(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 589 906**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.10.2007 PCT/SE2007/050803**

(87) Fecha y número de publicación internacional: **08.05.2008 WO08054320**

(96) Fecha de presentación y número de la solicitud europea: **31.10.2007 E 07835387 (7)**

(97) Fecha y número de publicación de la concesión europea: **20.07.2016 EP 2087634**

(54) Título: **Sistemas de telecomunicación y codificación de mensajes de control en tales sistemas**

(30) Prioridad:

01.11.2006 SE 0602317

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.11.2016

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

MILDH, GUNNAR

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistemas de telecomunicación y codificación de mensajes de control en tales sistemas

Sector técnico

La presente invención de refiere a los sistemas de telecomunicación y a la codificación de mensajes de control en tales sistemas. Aspectos concretos de la invención se refieren a los sistemas de telecomunicación inalámbrica.

Antecedentes de la invención

Hoy en día, un amplio espectro de sistemas de telecomunicación diferentes ha evolucionado tanto para la telecomunicación por cable como inalámbrica. Los sistemas de telecomunicación han sido, por ejemplo, estandarizados junto con los llamados sistemas de telefonía móvil de segundo generación (2G) y de tercera generación (3G). Se puede encontrar información acerca de la tecnología 3G (por ejemplo, W-CDMA o CDMA2000) y la tecnología 2G (por ejemplo, GSM) etc., en las especificaciones del Proyecto de asociación de 3ª generación (3GPP – 3rd Generation Partnership Project, en inglés), véase, por ejemplo, el sitio web en www.3gpp.org.

Un desarrollo posterior ha producido técnicas para permitir velocidades incluso mayores de transferencia intercelular de datos. Uno de tales ejemplos es el desarrollo en curso del SAE / LTE (Evolución de la arquitectura del sistema / Evolución a largo plazo – System Architecture Evolution / Long Term Evolution, en inglés), que es la siguiente etapa en términos de experiencia de servicio del usuario, mejorando la latencia, la capacidad y el rendimiento. Por ejemplo, esto incluye los trabajos del 3GPP en la Evolución de los Sistemas para móviles de 3G, y con ello la evolución de la Red de acceso por radio terrestre universal (UTRAN – Universal Terrestrial Radio Access Network, en inglés).

Tal como se puede ver en la figura 1, la UTRAN evolucionada comprende varios eNB (eNodo B) 1, que proporcionan terminaciones de protocolo de plano de usuario (plano-U) UTRA evolucionado y de plano de control (plano-C) hacia el Equipo de usuario (UE – User Equipment, en inglés). Los eNB están interconectados entre sí por medio de una interfaz X2 9. Se asume que siempre existe una interfaz X2 entre los eNB que necesitan comunicarse entre sí, por ejemplo, para el soporte de la transferencia intercelular de los UE en LTE-ACTIVA. Los eNB están asimismo conectados por medio de la interfaz S1 12 al EPC (Núcleo de paquetes evolucionado – Evolved Packet Core, en inglés). La interfaz S1 soporta una relación de muchas a muchas entre las aGW (Puertas de enlace de acceso – Access Gateways, en inglés) y los eNB.

El eNB tiene implementadas varias funciones para la Gestión de recursos de radio: Control de portadora de radio, Control de admisión de radio, Control de movilidad de conexión, Asignación (planificación) de recursos dinámicos y otros, como el experto puede comprender.

La Entidad de gestión de movilidad (MME – Mobility Management Entity, en inglés) tiene implementadas varias funciones para la distribución de mensajes de localización a los eNB.

La Entidad de plano de usuario (UPE – User Plane Entity, en inglés) alberga varias funciones para:

- compresión de cabecera de IP y codificación de flujos de datos de usuario;
- terminación de paquetes de plano-U por razones de localización;
- conmutación del plano-U para el soporte de la movilidad del UE.

Se puede encontrar información adicional, por ejemplo, en la especificación “3GPP TR 25.912 V7.1.0 (2006-09” y en otras especificaciones del 3GPP asociadas con la misma.

En esta conexión se ha acordado que los mensajes de Control de recursos de radio (RRC – Radio Resource Control, en inglés) intercambiados entre el eNodoB y el terminal (UE), deberían estar cifrados y con identidad protegida. Esto requiere la utilización de claves RRC en el eNodoB, y que el UE realice las funciones de seguridad. Las claves RRC se generan en la Red de núcleo (CN – Core Network, en inglés) y en el UE, y se envían desde la CN al eNodoB cuando el UE entra en el estado activo. Las claves RRC se envían asimismo entre los eNodoB cuando la movilidad intra-LTE se encuentra en modo activo. El RRC es parte de una subcapa de la Capa 3 de la interfaz de radio; existe solo en el plano de control y proporciona un servicio de transferencia intercelular de información al NAS (Estrato de no acceso – Non Access Stratum, en inglés). El RRC es responsable de controlar la configuración de las Capas 1 y 2 de la interfaz de radio. La Capa de no acceso es una capa funcional que ejecuta y soporta tráfico y señalización entre el UE (Equipo de usuario) y la CN (Red de núcleo).

El algoritmo de cifrado y protección de integridad requiere un número de secuencia único como entrada para cada mensaje RRC. No se debe utilizar dos veces el mismo número de secuencia y clave RRC; no obstante, se puede utilizar el mismo número de secuencia como entrada tanto para el cifrado como para la protección de la integridad.

Partes del número de secuencia se enviarán sobre la interfaz de radio con cada mensaje RRC, con el fin de codificar el número de secuencia sincronizado en el emisor y el receptor; no obstante, para limitar el número de bits enviados sobre la interfaz de radio, es posible utilizar un número de hipertrama (HFN – Hyper Frame Number, en inglés) (es decir, un mecanismo de contador de sobrecarga) que no es transferido por radio, sino que se guarda internamente en el eNodoB y en el terminal (UE). El HFN se utilizará asimismo como entrada al algoritmo de cifrado y protección de integridad. El HFN será un contador con número de bits suficiente, de tal manera que el número de secuencia utilizado como entrada al algoritmo de cifrado y protección de integridad será único durante la vida útil de la clave RRC.

