(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 617 068**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
H04W 80/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.10.2012 E 12007079 (2)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 2720432**

(54) Título: **Protocolo de sesión de red móvil para comunicación móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2017

(73) Titular/es:

QNECTIVE AG (100.0%)
Thurgauer Strasse 54
8050 Zürich, CH

(72) Inventor/es:

IOANNIS, IOANNIDIS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Protocolo de sesión de red móvil para comunicación móvil

1. Antecedentes de la invención

1.1. Campo de la invención

La presente invención pertenece al campo de la tecnología de la información y se refiere a un método y un sistema para efectuar una comunicación bajo inclusión del protocolo TCP entre al menos un primer dispositivo de comunicación y un segundo dispositivo de comunicación.

1.2. Descripción y desventajas de la técnica anterior

Los protocolos de Internet, tales como el TCP-IP, se han diseñado en los primeros días de Internet (años 80) y se han usado de modo consistente desde entonces. Los mismos protocolos se usan para que la primera conexión a Internet (marcado) realice más conexiones de banda ancha utilizadas hoy en día (ADSL, Cable, Wi-Fi). Estas conexiones a Internet funcionan bien para dispositivos que son estáticos (enchufados a un cable) o que están restringidos a una zona pequeña (Wi-Fi). Comenzando aproximadamente en 2006, el acceso a banda ancha móvil empezó a estar disponible y, en la actualidad, se usa cada vez más a nivel de consumidor. La tecnología utilizada varía entre GSM (GPRS y borde), 3G (UMTS) o 4G (HSPA) para las redes más avanzadas.

Sin embargo, hay una necesidad imperiosa de usar una conexión de banda ancha también en situaciones móviles, en las que no está presente una conexión basada en cable o una conexión basada en WiFi estable.

El acceso a banda ancha móvil permite que los teléfonos inteligentes y otros dispositivos digitales se conecten a Internet desde cualquier lugar en el que puede hacerse una llamada de teléfono móvil. Sin embargo, el problema con Internet móvil es que el usuario no está enlazado a un punto de acceso, si no que se mueve con su dispositivo de un punto de acceso a otro. Cuando se está moviendo, el dispositivo móvil se desconecta de la antena actual para conectarse a otra (denominado un traspaso). Sucede a menudo que la conexión se cae durante el traspaso debido a que se cambia la dirección IP o debido a que no hay ranuras suficientes para esta comunicación. Sucede también muy a menudo que la calidad de señal difiere significativamente de un lugar a otro, incluso sin traspaso de antenas, lo que hace que la capa de red móvil experimente muchas interrupciones de red no deseadas y múltiples intentos de reconexión.

La solicitud de patente europea EP 1 303 102 A2 describe una topología de uso de red que tiene un servidor que proporciona contenidos y aplicaciones a clientes que los piden, también a muchos dispositivos de cliente móviles. Con respecto a los múltiples protocolos diferentes que residen en servidores y clientes, con respecto a la falta de gestión de traspasos de sesiones o gestión de galletas informáticas (“cookies”) y con respecto a las frecuentes interrupciones de sesión, se define un problema a resolver para proporcionar sesiones permanentes capaces de soportar múltiples aplicaciones con múltiples protocolos en múltiples dispositivos.

Por lo tanto, EP 1 303 102 A2 propone la disposición de una sesión que se mantiene activa durante una o más desconexiones de red, es decir, durante un período más largo, denominado período de gracia, que permite que un usuario evite procedimientos de autenticación repetidos. De esta manera, se pueden llevar contenido y aplicaciones a los clientes evitando demasiado esfuerzo del usuario, cuando se debe continuar o reanudar una sesión después de una desconexión de red.

Sin embargo, no se puede ver ninguna explicación útil para gestionar mensajes en tiempo real en esta situación específica.

1.1. Objetivos de la invención

El objetivo de la presente invención es proporcionar un método y un sistema para asegurar una conexión a Internet con un grado configurable de fiabilidad que está mejor adaptado para uso móvil, y que está adaptado para la gestión de mensajes en tiempo real.

2. Compendio y ventajas de la invención

Este objetivo de la invención se consigue por las características indicadas en las reivindicaciones independientes adjuntas. Las disposiciones y realizaciones ventajosas adicionales de la invención se exponen en las reivindicaciones dependientes respectivas. Se deberá hacer referencia a continuación a las reivindicaciones adjuntas.

Según la característica básica de la presente invención, se describen un método y un sistema respectivo para efectuar una comunicación bajo inclusión de una capa de transporte de red, preferiblemente el protocolo TCP-IP, entre al menos un primer dispositivo de comunicación y un segundo dispositivo de comunicación, por ejemplo dos teléfonos móviles, que incluye un procedimiento de autenticación de usuario inicial o de inicio de sesión, en el que al menos un servidor controla la comunicación proporcionando una conexión entre el primer y el segundo dispositivo,

en el que la comunicación se extiende a través de las fronteras de red, p. ej., Wifi a GSM, o hace frente a repetidas desconexiones de red debidas a inestabilidades de red técnicas, cuyo método está caracterizado por las etapas de:

a) generar una sesión que está basada en datos de autenticación de usuario reconocido y se asocia con dicha comunicación tan pronto como se ha establecido con éxito una conexión entre dicho servidor y dicho cliente,

b) mantener válida dicha sesión a pesar de dichas desconexiones de red durante un período de gracia predeterminado, en el que dicho período de gracia está predefinido para ser suficientemente grande a fin de soportar un traspaso intrarredes o una desconexión temporal debida a la inestabilidad de red.

De esta manera, se evitan prolongados procedimientos de autenticación de usuario repetidos, dado que la misma sesión se puede usar para los mismos dos usuarios, aunque la conexión física se haya interrumpido una o más veces. De esta manera, la conexión parece ser fiable para una persona física, así como para un dispositivo de cliente, aunque no sea fiable real y físicamente debido a desconexiones de red temporales. La fiabilidad se puede parametrizar y configurar por ello mediante la longitud de dicho período de gracia en “segundos”. Así, se encuentra una solución para el objetivo de la invención.

Usando esta característica implementada en una capa de sesión adicional, que se denomina en la presente memoria Capa de sesión inventiva y se abrevia como iSL, con un período de gracia predefinido que se define cuando puede tener lugar de modo transparente una reconexión sin notificar a las capas de aplicación, la presente invención proporciona una conexión fiable configurable en caso de desconexiones cortas de la capa de transporte que ocurren frecuentemente en las redes móviles.

Así, se encuentra una solución mejorada adicional al problema mencionado anteriormente.

Ventajosamente, se gestiona una cola de espera por ambos extremos para mensajes en espera de reenvío que se mantenían sin enviar durante una de dichas desconexiones de red temporales, pero durante la misma sesión. Esto ahorra tiempo y es conveniente para el usuario.

Ventajosamente además, la aplicación de cliente y el usuario, como persona física, no han tomado conciencia de “pequeños” problemas en la red. Esto ahorrará tiempo de CPU y vida útil de la batería del cliente, por ejemplo de un teléfono móvil, un teléfono inteligente, etc., así como proporcionará una mejor experiencia del usuario.

Introducción a la invención: el protocolo TCP utilizado para la mayoría de conexiones a Internet garantiza una conexión fiable. Con sus mecanismos de acuse de recibo y de reconocimiento y retransmisión posteriores, se asegura que no hay ninguna pérdida de datos entre el remitente y el receptor. Si uno de ellos pierde la conexión, el canal de comunicación se cierra, incluso si la duración de la desconexión es corta. A menudo, antes de que un usuario pueda utilizar una aplicación en su teléfono móvil, la aplicación experimenta una fase de “inicialización” que consiste en que dicha aplicación se conecta a un servidor y que se intercambian datos (tales como una lista de contactos u otra sincronización) entre la aplicación de cliente respectiva y un servidor de aplicaciones. Una desconexión del servidor es cara usualmente para un dispositivo móvil, dado que estos datos se tienen que retransmitir cuando vuelve a conectarse. El problema con el TCP es que no se diseñó para la comunicación entre consumidores que acceden a Internet a través de un dispositivo móvil. En un entorno móvil, son comunes desconexiones cortas en la capa TCP, debido a interrupciones en la red inalámbrica subyacente o traspasos a otro tipo de red (tales como la conmutación de 3G a WiFi).

Teniendo en cuenta esta situación, la presente invención comprende la idea de renovar el protocolo TCP, o cualquier otro protocolo de transporte, en un nuevo protocolo de sesión que es capaz de gestionar desconexiones de red cortas y ocultarlas de la aplicación, haciendo uso de la conexión de red a fin de asegurar una conexión a Internet móvil más uniforme y más fiable. Esto lo implementa preferiblemente otra capa de sesión sobre la parte superior del TCP, que se denominará Capa de sesión inventiva (iSL) en el resto de este documento.

