(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 300 850**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04800299 .2**
(86) Fecha de presentación : **09.11.2004**
(87) Número de publicación de la solicitud: **1810473**
(87) Fecha de publicación de la solicitud: **25.07.2007**

(54) Título: **Aparato y método para la prevención del fraude cuando se accede a través de redes de área local inalámbricas.**

(45) Fecha de publicación de la mención BOPI:
16.06.2008

(45) Fecha de la publicación del folleto de la patente:
16.06.2008

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON
S-164 83 Stockholm, SE

(72) Inventor/es: **Ramos Robles, Luis;**
Fernández Alonso, Susana y
Ávila González, Víctor Manuel

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Aparato y método para la prevención del fraude cuando se accede a través de redes de área local inalámbricas.

Campo de la invención

La presente invención se refiere generalmente a medios y métodos para detectar posibles situaciones de fraude que pueden aparecer cuando los usuarios son habilitados para acceder a una red de telecomunicación a través de un número de puntos de acceso de una o más redes de área local inalámbricas (WLAN: wireless local area network). Más específicamente, la presente invención es particularmente aplicable en escenarios donde una sesión de usuario es habilitada para comprender simultáneamente más de una sesión de acceso establecida a través de un número de puntos de acceso.

Antecedentes

Operadores tradicionales de telefonía móvil y fija están entrando en el mercado de redes de área local inalámbrica (WLAN) para proporcionar acceso WLAN a sus abonados cuando usan terminales habilitados para WLAN en áreas de puntos sensibles. En este contexto, un usuario tiene una relación comercial con su operador de red de origen, tal como un operador de telefonía, que establece acuerdos de itineración con un número de proveedores de acceso WLAN (denominados en los sucesivo WISP's (WLAN Access Providers). En particular, un propio operador de red de origen también podría desplegar infraestructura de acceso WLAN y actuar con un proveedor de acceso WLAN (WISP).

Así, un escenario bastante corriente es cuando un usuario obtiene acceso WLAN desde proveedores de acceso WLAN (WISP's) diferentes que tienen acuerdos de itinerancia con el operador de red de origen del usuario. El operador de red de origen de usuario carga al usuario por el uso de acceso WLAN y paga a los proveedores de acceso WLAN (WISP's) correspondientes para proporcionar tal acceso WLAN a sus abonados. Según este escenario, una red de origen de usuario lleva a cabo una autenticación del usuario y recibe información de contabilidad desde el WISP que proporciona el acceso WLAN.

Teniendo en cuenta la posición intermediaria de los operadores de redes desde una perspectiva de cargo, los operadores de redes están interesados actualmente en tener más control sobre esas sesiones de acceso WLAN que sus usuarios podrían establecer. El control de las sesiones de acceso WLAN es llevado a cabo generalmente por cada WISP y varía de un escenario a otro o, en otras palabras, de una versión de infraestructura de WLAN a otra.

Una infraestructura de WLAN típica en un primer escenario, el denominado acceso WLAN basado en Web, incluye un número de puntos de acceso WLAN (AP's en lo sucesivo), que proveen a los usuarios de conectividad WLAN por una interfaz de radio, y un servidor de acceso WLAN (AS en lo sucesivo) que implementa el control de acceso y otras funciones tales como, por ejemplo, asignación de dirección IP (Internet Protocol) y aplicación de autorización. En este primer escenario, cada punto de acceso WLAN (AP) proporciona acceso WLAN a un usuario (UE) permitiendo que el usuario obtenga conectividad IP hacia el servidor de acceso WLAN (AS), pero el AS bloquea cualquier tráfico de usuario más allá hasta que el usuario ha sido autenticado satisfactoriamente.

Por tanto, como ilustra la Figura 1, el equipo de usuario (UE-1) incluye un explorador Web en el que el AS presenta (S-04) una página de inicio de sesión al usuario. El usuario introduce (S-05) credenciales de usuario en dicha página de inicio de sesión y el AS envía (S-06) tales credenciales hacia un servidor de autenticación (Auth-S) en la red de origen (HOME) para verificación. En la autenticación satisfactoria, es decir, en la verificación de credenciales, el AS concede acceso al usuario, envía (S-07) una indicación de comienzo de contabilidad hacia un servidor de contabilidad (Acc-S) en la red de origen (HOME) e inicia una sesión de acceso.

Para el fin de la presente invención, una sesión de acceso es un depósito de datos que una entidad, responsable del control de acceso a una red de acceso, mantiene con relación a un usuario de dicha red de acceso. Típicamente, esta sesión de acceso es iniciada una vez que el usuario ha sido autenticado, y es mantenida viva mientras el usuario está accediendo a la red de acceso bajo el control de dicha entidad. Los datos incluidos en la sesión de acceso incluyen típicamente un identificador de usuario, un identificador único de sesión de acceso y otros parámetros tales como, por ejemplo, un identificador de terminal y claves de seguridad.

Según esta primera realización, una vez que la sesión de acceso ha sido iniciada para el usuario, información sobre esta sesión de acceso es enviada a la red de origen. Ahora, siempre que el usuario se mueva entre puntos de acceso WLAN (AP's) diferentes dentro de la infraestructura del mismo proveedor de acceso WLAN (WISP), dichos AP's diferentes son conectados al mismo servidor de acceso WLAN (AS) y una reautenticación no es necesaria. Además, el AS es capaz de conservar la misma sesión de acceso que fue creada cuando se accede desde el primer AP.

Es decir, según este primer escenario, hay una sesión de acceso única para un usuario aunque el usuario se mueva desde un primer a un segundo AP, ambos bajo el control de un AS. De tal modo, como este enfoque centraliza el control de acceso en el AS, la información de sesión de acceso manejada por el AS, y enviada desde el AS a la red de origen, es suficiente para permitir que la red de origen tenga control de las sesiones de acceso WLAN que sus abonados establecen como usuarios de la red de acceso WLAN.

Una infraestructura de WLAN desarrollada actualmente en un segundo escenario, que sigue la norma 802.1x del IEEE, incluye un número de puntos de acceso WLAN (AP's) que proveen a los usuarios de conectividad WLAN por una interfaz de radio, como en el escenario anterior, y llevan a cabo un control de acceso de acuerdo con dicha norma 802.1x del IEEE, y, opcionalmente, un servidor de acceso WLAN (AS) que implementa funciones tales como, por ejemplo, asignación de dirección IP.

Según este segundo escenario mostrado en la Figura 2, cada AP (AP-1) es responsable de aplicar una autenticación de usuario (S-10) basado en Internet Engineering Task Force Request for Comments (IETF RFC) 2284 "Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)". Este método de protocolo de autenticación extensible (EAP) es ejecutado de extremo a extremo (S-11) entre el usuario (UE-1) y un servidor de autenticación (Auth-S) en la red de origen (HOME) de usuario, y antes de proporcionar conectividad IP al usuario. Una vez que la autenticación de usuario es completada satisfactoriamente, el AP (AP-1) concede acceso al usuario permitiendo el establecimiento de la conexión WLAN (S01), enviando (S-07) una indicación de comienzo de contabilidad hacia un servidor de contabilidad (Acc-S) en la red de origen (HOME) e iniciando una sesión de acceso para el usuario, como lo hace el AS en el primer escenario anterior. Después, el AP (AP-1) en este segundo escenario envía información de sesiones de acceso a la red de origen para que esta tenga control de las sesiones de acceso WLAN que sus abonados establecen como usuario de la red de acceso WLAN. Dado que el servidor de acceso WLAN (AS) es opcional en este segundo escenario, el usuario (UE) podría obtener conectividad IP del AS, siempre que exista, o del AP en caso contrario.

El segundo escenario descrito anteriormente presenta algunas ventajas respecto al primero. Por una parte, el control de acceso es llevado a cabo antes del establecimiento de conectividad IP, lo que es considerado más seguro. Por otra parte, una mayor variedad de métodos de autenticación pueden ser usados dentro de un marco de protocolo de autenticación extensible (EAP), como ejemplar representado para el segundo escenario. Esta variedad de métodos de autenticación para usar en el segundo escenario, y que no puede ser usada en el primero, incluye métodos de autenticación basados en el módulo de identidad de abonado (SIM: Subscriber Identity Module) tales como los explicados respectivamente en IETF draft-haverlnen-pppext-eap-sim-12 "EAP SIM Autenthication", Octubre de 2.003, y en IETF draft-arkko-pppext-eap-aka-11 "Extensible Authentication Protocol Authentication and Key Agreement (EAP AKA) Autenthication", Octubre de 2.003.

Sin embargo, el segundo escenario también presenta algunas desventajas respecto al primer escenario. Por ejemplo, cuando un usuario se mueve entre un primer y un segundo AP en el segundo escenario, una autenticación nueva del usuario es requerida otra vez. Esto es debido al hecho de que cada AP está dispuesto para controlar sesiones de acceso independientes, permitiendo así que un usuario mantenga vivas sesiones de acceso diferentes a la vez a través de AP's diferentes, y perteneciendo los AP's diferentes a un mismo proveedor de acceso WLAN (WISP) o a WISP's diferentes.

Por otra parte, el soporte para sesiones de acceso diferentes a través de AP's diferentes, como hace el segundo escenario, puede ser considerado como una ventaja adicional que proporciona soporte para llevar a cabo una preautenticación. En este aspecto, una preautenticación permite que un usuario, que ha obtenido acceso a un primer AP dado, pueda llevar a cabo un procedimiento de autenticación para un segundo AP, que es diferente que el primer AP, antes de moverse realmente a dicho segundo AP. De este modo, la transferencia desde un AP a otro puede ser efectuada más rápidamente, proporcionando así al usuario una percepción de una sesión continua de usuario.

Una mezcla ejemplar de los escenarios primero y segundo anteriores puede ser aprendida de la publicación internacional WO 2004/029823 en la que los puntos de acceso WLAN (AP's) están provistos de funciones de control de acceso de acuerdo con la norma 802.1x del IEEE y que incluyen una aplicación de "Protocolo de Autenticación Extensible" (EAP: Extensible Authentication Protocol). Una función de control de acceso, que es activa en un AP, solicita un código de acceso a cualquier usuario que intenta acceder a la red de acceso. El usuario podría haber obtenido tal código de acceso de fuentes diferentes tal como el operador de red de acceso (WISP) por ejemplo. El código de acceso incluye una diversidad de información sobre parámetros de uso y reglas comerciales que pueden ser usados por el AP para controlar el acceso por el usuario. Códigos de acceso pueden ser generados por la función de control de acceso en el AP, o por un servidor de control remoto en conexión con el AP, y comunicados al operador de red de acceso (WISP). De acuerdo con esta publicación, la generación de códigos de acceso está basada en reglas comerciales y parámetros de uso específicos del operador de red de acceso para el que los códigos de acceso son generados.

En esta publicación internacional, el servidor de control está dispuesto para comunicar con un número de AP's y para dirigir a un nuevo operador de red de acceso (WISP) a través del proceso de establecer una cuenta nueva. La cuenta es establecida de modo que el servidor de control puede monitorizar y seguir las actividades relacionadas con el AP correspondiente. Es decir, las cuentas y el control de actividades son llevados a cabo sobre una base por AP. En toda esta publicación no hay mención, ni incluso sugerencia, sobre posibles efectos o interferencias derivados de sesiones de acceso simultáneamente activas para un usuario a través de AP's diferentes y, aún menos, cuando mas de un operador de red de acceso (WISP) está implicado. Además, esta publicación ni considera ni sugiere que la autenticación de usuarios sea llevada a cabo por un operador de red de origen que mantiene un abono para los usuarios e implicado como una entidad intermedia de cargo.

Sin embargo, la existencia simultánea de varias sesiones de acceso para un usuario a través de AP's diferentes, y las razones por las que las varias sesiones de acceso fueron iniciadas, conduce a considerar situaciones diferentes en las que algunas de ellas son perfectamente permisibles desde la perspectiva de operadores de redes de origen mientras que otras podrían ser indicativas de actividades fraudulentas. Realmente, cada AP que inicia una sesión de acceso para

un usuario podría enviar información sobre esta sesión de acceso a la red de origen pero la red de origen no puede distinguir si varias sesiones de acceso para un usuario se derivan de un flujo permisible de acciones llevadas a cabo por el usuario. En este aspecto, sesiones de acceso y flujo de acciones diferentes pueden resultar de reautenticación, preautenticación, transferencia o accesos simultáneos simplemente.

Hablando generalmente, fraude ocurre cuando usuarios no autorizados están usando las credenciales de un usuario legítimo. Esto puede ocurrir porque tales credenciales han sido robadas o porque el usuario legítimo comete fraude hacia el operador de red de origen compartiendo las credenciales con otros usuarios.

Un primer ejemplo ilustrativo trata de usuarios de prepago que utilizan una autenticación de nombre de usuario - contraseña y tienen un cargo de tarifa plana. En este caso, una situación de fraude ocurre si varios usuarios utilizan los mismos nombres de usuario y contraseña para acceder a la red. Por ejemplo, como muestra la Figura 3, un primer usuario (UE-1) realiza un procedimiento de autenticación (S-09, S-10, S-11) con un primer punto de acceso WLAN (AP-1) y obtiene un acceso concedido y conectividad WLAN (S-01) a través del primer punto de acceso WLAN (AP-1). Entonces, el primer usuario (UE-1) proporciona su identidad y contraseña de usuario a un segundo usuario (UE-2) o el segundo usuario (UE-2) simula la identidad y la contraseña de usuario del primer usuario (UE-1), ambos modos pueden ser considerados un fraude. Este segundo usuario (UE-2) accede a la red desde un terminal diferente y se pone en contacto con un punto diferente de acceso WLAN (AP-2). Desde el punto de vista de la red, ambos usuarios primero y segundo (UE-1, UE-2) son el mismo usuario. El acceso es concedido para ambos casos.

Un segundo ejemplo ilustrativo trata de usuarios que utilizan un módulo de identidad de abonado (SIM: Subscriber Identity Module) para tener una autenticación basada en tarjeta SIM. Fraude puede ocurrir si hay una clonación de tarjeta SIM o si varios abonados utilizan la misma tarjeta SIM conectando la tarjeta SIM por medio de una protección (llave), y siendo movida la protección entre terminales de usuarios.

No obstante, la situación presentada anteriormente no es siempre una situación de fraude. Un operador podría estar interesado en permitir que ciertos abonados mantengan más de una sesión de una manera controlada, por ejemplo, abonados preferentes podrían ser autorizados a acceder a la red desde terminales diferentes, de modo que distinguir situaciones de fraude de otras situaciones aceptables es una cuestión importante para los operadores y, por tanto, es estudiada por la presente invención.

Las técnicas actualmente existentes entre una red de acceso, tal como una red de área local inalámbrica (WLAN), y una red de origen, tal como una red móvil, no permiten la detección de estas situaciones de fraude puesto que un servidor de contabilidad es la entidad que recibe información de contabilidad en la red de origen y, por tanto, que recibe información sobre la sesiones de acceso para un usuario, y el servidor de contabilidad no tiene medios para distinguir si varias sesiones de acceso para un usuario se derivan o no de un flujo permisible de acciones llevadas a cabo por el usuario. Por ejemplo, un operador de red de origen no puede suponer que la recepción de una indicación nueva de comienzo de contabilidad implica una nueva sesión de acceso para un usuario puesto que puede ser debida más bien a un procedimiento de transferencia entre dos AP's diferentes.

Por otra parte, la solución centralizada ofrecida por el servidor de control en la publicación internacional anterior está dirigida más bien a facilitar un control de acceso local sobre una base por AP, y según las premisas de cada operador de WLAN. Esta solución de técnica anterior no enseña ningún mecanismo mediante el cual las situaciones de fraude anteriores puedan ser distinguidas de situaciones permisibles desde una perspectiva de operador de red de origen.

