



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 269 821**

51 Int. Cl.:
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **02803742 .2**
86 Fecha de presentación : **07.11.2002**
87 Número de publicación de la solicitud: **1446934**
87 Fecha de publicación de la solicitud: **18.08.2004**

54 Título: **Procedimiento para establecer una conexión de telecomunicación y una red de telecomunicación.**

30 Prioridad: **20.11.2001 DE 101 56 572**
11.12.2001 DE 101 60 766
24.06.2002 DE 102 28 209

45 Fecha de publicación de la mención BOPI:
01.04.2007

45 Fecha de la publicación del folleto de la patente:
01.04.2007

73 Titular/es: **IP2H AG.**
Hofweg 11
3013 Bern, CH

72 Inventor/es: **Bergmann, Ansgar;**
Schenke, Andreas;
Gösele, Bernd;
Lorang, Martin;
Eigler, Karl y
Witthaut, Thomas

74 Agente: **Roeb Díaz-Álvarez, María**

ES 2 269 821 T3

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

Procedimiento para establecer una conexión de telecomunicación y una red de telecomunicación.

La presente invención se refiere a un procedimiento para establecer una conexión de telecomunicación entre un primer y un segundo abonado en una red de telecomunicación, en particular, entre dos equipos adecuados para la comunicación pudiendo asignarse direcciones a los abonados. Además, la presente invención se refiere a una red de telecomunicación para establecer una conexión de telecomunicación entre un primer y un segundo abonado, en particular, entre dos equipos adecuados para la comunicación, pudiendo asignarse direcciones a los abonados.

Por el documento US-A-5790548 se conoce un procedimiento en el que se asigna una sola dirección. El abonado tiene la posibilidad de rechazar direcciones asignadas en caso de que recibiera varias direcciones cuando varias unidades de comunicación están online. La correlación de una dirección a un abonado se dificulta mediante la codificación de la dirección al enviarla al abonado.

En redes de telecomunicación conocidas se usan direcciones y/o identificaciones para establecer una conexión de telecomunicación y para el encaminado (*routing*). Por el concepto "encaminado" podría entenderse aquí la funcionalidad de transmitir informaciones de un nodo de red a otro nodo de red en la red de telecomunicación, en caso necesario a través de nodos intermedios.

En las redes de telecomunicación conocidas, las direcciones y/o identificaciones se transmiten en texto claro. Las direcciones pueden estar asignadas a abonados o a equipos. Por ejemplo, se usan direcciones IP, que son específicas para el abonado o específicas para el equipo. Además, se usan direcciones Ethernet, que son específicas para el equipo. Las direcciones son fundamentales al establecer una conexión de telecomunicación entre dos abonados o entre dos equipos adecuados para la comunicación.

Las redes de telecomunicación son típicamente al menos en parte públicas, en el sentido de que los nodos de red de las redes de telecomunicación son accesibles para un gran grupo de personas no controlable. Aquí existen en gran medida posibilidades para explotar distintos nodos de red de forma adecuada, proveerlos de funciones, configurarlos y/o manipularlos.

La transmisión de direcciones y/o identificaciones que pueden ser asignadas a abonados o equipos y que habitualmente se realiza de forma no codificada permite una serie de ataques a la seguridad de los abonados o usuarios o contribuye fundamentalmente a ataques de este tipo. Aquí son pensables los siguientes ataques:

(a) Localización: un atacante puede controlar corrientes de datos y deducir el lugar en el que se encuentra un abonado o usuario. El atacante puede enviar mensajes dirigidas a una dirección del abonado o usuario con el fin de la localización, a los que el nodo de red del abonado o usuario contesta automáticamente según protocolo después de la recepción.

(b) Rastreo (*tracing*): Según el procedimiento descrito bajo (a), un atacante puede seguir el movimiento de un abonado o usuario.

(c) Las corrientes de datos asignadas al abonado o usuario pueden ser identificadas como tales y ser atacadas de forma selectiva, por ejemplo, con el fin de

desviar, borrar, falsificar o interceptar.

(d) Pueden generarse mensajes falsificados dirigidos al abonado o usuario.

Los procedimientos de seguridad usados y/o conocidos hasta ahora son adecuados para proteger los datos útiles del usuario. Se aplican procedimientos de codificación, de protección de la integridad y/o de la autenticación. No obstante, sigue sin estar codificada la información acerca de la dirección y/o identificación. Eventualmente se consigue autenticar las direcciones y/o identificaciones y proteger la integridad, aunque esto sólo puede ser comprobado por los puntos finales de la conexión de telecomunicación, puesto que para ello debe intercambiarse una llamada asociación de seguridad ("*Security association*").

No obstante, el resultado es que siguen siendo posibles los ataques descritos bajo (a) y (b) facilitándose los ataques descritos bajo (c) y (d).

Para dejarlo más claro, podría existir el siguiente escenario de ataque: un usuario tiene un PDA, asistente personal digital (*Personal Digital Assistant*), con tarjeta WLAN. Esta tarjeta WLAN tiene una dirección Ethernet fija, que se emite según protocolo automáticamente de forma repetida en texto claro. Asimismo es posible provocar con mensajes adecuados que el PDA envíe automáticamente la dirección IP. Con ello, el atacante puede localizar el usuario o abonado sin gran esfuerzo en lugares públicos, aeropuertos, estaciones o similares.

Para una comprensión mejor e inequívoca de la presente invención, a continuación se explicarán algunos conceptos usados:

Red de telecomunicación: por una red de telecomunicación se entiende aquí un sistema en el que equipos pueden tener la posibilidad de transmitir informaciones directamente, es decir, sin el uso de equipos adicionales, a otros equipos. En el sistema puede usarse siempre la misma tecnología de transmisión o pueden usarse distintas tecnologías de transmisión. Las tecnologías de transmisión usadas pueden ser, por ejemplo, transmisión por radio, transmisión por fibra óptica u otras transmisiones. Si dos equipos pueden comunicar directamente uno con otro puede depender de factores que varían con el tiempo, por ejemplo, por el movimiento de equipos o por cambios de la vía de transmisión y/o de las propiedades de transmisión.

