(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 808**

(51) Int. CI.:

H04L 12/40 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.11.2014 E 14194141 (9)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2019 EP 2876846**

(54) Título: **Procedimiento de detección de la repetición de un paquete de datos**

(30) Prioridad:

20.11.2013 FR 1302679

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.11.2019

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

DUPUTZ, PATRICK;
FOULADGAR, SEPIDEH y
PINTO, CARLOS

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de detección de la repetición de un paquete de datos

[0001] La presente invención se refiere a un procedimiento del tipo para detectar si un paquete de una pluralidad de paquetes emitidos por al menos una estación emisora a través de una red ha sido repetido, comprendiendo cada paquete un mensaje y un identificador del paquete, siendo la pluralidad de paquetes emitidos sucesivamente en varios periodos de tiempo consecutivos, comprendiendo el procedimiento las etapas siguientes:

- recepción por al menos una estación receptora del paquete y lectura del identificador del paquete recibido para obtener un identificador recibido,
- consulta mediante la estación receptora de una base de datos de identificadores que han sido ya recibidos para determinar si el identificador recibido ha sido ya recibido, y
- si el identificador recibido no ha sido ya recibido, actualización de la base de datos que comprende una memorización del identificador recibido.

[0002] La invención está relacionada con el ámbito de la seguridad en redes. El objetivo pretendido por la invención es la protección contra la repetición de paquetes de datos enviados sobre todo vía red tolerante a los plazos, o DTN (en inglés: *Delay Tolérant Network).* Por «repetición», se entiende el hecho de que un paquete de datos sea repetido, i. e. emitido por una entidad no autorizada.

[0003] El envío de paquetes de datos a través de un DTN engendra a veces una perturbación importante del ordenamiento de los paquetes. En recepción, la detección de la repetición de un paquete se complica. En efecto, se conserva la traza de todos los paquetes recibidos sobre una duración muy larga. Esto crea necesidades importantes en cuanto a potencia de tratamiento y en capacidad de memoria.

[0004] La mayoría de las soluciones ofrecidas en la técnica anterior se basan en la puesta en marcha de un contador en la emisión, que identifica de manera única los paquetes transmitidos, y de una tabla anti repetición deslizante, de tamaño fijo, que conserva la traza de los N últimos paquetes recibidos, yendo N típicamente de 32 a 256.

[0005] En estas soluciones, la estación receptora salvaguarda el valor del mayor de los identificadores de paquetes recibidos, llamado T, y acepta un nuevo paquete recibido si:

- el identificador es superior a T, o
- el identificador está comprendido en el intervalo [T-N+1;T] si el paquete no ha sido ya recibido.

[0006] El receptor rechaza los paquetes en los que:

- el identificador es inferior o igual a T-N+1, o
- el identificador está comprendido en el intervalo [T-N+1;T] si el paquete ha sido ya recibido.

[0007] Una solución contra la repetición se define en el marco de IPSec (RFC 4301). Más precisamente, los dos protocolos que siguen tratan este tema:

- el protocolo n 51, AH, definido por la RFC 4302, y
- el protocolo n 50, ESP, definido por la RFC 4303.

[0008] En una de las soluciones ofrecidas, la tabla anti repetición almacena los identificadores de los paquetes recibidos o de los paquetes no recibidos, pudiendo los identificadores sucesivos almacenarse en forma de intervalos, para minimizar el tamaño de la subtabla.

[0009] Otras soluciones buscan limitar el impacto de la recepción de un identificador superior a T+N, pues esta provoca la pérdida de una parte de la tabla anti repetición almacenada. Esta situación se presenta por ejemplo cuando varios paquetes se envían sobre una ruta, después de que una ruta más corta está disponible, acarreando la recepción de paquetes emitidos más tardíamente antes de la de paquetes emitidos anteriormente.

[0010] Así, en una de las soluciones ofrecidas, se consideran dos tablas anti repetición, una tabla de cabeza y una tabla de cola. Estas tablas se espacian por un intervalo que almacena los identificadores no recibidos. Si la estación de recepción recibe un paquete que tiene un identificador comprendido en este intervalo, es porque ese paquete no ha sido recibido y es transmitido hacia el destinatario del paquete. La tabla de cola es desplazada de manera que el valor del identificador recibido corresponde al límite alto de la tabla de cola.

[0011] Si el receptor recibe un paquete con un identificador superior a T pero inferior a T+N, la tabla de cabeza es desplazada de manera que el valor recibido corresponde al límite alto de la tabla de cabeza. Se desplaza

eventualmente la tabla de cola de forma que el espacio de memoria entre las dos tablas sea representativo únicamente de los identificadores no recibidos.

[0012] Si el receptor recibe un paquete con un identificador superior a T+N, la tabla de cola pasa por encima de la tabla de cabeza y se convierte en la nueva tabla de cabeza. El identificador recibido corresponde entonces al límite alto de la nueva tabla de cabeza.

[0013] Finalmente, con el mismo objetivo, en una de las soluciones ofrecidas, cuando el receptor recibe un paquete con un identificador superior a T+N, la estación receptora estima el número de paquetes válidos potencialmente perdidos si la tabla se desplaza. Si este número es superior a un cierto umbral, el paquete recibido se rechaza.

[0014] Las soluciones ofrecidas en la técnica anterior solo funcionan bien en la hipótesis de una perturbación muy limitada del ordenamiento de los paquetes de datos a través de la red de transporte.

[0015] Teniendo en cuenta las propiedades de un DTN en términos de caudal de los enlaces de redes, típicamente de 100 kbites/s a varios Mbites/s, y de la capacidad de almacenamiento de los relés de la red, típicamente de un minuto a varias horas de tráfico de red, las soluciones existentes ponen en marcha tablas anti repetición propias para almacenar un número muy elevado de identificadores de paquetes, por ejemplo del orden de un millón. Esto hace problemáticas a la vez la manipulación y el almacenamiento de la tabla. De ello se sigue:

- una latencia introducida por el mecanismo de protección contra la repetición susceptible de afectar de manera significativa al rendimiento del equipo de seguridad,
- un riesgo de falsa detección de la repetición de un paquete, y
- un riesgo de no detección de la repetición de un paquete.

[0016] El documento US 2011/153862 describe un procedimiento anti repetición que pretende mejorar los procedimientos en banda de tiempo finita.

[0017] El documento US 2009/158417 describe igualmente un procedimiento anti repetición que comprende la consulta de una base de datos.

[0018] Un objetivo de la invención es por tanto proveer un procedimiento de detección de una repetición que resuelve o minimiza los problemas citados.

[0019] A tal efecto, la invención tiene como objeto un procedimiento conforme a la reivindicación 1.