La clave RRC es generada durante el procedimiento de Conectar a la red o a otra red de núcleo, por el algoritmo de Autenticación y Acuerdo de clave (AKA – Authentication and Key Agreement, en inglés), que implica la tarjeta (U)SIM en el terminal y el HLR /HSS y otros nodos de la red de núcleo.

Este proceso lleva mucho tiempo, y resultaría beneficioso no necesitar la regeneración de la clave RRC tras diferentes eventos de movilidad, tales como transferencia intercelular y transiciones de estado Inactivo (Idle, en inglés) a Activo.

En el estándar WCDMA / UMTS existe una solución del estado de la técnica que se utiliza para poder mantener la seguridad de RRC durante eventos de movilidad. Esta solución está basada en:

a) guardar un valor INICIO en el UE / USIM que se utiliza para iniciar el contador de HFN tras una transición del estado Inactivo a Activo. El valor INICIO es transferido a la UTRAN durante el establecimiento de la conexión RRC. El HFN se inicia siempre en un valor que es mayor que el SFN utilizado previamente, con el fin de evitar la utilización del mismo HFN con la misma clave RRC.

b) durante las transferencias intercelulares inter-RNC, el HFN es transferido al RNC objetivo, el HFN es incrementado también normalmente mediante una o dos etapas durante la transferencia intercelular con el fin de evitar que se reutilice el mismo HFN para las mismas claves RRC. Esto se debe a que durante el proceso de transferencia intercelular el HFN podría ser incrementado en el RNC de origen, mientras que los recursos se están preparando en el RNC de objetivo.

Esta solución es, no obstante, bastante compleja, y requiere señalización adicional relativa a la seguridad. Un problema concreto con las soluciones actuales es que los HFN se utilizan para varias cosas, tanto como contador de sobrecarga para el número de secuencia más corto utilizado en la radio, pero se incrementa también durante los eventos de movilidad tales como transferencias intercelulares y transiciones del estado inactivo al activo.

Para SAE / LTE que tienen una división funcional ligeramente diferente entre la red de núcleo y la red de radio (por ejemplo, no hay ningún RNC) y para otras redes de telecomunicaciones estandarizadas que tienen la misma o similares capacidades, resulta beneficioso utilizar un método diferente.

Compendio de la invención

El concepto básico de la invención es la separación del contador de sobrecarga de número de secuencia de los contadores para eventos de movilidad, y utilizar todos los contadores como entradas separadas al algoritmo de cifrado RRC y protección de integridad. Los diferentes contadores se guardarían en el UE, el eNodoB y la CN, y serán sincronizados implícitamente debido a diferentes eventos.

Ejemplo de eventos podría ser que el número de secuencia corta utilizado en la radio se confirma, o que se haya realizado una transferencia intercelular, o que se hayan realizado transiciones del estado inactivo al activo.

Los contadores serían jerárquicos, es decir, cuando el contador de transición de estado (guardado en el UE y en la red de núcleo) es incrementado, los contadores de transferencia intercelular y de sobrecarga (guardados en el UE y en el eNodoB) son reiniciados a cero, y, cuando el contador de transferencia intercelular es incrementado, el contador de sobrecarga es reiniciado a cero.

Las ventajas con este planteamiento son que los números de secuencia de mensaje RRC siempre pueden ser ajustados a cero tras una transferencia intercelular o transición de estado, y no hay necesidad de señalar ningún valor de inicio para la radio siempre que el UE y la CN mantengan un seguimiento del contador de transición de estado (INACTIVO / ACTIVO) y el UE y la RAN mantengan un seguimiento del contador de transferencia intercelular (ACTIVO).

Dicho lo anterior de manera ligeramente diferente: Resultaría beneficioso tener una solución en LTE que separe eventos de confirmación de número de secuencia de eventos de movilidad (transferencias intercelulares, transiciones de estado). Se podría considerar una solución en la que existen 3 contadores diferentes que proporcionan entradas a la seguridad RRC. Un contador de sobrecarga para el número de secuencia, un contador de transferencia intercelular y un contador de transiciones de estado. Los contadores serían jerárquicos, es decir, cuando el contador de transición de estado es incrementado, los contadores de transferencia intercelular y de

sobrecarga son reiniciados a cero, y, cuando el contador de transferencia intercelular es incrementado, el contador de sobrecarga es reiniciado a cero.

Si se desea evitar contadores adicionales en el algoritmo de cifrado RRC / protección de integridad sería posible realizar el efecto del contador de transición de estado y de transferencia intercelular realizando, por el contrario, una función de codificación en la CN / UE en la clave RRC en cada transición de estado y, a continuación, realizar una función diferente en la RAN / UE en cada transferencia intercelular. De esa manera, la clave RRC sería nueva en cada evento de movilidad, haciendo posible el reinicio del contador de sobrecarga (HFN) a cero. Una ventaja añadida de este planteamiento sería dificultar el rastreo de la clave RRC si una clave RRC siguiente resulta comprometida (asumiendo que se utiliza una “función” suficientemente segura).

De acuerdo con la presente invención, se proporciona un método para la codificación de mensajes RRC intercambiados entre un nodo (eNB) y un equipo de usuario (UE) en un sistema de telecomunicación, utilizando claves RRC para la codificación de mensajes RRC, que comprende la etapa de separación de eventos de confirmación de número de secuencia y de eventos de movilidad en el proceso de codificación de mensajes RRC, en el que la etapa de separación comprende las etapas de:

- utilización de tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga,

- proporcionar salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de mensajes RRC.

El método de acuerdo con el primer aspecto en el que la etapa de separación puede comprender las etapas de:

realizar la codificación de mensajes de control relativos a transiciones de estado en un equipo de usuario y una red de núcleo;

realizar la codificación de mensajes de control relativos a eventos de transferencia intercelular en el equipo de usuario y en una parte de red de acceso por radio de la red de comunicaciones,

en el que los dos procesos de codificación son distintos uno de otro.

Además, se pueden prever claves RRC en un algoritmo de codificación.

