(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 392 678**

(51) Int. CI.:

G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09749130 .2**

(96) Fecha de presentación: **12.11.2009**

(97) Número de publicación de la solicitud: **2356608**

(97) Fecha de publicación de la solicitud: **17.08.2011**

(54) Título: **Procedimiento y dispositivo de diagnóstico de la primera recepción de un identificador, procedimiento de detección, soporte de registro y programa de ordenador para este procedimiento**

(30) Prioridad:

20.11.2008 FR 0857881

(45) Fecha de publicación de la mención BOPI:

12.12.2012

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

12.12.2012

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
92057 Paris La Défense

(72) Inventor/es:

GADACHA, HAYTHEM

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento y dispositivo de diagnóstico de la primera recepción de un identificador, procedimiento de detección, soporte de registro y programa de ordenador para este procedimiento

La invención se refiere a un procedimiento y un dispositivo de diagnóstico automático de la primera recepción de un identificador. La invención se refiere igualmente a un procedimiento de detección de un mensaje repetido, así como a un soporte de registro y a un programa de ordenador para llevar a cabo estos procedimientos.

Para ilustrar el interés de un procedimiento de diagnóstico de la primera recepción de un identificador, nos posicionamos en un contexto en el que un terminal recibe contenidos multimedia codificados. En tal contexto, se ejecuta un módulo conocido en general como DRM (Digital Rights Management) o CAS (Conditional Access System) en el terminal o en una tarjeta inteligente conectada a este terminal. Este agente DRM o CAS se encarga de verificar las condiciones de acceso al contenido multimedia codificado. Si las condiciones de acceso se cumplen, éste permite la descodificación del contenido multimedia. En caso contrario, se prohíbe la descodificación.

Por ejemplo, las condiciones de acceso son la detección de una licencia válida o de derecho de acceso válido. Por simplificar, supongamos en este caso que las condiciones de acceso consisten en una licencia que incluye:

- una clave CEK de descodificación del contenido multimedia,

- un conjunto de derechos que definen acciones permitidas sobre el contenido multimedia descodificado, tales como su visualización, su impresión, su salvaguarda u otra, y

- limitaciones que limitan el consumo de estos derechos, tales como una duración acumulada máxima T_c de utilización del contenido multimedia o un número máximo N_c de utilizaciones del contenido multimedia.

En estas condiciones, un usuario mencionado puede registrar el mensaje que contiene la licencia y presentarlo después de nuevo al agente DRM o CAS de vez en cuando como si se tratara de un nuevo mensaje. Esta acción de representación repetida de mensaje se denomina “repetición” de mensaje. La tentativa de repetir mensajes se conoce como ataque por repetición.

Cuando el terminal puede comunicar de forma bidireccional con el servidor de licencias que emite el mensaje que contiene la licencia, existe una solución eficaz para luchar contra los ataques por repetición. Esta solución consiste en insertar un número aleatorio determinado por el terminal en cada demanda o petición de licencia emitida por el terminal hacia el servidor. El mensaje que contiene la licencia solicitada, que es emitido por el servidor hacia el terminal, contiene el mismo número aleatorio recuperado en la demanda. Después de esto, el agente DRM o CAS puede diagnosticar simplemente un ataque por repetición comparando el número aleatorio emitido con el recibido como respuesta. No obstante, esta solución necesita una comunicación bidireccional entre el terminal y el servidor. Sin embargo, una comunicación bidireccional de ese tipo no es siempre posible. Por ejemplo, existen situaciones en las que los mensajes no pueden ser transmitidos más que desde el servidor hacia el terminal, pero no en el otro sentido.

En el caso de que la comunicación bidireccional no sea posible, se conoce el hecho de incluir un identificador UID en cada mensaje que no se desea ver repetido. El identificador UID identifica de forma única este mensaje entre un conjunto de mensajes susceptibles de ser generados. Cuando este mensaje es recibido por primera vez, el terminal registra el identificador UID en una memoria anti-repetición del terminal. Esta memoria anti-repetición se denomina a veces “caché anti-repetición”. Por el contrario, si este mensaje es recibido una segunda o más veces, el terminal detecta este ataque por repetición buscando el identificador UID contenido en el mensaje entre los ya contenidos en la memoria anti-repetición. Si el identificador UID se encuentra ya en la memoria anti-repetición, esto significa que este mensaje ha sido ya recibido y que se trata por tanto de un mensaje repetido.

Los documentos FR 2748144 y EP 1827019 A1 divulgan mecanismos anti-repetición.

El procedimiento de diagnóstico puesto en práctica incluye por tanto:

a) la búsqueda de un identificador recién recibido entre los contenidos en una memoria anti-repetición, para diagnosticar si se trata de la primera recepción o no de este identificador recién recibido, pudiendo contener esta memoria a lo sumo M identificadores.

La eficacia de este procedimiento de diagnóstico de la primera recepción de un identificador UID y por tanto de la detección de un mensaje repetido, está limitada por el tamaño de la memoria anti-repetición. En efecto, una memoria tiene necesariamente un tamaño limitado. El tamaño de la memoria anti-repetición depende del terminal utilizado, pero puede ser particularmente reducida cuando el agente DRM o CAS se encuentra en una tarjeta inteligente.

La memoria anti-repetición no puede contener, por tanto, más que un número limitado de identificadores UID. El

número máximo de identificadores UID registrables en la memoria anti-repetición ha sido indicado en la presente memoria como M. Por consiguiente, tras haber recibido por primera vez M mensajes y por tanto M identificadores UID, hay que borrar algunos identificadores UID de la memoria anti-repetición para poder registrar los nuevos identificadores UID recibidos. Por tanto, es posible repetir los mensajes cuyos identificadores UID hayan sido borrados.

La invención plantea mejorar la eficacia del procedimiento de diagnóstico a partir de la primera recepción de un identificador.