Según un aspecto preferido de la invención, se propone añadir una capa sobre la parte superior del TCP, que tiene cuidado de dichas desconexiones cortas anteriormente mencionadas, que son típicas del uso móvil de la red. Esta capa de sesión se usa sobre la parte superior del protocolo TCP-IP para asegurar la compatibilidad con los estándares de Internet. Esta capa de sesión permite mantener operativa la conexión de red (como se ve por la aplicación) durante un período de tiempo predefinido, denominado también en la presente memoria período de gracia. Este período de gracia está predefinido suficientemente grande, preferiblemente 20 segundos, cuando se aplica a llamadas de teléfono móvil y a IP sobre voz, para soportar traspasos intrarredes (por ejemplo, de red Wi-Fi a GSM) y desconexiones debidas a la inestabilidad de red. Esta capa tiene la ventaja de evitar reconexiones frecuentes, lo que proporciona, a su vez, mejor grado de utilización y ahorra también consumo de batería.

Un problema potencial con el hecho de mantener operativa la conexión durante una pérdida de red es que algunos mensajes son solamente válidos cuando se suministran en tiempo real (por ejemplo, el mensaje para comenzar una llamada en el caso de VoIP). En este caso, el período de gracia para un traspaso de red, como se ha mencionado anteriormente para 20 segundos, introduciría un retardo demasiado largo. Así, la capa de sesión inventiva anteriormente mencionada proporciona también una arquitectura flexible mediante la implementación de prioridades específicas para tipos de mensaje específicos respectivos:

un primer tipo de mensaje es: “crítico en el tiempo”. Si un mensaje es un mensaje en tiempo real, la capa iSL inventiva lo suprimirá durante el período de gracia. La capa iSL inventiva notifica al remitente de este mensaje el fallo de suministro;

un segundo tipo de mensaje es: “no crítico en el tiempo”. Estos mensajes no críticos en el tiempo, por ejemplo, mensajes de chat o de actualización de estado, tienen prioridad normal y se pueden suministrar más tarde. Estos mensajes se mantienen por ello en cola de espera en caso de desconexiones cortas y no sufren por ello desconexiones pequeñas.

Para una comprensión completa de la invención, se debe añadir que, cuando se pierde la conexión durante una llamada telefónica VoIP, la llamada permanece activa durante el período de gracia puesto que la desconexión corta no se ha hecho visible al resto de la aplicación. Si la conexión UDP se ve afectada también por la pérdida de la conexión de red, se suprimen paquetes de audio hasta que vuelve la conexión. Si no, el tráfico UDP puede seguir normalmente.

Además del período de gracia y las prioridades de mensaje, el método inventivo proporciona una detección robusta de desconexiones que son específicas de la comunicación móvil. Con los dispositivos móviles es posible que el dispositivo pierda conectividad sin que se detecte la pérdida de conexión. Esto sucede frecuentemente con los dispositivos móviles en los que el sistema operativo detiene características, tales como el mecanismo para mantener activo el TCP, cuando están en reposo a fin de ahorrar alimentación de la batería. Además de esto, los ajustes TCP para servidores que gestionan clientes móviles tienen a menudo parámetros para mantener activo el TCP establecidos para tiempos de espera largos, a fin de ser conveniente para la batería de los dispositivos móviles. De este modo, los servidores TCP de la técnica anterior detectarán de manera desventajosa desconexiones mucho después de que los clientes ya no puedan comunicarse. En este caso, la capa de sesión inventiva proporciona una notificación fiable de conexión/desconexión en ambos, cliente y servidor. Si el método inventivo detecta una desconexión, se cierra la toma TCP en espera. En la presente memoria, la capa de sesión inventiva detecta preferiblemente la desconexión mediante el reconocimiento: si no se ha recibido ningún reconocimiento en un intervalo predeterminado de tiempo de 5 segundos, la lógica inventiva del programa de capas de sesión interpreta esto como que está presente una desconexión. El servidor fuerza entonces el cierre de la toma TCP.

De esta manera, en resumen, las contribuciones inventivas esenciales son las siguientes:

una capa de sesión adicional sobre la parte superior de una capa de transporte (p. ej., TCP) para proporcionar una conexión estable de sesión en caso de comunicación móvil,

- el uso de un período de gracia,

- la puesta en cola de mensajes y la clasificación de la prioridad que tienen lugar durante el período de gracia,

- una detección robusta de la desconexión del cliente a través de una capa adicional.

3. Breve descripción de los dibujos

La presente invención se ilustra a modo de ejemplo y no está limitada por la forma de las figuras de los dibujos, en los que:

la figura 1 ilustra los componentes estructurales más básicos de un entorno de hardware y software de la técnica anterior, utilizado para un método de la técnica anterior y utilizable también para el método inventivo,

la figura 2A ilustra los componentes lógicos de una implementación de software del método inventivo, en el que la capa de sesión inventiva está implementada por debajo de una capa de aplicación y por encima de la capa de transporte TCP,

la figura 2B es una representación según la figura 2B, pero sin capa inventiva, como en la técnica anterior,

la figura 3 es una representación esquemática de los principales componentes de gestión de conexiones lógicas, abreviados en la presente memoria también como CMC, implementados en el lugar del cliente según un uso preferido del método inventivo para comunicación telefónica móvil en el chip lógico de un teléfono móvil,

la figura 4 es una representación según la figura 3, pero que muestra la situación en un servidor que presenta la funcionalidad de gestión de conexiones a una gran pluralidad de conexiones de red (usuarios finales) según la figura 3,

la figura 5 ilustra el flujo de control de las etapas más importantes de una realización preferida del método inventivo, que se implementa en el componente inventivo 38 de la figura 3 y el componente 46 de la figura 4, en una forma de visión de conjunto. Esta figura muestra el uso de la capa de sesión inventiva en el contexto de una aplicación VoIP con presencia del usuario (en línea/fuera de línea),

la figura 6 es una representación esquemática complementaria exhaustiva según la figura 5 que ilustra, junto con la figura 7, las diferencias del método inventivo con relación a la técnica anterior, que se muestra, a su vez, en la figura 7,

la figura 7 es una representación según la figura 6, pero sin implementación de las características inventivas,

la figura 8 es una representación esquemática de lugares de almacenamiento en un encabezamiento de mensaje utilizado por la presente invención,

la figura 9 es una ilustración esquemática del principio para usar colas de mensajes en el contexto inventivo.

4. Descripción detallada de la realización preferida

Con referencia general a las figuras y con referencia especial a continuación a la figura 1 de nuevo, el método inventivo se implementa en una arquitectura cliente-servidor para aplicaciones VoIP como se representa en la figura 1. Los dispositivos móviles, en particular los teléfonos móviles o teléfonos inteligentes 12, se conectan a Internet 10 a través de un canal de datos portador disponible de la técnica anterior, tal como se proporciona mediante un proveedor de servicios de telefonía móvil como Swisscom en Suiza, o Vodafone en Alemania, y se conectan entonces a un ordenador servidor de comunicación 14. Los dispositivos móviles 12 actúan como clientes en la arquitectura de sistemas de cliente-servidor de la figura 1. El servidor 14 está equipado con hardware y software de interfaz respectiva, como es conocido a partir de la técnica anterior, y se implementa para seguir la pista de cualquier estado de conexión de dispositivo respectivo, denominado en la presente memoria “presencia”, y propaga la información de presencia a los otros usuarios del sistema. La conexión de dichos clientes móviles 12 a dicho servidor 14 se realiza a través de capas de software diferentes, como se describirá en lo que sigue con referencia a las figuras 2A y 2B con más detalle.

La figura 2A ilustra los componentes lógicos de una implementación de software del método inventivo, en la que dicho método inventivo se implementa como una capa de sesión 22, por debajo de una capa de aplicación 21 y por encima de la capa de transporte TCP 23.

Sobre la parte superior de la capa de red 24 y las capas de hardware subyacentes, que no se representan, se implementan tres capas diferentes que proporcionan llamadas a procedimientos remotos (RPC) según la técnica anterior y un suministro fiable de mensajes.

En particular, directamente por encima de la capa de red 24, una toma TCP encriptada SSL segura se implementa para proporcionar la funcionalidad de programas de un suministro de mensajes ordenado fiable. Dado que, sin embargo, en las redes móviles es necesario a menudo que se cierre y se vuelva a conectar (por ejemplo, cuando se conmuta de una conexión Wi-Fi a una 3G) la conexión TCP, el método inventivo implementa su propia capa de sesión, la capa de sesión 22 inventiva sobre la parte superior de la misma, que garantiza una conexión de sesión fiable en caso de desconexiones de transporte cortas. Sobre la parte superior de la misma, existe el protocolo de capas de aplicación 21 que proporciona una interfaz RPC al software. La capa de aplicación 21 se puede usar para diferentes clases de conexiones. Dentro del contexto inventivo de esta realización concreta, sin embargo, se usan preferiblemente conexiones de usuario.

La figura 2B (técnica anterior) es una representación según la figura 2A, pero sin la capa inventiva, proporcionada con el objetivo de clarificar. Toda comunicación entre capas se realiza directamente entre la capa de aplicación 21 y la capa de transporte 23, que produce las desventajas mencionadas anteriormente.