Lo anterior se consigue también de acuerdo con un segundo aspecto de la invención que prevé un equipo de usuario (UE) dispuesto para intercambiar operativamente mensajes RRC codificados utilizando el método del primer aspecto de la presente invención.

El equipo de usuario está caracterizado por que:

- dispone de acceso a tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga,

- y en el que el equipo de usuario está dispuesto para proporcionar operativamente salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de los mensajes RRC.

Se prevé un tercer aspecto de la presente invención que comprende un nodo de comunicación en una parte de infraestructura de una red de comunicación inalámbrica, que comprende una unidad de procesamiento, una unidad de memoria y al menos una interfaz de comunicación, en el que la unidad de procesamiento está dispuesta para mantener al menos un contador almacenado en la unidad de memoria para su utilización en hacer seguros los mensajes de control de recursos de radio, es decir, RRC, caracterizado por que el nodo está dispuesto además para realizar una separación de eventos de confirmación de número de secuencia y de eventos de movilidad en el proceso de codificación de mensajes RRC, por ejemplo, mediante la obtención de tres contadores separados que se utilizan de manera jerárquica, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga; el nodo de comunicación está dispuesto para proporcionar operativamente salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de mensajes RRC.

Un cuarto aspecto de la presente invención se prevé en un sistema para la gestión de la comunicación en una red de telecomunicaciones inalámbrica, que comprende:

una puerta de enlace de acceso (eNodoB);

una red de núcleo;

en el que la puerta de enlace de acceso está dispuesta para comunicar con un equipo de usuario y la red de núcleo, y en el que la puerta de enlace de acceso está dispuesta para realizar una separación de eventos de confirmación de número de secuencia y de eventos de movilidad en el proceso de codificación de mensajes RRC, por ejemplo, mediante el acceso a tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga, y en el que cada una de la red de núcleo y la puerta de enlace de acceso están dispuestas para la utilización de los contadores para producir claves de contador de recursos de radio utilizadas en un algoritmo de codificación.

Un quinto aspecto de la presente invención se proporciona en un programa informático almacenado en un medio legible por ordenador, para su utilización en una parte del dispositivo de una red de telecomunicación inalámbrica, que comprende conjuntos de instrucciones para:

codificar mensajes de control de recursos de radio (RRC) utilizando claves RRC de codificación,

entre el equipo de usuario, la puerta de enlace de acceso y dispositivos de la red de núcleo;

utilizando tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga,

proporcionar salidas de los citados contadores como entradas a un algoritmo de codificación para producir las citadas claves RRC; y, opcionalmente, intercambiar valores de contador con otros dispositivos en la red de comunicación.

Breve descripción de los dibujos

A continuación, se describirá la invención de una manera no limitativa y con más detalle, con referencia a las realizaciones de ejemplo ilustradas en los dibujos adjuntos, en los cuales:

la figura 1 ilustra esquemáticamente una red de acuerdo con la presente invención;

la figura 2 ilustra esquemáticamente la red de acuerdo con la figura 1 en una vista diferente;

la figura 3 ilustra esquemáticamente en un diagrama de bloques, un método de acuerdo con la presente invención;

la figura 4 ilustra esquemáticamente en un diagrama de bloques, un dispositivo de infraestructura de acuerdo con la presente invención; y

la figura 5 ilustra esquemáticamente en un diagrama de bloques, un dispositivo de usuario de acuerdo con la presente invención.

Descripción detallada

En la figura 1 el número de referencia 10 indica de manera general una red de acuerdo con la presente invención, la UTRAN evolucionada comprende varios eNB (eNodo B) 1, que proporcionan terminaciones de protocolo de plano de usuario (plano-U) de la UTRA evolucionada y de plano de control (plano-C) hacia el equipo de usuario (UE). Los eNB están interconectados entre sí por medio de una interfaz X2 9. Se asume que siempre existe una interfaz X2 entre los eNB que necesitan comunicarse entre sí, por ejemplo, para soportar la transferencia intercelular de los UE en LTE_ACTIVA. Los eNB están asimismo conectados por medio de la interfaz S1 12 al EPC (Núcleo de paquetes evolucionado – Evolved Packet Core, en inglés). La interfaz S1 soporta relación de muchos a muchos entre varias aGW (Puertas de enlace de acceso – Access Gateway, en inglés) y varios eNB. Se debe observar que se pueden utilizar otras interfaces distintas de la interfaz X2 para la comunicación entre los eNB.

El eNB tiene implementadas varias funciones para la gestión de recursos de radio: control de portador de radio, control de admisión de radio, control de movilidad de conexión, asignación (planificación) de recursos dinámicos y otros, como comprenderá el experto.

La entidad de gestión de movilidad (MME – Mobility Management Entity, en inglés) 11 tiene implementadas funciones para la distribución de mensajes de localización a los eNB.

La figura 2 muestra con más detalle la red de la figura 1, comprendiendo al menos un dispositivo de puerta de acceso de infraestructura inalámbrico 1 (eNodoB), una red de núcleo de comunicación de infraestructura 2 (CN) que comprende, por ejemplo, un nodo de puerta de enlace 3 de red (por ejemplo, GGSN), un nodo de servicio de red 4 (por ejemplo, SGSN) y una conexión de acceso 5 a una red de comunicación 6 (por ejemplo, la red de telefonía o

una red de datos; por ejemplo, Internet). Los dispositivos de equipo de usuario (UE) 7 pueden conectarse a la puerta de enlace de acceso inalámbrico mediante algún protocolo de comunicación inalámbrica adecuado (que se explicará también a continuación). La red de infraestructura puede comprender también otros componentes (no se muestran todos en la figura 2), tales como un MSC (Centro de conmutación para móviles – Mobile Switching Centre, en inglés) 8, el VLR (Registro de ubicación de visitantes – Visitor Location Register, en inglés) o HLR (Registro de ubicación de abonados locales – Home Location Register, en inglés) dependiendo de la configuración, tal como comprenderá el experto en la materia.