El documento "Escenario de transferencia de WLAN", 3GPP TSG SA WG3 Security S3#33, S3-040352, Beijing, China, Mayo de 2004, (http://www.3gpp.org/fpt/tsg_sa/WG3_Security/TSGS3_33_Beijing/Docs/PDF/S3-040352.pdf) describe mecanismos para controlar el número máximo de sesiones simultáneas que puede establecer un usuario de WLAN. La red 3GPP (3d Generation Partnership Project) decide si un usuario es autorizado a establecer una sesión nueva con un punto de acceso basada en la solicitud de autenticación recibida y en las otras sesiones que el usuario ya ha establecido.

Un objeto de la presente invención es la provisión de un mecanismo para permitir la detección de posibles situaciones de fraude cuando varias sesiones de acceso son simultáneamente activas para un usuario a través de puntos de acceso (AP's) diferentes.

Además, el concepto de códigos de acceso descritos en la publicación internacional anterior, que incluye generación y manejo, no es una cuestión estándar soportada por AP's actualmente existentes que siguen la norma 802.1x del IEEE en el segundo escenario anterior. Cualquier desarrollo adicional respecto a la enseñanza en la publicación internacional anterior para incluir un mecanismo de detección de fraude cuando varias sesiones de acceso son activas para un usuario implicaría la modificación de AP's actualmente existentes.

De tal modo, un objeto adicional que pretende la presente invención es que el mecanismo para permitir la detección de posibles situaciones de fraude no produzca ningún efecto sobre los puntos de acceso existentes que funcionan de acuerdo con el segundo escenario anterior.

Sumario de la invención

Los objetos anteriores son conseguidos de acuerdo con la presente invención por la provisión de un aparato de acuerdo con la reivindicación 1, denominado dispositivo de agregación de sesiones en la memoria descriptiva presente, y un método de acuerdo con la reivindicación 13.

El dispositivo de agregación de sesiones es adecuado para controlar una pluralidad de sesiones de acceso establecidas por un usuario que accede a una red de área local inalámbrica (WLAN) a través de un número de puntos de acceso, en la que el usuario es abonado de una primera red de operador y los puntos de acceso pertenecen a segundas redes de operador, la primera red de operador y las segundas redes de operador. En particular, pueden ser dirigidas por un mismo operador o por operadores diferentes. Los puntos de acceso llevan a cabo procedimientos de control de acceso mediante los que el usuario es autenticado por la primera red de operador. Un dispositivo de agregación de sesiones de acuerdo con la invención tiene:

a) medios para recibir información de sucesos de autenticación para el usuario que accede a un punto de acceso dado con un equipo de usuario dado; y

b) medios para recibir información de sucesos de contabilidad que incluye información relacionada con una sesión de acceso establecida para el usuario en el punto de acceso dado con el equipo de usuario dado;

c) medios de autorización dispuestos para tomar una decisión sobre si el usuario es autorizado a acceder al punto de acceso dado cuando reciben información de sucesos de autenticación, y basados en otras sesiones de acceso que el usuario ha establecido; y

d) medios de procesamiento dispuestos para determinar si el curso actual de acciones corresponde a un flujo permisible, o a un posible flujo fraudulento, cuando reciben información de sucesos de contabilidad para el usuario que tiene una sesión de acceso en el punto de acceso dado con el equipo de usuario dado.

En una realización de la invención, estos medios de autorización incluyen medios para crear un registro de autenticación de acceso (AAR) para el usuario, una vez que una indicación de un suceso de autenticación es recibida indicando que el usuario ha sido autenticado a través de un punto de acceso dado. El registro de autenticación de acceso (AAR) comprende: un identificador de usuario que identifica al usuario diseccionado en la indicación, un identificador del equipo de usuario recibido en la indicación y un identificador del punto de acceso que aplicó tal autenticación.

En funcionamiento, un primer registro de autenticación de acceso es creado en el dispositivo de agregación de sesiones cuando el usuario es autenticado a través de un primer punto de acceso donde el usuario accede con su equipo de usuario, y un segundo registro de autenticación de acceso es creado cuando el usuario es preautenticado a través de un segundo punto de acceso. Además, como un usuario puede ser autorizado a acceder a través de más de un punto de acceso con más de un equipo de usuario, el dispositivo de agregación de sesiones también está dispuesto de tal manera que un primer registro de autenticación de acceso es creado cuando el usuario es autenticado a través de un primer punto de acceso con un primer equipo de usuario, y un segundo registro de autenticación de acceso es creado cuando el usuario es autenticado a través de un segundo punto de acceso con un segundo equipo de usuario, puesto que el usuario es autorizado a tener más de una sesión de acceso simultáneamente activas.

El dispositivo de agregación de sesiones puede ser mejorado cuando el registro de autenticación de acceso también comprende una indicación sobre el tipo de autenticación realizada para el usuario, y una medición de tiempo indicativa del momento cuando el registro de autenticación de acceso fue creado. La medición de tiempo puede ser consultada para determinar si un flujo actual de acciones es considerado una actividad permisible o una actividad fraudulenta.

Por otra parte, los medios de procesamiento en el dispositivo de agregación de sesiones, provistos de acuerdo con la invención, incluyen medios para crear un registro de sesión agregada (ASR) para el usuario una vez que el usuario ha establecido una sesión de acceso a través de un punto de acceso dado. Este registro de sesión agregada comprende: un identificador de usuario que identifica al usuario direccionado en la indicación, un identificador del equipo de usuario recibido en la indicación, un identificador del punto de acceso donde la sesión ha sido establecida y una lista de registros de autenticación de acceso asociados con este registro de sesión agregada.

En funcionamiento, un registro de sesión agregada en el dispositivo de agregación de sesiones es actualizado durante un procedimiento de transferencia para sustituir un primer identificador de un primer punto de acceso, donde el usuario ha accedido con el equipo de usuario, por un segundo identificador de un segundo punto de acceso donde el usuario ha establecido una sesión de acceso después de tener una preautenticación satisfactoria. En cuanto al registro de autenticación de acceso y dado que un usuario puede ser autorizado a acceder a través de puntos de acceso diferentes con equipos de usuario diferentes, el dispositivo de agregación de sesiones está dispuesto de modo que un primer registro de sesión agregada es creado cuando el usuario ha establecido una primera sesión de acceso a través de un primer punto de acceso con un primer equipo de usuario, y un segundo registro de sesión agregada es creado cuando el usuario ha establecido una segunda sesión de acceso a través de un segundo punto de acceso con un segundo equipo de usuario, puesto que el usuario es autorizado a tener más de una sesión de acceso simultáneamente activas.

El dispositivo de agregación de sesiones recibe indicaciones de sucesos de contabilidad tal como una indicación de parada de contabilidad. Así, cuando recibe una indicación de parada de contabilidad, es eliminado el registro de sesión agregada correspondiente a la sesión de acceso que el usuario había establecido con el equipo de usuario a través del punto de acceso.

El dispositivo de agregación de sesiones (SAD: Session Aggregator device) también puede ser mejorado cuando el registro de sesión agregada también comprende una medición de tiempo indicativa del momento cuando el registro de sesión agregada fue creado.

Además, el dispositivo de agregación de sesiones (SAD) también puede comprender un módulo de transformación global para correlacionar una identidad de autenticación y una identidad de contabilidad, siendo la identidad de autenticación recibida como el identificador de usuario que identifica al usuario en cada indicación de suceso de autenticación, y siendo la identidad de contabilidad recibida como el identificador de usuario que identifica al usuario en cada indicación de suceso de contabilidad.

La presente invención también provee un método para controlar una pluralidad de sesiones de acceso establecidas por un usuario que accede a una red de área local inalámbrica (WLAN) a través de un número de puntos de acceso, en el que el usuario es abonado de una primera red de operador y los puntos de acceso, que son dirigidos por segundas redes de operador, llevan a cabo procedimientos de control de acceso. El método de acuerdo con la invención comprende los pasos de:

(a) aplicar una autenticación de usuario en un punto de acceso donde el usuario ha establecido una conexión de capa 2 con un equipo de usuario;

(b) llevar a cabo una autenticación de usuario entre el equipo de usuario y un servidor de autenticación en la primera red de operador;

(c) establecer una sesión de acceso que concede acceso al usuario a través del punto de acceso en la autenticación satisfactoria de usuario;

(d) indicar un suceso de contabilidad hacia un servidor de contabilidad en la primera red de operador cuando el usuario consigue conectividad en la sesión de acceso;

(e) tomar una decisión de autorización basada en sesiones de acceso anteriores ya establecidas para el usuario con el equipo de usuario dado en la indicación de un suceso de autenticación recibida en una entidad centralizada; y

(f) determinar si un curso actual de acciones corresponde a un flujo permisible, o a un posible flujo fraudulento, para el usuario que tiene la sesión de acceso en el punto de acceso dado con el equipo de usuario dado, en la indicación del suceso de contabilidad recibido en una entidad centralizada.

De acuerdo con una realización preferida actualmente, el paso e) de tomar una decisión de autorización en este método incluye preferiblemente los pasos de:

- comprobar si el usuario con un identificador de usuario dado es nuevo desde un punto de vista de decisión de suceso;
- comprobar para un usuario no nuevo si es nuevo un identificador dado del equipo de usuario; y
- comprobar para un usuario no nuevo con un identificador nuevo de equipo de usuario si varias sesiones de acceso son autorizadas a ser simultáneamente activas para el usuario.

Siguiendo este método, esos pasos de comprobación resultantes al determinar un usuario no nuevo con un identificador nuevo de equipo de usuario, y varias sesiones de acceso no autorizadas a ser simultáneamente activas para el usuario, conducen a detectar una posible actividad fraudulenta. Sin embargo, cuando los pasos de comprobación anteriores producen un usuario no nuevo con un identificador no nuevo del equipo de usuario, el método comprende además un paso de comprobar si es nuevo un identificador dado del punto de acceso, lo que es entendido como una autenticación o preautenticación para el usuario y, por tanto, una actividad permisible.

Alineado con una realización correspondiente para el aparato anterior, y en favor de la coherencia y la unidad, el método también comprende un paso de crear un primer registro de autenticación de acceso (AAR) para el usuario una vez que una decisión de autorización positiva ha sido tomada para que el usuario acceda a través de un primer punto de acceso con un equipo de usuario. Además, el método comprende además un paso de crear un segundo registro de autenticación de acceso para el usuario cuando el usuario es autenticado o preautenticado a través de un segundo punto de acceso. Comprendiendo estos registros de autenticación de acceso: un identificador de usuario que identifica al usuario diseccionado en la indicación de un suceso de autenticación, un identificador del equipo de usuario recibido en dicha indicación y un identificador del punto de acceso que aplicó la autenticación.

De acuerdo con una realización preferida actualmente, el paso f) de determinar el curso actual de acciones en este método incluye los pasos de:

- comprobar si una autenticación satisfactoria tuvo lugar para el usuario con un identificador de usuario dado, con un identificador dado de equipo de usuario, y a través de un punto de acceso identificado por un identificador dado, y

- comprobar si ya ha sido indicada cualquier sesión de acceso anterior para esta autenticación satisfactoria.

Siguiendo este método, esos pasos de comprobación resultantes al determinar que no ha tenido lugar ninguna autenticación satisfactoria para el usuario con un identificador de usuario dado, con un identificador dado del equipo de usuario, y a través de un punto de acceso dado identificado por un identificador dado, conducen a detectar una posible actividad fraudulenta. Sin embargo, cuando los pasos de comprobación anteriores resultan el determinar que una autenticación satisfactoria ya ha tenido lugar para el usuario y que una sesión de acceso anterior para esta autenticación satisfactoria ya había sido indicada, el método determina que hay un procedimiento de transferencia en curso.

De acuerdo con una realización preferida actualmente, el método incluye además un paso de crear un registro de sesión agregada (ASR) para el usuario, cuando se determina que una autorización positiva ya ha sido efectuada para que el usuario acceda al punto de acceso dado, y ninguna sesión de acceso había sido indicada todavía, distinta que la actual, para esta autorización positiva. Este registro de sesión agregada comprende: un identificador de usuario que identifica al usuario diseccionado en la indicación de un suceso de contabilidad, un identificador del equipo de usuario recibido en dicha indicación, un identificador del punto de acceso donde la sesión ha sido establecida y una lista de registros de autenticación de acceso asociados con este registro de sesión agregada particular.

La introducción de registros de sesión agregada proporciona ventajas adicionales al método. Así, el método comprende además un paso de actualizar un registro de sesión agregada cuando se detecta una transferencia entre un primer punto de acceso y un segundo punto de acceso, siendo la actualización llevada a cabo sustituyendo un identificador del primer punto de acceso por un identificador del segundo punto de acceso, y eliminando de la lista el registro de autenticación de acceso (AAR) correspondiente al primer punto de acceso.

El método comprende además un paso de desconectar a un usuario de un punto de acceso dado, siendo la desconexión indicada con un suceso de contabilidad (S-17) hacia la entidad centralizada. En una realización que usa registros de autenticación de acceso y registros de sesión agregada, este paso incluye además los pasos de: eliminar el registro de autenticación de acceso correspondiente, actualizar el registro de sesión agregada asociado para eliminar de la lista el registro de autenticación de acceso y eliminar el registro de sesión agregada cuando la lista está vacía.

Descripción breve de los dibujos

Las características, objetos y ventajas de la invención resultarán evidentes leyendo esta descripción en conjunción con los dibujos adjuntos, en los que:

La Figura 1 muestra una infraestructura de WLAN de técnica anterior en un primer escenario, un denominado acceso WLAN basado en Web.

La Figura 2 muestra una infraestructura de WLAN de técnica anterior en un segundo escenario que sigue la norma 802.1x del IEEE.

La Figura 3 ilustra una secuencia de flujo que describe un problema actualmente existente que no puede ser resuelto con las técnicas existentes.

Las Figuras 4 y 5 muestran dos arquitecturas alternativas provistas en la presente invención.

Las Figuras 6a y 6b presentan un organigrama básico de una máquina de flujo de sucesos proporcionada para tomar decisiones de autorización y para determinar si el curso actual de acciones corresponde a una actividad permisible o una actividad fraudulenta.

La Figura 7a ilustra un diagrama de secuencia básica de una primera vista parcial de un primer curso de acciones donde un usuario es autenticado y autorizado a acceder a un primer punto de acceso, y accediendo el usuario al primer punto de acceso.

La Figura 7b1 ilustra un diagrama de secuencia básica de una segunda vista parcial que sigue a la Figura 7a en el primer curso de acciones donde el usuario es preautenticado y autorizado a acceder a un segundo punto de acceso.

La Figura 7c1 ilustra un diagrama de secuencia básica de una tercera vista parcial que sigue a las Figuras 7a y 7b1 en el primer curso de acciones donde el usuario lleva a cabo una transferencia entre los puntos de acceso primero y segundo.

La Figura 7c2 ilustra un diagrama de secuencia básica de una tercera vista parcial que sigue a las Figuras 7a y7b1 en un segundo curso de acciones mediante lo cual un segundo usuario simula credenciales del primer usuario para acceder al segundo punto de acceso donde el primer usuario había sido preautenticado.

La Figura 7b2 ilustra un diagrama de secuencia básica de una segunda vista parcial que sigue a la Figura 7a en un tercer curso de acciones donde el usuario es desconectado de un acceso conseguido a través del primer punto de acceso.

La Figura 7b3 ilustra un diagrama de secuencia básica de una segunda vista parcial que sigue a la Figura 7a en un cuarto curso de acciones donde el usuario con un segundo equipo de usuario es autenticado a través de un segundo punto de acceso y, siempre que el usuario sea autorizado a tener varias sesiones de acceso simultáneamente, el usuario puede acceder al segundo punto de acceso.

