(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 524 914**

(51) Int. CI.:

H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2004 E 04729183 (6)**

(97) Fecha y número de publicación de la concesión europea: **15.10.2014 EP 1620997**

(54) Título: **Reducción de sobrecarga y protección de direcciones en una pila de comunicación**

(30) Prioridad:

25.04.2003 EP 03101150

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.12.2014

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

KEVENAAR, THOMAS, A., M. y
KAMPERMAN, FRANCISCUS, L., A., J.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Reducción de sobrecarga y protección de direcciones en una pila de comunicación

La invención se refiere a un método de transmisión para la transmisión de datos usando un modelo de comunicación en capas, tal como se describe en la reivindicación 1.

La invención se refiere también a un método de recepción para recepción de datos usando un modelo de comunicación en capas tal como se describe en la reivindicación 5.

La invención se refiere adicionalmente a un sistema para la comunicación usando un modelo de comunicación en capas, tal como se describe en la reivindicación 9.

La invención se refiere adicionalmente a un dispositivo transmisor para la transmisión de datos usando un modelo de comunicación en capas, tal como se describe en la reivindicación 10.

La invención se refiere también a un dispositivo receptor para la recepción de datos usando un modelo de comunicación en capas, tal como se describe en la reivindicación 11.

La invención se refiere adicionalmente a una señal para el transporte de datos generada de acuerdo con un modelo de comunicación en capas, tal como se describe en la reivindicación 12.

La invención se refiere adicionalmente a un producto programa de ordenador transmisor para implementar la comunicación usando un modelo de comunicación en capas, tal como se describe en la reivindicación 13.

La invención se refiere también a un producto programa de ordenador receptor para implementar la comunicación usando un modelo de comunicación en capas, tal como se describe en la reivindicación 14.

En los protocolos de comunicación, es común usar un modelo en capas tal como el modelo de referencia OSI. Dicho modelo comprende un conjunto de capas, cada capa en un nivel de abstracción diferente. Dicho modelo puede incluir, desde la parte inferior a la superior: la capa física (PHY), la capa de control de acceso al medio (MAC), la capa de red (NWK) y la capa de aplicación (APL). En general, una trama (un fragmento de información intercambiado entre capas OSI iguales en diferentes dispositivos) consiste en una cabecera y una carga útil. Una o más tramas en el nivel n en la pila OSI se envían físicamente como carga útil de una o varias tramas en la capa inferior siguiente n-1. El nivel inferior implementa la comunicación física, por ejemplo a través de una conexión cableada o inalámbrica. En un sentido general, un único dispositivo podría tener una dirección diferente en las diferentes capas de la pila OSI. Las tramas a diferentes niveles incluyen cada una típicamente una dirección de origen, dirección de destino y a veces dirección de salto. Esto da como resultado mucha sobrecarga en la trama física, que se transmite en el nivel más bajo, debido a la múltiple inclusión de información de dirección. Esto presenta el problema de demasiada sobrecarga en aplicaciones restringidas, tal como protocolos de comunicación con una longitud de trama física limitada, o en aplicaciones de baja potencia. El documento US-A-5 627 829 (Altmaier Paulette et ál.), del 6 de mayo de 1997, describe un método de transmisión de datos usando un modelo de comunicación en capas.

Es un objetivo de la actual invención proporcionar un método de transmisión, en el que el tamaño de la trama física se reduce en tanto se mantiene sustancialmente la información contenida, y su protección criptográfica.

Este objetivo se realiza mediante un método de transmisión de acuerdo con la invención que se caracteriza porque el medio de transmisión comprende adicionalmente la etapa de eliminar al menos parcialmente la primera referencia de dirección en los datos transmitidos, y en el que se proporciona protección criptográfica para los primeros fragmentos de comunicación antes de que la primera referencia de dirección sea al menos parcialmente eliminada.

Este método acomete la protección del primer fragmento de comunicación del que se omite la primera referencia de dirección. Una cierta capa que desee proteger criptográficamente sus tramas podría generar un Código de Integridad del Mensaje (MIC) para cada trama. Se puede generar un MIC de una cadena arbitraria mediante el uso, por ejemplo, de un cifrado en bloque en el modo CBC-MAC (véase Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, pág. 353). En el caso de una protección de trama, la entrada al CBC-MAC será la trama a ser protegida, posiblemente precedida por un número que indique la longitud de la trama. Después de que se determine el MIC se añadirá a la carga útil de la trama antes de que se envíe la trama.

En algunas implementaciones (restringidas) una capa inferior asume que un mensaje que se inició por una capa más alta está también protegido criptográficamente por esa capa más alta y por ello la capa más baja no realizará ninguna operación criptográfica sobre este mensaje. El uso de este método se basa en el paradigma “la capa en donde se inicia el mensaje cuida de la protección criptográfica”, la sobrecarga criptográfica se reduce a como mucho un MIC por mensaje físico. Pero esto significa que, en el ejemplo anterior, la capa más alta no puede confiar en la

capa más baja para una protección criptográfica de la referencia de dirección que ha sido omitida en la capa más alta y ahora solamente aparece en la capa más baja.

En esta realización, la protección criptográfica de la primera referencia de dirección se proporciona mediante el cálculo de un MIC antes de omitir la primera referencia de dirección. Dado que la información duplicada ya no está disponible en la capa más alta, ésta aún se incluye en el MIC y por lo tanto se protege. La realización por lo tanto tiene la ventaja de que mantiene la protección criptográfica para incluir la referencia de dirección que ha sido omitida.

Una realización del método de acuerdo con la invención se describe en la reivindicación 2. Esta realización tiene la ventaja de que solamente se añade protección criptográfica en un nivel en la capa de comunicación, lo que reduce la sobrecarga.