Por razones de seguridad la funcionalidad de cifrado de mensajes en el Control de recursos de radio (RRC) está implementada con la red en diferentes entidades de la red, incluidos los UE. El cifrado de mensajes se realiza utilizando técnicas de codificación, en las que se utilizan semillas para generar entradas a algoritmos. La semilla se produce junto con otra información (por ejemplo, el número HFN), que no se debe repetir, con el fin de reducir el riesgo de ser comprometido, o al menos no se debe repetir en un periodo de tiempo razonable.

Con vistas a la seguridad, se realizan las siguientes asunciones:

1. Las claves RRC están separadas criptográficamente de las claves CN utilizadas para la protección de datos del NAS (estrato de no acceso) y del usuario final.

2. Las claves RRC son generadas directamente mediante un procedimiento de AKA a nivel de NAS (CN / UE), o inferidas en la CN / UE a partir del material de clave que fue generado mediante un procedimiento de AKA a nivel de NAS (CN / UE).

3. Las claves RRC son enviadas desde la CN al eNodoB cuando el UE entra en estado de LTE_ACTIVO (es decir, durante el establecimiento de la conexión de RRC o del contexto de S1.

4. Las claves RRC son enviadas entre los eNodo B durante la movilidad intra-LTE de modo activo.

5. Se utilizará un número de secuencia como entrada al cifrado y la protección de integridad del RRC. Solo se debe utilizar un número de secuencia dado una vez, para una clave RRC dada (excepto para la retransmisión idéntica). Se puede utilizar el mismo número de secuencia tanto para el cifrado como para la protección de integridad.

6. Se utiliza un número de hipertrama (HFN) (es decir, un mecanismo de contador de sobrecarga (OC – Overflow Counter, en inglés) en el eNodo B con el fin de limitar el número real de bits de número de secuencia necesarios para ser enviados por radio con cada mensaje RRC.

El concepto básico de la invención es la separación de contador de sobrecarga de número de secuencia y los contadores para eventos de movilidad, y la utilización de todos los contadores como entradas separada al algoritmo de cifrado de RRC y de protección de integridad. Los diferentes contadores estarían guardados en el UE, el eNodo B y la CN, y estarán sincronizados de manera implícita debido a diferentes eventos.

Ejemplo de eventos podría ser el número de secuencia corta utilizado en las confirmaciones de radio, o que se ha realizado una transferencia intercelular, o que se han realizado transiciones de estado inactivo a estado activo.

Los contadores pueden ser jerárquicos, es decir, cuando el contador de transición de estado (guardado en el UE y la red de núcleo) es incrementado, los contadores de transferencia intercelular y de sobrecarga (guardados en el UE y el eNodo B) son reiniciados a cero, y, cuando el contador de transferencia intercelular es incrementado, el contador de sobrecarga es reiniciado a cero.

Las ventajas con este planteamiento son que los números de secuencia de mensaje RRC siempre pueden ser ajustados a cero después de una transferencia intercelular o una transición de estado, y no es necesario señalizar ningún valor de inicio por radio siempre que el UE y la CN mantengan un seguimiento del contador de transición de estado (INACTIVO / ACTIVO) y el UE y la RAN hagan un seguimiento del contador de transferencia intercelular (ACTIVO).

Para decir lo anterior de manera ligeramente diferente: Resultaría beneficioso tener una solución en LTE que realice una separación de eventos de confirmación de número de secuencia y de eventos de movilidad (transferencia intercelular, transiciones de estado). Se podría considerar una solución en la que existen 3 contadores diferentes que proporcionan entradas a la seguridad de RRC: un contador de sobrecarga para el número de secuencia, un contador de transferencia intercelular y un contador de transiciones de estado. Los contadores serían jerárquicos, es decir, cuando el contador de transición de estado es incrementado, los contadores de transferencia intercelular y de sobrecarga son reiniciados a cero, y, cuando el contador de transferencia intercelular es incrementado, el contador de sobrecarga es reiniciado a cero.

Si se desea evitar contadores adicionales en el algoritmo de cifrado RRC / protección de integridad, sería posible realizar el efecto del contador de transiciones de estado y de transferencia intercelular realizando, por el contrario, una función de codificación en la CN / UE en la clave RRC en cada transición de estado y, a continuación, realizando una función diferente en la RAN / UE en cada transferencia intercelular. De esa manera, la clave RRC

sería nueva en cada evento de movilidad, haciendo posible reiniciar el contador de sobrecarga (HFN) a cero. Una ventaja añadida de este planteamiento sería dificultar el rastreo de la clave RRC si una clave RRC siguiente resulta comprometida (asumiendo que se utiliza una “función” suficientemente segura).

La figura 3 muestra un método de acuerdo con la presente invención:

301. mantener hasta tres contadores relacionados con diferentes eventos de red o de gestión, tal como se ha explicado anteriormente;

302. detectar eventos de la red

303. determinar el tipo de evento de la red

304. utilizar valores del contador como entradas a un algoritmo para la codificación de mensajes RRC.

305. opcionalmente, sincronizar los valores del contador entre diferentes entidades de la red utilizando una manera oportuna (es decir, de manera regular) o de una manera oportunista (es decir, utilizando mensaje de control para distribuir valores cuando están disponibles).

