(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 748 112**

(51) Int. CI.:

H04W 8/20 (2009.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.06.2011 E 11290280 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2538707**

(54) Título: **Método para cargar credenciales de suscriptor y equipo asociado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2020

(73) Titular/es:

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

(72) Inventor/es:

CONTE, ALBERTO y
CHAKRI, AL MAHDI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método para cargar credenciales de suscriptor y equipo asociado

Antecedentes de la invención

La presente invención se refiere al campo de la identificación en comunicaciones inalámbricas y, más específicamente, a las credenciales necesarias para identificar un equipo de usuario en una red inalámbrica.

En el estado de la técnica, la autentificación de un suscriptor de una red inalámbrica está asegurada mediante el uso de tarjetas de Módulo de identidad del suscriptor (SIM) (en tecnología 2G) y Tarjeta de circuito integrado universal (UICC) (en tecnologías 3G y Evolución a largo plazo (LTE)). El uso actual de tales tarjetas proporciona alta seguridad, pero también es muy restrictivo. De hecho, las tarjetas SIM o UICC establecen una conexión exclusiva entre dicha tarjeta y un operador de red. Como consecuencia, el suscriptor tiene que cambiar de tarjeta si quiere cambiar de operador de red, lo que puede ser problemático en el caso de un gran despliegue de equipos de máquina a máquina, ya que las tarjetas de todos los equipos tendrían que cambiarse. Además, En la tecnología de interoperabilidad mundial para acceso de microondas (WiMAX), se brinda la posibilidad de lograr un aprovisionamiento por aire para dispositivos Wimax en blanco (es decir, dispositivos Wimax que aún no están conectados a un operador de red) que permite suscribirse de forma remota y obtener un adjunto a un operador Wimax.

Sin embargo, dicha función remota no está disponible en redes 2G, 3G o LTE principalmente por razones de seguridad debido a la dificultad de asegurar una seguridad lo suficientemente alta en la transferencia por aire de las credenciales.

Los documentos "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment (Versión 9)" y US 2009/205028 A1 divulgan el aprovisionamiento de dispositvos M2M.

Sumario de la invención

Por lo tanto, es un objetivo de la presente invención asegurar una transferencia segura de credenciales para configurar tarjetas SIM o UICC en redes 2G, 3G y LTE. Este objetivo se consigue mediante un método que tiene las características de la reivindicación 1, un servidor de autentificación que tiene las características de la reivindicación 13 y un módulo de identidad integrado que tiene las características de la reivindicación 14. Realizaciones ventajosas se definen en las respectivas reivindicaciones dependientes.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que representa la etapa diferente de una primera realización de la presente invención;
La figura 2 es un diagrama de un equipo de usuario y sus conexiones con entidades de red en un primer esquema de configuración;
La figura 3 es un diagrama de un equipo de usuario y sus conexiones con entidades de red en un segundo esquema de configuración;
La figura 4 es un diagrama de bloques que representa la etapa diferente de una segunda realización de la presente invención;
La figura 5 es un diagrama de un equipo de usuario y sus conexiones con entidades de red en un tercer esquema de configuración;

Descripción detallada de la invención

Como se usa en el presente documento, el término "SIM" se refiere al acrónimo Módulo de identidad del suscriptor;
Como se usa en el presente documento, el término "UICC" se refiere al acrónimo Tarjeta de circuito integrada universal;
Como se usa en el presente documento, el término "USIM" se refiere al acrónimo Módulo de identidad del suscriptor universal;
Como se usa en el presente documento, el término "LTE" se refiere al acrónimo Evolución a largo plazo;
Como se usa en el presente documento, el término "WIMAX" se refiere al acrónimo Interoperabilidad mundial para acceso de microondas;
Como se usa en el presente documento, los términos "2G" y "3G" se refieren respectivamente a la expresión segunda generación y tercera generación;
Como se usa en el presente documento, el término "IMSI" se refiere al acrónimo Identidad de suscriptor móvil internacional;
Como se usa en el presente documento, el término "EAP" se refiere al acrónimo Protocolo de autentificación extensible;

Como se usa en el presente documento, el término "TTLS" se refiere al acrónimo Seguridad de capa de transporte en túnel;
Como se usa en el presente documento, el término "TLS" se refiere al acrónimo Seguridad de capa de transporte;
Como se usa en el presente documento, el término "OMA-DM" se refiere al acrónimo Gestión de dispositivos de alianza móvil abierta;
Como se usa en el presente documento, el término "GPS" se refiere al acrónimo Sistema de posicionamiento global;

Las realizaciones de la presente invención se refieren a un método para cargar de forma segura credenciales de suscriptor desde un servidor remoto a un equipo de usuario.