Ésta tiene por tanto como objeto un procedimiento de ese tipo que incluye:

b) la construcción de al menos un límite en función de N identificadores ya recibidos, donde N es estrictamente superior a M, estando este límite construido de manera que delimite, por un lado, una gama de identificadores que no han sido aún recibidos, y por otro lado, una gama de identificadores que contiene los N identificadores ya recibidos,

c) la comparación del identificador recién recibido con este límite para determinar si el identificador recién recibido pertenece al intervalo de los identificadores que no han sido aún recibidos,

d) si el identificador recién recibido pertenece al intervalo de los identificadores que no han sido aún recibidos, el diagnóstico de una primera recepción del identificador recién recibido y una nueva construcción del límite en función del identificador recién recibido, y

e) si el identificador recién recibido pertenece al intervalo de identificadores que contiene los N identificadores ya recibidos, la ejecución de la etapa a).

En el procedimiento que antecede, dado que el límite se calcula en función de más identificadores ya recibidos que los M identificadores contenidos en la memoria anti-repetición, este límite conserva intrínsecamente el rastro de un número de identificadores estrictamente superior al número M. Por lo tanto, al menos cuando el identificador recién recibido pertenece al intervalo de identificadores que no han sido aún recibidos, el grado de certidumbre sobre el diagnóstico planteado es superior al obtenido al final de la etapa a). La eficacia de este procedimiento se ve así mejorada.

Los modos de realización de este procedimiento de diagnóstico pueden incluir una o varias de las características siguientes:

• el procedimiento comprende:

- la construcción del Citado límite para diferentes clases de identificadores, siendo construido, para cada clase de identificadores, el límite asociado a esta clase en función de los N identificadores ya recibidos y pertenecientes a esta clase de identificadores,

- la identificación de la clase de identificadores a la que pertenece el identificador recién recibido entre las clases de identificadores existentes, y

- la etapa c) consiste en comparar el identificador recién recibido con el límite asociado a la clase identificada y no comparar el identificador recién recibido con los limites asociados a las clases a las que no pertenece;

• el procedimiento comprende:

- la identificación, con la ayuda de una ley predeterminada de repartición de los diferentes identificadores susceptibles de ser recibidos en diferentes secciones de la memoria anti-repetición, de la sección de la memoria anti-repetición en la que es registrable el identificador recién recibido, entre varias secciones existentes, y

- durante la etapa a), la búsqueda del identificador recién recibido solamente entre los identificadores contenidos en la sección identificada de la memoria anti-repetición y no entre los identificadores contenidos en las secciones de la memoria anti-repetición en las que el identificador recién recibido no es registrable;

• el procedimiento comprende:

- el conteo del número de identificadores recién recibidos durante una gama de tiempo,

- la comparación de este número con un umbral predeterminado, y

- si, y solamente si, el umbral predeterminado es superado, la detección de un ataque por repetición;

• el procedimiento comprende:

- el conteo del número de identificadores durante una gama de tiempo, para el que se ha diagnosticado que éstos no son recibidos por primera vez,

- la comparación de este número con un umbral predeterminado, y

- si, y solamente si, este umbral es superado, la detección de un ataque por repetición;

• si se ejecuta la etapa d), no se ejecuta la etapa a) para este identificador recién recibido;

• la construcción del límite comprende la determinación de un minorante o de un mayorante de los N identificadores ya recibidos.

Estos modos de realización del procedimiento de diagnóstico presentan además las ventajas siguientes:

- el hecho de repartir los identificadores en clases de identificadores y de tener un límite para cada clase de identificadores, permite incrementar la eficacia del procedimiento aumentando el número de casos en los que la etapa a) no tiene que ser ejecutada,

- el hecho de buscar el identificador recién recibido únicamente entre los identificadores contenidos en una sección particular de la memoria anti-repetición permite diagnosticar más rápidamente la primera recepción de un identificador,

- el conteo del número de identificadores recién recibidos y la comparación de este número con un umbral, permite detectar ataques por repetición,

- el conteo del número de identificadores que no son recibidos por primera vez y la comparación de este número con un umbral, permite asimismo detectar ataques por repetición,

- la no ejecución de la etapa a) cuando se ejecuta la etapa d), permite un ahorro del tiempo de ejecución puesto que es posible diagnosticar la primera recepción de un identificador sin tener que buscar ese identificador recién recibido entre los identificadores contenidos en la memoria anti-repetición.

La invención tiene igualmente por objeto un procedimiento de detección de un mensaje repetido, conteniendo cada mensaje un identificador que permite distinguirlo de los otros mensajes, incluyendo este procedimiento un diagnóstico automático de la primera recepción del identificador para establecer si un mensaje recibido es repetido, de acuerdo con el procedimiento de diagnóstico que antecede.

La invención tiene igualmente por objeto un soporte de registro de informaciones y un programa de ordenador que incluye instrucciones para ejecutar uno de los procedimientos anteriores, cuando estas instrucciones son ejecutadas por una computadora electrónica.

Por último, la invención tiene asimismo por objeto un dispositivo de diagnóstico automático de la primera recepción de un identificador, incluyendo este dispositivo:

• un módulo de búsqueda de un identificador recién recibido entre los contenidos en una memoria anti-repetición,

• la memoria anti-repetición, pudiendo contener esta memoria como máximo M identificadores con los que el identificador recién recibido puede ser comparado,

• un constructor de al menos un límite en función de N identificadores ya recibidos, donde N es estrictamente superior a M, estando construido el límite de manera que delimita por un lado una gama de identificadores que no han sido aún recibidos, y por otro lado, una gama de identificadores que contienen los N identificadores ya recibidos,

• un comparador del identificador recién recibido con este límite para determinar si el identificador recién recibido pertenece a la gama de identificadores que no han sido aún recibidos, siendo adecuado este comparador para:

- diagnosticar una primera recepción del identificador recién recibido si este nuevo identificador pertenece a la gama de identificadores que no han sido aún recibidos, y activar el constructor para poner en marcha una nueva construcción del límite en función del identificador recién recibido, y

- activar el módulo de búsqueda para poner en marcha la búsqueda del identificador recién recibido entre los contenidos en la memoria anti-repetición si el identificador recién recibido pertenece a la gama de identificadores que contienen los N identificadores ya recibidos.

La invención podrá ser mejor comprendida con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitativo, y realizada con referencia a los dibujos anexos, en los que:

- la figura 1 es una ilustración esquemática de la arquitectura de un sistema de transmisión de informaciones equipado con un dispositivo de diagnóstico de la primera recepción de un identificador,

- la figura 2 es una ilustración esquemática de una porción de un mensaje transmitido por el sistema de la figura 1,

- la figura 3 es un organigrama de un procedimiento de detección de un mensaje repetido que utiliza el dispositivo de diagnóstico del sistema de la figura 1.