Con referencia adicional a las figuras 3 y 4, la gestión de conexiones del método inventivo, según una realización preferida del mismo, se describe con más detalle, cuando se aplica a teléfonos móviles y a un servidor de comunicación respectivo.

El método inventivo, cuando se efectúa entre clientes y servidor, crea y mantiene un canal de comunicación estable entre cada cliente y el servidor. El método inventivo ejemplifica la conexión TCP y usa características inventivas, como se describe más adelante, sobre la parte superior de la capa TCP para garantizar una sesión estable en caso de desconexiones de red.

La figura 3 es una representación esquemática de los principales componentes de gestión de conexiones lógicas 30, abreviados en la presente memoria también como CMC, implementados en el lugar del cliente según un uso preferido del método inventivo para comunicación telefónica móvil en el chip lógico de un teléfono móvil.

El componente de gestión de conexiones 30 de clientes se ejecuta en un cliente de telefonía móvil. El método inventivo, en lo que se refiere a la parte móvil, se implementa preferiblemente de modo transparente para el usuario y puede invocarse a través de una “app” dentro del teléfono móvil, en el que, en particular, la funcionalidad real “capa entrelazada” es completamente transparente para el usuario.

La capa de sesión de cliente 38 inventiva puede estar integrada en cualquier aplicación que se beneficiaría de una conexión estable, preferiblemente integrando bibliotecas de enlaces estáticos o dinámicos.

El componente CMC 30 inventivo se puede simbolizar como una capa de software y gestiona el acceso a las diferentes redes radioeléctricas tales como Bluetooth, Wi-Fi, redes de teléfonos móviles usando GSM, UMTS, LTE, etc. El componente CMC 30 inventivo crea y mantiene conexiones al servidor usando el método inventivo al asegurar que el cliente permanece conectado tanto como sea posible, y se vuelve a conectar de modo transparente cuando se pierde la conexión. Esta es la función básica de la parte inventiva del cliente.

A continuación, la gestión de conexiones según una realización preferida de la invención en el lado del cliente se describe con más detalle en lo que sigue:

en el lado del cliente, el componente CMC 30 inventivo incluye un componente de toma TCP 39 de la técnica anterior que es una toma permitida de TLS (seguridad de capa de transporte). Establece la conexión de red usando la interfaz de programación de aplicaciones (API) del dispositivo.

El gestor de redes inalámbricas 32 de la técnica anterior sigue la pista de los diferentes enlaces de datos disponibles (tales como GPRS, EDGE, UMTS, Wi-Fi, etc.), de su estado y de su ancho de banda disponible. Basándose en esta información y en las preferencias del usuario predefinidas, el gestor de redes inalámbricas 32 elige uno de ellos para ejemplificar un canal de datos entre el cliente y el servidor. El componente CMC 30 inventivo sigue la pista del estado de una conexión al servidor y también informa a otros componentes de la técnica anterior sobre posibles cambios de estado de la conexión.

El protocolo de redes 36 implementa una lógica de la técnica anterior que permite que otros módulos envíen y reciban mensajes de red.

El gestor de sesiones 34 de la técnica anterior gestiona el estado del inicio de sesión del usuario.

Todos los componentes 32, 34 y 36 han programado, respectivamente, interfaces funcionales entre sí y, en particular, para la capa de sesión 38 inventiva a fin de implementar el control de red particular según la invención.

La figura 4 es una representación según la figura 3, pero que muestra la situación en un servidor que presenta la funcionalidad de gestión de conexiones a una gran pluralidad de sesiones de red (usuarios finales) según la figura 3.

Los componentes CMC de servidor 40 inventivos se ejecutan en un ordenador servidor y gestionan todas las sesiones de red conectadas al sistema.

Un gestor de conexiones de usuarios de servidor, como es conocido a partir de la técnica anterior, interactúa con la capa de sesión 46 inventiva y gestiona los mensajes de red con el componente de protocolos de redes de servidor 44. La capa de sesión 46 inventiva interactúa con los componentes 42 y 44 mencionados anteriormente, así como con la capa de toma TCP 49, a través de interfaces funcionales respectivas. La capa de sesión 46 proporciona un soporte inventivo para traspasos y desconexiones de corta duración implementando una reconexión transparente cuando la desconexión permanece dentro del período de gracia mencionado anteriormente. La capa de sesión 46 inventiva proporciona colas de prioridad de mensajes y la detección robusta de clientes desconectados, en la que esta funcionalidad está implementada en su totalidad dentro del ámbito de los componentes CMC de servidor 40.

A continuación, con referencia adicional a las figuras 5, 6 y 7, se describe la funcionalidad inventiva como está implementada en los componentes de control 36 y 46 inventivos, mediante algún flujo de control, a modo de ejemplo, en el que la secuencia respectiva de etapas está determinada predominantemente por las capas de sesión 36 y 46 inventivas.

La figura 5 ilustra el flujo de control de las etapas más importantes de una realización preferida del método inventivo, que está implementado en la capa de sesión 38 inventiva de la figura 3 y el componente 46 de la figura 4.

Cuando un cliente se conecta al servidor, el cliente pasa por estados de conexión diferentes. La figura 5 muestra los estados y las transiciones posibles. Se debe señalar que este flujo representa también la secuencia de estados del cliente considerada desde el punto de vista del servidor.

En primer lugar, el cliente se conecta. Si no hay ninguna sesión activa, pasará por un proceso de inicio de sesión 510 estándar de la técnica anterior, en el que, después de una conexión de red exitosa, se verifican las credenciales. Cuando se reciben las credenciales válidas, el servidor genera un testigo de sesión (denominado también clave de sesión) que está compuesto por el id de usuario, el id de dispositivo y una marca horaria. Los tres datos están concatenados y los datos resultantes se resumen con una clave K secreta.

Tiempo_t_testigo_de_sesión = HMAC (id de usuario + id de dispositivo + marca horaria, K)

Después de una autenticación exitosa con un testigo o unas credenciales de sesión, el cliente entra en el estado “En línea” (denominado también de sesión iniciada) 520. En esta etapa, el servidor ve al cliente como ’en línea’ y el servidor informa a todos los usuarios conectados de su cambio de estado.

Con más detalle, tan pronto como el usuario empieza un inicio de sesión, una toma TCP se abre al servidor especificado. Una vez conectado, el cliente esperará a que se encripte la toma. A continuación, se intercambian las

órdenes de inicio de sesión. Tras un inicio de sesión exitoso, se almacena el testigo de sesión enviado por el servidor.

Con un enfoque más próximo a continuación de la presente invención, si el cliente pierde la conectividad en el estado en línea, véase la etapa 530, según una característica básica de la invención, no se considera inmediatamente que el cliente esté fuera de línea. En vez de eso, el canal de comunicación del cliente está controlado para pasar a un estado 'desconectado temporalmente', indicado con el signo de referencia 540 durante un corto período de tiempo que está predefinido, por ejemplo, para tener aproximadamente 20 segundos de duración. Ese período se denomina en la presente memoria "período de gracia".

En este estado 540, el punto extremo de comunicación mejorada de manera inventiva sigue estando conectado y la cola de mensajes respectiva está activa tanto en el cliente como en el servidor. Los componentes inventivos en el cliente y en el servidor cooperan entonces a fin de establecer de nuevo la conexión TCP subyacente usando el testigo de sesión que se generó antes, es decir, se vuelve a conectar el TCP, véase la etapa 570.

Con más detalle, cuando el cliente se vuelve a conectar usando este testigo de sesión, el servidor verifica la identidad del cliente volviendo a calcular la función de resumen y verificando que corresponde al testigo enviado por el cliente. La seguridad de autenticación basándose en un testigo de sesión está basada en una función de resumen que es una función de una vía. La propiedad de una función de una vía es que se puede calcular fácilmente en una dirección, pero no es factible invertirla de modo computacional. La ventaja de este modo de generar el testigo de sesión es que no es necesario almacenar el testigo para cada usuario, dado que se puede generar sobre la marcha. No se pierden datos en caso de que el servidor vuelva a comenzar.

Si esto se realiza con éxito durante el período de gracia de, p. ej., 20 segundos, se puede continuar una comunicación normal, como era antes de la interrupción temporal 570.

Si, sin embargo, no sucede ninguna reconexión durante el período de gracia, la conexión del cliente pasa en una etapa 550 al estado 'fuera de línea', indicado por el signo de referencia 560. Cuando se alcanza este estado en el cliente, el servidor deja libre la cola de espera del punto extremo y suprime todos los mensajes. El servidor informa también a todos los usuarios conectados del cambio de estado. El servidor mantiene válida la clave de sesión durante 20 minutos, de manera que el usuario no tiene que volver a introducir las credenciales cuando vuelve la red. Después de 20 minutos, la clave de sesión deja de ser válida, etapa 590.

La característica inventiva implementada en este contexto particular es que el estado de "Fuera de línea" 560 solamente se alcanza después del "período de gracia", es decir, para desconexiones significativas y, así, el cliente no oscilará demasiado entre 'en línea' y 'fuera de línea', como sucede de manera desventajosa en la técnica anterior.

