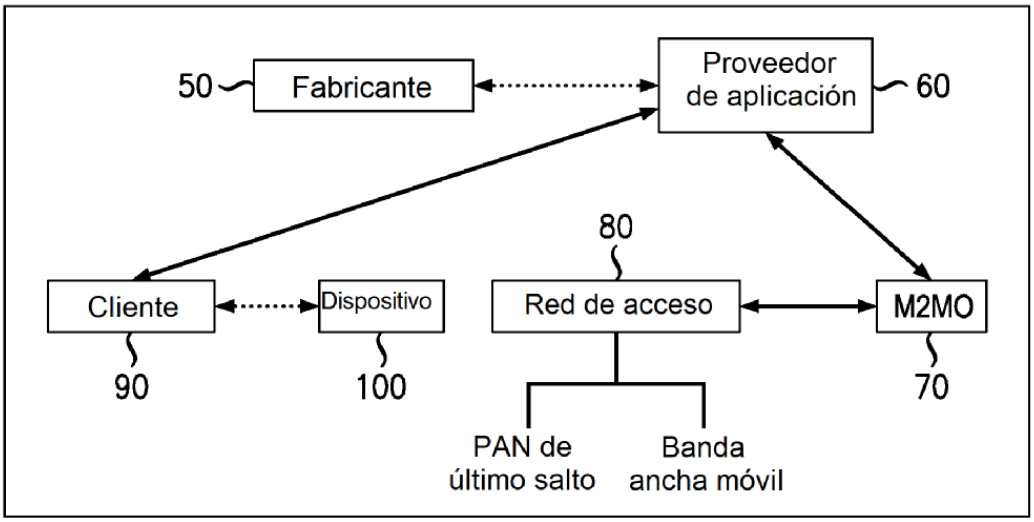
50
Fabricante
Proveedor
de aplicación
60
80
Cliente
Dispositivo
Red de acceso
M2MO
90
100
70
PAN de
último salto
Banda
ancha móvil

FIG. 2

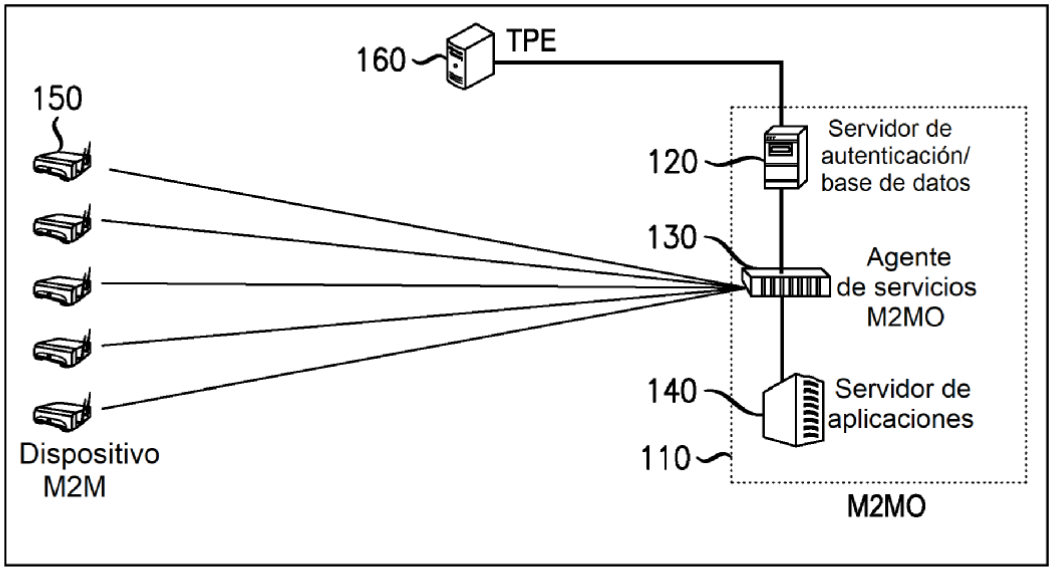
160
TPE
150
120
Servidor de autenticación/ base de datos
130
Agente de servicios M2MO
140
Servidor de aplicaciones
110
Dispositivo M2M
M2MO