En estas figuras, se utilizan las mismas referencias para designar los mismos elementos.

En lo que sigue de la presente descripción, las características y funciones bien conocidas por el experto en la materia no van a ser descritas en detalle.

La figura 1 representa un sistema 2 de transmisión de informaciones. A título ilustrativo, este sistema es un sistema de transmisión de contenido multimedia codificado. Contiene un servidor 4 de licencias conectado a una multiplicidad de terminales por medio de una red 6 de transmisión de informaciones. Por ejemplo, la red 6 es una red de transmisión de informaciones por satélite.

Para simplificar la figura 1, se ha representado solamente un terminal 8

El servidor 4 emite mensajes con destino a los terminales. Estos mensajes contienen las licencias que permiten a cada terminal descodificar un contenido multimedia recibido previamente. A este efecto, el servidor 4 comprende un generador 10 de identificadores UID. Este generador 10 genera, por cada mensaje emitido por el servidor 4, un identificador UID que identifica de forma única a este mensaje entre el conjunto de los mensajes enviados. Por ejemplo, el identificador UID se obtiene construyendo una huella digital de la licencia con la ayuda de funciones tales como una función de hash. El identificador UID puede ser obtenido asimismo generando un número aleatorio.

El tamaño requerido del identificador UID es una función del número de terminales a los que deben ser transmitidos los mensajes, así como del número de mensajes transmitidos a cada terminal. En este caso, el número de mensajes transmitidos a cada terminal corresponde al número de licencias compradas a partir de este terminal. Típicamente, el identificador UID está codificado sobre 16 octetos.

El terminal 8 recibe los mensajes transmitidos por el servidor 4. Por ejemplo, este terminal 8 es un descodificador apto para recibir una licencia y el contenido multimedia cifrado que se ha de descifrar después con la ayuda de la clave contenida en la licencia, para permitir su visualización no codificada en una pantalla 10.

El terminal 8 comprende un dispositivo 12 de diagnóstico automático de la primera recepción de un identificador UID. Para simplificar las ilustraciones, el dispositivo 12 ha sido representado por fuera del terminal 8. Sin embargo, en la práctica, este dispositivo 12 está integrado en el terminal 8 o implantado en un procesador de seguridad conectado al terminal 8. Por ejemplo, el procesador de seguridad es una tarjeta inteligente. Típicamente, el dispositivo 12 forma parte de un agente DRM o CAS.

El dispositivo 12 comprende una memoria anti-repetición 14. En este caso, esta memoria 14 está dividida en varias secciones SE_j. La intersección de dos secciones SE_j cualesquiera es nula.

El dispositivo 12 comprende igualmente una computadora electrónica 16 capacitada para diagnosticar la primera recepción de un identificador UID. A este efecto, esta computadora comprende:

- un módulo 20 de búsqueda de identificadores UID entre los contenidos en la memoria 14,

- un comparador 22 del identificador recién recibido con los límites,

- un constructor 24 de los límites utilizados por el comparador 22,

- un contador 26 de identificadores UID recibidos, y

- un contador 28 de mensajes repetidos.

Estos elementos están conectados entre sí, así como con la memoria 14 y con una memoria 30 por medio de un bus de comunicación.

En este caso, el dominio de los valores de los identificadores UID está repartido en diferentes clases Cj. Cada

identificador UID está así clasificado en una clase Cj. Para ello, se utiliza una función f_c predeterminada de clasificación. Esta función f_c devuelve por cada identificador UID el índice j de la clase a la que pertenece. En este caso, la función f_c es tal que la unión del conjunto de clases Cj corresponde al conjunto de identificadores UID que pueden ser generados en el sistema 2. Con preferencia, la intersección, dos a dos, de las clases Cj está vacía. De ese modo, un identificador UID dado no puede pertenecer más que a una sola clase Cj. Cada clase Cj reagrupa varios identificadores UID posibles.

Con preferencia, esta función f_c es secreta. Por ejemplo, la función f_c es la función que devuelve el resultado de la división completa del identificador UID recién recibido por 2^{m-8} donde m es el número de bits máximo utilizado para codificar un identificador UID en el sistema 2. Así, una función f_c de ese tipo divide el conjunto de identificadores UID que es posible generar en 2^8 clases. El resultado de esta función permite identificar la clase a la que pertenece el identificador UID recién recibido.

La memoria 30 comprende en particular una tabla 32 asociativa. Esta tabla 32 asocia a cada clase Cj de identificadores un límite S_{minj} y un límite S_{maxj} construidos pro el constructor 24. El límite S_{minj} constituye un minorante de los identificadores UID ya recibidos y pertenecientes a la clase C_j. A la inversa, el límite S_{maxj} constituye un mayorante para estos mismos identificadores UID ya recibidos. Así, estos límites delimitan un intervalo $[S_{minj}; S_{maxj}]$ que contiene todos los identificadores UID ya recibidos y que pertenecen a la clase C_j. Estos límites delimitan también dos intervalos $[-2^{m-1}; S_{minj}]$ y $[S_{maxj}; +2^{m-1}]$ de identificadores de UID que no han sido aún recibidos, donde m es el número de bits máximo utilizable para codificar un identificador UID en el sistema 2. En este caso, m es igual a 128.

Los contadores 26 y 28 están conectados a un reloj 34 fiable.

La computadora 16 es por ejemplo una computadora programable capacitada para ejecutar instrucciones registradas en un soporte de registro de informaciones. A este efecto, la computadora 16 está conectada a una memoria 36 que contiene un programa formado por instrucciones para la ejecución del procedimiento de la figura 3.

La figura 2 representa una porción de un mensaje transmitido desde el servidor 4 hacia el terminal 8. Este mensaje contiene una licencia L. La licencia L contiene un identificador UID, una clave criptográfica CEK, los derechos de explotación DE, las limitaciones CT y una signatura MAC que permite verificar la integridad de la licencia. La signatura MAC se calcula cobre el conjunto del contenido de la licencia tomando en consideración, en particular, el identificador UID.

