(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 327 310**

(21) Número de solicitud: 200801492

(51) Int. Cl.:

G06F 9/46 (2006.01)

H04L 29/08 (2006.01)

H04L 29/06 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **19.05.2008**

(43) Fecha de publicación de la solicitud: **27.10.2009**

(43) Fecha de publicación del folleto de la solicitud: **27.10.2009**

(71) Solicitante/s: **Universitat Autònoma de Barcelona**
Àrea I+D - Campus Univ., s/n
08913 Bellaterra, Barcelona, ES

(72) Inventor/es: **Garrigues Olivella, Carlos;**
Robles Martínez, Sergi y
Borrell Viader, Joan

(74) Agente: **No consta**

(54) Título: **Método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles y sistema de plataformas de computación protegidas.**

(57) Resumen:

Método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles y sistema de plataformas de computación protegidas.

La presente invención concierne, en un primer aspecto, a un método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles identificados mediante marcadores de trayecto o identificadores de agente, y en particular a un método que comprende utilizar unas entidades de autorización para generar nuevos marcadores de trayecto que permiten que el agente móvil pueda migrar y ser re-ejecutado legalmente en una misma plataforma un número de veces determinado dinámicamente en tiempo de ejecución. Un segundo aspecto de la invención concierne a un sistema de plataformas de computación protegidas frente a ataques externos de repetición de agentes móviles, y adaptado para aplicar el método propuesto.

ES 2 327 310 A1

DESCRIPCIÓN

Método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles y sistema de plataformas de computación protegidas.

Sector de la técnica

La presente invención concierne, en un primer aspecto, a un método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles identificados mediante marcadores de trayecto o identificadores de agente, y en particular a un método que comprende utilizar unas entidades de autorización para generar nuevos marcadores de trayecto que permiten que el agente móvil pueda migrar y ser re-ejecutado legalmente en una misma plataforma un número de veces determinado dinámicamente en tiempo de ejecución.

Un segundo aspecto de la invención concierne a un sistema de plataformas de computación protegidas frente a ataques externos de repetición de agentes móviles, y adaptado para aplicar el método propuesto.

Estado de la técnica anterior

Los agentes móviles pueden proporcionar múltiples beneficios en el desarrollo de aplicaciones distribuidas, pero su utilización también supone amenazas de seguridad. Diferentes investigaciones en el campo de la tecnología de agentes móviles han identificado y solucionado algunas de las cuestiones relacionadas con la seguridad que suponían una de dichas amenazas, pero aún existen muchas que permanecen sin resolver, tal como se indica en el artículo de J. Zachary "Protecting Mobile Code in the Wild" Internet Computing, IEEE, vol. 7. No. 2, págs. 78-82, 2003.

La mayor parte del trabajo de investigación llevado a cabo respecto a la seguridad de los agentes móviles está concentrado en el problema que presentan las plataformas maliciosas, ya que las plataformas tienen un control completo sobre la ejecución del agente, y pueden por tanto hacer casi cualquier cosa con el código o datos del agente. Por ello se considera que conseguir una solución completa es una tarea imposible. Sin embargo, varios problemas pueden ser mitigados. Por ejemplo, aunque a pesar de que no puede evitarse que las plataformas manipulen los resultados generados por la ejecución actual del agente en las mismas, sí que puede evitarse que las plataformas manipulen de manera no autorizada los resultados generados por el agente en otras plataformas.

La mayoría de soluciones propuestas en la protección de los agentes móviles frente a las plataformas maliciosas intentan proporcionar una solución genérica que cubra tantas amenazas de seguridad como sea posible, en general sin poner la solución en práctica en ninguna aplicación real. Por otra parte, la mayoría de aplicaciones reales basadas en agentes no tienen en cuenta la seguridad. Esta es probablemente la razón debido a la cual algunas propuestas en seguridad de agentes móviles han fallado a la hora de considerar algunos escenarios específicos donde sus soluciones pueden no ser válidas. Más específicamente, las soluciones presentadas para algunos ataques de repetición de agentes han fallado a la hora de considerar escenarios donde el agente tenga que recorrer un bucle que contenga un número determinado de plataformas un número de veces indeterminado (ver documento de Y. Y. Tsipenyuk, "Detecting External Agent Replay and State Modification Attacks", Master's thesis. University of California, 2004).

Los ataques de repetición de agente pueden ser clasificados en dos categorías diferentes (ver el artículo de B. Yee. "Monotonicity and partial results protection for mobile agents", en "Proceedings of the 23rd Int. Conf. on Distributed Computing Systems. IEEE Computer Society", 2003, págs. 582-591):

- Ataques de repetición internos: Estos ocurren cuando el agente es ejecutado en el interior de una sola plataforma utilizando diferentes entradas, con el fin de obtener diferentes respuestas y sacar conclusiones sobre su comportamiento.

- Ataques de repetición externos: Estos son ejecutados por plataformas maliciosas mediante el reenvío del agente a otra plataforma, haciendo así que el agente reejecute parte de su itinerario.

Los ataques de repetición internos son imposibles de evitar porque la plataforma tiene un control total sobre la ejecución, y siempre puede reiniciar al agente a su estado de llegada. Los ataques externos, al contrario, pueden ser evitados si las plataformas mantienen un registro de los agentes ejecutados previamente.

El problema de las soluciones actuales contra los ataques externos de repetición (las cuales se describirán posteriormente) es que éstas no permiten que un agente sea ejecutado n veces en la misma plataforma, especialmente si n es determinado en tiempo de ejecución. Sin embargo, el itinerario del agente a menudo contiene recorridos de ida y vuelta que requieren que la misma plataforma sea visitada varias veces. Así, las soluciones actuales fuerzan a los programadores a sacrificar parte de la flexibilidad inherente a los itinerarios de los agentes móviles.

Los ataques de repetición han sido considerados tradicionalmente como una forma de ataques de red (ver artículo de J. Zachary "Protecting Mobile Code in the Wild" Internet Computing, IEEE, vol. 7. No. 2, págs. 78-82, 2003). Estos están basados en la captura de algunos de los mensajes intercambiados entre dos entidades y su reenvío posterior. Estos ataques son llevados a cabo en general durante procesos de autorización o de ejecución de protocolos de intercambio de claves, con el fin realizar, por ejemplo, ataques de suplantación de identidad.

Los mecanismos tradicionales utilizados para prevenir los ataques de repetición están basados en la utilización de "nonces" (números utilizados una sola vez), sellos de tiempo, fichas (tokens) de sesión o cualquier otra clase de información que permita a las entidades vincular sus mensajes a la ejecución del protocolo actual (T. Aura, "Strategies against Replay Attacks" in Proceedings of the Computer Security Foundations Workshop. IEEE Computer Society, 1997, págs. 59-68).

Por ejemplo, un intercambio HTTP entre un explorador web y un servidor puede incluir una ficha de sesión que identifique únicamente la sesión de interacción actual. La ficha es enviada en general como una "cookie" http, y es calculada aplicando una función "hash" a los datos de la sesión, a las preferencias del usuario, etc.

Los sistemas de agentes móviles también están expuestos a ataques de repetición tradicionales. Cualquier comunicación entre dos agentes, o dos plataformas, o un agente y una plataforma está expuesta a esta clase de ataques. Para combatir esta clase de ataques, mecanismos tradicionales como los mencionados previamente (basados en "nonces" o fichas de sesión) pueden ser utilizados.

El documento de patente EP1879323 propone un método para proteger los datos y el itinerario de un agente móvil enviado desde un primer servidor a través de una red a la que están conectados una pluralidad de servidores. Se propone que los datos y el itinerario previstos para cada uno de los servidores a los cuales el agente móviles debe visitar siguiendo su itinerario programado, se encripten juntos en una estructura anidada, con un número de elementos igual al número de servidores a visitar, de manera que cada uno de dichos servidores pueda acceder únicamente, mediante la desencriptación correspondiente, a los datos previstos para él y a una sección del itinerario, respectivamente. En dicho documento se propone, con el fin de evitar ataques de repetición tradicionales, la utilización de "nonces", firmas digitales, claves públicas y privadas, funciones envoltorios, tales como funciones "hash", etc.

Los sistemas de agentes móviles están también expuestos, además de a los ataques de repetición tradicionales, a ataques de repetición de agente. Los ataques de repetición de agente no están basados en repetir un mensaje enviado por la red, sino en reejecutar un agente que ya había sido ejecutado previamente en una plataforma. Además, estos ataques no son realizados por atacantes externos, sino por las plataformas de agente que forman parte del itinerario del agente. Tal y como se ha dicho anteriormente los ataques de repetición de agente pueden ser divididos en dos clases: ataques de repetición internos y ataques de repetición externos.

Los ataques de repetición internos ocurren cuando una plataforma deshonesta ejecuta repetidamente un agente aplicándole las mismas o diferentes entradas cada vez. Una plataforma puede ejecutar un agente múltiples veces con el fin de entender su comportamiento, o hasta que la salida deseada sea obtenida. Esta clase de ataques es también conocido como "blackbox testing" (F. Hohl, "Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts", in Mobile Agents and Security, ser. Lecture Notes in Computer Science. Springer Verlag, 1998, vol. 1419, p. 92), y en general es llevado a cabo cuando el código del agente ha sido protegido utilizando alguna técnica de ofuscación.

Esta clase de ataques se llevan a cabo en el interior de una sola plataforma, y no pueden ser observados externamente por ninguna otra entidad. Incluso si el agente intentase registrar todas sus acciones en un servicio de monitorización externo, el entorno de ejecución podría todavía interferir con estas comunicaciones externas, y dirigir los mensajes hacia un receptor incorrecto, o alterar los contenidos de los mensajes, etc. Además, los intentos del agente de almacenar su información de estado en una entidad externa segura podrían ser fácilmente evitados por parte de plataformas maliciosas mediante la alteración de la ejecución del agente. En la práctica, los ataques de repetición internos son imposibles de prevenir o detectar (B. Yee. "Monotonicity and partial results protection for mobile agents", en "Proceedings of the 23rd Int. Conf. on Distributed Computing Systems. IEEE Computer Society", 2003, págs. 582-591).