[0020] Según unos modos particulares de realización, el procedimiento comprende una o varias de las características que corresponden a las reivindicaciones 2 a 11, tomadas aisladamente o según todas las combinaciones técnicamente posibles.

[0021] La invención se refiere igualmente a un programa de ordenador según la reivindicación 12.

[0022] La invención se refiere finalmente a una estación receptora adaptada para poner en marcha las etapas de un procedimiento tal como se describe más arriba.

[0023] La invención se comprenderá mejor con la lectura de la descripción que aparece a continuación, dada únicamente a título de ejemplo y realizada en referencia a los dibujos anexos en los que:

- la figura 1 es una vista esquemática de una instalación que pone en marcha un procedimiento según la invención.
- la figura 2 es una vista esquemática de un módulo de la estación emisora representada en la figura 1,
- la figura 3 es una vista esquemática que representa una base de datos de la estación receptora representada en la figura 1,
- la figura 4 es una vista esquemática que representa un algoritmo de las etapas del procedimiento según la invención puestas en marcha por la estación receptora representada en la figura 1.

[0024] En referencia a la figura 1, se describe una instalación 1 según la invención que pone en marcha un procedimiento según la invención que se describirá después.

[0025] La instalación 1 comprende una estación emisora E adaptada para emitir un mensaje M vía red 3, y una estación receptora R adaptada para recibir el mensaje M que ha transitado por la red 3 en forma de paquete.

[0026] Según variantes no representadas de la instalación 1, la instalación comprende una o varias estaciones emisoras diferentes y análogas a la estación emisora E, y/o una o varias estaciones receptoras diferentes y análogas a la estación receptora R.

[0027] La red 3 es por ejemplo una red DTN que pone en marcha un protocolo IP. Como variante, la red 3 pone en marcha otros protocolos de comunicación, por ejemplo, protocolos de comunicación de nivel 2 OSI, como Ethernet, o de niveles superiores.

[0028] La estación emisora E es por ejemplo un cifrador de red (un dispositivo que permite cifrar y descifrar un paquete), un puesto de radio táctico protegido, o un terminal móvil protegido.

[0029] Según una variante, la estación emisora E es igualmente receptora, es decir que posee todas las características estructurales y funcionales de la estación receptora R.

[0030] La invención se refiere igualmente a un programa de ordenador, para instalar en una estación receptora, constando dicho programa de instrucciones para poner en marcha un procedimiento tal como está definido más arriba cuando las instrucciones se ejecutan mediante la estación receptora.

[0031] La invención se refiere finalmente a una estación receptora adaptada para poner en marcha las etapas de un procedimiento tal como se describe más arriba.

[0032] La invención se comprenderá mejor con la lectura de la descripción que aparece a continuación, dada únicamente a título de ejemplo y realizada en referencia a los dibujos anexos en los que:

- la figura 1 es una vista esquemática de una instalación que pone en marcha un procedimiento según la invención.
- la figura 2 es una vista esquemática de un módulo de la estación emisora representada en la figura 1,
- la figura 3 es una vista esquemática que representa una base de datos de la estación receptora representada en la figura 1,
- la figura 4 es una vista esquemática que representa un algoritmo de las etapas del procedimiento según la invención puestas en marcha por la estación receptora representada en la figura 1.

[0033] En referencia a la figura 1, se describe una instalación 1 según la invención que pone en marcha un procedimiento según la invención que se describirá después.

[0034] La instalación 1 comprende una estación emisora E adaptada para emitir un mensaje M vía red 3, y una estación receptora R adaptada para recibir el mensaje M que ha transitado por la red 3 en forma de paquete.

[0035] Según variantes no representadas de la instalación 1, la instalación comprende una o varias estaciones emisoras diferentes y análogas a la estación emisora E, y/o una o varias estaciones receptoras diferentes y análogas a la estación receptora R.

[0036] La red 3 es por ejemplo una red DTN que pone en marcha un protocolo IP. Como variante, la red 3 pone en marcha otros protocolos de comunicación, por ejemplo, protocolos de comunicación de nivel 2 OSI, como Ethernet, o de niveles superiores.

[0037] La estación emisora E es por ejemplo un cifrador de red (un dispositivo que permite cifrar y descifrar un paquete), un puesto de radio táctico protegido, o un terminal móvil protegido.

[0038] Según una variante, la estación emisora E es igualmente receptora, es decir que posee todas las características estructurales y funcionales de la estación receptora R.

[0039] La estación emisora E comprende un módulo 5 de generación de números de secuencia representado en la figura 2.

[0040] La estación receptora R es por ejemplo un cifrador de red, un puesto de radio táctico protegido, o un terminal móvil protegido.

[0041] Igualmente, según una variante, la estación receptora R es igualmente emisora, es decir que posee todas las características estructurales y funcionales de la estación emisora E.

[0042] La estación receptora R comprende una base de datos 7 anti repetición dedicada a la protección contra la repetición del tráfico de datos emitidos por la estación emisora E, y representada en la figura 3.

[0043] Según un modo particular de realización, la estación receptora R tiene acceso por cualquier medio conocido por el experto en la materia a la base de datos 7, que está de preferencia incluida físicamente en la estación receptora. La estación receptora R alberga ventajosamente un programa de pilotaje adaptado para la puesta en marcha mediante la estación receptora R de un algoritmo 9 representado en la figura 4.

[0044] El funcionamiento de la instalación 1 se va a describir a continuación.

[0045] Como es visible en la figura 1, la estación emisora E encapsula el mensaje M en un paquete 11.

[0046] Los paquetes 11 se envían sucesivamente a la red 3 en varios periodos de tiempo consecutivos, ventajosamente con la misma duración. Por ejemplo, los periodos de tiempo duran 10 minutos.

[0047] Durante cada periodo de tiempo, N paquetes 11 se envían por ejemplo a la red 3, siendo N un número entero natural, de preferencia una potencia de 2.

[0048] Cada paquete 11 comprende ventajosamente un campo 15 que contiene un índice SPI (en inglés: *Security Parameter Index).* El índice SPI identifica de manera única, un contexto criptográfico utilizado por la estación emisora E para realizar la protección en confidencialidad y/o en integridad de los campos 17 SN y 21 que contienen el mensaje. El contexto criptográfico al que reenvía el índice SPI comprende por ejemplo una clave secreta K compartida antes entre la estación emisora E y la estación receptora R.

[0049] Cada paquete 11 comprende igualmente un campo 17 que contiene un identificador SN (en inglés: *Sequence Number).* El identificador SN protege el paquete 11 contra la repetición. El procedimiento garantiza la unicidad del valor del identificador SN para cada paquete 11.

[0050] Cada paquete 11 comprende opcionalmente un campo 19 que contiene un vector de inicialización SV.