Nodo de red: los equipos que comunican y que forman parte de una red de comunicación pueden ser denominados nodos de red.

Direcciones: en una red de telecomunicación se usan distintos tipos de direcciones. Puede distinguirse entre los siguientes tipos de direcciones:

Direcciones locales: por direcciones locales se entienden direcciones que se usan localmente, por ejemplo, entre nodos de red que pueden comunicar directamente uno con otro. Dicho de una forma más general, se trata de direcciones que son usadas en un área de la red de comunicación, aunque generalmente no en una comunicación extremo a extremo, a no ser que esta comunicación extremo a extremo también sea local. Una dirección local no se usa para el encaminado. Típicamente se representa una dirección de encaminado localmente en una dirección local. Las direcciones locales se usan típicamente en protocolos del nivel 2. Ejemplos para direcciones locales son direcciones Ethernet. Éstas se asignan hoy día habitualmente de forma específica para el equipo.

Dirección de encaminado: por direcciones de en-

caminado se entienden direcciones que se usan para el encaminado, es decir, para establecer rutas de comunicación extremo a extremo en una red de telecomunicación, usándose típicamente tablas de encaminado que son administradas en los nodos de red. Las direcciones de encaminado se usan típicamente en protocolos del nivel 3. Ejemplos para direcciones de encaminado son direcciones IP.

Direcciones topológicas: por direcciones topológicas se entienden aquí direcciones que permiten a un nodo de red determinar si un nodo adyacente está situado mejor respecto a un nodo destino que el nodo propio. La determinación está basada en un conjunto base T de posibles direcciones topológicas y en un procedimiento de valoración que, aplicado a tríos (a, b, c) de posibles direcciones topológicas, determina si a está situado mejor respecto a c que b. Ejemplos para direcciones topológicas son coordenadas geográficas, estando situada a mejor respecto a c que b si la distancia entre a y c es menor que la distancia entre b y c. Otro ejemplo de direcciones topológicas son las coordenadas introducidas en el documento WO 97/50195 con el procedimiento de valoración allí introducido. En determinadas condiciones, las direcciones topológicas permiten el encaminado sin tablas de encaminado.

Direcciones de identificación: por ellas se entienden aquí direcciones que se usan para identificar nodos de red o usuarios o abonados. Las direcciones de identificación contienen frecuentemente un componente que se usa como dirección de encaminado, por ejemplo, a un servidor adecuado.

Direcciones públicas: por éstas, se entienden aquí direcciones de identificación que son públicamente conocidas. Ejemplos son números de teléfono y direcciones DNS (servicio de nombres de dominio; *Domain Name System*).

Las direcciones de un tipo de dirección pueden pertenecer a varios de los tipos arriba descritos, por ejemplo, un número de teléfono sirve habitualmente al mismo tiempo como dirección de identificación, dirección pública y dirección de encaminado.

Basándose en los problemas arriba descritos, la presente invención tiene el objetivo de indicar un procedimiento para establecer una conexión de telecomunicación y una red de telecomunicación del tipo indicado al principio, según el cual se permite una conexión de telecomunicación segura entre abonados en la red de telecomunicación.

El objetivo anteriormente descrito se consigue tanto mediante un procedimiento para establecer una conexión de telecomunicación como mediante una red de telecomunicación con las características de las reivindicaciones 1 ó 37. Según éstas, el procedimiento y la red de telecomunicación están realizados y perfeccionados de tal forma que, antes del establecimiento de la conexión, una unidad de comunicación asigna un número de direcciones predeterminable a un segundo abonado, que el establecimiento de la conexión es realizado por la unidad de comunicación y que el segundo abonado usa al menos una de las direcciones asignadas en el establecimiento de la conexión.

Se ha entendido según la invención que gracias al uso alternativo posible de varias direcciones, la correlación de la dirección usada y un abonado es más difícil o imposible. Para ello, una unidad de comunicación asigna antes del establecimiento de la conexión un número de direcciones predeterminable a un se-

gundo abonado. El segundo abonado puede usar estas direcciones de forma fundamentalmente libre. A continuación, el establecimiento de la conexión es realizado por la unidad de comunicación. Esta unidad de comunicación puede efectuar la correlación entre direcciones asignadas al segundo abonado y a este abonado. El segundo abonado usa en el marco del procedimiento según la invención al menos una de las direcciones asignadas para establecer la conexión.

El primer abonado no conoce la correlación entre las direcciones asignadas y el segundo abonado. Por consiguiente, con el procedimiento según la invención y la red de telecomunicación según la invención se indica un procedimiento y una red de telecomunicación según los cuales es posible una conexión de telecomunicación segura entre abonados en la red de telecomunicación.

En vista de un grado especialmente elevado de seguridad, las direcciones podrían ser anonimizadas. Además, no se puede deducir de las direcciones ninguna relación con el segundo abonado, al menos no a primera vista.

Concretamente, las direcciones podrían ser administradas por la unidad de comunicación. La unidad de comunicación podría administrar las direcciones de varios abonados. Las direcciones podrían ser, en particular, direcciones de encaminado y/o locales, pudiendo tratarse concretamente de direcciones IP y/o de direcciones Ethernet.

Al establecer la conexión, el segundo abonado podría usar al menos una tupla de una dirección de encaminado y una dirección local. No obstante, también es pensable usar al mismo tiempo varias tuplas de este tipo.

La unidad de comunicación podría ser sencillamente un nodo de red de la red de telecomunicación. La función de la unidad de comunicación podría estar dividida, no obstante, también entre varios nodos de red de la red de telecomunicación. Podría predeterminarse una especie de división de trabajo entre los nodos de red.