Los ataques de repetición externos ocurren cuando una plataforma deshonesta hace migrar a un agente hacia una plataforma remota, sin que esta migración esté definida en el itinerario del agente. Esta clase de ataque es especialmente difícil de combatir, ya que es difícil distinguir entre una migración legal del agente hasta su siguiente destino y una migración repetida que el agente no tenía intención de llevar a cabo. Por ejemplo, suponiendo que el itinerario del agente incluya una migración desde una plataforma A a una B, entonces la plataforma A está autorizada a enviar agentes a la plataforma B, y el agente también está autorizado a ser ejecutado en la plataforma B. Como resultado, ningún mecanismo de autenticación puede ser utilizado para prevenir que la plataforma A reenvíe maliciosamente al agente a la plataforma B múltiples veces.

Con el fin de proporcionar una solución a este problema, Yee ("Monotonicity and partial results protection for mobile agents" en "Proceedings of the 23rd Int. Conf. on Distributed Computing Systems. IEEE Computer Society", 2003, págs. 582-591) sugiere considerar un ataque de repetición como una transición de estado ilegal. Cada plataforma dentro del itinerario implementa un algoritmo de detección de inconsistencias en transiciones de estado (STID), el cual es capaz de determinar cuándo una migración desde una plataforma hasta otra es una transición ilegal. El problema de este enfoque es que las plataformas deben ser conscientes de cuales son las transiciones de estado ilegales de cada agente ejecutado. Además, las transiciones de estado ilegales pueden ser identificadas erróneamente si el agente está ejecutando un bucle en el que la misma plataforma es visitada repetidamente.

Otros trabajos referentes a la protección de agentes móviles contra plataformas maliciosas sugieren la utilización de marcadores de trayecto para prevenir ataques de repetición. Algunos de tales trabajos son los expuestos en los siguientes documentos:

- "Methods for Protecting a Mobile Agent's Route", en "Proceedings of the 2nd Int. Information Security Workshop (ISW '99), ser. Lecture Notes in Computer Science", vol. 1729. *Springer-Verlag*, 1999, págs. 57-71, de los autores D. **Wcsthoff**, M. **Schneider**, C. **Unger**, y F. **Kaderali**;

- "On the problem of trust in mobile agent systems", en "Proceedings of the Symposium on Network and Distributed System Security". *Internet Society*. 1998, de U. G. **Wilhelm**, S. **Staamann**, y L. **Buttyan**;

- "A Secure Route Structure for Information Gathering Agent" en "Proceedings of the 3rd Pacific Rim Int. Workshop on Multi-Agents: Design and Applications of Intelligent Agents, ser. Lecture Notes in Artificial Intelligence", vol. 1881. *Springer-Verlag*, 2000, pp. 101-114, de T. **Li**, C. Y. **Seng** y K. Y. **Lam**;

- "Mobile Agent Protection With Data Encapsulation And Execution Tracing", Ph.D. dissertation. *The Florida State University*. 2003, de A. **Suen**;

- "Protecting Mobile Agent Itineraries", en "Mobile Agents for Telecommunication Applications (MATA). ser. Lecture Notes in Computer Science", vol. 2881. *Springer Verlag*, 2003, pp. 275-285, de J. **Mir** and J. **Borrell**; y

- "A Novel Solution of Mobile Agent Security: Task-Description-Based Mobile Agent", "*IJCSNS International Journal of Computer Science and Network Security*", vol. 6, no. 2B, pp. 121-125, 2006, de los autores H. **Che**, D. **Li**, J. **Sun**. and H. **Yu**.

Un marcador de trayecto es un identificador del agente que debe ser almacenado por las plataformas, de manera que así puedan detectar e impedir futuros intentos de reejecución del mismo agente. De nuevo, el problema de estas soluciones es que no tienen en cuenta el caso donde el itinerario del agente incluya una o más plataformas que deban ser visitadas más de una vez. Como resultado, una reejecución legal del agente en la misma plataforma puede ser malinterpretada como un ataque de repetición.

Estos aspectos fueron identificados en el artículo "Protecting Mobile Agent Loops", en "Mobility Aware Technologies and Applications, ser. Lecture Notes in Computer Science", vol. 3744. Springer-Verlag, 2005, págs. 74-83, por J. Cucurull, J. Ametller, J. A. Ortega-Ruiz, S. Robles, y J. Borrell, los cuales propusieron una solución basada en la inclusión de contadores dentro del marcador de trayecto del agente. A cada plataforma le es asignado un contador diferente, el cual indica el número máximo de veces que un agente puede ser ejecutado en una plataforma. Las plataformas mantienen un registro de qué agentes han sido ejecutados, y el número de veces que lo han sido. Antes de iniciar la ejecución de un agente, las plataformas verifican que el número de veces que el agente ha sido previamente ejecutado no exceda el número de ejecuciones permitidas registrado en el marcador de trayecto del agente.

El problema de esta propuesta, sin embargo, es que el número de veces que una plataforma dada puede ser visitada debe ser conocido de antemano, cuando se crea el itinerario del agente, de manera que esta información pueda ser introducida dentro del marcador de trayecto del agente. En consecuencia, esta propuesta no permite que el agente decida dinámicamente cuantas veces será visitada una plataforma dada.

Algunos de los trabajos propuestos para evitar que el agente sea ejecutado en más de una ocasión se han basado en preservar la denominada "propiedad de ejecución única" ("exactly-once execution property"). En general esta propiedad se tiene en consideración cuando se diseñan mecanismos de tolerancia a fallos para agentes móviles. Asegurar dicha propiedad implica que, cuando el agente se ha enviado a realizar una tarea determinada: en primer lugar, la tarea será finalmente ejecutada, independientemente de posibles fallos en la plataforma o en sus comunicaciones; y en segundo lugar que la tarea no será realizada más de una vez.

Las soluciones presentadas para asegurar la propiedad de ejecución única están basadas en la utilización de entidades externas que monitorizan la ejecución del agente. Cuando un fallo impide que el agente continúe su itinerario, otro agente es enviado para reanudar la ejecución en el punto que el agente original la dejó. El problema de estas soluciones es que las comunicaciones entre el agente y el sistema de monitorización producen una cantidad considerable de tráfico de red. Además, estos protocolos reducen severamente la autonomía del agente, debido a que el agente tiene que interactuar constantemente con la entidad de monitorización. Así, sacrifican una de las mayores ventajas asociadas con el uso de tecnología de agentes móviles.

En resumen, no se conoce ninguna solución presentada hasta ahora contra los ataques de repetición que permita que un agente sea ejecutado en una plataforma un número de veces determinado dinámicamente. Considerando que uno de los grandes atractivos de los agentes móviles es su dinamismo y flexibilidad, fijar de antemano en el código del agente el número de posibles migraciones a una plataforma puede ser un serio impedimento a la hora de implementar aplicaciones reales.

Explicación de la invención

Es necesario ofrecer una alternativa al estado de la técnica que permita realmente a un agente móvil ser reejecutado legalmente en una misma plataforma de computación, a la vez que impedir los ataques externos de repetición de agentes móviles descritos en el apartado anterior, mejorando la seguridad sin sacrificar la flexibilidad intrínseca a los agentes móviles.

Para ello la presente invención propone un método y un sistema basados en la utilización de entidades de autorización designadas para generar nuevos identificadores para el agente, permitiéndole así migrar a una misma plataforma cualquier número de veces. Por consiguiente, la invención propuesta permite a los programadores desarrollar aplicaciones basadas en agentes móviles de manera segura, sin renunciar a su flexibilidad intrínseca.

En un primer aspecto, la presente invención concierne a un método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles, que comprende utilizar un sistema de plataformas de computación conectadas a una red para la ejecución compartida de aplicaciones distribuidas basadas en agentes móviles, y que comprende utilizar marcadores de trayecto o identificadores de agente para permitir a uno o más agentes móviles ser legalmente ejecutados en una plataforma de computación más de una vez, a la vez que evitar una re-ejecución ilegal de dicho o dichos agentes móviles, por considerarla como un ataque externo de repetición.

A diferencia de las propuestas citadas en el apartado anterior que sugieren la utilización de marcadores de trayecto para prevenir ataques de repetición, el método propuesto por la presente invención comprende utilizar una o más entidades de autorización para generar como mínimo un nuevo marcador de trayecto o identificador a ser utilizado como autorización para el agente móvil, para permitirle ser ejecutado legalmente en dicha plataforma de computación un número de veces determinado dinámicamente en tiempo de ejecución.

Para un ejemplo de realización preferido el método comprende utilizar varias entidades de autorización para la generación de nuevos marcadores de trayecto para el agente móvil, con el fin de permitirle re-ejecutarse en diferentes plataformas de computación.

Por lo que se refiere a la mencionada re-ejecución legal, para un ejemplo de realización ésta hace referencia a la ejecución de diferentes tareas en diferentes respectivos nodos o etapas del itinerario del agente móvil, siendo cada uno de dichos nodos diferente y representativo de una visita a dicha plataforma de computación en un momento distinto al del resto de los nodos.

Para otro ejemplo de realización la mencionada re-ejecución legal hace referencia a la ejecución de una misma tarea en diferentes visitas respectivas a dicha plataforma de computación a lo largo del itinerario del agente móvil, siendo cada una de dichas visitas representada por un mismo nodo o etapa.

Es decir que cada nodo está asociado con una tarea y una plataforma concretas, y en el caso de que cada visita a una misma plataforma sea para ejecutar una tarea distinta, dichas visitas serán representadas por nodos diferentes asociados a una misma plataforma, y para el caso en que las sucesivas visitas a una misma plataforma son para ejecutar la misma tarea, dichas visitas serán representadas por un mismo nodo.

En cualquier caso en la presente memoria el término nodo se entiende como una respectiva visita a una plataforma, ya sea la misma u otra plataforma, con el fin de ejecutar una tarea, ya sea la misma o una diferente. En lo siguiente cuando se haga referencia a la ejecución de un nodo, ésta implicará la ejecución de la tarea asociada a dicho nodo en la plataforma también asociada a dicho nodo.

El método comprende generar y asociar un marcador de trayecto o identificador diferente a cada uno de varios agentes móviles, incluso si ejecutan exactamente las mismas tareas, y a cada instancia del mismo agente móvil.

Asimismo el método propuesto por el primer aspecto de la invención está previsto para la prevención de ataques de repetición, en lugar de en su detección posterior, ya que esta detección *a posteriori* es en muchos casos inútil.

El método comprende almacenar en cada plataforma de computación un identificador del nodo ejecutado previamente por cada agente móvil en dicha plataforma de computación, junto con su respectivo marcador de trayecto, con el fin de permitir que el agente pueda visitar una misma plataforma para ejecutar distintos nodos, o re- ejecutar el mismo nodo un número de veces determinado.