Una realización del método de acuerdo con la invención se describe en la reivindicación 3. Esta realización tiene la ventaja de que en una aplicación en donde cada mensaje es típicamente suficientemente corto para encajar en una trama (es decir en cada nivel el mensaje es más pequeño que la carga útil permitida máxima), se minimiza la sobrecarga de añadir un MIC mediante la realización de la operación en el nivel más alto posible, que es el nivel de inicio.

Una realización del método de acuerdo con la invención se describe en la reivindicación 4. La información duplicada a ser omitida se sustituye por un campo más corto que indica en dónde se puede hallar el dato omitido.

Es un objetivo adicional de la actual invención proporcionar un método de recepción, en el que el tamaño de la trama física se reduce en tanto se mantiene sustancialmente la información contenida, y su protección criptográfica.

Este objetivo se realiza mediante un método de recepción de acuerdo con la invención que se caracteriza porque la primera referencia de dirección se omite al menos parcialmente en los datos recibidos, y el método de recepción comprende adicionalmente la etapa de restauración de la primera referencia de dirección en la recuperación del primer fragmento de comunicación, y en el que la protección criptográfica del primer fragmento de comunicación se verifica después de que se recupere la primera referencia de dirección.

Realizaciones adicionales del método de recepción de acuerdo con la invención se describen en las reivindicaciones 6, 7 y 8. Estas realizaciones son complementarias a las realizaciones descritas anteriormente.

El sistema de acuerdo con la invención se caracteriza por que el medio transmisor se dispone para omitir al menos parcialmente la primera referencia de dirección de los datos transmitidos, y el medio de recepción se dispone para restaurar la primera referencia de dirección en la recuperación del primer fragmento de comunicación de los datos recibidos.

El dispositivo transmisor de acuerdo con la invención se caracteriza por que el dispositivo transmisor se dispone adicionalmente para eliminar al menos parcialmente la primera referencia de dirección en los datos transmitidos.

El dispositivo receptor de acuerdo con la invención se caracteriza por que la primera referencia de dirección está al menos parcialmente omitida en los datos recibidos, y el dispositivo receptor se dispone adicionalmente para restaurar la primera referencia de dirección en la recuperación del primer fragmento de comunicación.

La señal de acuerdo con la invención se caracteriza por que la señal transporta el segundo fragmento de comunicación en el que la primera referencia de dirección está al menos parcialmente omitida.

El producto programa de ordenador transmisor de acuerdo con la invención se caracteriza por que el producto programa de ordenador transmisor se dispone adicionalmente para omitir la primera referencia de dirección en los datos transmitidos.

El producto programa de ordenador receptor de acuerdo con la invención se caracteriza por que la primera referencia de dirección está al menos parcialmente omitida en los datos recibidos, y el producto programa de ordenador receptor se dispone adicionalmente para restaurar la primera referencia de dirección en la recuperación del primer fragmento de comunicación.

Estos y otros aspectos de la invención se describirán adicionalmente a modo de ejemplo y con referencia a los dibujos, en los que:

La Fig.1 ilustra un ejemplo de modelo de comunicación en capas,
la Fig. 2 muestra una relación entre una trama NWK y una trama MAC,
la Fig. 3 muestra la protección de las tramas usando un MIC,
la Fig. 4 muestra esa protección solamente en la capa de inicio,

la Fig. 5 muestra el proceso de cálculo del MIC y la omisión de los datos duplicados durante la generación de la trama,
la Fig. 6 muestra una comunicación en una disposición de salto múltiple,
la Fig. 7 muestra la misma comunicación usando la invención,
la Fig. 8 muestra otra realización de la misma comunicación de salto múltiple usando la invención,
la Fig. 9 muestra una realización recursiva de la invención, y
la Fig. 10 muestra una realización de la invención con un sub-direccionamiento a una capa más alta.

A todo lo largo de las figuras, los mismos números de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos se implementan típicamente en software y como tal representan entidades de software, tal como módulos u objetos de software.

Se ilustrará una primera realización de la invención mediante el ejemplo mostrado en la Fig. 1. La Fig. 1 muestra un ejemplo de un modelo de comunicación en capas 100, que comprende la capa física (PHY) 101, la capa de control de acceso al medio (MAC) 102, la capa de red (NWK) 103 y la capa de aplicación (APL) 104. La comunicación real 105 tiene lugar en el nivel más bajo. En la práctica se pueden usar más capas que las mostradas aquí. Se pueden usar diferentes canales de comunicación, incluyendo tecnologías ópticas, electrónicas e inalámbricas.

La Fig. 2 presenta un ejemplo de la relación entre dos tramas en capas adyacentes en la pila OSI, concretamente una trama NWK y una trama MAC, en una disposición de salto múltiple. Un mensaje en una red de salto múltiple, por ejemplo originada en la capa NWK, podría retransmitirse mediante uno o más dispositivos intermedios antes de llegar a su destino. Los dispositivos intermedios aplicarán algún algoritmo de enrutado para determinar a qué dispositivo se debería enviar a continuación el mensaje. La dirección del siguiente dispositivo intermedio se indica por la dirección NWK-HOP que se usa por los dispositivos receptores para determinar si hay un siguiente salto y si deberían enviar el mensaje más adelante.

La cabecera de la trama NWK contiene un campo de información (NWK-INF) 201 que da información acerca de, por ejemplo, el contenido del resto de la trama. Adicionalmente hay una dirección NWK del dispositivo donde se originó el mensaje (NWK-SRC) 204, su destino final (NWK-DEST) 202 y una carga útil (NWK-PAYLOAD) 205. En una disposición de salto múltiple también contendrá la dirección NWK del siguiente salto (NWK-HOP) 203 de modo que un dispositivo receptor pueda determinar si debería procesar la trama o descartarla. La capa MAC se usará para enviar la trama NWK como carga útil (MAC-PAYLOAD) 214 desde el dispositivo actual al siguiente salto y por ello contiene la dirección MAC del dispositivo actual (MAC-SRC) 213 y la dirección MAC del siguiente salto (MAC-DEST) 212. En muchos casos las entradas MAC-DEST y NWK-HOP se referirán al mismo dispositivo físico, es decir la información de direccionamiento se envía dos veces. En aplicaciones regulares, las direcciones en diferentes capas que se refieren al mismo dispositivo aparecen varias veces en una única trama física. En la invención la entrada de la dirección duplicada (en este ejemplo: NWK-HOP) se omite de la trama NWK y la capa NWK se basa en la entrada correspondiente (MAC-DEST) en la capa MAC.