Los derechos de explotación, así como las limitaciones sobre estos derechos de explotación, han sido definidos en la introducción de la presente descripción.

Ahora se va a describir el funcionamiento del sistema 2 con mayor detalle, con relación al procedimiento de la figura 3.

Inicialmente, durante una etapa 50, el terminal 8 recibe un nuevo mensaje transmitido por el servidor 4 a través de la red 6.

Durante una etapa 52, el terminal extrae el identificador UID contenido en el mensaje, y lo transmite al dispositivo 12. De manera más precisa, el identificador UID extraído está contenido en la licencia L. El identificador así transmitido al dispositivo 12 constituye el identificador UID recién recibido.

Durante una etapa 54, el dispositivo 12 identifica la clase C_j a la que pertenece el identificador UID recién recibido. Para ello, se aplica la función f_c al identificador UID recién recibido.

A continuación, durante una etapa 56, el dispositivo 12 busca en la tabla 32 cuáles son los límites S_{minj} y S_{maxj} asociados a la clase C_j identificada durante la etapa 54. Los limites así hallados son utilizados a continuación para el conjunto de las etapas descritas en lo que sigue.

Durante una etapa 58, el comparador 22 compara el identificador UID recién recibido con los límites S_{minj} y S_{maxj} hallados en la etapa 56. Si el identificador UID recién recibido pertenece al intervalo $[-2^{m-1}; S_{minj}]$ o $[S_{maxj}; +2^{m-1}]$, entonces el procedimiento avanza hasta una etapa 60. En caso contrario, se avanza a una etapa 62.

Durante la etapa 60, se diagnostica, sin proceder a ninguna comparación del identificador UID recién recibido con los contenidos en la memoria, que este identificador se ha recibido por primera vez. Por consiguiente, el mensaje recibido no se identifica como un mensaje repetido. Por ejemplo, esta información es enviada al terminal 8 que acepta el mensaje recibido y lo trata. El tratamiento consiste, por ejemplo, en extraer la clave CEK de la licencia, y después en descifrar con la ayuda de esta clave extraída, el contenido multimedia para poder visualizarlo en la pantalla 10.

Durante la etapa 60, se discrimina el caso en que el identificador UID es estrictamente superior al límite S_{maxj} del

caso en que el identificador UID es estrictamente inferior al límite S_{minj}.

Si el identificador UID es estrictamente superior al límite S_{maxj}, entonces durante una etapa 64, se construye un nuevo valor del límite S_{maxj} en función del identificador UID recién recibido. En efecto, el valor actual del límite S_{maxj} ya no es un mayorante de los identificadores UID ya recibidos y pertenecientes a la clase C_j. Por ejemplo, la construcción del nuevo valor del límite S_{maxj} consiste en reemplazar su valor actual por el valor del identificador UID recién recibido.

Una vez que el nuevo valor del límite S_{maxj} ha sido construido, durante una etapa 66, éste se registra en la tabla 32 en lugar del antiguo valor.

En un caso en el que el identificador UID recién recibido sea estrictamente inferior al límite S_{minj}, durante una etapa 68, se construye un nuevo valor del límite S_{minj} a partir del valor del identificador UID recién recibido. En efecto, en ese caso, el valor actual del límite S_{minj} no es ya un minorante de los identificadores UID ya recibidos y pertenecientes a la clase C_j. Por ejemplo, la construcción del nuevo valor del limite S_{minj} consiste en reemplazar su valor actual por el valor del identificador UID recién recibido.

Durante una etapa 70, el nuevo valor del límite s_{minj} se registra en la tabla 32 en lugar de su antiguo valor.

Al final de la etapa 66 o de la etapa 70, se avanza a una etapa 71 de identificación de la sección SE_i en la que debe ser registrado el antiguo valor del límite S_{maxj} o S_{minj}. En efecto, el antiguo valor del límite es el de un identificador UID recibido por primera vez, pero que no ha sido aún registrado en la memoria 14. Se trata por lo tanto como un identificador UID recibido por primera vez. Así, en las explicaciones que siguen, este antiguo valor del límite se denomina “identificador UID recién recibido”. A este efecto, se utiliza una función f_d predeterminada de repartición. Esta función f_d devuelve por cada identificador UID el índice j de la sección en la que debe ser registrado. En este caso, la función f_d es sobreyectiva. Además, asocia a cada identificador UID que puede ser generado un solo índice j. De ese modo, un identificador UID dado no puede ser registrado más que en una sola sección SE_j. Cada sección SE_j permite registrar varios identificadores UID. Por el contrario, el tamaño de cada sección SE_j no puede contener todos los identificadores UID susceptibles de ser generados en el sistema 2 y que son registrables en esa sección.

Por ejemplo, la función f_d es idéntica a la función f_c. En ese caso, es posible utilizar el resultado de la etapa 54. Otro ejemplo de función f_d es la función que devuelve el resto del identificador UID módulo 1024, lo que permite en ese caso reagrupar los identificadores en 1024 secciones.

A continuación, durante la etapa 72, el identificador UID recién recibido se registra en la sección identificada durante la etapa 71. Si esta sección no está llena, el identificador UID recién recibido es registrado adicionalmente a los identificadores UID ya contenidos en la misma sección. Por el contrario, si la sección SE_j de la memoria 14 ya está llena, el identificador UID se registra en lugar de otro identificador UID contenido en la misma sección. Este otro identificador UID puede ser, por ejemplo, elegido al azar o en base al principio del primero en entrar, primero en salir.

Al final de la etapa 72, el procedimiento retorna a la etapa 50.

La etapa 62 consiste en determinar en qué sección SE_j debe ser registrado el identificador UID recién recibido. Esta etapa es idéntica a la etapa 71.

A continuación, durante una etapa 73, el identificador UID recién recibido se busca únicamente entre los identificadores registrados en la sección identificada durante la etapa 62. Se comprende por tanto que la repartición de los identificadores UID en las diferentes secciones de la memoria con la ayuda de la función f_d permite acelerar esta comparación puesto que solamente una parte de los identificadores registrados en la memoria 14 deben ser comparados con el identificador UID recién recibido.