En la práctica, un proveedor podría ofrecer el uso de direcciones anonimizadas, pudiendo administrar el proveedor un número de direcciones predeterminable, que pertenecen a tipos de direcciones usados en una red de comunicación. El proveedor podría explotar un nodo de red denominado "registro de abonados (TR)". Este nodo de red podría implementar funcionalidades de base de datos, funciones criptológicas y protocolos específicos. La función de este registro de abonados podría estar dividida entre varios nodos de red. De esta forma estaría realizado un sistema dividido como unidad de comunicación o registro de abonados.

Los abonados a los que una unidad de comunicación ha asignado un número adecuado de direcciones cambian las direcciones de encaminado y direcciones locales usados según procedimientos que dificultan mucho o impiden una correlación entre las direcciones de encaminado y direcciones locales usadas o una asignación de direcciones de encaminado y direcciones locales usadas y un abonado.

En particular, en vista de una primera aplicación del procedimiento en un segundo abonado, el segundo abonado podría pasar antes del establecimiento de la conexión por un proceso de inicialización. Aquí, en el marco del proceso de inicialización, podrían instalarse en el segundo abonado las funciones, los parámetros, el software, firmware y/o hardware neces-

rios para una comunicación y/o para la realización de una función criptológica entre el segundo abonado y la unidad de comunicación. Las funciones, los parámetros, el software, firmware y/o hardware podrían ser instalados de forma especialmente sencilla por la unidad de comunicación. En el marco del proceso de inicialización, la unidad de comunicación podría asignar al segundo abonado, antes del establecimiento de la conexión, al menos una dirección inicial para al menos un tipo de dirección. La inicialización podría realizarse de tal forma que quede garantizada la confidencialidad.

De forma especialmente sencilla, la unidad de comunicación podría realizar la asignación de las direcciones al segundo abonado en el marco del proceso de inicialización.

Para simplificar aún más el procedimiento, podría estar instalada al menos una parte de los parámetros, del software y/o firmware en un componente hardware. Un componente hardware de este tipo podría comunicar con el segundo abonado a través de una interfaz definible. De forma especialmente práctica, el componente hardware podría ser una tarjeta IC, es decir, una tarjeta con circuito integrado.

En la práctica, un abonado que desea usar un nodo de red de forma asegurada, podría solicitar que la unidad de comunicación inicializara este nodo de red. Para ello, el abonado podría hacerse registrar correspondientemente en un proveedor de la unidad de comunicación y ser considerado un abonado suscrito. Un nodo de red inicializado correspondientemente podría denominarse a continuación un nodo de red suscrito que ser explotado con el procedimiento según la invención.

El abonado o nodo de red podría usar en el marco del procedimiento según la invención en intervalos de tiempo sucesivos una dirección de encaminado asignada por la unidad de comunicación y una dirección local asignada por la unidad de comunicación, respectivamente. La unidad de comunicación ha asignado estas direcciones previamente, por ejemplo, en el marco de la inicialización. Puede existir una relación de comunicación asegurada entre la unidad de comunicación y el abonado o nodo de red.

En vista de una función segura y de ocupar poco espacio en la memoria, el segundo abonado podría eliminar la dirección usada o las direcciones usadas de la asignación. Por razones de seguridad, las direcciones usadas sólo deberían usarse una vez o pocas veces.

A continuación, las funciones realizadas por el segundo abonado pueden realizarse preferiblemente de forma automática, también mediante uno o varios nodos de red, un módulo o varios módulos o un dispositivo del nodo de red.

En cuanto esté gastado el número de direcciones aún disponibles para el segundo abonado o en cuanto se haya quedado por debajo de un número predeterminable, el segundo abonado podría solicitar nuevas direcciones a la unidad de comunicación. La solicitud también podría realizarse de forma automática por el nodo de red o un módulo o un dispositivo del nodo de red. El número asignado podría ser predeterminado por la unidad de comunicación y podría variar de forma aleatoria entre un valor máximo y mínimo que pueden ser predeterminados. Una asignación de las direcciones de este tipo podría realizarse por razones de seguridad en el marco de una conexión asegurada.

Un cambio de las direcciones por el segundo abonado podría realizarse según distintos procesos o en distintas condiciones. Por ejemplo, podría cambiar el segundo abonado la dirección usada o las direcciones usadas en el marco de su activación. El cambio podría tener lugar justamente en el momento en el que se activa el abonado. El segundo abonado podría cambiar la dirección usada o las direcciones usadas de forma alternativa o adicional a esto después de finalizar la conexión. Dicho de otro modo, el cambio podría realizarse directamente después de finalizar una conexión.

El segundo abonado podría cambiar la dirección usada o las direcciones usadas también en el marco del tránsito del estado conectado al estado no conectado. Dicho de otro modo, el cambio podría realizarse durante el tránsito o simultáneamente con el tránsito del estado conectado al estado no conectado. Esto debe adaptarse al caso de aplicación en cuestión.

Como otra alternativa, el segundo abonado podría usar la dirección usada o las direcciones usadas después de haber transcurrido un intervalo de tiempo predeterminable.

Mientras esté activado el abonado o nodo de red sin estar conectado, podría mantener el uso de una dirección de encaminado y una dirección local durante un tiempo predeterminable, que podría variar de forma aleatoria entre un tiempo mínimo y máximo predeterminado por la unidad de comunicación. En principio, el abonado o nodo de red se considera conectado cuando actúa en una comunicación extremo a extremo con uno o varios otros nodos de red y/o como relé para una comunicación extremo a extremo.