[0051] Cada paquete 11 comprende también un campo 21 que contiene el mensaje M. El campo 21 que contiene el mensaje puede protegerse en confidencialidad. El cifrado del campo 21 que contiene el mensaje explota el valor del campo SV 19 y una clave secreta K compartida, identificada por el índice SPI.

[0052] Cada paquete 11 comprende finalmente un campo 23 que contiene un motivo de integridad ICV (en inglés: *Integrity Check Value).* El campo ICV 23 protege en su integridad el campo SN 17 y el campo 21 que contiene el mensaje. El cálculo del campo ICV 23 explota el valor del campo SV 19 y una clave secreta K compartida, identificada por el índice SPI.

[0053] Los campos 15, 17, 19 y 23 son ventajosamente de tamaño fijo, es decir el mismo tamaño para todos los paquetes.

[0054] El campo 15 se extiende por ejemplo sobre 32 bites.

[0055] El campo 17 se extiende por ejemplo sobre 32 bites.

[0056] El campo 19 se extiende por ejemplo sobre 128 bites.

[0057] El campo 21 es de tamaño variable.

[0058] El campo 23 se extiende por ejemplo sobre 32, 64, 80 o 128 bites.

[0059] El campo SV es opcional. La unicidad del identificador SN al estar garantizada por el procedimiento, según una variante, se utiliza el identificador SN como vector de inicialización.

[0060] El vector de inicialización SV es único para una clave K dada. Un generador de números aleatorios de buena calidad se utiliza por ejemplo para generar el valor del vector de inicialización SV y garantizar su unicidad.

[0061] La unicidad del identificador SN al estar garantizada por el procedimiento, según una variante, se utiliza el identificador SN como vector de inicialización.

[0062] El identificador SN comprende un indicador temporal T representativo del periodo de tiempo durante el que el paquete 11 se ha emitido, y un indicador de conteo C representativo de un orden de emisión del paquete dentro del periodo de tiempo durante el cual el paquete se ha emitido.

[0063] El valor del identificador SN se obtiene con ayuda del módulo 5 de generación de números de secuencia (figura 2) cuyo principio de funcionamiento se describe más adelante.

[0064] El campo 17 que contiene el identificador SN se rellena mediante el módulo 5 que genera:

- un identificador fuente que ocupa por ejemplo una parte alta 25 del campo 17,
- un identificador temporal T que ocupa por ejemplo una parte intermedia 27 del campo 17, y
- el indicador de conteo C que ocupa por ejemplo una parte baja 29 del campo 17.

[0065] La parte alta 25, la parte intermedia 27 y la parte baja 29 son ventajosamente de tamaño fijo.

[0066] Ventajosamente, el identificador fuente identifica de manera única la estación emisora E entre otras estaciones emisoras (no representadas).

[0067] El identificador temporal T es representativo del periodo temporal durante el que se emite el paquete 11. No es necesario transmitir una referencia horaria completa de la estación emisora E. Bastan algunos bites para la estación receptora R, si es necesario, para deducir la referencia horaria completa de la estación emisora E. Todos los paquetes 11 emitidos en el mismo periodo de tiempo tomado entre los periodos de tiempo consecutivos mencionados más arriba tienen el mismo indicador temporal T. Es en eso en lo que es representativo del periodo temporal el indicador temporal T.

[0068] Más generalmente, en la presente solicitud, se entiende que un parámetro es representativo de una noción si existe una tabla de correspondencia entre este parámetro y esta noción.

[0069] El contador que abastece al indicador de conteo C se inicializa por ejemplo en el momento del cambio de la clave secreta K y en cada cambio del indicador temporal T. El contador que abastece al indicador de conteo C se incrementa después de cada emisión de un paquete 11.

[0070] La base de datos 7 se configura para memorizar los identificadores SN que han sido ya recibidos. Como se verá después, la memorización de los identificadores SN ya recibidos es, o bien explícita, o implícita.

[0071] Por «explícita» se entiende que la información según la que el identificador SN se ha recibido se almacena en la base de datos 7, por ejemplo gracias a un bite por identificador recibido.

[0072] Por «implícita» se entiende que la información según la que el identificador SN se ha recibido se deduce de informaciones almacenadas en la base de datos 7. Esta información se obtiene al final de una o varias pruebas lógicas que tratan sobre los campos de la base de datos 7. Por ejemplo, la memorización implícita se realiza memorizando las franjas de identificadores que ya se han recibido. La memorización implícita se realiza por ejemplo a partir de los indicadores Tmax y Cmax y de la ausencia de una tabla SF o de una subtabla SF en la base de datos 7.

[0073] La base de datos 7 comprende un campo 31 que contiene un indicador temporal máximo Tmax, y una o varias tablas SF anti repetición.

[0074] El indicador temporal máximo Tmax es representativo del máximo de los indicadores temporales T de los paquetes 11 ya recibidos.

[0075] Cada tabla SF se adapta para la memorización de los identificadores SN de los paquetes 11 emitidos durante uno de los periodos de tiempo. Cada tabla SF se dedica respectivamente a uno de los periodos de tiempo durante los que los paquetes 11 se envían mediante la estación emisora E.

[0076] Cada tabla SF comprende un campo 33 que contiene el indicador temporal T al que se dedica, y una o varias subtablas F adaptadas a la memorización de los indicadores de conteo C.

[0077] Cada tabla SF comprende también un campo 35 que contiene un indicador de conteo máximo Cmax.

[0078] En la base de datos 7, las tablas SF están separadas de dos en dos. No existen dos tablas SF distintas que tengan el mismo indicador temporal T en el campo 33. Así, una tabla SF se identifica de manera única en la base de datos 7 por su campo 33.

[0079] El indicador de conteo máximo Cmax de las tablas SF es representativo de la subtabla F que existe, o ha existido, en la que se memoriza, o se ha memorizado, el indicador de conteo C más elevado ya recibido para un paquete 11 emitido durante el periodo de tiempo del que es representativo el indicador temporal T de la tabla SF.

[0080] Cada subtabla F comprende un campo 37 que contiene un identificador de la subtabla, y un campo 39 adaptado para memorizar los indicadores de conteo C de los identificadores SN ya recibidos. Cada subtabla F se dedica respectivamente a un intervalo (i. E. una franja) de indicadores de conteo C. El intervalo es ventajosamente de longitud fija. Por ejemplo, una subtabla F almacena 64 valores consecutivos de indicadores de conteo C.

[0081] En cada tabla SF, las subtablas F están separadas de dos en dos. No existen dos subtablas F que tengan el mismo identificador en sus campos 37 respectivos. Así, cada subtabla F de una tabla SF se identifica de manera única en la tabla SF por su campo 37.

[0082] El indicador de conteo máximo Cmax contenido en el campo 35 de cada tabla SF es por ejemplo igual al valor máximo contenido en los campos 37 de las subtablas F que la tabla SF contiene o ha contenido.