Al almacenarse en cada plataforma de computación los marcadores de trayecto de los agentes móviles que la han visitado previamente, se consigue que ningún agente pueda reejecutar el mismo nodo utilizando un marcador de trayecto que ya haya sido utilizado anteriormente.

Mediante la aplicación del método propuesto por la invención, con el fin de ofrecer una solución más eficaz a la hora de prevenir los ataques de repetición, no se produce una interacción del agente móvil con entidades externas, lo que permite que el agente se ejecute de manera autónoma, sin depender del control o interacción con ningún servicio de monitorización.

El método propuesto por el primer aspecto de la invención comprende la realización de las siguientes etapas, las cuales serán posteriormente descritas con mayor detalle para unos ejemplos de realización:

- crear en un primer momento, por parte de un usuario propietario o programador, un agente móvil protegido frente a ataques de repetición, incluyendo como mínimo un marcador de trayecto inicial o identificador, un itinerario protegido y el agente móvil propiamente dicho, con los datos incluidos en el mismo,

- enviar dicho agente móvil protegido a una plataforma de computación,

- recibir dicho agente móvil protegido en dicha plataforma de computación,

- extraer, por parte de dicha plataforma de computación, como mínimo parte de la información incluida en dicho agente móvil protegido y utilizarla para comprobar si dicho agente móvil protegido ya ha sido re-ejecutado anteriormente, mediante la comparación de parte o toda la información extraída con información almacenada en la plataforma de computación, incluyendo dicha información almacenada como mínimo los marcadores de trayecto de agentes ejecutados previamente, junto con unos respectivos identificadores de nodo representativos de las tareas de nodo ejecutadas por dichos agentes.

Respecto al mencionado itinerario protegido, el método comprende construirlo mediante la realización de las siguientes acciones:

- definir un conjunto de nodos o etapas que conforman dicho itinerario de agente móvil, siendo cada uno de dichos nodos, tal y como se ha indicado anteriormente, asociado a una determinada tarea y a una determinada plataforma, y estando cada uno de dichos nodos asociado a una entidad de autorización correspondiente que es la única encargada de generar nuevos marcadores de trayecto válidos utilizados como autorizaciones para la ejecución de la tarea asociada con dicho nodo;

- proteger dicho itinerario de agente utilizando un protocolo de protección.

Por motivos de claridad, en diferentes partes de la presente memoria se está describiendo el método haciendo referencia a una plataforma receptora de un agente móvil protegido, pero obviamente dicha descripción es aplicable a todas las plataformas de computación conectadas a la red del mencionado sistema que se encuentren en dicha situación, es decir que reciban un agente móvil protegido de la manera descrita.

El método comprende utilizar cada marcador de trayecto como una autorización que permite al agente móvil ejecutar un conjunto determinado de tareas, cada una de las cuales está asociada a un nodo de dicho conjunto de nodos.

Con el fin de definir dicho conjunto de nodos, el método comprende asignar la siguiente información a cada uno de los nodos que conforman el conjunto:

- un identificador de nodo;

- una plataforma de computación donde será ejecutado;

- una tarea;

- un tipo de nodo;

- plataforma siguiente;

- una entidad de autorización;

- un nodo de autorización;

- un identificador de agente.

Para la aplicación del método propuesto por el primer aspecto de la invención solamente es necesario clasificar los nodos en dos tipos de nodo, en concreto los siguientes:

- un tipo de nodo regular, el cual se refiere a un nodo que es una etapa del itinerario donde el agente móvil ejecuta su tarea y salta a la siguiente plataforma de computación del itinerario;

- un tipo de nodo bucle, el cual hace referencia a un nodo que es una etapa del itinerario donde el agente móvil determina si inicia o no una iteración de un número determinado de nodos.

Siguiendo con el resto de información asignada a cada nodo del conjunto de nodos, en particular el método comprende definir dicho nodo de autorización como un identificador del nodo donde el marcador de trayecto del agente

móvil debe ser generado, ya sea dicho marcador de trayecto inicial o uno de dichos nuevos marcadores de trayecto, y definir dicha entidad de autorización como la plataforma de computación correspondiente o el usuario propietario o programador que debe generar y firmar el marcador de trayecto.

El método comprende asignar o no un respectivo nodo de autorización a cada nodo, dependiendo de si el nodo se encuentra ubicado o no en el interior de un bucle de nodos.

En concreto el método comprende asignar como nodo de autorización a cada nodo que se encuentra ubicado en el interior de un bucle, el nodo de bucle ubicado al inicio del bucle (el cual en la presente memoria se entiende como que no se encuentra en el interior del bucle) y como su correspondiente entidad de autorización la plataforma de computación donde la tarea de dicho nodo inicial de bucle es ejecutada, y a cada nodo que no se encuentra ubicado en el interior de un bucle, asignarle ningún nodo de autorización y como su correspondiente entidad de autorización el propietario del agente móvil.

Por lo que se refiere al protocolo de protección utilizado para la protección del itinerario del agente móvil, el método propuesto por el primer aspecto de la invención comprende definirlo garantizando las siguientes propiedades:

- impedir a las plataformas de computación acceder o modificar cualquier parte del itinerario que está previsto para otras plataformas de computación;

- imposibilitar recorrer los nodos del itinerario en un orden diferente al del inicialmente establecido; y

- vincular de manera única cada nodo del itinerario con el agente móvil al cual pertenece, para imposibilitar la reutilización de cualquier parte del itinerario del agente móvil en un agente móvil diferente.

Para la definición de dicho protocolo el método comprende utilizar un identificador de agente único para vincular de manera unívoca los nodos de itinerario al agente móvil. Como identificador de agente puede utilizarse, en función del ejemplo de realización, desde un sello temporal unido a un número aleatorio formado por una gran cantidad de dígitos, o cualquier otra información que identifique de manera unívoca cada instancia del agente.

El método comprende generar cada uno de los marcadores de trayecto de cada agente móvil, ya sea dicho marcador de trayecto inicial o uno de dichos nuevos marcadores de trayecto, con la siguiente información:

- un identificador de agente idéntico a dicho identificador de agente incluido en el itinerario protegido y utilizado para vincular a los nodos de itinerario con el agente móvil, para asegurar que cualquier instancia de agente móvil pueda ser identificada de manera única;

- un nodo de autorización como un identificador del nodo donde el marcador de trayecto es generado;

- una fecha de caducidad tras la cual el marcador de trayecto no puede ser utilizado más; y

- un contador de bucle incrementado en una unidad cada vez que el agente móvil tiene que iniciar una nueva iteración de un bucle.

Cuando el marcador de trayecto generado es dicho marcador de trayecto inicial éste es generado por parte del usuario propietario o programador, una vez éste ha construido el mencionado itinerario protegido.

En cambio cuando el marcador de trayecto generado es uno de dichos nuevos marcadores de trayecto éste es generado por parte de la plataforma de computación correspondiente a la entidad de autorización asignada en el itinerario protegido.

Una vez el marcador de trayecto ha sido generado, el método comprende firmarlo por parte del usuario propietario o de la entidad de autorización y colocarlo en la parte superior de una pila de marcadores de trayecto del agente configurada para almacenar marcadores de trayecto previamente utilizados por el agente móvil durante su ejecución.

A excepción de en un estado inicial donde dicha pila se encuentra vacía antes de depositar en la misma el mencionado marcador de trayecto inicial, en el resto de casos la pila almacenará como mínimo parte de los mencionados marcadores de trayecto previamente utilizados por el agente móvil, conteniendo siempre en su parte superior el marcador de trayecto actual, es decir el que está siendo utilizado o se ha dispuesto para ser utilizado en el siguiente nodo.

Tal y como se ha indicado anteriormente una vez la plataforma ha recibido a un agente móvil protegido según el método de la presente invención, ésta procede a extraer parte de su información. Para un ejemplo de realización preferido dicha extracción de información llevada a cabo por la plataforma de computación desde el agente móvil protegido recibido concierne a:

- extraer la información del nodo actual del itinerario protegido para obtener el identificador de nodo, identificador de agente, tarea, tipo de nodo, plataforma siguiente, entidad de autorización y nodo de autorización; y

- recuperar el marcador de trayecto del agente de la parte superior de la pila de marcadores de trayecto del agente y extraer del marcador de trayecto recuperado el identificador de agente, el nodo de autorización, la fecha de caducidad y el contador de bucle.

Por lo que se refiere a la información almacenada en la plataforma de computación utilizada para compararla con la extraída del agente móvil, ésta se encuentra representada, para un ejemplo de realización, por una tabla, aunque para otros ejemplos de realización dicha información puede estructurarse de otra manera que no incluya la utilización de una tabla.

A continuación se describen un ejemplo de realización preferido del método propuesto por el primer aspecto de la invención, para el cual el método comprende en primer lugar utilizar, por parte de la plataforma de computación receptora del agente móvil protegido, el tipo del nodo actual para determinar si el agente está ejecutando un nodo tipo regular o un nodo tipo bucle.