En otra aplicación alternativa, el segundo abonado podría pasar en el marco del cambio de la dirección o de las direcciones usadas después de un intervalo de tiempo predeterminable al estado no conectado, antes de realizarse el cambio. Sería posible que el cambio de la dirección o de las direcciones no tuviera lugar hasta este momento. El intervalo de tiempo predeterminable podría variar de forma aleatoria dentro de unos límites predeterminados por la unidad de comunicación. Dicho de otro modo, el abonado o nodo de red pasa al estado no conectado cuando está conectado durante un tiempo más largo que un tiempo predeterminable, pudiendo variar este tiempo de forma aleatoria dentro de unos límites que pueden ser predeterminados por la unidad de comunicación. Un cambio de la dirección de encaminado y de la dirección local usadas no podría tener lugar hasta este momento. Para no interrumpir una conexión en su totalidad, podrían usarse, dado el caso, paralelamente dos o más direcciones, de modo que también en el tránsito a un estado no conectado se mantenga respecto a una dirección aún una conexión a través de otra dirección. Dicho de otro modo, el segundo abonado podría usar en el marco de la conexión al mismo tiempo varias direcciones o tuplas de direcciones.

Más concretamente, el abonado o nodo de red podría usar en un procedimiento preferible al mismo tiempo varias tuplas de direcciones de encaminado y direcciones locales asignadas y enmascarar de esta forma el cambio de direcciones. En este caso, cada comunicación va ligada a una tupla de una dirección de encaminado asignada y una dirección local asignada. En este procedimiento preferible, las comunicaciones finalizan cuando la tupla de direcciones correspondiente se usa durante demasiado tiempo, es decir, durante más tiempo que un intervalo de tiempo pre-

determinable, pudiendo variar este intervalo de tiempo de forma aleatoria dentro de unos límites predeterminados por la unidad de comunicación. Cada nueva comunicación extremo a extremo establecida por el abonado o nodo de red puede usar una nueva tupla de direcciones. Para cada comunicación extremo a extremo establecida por el abonado o nodo de red también se puede usar una nueva tupla de direcciones según un procedimiento descrito más adelante. Para ello no se interrumpen necesariamente las comunicaciones de niveles superiores.

Si en el abonado o en el nodo de red existe un número insuficiente de direcciones no usadas y el abonado o nodo de red solicita nuevas direcciones a la unidad de comunicación, no teniendo éxito repetidamente la transmisión de nuevas direcciones de la unidad de comunicación al abonado o nodo de red, por ejemplo, porque no se obtiene acceso a la unidad de comunicación, puede producirse el caso de que ya no estén disponibles direcciones asignadas. Un número insuficiente de direcciones significa, por ejemplo, que existen menos que un número de direcciones predeterminable, pudiendo variar el número predeterminable de forma aleatoria entre un valor máximo y mínimo predeterminado por la unidad de comunicación. En una situación de este tipo, el abonado o la unidad de comunicación pueden definir si en este caso el abonado o nodo de red ya no ofrece servicios hasta una nueva inicialización o si se siguen usando direcciones ya usadas.

Para la comunicación entre el abonado o nodo de red y la unidad de comunicación se establece una relación de comunicación entre el abonado o nodo de red y la unidad de comunicación, respectivamente. En vista de conseguir un alto grado de seguridad, en este caso es ventajoso que el segundo abonado o nodo de red y la unidad de comunicación se identifiquen y/o autenticen mutuamente en el marco de una relación de comunicación de este tipo. Aquí pueden usarse procedimientos criptológicos para la identificación y/o autenticación. Una corriente de datos podría codificarse de forma segura, para lo cual podrían usarse, por ejemplo, datos intercambiados en la autenticación. En principio, los datos intercambiados podrían estar provistos de una protección de integridad adicional. En una relación de comunicación protegida de esta forma, el abonado o nodo de red podría solicitar a continuación nuevas direcciones, por ejemplo, direcciones locales y direcciones de encaminado, que podrían intercambiarse de esta forma con seguridad.

En un caso concreto del establecimiento de una conexión, el primer abonado podría enviar para establecer la conexión con el segundo abonado una dirección pública del segundo abonado a la red de telecomunicación. No obstante, con esta dirección pública aún no se obtiene acceso al segundo abonado, es decir, la dirección pública no puede usarse como dirección de encaminado.

En el siguiente paso, la unidad de comunicación podría convertir la dirección pública en una dirección de encaminado. A continuación, la unidad de comunicación podría informar al segundo abonado de la petición del primer abonado de establecer una conexión. En el marco de esta información, la unidad de comunicación podría enviar, además, una dirección de encaminado y, dado el caso, una dirección pública del primer abonado al segundo abonado. Con la dirección pública, el segundo abonado tiene la posibilidad de

obtener informaciones acerca del primer abonado.

En caso de que el segundo abonado dé su consentimiento a la petición del primer abonado de establecer la conexión, la unidad de comunicación podría enviar, después del consentimiento del segundo abonado, una dirección de encaminado y, dado el caso, una dirección de identificación del segundo abonado al primer abonado. La dirección de encaminado enviada y, dado el caso, una dirección de identificación del segundo abonado podría acordarse entre la unidad de comunicación y el primer abonado y/o entre la unidad de comunicación y el segundo abonado.

En este caso, el primer abonado podría establecer una conexión con el segundo abonado basándose en la dirección de encaminado enviada y, dado el caso, en la dirección de identificación enviada del segundo abonado. Como alternativa a ello, también el segundo abonado podría establecer una conexión con el primer abonado. En este caso, la unidad de comunicación acordaría previamente la dirección de encaminado y, dado el caso, la dirección de identificación del primer abonado con el primer abonado y el segundo abonado.

En el marco del establecimiento de la conexión o en el marco de la conexión, el primero y el segundo abonado podrían autenticarse. Para ello, la unidad de comunicación podría haber enviado previamente parámetros de autenticación al primer o y/o al segundo abonado.

En vista de un enmascarado de la conexión o del establecimiento de la conexión entre el primero y el segundo abonado podrían realizarse determinados pasos de comunicación entre la unidad de comunicación y el primero y/o segundo abonado y/o entre el primero y el segundo abonado de forma temporal y/o causalmente desacoplada. De esta forma, un seguimiento del establecimiento de la conexión o de la conexión por parte de terceros no autorizados es fundamentalmente más difícil.