[0083] El campo 39 está ventajosamente adaptado para contener indicadores de conteo C que pertenecen a un intervalo correspondiente a N paquetes emitidos sucesivamente en el mismo periodo de tiempo. Por ejemplo, se trata de un campo de N bites, con N ventajosamente igual a 64 o 4096.

[0084] Por ejemplo, un bit a 0 en el campo 39 significa que el indicador de conteo C cuyo valor corresponde al emplazamiento de este bite no se ha recibido. Inversamente, un bit a 1 en el campo 39 significa que el indicador de conteo C cuyo valor corresponde al emplazamiento de este bite se ha recibido.

[0085] En una subtabla F, el primer bite del campo 39 corresponde a un indicador de conteo C de valor igual al valor del campo 37.

[0086] Todos los campos de la base de datos 7 tienen ventajosamente un tamaño fijo, incluyendo los de las tablas SF y de las subtablas F.

[0087] El funcionamiento de la instalación 1, es decir un procedimiento según la invención, se va a describir a continuación.

[0088] La estación emisora E (figura 1) crea y después envía los paquetes 11 a la red 3. Los paquetes 11 se identifican de manera única mediante el identificador SN representativo de un orden de emisión. Pero, por el funcionamiento interno de la red 3, los paquetes 11 llegan a la estación receptora R en un orden diferente del orden de emisión. Además, existe el riesgo de que uno o varios paquetes 11 sean interceptados y repetidos por un atacante que disponga de un acceso físico a la red 3.

[0089] La estación receptora R pone en marcha el algoritmo 9 esquematizado en la figura 4.

[0090] El algoritmo 9 comprende primero una etapa 100 de recepción de un paquete 11.

[0091] En una etapa 102, la estación receptora R lee el paquete 11 recibido. La estación receptora R obtiene el índice SPI contenido en el campo 15 (figura 1).

[0092] La estación receptora R realiza después una prueba 104 de reconocimiento del índice SPI y de búsqueda de la clave secreta K.

[0093] Si el índice SPI no se reconoce y no se encuentra ninguna clave secreta K, la estación receptora R pasa a una etapa 106 que comprende la generación de una alarma para significar que el contexto criptográfico se desconoce. Además, la estación receptora R bloquea el paquete 11 y el mensaje M que contiene.

[0094] Si el índice SPI se reconoce y se encuentra una clave secreta K correspondiente, la estación receptora R pasa a una etapa 108 que comprende ventajosamente un desciframiento y la verificación de integridad del paquete 11.

[0095] Para la verificación de integridad, la estación receptora R calcula un motivo de integridad a partir de los campos del paquete protegido en integridad por la estación emisora, de la clave secreta K y del vector de inicialización SV contenido en el campo 19 del paquete. Si el motivo de integridad calculado no es igual al motivo de integridad ICV contenido en el campo 23 del paquete 11, entonces la estación receptora R pasa a una etapa 112 de generación de una alarma para significar que el paquete 11 se altera y bloquea el paquete y el mensaje M que contiene.

[0096] Si el motivo de integridad calculado es igual motivo de integridad ICV, la estación receptora R realiza una etapa 114 de verificación del identificador SN recibido.

[0097] Si el resultado de la etapa 114 es que el identificador SN recibido se considera como repetido, entonces la estación receptora R pasa a una etapa 118 de generación de una alarma para significar que el paquete 11 se ha repetido y bloquea el mensaje M.

[0098] Si el resultado de la etapa 114 es que el identificador SN recibido se considera como no repetido, entonces la estación receptora R pasa a una etapa 120 de extracción del mensaje M del paquete 11, y de transmisión del paquete.

[0099] La etapa de verificación 114 consta de una subetapa (no representada) de consulta de la base de datos 7 de identificadores ya recibidos para determinar si el identificador (SN) recibido ha sido ya recibido, y de una subetapa (no representada) de actualización de la base de datos 7.

[0100] Opcionalmente, si el indicador temporal T del identificador SN recibido indica que el paquete 11 se ha emitido desde una duración superior a un umbral, entonces el paquete 11 se rechaza sin consulta de la base de datos 7. El umbral se define en función de la duración de vida de los mensajes M. Por ejemplo, el umbral vale dos horas.

[0101] En la subetapa de consulta, el paquete 11 se considera como ya recibido si el indicador temporal T del identificador SN recibido es inferior o igual al indicador temporal máximo Tmax y si no existe en la base de datos 7 una tabla SF específica del periodo temporal del que el indicador temporal es representativo. En este caso, el identificador SN recibido está implícitamente contenido en la base de datos 7. A pesar de la ausencia de una tabla SF susceptible de contener explícitamente el identificador SN recibido, se considera que el identificador SN recibido ha sido ya recibido. La razón de tal ausencia se dará más adelante.

[0102] Se considera igualmente que el paquete 11 ha sido ya recibido si:

- el indicador temporal T del identificador SN recibido es inferior o igual al indicador temporal máximo Tmax,
- existe en la base de datos 7 una tabla SF específica del periodo temporal del que el indicador temporal T es representativo, y
- existe en dicha tabla SF una subtabla F que ha memorizado ya el indicador de conteo C.

[0103] En este caso, el identificador SN recibido está explícitamente contenido en la base de datos 7.

[0104] Se considera igualmente que el paquete 11 ha sido ya recibido si:

- existe en la base de datos 7 una tabla SF específica del periodo temporal del que el indicador temporal T es representativo,
- no existe en dicha tabla SF una subtabla F que contenga el indicador de conteo C, y
- el indicador de conteo C se sitúa en un intervalo (de longitud igual a 64 por ejemplo) cuyo límite inferior es inferior o igual al indicador de conteo máximo Cmax de dicha tabla SF.

[0105] Se trata de un segundo caso de memorización implícita del identificador SN en la base de datos 7. La memorización es implícita porque, a pesar de la ausencia de una tabla SF susceptible de contener el indicador de conteo C recibido, se considera sin embargo que el identificador SN recibido ha sido ya recibido.

[0106] En todos los demás casos, el identificador SN recibido se considera como no recibido ya, es decir como no repetido.

[0107] La subetapa de actualización de la base de datos 7 depende del resultado de la subetapa de consulta.

[0108] Si el identificador SN recibido se considera como ya recibido, no hay ninguna actualización particular de la base de datos 7.

[0109] Si el identificador SN recibido se considera como recibido por primera vez, entonces se memoriza en la base de datos 7 de la siguiente manera.