FIG. 3

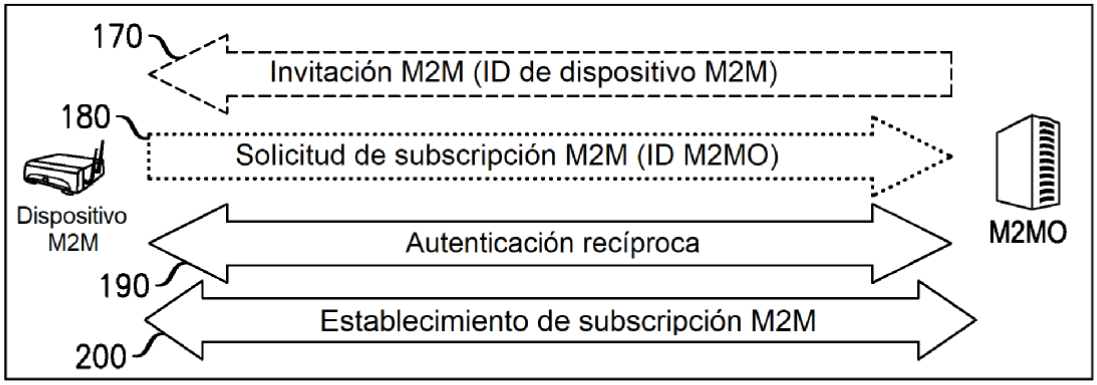
170
Invitación M2M (ID de dispositivo M2M)
180
Solicitud de subscripción M2M (ID M2MO)
Dispositivo M2M
M2MO
Autenticación recíproca
190
Establecimiento de subscripción M2M
200

FIG. 4

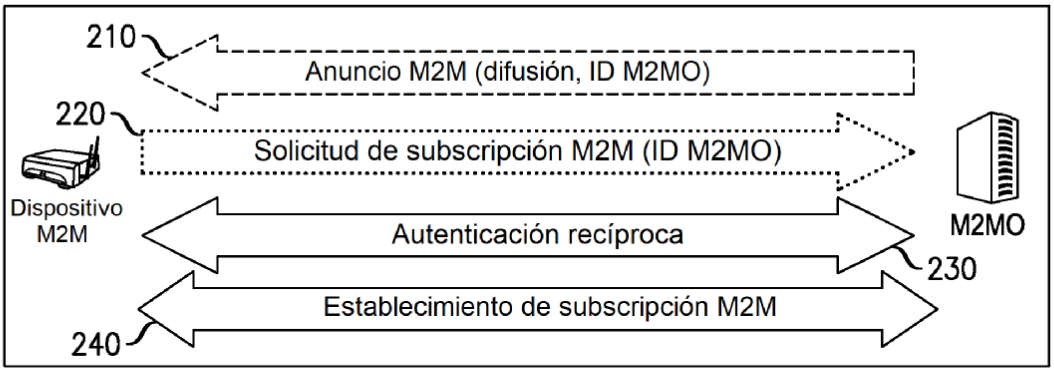
210
Anuncio M2M (difusión, ID M2MO)
220
Solicitud de subscripción M2M (ID M2MO)
Dispositivo M2M
M2MO
Autenticación recíproca
230
Establecimiento de subscripción M2M
240

FIG. 5

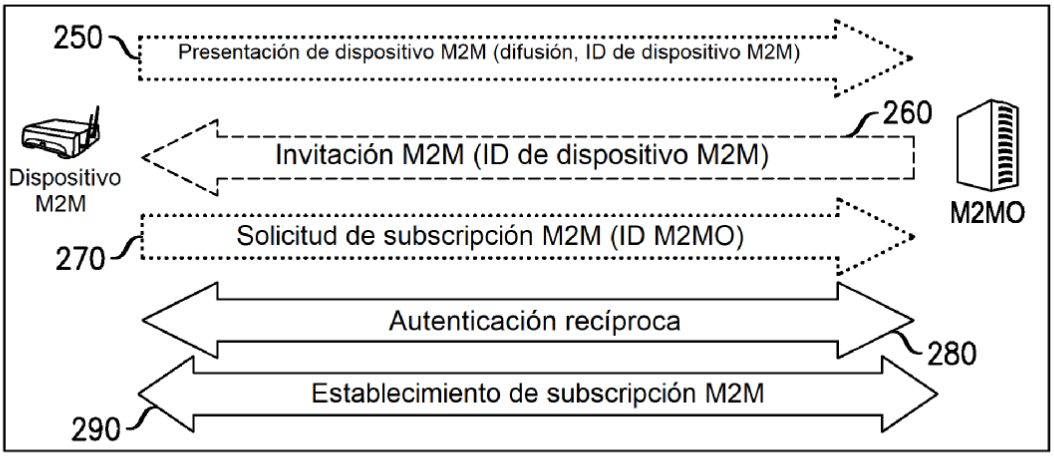
250
Presentación de dispositivo M2M (difusión, ID de dispositivo M2M)
260
Invitación M2M (ID de dispositivo M2M)
Dispositivo M2M
M2MO
Solicitud de subscripción M2M (ID M2MO)
270
Autenticación recíproca
280
Establecimiento de subscripción M2M
290