En este contexto, determinados pasos de comunicación entre la unidad de comunicación y el primero y/o segundo abonado y/o entre el primero y el segundo abonado podrían enmascararse mediante retardos, permutaciones o transacciones simuladas. Concretamente, los desacoplamientos temporales y/o causales y/o los retardos, permutaciones o transacciones simuladas podrían ser realizados por la unidad de comunicación y/o por el primero y/o segundo abonado.

Para evitar una investigación sistemática de datos o movimientos del segundo abonado, la unidad de comunicación o el segundo abonado podría bloquear el primer abonado para otros intentos de establecimiento de conexión, en caso de que un intento de establecimiento de conexión previa ya haya sido rechazado por la unidad de comunicación o el segundo abonado. Un bloqueo de este tipo podría realizarse de forma temporalmente limitada o de forma duradera. En principio, los intentos de establecimiento de conexión por parte de abonados no autorizados podrían ser bloqueados de forma temporalmente limitada o de forma duradera. Podría determinarse que sólo puedan comunicarse abonados suscritos.

En una configuración ventajosa de una red de telecomunicación, uno o varios abonados podrían presentar funciones de relé o actuar como relé. Dicho de otro modo, una parte de la red de comunicación podría presentar funciones de relé. En este caso, en un proveedor o en la unidad de comunicación, los abona-

dos o nodos de red suscritos sólo podrían actuar como relé para aquellos abonados o nodos de red o sólo podrían usar aquellos abonados o nodos de red como relé que usan los mismos protocolos para las funcionalidades de relé. Además, los abonados o nodos de red suscritos en un proveedor o en la unidad de comunicación sólo podrían actuar como relé para aquellos abonados o nodos de red o sólo podrían usar aquellos abonados o nodos de red como relé que están suscritos en el proveedor o en la unidad de comunicación o en otros proveedores o unidades de comunicación asociadas con el proveedor o la unidad de comunicación y que pueden autenticarse correspondientemente.

Además, un número de abonados predeterminable podría intercambiar direcciones de identidad codificadas. Es especialmente favorable que cada nodo de red suscrito haya intercambiado direcciones de identidad codificadas con todos sus nodos adyacentes suscritos, es decir, con todos los nodos de red suscritos a los que tiene acceso de forma directa y sin relé intermedio. Si ahora un nodo de red A desea usar, por ejemplo, un nodo adyacente X como relé, envía un mensaje en el procedimiento de transmisión (*broadcast*), que no contiene ni una dirección de encaminado ni una dirección local, pero que contiene en cambio una dirección de identidad codificada de X. En caso de que sea necesario que este mensaje contenga una dirección de encaminado y/o una dirección local de A, puede contener direcciones de este tipo nuevamente seleccionadas. Asimismo, X puede contestar con direcciones nuevamente seleccionadas haciendo referencia a la consulta.

En otra configuración ventajosa de una red de telecomunicación, la unidad de comunicación podría explotar al menos una pasarela a al menos una red parcial definible. Aquí, al menos un abonado predeterminable de la red parcial podría usar una dirección topológica.

En resumen, el procedimiento aquí descrito es especialmente adecuado si el proveedor o la unidad de comunicación explota también pasarelas a redes parciales, en las que se puede tener acceso a cada abonado o nodo de red suscrito desde la pasarela a través de una cadena de abonados o nodos de red suscritos, pudiendo usarse en la cadena direcciones topológicas de los abonados o nodos de red suscritos. En este caso, la pasarela podría comunicar con seguridad con la unidad de comunicación y las dos podrían comunicar con seguridad con un registro de localización (*Location Register*) explotado por el proveedor. En un caso especial, algunos de estos tres nodos de red podrían ser iguales.

Al establecer una relación de comunicación con un abonado o nodo de red suscrito que se encuentra en una red parcial de este tipo, el establecimiento de comunicación hasta la pasarela puede realizarse según el procedimiento arriba descrito. La información acerca de la dirección topológica se usa en la pared parcial. Para dificultar localizaciones basadas en la información acerca de la dirección topológica podrían usarse los siguientes procedimientos:

(A) El al menos un abonado o nodo de red predeterminable de la red parcial que usa direcciones topológicas podría realizar al menos un cambio de coordenadas. También podrían realizar cambios de coordenadas de este tipo otros abonados o nodos de red. Las coordenadas podrían estar disponibles de forma redundante. En este caso, para el encaminado sólo

podrían usarse una selección de las coordenadas.

(B) Para un grado de seguridad especialmente elevado, la valoración de la dirección para la selección de coordenadas podría realizarse siempre en la pasarela.

(C) También podría conseguirse un grado elevado de seguridad si una dirección topológica o una información acerca de la dirección que ha de ser usada o aprovechada para un establecimiento de comunicación se transmite siempre de forma codificada. Para ello, al menos un abonado o nodo de red predeterminable podría presentar un módulo de seguridad que realiza la descodificación de la dirección topológica o de la información acerca de la dirección recibida, el procesamiento para la selección del siguiente relé y la codificación de la información acerca de la dirección topológica que ha de ser transmitida. Es especialmente importante que el módulo de seguridad sea adecuado para la descodificación de la dirección topológica codificada. El módulo de seguridad podría estar protegido de forma adecuada de intervenciones, de modo que la información acerca de la dirección topológica que ha de ser aprovechada para un establecimiento de comunicación no pueda leerse en texto claro. Como módulo de seguridad podría usarse de forma especialmente práctica un chip.

Todas las funciones mencionadas en la presente descripción de uno o varios abonados podrían ser realizadas de forma especialmente fiable por al menos uno nodo de red, al menos un módulo o al menos un dispositivo de uno o varios nodos de red, preferiblemente de forma automática.