Según una característica opcional de una realización adicional del método inventivo, el control inventivo puede estar configurado para moverse directamente al estado de fuera de línea 560, sin pasar por el período de gracia.

En el estado de fuera de línea 560, según una característica separada independiente de la característica mencionada anteriormente, la lógica inventiva del servidor mantiene abierta una sesión para este cliente durante una cantidad de tiempo más larga, tal como, a modo de ejemplo, de 20 minutos de duración. De esta manera, puede suceder un próximo reinicio de sesión usando el mismo ID de sesión que antes, una vez que la conexión está operativa de nuevo.

Con referencia a la etapa de reconexión 590, después de un reinicio de sesión exitoso usando el testigo de sesión, el punto extremo antiguo en el lado del cliente será destruido y la cola de mensajes inventiva, si está disponible, se transfiere a un nuevo punto extremo.

Más particularmente, cuando el cliente detecta la desconexión anteriormente mencionada o no puede restablecer rápidamente una conexión, trata activamente de restablecer una conexión al servidor. El cliente tratará siempre, después de volverse a conectar con éxito, de restablecer la sesión antigua y, si esto sucede, de enviar los mensajes no críticos en el tiempo que estaban en cola de espera.

A continuación, se describen con más detalle algunas características de la capa de sesión inventiva:

para la característica inventiva de detección de pérdida de conexión: se puede detectar una pérdida de conexión según el método inventivo evaluando ventajosamente un caso más que en la técnica anterior, es decir, cuando un mensaje no se pudo suministrar a tiempo, lo que es detectado por la capa de sesión inventiva.

Los casos de la técnica anterior son únicamente los siguientes:

- el tiempo de espera de mantener activo el TCP, visible en el control TCP real, y

- se perdió la conexión de red, visible en la capa de red/enlace.

La detección inventiva de pérdida de conexión proporciona, así, un beneficio adicional de la capa de sesión inventiva dado que asegura que un usuario desconectado será detectado como “desconectado”, incluso en caso de problemas con “mantener activo el TCP” que sucede frecuentemente con plataformas móviles debido al hecho de que el teléfono va “en reposo” y no reacciona a la desconexión.

Para la característica inventiva de un inicio de sesión/reinicio de sesión de usuario usando una clave de sesión, véase la etapa 580 anterior:

después de un inicio de sesión exitoso, en el que se han verificado con éxito las credenciales, el servidor crea un testigo de sesión para este usuario. Esto es conocido a partir de la técnica anterior.

Según la invención, un usuario será conocido para el sistema (servidor) durante una cantidad predeterminada de tiempo, que es suficientemente grande para permitir un buen grado de utilización. Se debe señalar que, esta vez, no hay necesidad de introducir credenciales y el cliente puede volverse a conectar sin la acción del usuario utilizando este testigo de sesión generado inicial y dinámicamente que se envía al cliente después de dicho primer inicio de sesión exitoso y que ya desde entonces se almacena en el cliente. Esta validez extendida de manera inventiva del mismo testigo de sesión permite que los clientes reinicien la sesión con este mismo testigo cuando se perdió la conexión (es decir, cambió la toma subyacente) sin tener que pedir al usuario que vuelva a introducir las credenciales de inicio de sesión. Esto ahorra tiempo y proporciona mucha más comodidad al usuario. De esta manera, esta característica es básicamente un procedimiento de reconexión automatizado que se puede realizar sin ninguna interacción del usuario.

Según una característica preferida de la presente invención, el servidor gestiona completamente las claves de sesión del usuario y los testigos de sesión únicamente se envían como una cadena al cliente, como es conocido de modo similar a partir de una galleta informática en el HTTP. Tal cadena de testigos de sesión contiene toda la información que el servidor necesita para identificar al usuario (msisdn e id de dispositivo), así como una fecha/tiempo de expiración de la sesión. La integridad de esta información está protegida a través de un código de autenticación de mensajes resumidos (HMAC) que es parte también del testigo de sesión. Esto permite que el servidor verifique fácilmente si es válido un testigo de sesión y si ha expirado o no la sesión sin tener que almacenar el testigo en el propio servidor.

La figura 6 es una representación esquemática suplementaria exhaustiva según la figura 5, que ilustra, junto con la figura 7, las diferencias del método inventivo con relación a la técnica anterior, que se muestra, a su vez, en la figura 7, y con el enfoque de la información temporal. Para el texto dentro de las figuras 6 y 7, se hace referencia a la descripción de la figura 5, a fin de evitar repeticiones.

Con respecto al ahorro de tiempo usando la presente invención, la siguiente información temporal, a modo de ejemplo, de la vida real se proporciona como sigue:

según el método inventivo, la desconexión de red está básicamente oculta para la aplicación y, así, se produce lo siguiente:

1) Cuando la aplicación se vuelve a conectar desde una desconexión corta (estado 'Desconectado temporalmente’) se necesitan las siguientes etapas:

1. i) crear la conexión de red y la toma TLS (de 1 a 3 segundos, dependiendo del teléfono)

2) El estado del cliente/aplicación no cambia dado que ya estaba “conectado”.

3) En caso de una desconexión corta:

3. i) se cierra la toma TCP (< 1 segundo)

En resumen, solamente se realiza la acción requerida en el nivel TCP, el resto es gestionado por la capa de sesión inventiva.

La figura 7 es una representación según la figura 6, pero sin implementación de las características inventivas. La información temporal, a modo de ejemplo, de la vida real se proporciona como sigue:

1) Cuando la aplicación se conecta por primera vez, dicha aplicación realiza un cierto número de etapas:

1. i) crear la conexión de red y la toma TLS (de 1 a 3 segundos, dependiendo del teléfono)

1. ii) iniciar la sesión para el servidor, verificando dicho servidor las credenciales (< 1 segundo, dependiendo del teléfono)

1. iii) enviar la información de presencia a ‘en línea’, que el servidor transfiere a continuación a todos los contactos (< 1 segundo, pero requiere mucha cantidad de CPU y lógica en el servidor y, también, esta etapa implica a otros usuarios)

2) Después de estas etapas, se considera que el cliente está listo o ‘conectado’, o ‘en línea’.

3) En caso de una desconexión corta, sin una iSL, sucede lo siguiente:

3. i) se cierra la toma TCP (< 1 segundo)

3. ii) el servidor informa a todos los otros usuarios sobre el nuevo estado de ‘fuera de línea’ (< 1 segundo, pero requiere CPU y lógica en el servidor)

3. iii) la aplicación informa al usuario de que dicha aplicación está ‘fuera de línea’ (< 1 segundo, pero implica al usuario)

3. iv) se cierra la llamada y se inutilizan todos los otros canales de comunicación (chat) (de 1 a 2 segundos).

4) Cuando se hace esto, la aplicación está fuera de línea y está lista para volverse a conectar tan pronto como vuelva la red.

Un experto en la técnica apreciará que las interrupciones de red que ocurren frecuentemente dan como resultado únicamente una desconexión temporal del cliente móvil al servidor. De esta manera, a fin de volverse a conectar, el cliente desconectado da vueltas dentro del círculo 60 más pequeño, véase en la figura 6 impreso en líneas discontinuas, y no en el círculo que consume tiempo 70 de la técnica anterior, véase en la figura 7 impreso en líneas discontinuas. Como se pone de manifiesto a partir de la descripción de las figuras 5, 6 y 7, las capas de sesión 38 y 46 inventivas, respectivamente, proporcionan propiedades de elasticidad a las condiciones de red variables y hacen posible proporcionar una alta calidad de servicio al usuario, dado que se pueden compensar las interrupciones cortas de conectividad o las caídas de calidad.

A continuación, la característica inventiva separada de las colas de mensajes de red se describe con más detalle. Las colas de espera se implementan tanto en el cliente como en el servidor.

Una circunstancia implicada en la característica mencionada anteriormente de implementar dicho período de gracia dentro de la capa de sesión inventiva es que algunos mensajes son válidos solamente cuando se suministran en tiempo real. Para gestionar esta circunstancia de manera adecuada, la capa de sesión inventiva proporciona un soporte de diferentes clases de mensajes con diferentes prioridades respectivas.

Los mensajes que se deben suministrar en tiempo real (denominados críticos en el tiempo) se suprimen según la invención durante dicho período de gracia. Por ejemplo, en el caso de una aplicación de Voz sobre IP (VoIP), que obtiene beneficio de la invención implementando la capa de sesión inventiva en un teléfono móvil inteligente, y un servidor VoIP, un mensaje crítico en el tiempo sería una petición para hacer una llamada. Los mensajes no críticos en el tiempo se mantienen en una cola de espera interna a transmitir en caso de una reconexión exitosa. Los ejemplos de mensajes no críticos en el tiempo son mensajes de chat o actualizaciones de presencia.

Según una característica adicional preferida de la invención, que es en particular de valor práctico, el método de control inventivo distingue entre tres prioridades de mensaje: mensajes críticos en el tiempo, no críticos en el tiempo y directos.