Una vez determinado el tipo de nodo, si éste es de tipo regular el método comprende realizar, por parte de la plataforma de computación receptora del agente móvil protegido, parte, o la totalidad si es necesario, de las siguientes operaciones:

a) verificar la firma del marcador de trayecto para comprobar si el marcador de trayecto ha sido firmado por la entidad de autorización actual, y si dicha verificación no resulta exitosa descartar la ejecución del agente, o si resulta exitosa realizar la siguiente operación; esta verificación se lleva a cabo, para un ejemplo de realización, mediante el uso de un servidor de claves públicas para obtener la clave pública de la entidad de autorización actual, y su utilización para verificar la firma;

b) comprobar que el nodo de autorización actual, que está incluido en el marcador de trayecto es el mismo que el extraído del itinerario protegido, y si dicha comprobación falla descartar la ejecución del agente, o si es exitosa realizar la siguiente operación;

c) comprobar que el identificador de agente incluido en el marcador de trayecto es igual al obtenido del itinerario protegido, y si dicha comprobación falla descartar la ejecución del agente, o si es exitosa realizar la siguiente operación;

d) comprobar la fecha de caducidad del marcador de trayecto, y si el marcador de trayecto ha caducado descartar la ejecución del agente, o si no ha caducado realizar la siguiente operación;

e) utilizar el identificador de agente para buscar un marcador de trayecto previo del mismo agente en dicha información almacenada en dicha tabla (u otra estructura de datos) almacenada en la plataforma de computación, y:

e1) si no hay ningún marcador de trayecto con el mismo identificador de agente en dicha tabla, almacenar el nuevo marcador de trayecto junto con el identificador del nodo actual en dicha tabla;

e2) si existe un marcador de trayecto previo con el mismo identificador de agente en dicha tabla, lo que significa que el mismo agente ya había sido ejecutado con anterioridad en esta plataforma de computación, comprobar si el identificador del nodo actual del agente es igual al de la ejecución previa, mediante la consulta de dicha tabla; y

e2a) si el identificador del nodo actual del agente es diferente al de la ejecución previa, lo que significa que el agente va a ejecutar una tarea diferente correspondiente a un nodo del itinerario distinto, almacenar el marcador de trayecto junto con el nuevo identificador del nodo actual en dicha tabla;

e2b) si el identificador del nodo actual del agente es igual al de la ejecución previa, lo que significa que la tarea de este nodo del itinerario había sido ejecutada en la ejecución previa, comparar el contador de bucle actual con el incluido en el marcador de trayecto previo, y:

e2b1) si el contador de bucle actual es mayor que el previo, lo que significa que el agente está realizando una nueva iteración de un bucle, reemplazar, en dicha tabla, el marcador de trayecto previo con el actual;

e2b2) si el contador de trayecto actual no es mayor que el previo, lo que significa que el marcador de trayecto ya ha sido utilizado, descartar la ejecución del agente;

f) si la ejecución del agente no ha sido descartada en ninguna de las operaciones previas, ejecutar la tarea correspondiente al nodo actual.

Las operaciones a) a f) son, en general, llevadas a cabo en dicha plataforma de computación receptora del agente móvil protegido.

Si se ha determinado que el nodo actual es de tipo bucle el método comprende realizar, por parte de la plataforma de computación receptora del agente móvil protegido, parte, o la totalidad si es necesario, de las siguientes operaciones:

i) verificar la firma del marcador de trayecto para comprobar si dicho marcador de trayecto ha sido firmado por la entidad de autorización actual o por la plataforma de computación actual, y si ambas comprobaciones fallan descartar la ejecución del agente, o si al menos una de ambas comprobaciones es exitosa realizar la siguiente operación;

ii) realizar la siguiente operación:

- comprobar que el nodo de autorización actual, que está incluido en el marcador de trayecto, es el mismo que el extraído del itinerario protegido o coincide con el nodo actual y si ambas comprobaciones fallan descartar la ejecución del agente, o si al menos una es exitosa realizar dichas operaciones c) a e);

iii) generar y firmar un nuevo marcador de trayecto conteniendo la misma información que el marcador de trayecto previo, a excepción del nodo de autorización, siendo asignado como nodo de autorización el nodo actual, y a excepción también del contador de bucle, el cual es incrementado en una unidad;

iv) comprobar si el agente está visitando el nodo de tipo bucle por primera vez, lo que significa que el agente todavía no ha realizado ninguna iteración previa del bucle iniciado en el nodo tipo bucle, y:

iva) si el agente está visitando el nodo bucle por primera vez, añadir el nuevo marcador de trayecto a la pila de marcadores de trayecto del agente, colocándolo en la parte superior de la misma;

ivb) si el agente ya ha realizado alguna iteración del bucle anteriormente, reemplazar el marcador de trayecto actual, el cual estaba dispuesto en la parte superior de la pila de marcadores de trayecto del agente, con el nuevo marcador de trayecto;

v) realizar dicha operación f);

vi) determinar, por parte del agente, si debe realizar una iteración del bucle; y:

via) si una iteración debe ser llevada a cabo, hacer saltar el agente móvil protegido a la siguiente plataforma del interior del bucle actual, comprobar el tipo de nodo y en función del tipo de nodo realizar las operaciones a) a f) o i) a vi);

vib) si no se requiere la realización de una iteración del bucle, extraer, por parte del agente, el marcador de trayecto de la parte superior de la pila, saltar el agente móvil protegido a la siguiente plataforma fuera del bucle actual, comprobar el tipo de nodo y en función del tipo de nodo realizar las operaciones a) a f) o i) a vi).

Las operaciones i) a v) son, en general, llevadas a cabo en dicha plataforma de computación receptora del agente móvil protegido.

Comparando las operaciones a realizar cuando el nodo es de tipo bucle con las anteriormente descritas para un nodo de tipo regular, puede verse cómo una de las diferencias principales entre ellas es la comprobación que para el nodo de tipo regular, se hace en la operación b), que, para el nodo de tipo bucle, se hace en ii), y que se diferencia de la operación b) en que la comparación del nodo de autorización actual incluido en el marcador de trayecto, se hace no solamente con el extraído del itinerario protegido, sino también con el nodo actual, lo que permite al agente ejecutar el nodo tipo bucle actual utilizando un marcador de trayecto generado por la misma plataforma en una iteración anterior.

Otra diferencia es la referente a la verificación de la firma del marcador de trayecto, que en i), a diferencia de en la operación a), contempla que si ésta no ha sido llevada a cabo por la entidad de autorización actual, se realice una comprobación de si la firma del marcador de trayecto actual ha sido realizada por la plataforma de computación actual (por ejemplo utilizando su propia clave pública), lo que permite al agente ejecutar el nodo tipo bucle actual utilizando un marcador de trayecto generado por la misma plataforma en una iteración anterior.

Finalmente mediante las operación iii) de generación y forma de un nuevo marcador de trayecto para el agente móvil, se posibilita una nueva ejecución de todos los nodos incluidos en el bucle iniciado en el nodo actual tipo bucle. Al disponer el nuevo marcador de trayecto en la parte superior de la pila del agente (operación iva) ó ivb)), se permite que éste recupere el marcador de trayecto utilizado antes de entrar en el bucle (operación vib)), lo cual es una característica esencial para el presente ejemplo de realización, ya que el nuevo marcador de trayecto por la plataforma actual no será válido cuando el agente salga del bucle.

Por lo que se refiere a la determinación llevada a cabo en la operación vi) por parte del agente móvil, ésta puede llevarse a cabo de diversas maneras, en función del ejemplo de realización, habiendo marcado el programador, en general, una o más condiciones a verificar por el agente móvil, en función de cuyo cumplimiento éste determina si salir o no del bucle.

Para un ejemplo de realización dichas condiciones son simplemente que una variable alcance un valor que esté por debajo de una tolerancia, llevándose a cabo dicha verificación mediante la lectura, por parte del agente, de dicha

variable, y la repetición de dicha lectura hasta que ésta ofrezca dicho valor por debajo de la tolerancia marcada por el programador, en cuyo caso el agente determina salir del bucle.

Un segundo aspecto de la presente invención concierne a un sistema de plataformas de computación protegidas frente a ataques externos de repetición de agentes móviles, que comprende una pluralidad de plataformas de computación conectadas a una red y adaptadas para ejecutar aplicaciones distribuidas basadas en agentes móviles que incluyen marcadores de trayecto o identificadores de agente para permitir a uno o más agentes móviles ser legalmente ejecutados en una o más de dichas plataformas de computación más de una vez, a la vez que evitar una re-ejecución ilegal de dicho o dichos agentes móviles, considerada como un ataque externo de repetición.

A diferencia de las propuestas convencionales el sistema propuesto por el segundo aspecto de la invención comprende una o más entidades de autorización en conexión con dicha red, previstas para generar como mínimo un nuevo marcador de trayecto o identificador a ser utilizado como autorización, para el agente móvil, para permitirle ser ejecutado legalmente en dicha o dichas plataformas de computación un número de veces determinado dinámicamente en tiempo de ejecución.

Para un ejemplo de realización del sistema propuesto, dicha entidad de autorización es una de dichas plataformas de computación, y para otro ejemplo de realización es un programador o usuario propietario de dicho agente móvil.

El sistema propuesto por el segundo aspecto de la presente invención está adaptado para aplicar el método propuesto por el primer aspecto.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se comprenderán más plenamente a partir de la siguiente descripción detallada de unos ejemplos de realización con referencia a los dibujos adjuntos, que deben tomarse a título ilustrativo y no limitativo, en los que:

la Fig. 1 ilustra de manera esquemática una serie de nodos que forman un itinerario simple donde una misma plataforma es visitada dos veces según el método propuesto por la presente invención para un ejemplo de realización;

la Fig. 2 muestra de manera esquemática un itinerario de nodos que incluye a un bucle formado por tres plataformas de computación que pueden ser visitadas repetidamente según el método propuesto por el primer aspecto de la presente invención para un ejemplo de realización más complejo que el de la Fig. 1;

la Fig. 3 ilustra de manera esquemática otro itinerario de nodos que incluye a dos bucles, uno dentro del otro, formado por unas plataformas de computación que pueden ser visitadas repetidamente según el método propuesto por el primer aspecto de la presente invención para otro ejemplo de realización más;

la Fig. 4 es una representación esquemática de los componentes incluidos en el interior de un agente móvil protegido contra ataques de repetición mediante la aplicación del método propuesto por la presente invención; y

las Figs. 5a y 5b muestran sendas partes de un mismo diagrama de flujo, que representan las distintas operaciones a realizar según el método propuesto por el primer aspecto de la invención, para el anteriormente explicado ejemplo de realización preferido, tras comprobar si el nodo es de tipo regular, en cuyo caso se realizan las operaciones a) a f) ilustradas en la Fig. 5a (todas o en parte en función del camino seguido en el diagrama de flujo), o de tipo bucle, en cuyo caso se realizan las operaciones i) a vi) ilustradas en la Fig. 5b (todas o en parte en función del camino seguido).

Descripción detallada de unos ejemplos de realización

Haciendo en primer lugar referencia a la Fig. 1, en ella puede apreciarse el caso más sencillo en cuanto al itinerario a recorrer por un agente móvil, donde dicho itinerario no contiene ningún bucle de nodos. En este caso cuando el agente tenga que migrar a una plataforma determinada varias veces, lo hará en diferentes etapas o nodos de su itinerario, lo que significa que ejecutará diferentes tareas. En concreto en dicha Fig. 1 la plataforma B es visitada dos veces, una primera visita en el nodo 2 y una segunda visita en el nodo 4.

Para este caso los ataques de repetición son sencillos de prevenir, mediante el almacenamiento de un identificador del nodo o de la tarea ejecutada, junto con el marcador de trayecto del agente.

Dicha Fig. 1 es un ejemplo de itinerario que puede protegerse contra ataques de re-ejecución utilizando protocolos más simples que los propuestos por la presente invención, alguno de los cuales se han citado en el apartado de estado de la técnica.