Si una capa inicia un mensaje o genera una trama que contiene información (tal como una dirección) que se duplicará en una capa inferior, o bien directamente o bien a través de algún mapeado invertible tal como una tabla de búsqueda de direcciones, la capa más alta omitirá la información duplicada e indicará en uno de los campos (por ejemplo en el campo NWK-INF) qué información se omite y opcionalmente desde dónde puede recuperarse. Una simple realización de cómo indicar esto es definir bits que indiquen si se omite una cierta entrada. Con referencia a la Figura 2 y suponiendo que en la capa NWK es a veces posible omitir NWK-DEST 202, NWK-HOP 203 y NWK-SRC 204, el campo NWK-INF 201 contendría tres bits, cada uno refiriéndose a una de las entradas de direcciones que indican qué entradas de dirección están presentes (u omitidas). Se pueden usar bits adicionales o reglas implícitas para determinar qué campos se han de usar en la capa más baja. La capa de inicio en el extremo de recepción leerá los bits en el campo NWK-INF y obtendrá las direcciones omitidas desde las capas más bajas, directamente o usando el mapeado invertido que en muchos casos tomará la forma de una tabla de búsqueda.

Alternativamente, en lugar de omitir un campo, se podría sustituir por un campo más corto. Este campo más corto contendría entonces alguna clase de puntero o indicador de referencia que daría información de dónde se puede hallar la información omitida. De nuevo, sería posible usar un bit en, por ejemplo, el campo NWK-INF para indicar si se ha sustituido o no un campo.

Alternativamente, en lugar de añadir un campo de bit al campo NWK-INF, se puede usar una tecnología diferente para indicar que el campo omitido está sustituido por un campo corto. Si por ejemplo no se usa completamente el intervalo de valores válidos del campo omitido, pero está disponible un intervalo reservado que comienza con un prefijo especial, se podría usar este prefijo especial para indicar que el campo ha sido sustituido. Supongamos que el campo a ser omitido es por la derecha y tiene un intervalo de valores válidos de 0x00000000-0xeffffffff, entonces el prefijo 0xf... se podría usar para indicar que el campo ha sido sustituido por un campo más corto de por ejemplo solamente 2 bytes. El valor de este campo debería estar entonces de acuerdo con el prefijo y por ello estar limitado al intervalo 0xf000-0xffff.

La idea es especialmente de ventaja en la aplicación en donde está limitado el tamaño de la trama física de los mensajes. Un ejemplo típico de una aplicación de ese tipo es un sistema de dispositivos de conexión inalámbrica de bajo coste y/o baja potencia, tales como sensores, seguridad doméstica, automatización de edificios, medición remota, juegos, ratones, teclados, etc. Este método es incluso más beneficioso si las direcciones usadas en las diferentes capas OSI son idénticas en cuyo caso no se ha de realizar ninguna transmisión entre direcciones.

En una segunda realización de la invención, se mantiene la protección criptográfica para la dirección que ha sido omitida.

La Fig. 3 ilustra la situación en la que una cierta capa, tal como la capa NWK, desea proteger criptográficamente sus tramas generando un Código de Integridad del Mensaje (MIC) para cada trama que incluye la información de dirección. En este caso NWK-MIC 306 protege la trama NWK completa 301..305 mientras que MAC-MIC 315 protege la trama MAC completa 311..314 que incluye la trama NWK.

En un sistema de ejemplo, un tamaño máximo típico de una trama MAC podría ser de 102 bytes y el tamaño de un MIC se podría definir como de 4, 8 o 16 bytes. Si hay un MIC en cada capa de la pila OSI, habría 12 a 48 bytes MIC en una trama dando como resultado una sobrecarga de aproximadamente el 10-50%, suponiendo que los mensajes normalmente encajan en una única trama.

En algunas implementaciones (restringidas) una capa inferior supone que un mensaje que se inició por una capa más alta está también criptográficamente protegido por esa capa más alta, esto es para reducir la sobrecarga criptográfica tal como el envío de unos MIC adicionales.

Usando este enfoque en base al paradigma “la capa en donde se inicia el mensaje cuida de la protección criptográfica”, habrá al menos un MIC por mensaje tal como se muestra en la Fig. 4 para un mensaje que se origina desde la capa NWK. Esto significa que, en el ejemplo anterior, la capa NWK no puede confiar en la capa MAC para protección criptográfica de un NWK-HOP 403 (o, MAC-DEST 412).

Sin embargo, la información protegida debería incluir la información duplicada que se va a omitir durante la transferencia.

Si la capa que inicia el mensaje aún desea proteger la información duplicada usando un MIC, generará el MIC sobre toda la información relevante, incluyendo la información duplicada. Después de que se calcule el MIC, se elimina la información duplicada de la trama y se traduce mediante un mapeado invertible (por ejemplo una tabla de búsqueda) a la información correspondiente en las capas inferiores. Cuando se recibe la trama, se recupera la información apropiada desde las capas inferiores y se traduce en la información apropiada en la capa de inicio mediante el uso del mapeado invertido. Esta información se inserta en la trama en el lugar apropiado después de que se verifique el MIC.

Como se ilustra en la Fig. 5, la capa NWK calculará el MIC sobre la trama completa 501..505, incluyendo NWK-HOP, en la etapa del proceso 550. A continuación, se elimina NWK-HOP de la trama en la etapa del proceso 551, tal como se simboliza por la cruz 507 y se envía a la capa MAC para ser usada como, o ser traducida en, la MAC-DEST. La capa NWK del dispositivo receptor traduce MAC-DEST en NWK-HOP e inserta NWK-HOP en la trama antes de comprobar el NWK-MIC.