La figura 1 representa un diagrama de bloques con las diferentes etapas del método y la figura 2 representa un ejemplo de una estructura de red y las conexiones establecidas con el equipo de usuario 1 durante las etapas del método, dichas conexiones siendo conexiones inalámbricas.

La primera etapa 101 se refiere a la implementación, por el fabricante del equipo de usuario, de un certificado X. 509, una pila de protocolo de establecimiento de túnel y una autentificación de cliente dentro de un módulo de identidad integrado 3 de un equipo de usuario 1. La autentificación del cliente se refiere a los parámetros del módulo de identidad de suscriptor universal (USIM) provisional, por ejemplo, una clave secreta provisional y una identidad de suscriptor móvil internacional (IM-SI) provisional. Dichos parámetros provisionales de USIM son proporcionados por una entidad dedicada de la red 2 en este documento denominada Autoridad de autentificación primaria (PAA) 5 que corresponde a una autoridad de la red 2 capaz de establecer una conexión entre un equipo de usuario 1 y un servidor remoto de la red 2. La implementación del certificado X. 509, la pila de protocolos de establecimiento de túnel y la autentificación del cliente se consiguen mediante el fabricante del módulo de identidad integrado 3 o mediante el fabricante del equipo del usuario 1. Además, cabe señalar que el módulo de identidad integrado 3 puede referirse a una tarjeta SIM o una UICC.

La segunda etapa 102 se refiere al establecimiento de una conexión segura entre un servidor de autentificación remota 7 de un operador de red Noi con i = 1, 2, 3 y el equipo de usuario 1 y comprende las siguientes subetapas:

- La primera subetapa 201 corresponde a la activación del equipo de usuario 1 y la autentificación de dicho equipo de usuario 1 por la PAA 5 utilizando la autentificación del cliente incrustada en el módulo de identidad integrado 3 del equipo de usuario 1. La PAA 5 permite así establecer una conexión inicial con un servidor de la red 2. Sin embargo, cabe señalar que la PAA no proporciona ningún servicio (llamadas, conexiones a Internet...) que no sean la conexión inicial hacia un servidor de lanzamiento 9 del fabricante del equipo del usuario y un servidor de autentificación 7 de un operador de red NO.
- La segunda subetapa 202 corresponde a la conexión del equipo de usuario a un servidor de lanzamiento 9 del fabricante del equipo del usuario. Esto puede hacerse mediante un script automático instalado en el equipo de usuario 1. El operador de red es elegido (ya sea por el usuario (a través de su equipo de usuario 1) o por el fabricante del equipo de usuario, según la configuración), por ejemplo, el operador de red NO2 en la figura 2, convirtiéndose el usuario en suscriptor de NO2. También se genera y se guarda una clave de seguridad en el equipo de usuario 1 en un lado y se envía, mediante el servidor de lanzamiento 9, al servidor de autentificación 7 del operador de red elegido NO2 en el otro lado.
- La tercera subetapa 203 corresponde al establecimiento por parte del operador de red elegido NO2 de una sesión de gestión segura entre el servidor de autentificación 7 de dicho operador de red elegido NO2 y el equipo de usuario 1. Tal sesión se puede lograr, por ejemplo, utilizando un protocolo de criptografía simétrica utilizando la clave de seguridad generada en la etapa 202.

La tercera etapa 103 corresponde al establecimiento de un túnel seguro 11 entre el módulo de identidad integrado 3 y el servidor de autentificación 7 del NO2 a través de la conexión segura establecida. De hecho, los protocolos de gestión UICC existentes permiten configurar todos los parámetros USIM, excepto la clave secreta, de modo que es necesario establecer un túnel para cargar dicha clave secreta. Tal establecimiento se logra utilizando la pila de protocolos de establecimiento de túnel integrada en el módulo de identidad integrado 3 y el uso del certificado X. 509 para asegurar la protección de seguridad del túnel 11. Se pueden usar diferentes protocolos para establecer el túnel seguro 11 como, por ejemplo, un protocolo de autentificación extensible (EAP). La pila de protocolos de establecimiento de túnel corresponde, por ejemplo, a un cliente de seguridad de capa de transporte en túnel de protocolo de autentificación extensible (EAP-TTLS) y la autentificación para el establecimiento del túnel 11 se realiza basándose en EAP-TTLS y conduce a la creación de un túnel de transporte de seguridad de capa (TLS) 11 entre el módulo de identidad integrado 3 y el servidor de autentificación 7.