Descripción detallada de realizaciones preferidas

Lo siguiente describe algunas realizaciones preferidas para llevar a cabo una detección eficaz de posibles situaciones de fraude cuando varias sesiones de acceso son simultáneamente activas para un usuario a través de puntos de acceso diferentes, y para distinguir estas posibles situaciones de fraude de otras situaciones permisibles, presentando ambas características aparentemente similares aunque derivadas de flujos diferentes de acciones.

Por tanto, la presente invención provee un número de pasos que son llevados a cabo para conocer las acciones ocurridas. Por una parte, los mensajes de contabilidad recibidos en el servidor de contabilidad (Acc-S) son usados para indicar si una sesión de acceso es creada (comienzo de contabilidad) o todavía está viva (intermedio de contabilidad) o ha sido finalizada (parada de contabilidad) y los datos correspondientes suprimidos así.

Por otra parte, el manejo de mensajes de contabilidad no es suficiente para tomar decisiones de autorización basadas en el número de sesiones de acceso ya existentes para un usuario. Estas decisiones de autorización son tomadas durante el propio proceso de autenticación o inmediatamente después, de modo que una vez que el usuario ha sido autenticado en un servidor de autenticación (Auth-S) de la red de origen (HOME), una comprobación de control puede ser llevada a cabo para determinar si una nueva sesión de acceso es permitida o no, dependiendo de la existencia de otras sesiones de acceso para dicho usuario, y antes de enviar una respuesta satisfactoria a una entidad de la red de acceso (WLAN) a través de donde el usuario está accediendo. Es decir, aunque la autenticación sea satisfactoria, la respuesta a una solicitud de acceso recibida desde la red de acceso (WLAN) podría ser negativa, especialmente si una posible situación de fraude ha sido determinada durante la comprobación de control.

La comprobación de control exige medios para recoger información de sucesos relacionados con ambos procedimientos, o sea procedimientos de autenticación y contabilidad, y el uso de un dispositivo centralizado para recibir mensajes que se dirigen inicialmente a ambas entidades correspondientes, servidor de autenticación (Auth-S) y servidor de contabilidad (Acc-S) respectivamente. Este dispositivo centralizado, que es denominado dispositivo de agregación de sesiones (SAD: Session Aggregator device) en la presente memoria descriptiva, tiene los medios para recoger información de sucesos de autenticación y contabilidad y, por tanto, está encargado de gestionar tal comprobación de control.

Actualmente, los protocolos “RADIUS (Remote Authentication Dial-In User Service)” y “Diameter” son los usados más corrientemente para comunicar un servidor de acceso a red (NAS: Network Access Server), que en particular podría ser un punto de acceso WLAN (AP), con el servidor de autenticación (Auth-S) y el servidor de contabilidad (Acc-S).

De acuerdo con una primera realización de la invención ilustrada en la Figura 4, esta comunicación podría ser conseguida teniendo el dispositivo de agregación de sesiones (SAD) interpuesto entre el punto de acceso WLAN (AP) y tanto el servidor de autenticación (Auth-S) como el servidor de contabilidad (Acc-S) y, por tanto, actuando como proxy RADIUS o como un proxy Diameter para ambos mensajes de autenticación y contabilidad. De acuerdo con una segunda realización alternativa ilustrada en la Figura 5, el servidor de autenticación (Auth-S) y el servidor de contabilidad (Acc-S), ambos en comunicación con el punto de acceso WLAN (AP), envían los mensajes pertinentes de autenticación y contabilidad al dispositivo de agregación de sesiones (SAD).

Entonces, el dispositivo de agregación de sesiones (SAD) puede analizar la información de sesiones recibida en mensajes de contabilidad, tal como un identificador de usuario y un identificador del terminal de usuario, para determinar si sesiones de acceso diferentes corresponden a la misma sesión de usuario o a sesiones de usuario diferentes. En este aspecto y para el fin de la presente invención, una sesión de usuario es una progresión de sucesos relacionados con el uso de una o más aplicaciones a través de una red de acceso dada (WLAN) con independencia del punto de entrada a dicha red de acceso o, en otras palabras, una sesión de usuario puede comprender una pluralidad de sesiones de acceso que un usuario ha establecido a través de un número de puntos de acceso (AP’s) de una red de acceso dada.

Además, el dispositivo de agregación de sesiones (SAD) puede manejar información de sesiones sobre varias sesiones de usuario que un usuario podría tener en redes de acceso diferentes, tales como un número de redes de acceso WLAN y una red Global System for Mobile Communications Packet Radio System (GPRS), comprendiendo cada sesión de usuario una pluralidad de sesiones de acceso que el usuario ha establecido a través de un número de

servidores de acceso a red (NAS), que en particular podrían ser puntos de acceso (AP's), de una red de acceso dada. Esta información de sesiones, una vez procesada, puede ser enviada a un sistema de gestión de fraudes que, a su vez, puede emprender acciones tales como activar alarmas o suprimir sesiones sospechosas.

El dispositivo de agregación de sesiones (SAD) es responsable del proceso de tomar decisiones de autorización, actuando como una entidad de entrada (frontal) interpuesta entre un servidor de acceso a red (AP) y el servidor de autenticación (Auth-S)(A1, A3) y el servidor de contabilidad (Acc-S) (A2, A4) de acuerdo con la primera realización ilustrada en la Figura 4, o como una entidad de salida (posterior) donde mensajes de autenticación y contabilidad son enviados (A5, A6) desde el servidor de autenticación (Auth-S) y el servidor de contabilidad (Acc-S) de acuerdo con la segunda realización ilustrada en la Figura 5.

Un proceso básico de tomar decisiones de autorización y efectuar comprobaciones de control es descrito adicionalmente con respecto a la segunda realización anterior mostrada en la Figura 5, y una red WLAN siendo la red de acceso. Por tanto, el dispositivo de agregación de sesiones (SAD) está provisto de una máquina de flujo de sucesos ilustrada por combinación de las Figuras 6a y 6b. Esta máquina de flujo de sucesos puede funcionar cuando recibe una indicación que muestra una autenticación satisfactoria de un usuario, y una indicación que muestra si la contabilidad empieza, continúa o termina para un usuario con una sesión de acceso dada.

Aunque protocolos diferentes pueden ser adecuados para uso como protocolos respectivos entre el dispositivo de agregación de sesiones (SAD) y el servidor de autenticación (Auth-S) y el servidor de contabilidad (Acc-S), en favor de la sencillez, el proceso de tomar decisiones de autorización y efectuar comprobaciones de control es explicado con referencia a un protocolo RADIUS. En este aspecto, varios flujos pueden aparecer dependiendo de actividades diferentes que los usuarios podrían llevar a cabo. Algunos de estos flujos posibles son descritos de una manera ilustrativa y no restrictiva con referencia a una primera combinación de las Figuras 7a, 7b1 y 7c1, con referencia a una segunda combinación de las Figuras 7a, 7b1 y 7c2, con referencia a una tercera combinación de las Figuras 7a y 7b2 y con referencia a una cuarta combinación de las Figuras 7a y 7b3.

Un primer flujo de acciones empieza como se ilustra en la Figura 7a cuando un usuario (UE-1), que es un abonado de una red de origen (HOME), ha accedido inicialmente (S-09) a un punto de acceso WLAN (AP-1). El punto de acceso WLAN (AP-1) aplica (S-10) la autenticación de usuario reorientando al usuario a un servidor de autenticación (Auth-S) en la red de operador de origen (HOME). El servidor de autenticación (Auth-S) utiliza un procedimiento de autenticación adecuado, como indicado probablemente en el perfil de usuario, para autenticar al usuario (S-11). De acuerdo con la invención, y siempre que el procedimiento de autenticación sea satisfactorio, el dispositivo de agregación de sesiones es informado (S-13). El dispositivo de agregación de sesiones (SAD) procesa la información con una máquina de flujo de sucesos (flujo de sucesos) para decidir si el usuario es autorizado a obtener acceso teniendo en cuenta otras sesiones de acceso que el usuario podría haber establecido ya.

En este caso particular, la hipótesis es que el usuario es un usuario nuevo que intenta un primer acceso, y la máquina de flujo de sucesos que recibe una indicación de autenticación satisfactoria de usuario, el tratamiento de suceso de autenticación (S-13) mostrado en las Figuras 6a y 7a, dispara la creación de un registro de autenticación de acceso (AAR: Access Authentication Record) para el usuario en el dispositivo de agregación de sesiones (SAD), lo que es un resultado positivo en este caso. El punto de acceso (AP-1) es informado (S-14, S-12) sobre el resultado de esta decisión, preferiblemente a través del servidor de autenticación (Auth-S) según esta segunda realización, aunque podría ser informado directamente desde el dispositivo de agregación de sesiones (SAD) si una interfaz adecuada es provista con este fin, como A1 en la Figura 4, y datos de direccionamiento correspondientes son recibidos por vía del servidor de autenticación (Auth-S), como A3 en la Figura 4. Siempre que tanto el procedimiento de autenticación como la decisión de autorización tengan un resultado positivo, el acceso es concedido en el punto de acceso (AP-1).

Más específicamente, un registro de autenticación de acceso (AAR) es creado para un usuario una vez que el usuario es autenticado a través de un punto de acceso (AP-1) particular, y con independencia de ser debido a una autenticación o a una preautenticación. El registro de autenticación de acceso (AAR) demuestra que una autenticación satisfactoria ha ocurrido para el usuario y, al mismo tiempo, conserva información sobre sucesos de procedimiento asociados con el procedimiento de autenticación tal como, por ejemplo, un identificador del terminal de usuario, un identificador de usuario con fines de autenticación, un identificador del punto de acceso (AP-1) que solicita el acceso, momento de la autenticación y tipo de autenticación. Como varias sesiones de acceso pueden ser establecidas por un usuario a través de puntos de acceso diferentes, y dado que cada punto de acceso solicita una autenticación del usuario desde la red de operador de origen donde el usuario es un abonado, puede haber varios registros de autenticación de acceso (AAR's) por abonado.

En esta etapa, el usuario (UE-1) obtiene conectividad WLAN (S-01) a través del punto de acceso (AP-1) en el que una sesión de acceso es creada para el usuario, y comunicada hacia un servidor de contabilidad (Acc-S) con una indicación de comienzo de contabilidad (S-07). El dispositivo de agregación de sesiones (SAD) también es informado (S-15) sobre el suceso de contabilidad y procesa la información recibida con la máquina de flujo de sucesos (flujo de sucesos) para determinar si el curso actual de acciones corresponde o no a un flujo permisible. En el caso actual, como presenta la Figura 6a, un registro de autenticación de acceso (AAR) existente es hallado para el usuario que indica que el usuario ya había sido autenticado y, como ninguna sesión de acceso anterior había sido establecida aparte de la indicada actualmente con la indicación de comienzo de contabilidad, un registro de sesión agregada (ASR: Aggregated

Session Record) es creado para demostrar que una primera sesión de acceso es establecida por el usuario a través del punto de acceso (AP-1) dado.

Este primer flujo de acciones puede avanzar con un paso adicional ilustrado en la Figura 7b1, en el que un procedimiento de preautenticación es llevado a cabo a través de un segundo punto de acceso (AP-2). La elección del segundo punto de acceso (AP-2) podría ser debida a razones diferente tales como el área de cobertura o la calidad de recepción, por ejemplo.

Por tanto, el equipo de usuario (UE-1) inicia un denominado intento de preautenticación (S-22) para el segundo punto de acceso (AP-2), y el último aplica (S-10) la autenticación de usuario que el usuario lleva a cabo (S-11) con un servidor de autenticación (Auth-S) de la red de operador de origen. De acuerdo con la invención, el dispositivo de agregación de sesiones (SAD) es informado (S-13) sobre ello y procesa la información con la máquina de flujo de sucesos (flujo de sucesos) como se efectúa para una autenticación normal. En este caso, y siguiendo el organigrama de la Figura 6a, la máquina de flujo de sucesos comprueba los registros de autenticación de acceso (AAR's) existentes y halla que el usuario no es nuevo; la identidad de equipo de usuario, por ejemplo una dirección MAC (Media Access Control), no es nueva; y el punto de acceso (AP-2) por donde el usuario accede es diferente que el almacenado en el registro de autenticación de acceso (AAR) anterior para el usuario. La máquina de flujo de sucesos en el dispositivo de agregación de sesiones (SAD) decide con esta información la creación de un segundo registro de autenticación de acceso (AAR) y devuelve (S-14, S-12) un resultado positivo hacia el segundo punto de acceso (AP-2) donde el usuario ha sido preautenticado, preferiblemente a través del servidor de autenticación (Auth-S). Ahora, el segundo punto de acceso (AP-2) marca el acceso concedido para el usuario aunque el usuario no haya conseguido todavía la conectividad WLAN.

En esta etapa, acciones diferentes podrían ocurrir a continuación del procedimiento de preautenticación anterior, acciones diferentes que la presente invención puede distinguir gracias al dispositivo de agregación de sesiones (SAD) y los medios incluidos en él.

Una primera acción ejemplar mostrada en la Figura 7c1 completa el primer flujo de acciones comentado anteriormente cuando se sigue la secuencia en las Figuras 7a, 7b1 y 7c1, e ilustra un procedimiento de transferencia que puede ser llevado a cabo después de haber completado el procedimiento de preautenticación. La transferencia empieza por el equipo de usuario (UE-1) consiguiendo conectividad WLAN (S-01) con el segundo punto de acceso (AP-2) donde el acceso ya ha sido concedido. El segundo punto de acceso (AP-2), cuando detecta conectividad de usuario, crea una sesión de acceso para el usuario e informa sobre ello con una indicación de comienzo de contabilidad (S-07) hacia el servidor de contabilidad (Acc-S). De acuerdo con la invención, el dispositivo de agregación de sesiones (SAD) también es informado (S-15) sobre el suceso, y procesa la información recibida con la máquina de flujo de sucesos (flujo de sucesos). El dispositivo de agregación de sesiones (SAD) detecta para ese usuario un primer registro de autenticación de acceso (AAR) creado cuando el usuario fue autenticado en primer lugar a través del primer punto de acceso (AP-1), un primer registro de sesión agregada (ASR) creado cuando el usuario había establecido una primera sesión de acceso con el primer punto de acceso (AP-1), y un segundo registro de autenticación de acceso (AAR) creado cuando el usuario fue preautenticado a través del segundo punto de acceso (AP-2) antes de la transferencia actual.

En este caso y siguiendo el organigrama de la Figura 6a, la máquina de flujo de sucesos que trata de una indicación de comienzo de contabilidad encuentra registros de autenticación de acceso (AAR's) para el usuario así como un registro de sesión agregada (ASR) asociado y determina que una transferencia está en curso. Antes o después, como se muestra en la Figura 7c1, el primer punto de acceso (AP-1) detecta que dicho usuario (UE-1) ya no es activo, probablemente con ayuda de un tiempo muerto de inactividad para el usuario, y el primer punto de acceso (AP-1) envía (S-17) una indicación de parada de contabilidad para el usuario hacia el servidor de contabilidad (Acc-S). En cuanto a otros sucesos de autenticación y contabilidad, el dispositivo de agregación de sesiones (SAD) también recibe esta información y la procesa con la porción de la máquina de flujo de sucesos mostrada en la Figura 6b. En este aspecto, la última parada de contabilidad disparada desde el primer punto de acceso (AP-1) y la identificación anterior de transferencia podrían ocurrir más o menos simultáneamente, y la máquina de flujo de sucesos de las Figuras 6a y 6b incluye un temporizador primero (T0) y un temporizador segundo (T1) para distinguir apropiadamente las situaciones fraudulentas de las permisibles.