[0110] Si no existe tabla SF susceptible de memorizar el identificador SN recibido, se crea una nueva tabla SF susceptible de memorizar el identificador SN recibido en la base de datos. Por otra parte, el indicador temporal máximo Tmax es actualizado para tomar el valor del indicador temporal T. Llegado el caso, se crean nuevas tablas SF en la base de datos 7 para cubrir los periodos de tiempo situados entre el periodo de tiempo correspondiente al antiguo valor del indicador temporal máximo Tmax (antes de su actualización) y el periodo de tiempo correspondiente al nuevo valor del indicador temporal máximo Tmax (después de su actualización).

[0111] El indicador de conteo C del identificador SN recibido se memoriza e la subtabla F dedicada a la franja de valores en la que se encuentra el indicador de conteo C. Si no existe subtabla F susceptible de memorizar el indicador de conteo C, se crea en la base de datos 7 una nueva subtabla F susceptible de memorizar el indicador de conteo C. Si el indicador de conteo C es superior al indicador de conteo máximo Cmax, entonces el indicador de conteo máximo Cmax es aumentado para tomar el valor del campo 37 de la subtabla creada para almacenar el indicador de conteo C.

[0112] Llegado el caso, se crean nuevas subtablas SF en la base de datos 7 para cubrir las franjas de indicadores de conteo C situadas entre la franja correspondiente al antiguo valor del indicador de conteo máximo Cmax (antes de su actualización) y la franja correspondiente al nuevo valor del indicador de conteo máximo Cmax (tras su actualización). La estación receptora R realiza además una etapa de gestión (no representada) de la base de datos que comprende un borrado condicional de cualquiera de las subtablas F si la subtabla F está llena.

[0113] Por «lleno» se entiende que todos los paquetes que son emitidos por una parte durante el periodo temporal de la tabla SF que contiene dicha subtabla F y que tienen por otra parte un indicador de conteo C comprendido

en la franja sucesiva de dicha subtabla F, han sido recibidos. Por ejemplo, todos los bites del campo 39 de la subtabla F llena valen «1».

[0114] Ventajosamente, la etapa de gestión comprende también un borrado condicional de cualquiera de las tablas SF si todos los paquetes emitidos durante el periodo temporal de dicha tabla han sido recibidos.

[0115] Ventajosamente, la etapa de gestión comprende también un borrado condicional de cualquiera de las tablas SF si el indicador temporal T (campo 33) de la tabla SF indica que la tabla SF es demasiado antigua, i. e. que una duración superior a un cierto umbral ha transcurrido desde el periodo de tiempo del que es representativo el indicador temporal T de la tabla SF.

[0116] Opcionalmente, con el fin de liberar espacio de memoria, cuando el espacio de memoria permitido para el almacenamiento de la base de datos 7 está saturado:

- si la base de datos 7 comprende varias tablas SF, entonces la tabla SF más antigua (con el valor más débil del indicador temporal T) se suprime de la base de datos 7.
- si no, la subtabla F más antigua (con el identificador menos elevado en el campo 37) se suprime.

[0117] Finalmente, para reducir al mínimo el espacio de memoria ocupada por la base de datos 7, ésta se comprime.

[0118] El contenido de la base de datos 7, sobre todo el indicador de recepción del campo 39 de las subtablas F, se caracteriza por una mayoría de bites a 1 (paquetes recibidos) y un reparto aleatorio de bites a 0 (paquetes no recibidos o perdidos), que corresponden a la tasa de pérdida de paquetes por la red 3, que es por ejemplo de alrededor de un 20 % de los paquetes emitidos.

[0119] Opcionalmente, se pone en marcha un algoritmo de compresión sin pérdida de datos, por ejemplo una codificación de Huffman. El algoritmo preserva la estructura de datos de la base de datos 7. Solo se comprime el contenido de las tablas SF. Para cada tabla SF, todas las tablas F se concatenan y comprimen en un solo bloque de datos.

[0120] Esto permite un acceso directo a cada tabla SF a partir de la base de datos 7 en su forma comprimida.

[0121] Un programa de instrucciones de software se almacena ventajosamente en la estación receptora R. Cuando la estación receptora R ejecuta el programa, pone en marcha las etapas 100 a 120 descritas más arriba, así como la etapa de gestión de la base de datos.

[0122] El programa se ejecuta por ejemplo dentro de una arquitectura de microprocesador de la estación de recepción R que comprende:

- uno o varios núcleos microprocesadores, por ejemplo CPU ARM CORTEX A15,
- una memoria volátil, por ejemplo, DDR SDRAM,
- una memoria no volátil de fuerte capacidad, por ejemplo una memoria Flash,
- una memoria volátil salvaguardada, por ejemplo, NVRAM, y
- uno o varios puertos de entrada/salida, que permiten la recepción y la emisión de paquetes de datos protegidos contra la repetición.

[0123] La base de datos 7 se archiva ventajosa y completamente en su forma comprimida en la memoria Flash. El uso de un sistema de explotación que incluye un sistema de ficheros facilita y optimiza la explotación de la memoria Flash.

[0124] Los elementos de la base de datos 7 modificados, y aún no archivados y comprimidos en memoria Flash, se salvaguardan ventajosamente en la memoria NVRAM, que es no volátil.

[0125] El estado corriente de la base de datos 7 se obtiene entonces mediante una combinación del contenido de las memorias Flash (archivo completo comprimido) y NVRAM (elementos modificados con respecto al contenido del archivo comprimido).

[0126] En caso de corte brutal de la alimentación eléctrica en todo o parte de la estación receptora R, se preserva el estado de la base de datos 7. En la siguiente puesta en marcha, un procedimiento simple de reconstrucción del estado de la base de datos que combina la información archivada en memoria Flash y salvaguardada en memoria NVRAM, permite una vuelta rápida de la estación receptora R al estado operativo.

[0127] Cuando la memoria NVRAM está llena, o de manera periódica, por ejemplo cada dos minutos, la base de datos 7 archivada y comprimida en memoria Flash se actualiza y la NVRAM se vacía.

[0128] Esto prolonga la duración de la vida de la memoria Flash no volátil mediante una reducción del número de ciclos de escritura, y optimiza el uso de la débil capacidad de la memoria NVRAM.

[0129] Gracias a las características descritas más arriba, el tamaño de la base de datos 7 se reduce. Esto reduce la latencia introducida por el mecanismo de protección contra la repetición, el riesgo de falsa detección de la repetición de un paquete, y el riesgo de no detección de la repetición de un paquete.

[0130] La solución ofrecida no degrada por otro lado el rendimiento de la red 3.

[0131] El procedimiento según la invención se adapta para combinarse eficazmente con una protección de tipo IPSEC AH y ESP, gracias a la mutualización de los mecanismos de encapsulado protocolarios y criptográficos.

[0132] El procedimiento es compatible con diferentes modos de difusión: punto a punto, y punto a multipunto.

[0133] El procedimiento es aplicable a otros protocolos de comunicación aparte de IP, por ejemplo, a los protocolos de comunicación de nivel 2 OSI, como Ethernet, o de niveles superiores.