Los mensajes críticos en el tiempo no se suministrarán si se tarda más tiempo que un valor dado de tiempo de espera. Un valor razonable de tiempo de espera para una aplicación VoIP, que no iniciará una acción con demasiado retardo, ni tampoco ninguna desconexión falsamente detectada en redes lentas, sería alrededor de 5 segundos.

Los mensajes no críticos en el tiempo se pondrán en cola de espera indefinidamente y se suministrarán después de la reconexión.

Los mensajes directos no se pondrán en cola de espera en absoluto y se usan principalmente durante el procedimiento de inicio de sesión para evitar la cola de espera mientras que el usuario no haya iniciado la sesión. Las colas de espera se asignan a los puntos extremos basándose en el usuario y el dispositivo, por consiguiente, no puede haber una cola de espera sin que esté autenticado el usuario.

La distinción entre mensajes directos y otros mensajes está incluida en el encabezamiento de mensaje (véase también la figura 8), puesto que se tiene que tratar de modo distinto cuando la recibe la capa iSL. No se reconoce un mensaje directo. Se reconocen otros mensajes.

La prioridad de un mensaje no directo (crítico en el tiempo o no crítico en el tiempo) está definida solamente por el lugar en el que el mensaje se pone en cola de espera. No se porta en el encabezamiento de mensaje.

La figura 8 es una representación esquemática de lugares de almacenamiento en un encabezamiento de mensaje utilizado por la presente invención.

El campo de encabezamientos inventivo tiene, por ejemplo, 10 *bytes* de largo.

El campo de almacenamiento 82 indica el tipo de mensaje. Tiene 2 *bytes* de largo.

El campo de almacenamiento 84 contiene el número de secuencia, 4 *bytes*, como en la técnica anterior.

El campo de almacenamiento 86 contiene la longitud de bloque, 4 *bytes*, como en la técnica anterior.

El campo de almacenamiento 88 contiene la carga útil, como en la técnica anterior.

1) El tipo de mensaje almacenado en el campo 82 dice a la capa de sesión inventiva (iSL) qué mensaje se está recibiendo. Podría ser cualquiera de los siguientes:

- Un reconocimiento. En este caso, la cola de prioridad de mensajes se actualiza como se explica en la figura 9.
- Un mensaje. En este caso, la iSL envía de vuelta un reconocimiento y el mensaje se hace pasar a la capa de aplicación para ser tratado.
- Un mensaje directo. No se envía ningún reconocimiento y el mensaje se hace pasar a la capa de aplicación para ser tratado.
- Un mensaje de sincronización. Este se envía cuando se crea una nueva toma y se debe sincronizar el número de secuencia.

2) El número de secuencia almacenado en el campo 84 es un número exclusivo incremental para cada mensaje.

3) La longitud de bloque almacenada en el campo 86 es la longitud del mensaje.

4) La carga útil almacenada en el campo 88 comprende el propio mensaje.

Se debe señalar que la iSL tiene cuidado solamente de las colas de reconocimiento y prioridad. El análisis sintáctico del mensaje se realiza en la capa de aplicación.

La figura 9 es una ilustración esquemática del método inventivo de cómo funcionan las colas de prioridad. Las colas de prioridad se usan en el lado de envío de la capa iSL, es decir, en el cliente cuando envía un mensaje al servidor, y en el servidor cuando envía un mensaje a un cliente.

Con referencia a la figura 9, esta figura gestiona el problema de saber qué mensaje ya se ha enviado y recibido y qué mensaje se tendrá que reenviar después de una reconexión exitosa.

La flecha 92 indica una lista de mensajes mostrada en la fila superior, dispuestos por un número de secuencia mostrado en la fila inferior. Se tienen que enviar los mensajes. En esta etapa, se supone que el usuario (o aplicación de cliente) pierde la conexión. La situación en la que se ha perdido la conexión se representa por la flecha 94.

Entre ambas situaciones 92 y 94, si no existiera un reconocimiento inventivo mediante la capa iSL inventiva, no se sabría qué mensaje se envió y qué mensaje no se envió. En una aplicación VoIP, la consecuencia que percibe el usuario sería que los mensajes se perderían o se enviarían más de una vez. Con más detalle, la capa de sesión inventiva mantiene en una cola de espera todos los mensajes no críticos en el tiempo. En caso de desconexión y reconexión cortas, se reenvían los mensajes que no se reconocen. Sin la capa de sesión inventiva, los mensajes probablemente se suprimirían y se perderían. Sin el mecanismo de reconocimiento inventivo, los mensajes se reenviarían (duplicarían).

El método inventivo, implementado en la capa de sesión inventiva, proporciona tal mecanismo:

los mensajes se ponen en cola de espera y se asigna a los mismos un número de secuencia. Se procesan primero como “esperando al reconocimiento”, que se representa por un pequeño reloj de arena debajo del mensaje. Suponiendo que el remitente (usuario A) envía un mensaje M al usuario B. La capa de sesión inventiva del usuario B lo recibirá y lo reconocerá. Cuando el Usuario A recibe el reconocimiento para este mensaje, se reconocerán todos los mensajes con números de secuencia más pequeños. Los mensajes reconocidos se eliminan de la cola de espera periódicamente, una vez recibido el reconocimiento desde el otro lado.

En caso de desconexión, se reenviará el mensaje no reconocido y se eliminará el mensaje reconocido. Esta situación se ilustra por la flecha 96.

En otras palabras, y con más detalle, según una implementación preferida, cada mensaje enviado a la toma es aumentado con un número de secuencia y un campo de reconocimiento. Cuando se envía con éxito un mensaje, se reconoce y se puede eliminar, así, de esta “cola de mensajes”.

No se ponen en cola de espera los mensajes con prioridad directa.

A continuación, el envío, la recepción y el reenvío de mensajes se describen según esa característica inventiva:

enviar un mensaje, implementado en el servidor y en el cliente:

cuando la capa de sesión inventiva envía un mensaje, lo añadirá a una de las colas de espera, excepto para los mensajes directos. A continuación, el mensaje se escribe en la toma subyacente.

Recibir un mensaje:

cuando la capa de control inventiva lee un bloque de datos de la toma, verifica el encabezamiento para ver si es un reconocimiento o un mensaje.

Si es un reconocimiento, la capa de sesión inventiva marcará todos los mensajes con un número de secuencia más pequeño como reconocidos y eliminará el mensaje reconocido de la cola de mensajes.

Si es un mensaje, la capa de sesión inventiva recordará emitir un reconocimiento en el siguiente latido ("heartbeat"). El mecanismo de latidos está implementado para una optimización temporal a fin de evitar que se envíe un reconocimiento para cada mensaje recibido.

"Latido":

un latido está implementado en la capa inventiva. El latido según la invención tiene dos objetivos especiales:

1. Emitir reconocimientos del último número de secuencia recibido (si está en espera uno) y

2. Verificar los tiempos de espera.

De esta manera, tal implementación de latidos asegura que el último mensaje entrante se reconoce tan pronto como sea posible para el remitente, y la capa de sesión trata esos mensajes críticos en el tiempo de modo privilegiado.

Reenviar mensajes:

cuando un cliente inventivo hace gestiones para volver a conectarse, se envía una orden a las colas de espera para que reenvíen todos los mensajes no reconocidos que no han acabado el tiempo de espera.

De esta manera, la cola de mensajes se puede procesar más rápido que en la técnica anterior, en la que sería necesario un reinicio de sesión.

Para las prioridades de mensajes de red, como están implementadas en el lado del cliente, existe solamente un ejemplo de punto extremo que está activo mientras se ejecuta el software. Este punto extremo se usa durante la fase de inicio de sesión para enviar mensajes de inicio de sesión y para la comunicación de protocolos normales a continuación. Según la invención, su cola de mensaje subyacente se deja libre solamente en una finalización de sesión explícita, es decir, en la destrucción de la sesión.

Además, algunas definiciones y parámetros temporales, a modo de ejemplo, utilizables por el método inventivo, en este caso para una aplicación VoIP, se proporcionan a continuación en lo que sigue:

- El intervalo entre latidos (5 s): un latido para el tiempo de espera y el reconocimiento.
- El "Período de gracia de desconexión" (20 s): un período hasta que un dispositivo del punto extremo desconectado se establece en FUERA DE LÍNEA, denominado período de gracia.
- El Tiempo de espera de sesión (20 min): un período durante el que está activa la sesión.
- El Tiempo de espera de inicio de sesión (10 min): un período después del que será desconectado un punto extremo utilizado para el inicio de sesión, si no sucede ningún inicio de sesión exitoso en ese tiempo.
- Una toma TCP de la técnica anterior se mantiene en el estado "conectado" durante aproximadamente 10 segundos, a modo de ejemplo, según esta realización inventiva.

El método inventivo se puede modificar en diversos aspectos: el período de gracia se puede implementar en el lado del servidor y en el lado del cliente o en el lado del servidor solamente. En la implementación práctica de la invención, el período de gracia se calcula solamente en el servidor. Cuando el período de gracia de un cliente acaba, digamos un cliente, denominado cliente A, el servidor envía un mensaje a todos los otros clientes de que el cliente A está fuera de línea. Estos otros clientes ven al cliente A como fuera de línea. En el lado del cliente A, el cliente móvil trata continuamente de volver a conectarse independientemente del período de gracia.