La presente invención se utiliza en los eNodoB, la red de núcleo y el UE, tal como se ha explicado anteriormente. En la red de infraestructura, el eNodoB es responsable de mantener los contadores de transferencia intercelular y de sobrecarga. Tal como se muestra en la figura 4, un eNodoB 400 puede comprender al menos una unidad de procesamiento 4001, al menos una unidad de memoria 402 (volátil y/o no volátil), opcionalmente una unidad de interfaz de control 403, al menos una interfaz de comunicación 404 de la red de infraestructura y, al menos una interfaz de la red inalámbrica 405. El eNodoB se debe considerar como entidad lógica que comprende varios bloques de funciones tales como las funciones de conexión lógica para manejar la conexión y la comunicación entre los UE y el eNodoB, las funciones de interfaz de radio física y las funciones de comunicación de infraestructura para manejar la comunicación entre la red de núcleo y el eNodoB. No obstante, el experto debe entender que parte de estos bloques funcionales pueden residir en dispositivos separados, formando conjuntamente el eNodoB. La unidad de memoria 402 puede comprender cualquier tipo adecuado, tal como RAM, DRAM, ROM, EEP-ROM, Flash, disco duro y otros, como el experto comprenderá. La interfaz de radio puede utilizar cualquier protocolo de radio adecuado tal como entiende el experto, bien un protocolo fijo, una combinación de protocolos fijos o bien una solución de radio definida mediante software. La unidad de procesamiento puede comprender, por ejemplo, al menos uno de un microprocesador, una FPGA (Matriz de puertas programables en campo – Field Programmable Gate Array, en inglés), un procesador de señal digital (DSP – Digital Signal Processor, en inglés) o un ASIC (Circuito integrado específico para una aplicación – Application Specific Integrated Circuit, en inglés).

Tal como se puede ver en la figura 5, el UE 500 puede comprender al menos una unidad de procesamiento 501, una unidad de interfaz de usuario 502, al menos una unidad de memoria 503 (volátil y/o no volátil) que pueden ser de los mismos tipos que se han explicado anteriormente en relación con la figura 4), al menos una interfaz de comunicación inalámbrica (incluido el equipo de RF, tal como transceptor y antena) 504. La interfaz inalámbrica está dispuesta para comunicar con un protocolo de radio compatible con SAE / LTE o similar, utilizando codificación similar de mensajes RRC; la interfaz inalámbrica puede estar utilizando los estándares de radio fija o una solución de radio definida mediante software. El UE puede comprender otras unidades y componentes, como el experto comprende. La unidad de procesamiento puede, por ejemplo, comprender al menos uno de un microprocesador, una FPGA (Matriz de puertas programables en campo), un procesador de señal digital (DSP), o un ASIC (Circuito integrado específico para una aplicación). El UE mantiene los eventos de contador de transiciones de estado, el contador de transferencia intercelular y el contador de sobrecarga.

De manera similar, la CN mantiene un contador para los eventos de transición de estado. Este contador puede estar situado en cualquier ubicación adecuada, tal como en un HLR o VLR o un nodo de soporte, dependiendo de la configuración de la red.

Los valores de los contadores se distribuyen a las otras partes de los procesos RRC donde es necesario, dependiendo del evento, con el fin de que se utilicen como valores de entrada en la generación de claves del proceso RRC. Esto asegura la sincronización entre entidades dependientes de la configuración de la red, tal como entre el UE y el eNodoB o el UE y la CN. En el mecanismo de cifrado en el proceso RRC existen entrada para varios valores del contador para recibir los valores de contador apropiados necesarios para la sincronización y el cifrado de los mensajes de control.

Se debe observar que la expresión “que comprende” no excluye la presencia de otros elementos o etapas diferentes de las enumeradas, y las palabras “un” o “una” precediendo a un elemento no excluyen la presencia de una pluralidad de tales elementos. Se debe observar, además, que ningún signo de referencia limita el alcance de las reivindicaciones, que la invención puede ser implementada, al menos en parte, por medio tanto de hardware como de software, y que varios “medios” o “unidades” pueden ser representados por el mismo elemento de hardware.

Las realizaciones mencionadas y descritas anteriormente están dadas solo a modo de ejemplos, y no deben limitar la presente invención. Otras soluciones, usos, objetivos y funciones dentro del alcance de la invención según se

reivindican y describen en las reivindicaciones de patentes que siguen, resultarán evidentes para el experto en la materia.

Abreviaturas y definiciones

aGWs	Puertas de enlace de acceso	Access Gateways, en inglés
AKA	Autenticación y acuerdo de clave	Authentication and Key Agreement, en inglés
CN	Red de núcleo	Core Network, en inglés
GGSN	Nodo de soporte de GPRS de puerta de enlace	Gateway GPRS Support Node, en inglés
GPRS	Servicio de radio en paquetes general	General Packet Radio Service, en inglés
HFN	Número de hipertrama	HyperFrame Number, en inglés
HLR	Registro de ubicación de abonados locales	Home Location Register, en inglés
IP	Protocolo de Internet	Internet Protocol, en inglés
LTE	Evolución a largo plazo	Long Term Evolution, en inglés
MME	Entidad de gestión de la movilidad	Mobility Management Entity, en inglés
MSC	Centro de conmutación de movilidad	Mobility Switching Centre, en inglés
NAS	Estrato de no acceso	Non Access Stratum, en inglés
RAN	Red de acceso por radio	Radio Access Network, en inglés
RRC	Control de recursos de radio	Radio Resource Control, en inglés
SGSN	Nodo de soporte de GPRS de servicio	Serving GPRS Support Node, en inglés
UE	Equipo de usuario	User Equipment, en inglés
UPE	Entidad de plano de usuario	User Plane Entity, en inglés
VLR	Registro de ubicación de visitantes	Visitor Location Register, en inglés

REIVINDICACIONES

1. Método para la codificación de mensajes de control de recursos de radio (RRC) intercambiados entre un nodo (eNB) (1) y un equipo de usuario (UE) (7) en un sistema de telecomunicación, utilizando claves RRC para la codificación de mensajes RRC, caracterizado por la etapa de separación de eventos de confirmación de número de secuencia y de eventos de movilidad en el proceso de codificación de mensajes RRC,

en el que la etapa de separación comprende las etapas de:

- utilización de tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga,

- proporcionar salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de mensajes RRC.

2. Método de acuerdo con la reivindicación 1, en el que la etapa de separación comprende las etapas de:

- realización de una codificación de mensajes RRC relacionados con transiciones de estado en el equipo de usuario (7) y una red de núcleo (2);

- realización de una codificación de mensajes RRC relacionados con eventos de transferencia intercelular en el equipo de usuario y en una parte de red de acceso por radio de la red de comunicaciones,

en el que los dos procesos de codificación son distintos uno de otro.

3. Método de acuerdo con una cualquiera de las reivindicaciones 1 y 2, en el que se utiliza un algoritmo de codificación para producir una clave RRC.