En el caso presente, como se muestra en la Figura 7c1, la transferencia es determinada en primer lugar y, según el organigrama mostrado en la Figura 6b, el registro de sesión agregada (ASR) es actualizado para sustituir el identificador del primer punto de acceso (AP-1) por el identificador del segundo punto de acceso (AP-2). Entonces, cuando se trata del suceso de parada de contabilidad (S-18), se elimina el primer registro de autenticación de acceso (AAR) asociado con el primer punto de acceso (AP-1). Finalmente, el procedimiento de transferencia en la Figura 7c1 es completado acusando recibo de tal suceso de contabilidad de vuelta al primer punto de acceso (AP-1).

Una segunda acción ejemplar mostrada en la Figura 7c2 completa el segundo flujo de acciones comentado anteriormente cuando se sigue la secuencia en las Figuras 7a, 7b1 y 7c2, e ilustra una actividad fraudulenta que podría ocurrir después de haber completado el procedimiento de preautenticación mostrado en la Figura 7b1. Brevemente, el curso de acciones llevadas a cabo cuando se siguen las secuencias en las Figuras 7a y 7b1, y antes de iniciar la secuencia en la Figura 7c2, puede ser resumido como: un primer usuario (UE-1) ha conseguido conectividad WLAN en un primer punto de acceso (AP-1); un primer registro de autenticación de acceso (AAR) y un primer registro de sesión agregada (ASR) han sido creados en el dispositivo de agregación de sesiones (SAD); una preautenticación del

primer usuario ha sido llevada a cabo a través de un segundo punto de acceso (AP-2) y, como un resultado de esta preautenticación, un segundo registro de autenticación de acceso (AAR) también ha sido creado en el dispositivo de agregación de sesiones (SAD).

En este momento, una actividad fraudulenta pude ser llevada a cabo por un usuario atacante (UE-2) que roba las claves de seguridad del primer usuario (UE-1) y utiliza un terminal propio (UE-2) con un identificador de terminal diferente, o sea, con una dirección MAC (Media Access control) diferente que la usada por el primer usuario (UE-1). Como ilustra la Figura 7c2, el usuario atacante (UE-2) puede conseguir así conectividad WLAN (S-01) con el segundo punto de acceso (AP-2) donde el primer usuario (UE-1) ha sido preautenticado. El segundo punto de acceso (AP-2) crea una sesión de acceso para el usuario e informa sobre ella con una indicación de comienzo de contabilidad (S-07) hacia el servidor de contabilidad (Acc-S). En cuanto a casos anteriores y de acuerdo con la invención, el dispositivo de agregación de sesiones (SAD) también es informado (S-15) sobre el suceso y procesa la información recibida con la máquina de flujo de sucesos (flujos de sucesos) mostrada en la Figura 6a. En realidad, al tratar de un comienzo de contabilidad en la máquina de flujos de sucesos, ningún registro de autenticación de acceso (AAR) es hallado para el usuario con la dirección MAC (Media Access Control) recibida, que corresponde al usuario atacante (UE-2), puesto que los registros de autenticación de acceso (AAR's) primero y segundo existentes en el dispositivo de agregación de sesiones incluyen ambos la dirección MAC del primero usuario (UE-1). Así, un fraude posible es detectado y puede ser comunicado de vuelta (S-16, S-08) al segundo punto de acceso (AP-2), para negar el acceso para el usuario atacante (UE-2), o a un sistema externo de gestión de fraudes según las premisas del operador de origen, que no es mostrado en ningún dibujo.

Una variante de la actividad fraudulenta descrita anteriormente con la segunda acción ejemplar mostrada en la Figura 7c2 es cuando el usuario atacante (UE-2) no solo ha robado o simulado las claves de seguridad del primer usuario (UE-1) sino también el identificador de terminal, una dirección MAC, de dicho primer usuario (UE-1). Según esta hipótesis, el segundo punto de acceso (AP-2) donde el primer usuario (UE-1) fue preautenticado crea una sesión de acceso para el usuario e informa sobre ella con una indicación de comienzo de contabilidad (S-07) hacia el servidor de contabilidad (Acc-S) como se ilustra en la Figura 7c2 y se comentó previamente. Después, el dispositivo de agregación de sesiones (SAD), que recibe (S-15) y procesa tal información con la máquina de flujo de sucesos (flujo de sucesos), encuentra el segundo registro de autenticación de acceso (AAR) creado cuando se preautentica al primer usuario (UE-1), y también encuentra el primer registro de sesión agregada (ASR) creado cuando el primer usuario consiguió conectividad WLAN con el primer punto de acceso (AP-1). Siguiendo el flujo mostrado en la Figura 6a, la máquina de flujo de sucesos (flujo de sucesos) determina que hay una transferencia en curso, como cualquiera puede determinar comparando el curso de acciones para el procedimiento de transferencia también descrito anteriormente. Sin embargo, este caso no es una transferencia y un tiempo muerto (T0) de un temporizador dispuesto cuando se determina la transferencia termina antes de recibir una indicación correspondiente de parada de contabilidad, lo que conduce a que la máquina de flujo de sucesos determine una posible situación de fraude también para este caso.

Una tercera acción ejemplar mostrada en la Figura 7b2 completa el tercer flujo de acciones comentado anteriormente cuando se sigue la secuencia en las Figuras 7a y 7b2, e ilustra los pasos llevados a cabo por entidades diferentes cuando el primer usuario (UE-1), que había sido autenticado y había conseguido conectividad WLAN siguiendo la secuencia en la Figura 7a, inicia una desconexión WLAN (S-20). Como ilustra la Figura 7b2, la desconexión WLAN (S-20) es recibida en el punto de acceso (AP-1) que sirve al usuario (UE-1), y el primer punto de acceso envía (S-17) una indicación de parada de contabilidad al servidor de contabilidad (Acc-S). Esta indicación también es recibida (S-15) en el dispositivo de agregación de sesiones (SAD), procesando este último tal información con la máquina de flujo de sucesos (flujo de sucesos) que encuentra el primer registro de autenticación de acceso (AAR) creado cuando se autentica al primer usuario (UE-1), y también encuentra el primer registro de sesión agregada (ASR) asociado creado cuando el primer usuario consiguió conectividad WLAN con el primer punto de acceso (AP-1). El dispositivo de agregación de sesiones (SAD) que trata de tal parada de contabilidad elimina el primer registro de sesión agregada (ASR) asociado y, como una parte de esta rutina, también elimina los registros de autenticación de acceso (AAR's) asociados que en el caso presente solo es dicho primer registro de autenticación de acceso (AAR). Un comportamiento similar puede se obtenido si el usuario no desconecta explícitamente del primer punto de acceso (AP-1) en el que termina un tiempo muerto de inactividad de usuario, lo que es extendido en el primer punto de acceso (AP-1) como una desconexión implícita que produce el mismo efecto que la desconexión explícita.

Una cuarta acción ejemplar mostrada en la Figura 73b completa el cuarto flujo de acciones comentado anteriormente cuando se sigue la secuencia en las Figuras 7a y 73b, e ilustra el procedimiento seguido para conceder o negar acceso a usuarios con más que el equipo de usuario simultáneamente. Así, una vez que un usuario con un primer equipo de usuario (UE-1) ha sido autenticado y ha conseguido conectividad WLAN con un primer punto de acceso (AP-1) como se muestra en la Figura 7a, hay un primer registro de autenticación de acceso (AAR) y un primer registro de sesión agregada (ASR) creados para el usuario en el dispositivo de agregación de sesiones (SAD). La secuencia en la Figura 7b3 empieza cuando el mismo usuario con un segundo equipo de usuario (UE-1bis) intenta acceder (S-09) a un segundo punto de acceso (AP-2), que puede ser según las premisas del mismo operador (WISP: WLAN Access Provider = proveedor de acceso WLAN) que es el primer punto de acceso (AP-1), o según las premisas de otro operador no mostradas en ningún dibujo. Entonces, el segundo punto de acceso (AP-2) aplica (S-10) la autenticación de usuario (S-11) hacia un servidor de autenticación (Auth-S) en la red de operador de origen que mantiene un abono para el usuario. En la autenticación de usuario satisfactoria, el dispositivo de agregación de sesiones (SAD) procesa la información recibida con la máquina de flujo de sucesos (flujo de sucesos). Cuando se trata del suceso de autenticación según la Figura 6a, la máquina de flujo de sucesos encuentra que el usuario no es nuevo, y el identificador del equipo

de usuario (UE-1bis) es diferente que el usado en el acceso anterior, o sea, la dirección MAC (Media Access Control) recibida es diferente que la anterior. El resultado del proceso en esta etapa depende de si más de una sesión de acceso son autorizadas a ser simultáneamente activas para el usuario, lo que puede ser determinado basado en opciones de abono según la perspectiva del operador de origen. Siempre que el usuario es autorizado a conseguir acceso a través de puntos de acceso diferentes (AP-1, AP-2) con equipos de usuario diferentes (UE-1, UE-1bis), el dispositivo de agregación de sesiones (SAD) crea un segundo registro de autenticación de acceso (AAR) y envía un acuse de recibo satisfactorio de vuelta (S-14, S-12) al segundo punto de acceso (AP-2) en el que el acceso es concedido. En caso contrario, el dispositivo de agregación de sesiones (SAD) supone que el segundo equipo de usuario (UE-1bis) es usado por un usuario atacante que ha robado las claves o credenciales de usuario para intentar acceder a la red, lo que es entendido como un fraude posible, y devuelto con el acuse de recibo (S-14, S-12) hacia el segundo punto de acceso (AP-2) para que este último niegue acceso al usuario. El dispositivo de agregación de sesiones (SAD) también puede informar a un sistema externo de gestión de fraudes para emprender las acciones apropiadas.

En el caso de que el acceso ha sido concedido, el usuario puede conseguir (S-01) conectividad WLAN con el segundo equipo de usuario (UE-1bis) a través del segundo punto de acceso (AP-2), enviando este último (S-07) una indicación de comienzo de contabilidad hacia el servidor de contabilidad (Acc-S) y, como en casos anteriores, el dispositivo de agregación de sesiones (SAD) que recibe (S-15) y procesa tal información con la máquina de flujo de sucesos (flujo de sucesos). El dispositivo de agregación de sesiones (SAD), cuando trata del comienzo de contabilidad, sigue la secuencia de proceso mostrada en la Figura 6a y encuentra un registro de autenticación de acceso (AAR) existente para el usuario, o sea el segundo registro de autenticación de acceso (AAR) creado durante la autenticación con el segundo equipo de usuario (UE-1bis). Dado que ningún registro de sesión agregada (ASR) asociado es hallado para dicho segundo registro de autenticación de acceso (AAR), el dispositivo de agregación de sesiones (SAD) crea un segundo registro de sesión agregada (ASR) para el usuario (UE-1bis) y devuelve (S-16, S-08) esta información con acuse de recibo hacia el segundo punto de acceso (AP-2) donde el usuario ha obtenido conectividad WLAN para el segundo equipo de usuario (UE-1bis).

Considerando los medios que el dispositivo de agregación de sesiones (SAD) tiene para recoger información de sucesos de autenticación y contabilidad para realizar la comprobación de control con la máquina de flujo de sucesos, el dispositivo de agregación de sesiones (SAD) incluye medios para recibir un identificador de usuario que identifica al usuario, un identificador de terminal o equipo de usuario, tal como una dirección MAC (Media Access Control), que identifica el terminal con el que accede el usuario, y con una dirección IP de servidor de acceso a red que identifica el punto de acceso a través del que accede el usuario. Estos identificadores son recibidos preferiblemente como parámetros incluidos en los mensajes que indican tratar de un suceso de autenticación (S-13) y de un suceso de contabilidad (S-15, S-17) recibidos en el dispositivo de agregación de sesiones (SAD) de acuerdo con la invención.

De acuerdo con realizaciones preferidas actualmente, un registro de autenticación de acceso (AAR) creado en el dispositivo de agregación de sesiones (SAD) incluye el identificador de usuario usado durante el procedimiento de autenticación al que corresponde el registro de autenticación de acceso (AAR), el identificador de equipo de usuario usado durante este procedimiento de autenticación, y la dirección IP de punto de acceso que ha aplicado tal autenticación. El registro de autenticación de acceso (AAR) incluye ventajosamente una indicación sobre el tipo de autenticación realizada para el usuario, y una medición de tiempo que indica el momento cuando el registro de autenticación de acceso (AAR) fue creado. Igualmente, un registro de sesión agregada (ASR) creado en el dispositivo de agregación de sesiones (SAD) incluye un identificador de usuario usando cuando se consigue conectividad WLAN y asociado con la sesión de acceso a la que corresponde el registro de sesión agregada (ASR), un identificador de equipo de usuario usado durante esta sesión de acceso, la dirección IP de punto de acceso donde la sesión de acceso ha sido establecida, y una lista que incluye los registros de autenticación de acceso (AAR's) asociados con este registro de sesión agregada (ASR) particular. Ventajosamente, el registro de sesión agregada (ASR) también incluye una medición de tiempo que indica el momento cuando fue creado en el dispositivo de agregación de sesiones (SAD).

Además, dado que el identificador de usuario usado para el procedimiento de autenticación, o sea una identidad de autenticación, podría ser diferente que el usado cuando se consigue conectividad WLAN, o sea una identidad de contabilidad, de acuerdo con una realización de la invención se proporciona un módulo de transformación global en el dispositivo de agregación de sesiones (SAD) para correlacionar identidades de autenticación e identidades de contabilidad para cada usuario, siendo una identidad de autenticación recibida como el identificador de usuario que identifica al usuario en cada indicación de un suceso de autenticación (S-13), mientras que una identidad de contabilidad es recibida como el identificador de usuario que identifica al usuario en cada indicación de un suceso de contabilidad (S-15, S-17).

Alternativamente, siempre que varias identidades de autenticación y varias identidades de contabilidad puedan ser usadas por un usuario, un primer módulo de transformación puede residir en el servidor de autenticación (Auth-S) para transformar dichas varias identidades de autenticación en una identidad de usuario única que identifica al usuario según las premisas del operador de origen, y un segundo módulo de transformación puede residir en el servidor de contabilidad (Acc-S) para transformar dichas varias identidades de contabilidad en la identidad de usuario única que identifica al usuario según las premisas del operador de origen. Dicha identidad de usuario única, que identifica al usuario según las premisas del operador de origen, es usada tanto por el servidor de autenticación (Auth-S) como el servidor de contabilidad (Acc-S) como el identificador de usuario que identifica al usuario en cada indicación respectiva de un suceso de autenticación (S-13) y un suceso de contabilidad (S-15).

En otra realización alternativa más, el módulo de transformación global solo existe en una base de datos centralizada de servidores de abonados según las premisas del operador de origen, en la que las preguntas individuales procedentes del servidor de autenticación (Auth-S) y del servidor de contabilidad (Acc-S) son dirigidas para obtener un identificador de usuario único para identificar al usuario en el dispositivo de agregación de sesiones (SAD).

Ventajas adicionales pueden ser obtenidas teniendo un dispositivo de agregación de sesiones (SAD) centralizado para controlar las actividades de usuario cuando más de una sesión de acceso pueden ser simultáneamente activas para un usuario. Una ventaja importante es el soporte adicional que el dispositivo de agregación de sesiones (SAD) ofrece para servicios de firma única (SSO: Single Sign-On). La firma única (SSO) es un principio emergente mediante el que un usuario que ha sido autenticado una vez cuando accede por primera vez a un primer punto de acceso en una primera red de acceso, puede acceder a un segundo punto de acceso en una segunda red de acceso sin necesitar una nueva autenticación. Por tanto, cuando el usuario accede por primera vez al segundo punto de acceso, este último, en lugar de aplicar la autenticación de usuario, dispara una solicitud de autenticación hacia el servidor de autenticación (Auth-S), siendo esta solicitud de autenticación recibida también en el dispositivo de agregación de sesiones (SAD) y procesada en él con ayuda de la máquina de máquina de flujo de sucesos (flujo de sucesos). Además, el dispositivo de agregación de sesiones (SAD) también puede ser puesto en contacto desde una red de servicios, que ofrece servicios a usuarios que son abonados de la primera red de operador, para verificar si un usuario ha sido autenticado previamente o no.