La cuarta etapa 104 corresponde a la carga de las credenciales de suscriptor desde el servidor de autentificación 7 del NO2 en el módulo de identidad integrado 3 a través del túnel seguro establecido 11. De hecho, para cargar de forma segura las credenciales de suscriptor, la carga debe ser "opaca" para el equipo de usuario 1, es decir, que el equipo de usuario 1 no debe poder leer las credenciales del suscriptor.

Por lo tanto, la configuración del túnel TLS permite la carga de las credenciales desde el servidor de autentificación 7 al módulo de identidad integrado 3 mientras evita el manejo de dichas credenciales por parte del equipo de usuario

1. Además, la pila de protocolos de establecimiento de túnel permite la instalación de las credenciales en el módulo de identidad integrado 3.

Las credenciales de suscriptor se refieren al menos a un parámetro de un módulo de identidad de suscriptor universal (USIM). Dependiendo de las realizaciones, solo se puede cargar la clave secreta u otros parámetros USIM tales como el IMSI. Sin embargo, como la capacidad de la unidad central de procesamiento (CPU) del módulo de identidad integrado 3 es generalmente limitada, puede preferirse cargar solo la clave secreta. En tal caso, los otros parámetros USIM, tal como el IMSI, se puede cargar utilizando un método de gestión UICC clásico como Gestión de dispositivos de alianza móvil abierta (OMA-DM), por ejemplo.

Cuando se cargan las credenciales del suscriptor, el suscriptor puede acceder a los servicios proporcionados por el operador de red al que está conectado el equipo de usuario (NO2 en el presente caso).

Si posteriormente, por ejemplo, al final del contrato de suscripción, el suscriptor o el fabricante del equipo del usuario según la configuración, decide cambiar de operador de red, por ejemplo, debido a una mejor oferta de otro operador de red (NO3, por ejemplo). El proceso de cambio de un operador a otro se logra simplemente enviando, desde el servidor de lanzamiento 9 del fabricante del equipo de usuario una solicitud al servidor de autentificación 7 del operador de red NO3 recientemente elegido para instalar un nuevo USIM en el módulo de identidad integrado 3 del equipo de usuario 1. Dicha solicitud es activada por el equipo de usuario 1 del fabricante del equipo de usuario dependiendo de la configuración.

En la recepción de la solicitud, el operador de red NO3 aplica el procedimiento descrito anteriormente en las etapas 102-104 para crear un túnel seguro 13 con el módulo de identidad integrado 3 del equipo de usuario 1 y cargar los nuevos parámetros USIM como se describe en la figura 3.

Para comprender mejor las realizaciones de la presente invención, a continuación se describirá un ejemplo.

El ejemplo se refiere a un fabricante de automóviles que produce automóviles equipados con un sistema de posicionamiento global (GPS) conectado. En este ejemplo, la configuración corresponde a una configuración de despliegue grande en la que el fabricante del automóvil decide la elección del operador de red.

Durante el montaje del automóvil, el fabricante del automóvil instala una UICC con una pila de protocolos de establecimiento de túnel, un certificado X. 509 y una autentificación de cliente que comprende parámetros USIM provisionales proporcionados por la PAA.

Al vender un automóvil, el GPS conectado incrustado en el automóvil se autentifica y autoriza en la red durante su activación inicial gracias a los parámetros provisionales de USIM. Además, un script automático implementado en la UICC activa una conexión inicial hacia el servidor de lanzamiento del fabricante del automóvil en la activación del GPS. El servidor de lanzamiento envía por un lado una clave de seguridad al GPS conectado y al servidor de autentificación y, por otro lado, una solicitud de activación del GPS conectado al servidor de autentificación del operador de red elegido. En la recepción de la solicitud de activación, el servidor de autentificación estableció una sesión de administración segura con el GPS conectado utilizando la clave de seguridad. A continuación, el servidor de autentificación crea un túnel TLS seguro hacia el UICC utilizando la pila de protocolos de establecimiento del túnel y el certificado X. 509 incrustado en la UICC y carga las credenciales del suscriptor en la UICC a través del túnel TLS. Además, el servidor de autentificación puede instalar otra información de configuración, tal como una lista de preferencias de red, una lista de preferencias de itinerancia...

Al final de la carga, el GPS conectado está conectado al operador de red seleccionado y puede acceder a los servicios proporcionados por dicho operador.

Además, en el caso de una decisión del usuario de su operador de red preferido, se puede utilizar un procedimiento más simple en el que no sea necesario una entidad de red dedicada como la PAA. Por lo tanto, de acuerdo con otra realización, las diferentes etapas del método para cargar las credenciales de suscriptor se proporcionan a continuación basándose en el diagrama de bloques presentado en la figura 4 y el diagrama de red de la figura 5.