Si la información de dirección no sólo está omitida sino también sustituida por otra información, tal como se ha descrito anteriormente, esta otra información podría estar también opcionalmente protegida teniendo el MIC tanto sobre la información omitida, como sobre la de sustitución.

Esta realización tiene la ventaja adicional de que la protección criptográfica de la información omitida se mantiene.

La Fig. 6 muestra un mensaje desde M1 650 a través de M2 651 a M3 652 en una disposición de salto múltiple de acuerdo con una forma de comunicación tradicional.

La Fig. 7 muestra un mensaje desde M1 650 a través de M2 651 a M3 652 en una disposición de salto múltiple de acuerdo con una realización de la invención. Muestra que se omite NWK-HOP por referencia a MAC-DEST. Las líneas discontinuas y las cruces 711..712 indican que los campos se omiten realmente para reducir el tamaño de la trama. Una ventaja adicional de esta realización es que la trama NWK no cambia en comunicaciones posteriores entre saltos, reduciendo posiblemente adicionalmente la sobrecarga de procesamiento en los nodos.

Una realización que consigue ahorros adicionales en la reducción del tamaño de trama se representa en la Fig. 8. En la primera y última comunicación los campos NWK-SRC y NWK-DEST respectivamente se omiten también. Con el coste de un procesamiento en algún modo irregular, se obtiene una reducción adicional del tamaño de la comunicación.

En una realización diferente la invención se aplica recursivamente. La Fig. 9 muestra cómo campos en la capa de aplicación pueden referirse a campos en la capa de red, en la que estos campos se omiten también posiblemente debido a que se refieren a campos en una capa aún inferior.

En una realización adicional el direccionamiento no es el mismo en cada nivel. Mostramos un ejemplo donde la capa NWK usa las direcciones de los dispositivos, pero la capa APL direcciona las aplicaciones dentro de estos dispositivos, por ejemplo añadiendo cinco bits a la dirección del dispositivo 1001, 1003. Estos bits especifican una de las 32 aplicaciones dentro del dispositivo seleccionado. En esta realización la dirección en la capa APL no puede omitirse completamente, dado que estos cinco bits no están disponibles en un nivel más bajo. Solamente los prefijos de los campos 1001, 1003 se duplican en una capa inferior. Por lo tanto los campos 1010, 1011 no se omiten sino que se sustituyen por campos más cortos 1002, 1004 como se muestra en la Fig. 10.

Son posibles alternativas. En la descripción anterior, “comprendiendo” no excluye otros elementos o etapas, “un” o “una” no excluye una pluralidad, y un único procesador u otra unidad pueden cumplir también las funciones de varios medios enumerados en las reivindicaciones. La comunicación real incluye la comunicación real entre diferentes dispositivos o partes de un dispositivo, por medio de una tecnología óptica, electrónica, inalámbrica, microondas o cualquier otra adecuada, o incluso comunicación entre componentes de software dentro de un sistema de procesamiento o entre sistemas de procesamiento.

REIVINDICACIONES

1. Un método de transmisión para la transmisión de datos usando un modelo de comunicación en capas, comprendiendo las etapas de

generación en una primera capa de un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante un código de integridad del mensaje y que comprende una primera referencia de dirección que se refiere a una primera entidad,
generación en una segunda capa por debajo de la primera capa de un segundo fragmento de comunicación en base al primer fragmento de comunicación y comprendiendo adicionalmente una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad,
transmisión de los datos comprendiendo el segundo fragmento de comunicación,
en el que
los datos transmitidos comprenden el código de integridad del mensaje y el método de transmisión comprende adicionalmente la etapa de
eliminar al menos parcialmente la primera referencia de dirección en los datos transmitidos, en el que se proporciona la protección criptográfica para el primer fragmento de comunicación antes de que la primera referencia de dirección se elimine al menos parcialmente.

2. El método de transmisión de acuerdo con la reivindicación 1, en el que se proporciona la protección criptográfica solamente en una única capa en el modelo de comunicación.

3. El método de transmisión de acuerdo con la reivindicación 2, en el que la única capa es igual a la capa en donde se inicia el mensaje.

4. El método de transmisión de acuerdo con la reivindicación 1, en el que la primera referencia de dirección se sustituye por un campo de información que se refiere a la segunda referencia de información.

5. Un método de recepción para recibir datos usando un modelo de comunicación en capas, que comprende la etapa de

recibir datos que comprenden un segundo fragmento de comunicación,

- el segundo fragmento de comunicación

comprende una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad
basándose en un primer fragmento de comunicación criptográficamente protegido que se protege criptográficamente mediante el código de integridad del mensaje, comprendiendo el primer fragmento de comunicación una primera referencia de dirección a la primera entidad, y

recuperando el primer fragmento de comunicación del segundo fragmento de comunicación, en el que la primera referencia de dirección está al menos parcialmente omitida en los datos recibidos,
el código de integridad del mensaje se recibe como parte de los datos recibidos, y
el método de recepción comprende adicionalmente la etapa de restaurar la primera referencia de dirección al recuperar el primer fragmento de comunicación, y en el que se verifica la protección criptográfica del primer fragmento de comunicación después de que se restaure la primera referencia de dirección.

6. El método de recepción de acuerdo con la reivindicación 5, en el que se proporciona protección criptográfica solamente en una única capa en el modelo de comunicación.

7. El método de recepción de acuerdo con la reivindicación 6, en el que la única capa es igual a la capa en donde se inicia el mensaje.

8. El método de recepción de acuerdo con la reivindicación 5, en el que el método de recepción recupera la primera referencia de dirección usando un campo de información en los datos recibidos que sustituye a la primera referencia de dirección y se refiere a la segunda referencia de dirección.