La invención es descrita anteriormente con respecto a varias realizaciones de una manera ilustrativa y no restrictiva. Evidentemente, variaciones y combinaciones de estas realizaciones son posibles a la luz de las enseñanzas anteriores, y cualquier modificación de las realizaciones que está dentro del alcance de las reivindicaciones está destinada a ser incluida en ellas.

REIVINDICACIONES

1. Un dispositivo de agregación de sesiones (SAD) para controlar una pluralidad de sesiones de acceso establecidas por un usuario que accede a una red de área local inalámbrica (WLAN) a través de un número de puntos de acceso (AP-1, AP-2), siendo el usuario abonado de una primera red de operador (HOME), pertenecientes los puntos de acceso a segundas redes de operador (WISP-1; WISP-2) y llevando a cabo procedimientos de control de acceso mediante los cuales el usuario es autenticado por la primera red de operador (HOME), comprendiendo el dispositivo de agregación de sesiones:

a) medios para recibir indicación de un suceso de autenticación (S-13) para el usuario que accede a un punto de acceso dado (AP-1; AP-2) con un equipo de usuario dado (UE-1, UE-2, UE-1bis); y

b) medios para recibir indicación de un suceso de contabilidad (S-15) que incluye información relacionada con una sesión de acceso establecida para el usuario en el punto de acceso dado con el equipo de usuario dado;

c) medios de autorización dispuestos para tomar una decisión sobre si el usuario es autorizado a acceder al punto de acceso dado cuando recibe información de sucesos de autenticación (S-13), y basada en otras sesiones de acceso que el usuario ha establecido; y

caracterizado por:

d) medios de procesamiento dispuestos para determinar si el curso presente de acciones corresponde a un flujo permisible o a un posible flujo fraudulento cuando se recibe información de sucesos de contabilidad (S-15) para el usuario que tiene una sesión de acceso en el punto de acceso dado con el equipo de usuario dado.

2. El dispositivo de agregación de sesiones (SAD) de la reivindicación 1, en el que los medios de autorización incluyen medios para crear un registro de autenticación de acceso para el usuario una vez que una indicación de un suceso de autenticación (S-13) es recibida indicando que el usuario ha sido autenticado a través de un punto de acceso dado (AP-1, AP-2), comprendiendo el registro de autenticación de acceso:

- un identificador de usuario que identifica al usuario direccionado en la indicación (S-13);
- un identificador del equipo de usuario (UE-1, UE-2, UE-1bis) recibido en la indicación (S-13); y
- un identificador del punto de acceso (AP-1, AP-2) que aplicó la autenticación.

3. El dispositivo de agregación de sesiones (SAD) de la reivindicación 2, en el que un primer registro de autenticación de acceso es creado cuando el usuario es autenticado a través de un primer punto de acceso (AP-1) donde el usuario accede con su equipo de usuario (UE-1), y un segundo registro de autenticación de acceso es creado cuando el usuario es preautenticado a través de un segundo punto de acceso (AP-2) con el equipo de usuario (UE-1).

4. El dispositivo de agregación de sesiones (SAD) de la reivindicación 2, en el que un primer registro de autenticación de acceso es creado cuando el usuario es autenticado a través de un primer punto de acceso (AP-1) donde el usuario accede con un primer equipo de usuario (UE-1), y un segundo registro de autenticación de acceso es creado cuando el usuario es autenticado a través de un segundo punto de acceso (AP-2) donde el usuario accede con un segundo equipo de usuario (UE-1bis), siendo el usuario autorizado a tener más de una sesión de acceso simultáneamente activas.

5. El dispositivo de agregación de sesiones (SAD) de la reivindicación 2, en el que el registro de autenticación de acceso comprende además una indicación sobre el tipo de autenticación realizada para el usuario, y una medición de tiempo indicativa del momento cuando el registro de autenticación de acceso fue creado.

6. El dispositivo de agregación de sesiones (SAD) de la reivindicación 1, en el que los medios de procesamiento incluyen medios para crear un registro de sesión agregada para el usuario, una vez que una indicación de un suceso de contabilidad (S-15) es recibida indicando que el usuario ha establecido una sesión de acceso a través de un punto de acceso dado (AP-1, AP-2), comprendiendo el registro de sesión agregada:

- un identificador de usuario que identifica al usuario direccionado en la indicación (S-15);
- un identificador del equipo de usuario (UE-1, UE-2, UE-1bis) recibido en la indicación (S-15);
- un identificador del punto de acceso (AP-1, AP-2) donde la sesión ha sido establecida; y
- una lista de registros de autenticación de acceso asociados con este registro de sesión agregada particular.

7. El dispositivo de agregación de sesiones (SAD) de la reivindicación 6, en el que el registro de sesión agregada es actualizado durante un procedimiento de transferencia para sustituir un primer identificador de un primer punto de acceso (AP-1), donde el usuario ha accedido con el equipo de usuario (UE-1), por un segundo identificador de un segundo punto de acceso (AP-2) donde el usuario ha establecido una sesión de acceso después de tener una preautenticación satisfactoria.

8. El dispositivo de agregación de sesiones (SAD) de la reivindicación 6, en el que el registro de sesión agregada es eliminado cuando recibe una indicación de parada de contabilidad (S-17) correspondiente a la sesión de acceso que el usuario había establecido con el equipo de usuario (UE-1) a través del punto de acceso (AP-1).

9. El dispositivo de agregación de sesiones (SAD) de la reivindicación 2, en el que un primer registro de sesión agregada es creado cuando el usuario ha establecido una primera sesión de acceso a través de un primer punto de acceso (AP-1) con un primer equipo de usuario (UE-1), y un segundo registro de sesión agregada es creado cuando el usuario ha establecido una segunda sesión de acceso a través de un segundo punto de acceso (AP-2) con un segundo equipo de usuario (UE-1bis), siendo el usuario autorizado a tener más de una sesión de acceso simultáneamente activas.

10. El dispositivo de agregación de sesiones (SAD) de la reivindicación 6, en el que el registro de sesión agregada comprende además una medición de tiempo indicativa del momento cuando el registro de sesión agregada fue creado.

11. El dispositivo de agregación de sesiones (SAD) de la reivindicación 1, que comprende además un módulo de transformación global para correlacionar una identidad de autenticación y una identidad de contabilidad, siendo la identidad de autenticación recibida como el identificador de usuario que identifica al usuario en cada indicación de suceso de autenticación (S-13), y siendo la identidad de contabilidad recibida como el identificador de usuario que identifica al usuario en cada indicación de suceso de contabilidad (S-15, S-17).

12. El dispositivo de agregación de sesiones (SAD) de la reivindicación 1, en el que la primera red de operador y las segundas redes de operador son dirigidas por un mismo operador de red.

13. Un método para controlar una pluralidad de sesiones de acceso establecidas por un usuario que accede a una red de área local inalámbrica (WLAN) a través de un número de puntos de acceso (AP-1, AP-2), siendo el usuario abonado de una primera red de operador (HOME), siendo los puntos de acceso dirigidos por segundas redes de operador (WISP-1, WISP-2) y llevando a cabo procedimientos de control de acceso, comprendiendo el método los pasos de:

a) aplicar (S-10) una autenticación de usuario en un punto de acceso (AP-1, AP-2) donde el usuario ha accedido (S-09, S-22) con un equipo de usuario (UE-1, UE-2, UE-1bis);

b) llevar a cabo (S-11, S-12) una autenticación de usuario entre el equipo de usuario (UE-1, UE-2, UE-1bis) y un servidor de autenticación (Auth-S) en la primera red de operador (HOME);

c) establecer una sesión de acceso (S-01) que concede acceso al usuario a través del punto de acceso (AP-1, AP-2) en la autenticación de usuario satisfactoria (S-12); y

d) indicar un comienzo de contabilidad (S-07) hacia un servidor de contabilidad (Acc-S) en la primera red de operador (HOME) cuando el usuario consigue conectividad (S-01) en la sesión de acceso;

e) tomar una decisión de autorización (S-14, S-12) basada en sesiones de acceso anteriores ya establecidas para el usuario con el equipo de usuario dado (UE-1, UE-2, UE-1bis) en la indicación de un suceso de autenticación (S-13) recibida en una entidad centralizada (SAD);

caracterizado por el paso de:

f) determinar (S-16, S-08) si un curso actual de acciones corresponde a un flujo permisible, o a un posible flujo fraudulento, para el usuario que tiene la sesión de acceso en el punto de acceso dado (AP-1, AP-2) con el equipo de usuario dado (UE-1, UE-2, UE-1bis) en la indicación de un suceso de contabilidad (S-15) recibido en una entidad centralizada (SAD).

14. El método de la reivindicación 13, en el que el paso e) de tomar una decisión de autorización incluye los pasos de:

e1) comprobar si el usuario con un identificador de usuario dado es nuevo desde un punto de vista de decisión de suceso;

e2) comprobar para un usuario no nuevo si un identificador dado (dirección MAC) del equipo de usuario es nuevo; y

e3) comprobar para un usuario no nuevo con un identificador nuevo de equipo de usuario si varias sesiones de acceso son autorizadas a ser simultáneamente activas para el usuario.

15. El método de la reivindicación 14, en el que pasos de comprobación resultantes al determinar un usuario no nuevo con un identificador nuevo de equipo de usuario, y varias sesiones de acceso no autorizadas a ser simultáneamente activas para el usuario, conducen a detectar una posible actividad fraudulenta.

16. El método de la reivindicación 14, que comprende además un paso de comprobar para un usuario no nuevo con un identificador no nuevo del equipo de usuario si un identificador dado del punto de acceso (AP-1, AP-2) es nuevo, lo que es entendido como una autenticación o preautenticación para el usuario.

17. El método de la reivindicación 13, que comprende además un paso de crear un primer registro de autenticación de acceso para el usuario una vez que una decisión de autorización positiva ha sido tomada para que el usuario acceda a través de un primer punto de acceso (AP-1) con un equipo de usuario (UE-1), comprendiendo el registro de autenticación de acceso:

- un identificador de usuario que identifica al usuario direccionado en la indicación de un suceso de autenticación (S-13);
- un identificador del equipo de usuario (UE-1) recibido en la indicación de un suceso de autenticación (S-13); y
- un identificador del punto de acceso (AP-1) que aplicó la autenticación.

18. El método de la reivindicación 17, que comprende además un paso de crear un segundo registro de autenticación de acceso para el usuario cuando el usuario es preautenticado a través de un segundo punto de acceso (AP-2).

19. El método de la reivindicación 13, en el que el paso f) de determinar el curso actual de acciones incluye los pasos de:

f1) comprobar si una autenticación satisfactoria tuvo lugar para el usuario con un identificador de usuario dado, con un identificador dado (UE-1, UE-2, UE-1bis) de equipo de usuario y a través de un punto de acceso identificado por un identificador dado (AP-1, AP-2); y

f2) comprobar si ya ha sido indicada cualquier sesión de acceso anterior para esta autenticación satisfactoria.

20. El método de la reivindicación 19, en el que los pasos de comprobación resultantes al determinar que ninguna autenticación satisfactoria ha tenido lugar para el usuario con un identificador de usuario dado, con un identificador dado (UE-1) del equipo de usuario y a través de un punto de acceso dado identificado por un identificador dado (AP-2), conducen a detectar una posible actividad fraudulenta.

21. El método de la reivindicación 19, en que los pasos de comprobación resultantes al determinar que una autenticación satisfactoria ya ha tenido lugar para el usuario y una sesión de acceso anterior para esta autenticación satisfactoria ya ha sido indicada, son entendidos como que un procedimiento de transferencia está en curso.

22. El método de la reivindicación 17, que incluye además un paso de crear un registro de sesión agregada para el usuario, cuando se determina que una autorización positiva ya ha sido efectuada para que el usuario acceda al punto de acceso dado y ninguna sesión de acceso ha sido indicada todavía para esta autorización positiva, comprendiendo el registro de sesión agregada:

- un identificador de usuario que identifica al usuario direccionado en la indicación de un suceso de contabilidad (S-15);
- un identificador del equipo de usuario (UE-1, UE-2, UE-1bis) recibido en la indicación de un suceso de contabilidad (S-15);
- un identificador del punto de acceso (AP-1, AP-2) donde la sesión ha sido establecida; y
- una lista de registros de autenticación de acceso asociados con este registro de sesión agregada particular.

23. El método de las reivindicaciones 21 y 22, comprendiendo además un paso de actualizar un registro de sesión agregada cuando se detecta una transferencia entre un primer punto de acceso (AP-1) y un segundo punto de acceso (AP-2), siendo la actualización llevada a cabo sustituyendo un identificador del primer punto de acceso (AP-1) por un identificador del segundo punto de acceso (AP-2), y eliminando de la lista el registro de autenticación de acceso correspondiente al primer punto de acceso.

24. El método de las reivindicación 13 o 23, que comprende además un paso de desconectar a un usuario con una sesión de acceso establecida a través de un punto de acceso dado (AP-1), siendo la desconexión indicada con un suceso de contabilidad (S-17) hacia una entidad centralizada (SAD).

25. El método de la reivindicación 24, en el que el paso de desconectar incluye los pasos de: eliminar el registro de autenticación de acceso correspondiente, actualizar el registro de sesión agregada asociado para eliminar el registro de autenticación de acceso de la lista, y eliminar el registro de sesión agregada cuando la lista está vacía.