Si el identificador UID recién recibido es idéntico a uno de los registrados en la memoria 14, entonces, durante una etapa 74, el dispositivo 12 diagnostica que no se trata de la primera recepción de este identificador. Por consiguiente, el mensaje que contiene este identificador ha sido repetido. Esta información se comunica al terminal 8.

Esta identificación de un mensaje repetido dispara en el terminal 8 medidas correctoras o coercitivas. Por ejemplo, el mensaje repetido puede ser rechazado de modo que la clave CEK no sea extraída de la licencia, lo que hace imposible el desciframiento del contenido multimedia.

En el caso de que el identificador UID recién recibido no esté en la sección identificada durante la etapa 62, entonces, durante una etapa 76, el dispositivo 12 diagnostica que este identificador UID es recibido por primera vez. Esta información es comunicada al terminal 8 que reacciona en consecuencia. Por ejemplo, el terminal 8 acepta el mensaje recibido, extrayendo la licencia y en particular la clave CEK que autoriza al desciframiento del contenido multimedia con la ayuda de la clave extraída.

A continuación, durante una etapa 78, el identificador UID recién recibido es registrado en la sección identificada durante la etapa 62. Esta etapa es idéntica a la etapa 72.

Al final de la etapa 74 ó 78, el procedimiento retorna a la etapa 50.

En este caso, el valor del límite S_{maxj} se construye por recurrencia a partir del antiguo valor del límite S_{maxj} y del identificador recién recibido. Por consiguiente, el valor del límite S_{maxj} es función de los N identificadores ya recibidos y pertenecientes a la misma clase C_j. El valor del límite S_{maxj} no es reinicializado. Así, rápidamente, este número N supera al número M de identificadores registrables en la memoria 14 y a los que puede ser comparado el identificador recién recibido. En el caso en que la memoria 14 está dividida en varias secciones, el número M corresponde al número máximo de identificadores UID registrables en la sección SE_j. En efecto, en este caso, el identificador recién recibido se busca únicamente entre los contenidos en la sección SE_j en la que debe ser registrado. Ocurre lo mismo para la construcción del límite S_{minj}.

En paralelo con las etapas 50 a 78, el dispositivo 12 procede a una fase 84 de identificación de un ataque masivo por repetición.

Inicialmente, durante una etapa 86, el instante actual t_0 proporcionado por el reloj 34 es registrado por el contador 26. Al mismo tiempo, un contador Nm-c es inicializado a cero.

A continuación, durante una etapa 88, se incrementa en uno el contador Nm-c por cada identificador UID recién recibido. Después, durante una etapa 90, el contador Nm-c se compara con un umbral Nm-s predeterminado. Este umbral Nm-s es, por ejemplo, fijado por el operador. Por ejemplo, su valor es 40.

Si el contador Nm-c no ha alcanzado el valor del umbral Nm-s, entonces el procedimiento retorna a la etapa 88.

Si el contador Nm-c ha alcanzado el valor del umbral Nm-s, entonces el instante actual t_1 es registrado por el contador 26.

A continuación, durante una etapa 92, intervalo de tiempo Δt_c entre los instantes t_0 y t_1, se compara con un umbral de tiempo predeterminado Ts. Este umbral Ts es fijado por el operador. Por ejemplo, este umbral es igual a 6 horas.

Si el intervalo Δt_c es inferior al umbral Ts, durante una etapa 94, el dispositivo 12 detecta un ataque masivo por repetición. En efecto, un ataque masivo por repetición se traduce en el envío de un número anormalmente elevado de identificadores UID durante un período de tiempo corto. En caso contrario, no se detecta ningún ataque por repetición. Si se detecta un ataque por repetición, esta información es comunicada al terminal 8. Como respuesta, el terminal 8 dispara medidas correctoras o coercitivas.

La fase 84 se repite de vez en cuando.

En paralelo con la fase 84, se ejecuta otra fase 100 de detección de un ataque masivo por repetición.

Inicialmente, durante una etapa 102, el contador 28 registra el instante actual t_0 e inicializa un contador Nm-r en el valor cero.

A continuación, durante una etapa 104, el contador Nm-r se incrementa en uno cada vez que se diagnostica que un identificador UID ha sido ya recibido. A continuación, durante una etapa 106, el contador Nm-r se compara con un umbral Nm-r-s. El valor de este umbral Nm-r-s es, por ejemplo, de diez.

Tantas veces como sea este contador Nm-r inferior a este umbral Nm-r-s, se repite la etapa 104.

Por contra, en caso contrario, el contador 28 registra el instante actual t_1. A continuación, durante una etapa 108, el intervalo Δt_c obtenido calculando la diferencia ente los instantes t_0 y t_1, se compara con un umbral T_r. El valor de este umbral T_r es, por ejemplo, de 5. Si el intervalo Δt_r es inferior al umbral T_r, entonces esto significa que un número importante de identificadores UID no han sido recibidos por primera vez durante un período de tiempo predeterminado. Una situación de ese tipo es representativa de un ataque masivo por repetición. Así, durante una etapa 110, el contador 28 detecta la existencia de un ataque masivo por repetición. Esta información es transmitida al terminal 8 que la trata de forma similar a la que se ha descrito en relación con la etapa 94.

Después de la etapa 110, o si el intervalo Δt_r es superior al umbral T_r, el procedimiento retorna a la etapa 102.

Así, las fases 84 y 100 permiten detectar ataques por repetición y con ello tomar las medidas correctoras o coercitivas correspondientes. Estas medidas correctoras o coercitivas pueden ser una sanción directa tal como la prohibición de cualquier descodificación con la ayuda del terminal 8. Estas sanciones pueden ser igualmente

sanciones progresivas que aumenten a medida del número de ataques por repetición detectados. Por último, la medida correctora o coercitiva puede aumentar también la vigilancia sobre los ataques por repetición para confirmar la realidad de tales ataques. Se puede aumentar la vigilancia aumentando la frecuencia a la que se ejecutan las fases 84 y 100.

Otros numerosos modos de realización son posibles. Por ejemplo, cuando un servidor tiene necesidad de detectar si se han recibido los identificadores por primera vez, el dispositivo de diagnóstico de la primera recepción de un identificador que se ha descrito en la presente memoria, puede ser puesto en práctica en el lado del servidor. Por ejemplo, en ese caso, éstas son las peticiones transmitidas desde los terminales hacia el servidor que incluyen cada uno de los identificadores UID.