4. Equipo de usuario (UE) (7, 500) en una red de telecomunicaciones, que comprende una unidad de procesamiento (501), una unidad de memoria (502) y al menos una interfaz de comunicación inalámbrica (504), en el que la unidad de procesamiento (501) está dispuesta para intercambiar operativamente mensajes RRC codificados con un nodo (eNB) (1) y/o una parte de red de núcleo (2) en la red de telecomunicaciones mediante la utilización de claves RRC para la codificación de mensajes RRC, caracterizado por que el UE está dispuesto para distinguir entre eventos de confirmación de número de secuencia y eventos de movilidad en la generación de claves utilizadas como entradas a un algoritmo de codificación para la codificación de mensajes RRC; en el que el equipo de usuario dispone de acceso a tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga, el equipo de usuario está dispuesto para proporcionar operativamente las salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de mensajes RRC.

5. El equipo de usuario (7) de acuerdo con la reivindicación 4, dispuesto para:

- realizar una codificación de mensajes RRC relativos a transiciones de estado en el equipo de usuario en relación con entidades de la red de núcleo (2);

- realizar una codificación de mensajes RRC relativos a eventos de transferencia intercelular en el equipo de usuario en relación con una parte de red de acceso por radio (1) de la red de comunicaciones.

6. El equipo de usuario de acuerdo con la reivindicación 5, en el que se utiliza un algoritmo de codificación para producir una clave RRC.

7. Nodo de comunicación (400) en una parte de infraestructura (2) de una red de comunicación inalámbrica (10), que comprende una unidad de procesamiento (401), una unidad de memoria (402) y al menos una interfaz de comunicación (404, 405), en el que la unidad de procesamiento está dispuesta para intercambiar operativamente mensajes RRC codificados con otros nodos de la red de telecomunicaciones y/o con un equipo de usuario (UE) utilizando claves RRC para la codificación de mensajes RRC, caracterizado por que el nodo está dispuesto para distinguir entre eventos relativos a la confirmación de número de secuencia y eventos de movilidad en la generación de claves utilizadas como entradas a un algoritmo de codificación para la codificación de mensajes RRC, en el que el nodo está además dispuesto para obtener tres contadores separados, que se utilizan de manera jerárquica, de tal manera que, cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga; el nodo está dispuesto para proporcionar operativamente las salidas de los citados contadores como entradas a un algoritmo de codificación para la codificación de mensajes RRC.

8. Nodo de acuerdo con la reivindicación 7, dispuesto además para:

- realizar una codificación de mensajes RRC relativos a transiciones de estado en el equipo de usuario en relación con entidades de la red de núcleo (2);

- realizar una codificación de mensajes RRC relativos a eventos de transferencia intercelular en el equipo de usuario en relación con una parte de red de acceso por radio (1) de la red de comunicaciones.

9. Nodo de acuerdo con la reivindicación 7 o la reivindicación 8, en el que se utiliza un algoritmo de codificación para producir la clave RRC.

10. Nodo de acuerdo con cualquiera de las reivindicaciones 7 a 9, dispuesto además para mantener al menos un contador guardado en la unidad de memoria para su utilización en asegurar los mensajes de control de recursos de radio, es decir, RRC.

11. Sistema de gestión de la comunicación en una red de telecomunicaciones inalámbricas, que comprende:

- una puerta de enlace de acceso (eNodoB) (1);

- una red de núcleo (2);

en el que la puerta de enlace de acceso está dispuesta para comunicar con un equipo de usuario y la red de núcleo, y en el que la puerta de acceso está dispuesta para intercambiar operativamente mensajes RRC codificados con otros nodos en la red de telecomunicaciones mediante la utilización de claves RRC para la codificación de mensajes RRC, caracterizado por que el dispositivo está dispuesto para distinguir entre eventos relativos a la confirmación de número de secuencia y eventos relativos a la movilidad, en el que el eNodoB está dispuesto además para acceder a tres contadores diferentes, que son contadores jerárquicos, de tal manera que cuando el primer contador es incrementado debido a que se produce una transición de estado, los contadores segundo y tercero son reiniciados a cero, y, cuando el segundo contador es incrementado debido a una transferencia intercelular, el tercer contador es reiniciado a cero, en el que el tercer contador es un contador de sobrecarga, y en el que cada red de núcleo y puerta de enlace de acceso están dispuestas para utilizar los contadores para producir claves de control de recursos de radio en un algoritmo de codificación.

12. Sistema de acuerdo con la reivindicación 11, dispuesto para:

- realizar una codificación de mensajes RRC relacionados con transiciones de estado en un equipo de usuario en relación con entidades de la red de núcleo (2);

- realizar una codificación de mensajes RRC relacionados con eventos de transferencia intercelular en el equipo de usuario en relación con una parte de red de acceso por radio (1) de la red de comunicaciones,

13. Sistema de acuerdo con la reivindicación 12, en el que se utiliza un algoritmo de codificación para producir la clave RRC.

14. Programa informático guardado en un medio legible por ordenador para su utilización en una parte de un dispositivo de una red de telecomunicaciones inalámbrica, configurado para, cuando es ejecutado en un ordenador, poner en práctica el método de las reivindicaciones 1 a 3.