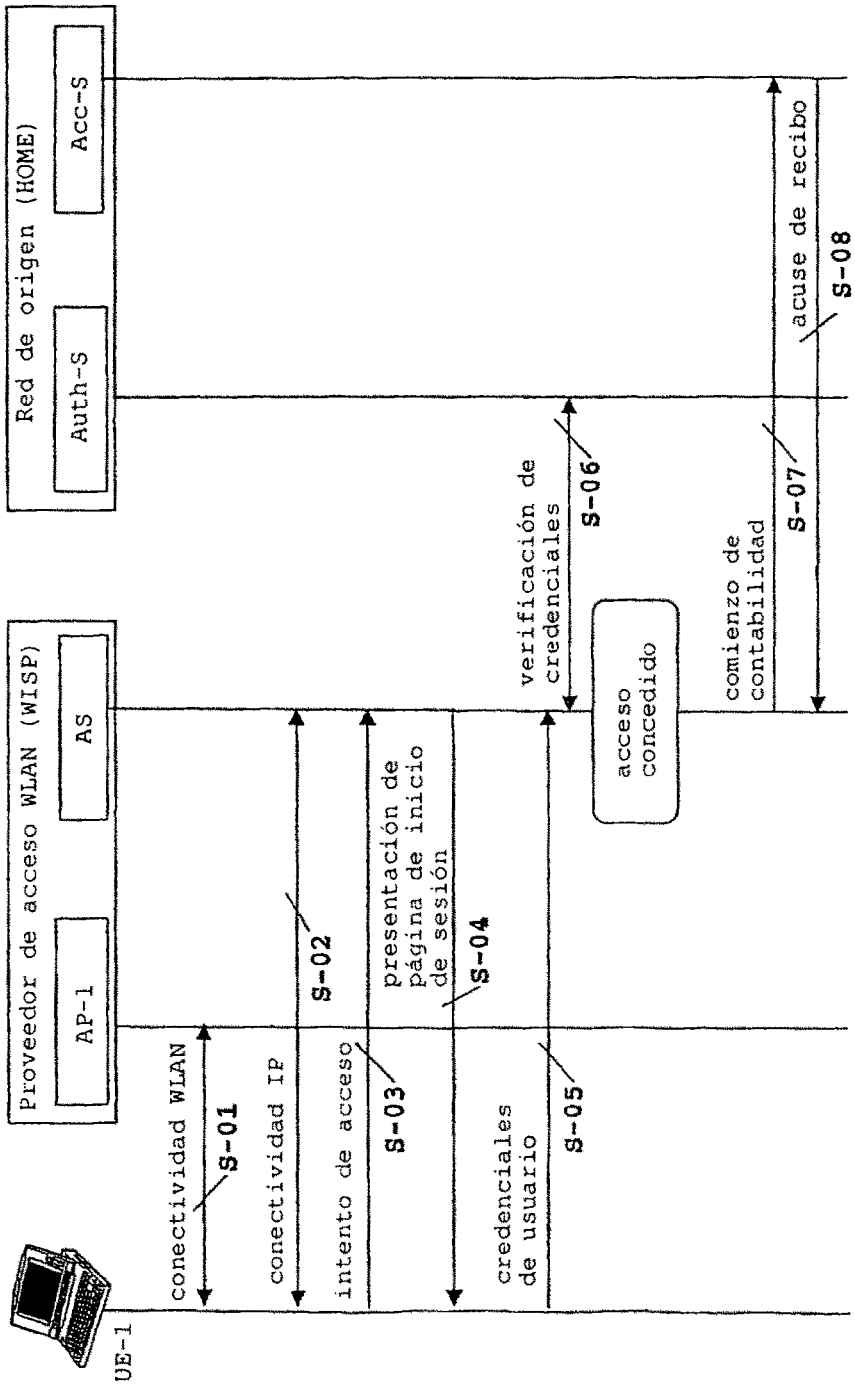

FIG.-1-

Técnica Anterior

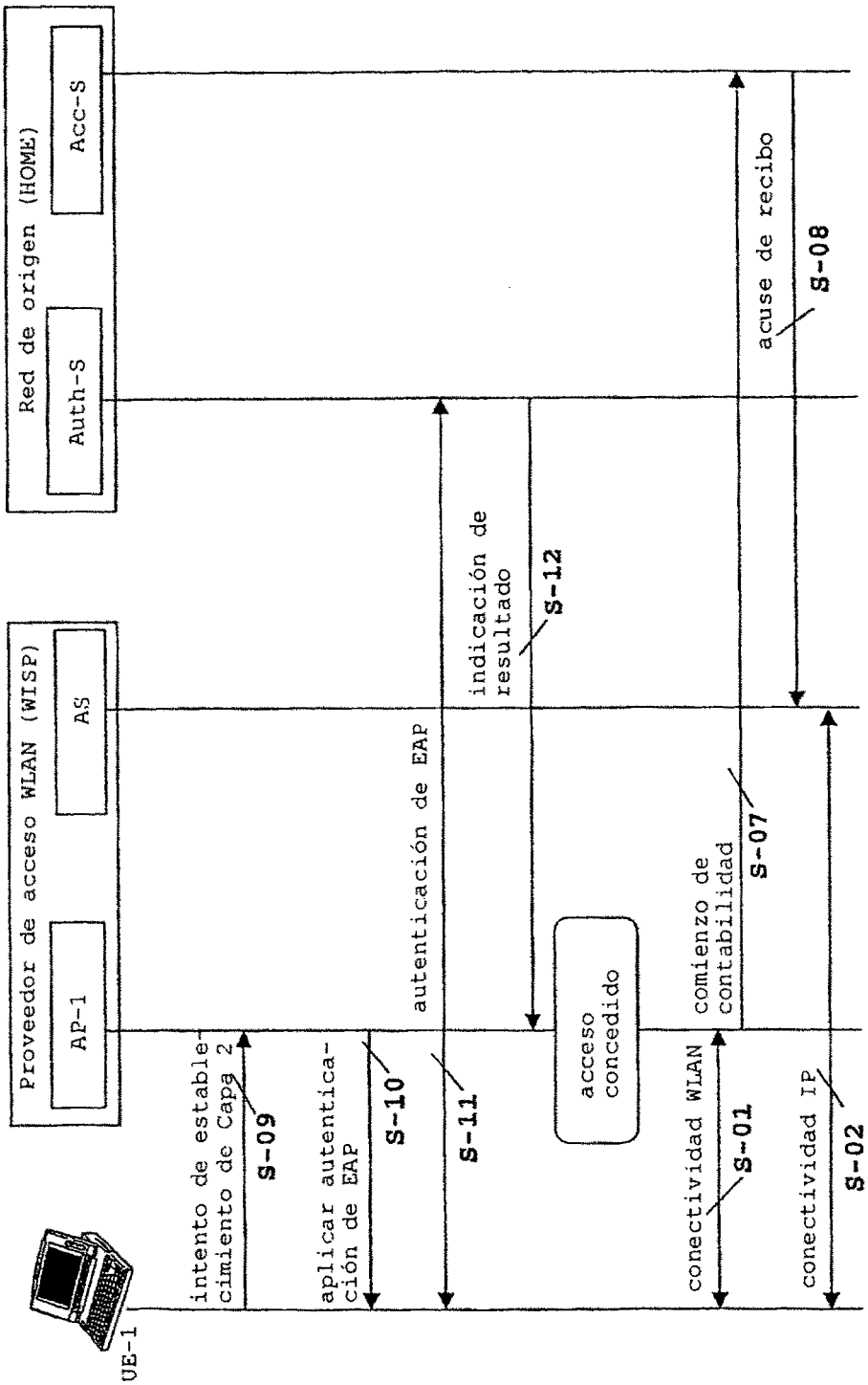

FIG.-2-

Técnica Anterior

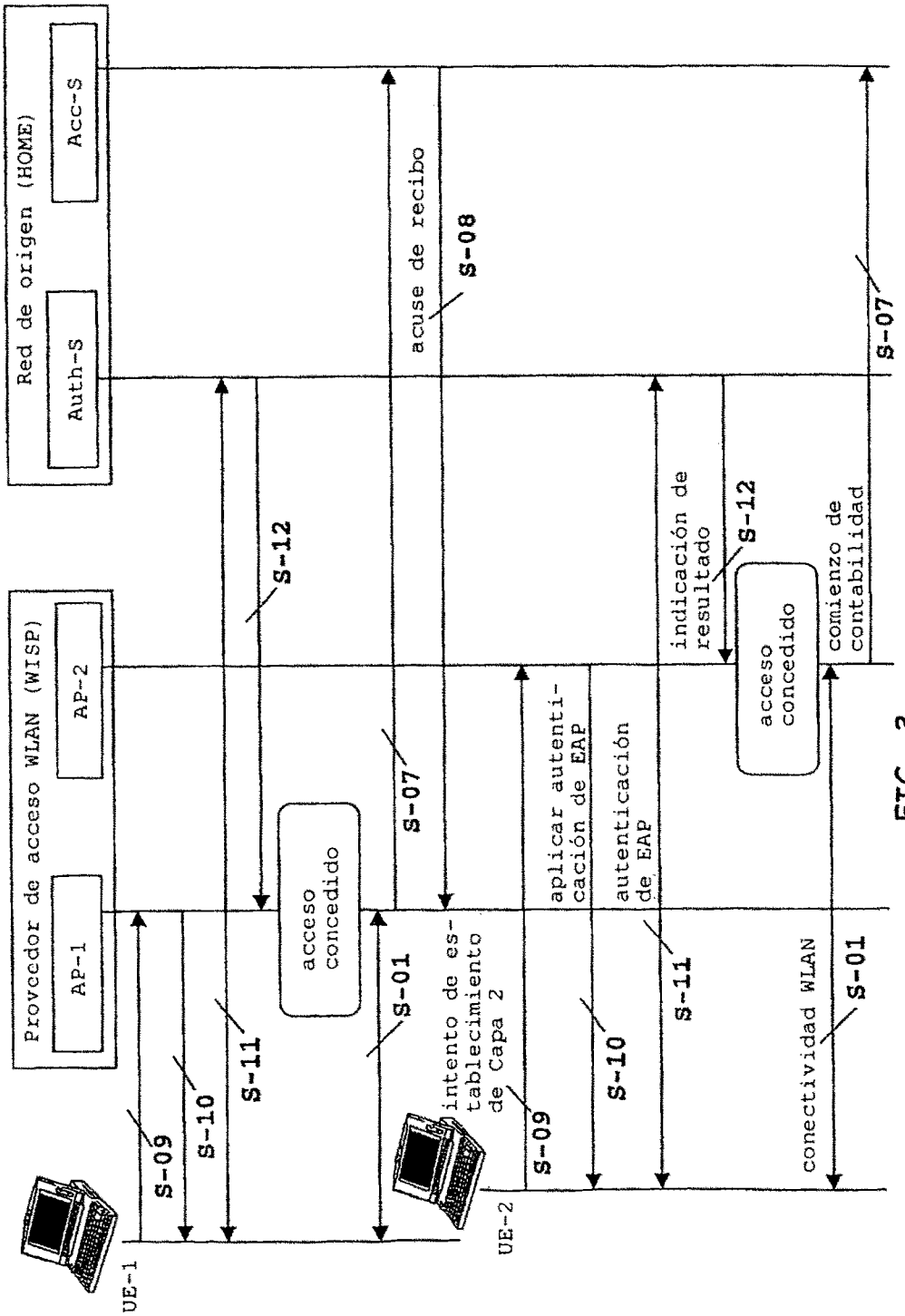

FIG.-3-

Técnica Anterior

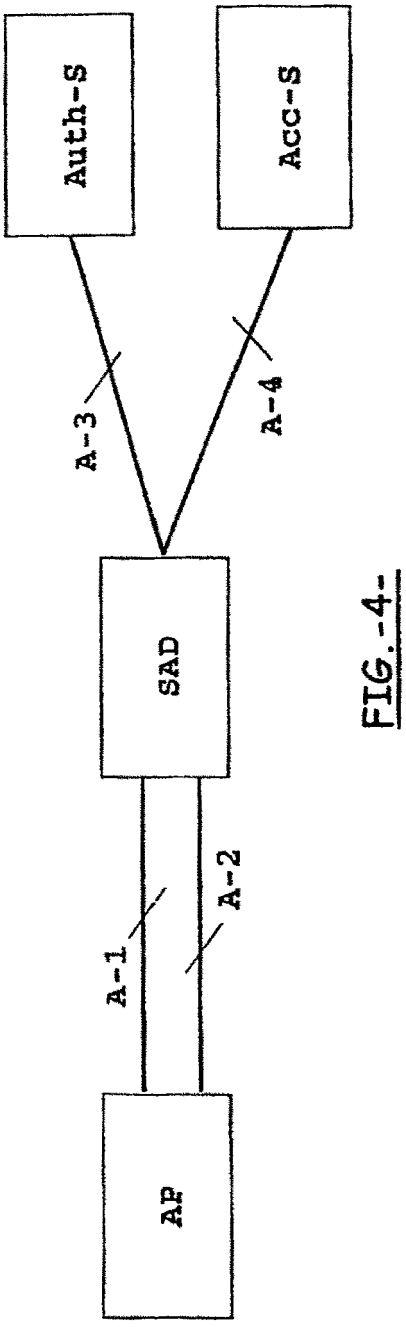

FIG.-4-

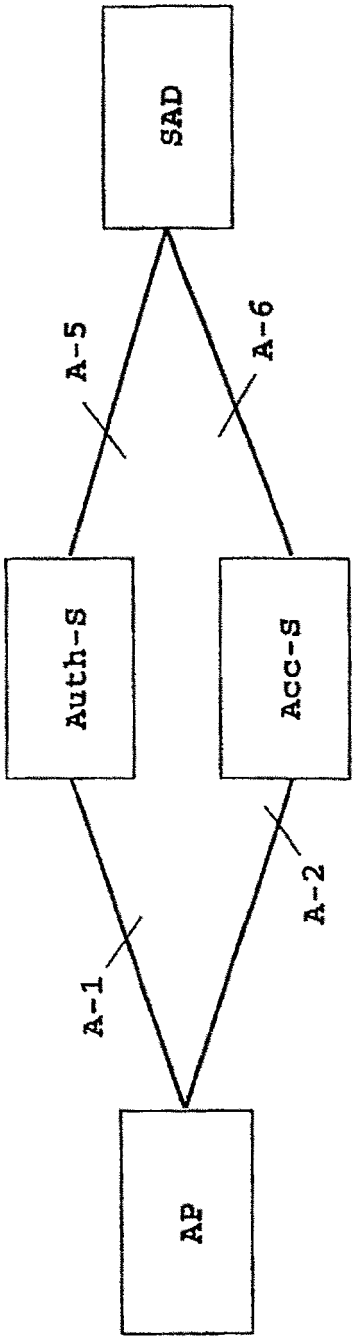

FIG.-5-

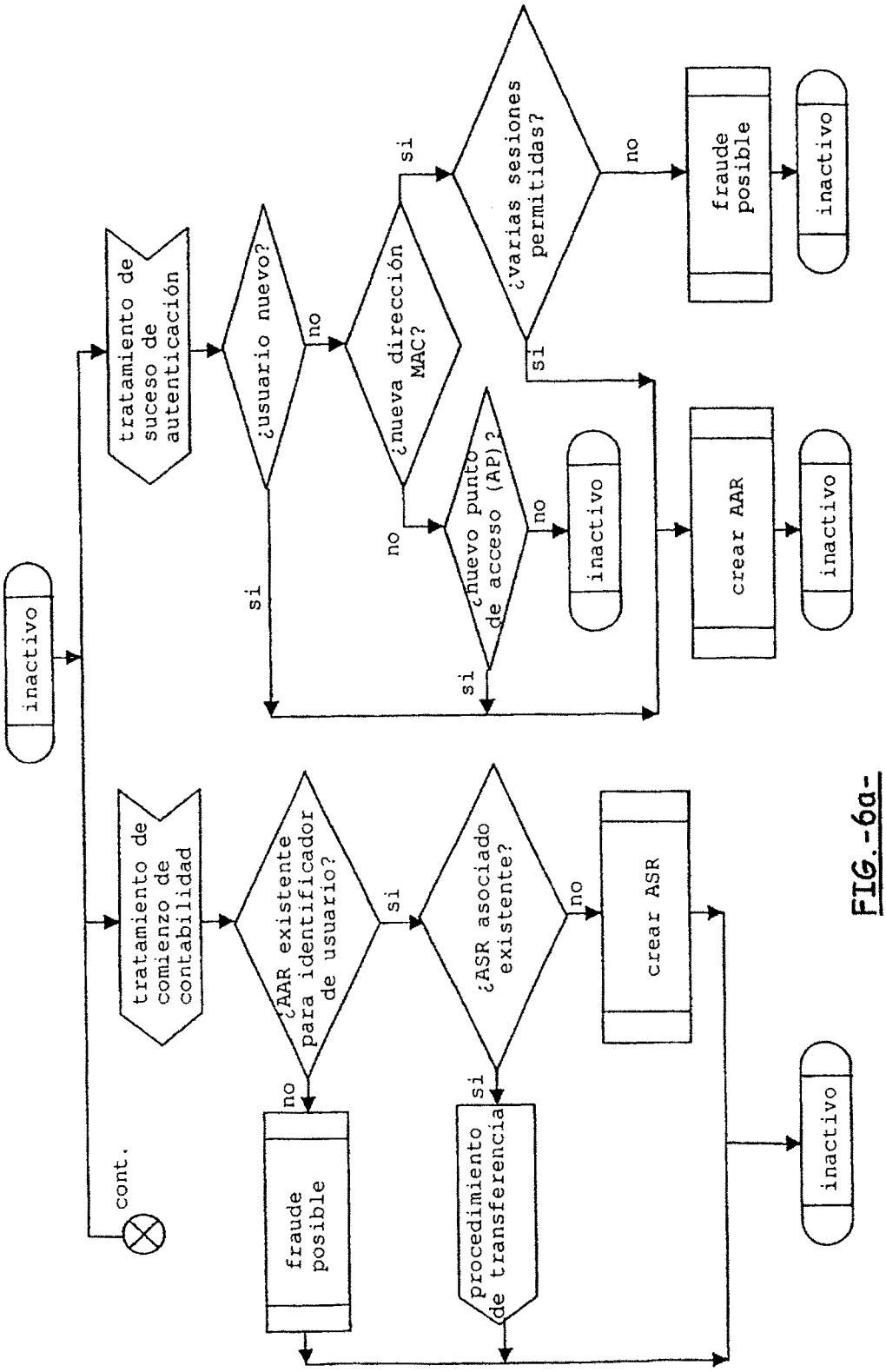
inactivo
tratamiento de suceso de autenticación
¿usuario nuevo?
no
si
¿nueva dirección MAC?
si
no
¿varias sesiones permitidas?
si
no
fraude posible
inactivo
¿nuevo punto de acceso (AP)?
si
no
inactivo
crear AAR
inactivo
tratamiento de comienzo de contabilidad
¿AAR existente para identificador de usuario?
no
si
¿ASR asociado existente?
si
no
crear ASR
fraude posible
procedimiento de transferencia
inactivo
cont.