El terminal 8 no es necesariamente un descodificador. Se puede tratar de un terminal móvil, de un ordenador, de una tarjeta inteligente, o de cualquier otro terminal electrónico en el que sea necesario identificar la primera recepción de un identificador.

La memoria 14 puede ser un fichero tal como, por ejemplo, un fichero almacenado en un disco duro.

En la memoria 14, los identificadores UID pueden estar asociados a etiquetas de tiempo TS o “Time Stamp”. Estas etiquetas de tiempo indican cuál ha sido el orden de registro de los identificadores UID en la memoria 14, o cuál es el instante de registro de cada uno de esos identificadores. Estas etiquetas de tiempo permiten reemplazar el identificador UID más viejo contenido en una sección o en el conjunto de la memoria 14, por el identificador recién recibido cuando ésta se ha llenado. Cuando se utilizan etiquetes de tiempo, el reloj 34 puede ser asimismo omitido. Por ejemplo, para la realización de las fases 84 y 100, se utiliza la etiqueta de tiempo asociada a cada identificador recibido antes que una medición del instante de recepción de este identificador UID con la ayuda del reloj 34.

Los valores de los límites S_{minj} y S_{maxj} asociados a cada clase pueden ser reinicializados de vez en cuando.

Los valores de los límites S_{minj} y S_{maxj} no son necesariamente inicializados a cero. Por ejemplo, los límites S_{minj} y S_{maxj} pueden ser inicializados en valores no nulos obtenidos a partir del conocimiento que se tiene sobre los identificadores UID ya utilizados en el sistema 2.

Otras funciones f_c son posibles. Otro ejemplo de función f_c es la función que retorna el resto del identificador UID módulo 127, lo que permite en ese caso definir 127 clases.

La función f_d puede ser diferente de la función f_c. En ese caso, es necesario aplicar esta función f_d al valor del identificador UID recién recibido durante la etapa 71 para determinar en qué sección éste debe ser registrado.

Las funciones f_c y f_d son conocidas públicamente o, por el contrario, mantenidas en secreto.

La función f_c o la f_c puede, por ejemplo, ser elegida en los códigos de redundancia cíclica CRC8 o CRC16 para definir respectivamente 256 secciones o 65535 secciones.

En un modo de realización alternativo, la función f_d puede ser seleccionada dinámicamente según la clase de identificador UID recién recibido, estando esta última determinada por f_c. En ese caso, la función f_d aplicada podrá ser indicada como f_{cd} o $f_d(f_c)$.

Los mensajes que contienen los identificadores UID no son necesariamente recibidos por medio de una red de telecomunicación. Por ejemplo, estos mensajes pueden ser transportados desde el servidor 4 hasta el terminal 8 por medio de un soporte de registro tal como un CD-ROM o una llave USB (Universal Serial Bus).

La tabla 32 asociativa puede ser reemplazada por otros mecanismos similares. Por ejemplo, los límites S_{minj} y S_{maxj} pueden ser almacenados en la sección de la memoria 14 correspondiente a la clase a la que estén asociados.

Durante la etapa 58, es igualmente posible transformar con la ayuda de una función monótona g, el identificador UID recién recibido en un identificador UID’. A continuación, es el identificador UID’ el que se compara con límites S_{minj}’ y S_{maxj}’. En esta variante, los límites S_{minj}’ y S_{maxj}’ están construidos según se ha descrito en relación con las etapas 64 y 68, excepto en que la construcción del nuevo valor de los límites S_{minj}’ y S_{maxj}’ se realiza utilizando el identificador UID’ en lugar del identificador UID. Estos límites S_{minj}’ y S_{maxj}’ son construidos por tanto en función de N identificadores UID ya recibidos. Además, la función g es una función monótona creciente o decreciente. Así, la comparación del identificador UID’ con los límites S_{minj}’ y S_{maxj}’ es el equivalente funcional de una comparación del identificador UID con los límites S_{minj} y S_{maxj}. De ese modo, se califica igualmente esta comparación del identificador UID’ con el límite S_{minj}’ o S_{maxj}’ como etapa de “comparación del identificador UID recién recibido con el límite S_{minj} o S_{maxj}”.

Con preferencia, los límites S_{minj} y S_{maxj} se utilizan simultáneamente. Sin embargo, lo que se ha descrito funciona igualmente si se utiliza solamente uno de estos límites S_{minj} o S_{maxj}.

En un modo de realización simplificado, los identificadores UID no están repartidos entre diferentes clases. En ese caso, no existe más que un solo límite S_{min} y un solo límite S_{max} asociado al conjunto de los identificadores susceptibles de ser generados. De forma similar, en un modo de realización simplificado, la memoria 14 no está dividida en varias secciones. Esto permite evitar el recurso a una función de repartición.

Los umbrales utilizados durante las fases 84 y 100 pueden ser fijados en función de un histórico de intercambios de mensajes entre el terminal 8 y el servidor 4, o en función de un perfil de usuario.

En otro modo de realización, el período de observación Δt_c o Δt_r es fijo.

En otro modo de realización simplificado, los contadores 26 y 28 se omiten y las fases 84 y 100 lo son igualmente. Así, en esos modos de realización, los ataques por repetición no son detectados en función del número de identificadores UID recibidos o en función del número de veces que un identificador UID se diagnostica como no recibido por primera vez.

REIVINDICACIONES

1.- Procedimiento de diagnóstico automático de la primera recepción de un identificador, incluyendo este procedimiento:

a) la búsqueda (73) de un identificador recién recibido entre los contenidos en una memoria anti-repetición, pudiendo contener esta memoria anti-repetición a lo sumo M identificadores a los que el identificador recién recibido puede ser comparado;

caracterizado porque comprende;

b) la construcción (64, 68) de al menos un límite en función de los N identificadores ya recibidos, donde N es estrictamente superior a M, siendo construido este límite de manera que delimita, por un lado, una gama de identificadores que no han sido aún recibidos, y por otro lado, una gama de identificadores que contienen los N identificadores ya recibidos,

c) la comparación (58) del identificador recién recibido con este límite para determinar si el identificador recién recibido pertenece a la gama de los identificadores que no han sido aún recibidos,

d) si el identificador recién recibido pertenece a la gama de identificadores que no han sido aún recibidos, el diagnóstico (60) de una primera recepción del identificador recién recibido y una nueva construcción (64, 68) del límite en función del identificador recién recibido, y

e) si el identificador recién recibido pertenece a la gama de los identificadores que contienen los N identificadores ya recibidos, la ejecución de la etapa a).