[0134] El procedimiento según la invención permite manipular las subtablas F de anti repetición de pequeño tamaño, típicamente de 64 bites, conservando la traza de numerosos paquetes recibidos. Este tamaño es compatible con las arquitecturas de microprocesador del momento, y optimiza los accesos a las subtablas F y su manipulación. El procedimiento permite igualmente manipular subtablas de anti repetición de mayor tamaño, típicamente de 4096 bites, para sacar partido de los mecanismos de caché de las arquitecturas de procesador modernas y del tamaño importante de los bloques de memorias de tipo Flash NOR/NAND.

[0135] La implementación material del procedimiento se adapta a las prestaciones de las tecnologías empleadas corrientemente en un equipo de seguridad de tipo infraestructura, sobre todo en términos de capacidad de las memorias (SDRAM, SRAM salvaguardada, NVRAM y Flash) y de envejecimiento de estas memorias (Flash NOR y NAND, en particular).

REIVINDICACIONES

1. Procedimiento para detectar si un paquete (11) de una pluralidad de paquetes emitidos por al menos una estación emisora (E) a través de una red (3) ha sido repetido, comprendiendo cada paquete (11) un mensaje (M) y un identificador (SN) del paquete (11), siendo la pluralidad de paquetes emitidos sucesivamente en varios periodos de tiempo consecutivos, comprendiendo el procedimiento las etapas siguientes:

- recepción (100) por al menos una estación receptora (R) del paquete (11) y lectura del identificador (SN) del paquete (11) recibido para obtener un identificador (SN) recibido,
- consulta (114) mediante la estación receptora (R) de una base de datos (7) de identificadores que han sido ya recibidos para determinar si el identificador (SN) recibido ha sido ya recibido, y
- si el identificador (SN) recibido no ha sido ya recibido, actualización de la base de datos (7) que comprende una memorización del identificador (SN) recibido,

caracterizado porque:

- el identificador (SN) comprende un indicador de pertenencia a los grupos de paquetes,
- la base de datos (7) comprende una o varias subtablas (F) adaptadas a la memorización de los identificadores (SN) de los paquetes ya recibidos, dedicándose cada subtabla (F) a uno de los grupos, y
- el procedimiento comprende además una etapa de gestión de la base de datos (7) que comprende un borrado condicional de cualquiera de las subtablas (F) si todos los paquetes del grupo al que dicha subtabla (F) se dedica son recibidos.

2. Procedimiento según la reivindicación 1, **caracterizado porque**:

- el indicador de pertenencia comprende un indicador de conteo (C) representativo de un orden de emisión de dicho paquete (11),
- la o las subtablas (F) se adaptan a la memorización de los indicadores de conteo (C) que pertenecen respectivamente a un intervalo o a intervalos sucesivos de indicadores de conteo, dedicándose cada subtabla (F) respectivamente a una de dichas franjas sucesivas, y
- la etapa de gestión de la base de datos (7) comprende un borrado condicional de cualquiera de las subtablas (F) si la subtabla (F) está llena.

3. Procedimiento según la reivindicación 2, **caracterizado porque:**

- el indicador de pertenencia comprende además un indicador temporal (T) representativo del periodo de tiempo durante el cual el paquete (11) se ha emitido, siendo el indicador de conteo (C) representativo de un orden de emisión de dicho paquete (11) dentro del periodo de tiempo durante el cual el paquete (11) se ha emitido.
- la base de datos (7) comprende una o varias tablas (SF), adaptándose cada tabla (SF) respectivamente para la memorización de los identificadores (SN) de los paquetes emitidos durante uno de los periodos de tiempo, dedicándose cada tabla (SF) respectivamente a uno de los periodos de tiempo, y
- cada tabla (SF) comprende una o varias de las subtablas (F).

4. Procedimiento según la reivindicación 3, **caracterizado porque** la etapa de gestión de la base de datos (7) comprende un borrado condicional de cualquiera de las tablas (SF) si todos los paquetes emitidos durante el periodo temporal de dicha tabla (SF) se han recibido.

5. Procedimiento según la reivindicación 3 o 4, **caracterizado porque** la etapa de gestión de la base de datos (7) comprende un borrado condicional de cualquiera de las tablas (SF) si el tiempo transcurrido entre el periodo de tiempo específico en dicha tabla (SF) y un indicador de tiempo corriente es superior a un valor dado.

6. Procedimiento según cualquiera de las reivindicaciones 3 a 5, **caracterizado porque** la base de datos (7) comprende un indicador temporal máximo (Tmax) representativo del máximo de los indicadores temporales de los paquetes ya recibidos, y cada tabla (SF) comprende un indicador de conteo máximo (Cmax) representativo del intervalo de indicadores de conteo (C) más elevado de todos los identificadores (SN) ya memorizados en dicha tabla (SF), y **porque**, en la etapa de consulta, el paquete (11) se considera como ya recibido si el indicador temporal (T) es inferior o igual al indicador temporal máximo (Tmax) y si:

- no existe en la base de datos (7) una tabla (SF) específica del periodo temporal del que el indicador temporal (T) es representativo, o
- existe en la base de datos (7) una tabla (SF) específica del periodo temporal del que el indicador temporal (T) es representativo, y existe en dicha tabla (SF) una subtabla (F) que ha memorizado ya el indicador de conteo (C), o
- existe en la base de datos (7) una tabla (SF) específica del periodo temporal del que el indicador temporal (T) es representativo, y no existe en dicha tabla (SF) una subtabla (F) que contenga el indicador de conteo (C), y el indicador de conteo (C) es inferior o igual al indicador de conteo máximo (Cmax) de dicha tabla (SF).

7. Procedimiento según cualquiera de las reivindicaciones 3 a 6, **caracterizado porque** comprende además una etapa (108) de verificación de la integridad de al menos el identificador (SN) recibido, y de generación (112) de una alarma si el identificador (SN) recibido no está íntegro.

8. Procedimiento según la reivindicación 7, **caracterizado porque** cada paquete (11) comprende un parámetro de seguridad (SPI) representativo de una clave secreta (K) compartida entre el emisor (E) y la estación receptora (R), utilizándose la clave secreta (K) en la etapa (108) de verificación de la integridad.

9. Procedimiento según cualquiera de las reivindicaciones 3 a 8, **caracterizado porque** la estación receptora (R) se adapta para recibir los paquetes procedentes de varias estaciones emisoras (E) y para consultar varias bases de datos (7) de identificadores ya recibidos, comprendiendo el identificador (SN) recibido un indicador (ID) representativo de la estación emisora (E) que ha emitido el paquete (11) recibido, siendo la base de datos (7) consultada en la etapa de consulta (114), elegida en función del indicador (ID) del identificador (SN) recibido.