La primera etapa 1001 corresponde a la etapa 101 de la realización anterior y se refiere a la implementación, por el fabricante del equipo de usuario, de un certificado X. 509, una pila de protocolo de establecimiento de túnel y una autentificación de cliente dentro de un módulo de identidad integrado 3 de un equipo de usuario 1.

La segunda etapa 1002 corresponde al establecimiento de una conexión segura entre un servidor de autentificación remota 7 de un operador de red NOi con i = 1, 2, 3 y el equipo de usuario 1.

Dicha etapa 1002 comprende la subetapa 2001, que es la conexión del equipo de usuario 1 a un servidor de lanzamiento 9 del fabricante del equipo de usuario. Dicha conexión se logra al enchufar, por ejemplo, con un cable 14, el equipo de usuario 1 a un ordenador personal conectado 15. Luego, el usuario inicia sesión en el sitio web del fabricante del equipo del usuario (correspondiente a un servidor de lanzamiento 9 de dicho fabricante) y crea una

cuenta para configurar su suscripción al equipo del usuario 1. Durante esta etapa, el usuario selecciona un operador de red (NO2 en el presente caso) y posiblemente algunos otros detalles de configuración (modelo de suscripción, preferencias de itinerancia...). Luego, el servidor de lanzamiento 9 envía una solicitud de activación al servidor de autentificación 7 del operador de red seleccionado NO2, comprendiendo dicha solicitud la información necesaria, tal como la dirección del Protocolo de Internet (IP), la clave de sesión de gestión... así como el modelo de suscripción seleccionado por el usuario, preferencias de itinerancia... para que el operador de red seleccionado NO2 tenga toda la información necesaria para administrar la conexión del equipo de usuario 1.
La subetapa 2002 se refiere al establecimiento, mediante el servidor de autentificación 7 del operador de red NO2 de una sesión segura con el módulo de identidad integrado 3.

La tercera etapa 1003 corresponde al establecimiento de un túnel seguro 17 entre el servidor de autentificación 7 del operador de red NO2 y el módulo de identidad integrado 3 y se realiza como se describió anteriormente en la etapa 103.

La cuarta etapa 1004 se refiere a la carga e instalación de las credenciales de suscriptor dentro del módulo de identidad integrado 3.

Cuando termina la configuración del módulo de identidad integrado 3, el usuario puede desconectar su equipo del ordenador personal 15 y puede conectarse al operador de red NO2 y obtener acceso a los servicios ofrecidos.

Además, en caso de cambio de operador de red, las etapas 1002-1004 se logran eligiendo otro operador de red para conectarse a dicho nuevo operador de red.

Por lo tanto, las realizaciones de la presente invención permiten una carga remota e instalación de credenciales de suscriptor dentro de un módulo de identidad integrado, al tiempo que aseguran los requisitos de seguridad y confidencialidad gracias al establecimiento de un túnel seguro entre un servidor de autentificación remoto y el módulo de identidad integrado. Dicha solución permite cambiar de un operador a otro sin tener que cambiar o reconfigurar manualmente el módulo de identidad integrado, lo que lleva a la posibilidad de que el operador cambie una gran cantidad de dispositivos sin requerir medios logísticos importantes.

REIVINDICACIONES

1. Método para cargar credenciales de suscriptor desde un servidor de autentificación remoto (7) de un operador de red (NOi) en un equipo de usuario (1) equipado con un módulo de identidad integrado (3) a través de una red (2), en donde dicho módulo de identidad integrado (3) comprende medios para establecer un túnel seguro (11, 13, 17) con el servidor de autentificación remota (7), y en donde dicho método comprende las siguientes etapas:

- instalar (101, 1001) una pila de protocolos de establecimiento de túnel, un certificado X. 509 y una autentificación de cliente en el módulo de identidad integrado (3);
- establecer (102, 1002) una conexión segura entre el servidor de autentificación remoto (7)

y el equipo de usuario (1) que usa la autentificación del cliente mediante:

- establecer una conexión entre el equipo de usuario (1) y un servidor (9) del fabricante del equipo de usuario;
- enviar desde el servidor (9) del fabricante del equipo del usuario al servidor de autentificación remota (7), una solicitud para obtener un adjunto del equipo de usuario (1) al operador de red (NO1, NO2, NO3) correspondiente a dicho servidor de autentificación remota (7),
- establecer mediante el servidor de autentificación remoto (7) la conexión segura utilizando una sesión de gestión segura,
- establecer (103, 1003) el túnel seguro (11, 13, 17) entre el módulo de identidad integrado (3) y el servidor de autentificación remota (7) a través de la conexión segura establecida utilizando el certificado X. 509;
- cargar las credenciales de suscriptor desde el servidor de autentificación remota (7) en el módulo de identidad integrado (3) a través del túnel seguro establecido (11, 13, 17).