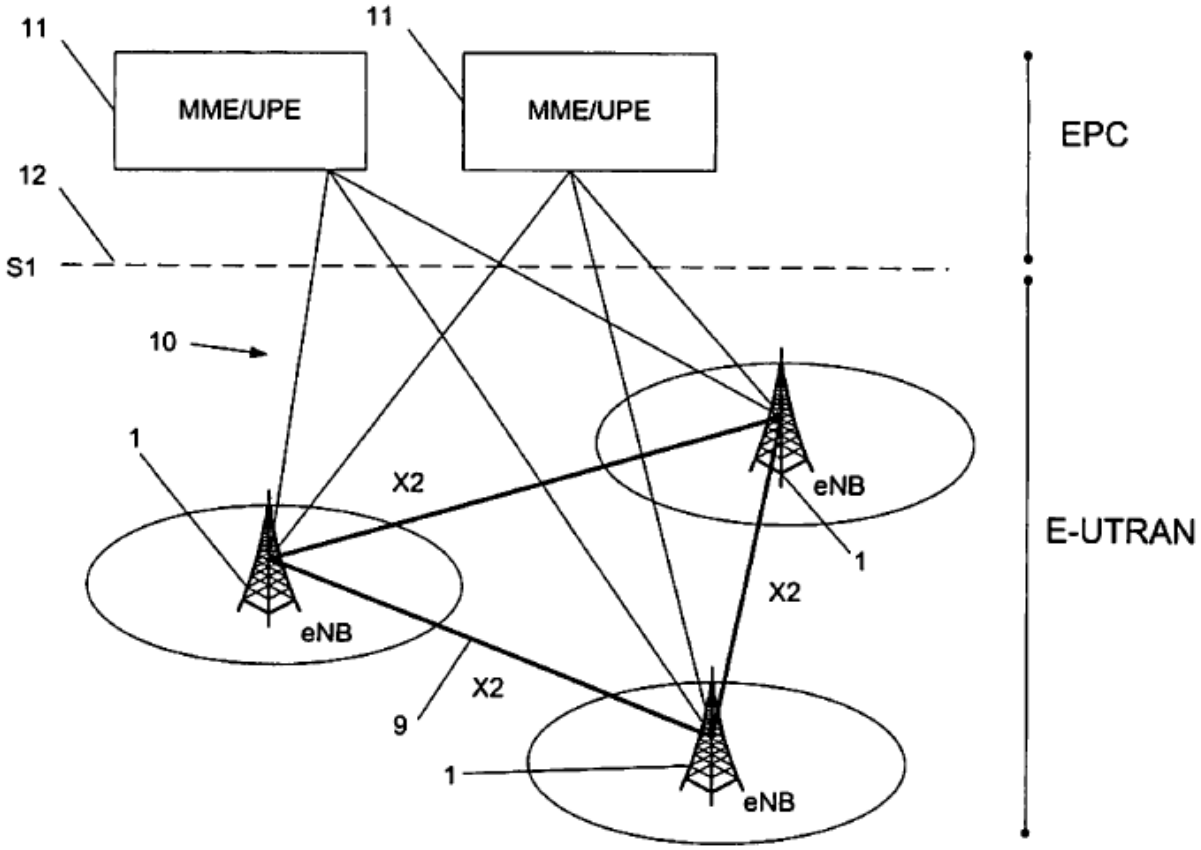
11
MME/UPE
11
MME/UPE
EPC
12
S1
10
1
X2
eNB
1
X2
eNB
E-UTRAN
9
X2
1
eNB