Se propone también tener el período de gracia implementado en el cliente A y activar algunas acciones cuando acaba el período de gracia. Tal acción puede ser informar al usuario o detener la reconexión.

La longitud del período de gracia y otros parámetros temporales se pueden modificar para adaptarse a la aplicación. En la realización mencionada anteriormente del método y el caso de uso inventivos para comunicación móvil, se eligieron los 20 segundos puesto que corresponde al tiempo necesario para el traspaso de redes.

Es posible usar el mismo mecanismo en cualquier capa de transporte. Estará funcionando con el UDP solamente con una ligera modificación. Según un aspecto adicional de la invención, se propone poner en cola de espera los paquetes UDP durante el período de gracia y enviarlos de nuevo cuando vuelve la conexión, aunque esto tendría sentido solamente para paquetes en “tiempo no real”. La ligera modificación sería para adaptarse al hecho de que el UDP no es un transporte fiable y se podrían perder algunos paquetes. Por ejemplo, no podría basarse en un reconocimiento para dejar caer la conexión.

Además, el mecanismo de colas de prioridad se puede extender a más de una prioridad.

Teniendo en cuenta la descripción anterior, un experto en la técnica apreciará que, considerado desde un punto de vista práctico del usuario, existen tipos de mensaje diferentes que se pueden asociar con las propiedades de prioridad mencionadas anteriormente.

Se puede resumir el método inventivo para proporcionar:

a) un grado configurable de fiabilidad para mensajes adaptados al uso móvil añadidos sobre la parte superior de las conexiones TCP a través de diversas capas de hardware subyacentes, dado que la ordenación básica y la fiabilidad (limitada) son proporcionadas por el TCP,

b) una optimización que usa los testigos de sesión anteriormente mencionados para reducir la sobrecarga de un inicio de sesión completo,

c) mensajes en tiempo real para servir a las necesidades específicas de aplicaciones en tiempo real, tales como VoIP.

El aspecto anterior bajo el apartado b) se podría implementar con seguridad independientemente, mientras que el aspecto bajo el apartado c) es una prolongación del aspecto del apartado a).

La presente invención se puede realizar en hardware, software o una combinación de hardware y software. Una herramienta según la presente invención se puede realizar de forma centralizada en un sistema de ordenador servidor, o de forma distribuida en la que elementos diferentes están distribuidos a través de varios sistemas informáticos interconectados, en particular teléfonos inteligentes. Es adecuada cualquier clase de sistema informático u otro aparato adaptado para llevar a cabo los métodos descritos en la presente memoria. Una combinación típica de hardware y software podría ser un sistema informático de uso general con un programa informático que, cuando se está cargando y ejecutando, controla el sistema informático de manera que lleva a cabo los métodos descritos en la presente memoria.

Los recursos de hardware de almacenamiento permanente mencionados en la presente memoria, tales como unidades de disco duro, o dispositivos ópticos, o magnetoópticos tales como discos compactos, o Discos versátiles digitales (DVD), o dispositivos ROM Flash, son, en general, de uso intercambiable, a menos que se especifique explícitamente de modo distinto. De esta manera, para la mayoría de los objetivos de almacenamiento, se puede usar un dispositivo de almacenamiento permanente no volátil, tal como se ha mencionado anteriormente, cuando el sistema informático en cuestión no tiene ninguna dedicación o relación especial para usarse como un sistema portátil o adaptable al bolsillo. Entonces, por supuesto, en ausencia de una unidad de disco duro, se prefiere un dispositivo de almacenamiento FLASH-ROM.

Una memoria volátil se usa, de modo general, para almacenar temporalmente programas o datos y, en particular, para cargar programas o submódulos de programa, y para el intercambio inmediato de datos con la Unidad central de procesamiento (CPU) de un ordenador.

La presente invención puede estar también embebida en un producto de programa informático, que comprende todas las características que permiten la implementación de los métodos descritos en la presente memoria y que, cuando está cargado en un sistema informático, es capaz de llevar a cabo estos métodos.

Medios de programa informático o programa informático, en el presente contexto, significan cualquier expresión, en cualquier lenguaje, código o notación, de un conjunto de instrucciones destinadas a hacer que un sistema tenga una capacidad de procesamiento de información para realizar una función particular directamente o después de cualquiera o ambos de las siguientes:

a) conversión a otro lenguaje, código o notación;

b) reproducción en una forma material diferente.

Lista de signos de referencia:

10 Internet

12 teléfono móvil, hardware y software

14 servidor de comunicación móvil, hardware + software

20 apilamiento de capas

21 capa de aplicación

22 capa de control inventiva

23 capa de transporte

24 capa de red

30 componentes de gestión de conexiones de clientes

32 gestor de redes inalámbricas

34 gestor de sesiones

36 control de protocolo de redes de cliente

38 capa de control inventiva de clientes

39 toma TCP de clientes

40 componentes de gestión de conexiones de servidor

42 gestor de conexiones de usuarios de servidor

44 control de protocolo de redes de servidor

46 capa de control inventiva de servidores

49 toma TCP de servidores

Etapas de la realización del método inventivo en el cliente:

510 conectando

520 *login*, inicio de sesión

530 estado de sesión iniciada

540 la red está interrumpida, perdiendo conectividad

550 la desconexión-conexión está interrumpida temporalmente

560 volviendo a conectar (mismo testigo de sesión)

570 el servidor finaliza la sesión al cliente

580 estado de sesión finalizada

585 terminar la sesión

590 reiniciar la sesión y volver a conectarse con las mismas credenciales y la misma clave de sesión

60: bucle más rápido de etapas según la invención

70: bucle más lento de etapas según la técnica anterior

92, 94, 96: flechas que representan información del estado de colas de espera diferentes en situaciones diferentes conectada, o no, o conectada de nuevo respectivas

REIVINDICACIONES

1. Un método, implementado en un ordenador servidor (14), para efectuar una comunicación bajo inclusión de una capa de transporte de red (10), preferiblemente el protocolo TCP-IP, entre al menos un primer dispositivo de comunicación (12) y un segundo dispositivo de comunicación (12), que incluye un procedimiento de autenticación de usuario inicial (510), en el que al menos dicho ordenador servidor (14) controla dicha comunicación proporcionando una conexión entre dichos dispositivos de comunicación primero y segundo, en el que dicha comunicación se extiende a través de las fronteras de red o hace frente a repetidas desconexiones de red debidas a inestabilidades de red técnicas,

caracterizado por las etapas de:

a) generar una sesión que está basada en datos de autenticación de usuario reconocido y se asocia con dicha comunicación tan pronto como se ha establecido con éxito una conexión entre dicho ordenador servidor (14) y un cliente (12),

b) mantener (60) válida dicha sesión a pesar de dichas desconexiones de red durante un período de gracia predeterminado, en el que dicho período de gracia está predefinido para ser suficientemente grande a fin de soportar un traspaso intrarredes o una desconexión temporal debida a la inestabilidad de red,

c) en el que los mensajes se definen como “críticos en el tiempo” y como “no críticos en el tiempo”,

d) y dicho ordenador servidor (14) mantiene (60) operativa dicha sesión para dichos mensajes no críticos en el tiempo durante dicho período de gracia predeterminado, y en el que dichos mensajes no críticos en el tiempo se ponen en cola de espera durante dicho período de gracia,

e) en el que dichos mensajes críticos en el tiempo se suprimen de una cola de mensajes después de un valor dado del tiempo de espera durante dicho período de gracia.

2. El método según la reivindicación 1, en el que las etapas de la reivindicación 1 las realiza una capa de software de servidor (22, 46) adicional que actúa como capa de sesión sobre la parte superior del TCP.

3. El método según la reivindicación precedente, en el que se definen adicionalmente mensajes “directos” para los mensajes enviados durante el procedimiento de autenticación de usuario o de inicio de sesión, en el que dichos mensajes “directos” no se ponen en cola de espera a fin de evitar una cola de mensajes existente.

4. El método según la reivindicación 1, en el que dicho servidor (14) verifica una desconexión de la toma TCP para uno de dichos dispositivos móviles y, si se detecta una desconexión, cierra la toma TCP en espera respectiva.

5. El método según la reivindicación 2, en el que dicha capa de sesión (46) adicional se implementa entre una capa de aplicación (21) y dicha capa TCP (23), y en el que las llamadas a procedimientos remotos (RPC) de dicha capa de aplicación se usan para invocar actividades de dicha capa de sesión (46) adicional.

6. El método según la reivindicación 1, utilizado para una aplicación de “Voz sobre IP” en tiempo real, en el que dicho período de gracia se preestablece en aproximadamente 20 segundos y el valor del tiempo de espera para los mensajes críticos en el tiempo se preestablece en aproximadamente 5 segundos.