2. Método para cargar credenciales de suscriptor según la reivindicación 1, en el que el módulo de identidad integrado (3) es una tarjeta de circuito integrado universal (UICC).

3. Método para cargar credenciales de suscriptor según las reivindicaciones 1 o 2, en el que el módulo de identidad integrado (3) es una tarjeta de módulo de identidad de suscriptor (SIM).

4. Método para cargar credenciales de suscriptor según una de las reivindicaciones anteriores, en el que las credenciales de suscriptor comprenden al menos un parámetro de un módulo de identidad de suscriptor universal (USIM).

5. Método para cargar credenciales de suscriptor según la reivindicación 4, en el que las credenciales comprenden una clave secreta de un módulo de identidad de suscriptor universal (USIM).

6. Método para cargar credenciales de suscriptor según la reivindicación 4, en el que las credenciales comprenden una identidad internacional de suscriptor móvil (IM-SI).

7. Método para cargar credenciales de suscriptor según una de las reivindicaciones anteriores, en el que la autentificación del cliente comprende al menos un parámetro genérico provisional de un módulo de identidad de suscriptor universal (USIM) que permite una conexión inicial al servidor de autentificación remota (7).

8. Método para cargar credenciales de suscriptor según la reivindicación 7, en el que el al menos un parámetro genérico provisional de un módulo de identidad de suscriptor universal (USIM) que permite una conexión inicial al servidor de autentificación remoto (7) es proporcionado por una entidad dedicada (5) de la red (2).

9. Método para cargar credenciales de suscriptor según una de las reivindicaciones anteriores, en el que los medios para establecer el túnel seguro (11, 13, 17) con el servidor de autentificación remota (7) comprenden un protocolo de autentificación extensible (EAP) del cliente.

10. Método para cargar credenciales de suscriptor según la reivindicación 8, en el que los medios para establecer un túnel seguro (11, 13, 17) con el servidor de autentificación remoto (7) comprenden un protocolo de autentificación extensible de cliente de seguridad de capa de transporte en túnel (EAP-TTLS).

11. Método para cargar credenciales de suscriptor según una de las reivindicaciones anteriores, en el que la conexión segura establecida entre el servidor de autentificación remota (7) y el equipo de usuario (1) es al menos en parte una conexión inalámbrica.

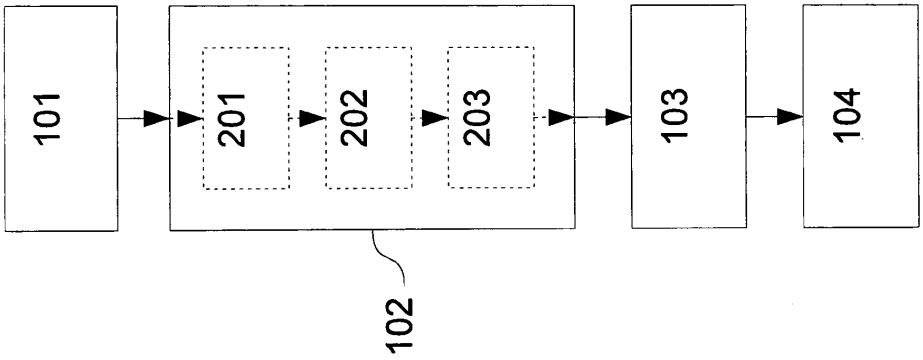
12. Método para cargar credenciales de suscriptor según una de las reivindicaciones anteriores, en el que el servidor de autentificación remota (7) es un servidor de autentificación de un operador de red móvil (NO1, NO2, NO3).

13. Servidor de red (7) que comprende medios para establecer una conexión segura con un equipo de usuario (1) usando una sesión de gestión segura y medios para establecer un túnel seguro con un módulo de identidad integrado (3) implementado en dicho equipo de usuario (1) basado en dicha sesión de gestión segura y utilizando un

certificado X. 509 instalado en el módulo de identidad integrado (3), en donde los medios para establecer el túnel seguro comprenden medios para recibir desde un servidor (9) del fabricante del equipo del usuario, una solicitud para obtener un adjunto del equipo de usuario (1) al operador de red (NO1, NO2, NO3) correspondiente a dicho servidor de red (7) y medios para establecer la conexión segura utilizando la sesión de gestión segura, en donde el servidor de red (7) comprende medios para cargar credenciales de suscriptor en el módulo de identidad integrado (3) a través del túnel seguro establecido.