Fig. 1

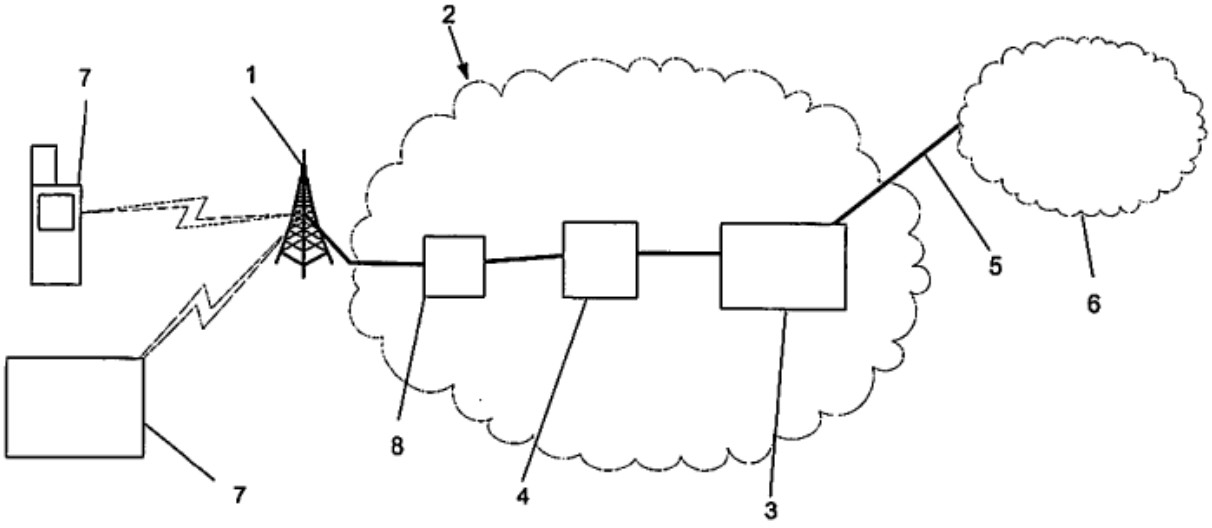

Fig. 2

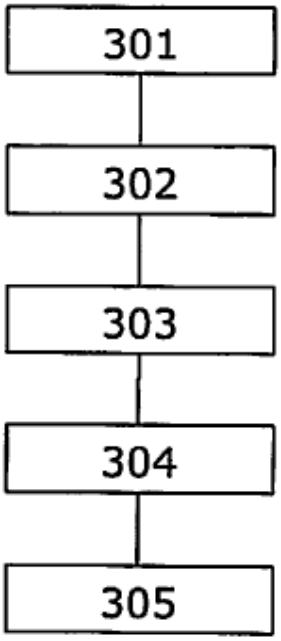

Fig. 3

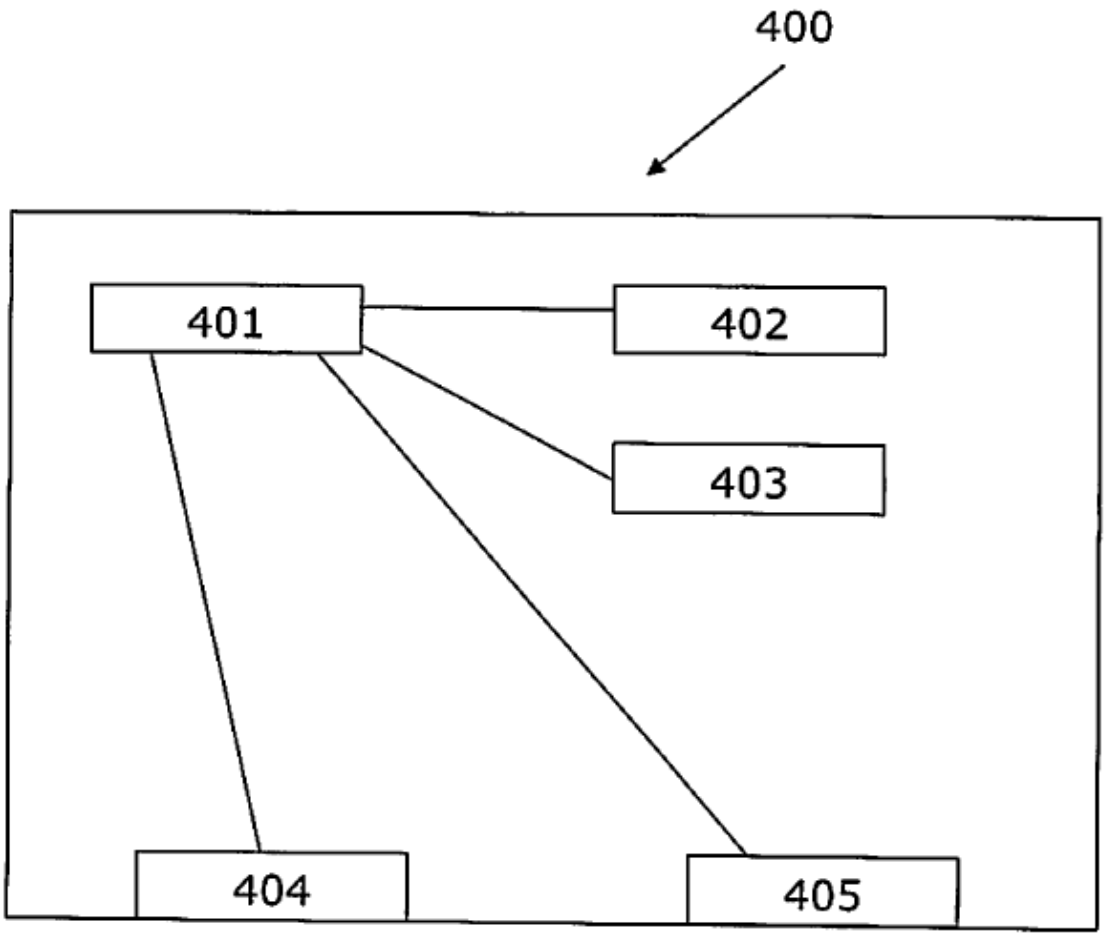

Fig. 4

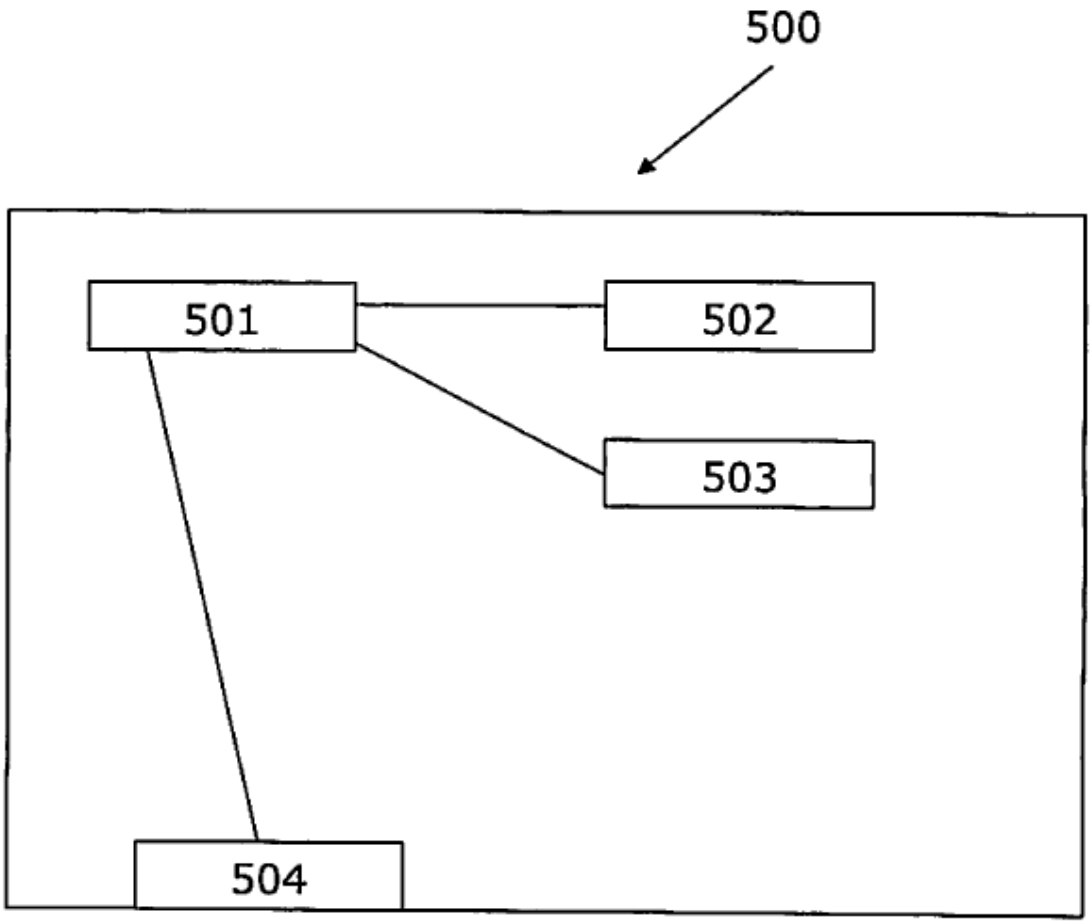

Fig. 5