7. Un método, implementado en un dispositivo de comunicación de cliente (12), particularmente un teléfono móvil, para efectuar una comunicación bajo inclusión de una capa de transporte de red (10), preferiblemente el protocolo TCP-IP, entre al menos dicho dispositivo de comunicación de cliente (12) y un segundo dispositivo de comunicación (12), que incluye un procedimiento de autenticación de usuario inicial (510), en el que al menos un ordenador servidor (14) controla dicha comunicación proporcionando una conexión entre dichos dispositivos de comunicación primero y segundo, en el que dicha comunicación se extiende a través de las fronteras de red o hace frente a repetidas desconexiones de red debidas a inestabilidades de red técnicas,

caracterizado por las etapas de:

a) generar una sesión que está basada en datos de autenticación de usuario reconocido y se asocia con dicha comunicación tan pronto como se ha establecido con éxito una conexión entre dicho ordenador servidor (14) y dicho dispositivo de comunicación de cliente (12),

b) mantener (60) válida dicha sesión a pesar de dichas desconexiones de red durante un período de gracia predeterminado, en el que dicho período de gracia está predefinido para ser suficientemente grande a fin de soportar un traspaso intrarredes o una desconexión temporal debida a la inestabilidad de red,

c) en el que los mensajes se definen como “críticos en el tiempo” y como “no críticos en el tiempo”,

d) en el que dichos mensajes críticos en el tiempo se suprimen de una cola de mensajes después de un valor dado del tiempo de espera durante dicho período de gracia,

e) notificándose al dispositivo de comunicación de cliente (12) sobre el fallo de suministro de dicho mensaje crítico en el tiempo.

8. El método según la reivindicación 7, en el que las etapas de la reivindicación 7 las realiza una capa de software de cliente (22, 38) adicional que actúa como capa de sesión sobre la parte superior del TCP.

9. El método según la reivindicación precedente, en el que se definen adicionalmente mensajes “directos” para los mensajes enviados durante el procedimiento de autenticación de usuario o de inicio de sesión, en el que dichos mensajes “directos” no se ponen en cola de espera a fin de evitar una cola de mensajes existente.

10. El método según la reivindicación 7, en el que dicho dispositivo de cliente (12) verifica una desconexión de la toma TCP para uno de dichos dispositivos móviles y, si se detecta una desconexión, cierra la toma TCP en espera respectiva.

11. El método según la reivindicación 7, en el que dicha capa de sesión (22, 38) adicional se implementa entre una capa de aplicación (21) y dicha capa TCP (23), y en el que las llamadas a procedimientos remotos (RPC) de dicha capa de aplicación se usan para invocar actividades de dicha capa de sesión (46) adicional.

12. El método según la reivindicación 7, utilizado para una aplicación de “Voz sobre IP” en tiempo real, en el que dicho período de gracia se preestablece en aproximadamente 20 segundos y el valor del tiempo de espera para los mensajes críticos en el tiempo se preestablece en aproximadamente 5 segundos.

13. Un sistema de ordenador servidor que tiene un componente funcional (40) que se programa para realizar las etapas de un método según una de las reivindicaciones 1 a 6 precedentes.

14. Un sistema informático móvil, preferiblemente un teléfono móvil que tiene un componente funcional (30) que se programa para realizar las etapas de un método según una de las reivindicaciones 7 a 12 precedentes.

15. Un programa informático para su ejecución en un sistema de procesamiento de datos, que comprende un componente funcional para realizar las etapas respectivas del método según una de las reivindicaciones 1 a 12 precedentes, cuando dicho programa informático se ejecuta en un ordenador servidor (14) o un dispositivo informático móvil (12).

16. Un producto de programa informático almacenado en un soporte utilizable por ordenador, que comprende medios de programa legibles por ordenador que incluyen un componente funcional para hacer que un ordenador realice las etapas del método según una de las reivindicaciones 1 a 12 precedentes, cuando dicho programa informático se ejecuta en un ordenador servidor (14) o un dispositivo informático móvil (12), cuando se ejecuta dicho producto de programa informático.

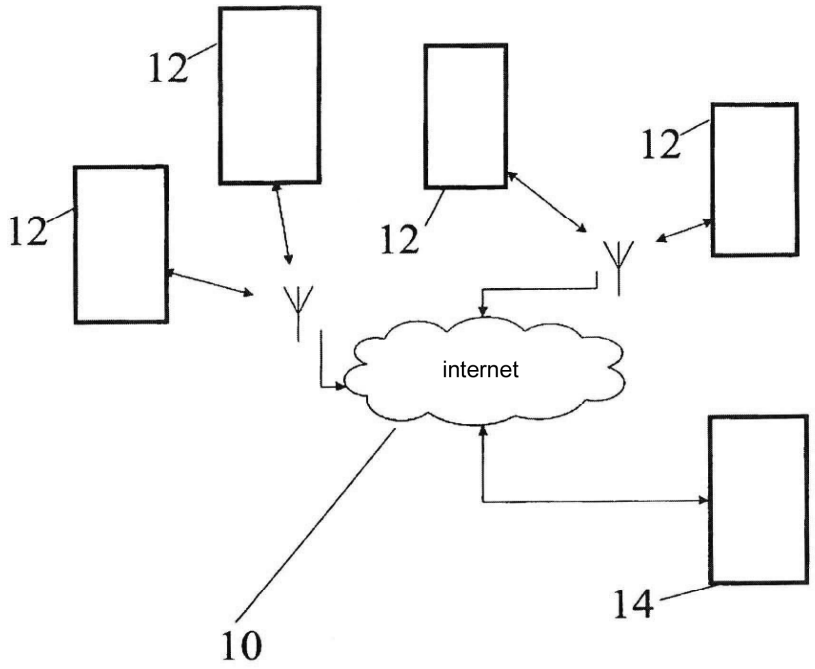


FIG. 1

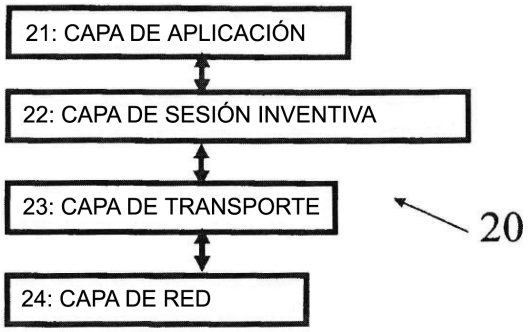
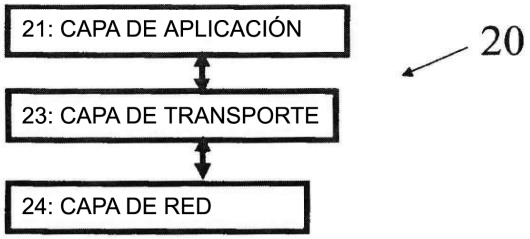


FIG. 2A



TÉCNICA ANTERIOR

FIG. 2B

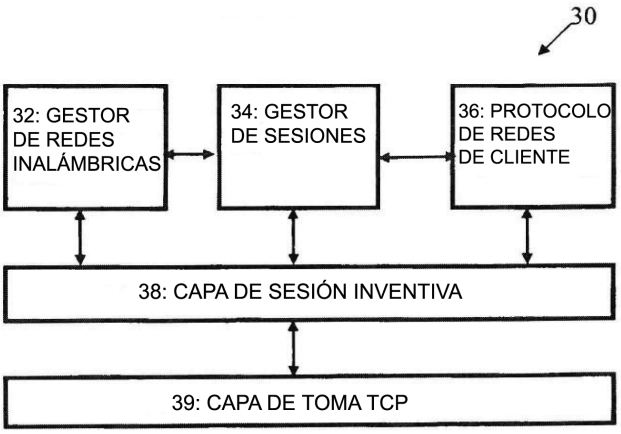

30
32: GESTOR DE REDES INALÁMBRICAS
34: GESTOR DE SESIONES
36: PROTOCOLO DE REDES DE CLIENTE
38: CAPA DE SESIÓN INVENTIVA
39: CAPA DE TOMA TCP

FIG. 3

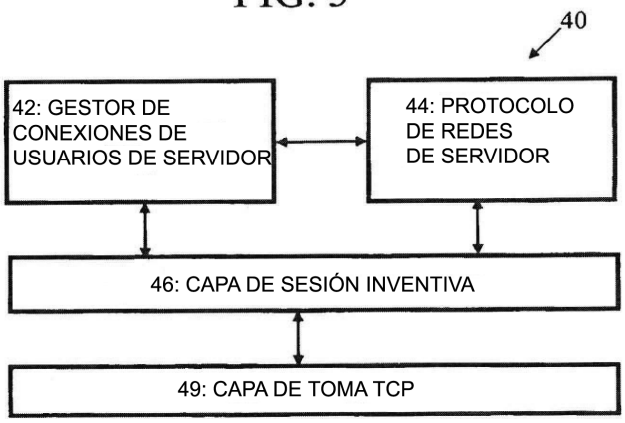

40
42: GESTOR DE CONEXIONES DE USUARIOS DE SERVIDOR
44: PROTOCOLO DE REDES DE SERVIDOR
46: CAPA DE SESIÓN INVENTIVA
49: CAPA DE TOMA TCP