9. Sistema para la comunicación que usa un modelo de comunicación en capas, comprendiendo el sistema

un medio transmisor

que se dispone para generar en una primera capa un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente

protegido mediante un código de integridad del mensaje, comprendiendo el primer fragmento de comunicación una primera referencia de dirección que se refiere a una primera entidad, y
que se dispone adicionalmente para generar en una segunda capa por debajo de la primera capa un segundo fragmento de comunicación en base al primer fragmento de comunicación y que comprende adicionalmente una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad,

un medio de comunicación

que se dispone para transmitir datos que comprenden el segundo fragmento de comunicación, y

un medio de recepción

que se dispone para recibir datos que comprenden el segundo fragmento de comunicación, y
que se dispone adicionalmente para recuperar el primer fragmento de comunicación del segundo fragmento de comunicación,
en el que

el medio transmisor se dispone para omitir al menos parcialmente la primera referencia de dirección de los datos transmitidos, se dispone para transmitir el código de integridad del mensaje como una parte de los datos transmitidos, y se dispone para proporcionar protección criptográfica para el primer fragmento de comunicación antes de omitir al menos parcialmente la primera referencia de dirección, y
el medio de recepción se dispone para restaurar la primera referencia de dirección con la recuperación del primer fragmento de comunicación de los datos recibidos y se dispone para verificar la protección criptográfica del primer fragmento de comunicación después de la restauración de la primera referencia de dirección.

10. Un dispositivo transmisor para la transmisión de datos usando un modelo de comunicación en capas, disponiéndose el dispositivo transmisor para generar en una primera capa un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante un código de integridad del mensaje y que comprende una primera referencia de dirección que se refiere a una primera entidad,
disponiéndose adicionalmente para generar en una segunda capa por debajo de la primera capa un segundo fragmento de comunicación en base al primer fragmento de comunicación y comprendiendo adicionalmente una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad,
disponiéndose adicionalmente para transmitir datos que comprenden el segundo fragmento de comunicación, en el que
el dispositivo transmisor se dispone adicionalmente para eliminar al menos parcialmente la primera referencia de dirección en los datos transmitidos, se dispone para transmitir el código de integridad del mensaje como una parte de los datos transmitidos y se dispone para proporcionar protección criptográfica para el primer fragmento de comunicación antes de omitir al menos parcialmente la primera referencia de dirección.

11. Un dispositivo receptor para la recepción de datos usando un modelo de comunicación en capas, disponiéndose el dispositivo receptor para recibir datos que comprenden un segundo fragmento de comunicación,

-comprendiendo el segundo fragmento de comunicación una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad,
basándose en un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante el código de integridad del mensaje, comprendiendo el primer fragmento de comunicación una primera referencia de dirección a la primera entidad, y

disponiéndose adicionalmente para recuperar el primer fragmento de comunicación del segundo fragmento de comunicación, en el que
la primera referencia de dirección está al menos parcialmente omitida en los datos recibidos,
el código de integridad del mensaje se recibe como una parte de los datos recibidos, y
el dispositivo receptor se dispone adicionalmente para restaurar la primera referencia de dirección en la recuperación del primer fragmento de comunicación y se dispone para verificar la protección criptográfica del primer fragmento de comunicación después de la restauración de la primera referencia de dirección.

12. Una señal para transportar datos generados de acuerdo con un modelo de comunicación en capas,

siendo generados los datos de acuerdo con un modelo de comunicación en capas que comprende

una primera capa en la que se genera un primer fragmento de comunicación criptográficamente protegido siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante un código de integridad del mensaje y comprendiendo una primera referencia de dirección que se

refiere a una primera entidad, se genera una segunda capa por debajo de la primera capa en la que se genera un segundo fragmento de comunicación que comprende una segunda referencia de dirección que se refiere a una segunda entidad relacionada con la primera entidad y en base al primer fragmento de comunicación, en el que

la señal transporta el segundo fragmento de comunicación en el que la primera referencia de dirección está al menos parcialmente omitida y la señal transporta el código de integridad del mensaje.

13. Un producto de programa de ordenador transmisor para implementar una comunicación usando un modelo de comunicación en capas, disponiéndose el producto de programa de ordenador transmisor
para generar en una primera capa un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante un código de integridad del mensaje y comprendiendo una primera referencia de dirección a una primera entidad,
disponiéndose adicionalmente para generar en una segunda capa por debajo de la primera capa un segundo fragmento de comunicación en base al primer fragmento de comunicación y que comprende adicionalmente una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con la primera entidad,
disponiéndose adicionalmente para transmitir datos que comprenden el segundo fragmento de comunicación, en el que
el producto de programa de ordenador transmisor se dispone adicionalmente para omitir la primera referencia de dirección en los datos transmitidos, se dispone para transmitir el código de integridad del mensaje como una parte de los datos transmitidos y se dispone para proporcionar protección criptográfica para el primer fragmento de comunicación antes de omitir al menos parcialmente la primera referencia de dirección.

14. Un producto programa de ordenador receptor para implementar la comunicación usando un modelo de comunicación en capas, disponiéndose el producto programa de ordenador receptor para disponer datos que comprenden un segundo fragmento de comunicación,

- el segundo fragmento de comunicación

comprende una segunda referencia de dirección que se refiere a una segunda entidad que se relaciona con una primera entidad
basándose en un primer fragmento de comunicación criptográficamente protegido, siendo criptográficamente protegido el primer fragmento de comunicación criptográficamente protegido mediante el código de integridad del mensaje, que comprende una primera referencia de dirección a la primera entidad, y

disponiéndose adicionalmente para recuperar el primer fragmento de comunicación del segundo fragmento de comunicación,

una primera capa en la que se genera un primer fragmento de comunicación que comprende una primera referencia de dirección que se refiere a una primera entidad,
una segunda capa por debajo de la primera capa en la que se genera un segundo fragmento de comunicación que comprende una segunda referencia de dirección que se refiere a una segunda entidad relacionada con la primera entidad y basado en el primer fragmento de comunicación,
en el que
la primera referencia de dirección está omitida al menos parcialmente en los datos recibidos,
el código de integridad del mensaje se recibe como una parte de los datos recibidos, y
el producto de programa de ordenador receptor se dispone adicionalmente para restaurar la primera referencia de dirección con la recuperación del primer fragmento de comunicación y se dispone para verificar la protección criptográfica del primer fragmento de comunicación después de la restauración de la primera referencia de dirección.