En la Fig. 2 se ilustra un itinerario de nodos representativo de un caso más complejo para el que el agente móvil tiene que ejecutar una misma tarea en la misma plataforma varias veces, un número de veces el cual es determinado dinámicamente mediante el método propuesto por la presente invención.

En particular en dicha Fig. 2 se ilustra un itinerario formado por cinco nodos, con un bucle iniciado en el nodo 2, que se ejecuta en la plataforma B, y que incluye a los nodos 3 y 4. En este caso y haciendo referencia a la clasificación de tipo de nodos descrita en un apartado anterior, los nodos 1, 3, 4 y 5 son de tipo regular y el nodo 2 es de tipo bucle, ya que pude decidir si entrar en el bucle o no, es decir, si seguir hacia el nodo 5.

En este caso la detección de ataques de repetición de agente es más complicada, ya que por ejemplo cuando la plataforma C reenvía al agente a la plataforma D, ésta última debe averiguar si una nueva ejecución es un ataque de repetición o una nueva iteración del bucle, lo cual no se podría llevar a cabo con las propuestas convencionales, pero sí mediante la aplicación del método propuesto por la presente invención, en concreto mediante la realización de las operaciones a) a f) para los nodos 1, 3, 4 y 5, y las operaciones i) a vi) para el nodo 2.

La Fig. 3 ilustra un itinerario aún más complicado que el de la Fig. 2, ya que incorpora dos bucles, uno externo formado por los nodos 1, 2 y 3, y otro interno formado por los nodos 3 y 4. En este caso los nodos 1 y 3 son de tipo bucle, y los nodos 2, 4 y 5 son de tipo regular.

En dicha Fig. 3 se han indicado las entidades de autorización, referidas como EA, y los nodos de autorización, referidos como NA, asignados a cada nodo según la descripción hecha en el apartado de explicación de la invención. En concreto los nodos 1 y 5, que no se encuentran en el interior de ningún bucle, no tienen ningún nodo de autorización y su entidad de autorización es el propietario o programador del agente móvil. Por su parte los nodos 2 y 3, que se encuentran en el interior del bucle externo, tienen como entidad de autorización la plataforma A y como nodo de autorización el nodo 1. Por último, el nodo 4, que se encuentra ubicado en el interior de bucle interno, tiene como entidad de autorización la plataforma C y como nodo de autorización el nodo 3. Es decir que para el itinerario ilustrado por la Fig. 3, existen tres entidades de autorización: el propietario del agente, la plataforma A y la plataforma C.

Según la Fig. 3, para un ejemplo de realización preferido las operaciones a) a f) (todas ellas siempre y cuando no se descarte la ejecución del agente como resultado de alguna de las mismas) se llevan a cabo cuando los nodos que reciben al agente móvil protegido son los nodos 2, 4 y 5, y las etapas i) a vi) cuando el nodo receptor es el nodo de tipo bucle 1 o el 3, en su totalidad, es decir desde i) hasta vi), siempre y cuando no se descarte la ejecución del agente como resultado de algunas de dichas operaciones.

Para un ejemplo de realización basado en la Fig. 3, para el que el agente requiera realizar una serie de iteraciones del bucle externo, la plataforma A genera y firma un nuevo marcador de trayecto para cada nueva iteración (etapa iii)) y también verifica (operación i)) que la firma del marcador de trayecto del agente que recibe dicha plataforma A haya sido realizada por el propietario (caso en que no se haya realizado una iteración previa del bucle externo) o por ella misma (caso en que se haya realizado una iteración previa del bucle externo, y que por tanto el agente portase un marcador de trayecto generado y firmado por la plataforma A). El agente móvil determina en la operación vi) si sale o no del bucle, por ejemplo en el caso del bucle externo dicha determinación se producirá en la plataforma A, y si la determinación es salir del bucle, ésta implicará un salto del agente hasta la plataforma E para ejecutar el nodo 5, en cuyo caso el marcador de trayecto dispuesto en la parte superior de la pila, y que le ha permitido realizar una iteración del bucle, es extraído de la pila del agente, de manera que el marcador de trayecto original y generado y firmado por el propietario puede ser utilizado de nuevo para continuar la ejecución en la plataforma E.

La plataforma C actuaría de manera análoga a la descrita en el párrafo anterior para la plataforma A, para permitir realizar iteraciones legales del bucle interno que no sean interpretadas como ataques de reejecución.

En la Fig. 4 se ha ilustrado de manera esquemática el contenido de un agente móvil protegido creado según el método propuesto por el primer aspecto de la presente invención.

En concreto en dicha Fig. 4 puede verse el itinerario protegido creado por el programador, formado por n nodos, la pila de marcadores de trayecto y, en detalle, uno de los marcadores de trayecto de la pila, firmado por la entidad de autorización correspondiente, apreciándose que contiene los elementos descritos en el apartado de explicación de la invención, es decir un identificador de agente, un nodo de autorización, una fecha de caducidad y un contador de bucle.

En dicha Fig. 4 también se aprecia, a la derecha, la información que contiene cada uno de los nodos del conjunto de nodos que conforman el itinerario protegido incluido en el agente móvil protegido, es decir un identificador de nodo, uno de agente, una entidad y un nodo de autorización, el tipo de nodo y la tarea a realizar en dicho nodo, así como la plataforma de computación donde será ejecutado y la plataforma siguiente.

La utilización de dicha información por parte de una plataforma que reciba al agente móvil protegido ya ha sido convenientemente explicada con anterioridad.

Mediante el método propuesto por la invención cada plataforma solamente ejecutará el nodo actual del itinerario del agente si el marcador de trayecto actual (el que se encuentra en la parte superior de la pila) ha sido firmado por la entidad de autorización apropiada.

Al asociar cada nodo del itinerario a ambos, una entidad y un nodo de autorización se impide la posibilidad de que un atacante intentase efectuar un ataque de repetición con un agente, reutilizando un marcador de trayecto firmado

por la entidad de autorización apropiada pero no generado en el nodo del itinerario apropiado, es decir en el nodo de autorización. Este ataque será detectado por las plataformas cuando verifiquen si el marcador de trayecto ha sido generado y firmado en el nodo apropiado, es decir el de autorización.

Cada nodo del itinerario contiene asimismo un identificador de agente, el cual también está incluido en el marcador de trayecto del agente, con lo cual se evita que un marcador de trayecto dado sea reutilizado en diferentes agentes, ya que esto será detectado por las plataformas de computación cuando, aplicando el método propuesto, comparen el identificador de agente extraído del nodo actual con el incluido en el marcador de trayecto.

Tal y como se ha explicado anteriormente, el método propuesto por la presente invención también comprende proteger, por ejemplo mediante encriptación, el itinerario del agente con el fin de que ningún atacante pueda cambiar la información asociada con un nodo dado. Esta protección también evita que la tarea del agente sea ejecutada en una plataforma diferente de las establecidas inicialmente.

El método propuesto no requiere que el agente interactúe con entidades externas, y solamente asume que los nodos tipo bucle serán ejecutados en plataformas fiables para el programador, ya que no es posible evitar que las plataformas manipulen la ejecución del agente que llega a las mismas.

Para un ejemplo de realización, las plataformas impiden que sus tablas de marcadores de trayecto se llenen en exceso eliminando las entradas que hayan caducado. Adicionalmente se puede aplicar otra política con el fin de posibilitar la eliminación de entradas cuando no quepan más marcadores de trayecto en una tabla (por ejemplo eliminando los más antiguos.

Con el fin de demostrar la viabilidad del método propuesto por la presente invención, a continuación se describe un ejemplo de implementación del mismo aplicando el método propuesto a un escenario como el que se describe en "Secure integration of distributed medical data using mobile agents", de "IEEE Intelligent Systems 2006"; 21(6):47-54, por los autores Vieira-Marques P, Robles S, Cucurull J, Cruz-Correia R, Navarro G, Martí R.

Este escenario corresponde al de instituciones médicas en las que se ha implantado un sistema de gestión de información basado en agentes móviles. En estos escenarios, el proceso de registro de pacientes está gestionado por una plataforma de agentes, la cual mantiene un registro de los pacientes atendidos por la institución. Además, cada uno de los departamentos de la institución médica posee una plataforma de agentes que gestiona el historial de los pacientes atendidos, y los servicios que se les han realizado.

En estos escenarios, los agentes móviles se utilizan, entre otras tareas, para automatizar el proceso de recuperación de historiales clínicos distribuidos por diferentes instituciones. Supongamos que se requiere realizar una operación quirúrgica urgente a una víctima de un accidente. Antes de empezar cualquier operación en la que haya contacto con sangre, el personal médico debe saber si el paciente es portador del virus del VIH o la Hepatitis B. La realización de las pruebas pertinentes antes de la intervención es inviable, debido a que se necesitan días para obtener los resultados. Tampoco es posible confiar en los pacientes para obtener esta información; ya que pueden estar inconscientes. Por este motivo, la recuperación de esta información se realiza mediante una aplicación basada en agentes móviles.

La aplicación es iniciada por un profesional médico que introduce los datos del paciente y la identificación de los resultados de las pruebas que se deben obtener en un interfaz gráfico. A partir de aquí, la aplicación genera un agente móvil al cual introduce toda la información recopilada anteriormente. El agente móvil, en primer lugar, consulta una base de datos con información acerca de todas las instituciones que realizan las pruebas del VIH y la Hepatitis B, en este caso concreto. El agente obtiene así una lista de todas aquellas instituciones en las que se realizan estas pruebas.

A continuación, el agente lleva a cabo una consulta remota a cada una de estas instituciones para determinar si el paciente ha sido visitado alguna vez en dicha institución o no. En caso positivo, el agente móvil se desplaza al departamento pertinente de la institución médica para elegir y extraer los resultados que se necesitan. Este proceso se repite para todas y cada una de las instituciones que realizan las pruebas correspondientes al virus del VIH y de la Hepatitis B. Como puede observarse, el uso de la tecnología de agentes móviles permite automatizar y agilizar enormemente el proceso de recuperación y extracción de información.

Sin embargo, el uso de agentes móviles puede conllevar problemas de robo de información privada de los pacientes si no se utilizan las medidas de seguridad adecuadas. Un atacante podría capturar el agente y reejecutarlo más adelante para obtener información privada de un paciente. Por ejemplo, un agente podría ser capturado y reenviado a la misma institución más adelante para obtener resultados de pruebas posteriores realizadas al paciente.