2.- Procedimiento según la reivindicación 1, en el que el procedimiento comprende:

- la construcción (64,68) de dicho límite para diferentes clases de identificadores, estando el límite para cada clase de identificadores asociados a esta clase, construido en función de los citados al menos N identificadores ya recibidos y pertenecientes a esta clase de identificadores,

- la identificación (54) de la clase de identificadores a la que pertenece el identificador recién recibido ente las clases de identificadores existentes, y

- la etapa c) consiste en comparar (58) el identificador recién recibido con el limite asociado a la clase identificada y en no comparar el identificador recién recibido con los limites asociados a las calases a las que no pertenece.

3.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:

- la identificación (62, 71), con la ayuda de una ley predeterminada de repartición de los diferentes identificadores susceptibles de ser recibidos en diferentes sección de la memoria anti-repetición, de la sección de memoria anti-repetición en la que el identificador recién recibido es registrable, entre varias secciones existentes, y

- durante la etapa a), la búsqueda (73) del identificador recién recibido solamente entre los identificadores contenidos en la sección identificada de la memoria anti-repetición y no entre los identificadores contenidos en las secciones de la memoria anti-repetición en las que el identificador recién recibido no es registrable.

4.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:

- el conteo (88) del número de identificadores recién recibidos durante un intervalo de tiempo,

- la comparación (90) de este número con un umbral predeterminado, y

- si, y solamente si, el umbral predeterminado es rebasado, la detección de un ataque por repetición (94).

5.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:

- el conteo (104) del número de identificadores, durante un intervalo de tiempo, para los que se diagnostique que no son recibidos por primera vez,

- la comparación (106) de este número con un umbral predeterminado, y

- si, y solamente si, este umbral es rebasado, la detección de un ataque por repetición (110).

6.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que, si se ejecuta la etapa d), no se

ejecuta la etapa a) para este identificador recién recibido.

7.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la construcción del límite comprende la determinación de un minorante o de un mayorante de los N identificadores ya recibidos.

8.- Procedimiento de detección de la repetición de un mensaje, conteniendo cada mensaje un identificador que permite distinguirlo de los otros mensajes, incluyendo este procedimiento:

- un diagnostico automático de la primera recepción del identificador para establecer si un mensaje recibido está repetido;

caracterizado porque el diagnóstico se realiza conforme al procedimiento de diagnóstico de una cualquiera de las reivindicaciones anteriores.

9.- Soporte (36) de registro de informaciones, caracterizado porque incluye instrucciones para la ejecución de un procedimiento conforme a una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por una computadora electrónica.

10.- Programa de ordenador, caracterizado porque incluye instrucciones para la ejecución de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8, cuando estas instrucciones son ejecutadas por una computadora electrónica.

11.- Dispositivo de diagnóstico automático de la primera recepción de un identificador, incluyendo este dispositivo:

• un módulo de búsqueda (20) de un identificador recién recibido entre los contenidos en una memoria anti-repetición,

• una memoria (14) anti-repetición, pudiendo esta memoria contener a lo sumo M identificadores a los que puede ser comparado el identificador recién recibido;

caracterizado porque el dispositivo comprende:

• un constructor (24) de al menos un límite en función de N identificadores ya recibidos, donde N es estrictamente superior a M, estando construido el límite de manera que delimita, por un lado, una gama de identificadores que no han sido aún recibidos y, por otro lado, una gama de identificadores que contienen los N identificadores ya recibidos,

• un comparador (22) del identificador recién recibido con este límite, para determinar si el identificador recibido pertenece a la gama de los identificadores que no han sido aún recibidos, siendo este comparador adecuado para:

- diagnosticar una primera recepción del identificador recién recibido si este nuevo identificador pertenece a la gama de los identificadores que no han sido aún recibidos, y activar el constructor para poner en marcha una nueva construcción del limite en función del identificador recién recibido, y

- activar el módulo de búsqueda para poner en marcha la búsqueda del identificador recién recibido entre los contenidos en la memoria anti-repetición si el identificador recién recibido pertenece a la gama de los identificadores que contienen los N identificadores ya recibidos.