14. Módulo de identidad integrado (3) implementado en un equipo de usuario (1) y que comprende medios para establecer un túnel seguro (11, 13, 17) con un servidor remoto (7) a través de una conexión establecida entre dicho servidor remoto (7) y dicho equipo de usuario (1) que utiliza un certificado X.509 instalado en el módulo de identidad integrado (3) y medios configurados para recibir, a través del túnel seguro establecido, e instalar credenciales de suscriptor en dicho módulo de identidad integrado (3) en donde los medios para establecer un túnel seguro (11, 13, 17) con un servidor remoto (7) comprenden medios para establecer una conexión con un servidor (9) del fabricante del equipo de usuario para solicitar un adjunto del equipo de usuario (1) al operador de red (NO1, NO2, NO3) correspondiente a dicho servidor remoto (7).

Fig.1



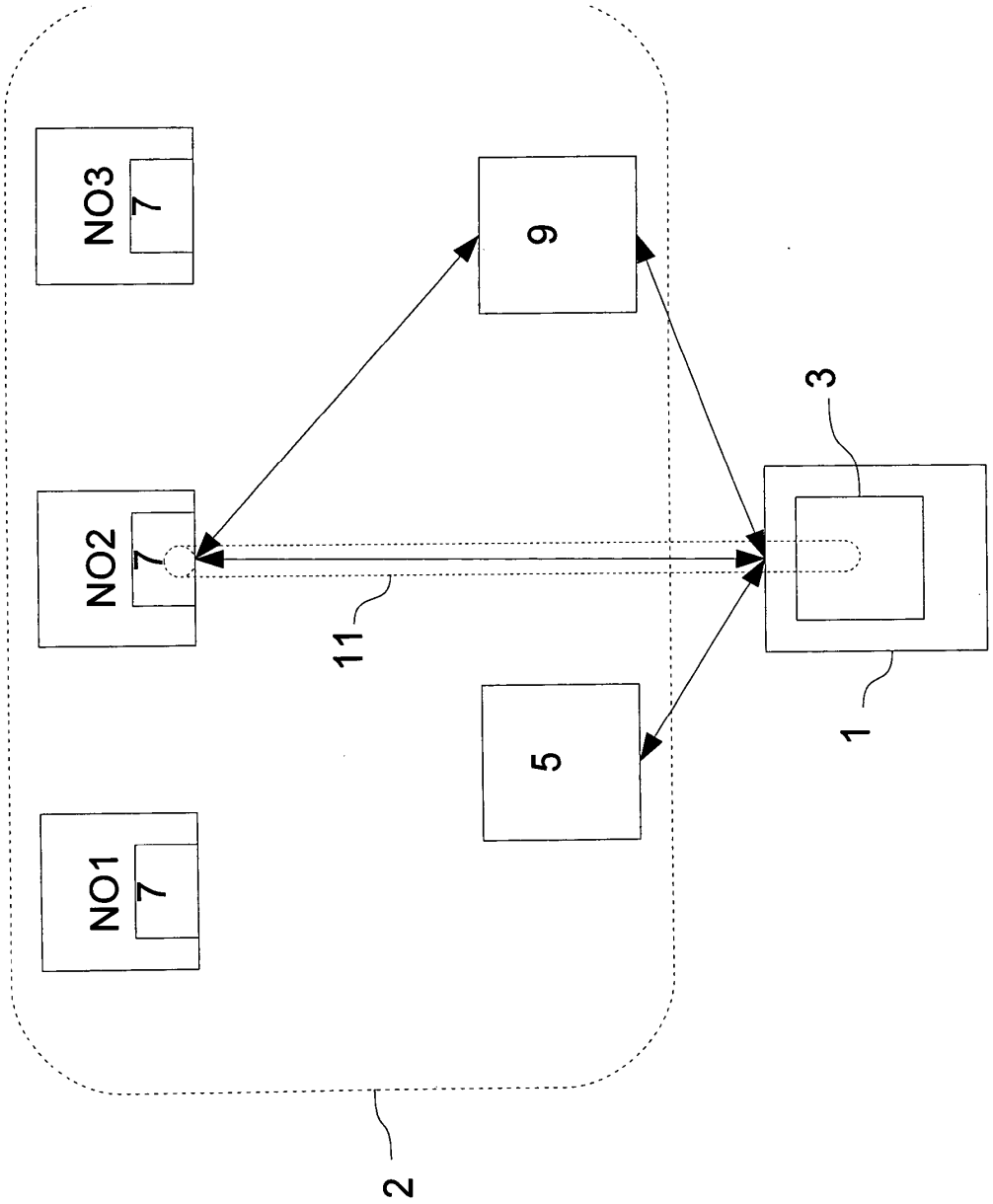


Fig.2

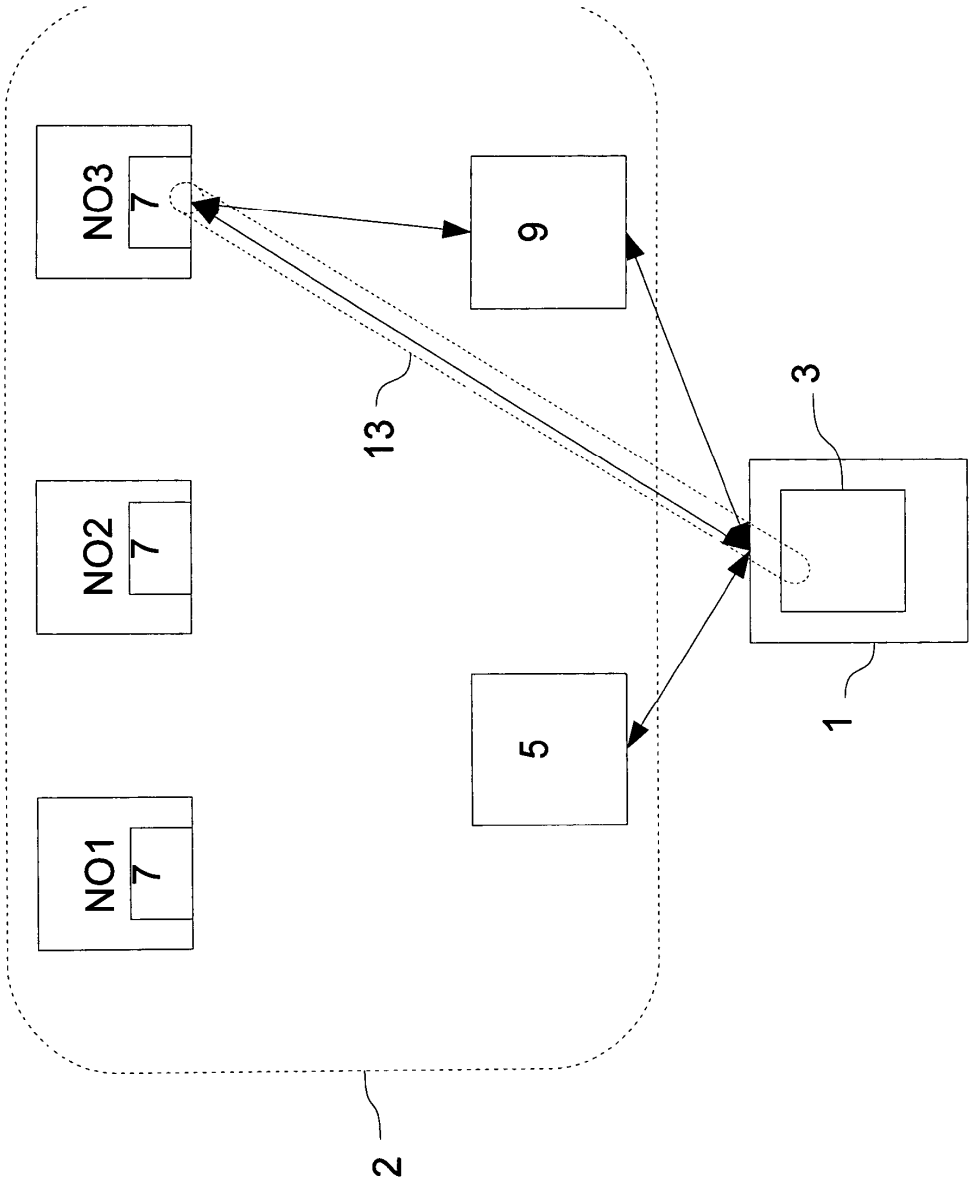


Fig.3

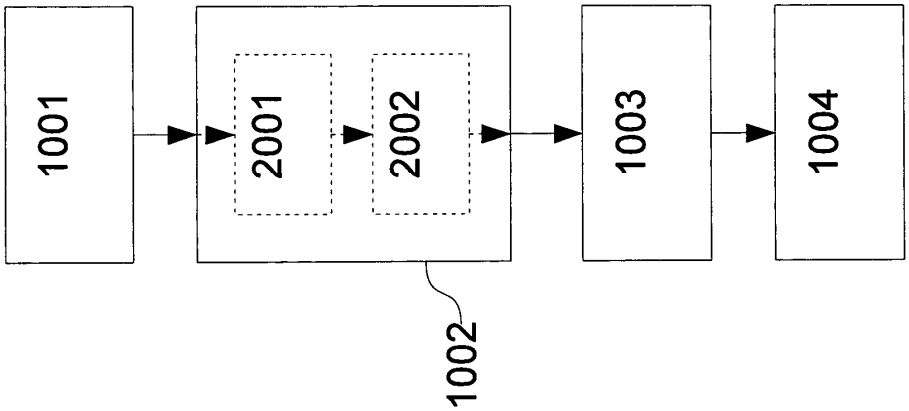


Fig.4

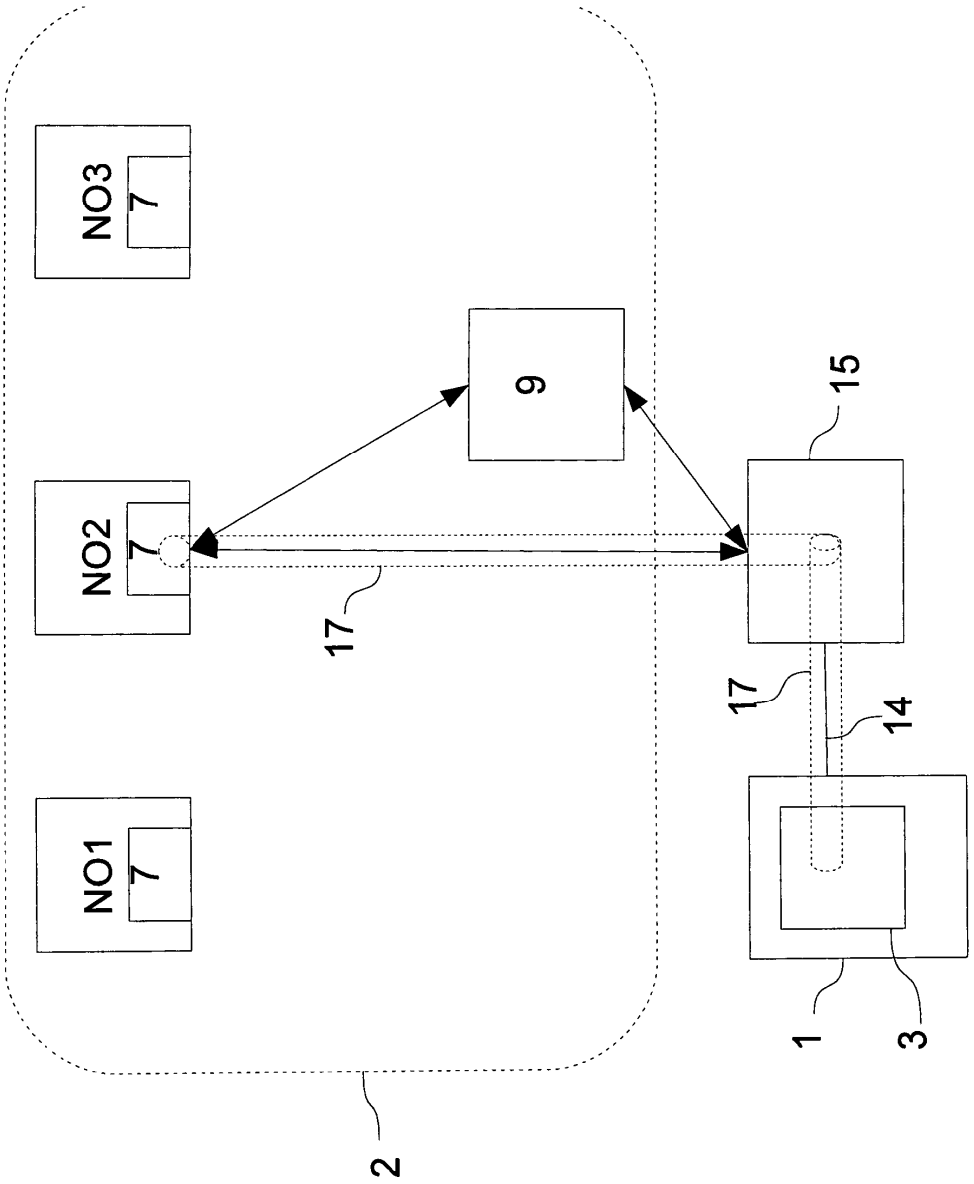


Fig.5