Además, dicho ataque de reejecución podría suponer también pérdidas económicas para el paciente, en caso de que el agente visitara una institución privada para llevar a cabo un servicio de pago. Por ejemplo, una radiografía del paciente realizada en un centro médico podría ser transportada por el agente para su posterior análisis a una institución privada. La utilización del agente móvil permitiría al paciente evitarse un desplazamiento a dicha institución. Sin embargo, si el agente fuese reenviado por un atacante a la misma institución en repetidas ocasiones, el paciente acabaría pagando múltiples veces por el mismo servicio.

Por lo tanto, la implementación del método de de protección contra ataques de reejecución presentado en la presente invención es imprescindible para la utilización segura de agentes móviles en este escenario de aplicación distribuida. Este escenario es un ejemplo claro de necesidad de utilización de mecanismos adecuados para la prevención de los ataques de reejecución. En esta implementación, se ha aplicado el método propuesto a un escenario relacionado con instituciones médicas, pero el método propuesto por la presente invención es aplicable a muchos otros escenarios relacionados, por ejemplo, con instituciones financieras, agencias de viaje, o cualquier otro que conlleve tratamiento de información confidencial o transacciones comerciales.

Un experto en la materia podría introducir cambios y modificaciones en los ejemplos de realización descritos sin salirse del alcance de la invención según está definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para la protección de plataformas de computación frente a ataques externos de repetición de agentes móviles, del tipo que comprende utilizar un sistema de plataformas de computación conectadas a una red para la ejecución compartida de aplicaciones distribuidas basadas en agentes móviles, y que comprende utilizar marcadores de trayecto o identificadores de agente para permitir a al menos un agente móvil ser legalmente ejecutado en una plataforma de computación más de una vez, a la vez que evitar una re-ejecución ilegal de dicho agente móvil, considerada como un ataque externo de repetición, **caracterizado** porque comprende:

- crear un agente móvil protegido frente a ataques de reejecución, incluyendo al menos un marcador de trayecto inicial o identificador, un itinerario protegido y dicho agente móvil propiamente dicho, que es al menos uno,

- generar al menos un nuevo marcador de trayecto o identificador, para dicho agente móvil protegido, que es al menos uno, utilizando al menos una entidad de autorización;

- enviar dicho agente móvil protegido a dicha plataforma de computación,

- recibir dicho agente móvil protegido en dicha plataforma de computación, y

- utilizar, por parte de dicha plataforma de computación, dicho nuevo marcador de trayecto o identificador del agente móvil recibido como una autorización para permitir a dicho agente móvil ser ejecutado legalmente en al menos dicha plataforma de computación un número de veces determinado dinámicamente en tiempo de ejecución, donde para llevar a cabo dicha etapa de utilización de dicho nuevo marcador de trayecto, o identificador del agente móvil recibido, como una autorización, el método comprende extraer, por parte de dicha plataforma de computación, al menos parte de la información incluida en dicho agente móvil protegido y utilizarla para comprobar si dicho agente móvil protegido ya ha sido ejecutado anteriormente, mediante al menos la comparación de al menos parte de dicha información extraída con información almacenada en dicha plataforma de computación, incluyendo dicha información almacenada al menos marcadores de trayecto de agentes ejecutados previamente, junto con unos respectivos identificadores de nodo representativos de las tareas de nodo ejecutadas por dichos agentes.

2. Método según la reivindicación 1, **caracterizado** porque comprende almacenar en dicha plataforma de computación un identificador de la tarea ejecutada por dicho agente móvil protegido en dicha plataforma de computación, junto con su respectivo marcador de trayecto, con el fin de permitir que sea re-ejecutada un número de veces determinado.

3. Método según la reivindicación 2, **caracterizado** porque dicha re-ejecución legal hace referencia a la ejecución de diferentes tareas en diferentes respectivos nodos o etapas del itinerario del agente móvil, siendo cada uno de dichos nodos diferente y representativo de una visita a dicha plataforma de computación en un momento distinto al del resto de los nodos, estando cada nodo asociado con una tarea y una plataforma concretas.

4. Método según la reivindicación 2, **caracterizado** porque dicha re-ejecución legal hace referencia a la ejecución de una misma tarea en diferentes visitas respectivas a dicha plataforma de computación a lo largo del itinerario del agente móvil, siendo cada una de dichas visitas representada por un mismo nodo, o etapa, asociado con una tarea y una plataforma concretas.

5. Método según la reivindicación 2, **caracterizado** porque comprende generar y asociar un marcador de trayecto o identificador diferente a cada uno de varios agentes móviles, incluso si ejecutan exactamente las mismas tareas, y a cada instancia del mismo agente móvil.

6. Método según la reivindicación 5, **caracterizado** porque comprende llevar a cabo dicha creación de dicho agente móvil protegido por parte de un usuario propietario o programador.

7. Método según la reivindicación 6, **caracterizado** porque comprende construir dicho itinerario protegido mediante la realización de las siguientes acciones:

- definir un conjunto de nodos o etapas que conforman dicho itinerario de agente móvil, siendo cada uno de dichos nodos representativo de una respectiva visita a dicha plataforma de computación en un momento distinto para ejecutar una tarea correspondiente, y estando cada uno de dichos nodos asociado a una entidad de autorización correspondiente que es la única encargada de generar nuevos marcadores de trayecto válidos utilizados como autorizaciones para la ejecución de la tarea asociada con dicho nodo;

- proteger dicho itinerario de agente utilizando un protocolo de protección.

8. Método según la reivindicación 7, **caracterizado** porque, con el fin de definir dicho conjunto de nodos, el método comprende asignar la siguiente información a cada uno de los nodos que conforman el conjunto:

- un identificador de nodo;

- una plataforma de computación donde será ejecutado;

- una tarea;

- un tipo de nodo;

- plataforma siguiente;

- una entidad de autorización;

- un nodo de autorización;

- un identificador de agente.

9. Método según la reivindicación 8, **caracterizado** porque comprende, con el fin de definir dicho tipo de nodo, establecer los siguientes dos tipos de nodo:

- un tipo de nodo regular, el cual se refiere a un nodo que es una etapa del itinerario donde el agente móvil ejecuta su tarea y salta a la siguiente plataforma de computación del itinerario;

- un tipo de nodo bucle, el cual hace referencia a un nodo que es una etapa del itinerario donde el agente móvil determina si inicia o no una iteración de un número determinado de nodos.

10. Método según la reivindicación 9, **caracterizado** porque comprende definir dicho nodo de autorización como un identificador del nodo donde el marcador de trayecto del agente móvil debe ser generado, ya sea dicho marcador de trayecto inicial o uno de dichos nuevos marcadores de trayecto, y definir dicha entidad de autorización como la plataforma de computación correspondiente o el usuario propietario o programador que debe generar y firmar el marcador de trayecto.

11. Método según la reivindicación 10, **caracterizado** porque comprende asignar o no un respectivo nodo de autorización a cada nodo, dependiendo de si el nodo se encuentra ubicado o no en el interior de un bucle.

12. Método según la reivindicación 11, **caracterizado** porque comprende asignar como nodo de autorización, a cada nodo que se encuentra ubicado en el interior de un bucle, el nodo de bucle ubicado al inicio del bucle y como su correspondiente entidad de autorización la plataforma de computación donde la tarea de dicho nodo inicial de bucle es ejecutada, y a cada nodo que no se encuentra en el interior de un bucle, ningún nodo de autorización y como su correspondiente entidad de autorización a dicho usuario propietario del agente móvil.

13. Método según la reivindicación 12, **caracterizado** porque comprende utilizar un identificador de agente para vincular los nodos de itinerario al agente móvil.

14. Método según la reivindicación 12, **caracterizado** porque comprende generar dicho marcador de trayecto para el agente móvil, ya sea dicho marcador de trayecto inicial o uno de dichos nuevos marcadores de trayecto, con la siguiente información:

- un identificador de agente idéntico a dicho identificador de agente incluido en el itinerario protegido y utilizado para vincular a los nodos de itinerario con el agente móvil, para asegurar que cualquier instancia de agente móvil pueda ser identificada de manera única;

- un nodo de autorización como un identificador del nodo donde dicho marcador de trayecto es generado;

- una fecha de caducidad tras la cual el marcador de trayecto no puede ser utilizado más; y

- un contador de bucle incrementado en una unidad cada vez que el agente móvil tiene que iniciar una nueva iteración de un bucle.

15. Método según la reivindicación 14, **caracterizado** porque cuando dicho marcador de trayecto generado es dicho marcador de trayecto inicial éste es generado por parte de dicho usuario propietario o programador, y cuando es uno de dichos nuevos marcadores de trayecto éste es generado por parte de la plataforma de computación correspondiente a la entidad de autorización asignada en dicho itinerario protegido.

16. Método según la reivindicación 15, **caracterizado** porque comprende firmar dicho marcador de trayecto generado por dicho usuario propietario o dicha entidad de autorización y colocarlo en la parte superior de una pila de marcadores de trayecto del agente configurada para almacenar marcadores de trayecto previamente utilizados por el agente móvil durante su ejecución.

17. Método según la reivindicación 16, **caracterizado** porque dicha extracción de información llevada a cabo por dicha plataforma de computación desde dicho agente móvil protegido recibido concierne a:

- extraer la información del nodo actual de dicho itinerario protegido para obtener dicho identificador de nodo, identificador de agente, tarea, tipo de nodo, plataforma siguiente, entidad de autorización y nodo de autorización; y

- recuperar el marcador de trayecto del agente de la parte superior de la pila de marcadores de trayecto del agente y extraer del marcador de trayecto recuperado el identificador de agente, el nodo de autorización, la fecha de caducidad y el contador de bucle.

18. Método según la reivindicación 17, **caracterizado** porque comprende en primer lugar utilizar, por parte de dicha plataforma de computación receptora del agente móvil protegido, el tipo del nodo actual para determinar si el agente está ejecutando un nodo tipo regular o un nodo tipo bucle.