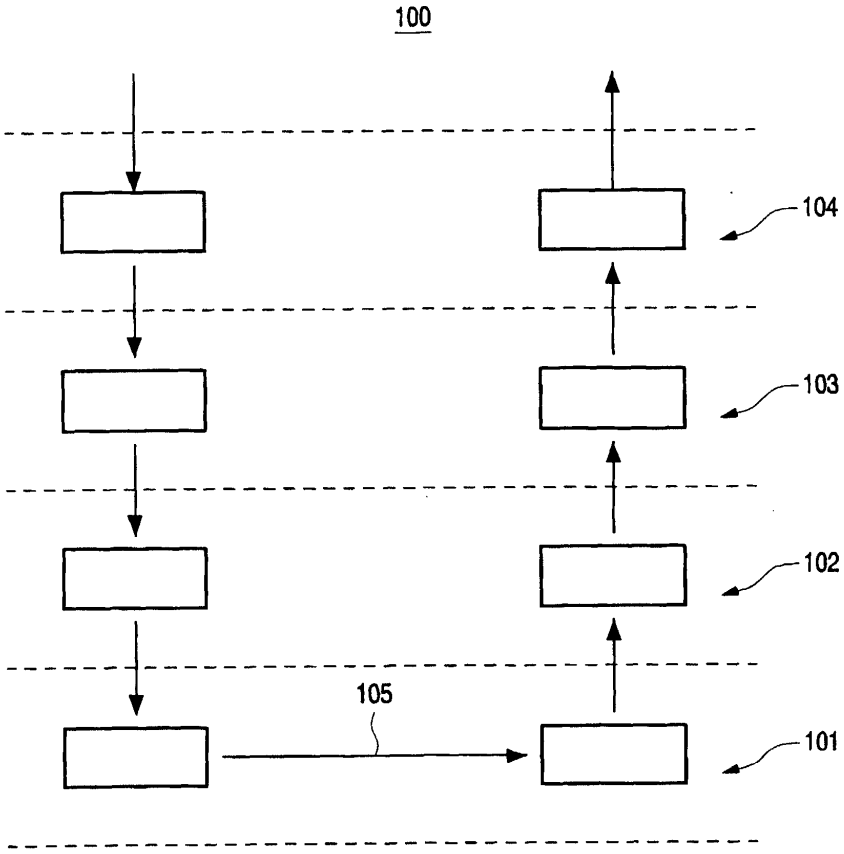

Fig.1

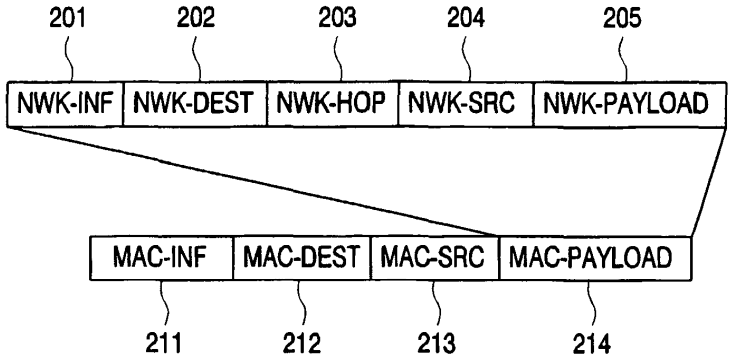

Fig.2

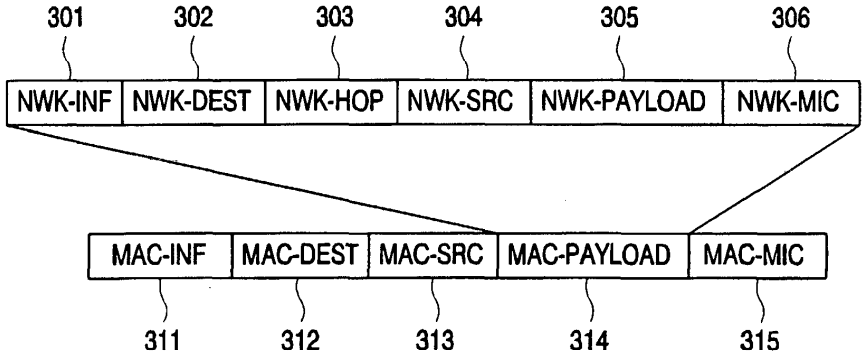

Fig.3

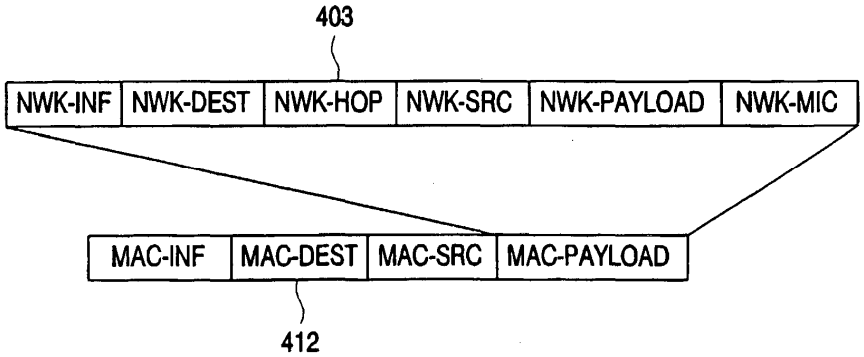

Fig.4

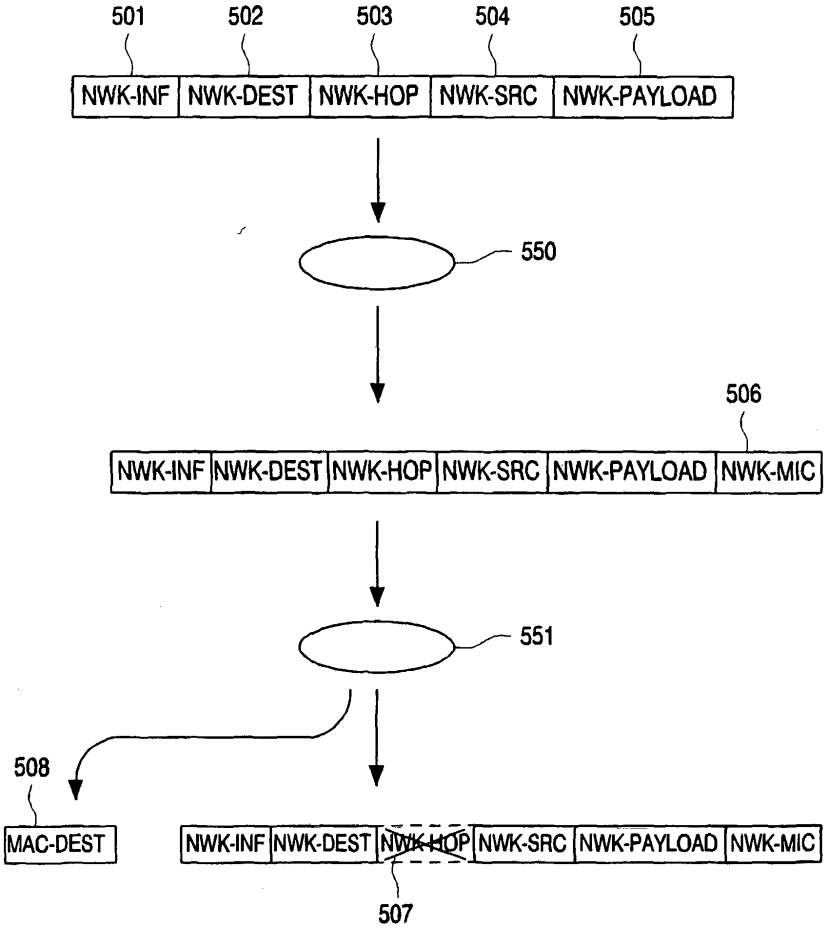
501
502
503
504
505
NWK-INF
NWK-DEST
NWK-HOP
NWK-SRC
NWK-PAYLOAD
550
506
NWK-INF
NWK-DEST
NWK-HOP
NWK-SRC
NWK-PAYLOAD
NWK-MIC
551
508
MAC-DEST