FIG. 4

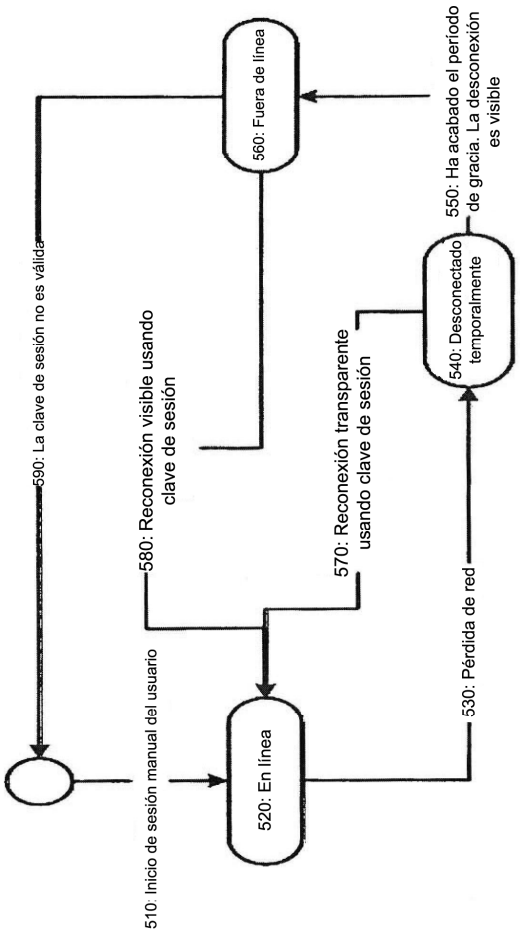

590: La clave de sesión no es válida
560: Fuera de línea
550: Ha acabado el periodo de gracia. La desconexión es visible
580: Reconexión visible usando clave de sesión
540: Desconectado temporalmente
570: Reconexión transparente usando clave de sesión
510: Inicio de sesión manual del usuario
520: En línea
530: Pérdida de red

FIG. 5

Con período de gracia

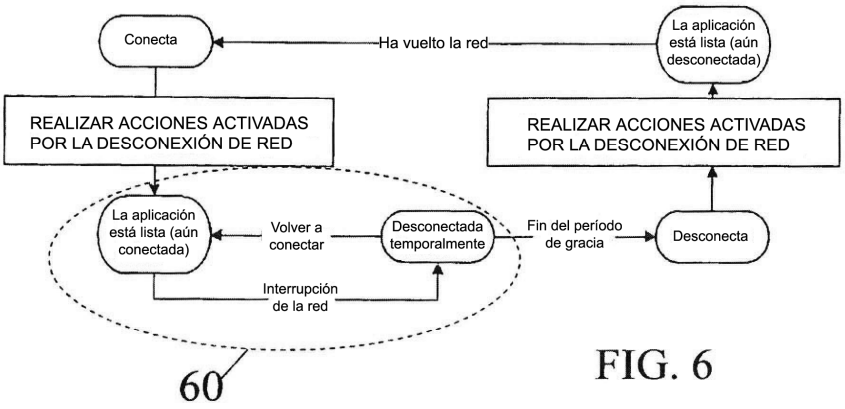


FIG. 6

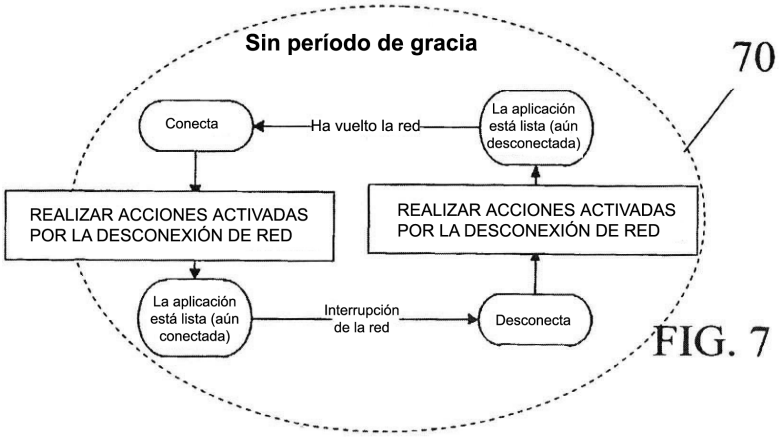


FIG. 7

TÉCNICA ANTERIOR

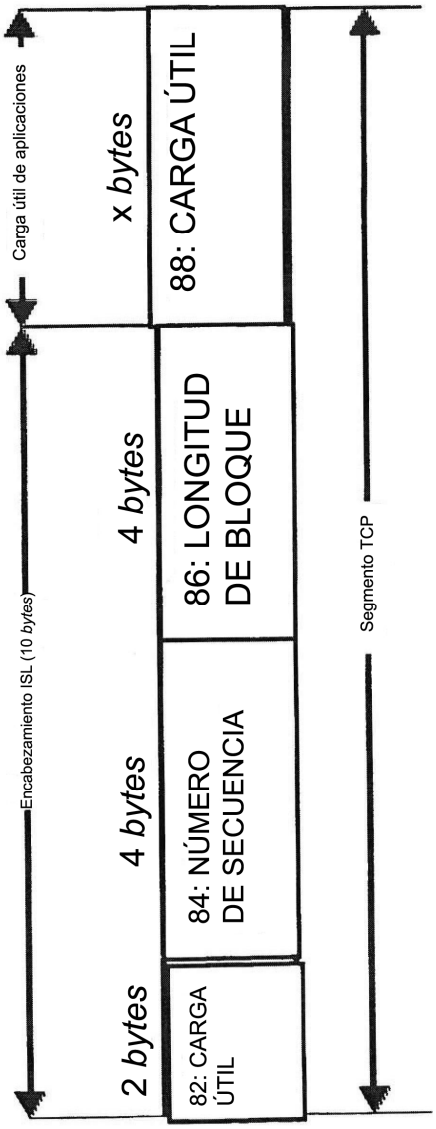

Carga útil de aplicaciones
x bytes
88: CARGA ÚTIL
Encabezamiento ISL (10 bytes)
4 bytes
86: LONGITUD DE BLOQUE
4 bytes
84: NÚMERO DE SECUENCIA
2 bytes
82: CARGA ÚTIL
Segmento TCP

FIG. 8

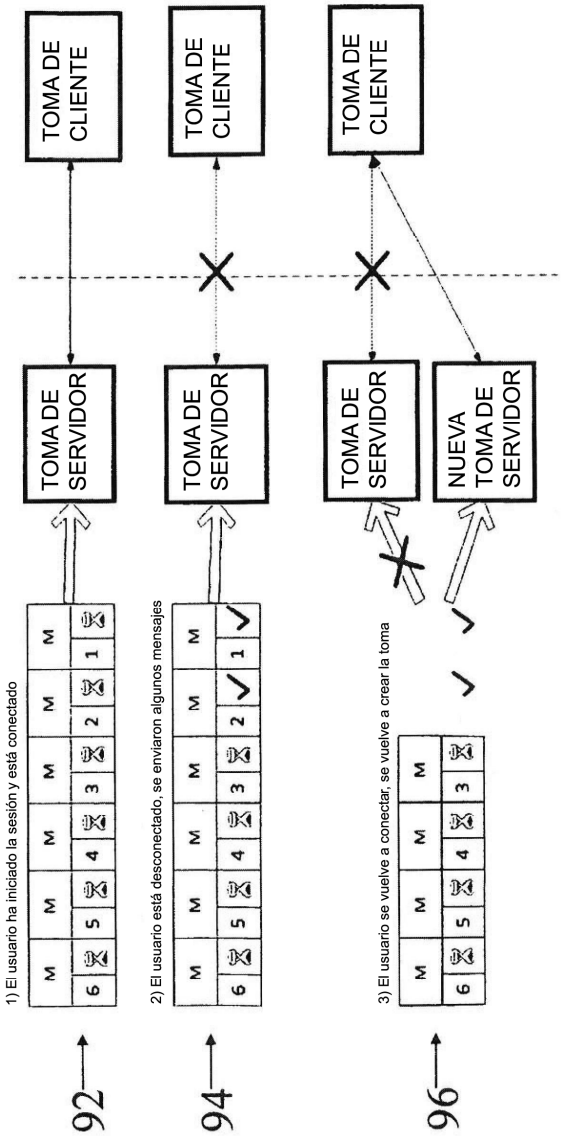

TOMA DE CLIENTE
TOMA DE CLIENTE
TOMA DE CLIENTE
TOMA DE SERVIDOR
TOMA DE SERVIDOR
TOMA DE SERVIDOR
NUEVA TOMA DE SERVIDOR
1) El usuario ha iniciado la sesión y está conectado
2) El usuario está desconectado, se enviaron algunos mensajes
3) El usuario se vuelve a conectar, se vuelve a crear la toma
92
94
96

FIG. 9