19. Método según la reivindicación 18, **caracterizado** porque comprende realizar, por parte de dicha plataforma de computación receptora del agente móvil protegido, al menos parte de las siguientes operaciones si dicho nodo actual es un nodo de tipo regular:

a) verificar la firma del marcador de trayecto para comprobar si el marcador de trayecto ha sido firmado por la entidad de autorización actual, y si dicha verificación no resulta exitosa descartar la ejecución del agente, o si resulta exitosa realizar la siguiente operación;

b) comprobar que el nodo de autorización actual, que está incluido en el marcador de trayecto, es el mismo que el extraído del itinerario protegido y si dicha comprobación falla descartar la ejecución del agente, o si es exitosa realizar la siguiente operación;

c) comprobar que el identificador de agente incluido en el marcador de trayecto es igual al obtenido del itinerario protegido, y si dicha comprobación falla descartar la ejecución del agente, o si es exitosa realizar la siguiente operación;

d) comprobar la fecha de caducidad del marcador de trayecto, y si el marcador de trayecto ha caducado descartar la ejecución del agente, o si no ha caducado realizar la siguiente operación;

e) utilizar el identificador de agente para buscar un marcador de trayecto previo del mismo agente en dicha información almacenada en la plataforma de computación que incluye marcadores de trayecto de agentes ejecutados previamente junto con los respectivos identificadores de nodo representativos de las tareas ejecutadas por dichos agentes, siendo dicha información almacenada representada por una tabla, y:

e1) si no hay ningún marcador de trayecto con el mismo identificador de agente en dicha tabla, almacenar el nuevo marcador de trayecto junto con el identificador del nodo actual en dicha tabla;

e2) si existe un marcador de trayecto previo con el mismo identificador de agente en dicha tabla, lo que significa que el mismo agente ya había sido ejecutado con anterioridad en esta plataforma de computación, comprobar si el identificador del nodo actual del agente es igual al de la ejecución previa, mediante la consulta de dicha tabla; y

e2a) si el identificador del nodo actual del agente es diferente al de la ejecución previa, lo que significa que el agente va a ejecutar una tarea diferente correspondiente a un nodo del itinerario distinto, almacenar el marcador de trayecto junto con el nuevo identificador del nodo actual en dicha tabla;

e2b) si el identificador del nodo actual del agente es igual al de la ejecución previa, lo que significa que la tarea de este nodo del itinerario había sido ejecutada en la ejecución previa, comparar el contador de bucle actual con el incluido en el marcador de trayecto previo, y:

e2b1) si el contador de bucle actual es mayor que el previo, lo que significa que el agente está realizando una nueva iteración de un bucle, reemplazar, en dicha tabla, el marcador de trayecto previo con el actual;

e2b2) si el contador de trayecto actual no es mayor que el previo, lo que significa que el marcador de trayecto ya ha sido utilizado, descartar la ejecución del agente;

f) si la ejecución del agente no ha sido descartada en ninguna de las operaciones previas, ejecutar la tarea correspondiente al nodo actual.

20. Método según la reivindicación 19, **caracterizado** porque comprende realizar, por parte de dicha plataforma de computación receptora del agente móvil protegido, al menos parte de las siguientes operaciones si dicho nodo actual es un nodo de tipo bucle:

i) verificar la firma del marcador de trayecto para comprobar si dicho marcador de trayecto ha sido firmado por la entidad de autorización actual o por la plataforma de computación actual, y si ambas comprobaciones fallan descartar la ejecución del agente, o si al menos una de ambas comprobaciones es exitosa realizar la siguiente operación;

ii) realizar la siguiente operación:

- comprobar que el nodo de autorización actual, que está incluido en el marcador de trayecto, es el mismo que el extraído del itinerario protegido o coincide con el nodo actual y si ambas comprobaciones fallan descartar la ejecución del agente, o si al menos una es exitosa realizar dichas operaciones c) a e);

iii) generar y firmar un nuevo marcador de trayecto conteniendo la misma información que el marcador de trayecto previo, a excepción del nodo de autorización, siendo asignado como nodo de autorización el nodo actual, y a excepción también del contador de bucle, el cual es incrementado en una unidad;

iv) comprobar si el agente está visitando el nodo de tipo bucle por primera vez, lo que significa que el agente todavía no ha realizado ninguna iteración previa del bucle iniciado en el nodo tipo bucle, y:

iva) si el agente está visitando el nodo bucle por primera vez, añadir el nuevo marcador de trayecto a la pila de marcadores de trayecto del agente, colocándolo en la parte superior de la misma;

ivb) si el agente ya ha realizado alguna iteración del bucle anteriormente, reemplazar el marcador de trayecto actual, el cual estaba dispuesto en la parte superior de la pila de marcadores de trayecto del agente, con el nuevo marcador de trayecto;

v) realizar dicha operación f);

vi) determinar, por parte del agente, si debe realizar una iteración del bucle; y:

via) si una iteración debe ser llevada a cabo, hacer saltar el agente móvil protegido a la siguiente plataforma del interior del bucle actual, comprobar el tipo de nodo y en función del tipo de nodo realizar las operaciones a) a f) o i) a vi);

vib) si no se requiere la realización de una iteración del bucle, extraer, por parte del agente, el marcador de trayecto de la parte superior de la pila, saltar el agente móvil protegido a la siguiente plataforma fuera del bucle actual, comprobar el tipo de nodo y en función del tipo de nodo realizar las operaciones a) a f) o i) a vi).

21. Método según la reivindicación 19, **caracterizado** porque dichas operaciones a) a f) son llevadas a cabo en dicha plataforma de computación.

22. Método según la reivindicación 20, **caracterizado** porque dichas operaciones i) a v) son llevadas a cabo en dicha plataforma de computación.

23. Sistema de plataformas de computación protegidas frente a ataques externos de repetición de agentes móviles, del tipo que comprende una pluralidad de plataformas de computación conectadas a una red y adaptadas para ejecutar aplicaciones distribuidas basadas en agentes móviles que incluyen marcadores de trayecto o identificadores de agente para permitir a al menos un agente móvil ser legalmente ejecutado en al menos una de dichas plataformas de computación más de una vez, a la vez que evitar una re-ejecución ilegal de dicho agente móvil, considerada como un ataque externo de repetición, **caracterizado** porque comprende al menos una entidad de autorización en conexión con dicha red, prevista para generar al menos un nuevo marcador de trayecto o identificador a ser utilizado como autorización, para dicho agente móvil, que es al menos uno, para permitirle ser ejecutado legalmente en al menos dicha plataforma de computación un número de veces determinado dinámicamente en tiempo de ejecución.

24. Sistema según la reivindicación 23, **caracterizado** porque dicha entidad de autorización es una de dichas plataformas de computación.

25. Sistema según la reivindicación 23, **caracterizado** porque dicha entidad de autorización es un programador o usuario propietario de dicho agente móvil.

26. Sistema según la reivindicación 23, 24 ó 25, **caracterizado** porque está adaptado para aplicar el método según una cualquiera de las reivindicaciones 1 a 22.

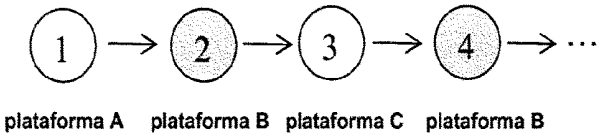

Fig. 1

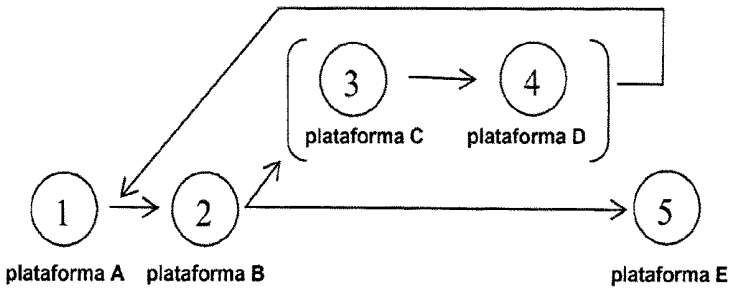

Fig. 2

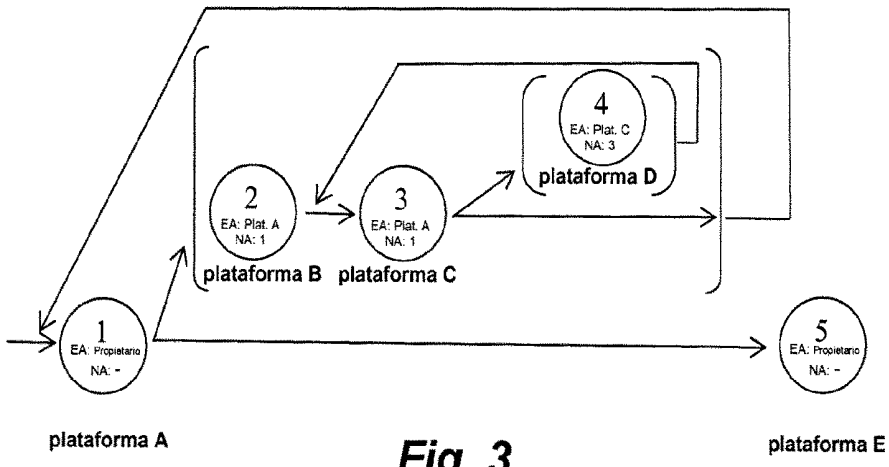

Fig. 3

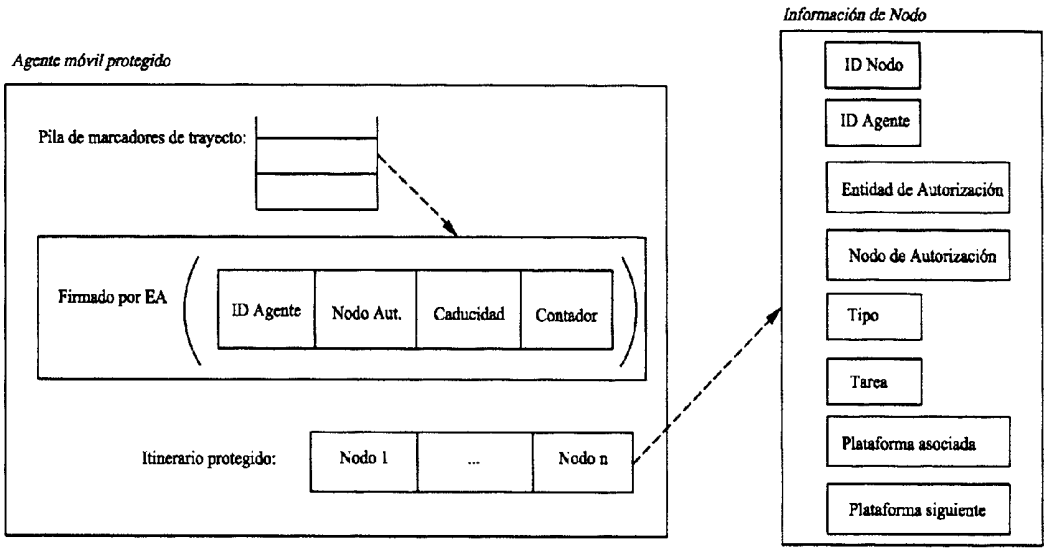
Información de Nodo
Agente móvil protegido
Pila de marcadores de trayecto:
Firmado por EA
ID Agente
Nodo Aut.
Caducidad
Contador
Itinerario protegido:
Nodo 1
...
Nodo n
ID Nodo
ID Agente
Entidad de Autorización
Nodo de Autorización
Tipo
Tarea
Plataforma asociada
Plataforma siguiente