FIG. 6

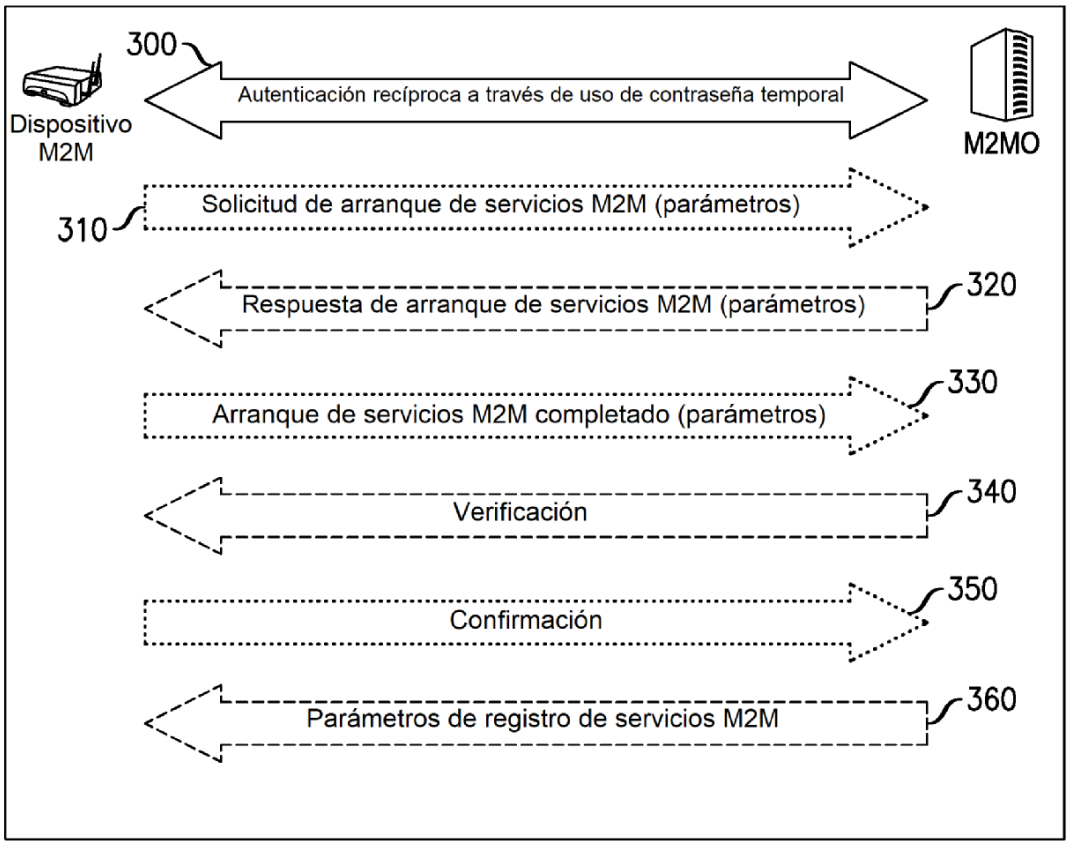
300
Autenticación recíproca a través de uso de contraseña temporal
Dispositivo M2M
M2MO
310
Solicitud de arranque de servicios M2M (parámetros)
320
Respuesta de arranque de servicios M2M (parámetros)
330
Arranque de servicios M2M completado (parámetros)
340
Verificación
350
Confirmación
360
Parámetros de registro de servicios M2M