NWK-INF
NWK-DEST
NWK-HOP
NWK-SRC
NWK-PAYLOAD
NWK-MIC
507

Fig.5

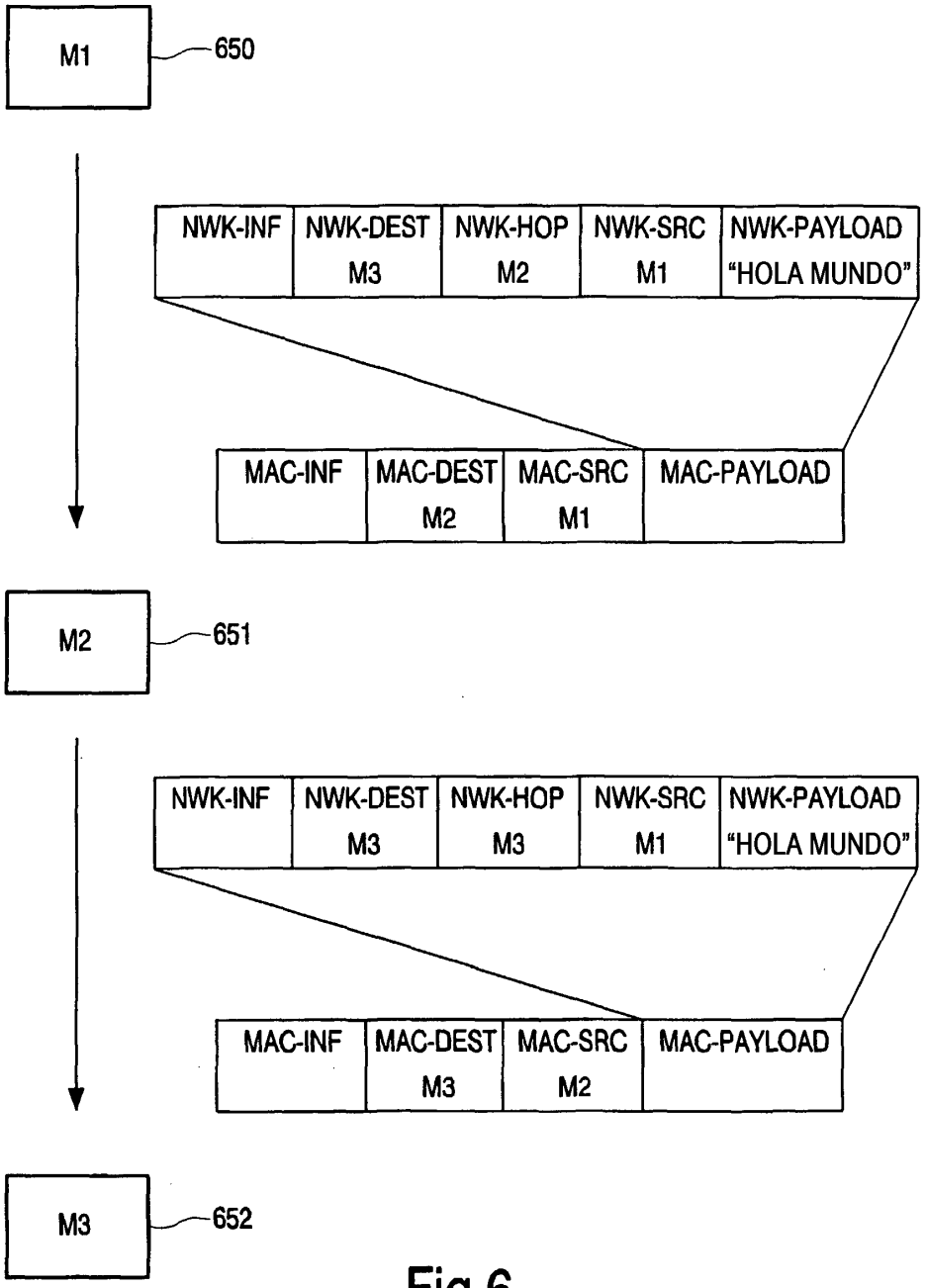
M1
650
NWK-INF
NWK-DEST
M3
NWK-HOP
M2
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
MAC-INF
MAC-DEST
M2
MAC-SRC
M1
MAC-PAYLOAD
M2
651
NWK-INF
NWK-DEST
M3
NWK-HOP
M3
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
MAC-INF
MAC-DEST
M3
MAC-SRC
M2
MAC-PAYLOAD
M3
652