Fig. 4

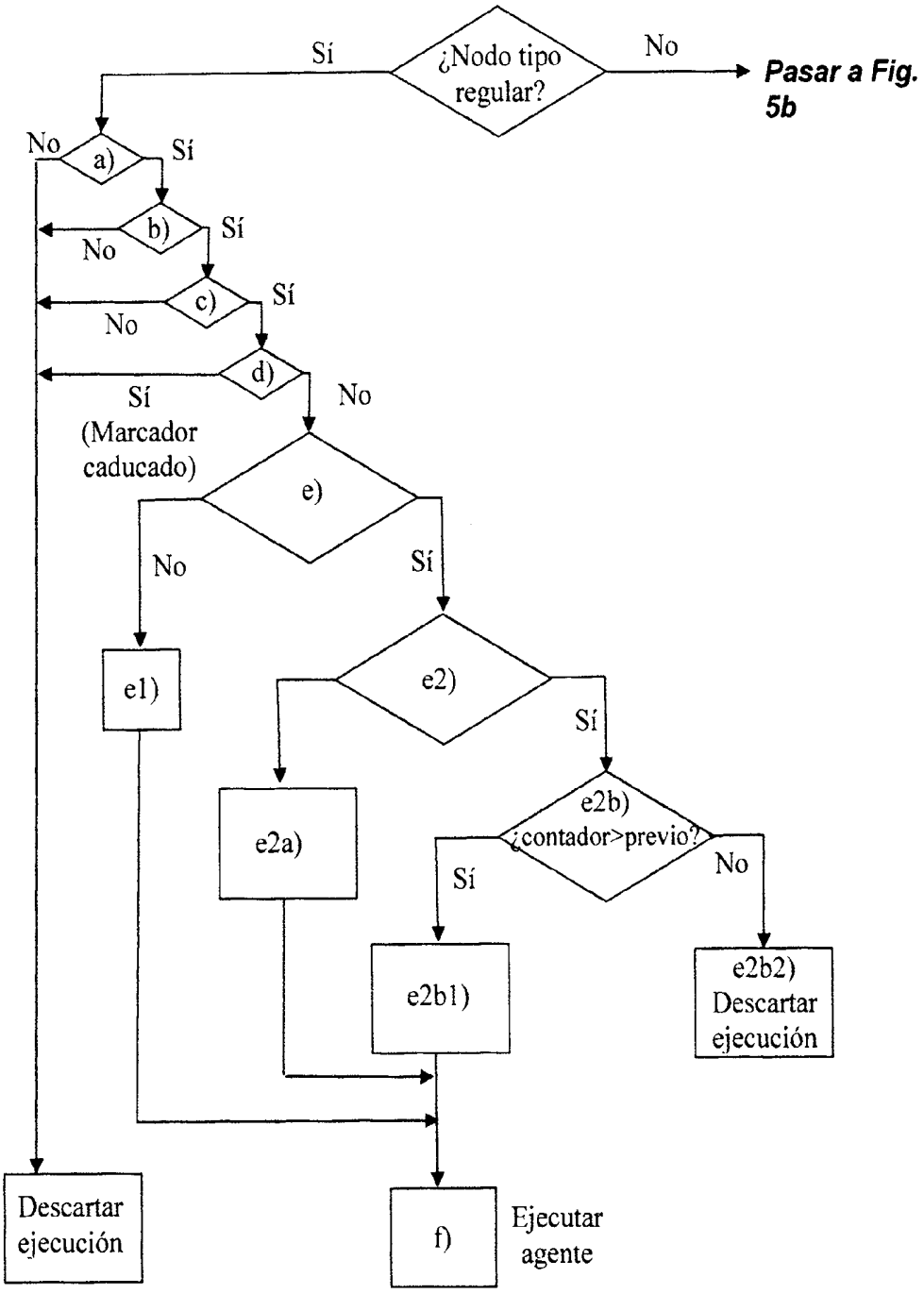
¿Nodo tipo regular?
Sí
No
Pasar a Fig. 5b
a)
b)
c)
d)
e)
e1)
e2)
e2a)
e2b)
¿contador>previo?
e2b1)
e2b2) Descartar ejecución
Descartar ejecución
f)
Ejecutar agente
(Marcador caducado)

Fig. 5a

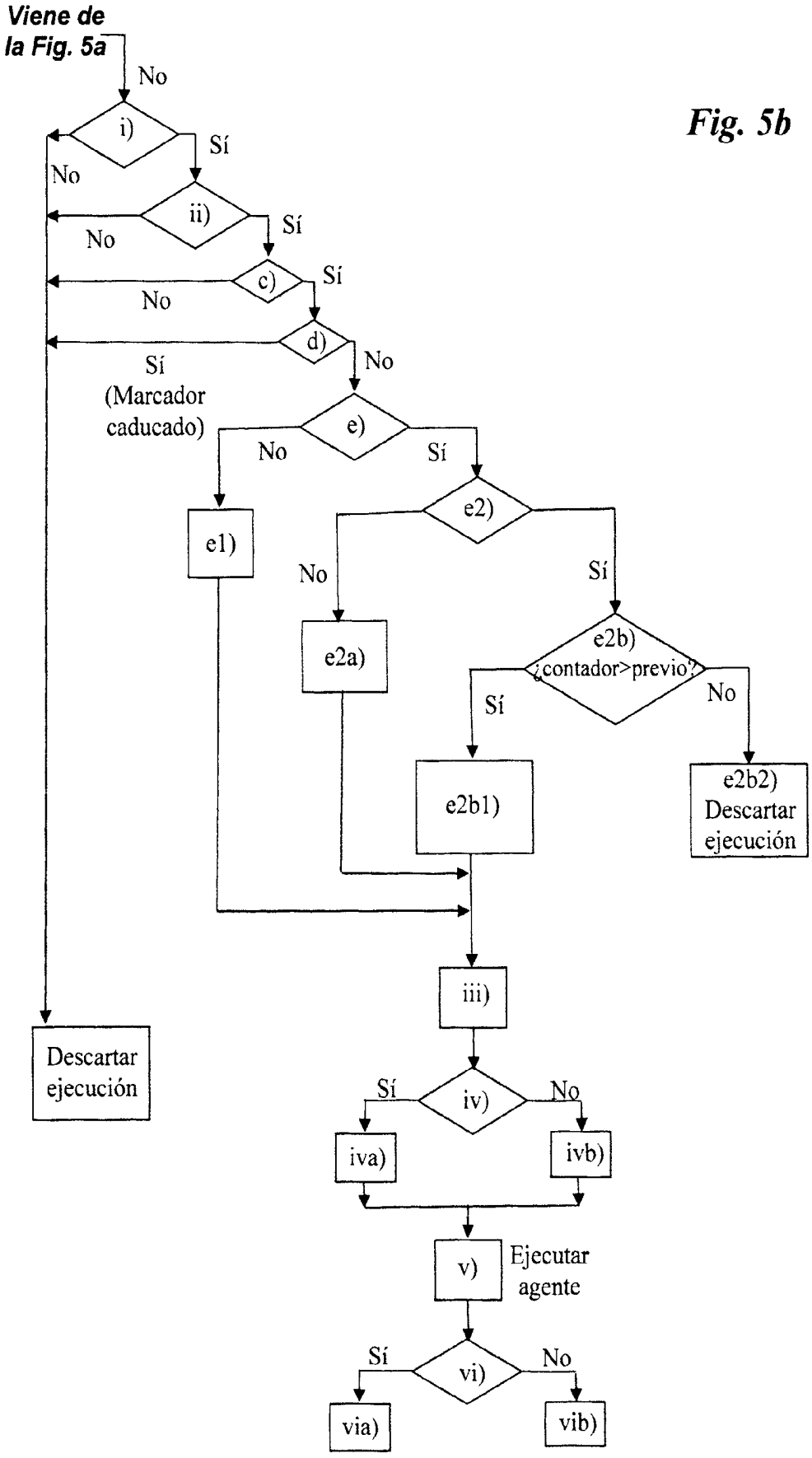
Viene de la Fig. 5a
No
i)
Sí
No
ii)
Sí
No
c)
Sí
No
d)
No
Sí
(Marcador caducado)
e)
No
Sí
e1)
e2)
No
Sí
e2a)
e2b)
¿contador>previo?
Sí
No
e2b1)
e2b2) Descartar ejecución
iii)
Descartar ejecución
Sí
iv)
No
iva)
ivb)
v)
Ejecutar agente
Sí
vi)
No
via)
vib)

Fig. 5b

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 327 310

(21) Nº de solicitud: 200801492

(22) Fecha de presentación de la solicitud: **19.05.2008**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** Ver hoja adicional

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
Y	US 2004037423 A1 (GHANEA-HERCOCK et al.) 26.02.2004, resumen; párrafos [24-97]; figuras 2-9.	1-26
Y	EP 1067457 A1 (SONY INT EUROP GMBH) 10.01.2001, resumen; párrafos [20-32],[44-58]; figuras 3,6.	1-26
A	US 6055562 A (DEVARAKONDA et al.) 25.04.2000, resumen; columna 1, línea 44 - columna 3, línea 58; figura 1.	1-26
A	A Securing dynamic itineraries for mobile agent applications. (CARLES GARRIGUES et al.), Journal of Network and Computer Applications Volume 31, Issue 4, Noviembre 2008, Páginas 487-508. Available online 23 Diciembre 2007. Todo el documento.	1-26

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
14.10.2009	J. Santaella Vallejo	1/2

INFORME DEL ESTADO DE LA TÉCNICA

Nº de solicitud: 200801492

CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

G06F 9/46 (2006.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)