FIG. 7

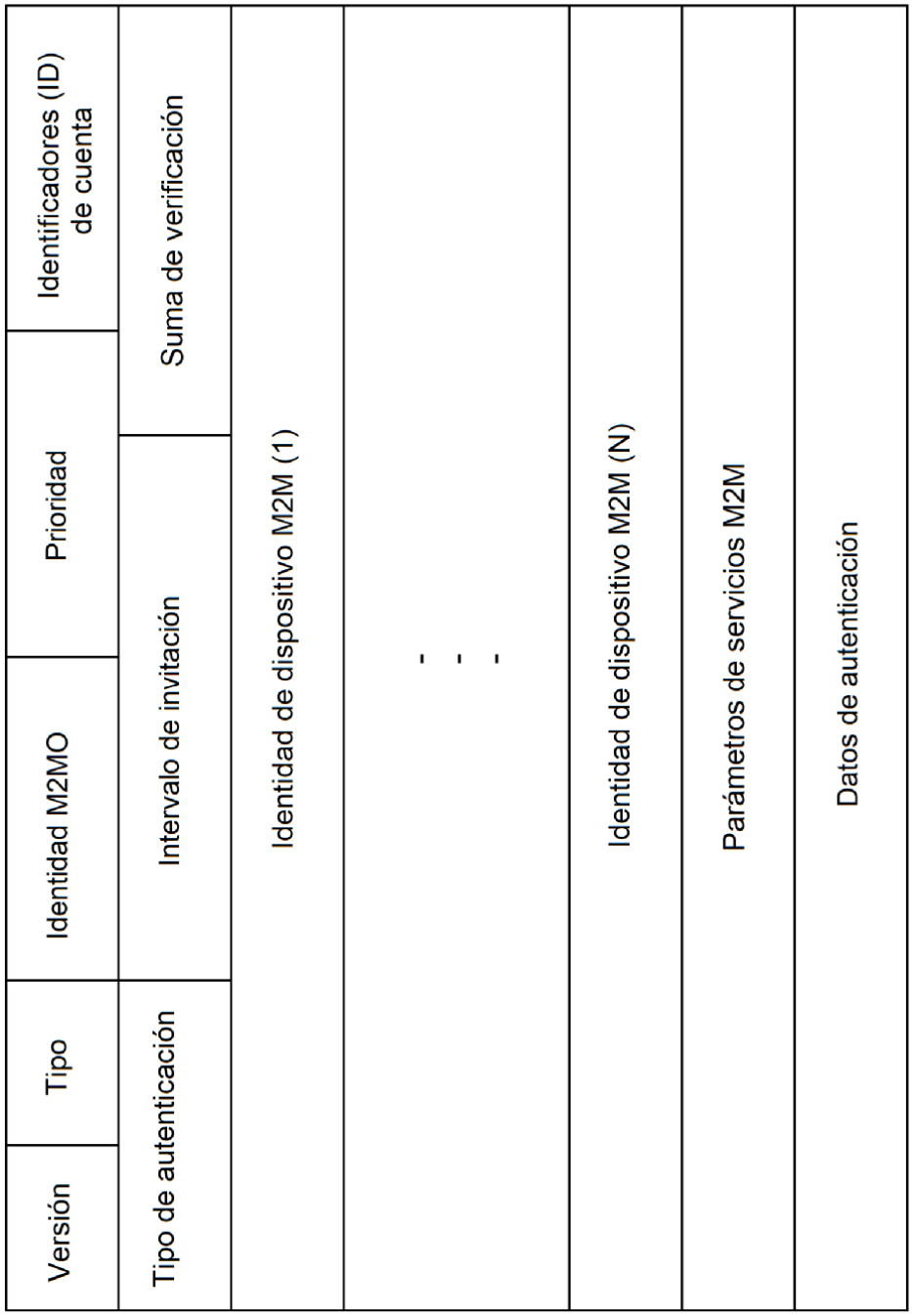
Versión
Tipo
Identidad M2MO
Prioridad
Identificadores (ID) de cuenta
Tipo de autenticación
Intervalo de invitación
Suma de verificación
Identidad de dispositivo M2M (1)
-
-
-
Identidad de dispositivo M2M (N)
Parámetros de servicios M2M
Datos de autenticación