Al aplicar el procedimiento aquí descrito en redes de comunicación hay que tener en cuenta que cambios demasiado frecuentes de la dirección de encaminado pueden conducir a una carga significativa de la red, si se usan, por ejemplo, protocolos de estado de enlace, por ejemplo, OSPF. El procedimiento puede aplicarse de forma especialmente favorable si el proveedor explota también pasarelas a abonados en las que puede tenerse acceso a cada nodo de red o abonado suscrito desde la pasarela a través de una cadena de abonados o nodos de red suscritos. Esto puede ser, por ejemplo, redes parciales WLAN, que siempre son especialmente expuestas a ataques.

En los procedimientos según la invención pueden usarse funciones criptológicas y procedimientos como, por ejemplo, procedimientos para la codificación, autenticación y protección de la integridad. Aquí no se describirán funciones y procedimientos especiales de este tipo, pudiendo usarse en el marco de la invención, por lo contrario, todas las funciones y procedimientos adecuados de este tipo.

Además, en el marco de la presente invención se mencionan protocolos para la comunicación entre nodos de red. Aquí no se hace una descripción detallada de los protocolos. Por lo contrario, es posible usar en el marco de la presente invención cualquier protocolo que proporcione las funcionalidades necesarias y adecuadas.

En el marco de la presente invención se habla siempre del establecimiento de una conexión de telecomunicación entre un primer y un segundo abonado. La invención sirve, en particular, para la protección de la confidencialidad de direcciones y/o identificaciones. En este sentido, un establecimiento de una conexión de telecomunicación aquí descrito también podría entenderse en el sentido de un establecimiento durante una conexión de telecomunicación ya exis-

tente. Este establecimiento sería en este caso un establecimiento de una conexión de telecomunicación con mayor seguridad o mayor protección de la confidencialidad de direcciones y/o identificaciones que sirve para asegurar la conexión de telecomunicación existente. En este sentido, el establecimiento según la invención de una conexión de telecomunicación no se refiere forzosamente al comienzo de una conexión de telecomunicación sino también se refiere a una especie de complemento de una conexión de telecomunicación existente mediante una conexión de telecomunicación de mayor seguridad.

Ahora existen distintas posibilidades de configurar y perfeccionar de forma ventajosa la teoría de la presente invención. Para ello se remite, por un lado, a las reivindicaciones que se exponen más adelante y, por otro lado, a la explicación expuesta a continuación de un ejemplo de realización preferible de la invención con ayuda del dibujo. En relación con la explicación del ejemplo de realización preferible de la invención con ayuda del dibujo se explicarán también configuraciones y variantes generalmente preferibles de la teoría. La única figura del dibujo muestra:

Fig. una representación esquemática de un ejemplo de realización del procedimiento según la invención para establecer una conexión de telecomunicación.

La única figura muestra en una representación esquemática un ejemplo de realización del procedimiento según la invención para establecer una conexión de telecomunicación entre un primer abonado A y un segundo abonado BK, nodo de usuario, en una red de telecomunicación. Se pueden asignar direcciones a los abonados A, BK. En vista de una conexión de telecomunicación segura entre los abonados A y BK en la red de telecomunicación, antes del establecimiento de la conexión, la unidad de comunicación TR, registro de abonados, asigna al segundo abonado BK un número de direcciones predeterminable. La unidad de comunicación TR realiza el establecimiento de la conexión. El segundo abonado BK usa en el establecimiento de la conexión al menos una de las direcciones asignadas por la unidad de comunicación TR.

En primer lugar, el nodo de red o abonado A envía una dirección pública bkö de BK a la red de telecomunicación. En el procedimiento aquí descrito es condición previa que el servidor de nombres, nodo de red, que pertenece a bkö, que es el que convierte bkö en una dirección de encaminado, sea el registro de abonados TR o la unidad de comunicación de BK.

En el procedimiento posterior, el TR establece una relación de comunicación segura con BK, transmite la petición de A respecto al establecimiento de conexión, dado el caso, junto con otras informaciones acerca de A, por ejemplo, la dirección de encaminado y, si está disponible, la dirección pública de A, recoge el consentimiento de BK de enviar una dirección de encaminado de BK a A y acuerda con BK una dirección de encaminado bkr que ha de ser usada. En caso de que A esté suscrito al igual que BK, TR envía parámetros de autenticación a BK, A continuación, TR envía bkr a A. En caso de que también A esté suscrito, TR usa para ello una relación de comunicación asegurada y transmite parámetros de autenticación a A que se adaptan a los parámetros de autenticación enviados a BK. A puede establecer, a continuación, una comunicación con BK y los dos pueden autenticarse, dado el caso. Este procedimiento sólo es seguro si A está suscrito. TR o BK pueden rechazar enviar la información de encaminado o dirección de encaminado.

Como alternativa a ello, BK también podría establecer la conexión con A reaccionando así a la petición de A de establecer una conexión. En este caso, BK y A pueden autenticarse eventualmente. También en este caso, TR establece en primer lugar una relación de comunicación segura con BK y transmite la petición de A de establecer una conexión, dado el caso, con otras informaciones acerca de A, por ejemplo, la dirección de encaminado y, en caso de que esté disponible, la dirección pública de A. En caso de que A esté suscrito al igual que BK, TR envía parámetros de autenticación a BK. También este procedimiento alternativo sólo está seguro si A está suscrito. TR puede negarse a enviar la información de encaminado.

Para impedir que un atacante dirija sistemáticamente consultas a TR para correlacionar las corrientes de datos posteriores a BK, TR puede bloquear el nodo de red que envía la consulta de forma transitoria o duradera para otras consultas después de la primera consulta rechazada y/o puede bloquear todas las consultas de nodos de red no especialmente autorizados y suscritos respecto a BK de forma transitoria o duradera para impedir más consultas.