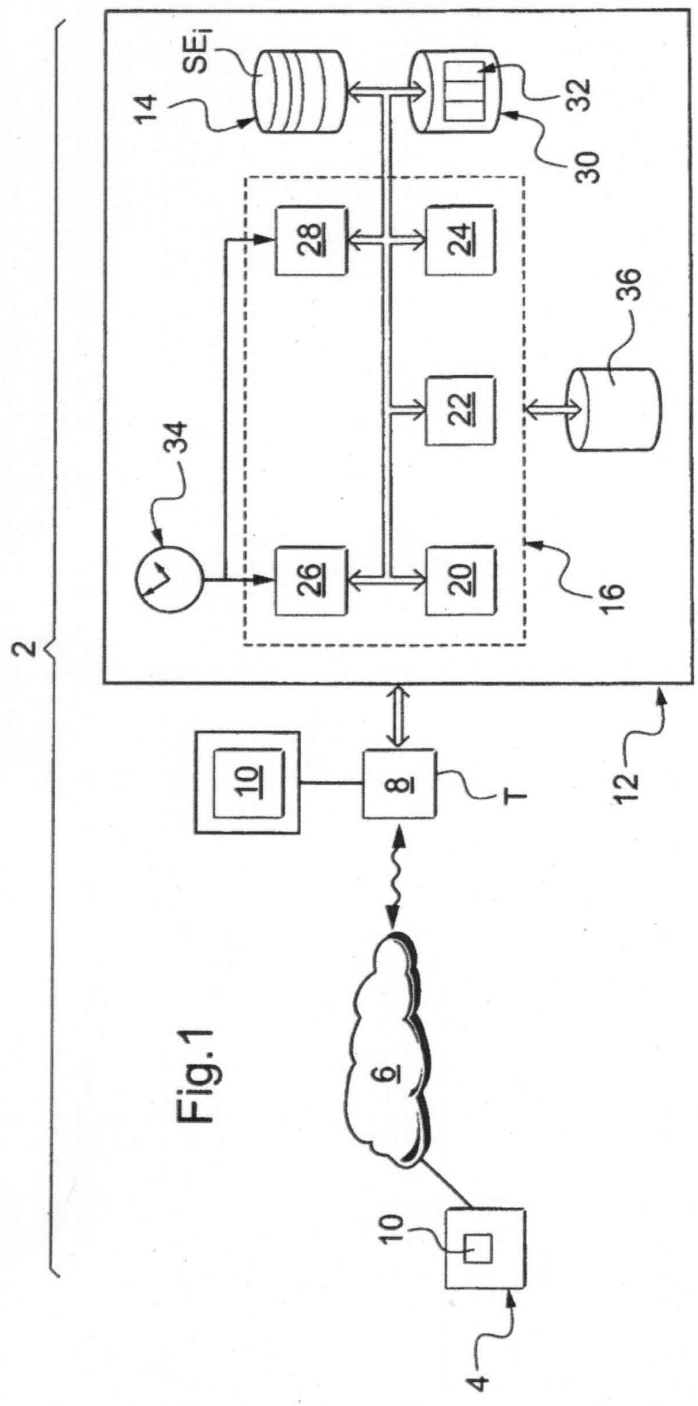

2
14
SEi
32
30
28
24
36
34
22
26
20
16
10
8
T
12
6
10
4

Fig.1

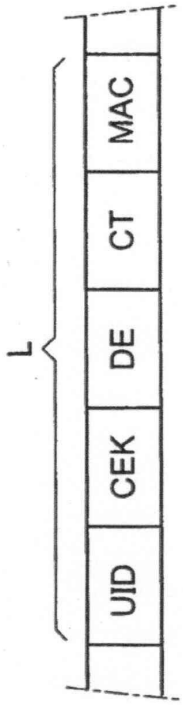
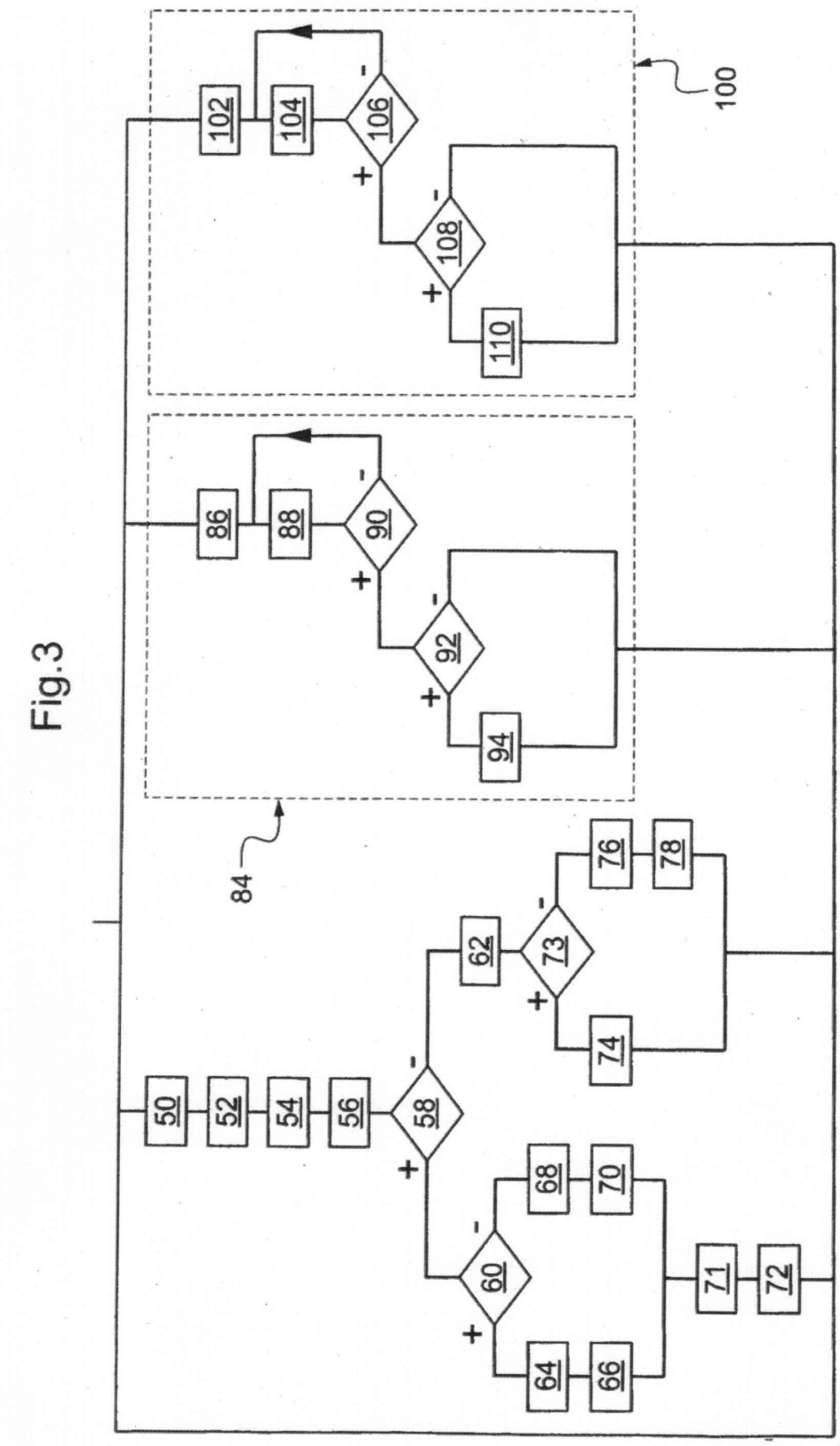

L
UID
CEK
DE
CT
MAC

Fig.2

Fig.3


100
102
104
106
108
110
84
86
88
90
92
94
50
52
54
56
58
60
62
64
66
68
70
71
72
73
74
76
78
+
-