10. Procedimiento según cualquiera de las reivindicaciones 3 a 9, **caracterizado porque**, en la base de datos (7), para cada tabla (SF), las subtablas (F) de la tabla (SF) están concatenadas y comprimidas en un solo bloque de datos.

11. Procedimiento según cualquiera de las reivindicaciones 3 a 10, **caracterizado porque** la estación receptora (R) pone en marcha:

- una memoria Flash en la que la base de datos (7) se archiva integralmente, de preferencia en un estado comprimido,
- una memoria viva volátil que consta de una copia al menos parcial de la base de datos (7), y
- una memoria no volátil, de preferencia una memoria NVRAM, que consta de partes de la base de datos (7) actualizadas durante la etapa de actualización y todavía no archivadas en la memoria Flash.

12. Programa de ordenador para instalar en una estación receptora (R), constando dicho programa de instrucciones para poner en marcha un procedimiento según cualquiera de las reivindicaciones 1 a 11 cuando las instrucciones se ejecutan mediante la estación receptora (R).

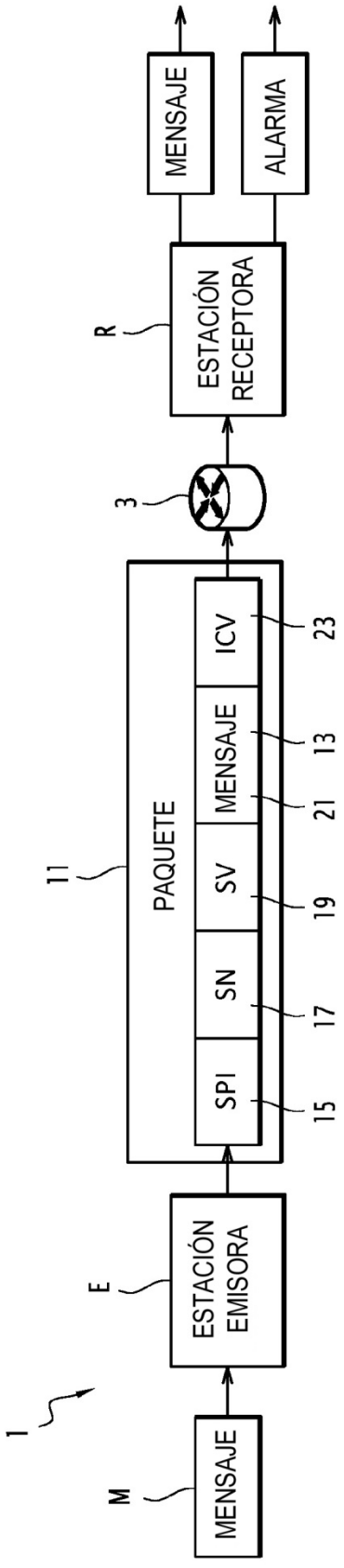
1
M
MENSAJE
E
ESTACIÓN EMISORA
11
PAQUETE
SPI
15
SN
17
SV
19
MENSAJE
21
13
ICV
23
3
R
ESTACIÓN RECEPTORA
MENSAJE
ALARMA

FIG.1

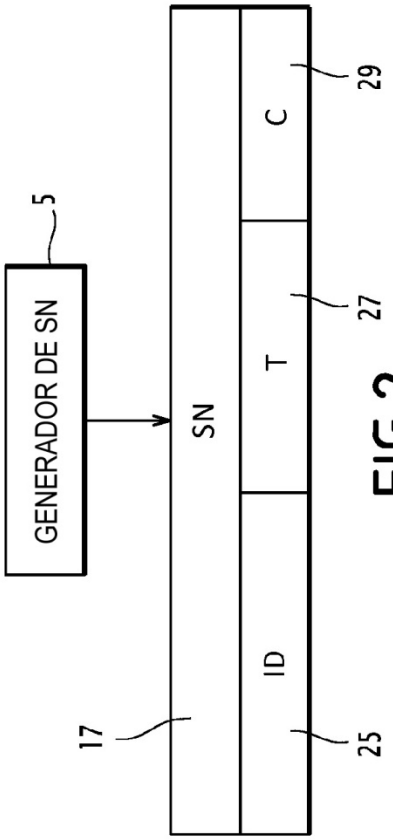
5
GENERADOR DE SN
17
SN
ID
25
T
27
C
29

FIG.2

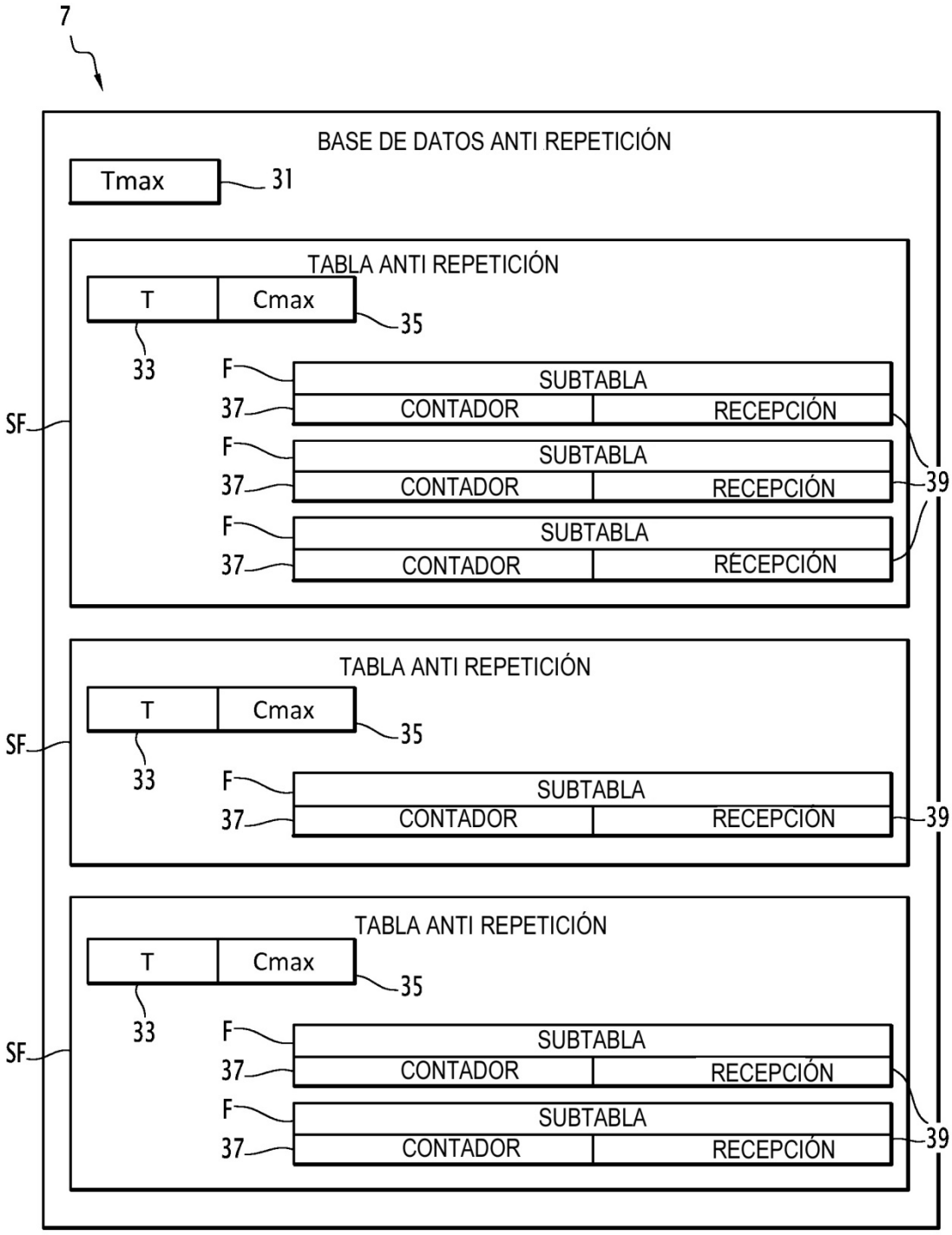
7
BASE DE DATOS ANTI REPETICIÓN
Tmax
31
TABLA ANTI REPETICIÓN
T
Cmax
35
33
F
SUBTABLA
37
CONTADOR
RECEPCIÓN
SF
39
TABLA ANTI REPETICIÓN
TABLA ANTI REPETICIÓN