Respecto a otras configuraciones y variantes ventajosas de la teoría según la invención se remite, por un lado, a la parte general de la descripción y, por otro lado, a las reivindicaciones adjuntas.

Finalmente habría que resaltar en particular que el ejemplo de realización elegido de forma puramente arbitraria sólo sirve para la explicación de la teoría según la invención, sin limitarla de ninguna manera a este ejemplo de realización.

REIVINDICACIONES

1. Procedimiento para establecer una conexión de telecomunicación entre un primer y un segundo abonado (A, BK) en una red de telecomunicación, en particular, entre dos equipos adecuados para la comunicación, pudiendo asignarse direcciones a los abonados (A, BK), **caracterizado** porque, antes del establecimiento de la conexión, una unidad de comunicación (TR) asigna un número de direcciones predeterminable a un segundo abonado (BK), porque el establecimiento de la conexión es realizado por la unidad de comunicación (TR) y porque el segundo abonado (BK) usa al menos una de las direcciones asignadas en el establecimiento de la conexión.

2. Procedimiento según la reivindicación 1, **caracterizado** porque las direcciones son anonimizadas y/o porque las direcciones son administradas por la unidad de comunicación (TR).

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado** porque las direcciones son direcciones de encaminado y/o locales o porque son direcciones IP y/o direcciones Ethernet.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado** porque el segundo abonado (BK) usa al menos una tupla de una dirección de encaminado y una dirección local.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** porque como unidad de comunicación (TR) se usa un nodo de red de la red de telecomunicación o porque la función de la unidad de comunicación (TR) se divide entre varios nodos de red de la red de telecomunicación.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** porque, antes del establecimiento de la conexión, el segundo abonado (BK) pasa por un proceso de inicialización.

7. Procedimiento según la reivindicación 6, **caracterizado** porque en el marco del proceso de inicialización se instalan en el segundo abonado (BK) las funciones, los parámetros, el software, firmware o hardware necesarios para una comunicación y/o la realización de una función criptológica entre el segundo abonado (BK) y la unidad de comunicación (TR).

8. Procedimiento según la reivindicación 7, **caracterizado** porque las funciones, los parámetros, el software, firmware o hardware son instalados por la unidad de comunicación (TR).

9. Procedimiento según una de las reivindicaciones 6 a 8, **caracterizado** porque en el marco del proceso de inicialización, la unidad de comunicación (TR) asigna al segundo abonado (BK), antes del establecimiento de la conexión, al menos una dirección inicial para al menos un tipo de dirección y/o porque la unidad de comunicación (TR) realiza la asignación de las direcciones al segundo abonado (BK) en el marco del proceso de inicialización.

10. Procedimiento según una de las reivindicaciones 7 a 9, **caracterizado** porque al menos una parte de los parámetros, del software y/o firmware se instalan en un componente hardware.

11. Procedimiento según la reivindicación 9, **caracterizado** porque el componente hardware comunica con el segundo abonado (BK) mediante una interfaz definible o se usa como componente hardware una tarjeta IC.

12. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado** porque el segundo abona-

do (BK) elimina la dirección usada o las direcciones usadas de la asignación o porque el segundo abonado (BK) solicita nuevas direcciones a la unidad de comunicación (TR) en cuanto se haya gastado el número de direcciones aún disponibles en el segundo abonado (BK) o en cuanto el número haya quedado por debajo de un número predeterminable.

13. Procedimiento según la reivindicación 12, **caracterizado** porque el número es predeterminado por la unidad de comunicación (TR).

14. Procedimiento según una de las reivindicaciones 1 a 13, **caracterizado** porque la asignación de las direcciones se realiza en el marco de una conexión asegurada o porque el segundo abonado (BK) cambia la dirección usada o las direcciones usadas en el marco de su activación.

15. Procedimiento según una de las reivindicaciones 1 a 14, **caracterizado** porque el segundo abonado (BK) cambia la dirección usada o las direcciones usadas después de finalizar la conexión o porque el segundo abonado (BK) cambia la dirección usada o las direcciones usadas en el marco del tránsito del estado conectado al estado no conectado o porque el segundo abonado (BK) cambia la dirección usada o las direcciones usadas después de un intervalo de tiempo predeterminable.

16. Procedimiento según la reivindicación 14 ó 15, **caracterizado** porque el segundo abonado (BK) pasa en el marco del cambio de la dirección o de las direcciones usadas después de un intervalo de tiempo predeterminable al estado no conectado, antes de realizarse el cambio.

17. Procedimiento según una de las reivindicaciones 1 a 16, **caracterizado** porque el segundo abonado (BK) usa en el marco de la conexión al mismo tiempo varias direcciones o tuplas de direcciones o porque el segundo abonado (BK) y la unidad de comunicación (TR) se identifican y/o autentican mutuamente en el marco de una relación de comunicación.

18. Procedimiento según una de las reivindicaciones 1 a 17, **caracterizado** porque el primer abonado (A) envía para establecer la conexión con el segundo abonado (BK) una dirección pública del segundo abonado (BK) a la red de telecomunicación.

19. Procedimiento según la reivindicación 18, **caracterizado** porque la unidad de comunicación (TR) convierte la dirección pública en una dirección de encaminado.

20. Procedimiento según una de las reivindicaciones 1 a 19, **caracterizado** porque la unidad de comunicación (TR) informa al segundo abonado (BK) de la petición del primer abonado (A) de establecer una conexión.

21. Procedimiento según una de las reivindicaciones 1 a 20, **caracterizado** porque la unidad de comunicación (TR) envía una dirección de encaminado o una dirección pública del primer abonado (A) al segundo abonado (BK) o porque la unidad de comunicación (TR) envía, después del consentimiento del segundo abonado (BK), una dirección de encaminado del segundo abonado (BK) al primer abonado (A).

22. Procedimiento según la reivindicación 21, **caracterizado** porque la dirección de encaminado enviada del segundo abonado (BK) es acordada con la unidad de comunicación (TR).