FIG.-6a-

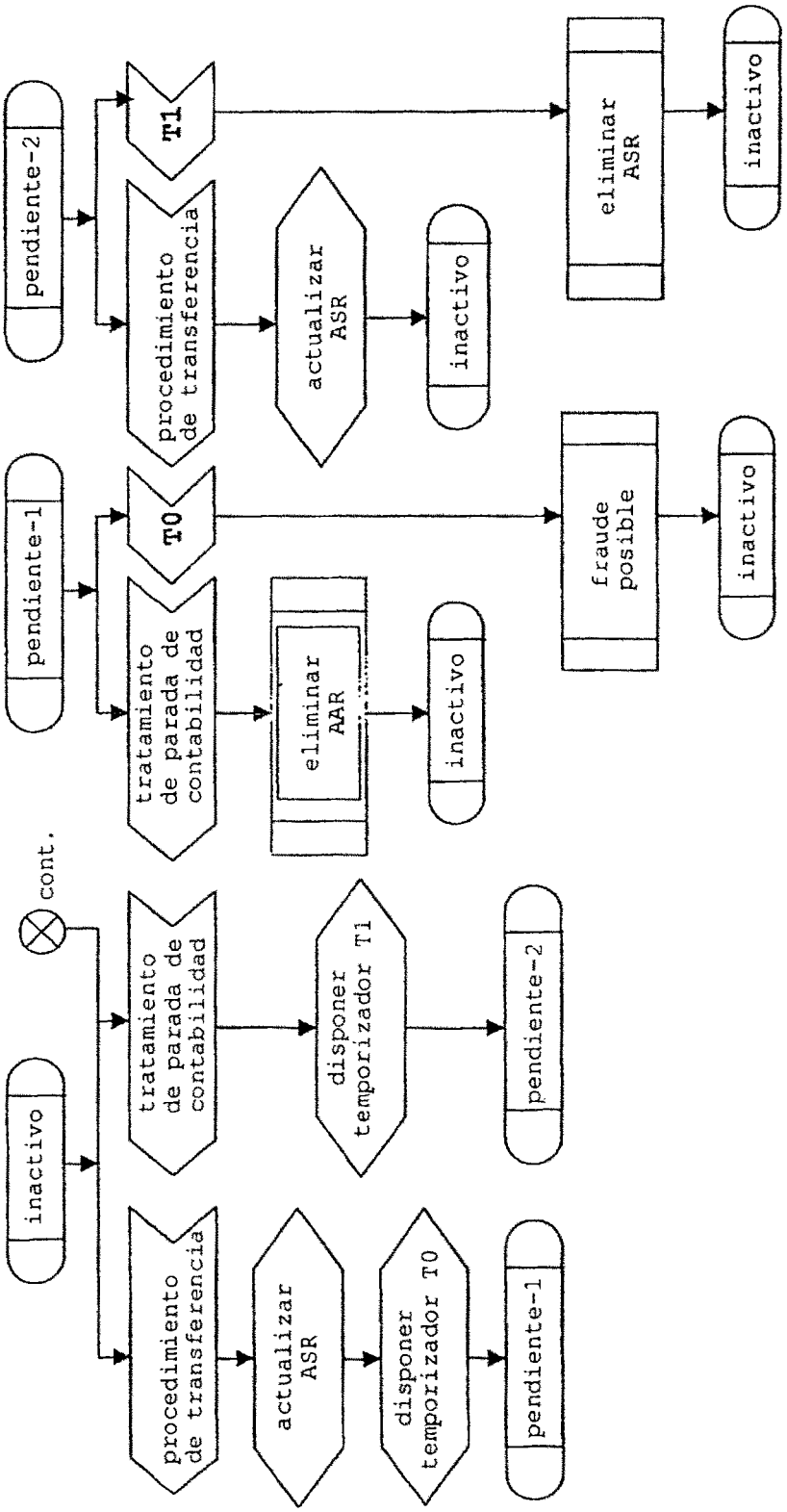
inactivo
cont.
procedimiento de transferencia
actualizar ASR
disponer temporizador T0
pendiente-1
tratamiento de parada de contabilidad
disponer temporizador T1
pendiente-2
pendiente-1
T0
tratamiento de parada de contabilidad
eliminar AAR
inactivo
pendiente-2
T1
procedimiento de transferencia
actualizar ASR
inactivo
fraude posible
inactivo
eliminar ASR
inactivo

FIG.-6b-

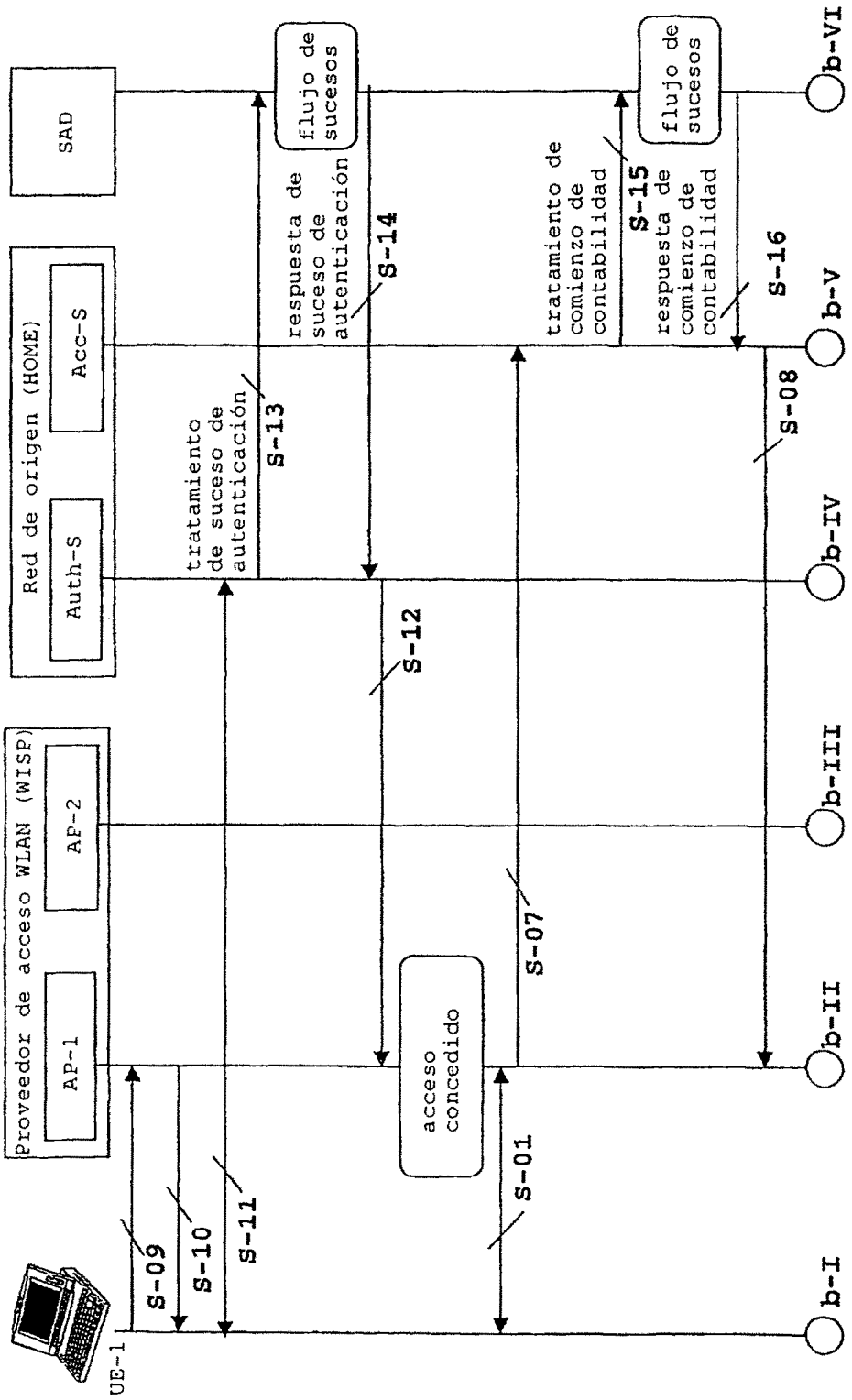
SAD
flujo de sucesos
respuesta de suceso de autenticación
S-14
tratamiento de comienzo de contabilidad
S-15
flujo de sucesos
respuesta de comienzo de contabilidad
S-16
b-VI
b-V
Red de origen (HOME)
Acc-S
Auth-S
tratamiento de suceso de autenticación
S-13
S-08
b-IV
S-12
Proveedor de acceso WLAN (WISP)
AP-2
AP-1
b-III
S-07
acceso concedido
b-II
S-01
S-09
S-10
S-11
b-I
UE-1

FIG.-7a-

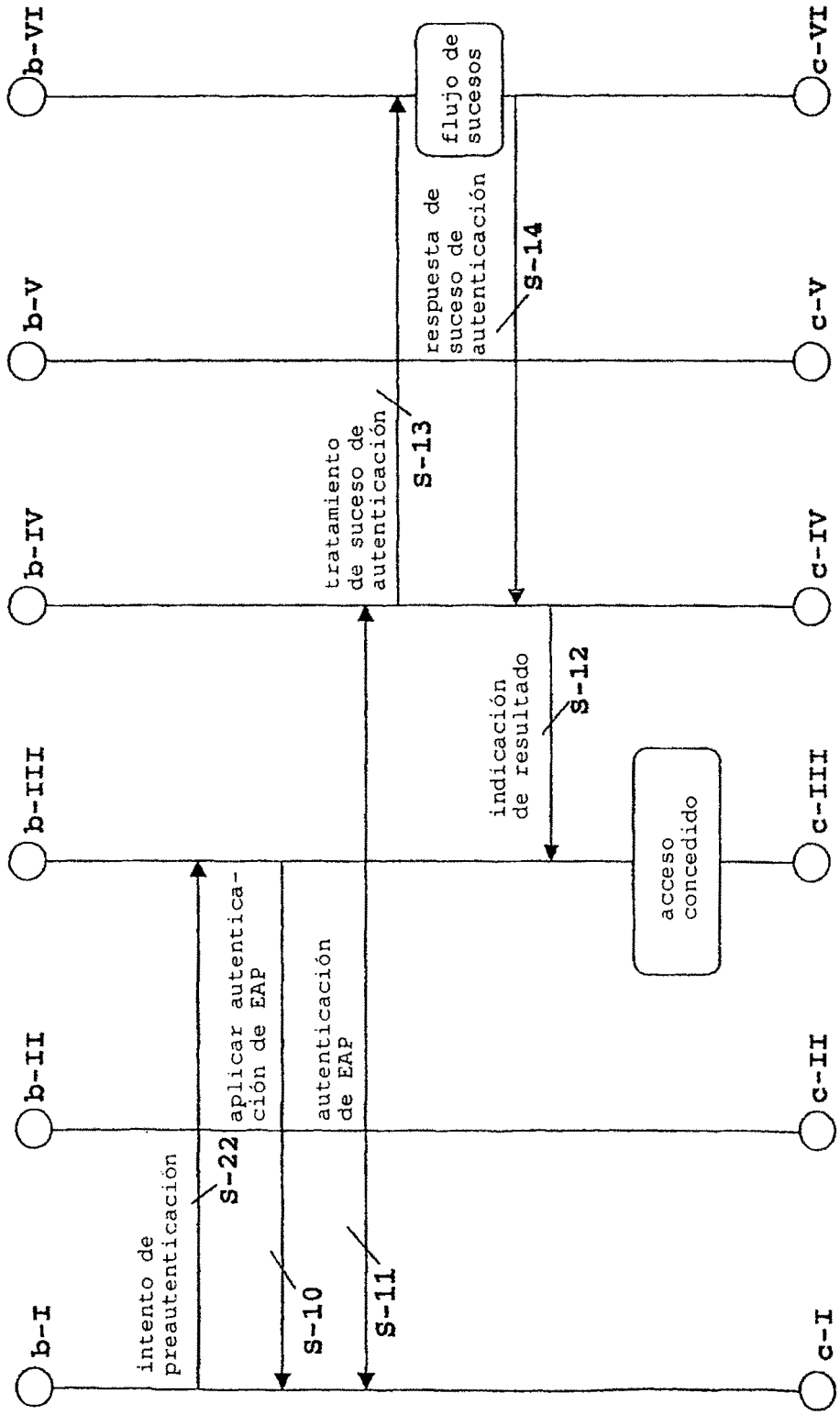
b-I
b-II
b-III
b-IV
b-V
b-VI
c-I
c-II
c-III
c-IV
c-V
c-VI
intento de preautenticación
S-22
aplicar autentica-ción de EAP
S-10
autenticación de EAP
S-11
tratamiento de suceso de autenticación
S-13
respuesta de suceso de autenticación
S-14
flujo de sucesos
indicación de resultado
S-12
acceso concedido