FIG. 8

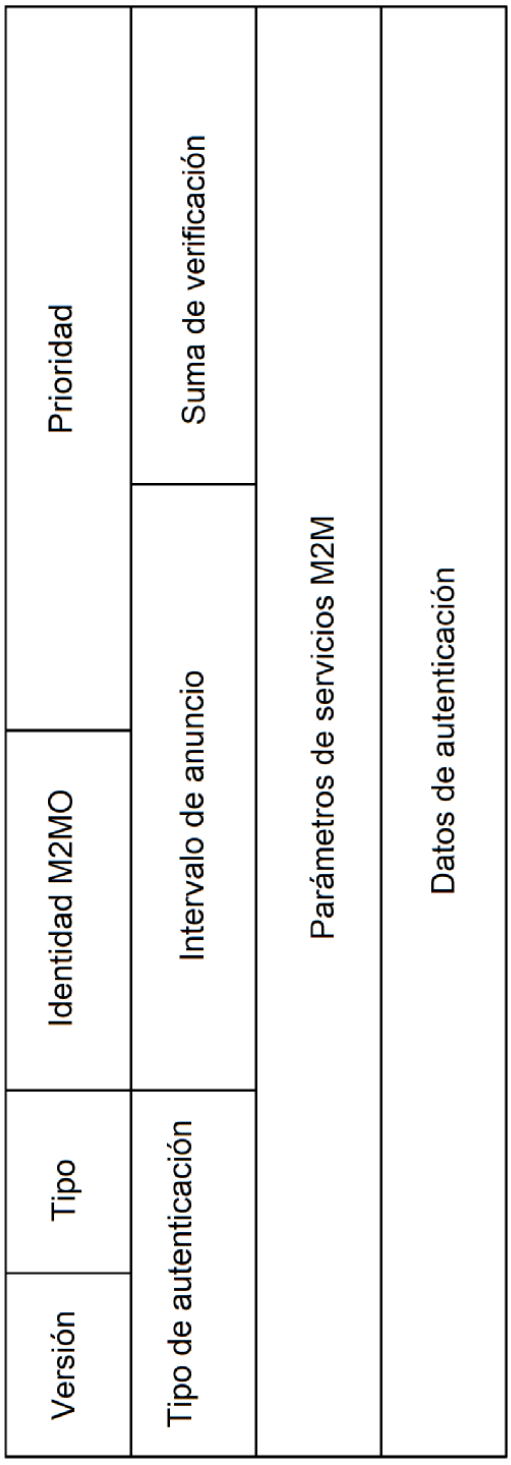
Versión
Tipo
Identidad M2MO
Prioridad
Tipo de autenticación
Intervalo de anuncio
Suma de verificación
Parámetros de servicios M2M
Datos de autenticación

FIG. 9

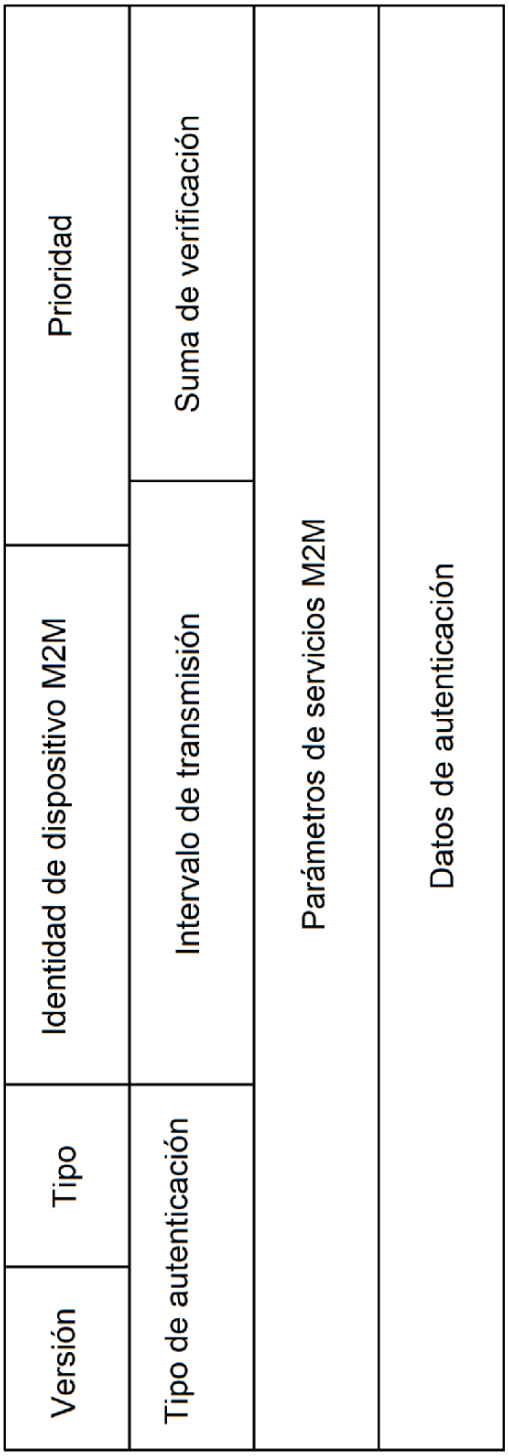
Versión
Tipo
Identidad de dispositivo M2M
Prioridad
Tipo de autenticación
Intervalo de transmisión
Suma de verificación
Parámetros de servicios M2M
Datos de autenticación

FIG. 10