23. Procedimiento según la reivindicación 21 ó 22, **caracterizado** porque, basándose en la dirección

de encaminado del segundo abonado (BK), el primer abonado (A) establece una conexión con el segundo abonado (BK).

24. Procedimiento según una de las reivindicaciones 1 a 23, **caracterizado** porque el segundo abonado (BK) establece una conexión con el primer abonado (A) y/o porque se autentican el primero y el segundo abonado (A, BK).

25. Procedimiento según una de las reivindicaciones 1 a 24, **caracterizado** porque la unidad de comunicación (TR) envía parámetros de autenticación al primero y/o al segundo abonado (A, BK).

26. Procedimiento según una de las reivindicaciones 1 a 25, **caracterizado** porque determinados pasos de comunicación entre la unidad de comunicación (TR) y el primero y/o segundo abonado (A, BK) o entre el primero y el segundo abonado (A, BK) se realizan de forma temporal y/o causalmente desacoplada o porque determinados pasos de comunicación entre la unidad de comunicación (TR) y el primero o segundo abonado (A, BK) o entre el primero y el segundo abonado (A, BK) se enmascaran mediante retardos, permutaciones o transacciones simuladas.

27. Procedimiento según la reivindicación 26, **caracterizado** porque los desacoplamientos temporales o causales o los retardos, permutaciones o transacciones simuladas son realizados por la unidad de comunicación (TR) o por el primero o segundo abonado (A, BK).

28. Procedimiento según una de las reivindicaciones 1 a 27, **caracterizado** porque la unidad de comunicación (TR) o el segundo abonado (BK) bloquea el primer abonado (A) para otros intentos de establecimiento de conexión, en caso de que un intento de establecimiento de conexión previo ya haya sido rechazado por la unidad de comunicación (TR) o el segundo abonado (BK).

29. Procedimiento según la reivindicación 28, **caracterizado** porque el bloqueo se realiza de forma temporalmente limitada o de forma duradera.

30. Procedimiento según una de las reivindicaciones 1 a 29, **caracterizado** porque los intentos de establecimiento de conexión por parte de abonados no

autorizados se bloquean de forma temporalmente limitada o de forma duradera.

31. Procedimiento según una de las reivindicaciones 1 a 30, **caracterizado** porque uno o varios abonados presentan funciones de relé o porque un número de abonados predeterminable intercambia direcciones de identidad codificadas.

32. Procedimiento según una de las reivindicaciones 1 a 31, **caracterizado** porque desde la unidad de comunicación (TR) se explota al menos una pasarela a al menos una red parcial definible.

33. Procedimiento según la reivindicación 32, **caracterizado** porque al menos un abonado predeterminable de la red parcial usa una dirección topológica.

34. Procedimiento según la reivindicación 33, **caracterizado** porque el al menos un abonado predeterminable de la red parcial realiza al menos un cambio de coordenadas y/o porque la dirección topológica se transmite siempre de forma codificada.

35. Procedimiento según la reivindicación 33 ó 34, **caracterizado** porque al menos un abonado predeterminable usa un módulo de seguridad para la descodificación de la dirección topológica codificada.

36. Procedimiento según una de las reivindicaciones 1 a 35, **caracterizado** porque la función de uno o varios abonados es realizada por al menos un nodo de red, al menos un módulo o al menos un dispositivo de uno o varios nodos de red.

37. Red de telecomunicación, en particular, para la aplicación del procedimiento según una de las reivindicaciones 1 a 36, para establecer una conexión de telecomunicación entre un primer y un segundo abonado (A, BK), en particular, entre dos equipos adecuados para la comunicación, pudiendo asignarse direcciones a los abonados (A, BK), **caracterizada** porque, antes del establecimiento de la conexión, una unidad de comunicación (TR) puede asignar un número de direcciones predeterminable a un segundo abonado (BK), porque la unidad de comunicación (TR) está realizada para establecer la conexión y porque el segundo abonado (BK) está realizado para el uso de al menos una de las direcciones asignadas en el establecimiento de la conexión.

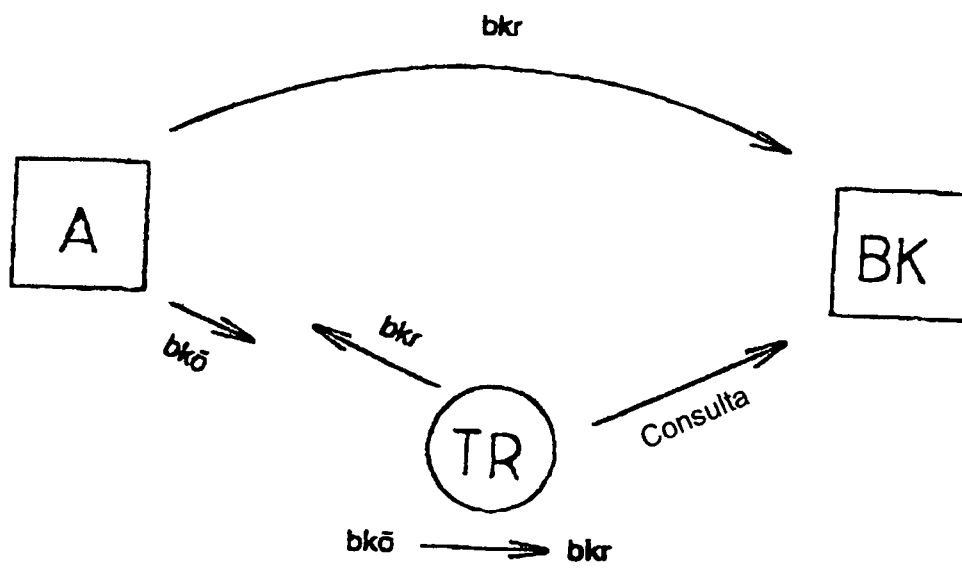


Fig.