FIG.-7b1-

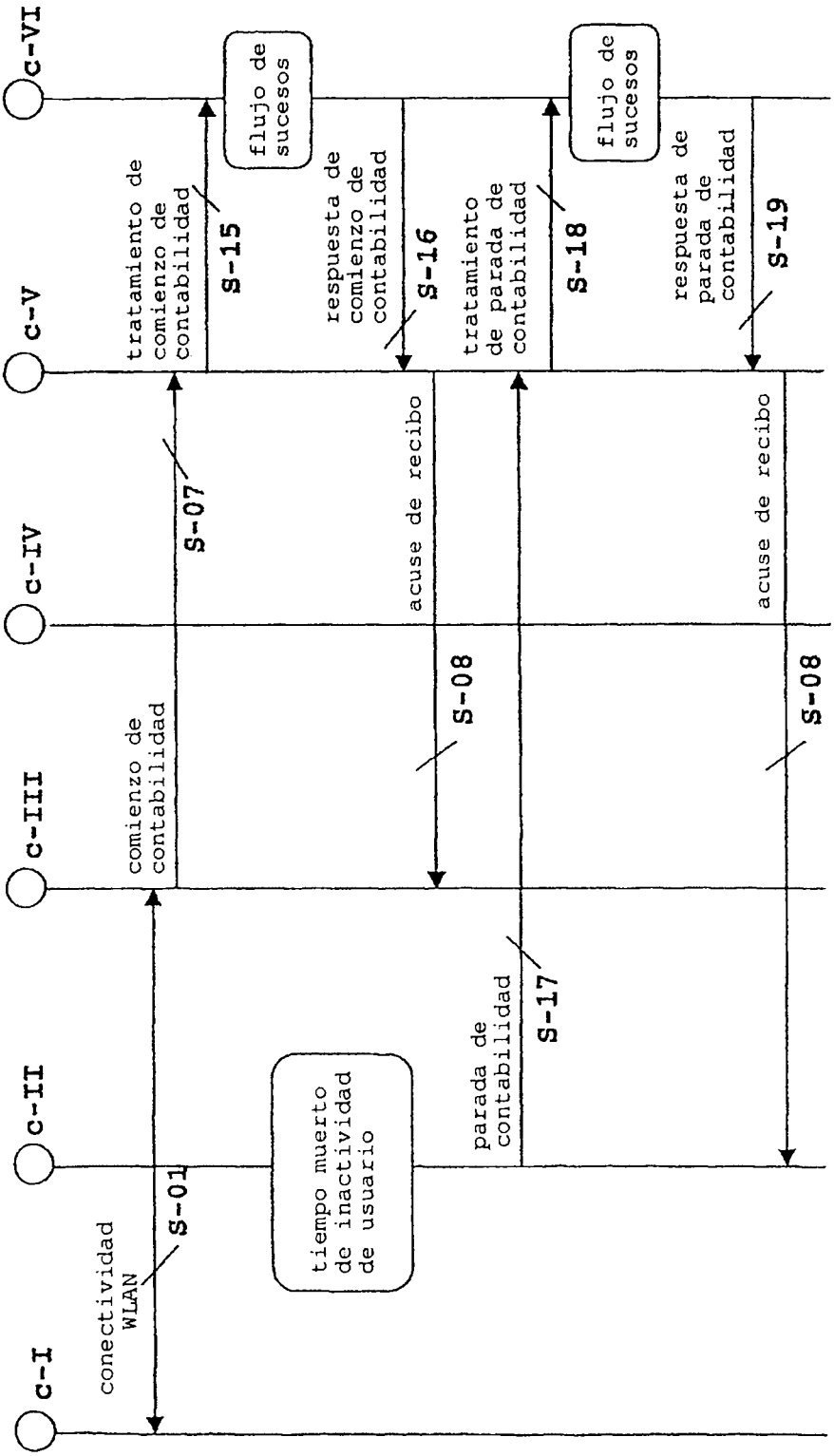
c-I
c-II
c-III
c-IV
c-V
c-VI
conectividad WLAN
S-01
tiempo muerto de inactividad de usuario
comienzo de contabilidad
S-07
S-08
acuse de recibo
tratamiento de comienzo de contabilidad
S-15
flujo de sucesos
respuesta de comienzo de contabilidad
S-16
parada de contabilidad
S-17
tratamiento de parada de contabilidad
S-18
flujo de sucesos
respuesta de parada de contabilidad
S-19
S-08
acuse de recibo

FIG.-7c1-

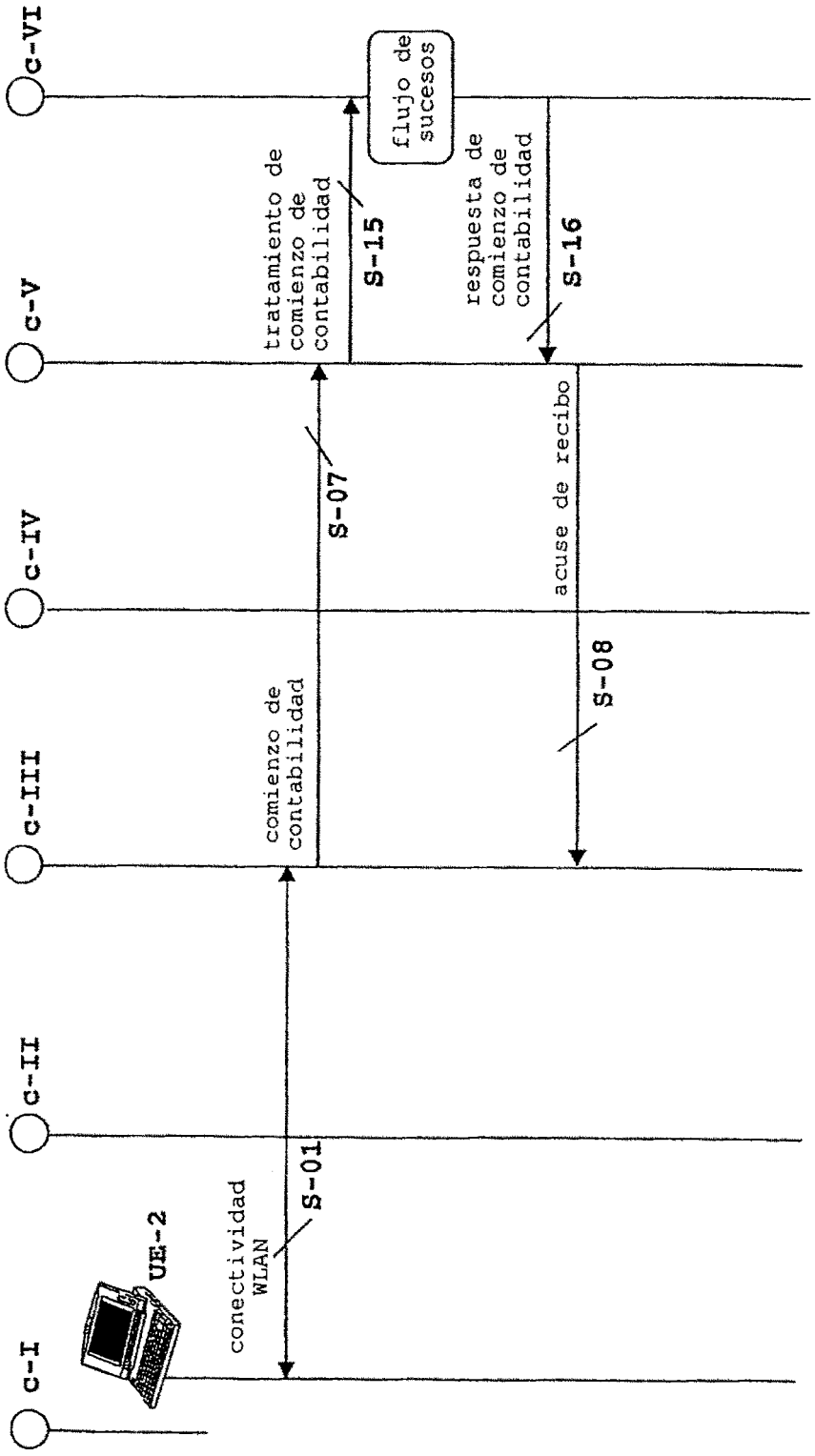
c-VI
c-V
c-IV
c-III
c-II
c-I
flujo de sucesos
tratamiento de comienzo de contabilidad
S-15
respuesta de comienzo de contabilidad
S-16
S-07
acuse de recibo
comienzo de contabilidad
S-08
S-01
conectividad WLAN
UE-2

FIG.-7c2-

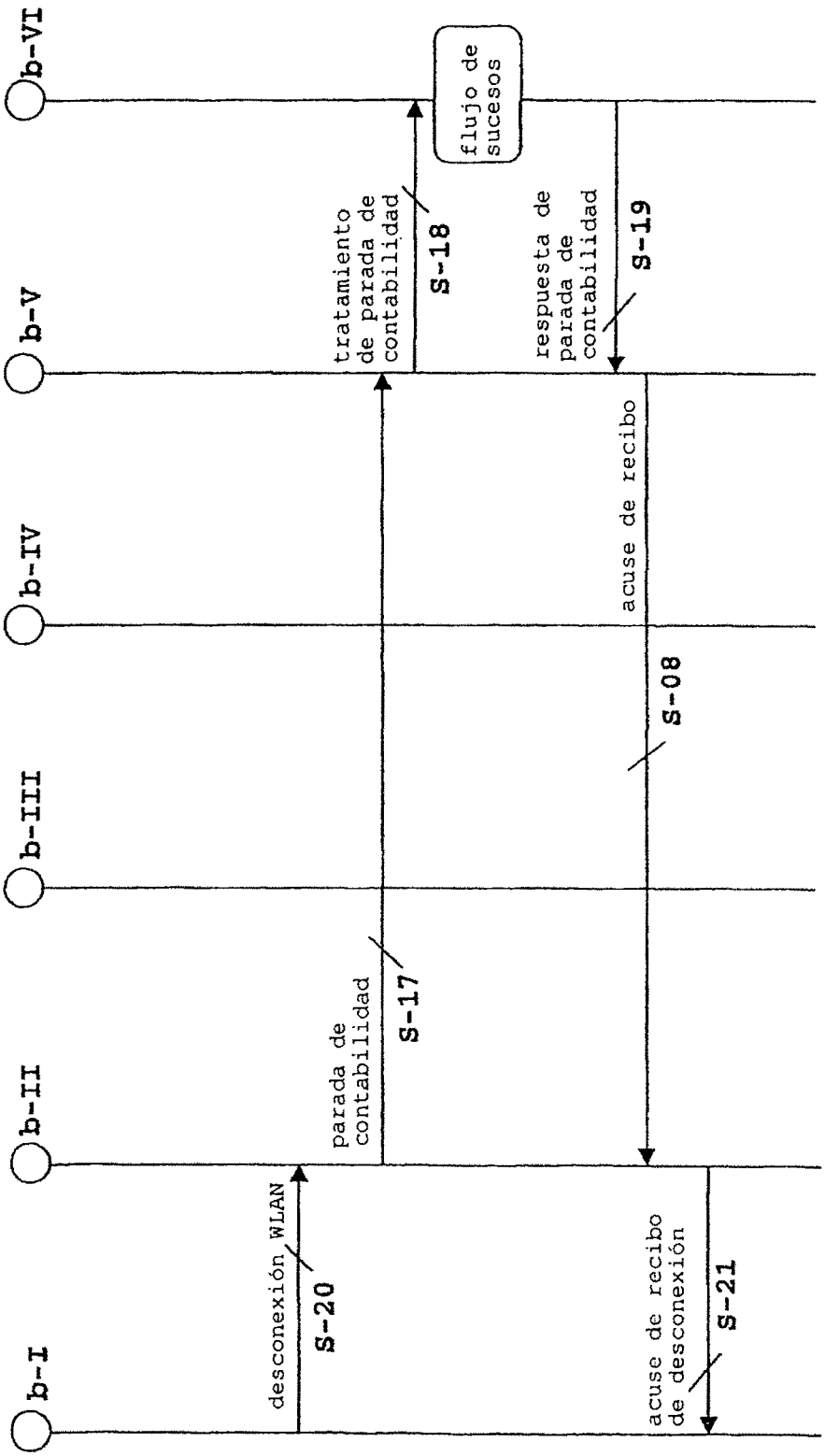
b-VI
b-V
b-IV
b-III
b-II
b-I
flujo de sucesos
tratamiento de parada de contabilidad
S-18
respuesta de parada de contabilidad
S-19
acuse de recibo
S-08
parada de contabilidad
S-17
desconexión WLAN
S-20
acuse de recibo de desconexión
S-21

FIG.-7b2-

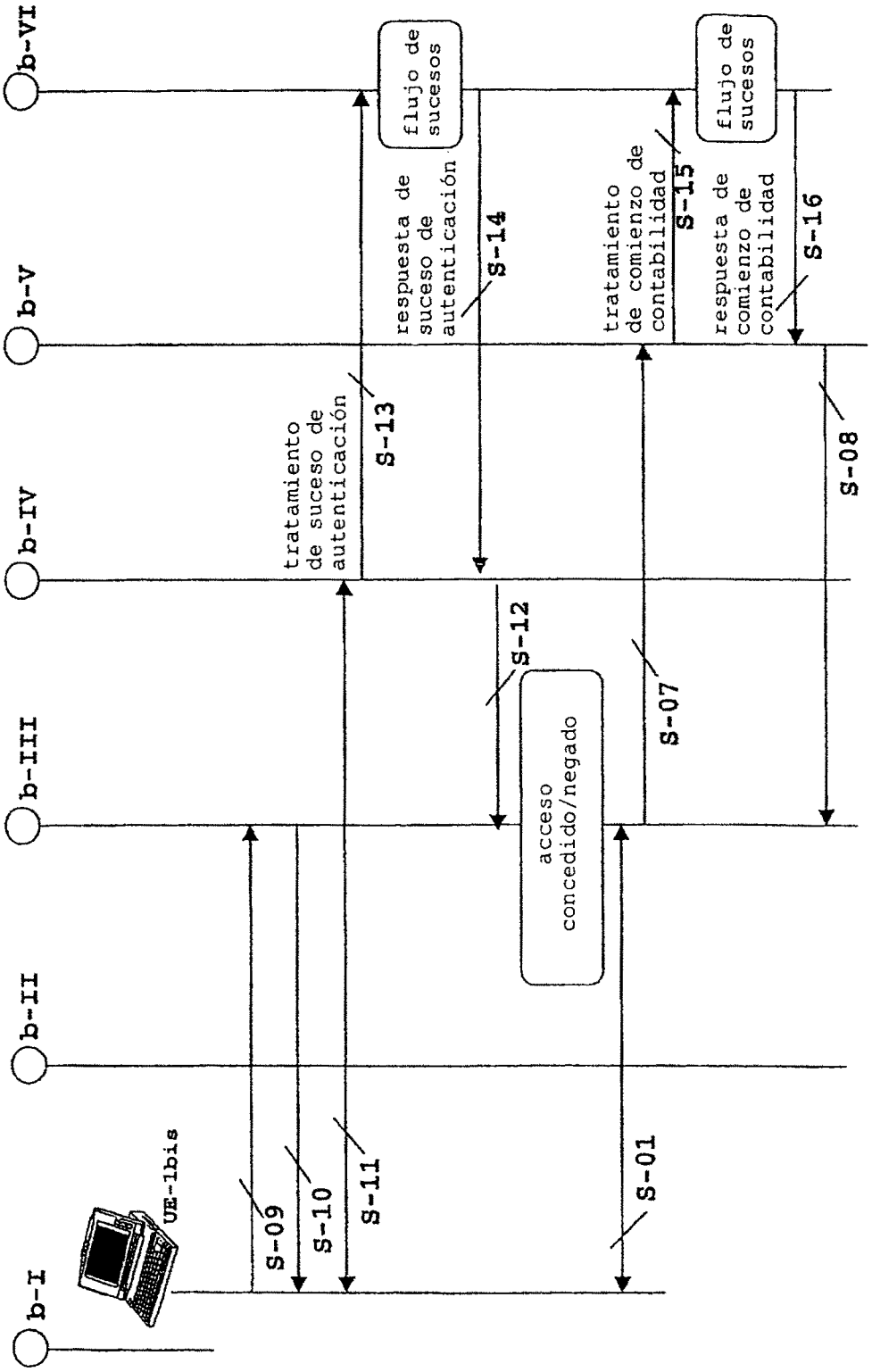
b-VI
b-V
b-IV
b-III
b-II
b-I
UE-1bis
flujo de sucesos
respuesta de suceso de autenticación
S-14
tratamiento de suceso de autenticación
S-13
tratamiento de comienzo de contabilidad
S-15
flujo de sucesos
respuesta de comienzo de contabilidad
S-16
S-08
S-12
acceso concedido/negado
S-07
S-09
S-10
S-11
S-01

FIG.-7b3-