FIG.3

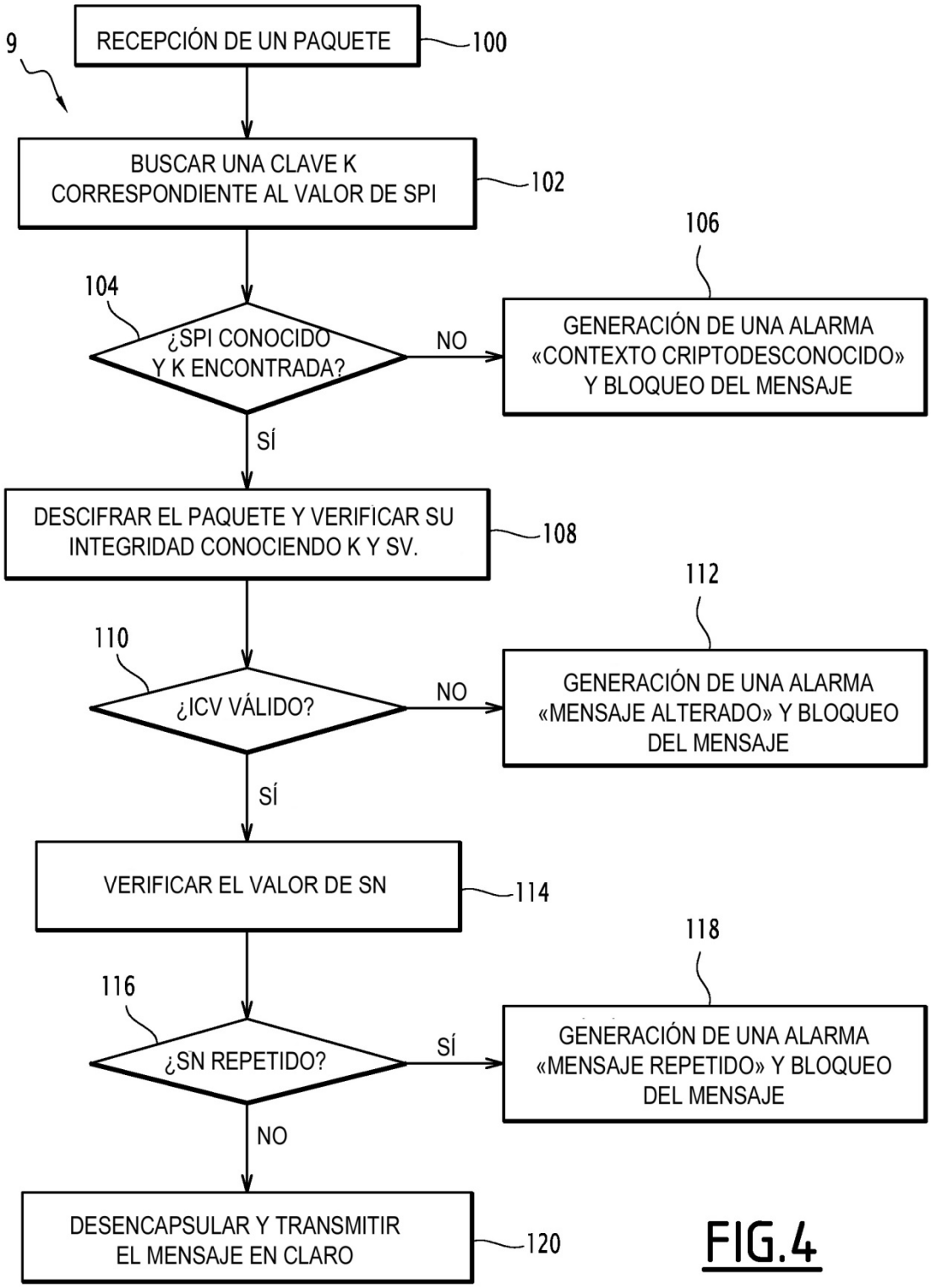
9
RECEPCIÓN DE UN PAQUETE
100
BUSCAR UNA CLAVE K CORRESPONDIENTE AL VALOR DE SPI
102
104
¿SPI CONOCIDO Y K ENCONTRADA?
NO
106
GENERACIÓN DE UNA ALARMA «CONTEXTO CRIPTODESCONOCIDO» Y BLOQUEO DEL MENSAJE
SÍ
DESCIFRAR EL PAQUETE Y VERIFICAR SU INTEGRIDAD CONOCIENDO K Y SV.
108
110
¿ICV VÁLIDO?
NO
112
GENERACIÓN DE UNA ALARMA «MENSAJE ALTERADO» Y BLOQUEO DEL MENSAJE
SÍ
VERIFICAR EL VALOR DE SN
114
116
¿SN REPETIDO?
SÍ
118
GENERACIÓN DE UNA ALARMA «MENSAJE REPETIDO» Y BLOQUEO DEL MENSAJE
NO
DESENCAPSULAR Y TRANSMITIR EL MENSAJE EN CLARO
120

FIG.4