Fig.6

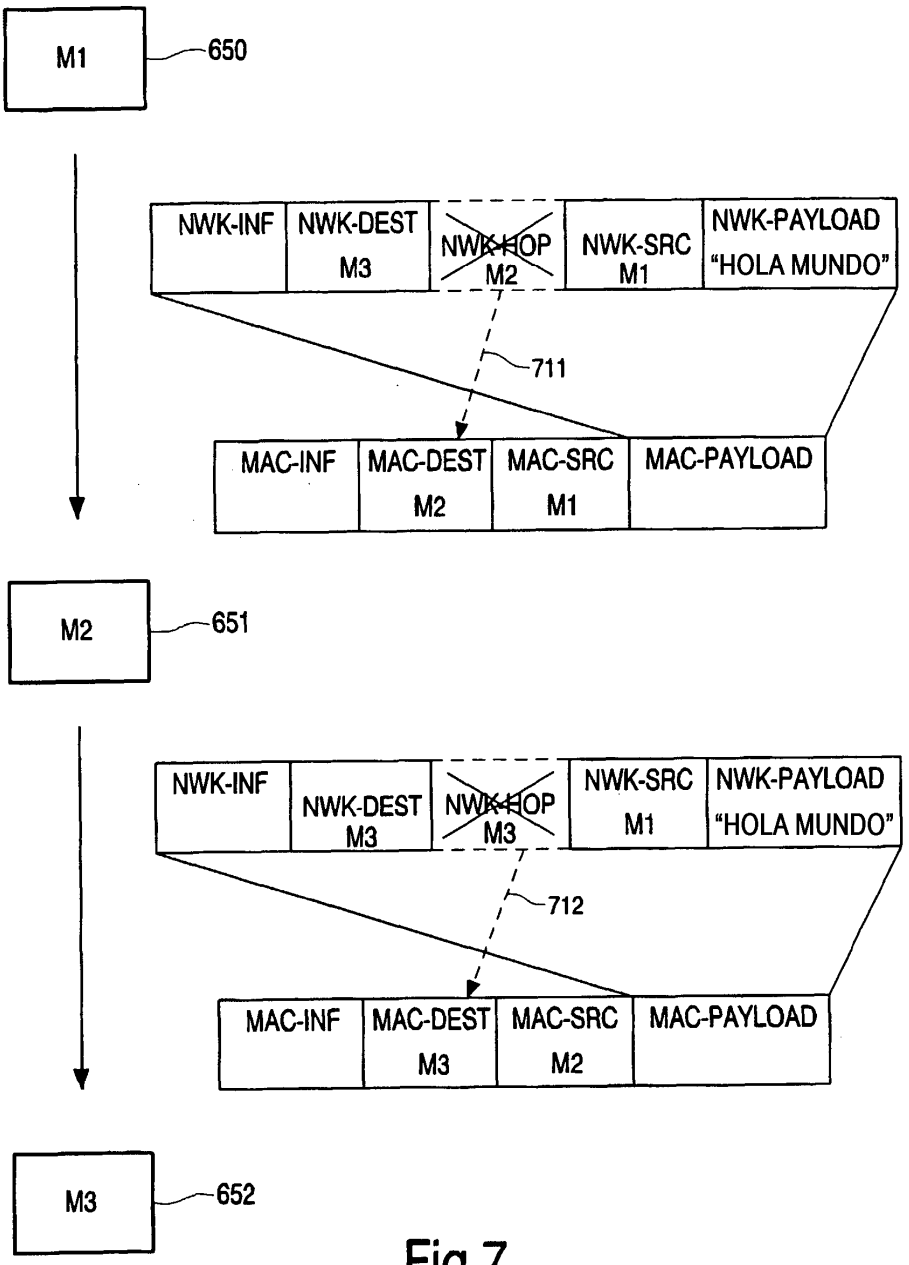
M1
650
NWK-INF
NWK-DEST
M3
NWK-HOP
M2
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
711
MAC-INF
MAC-DEST
M2
MAC-SRC
M1
MAC-PAYLOAD
M2
651
NWK-INF
NWK-DEST
M3
NWK-HOP
M3
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
712
MAC-INF
MAC-DEST
M3
MAC-SRC
M2
MAC-PAYLOAD
M3
652

Fig.7

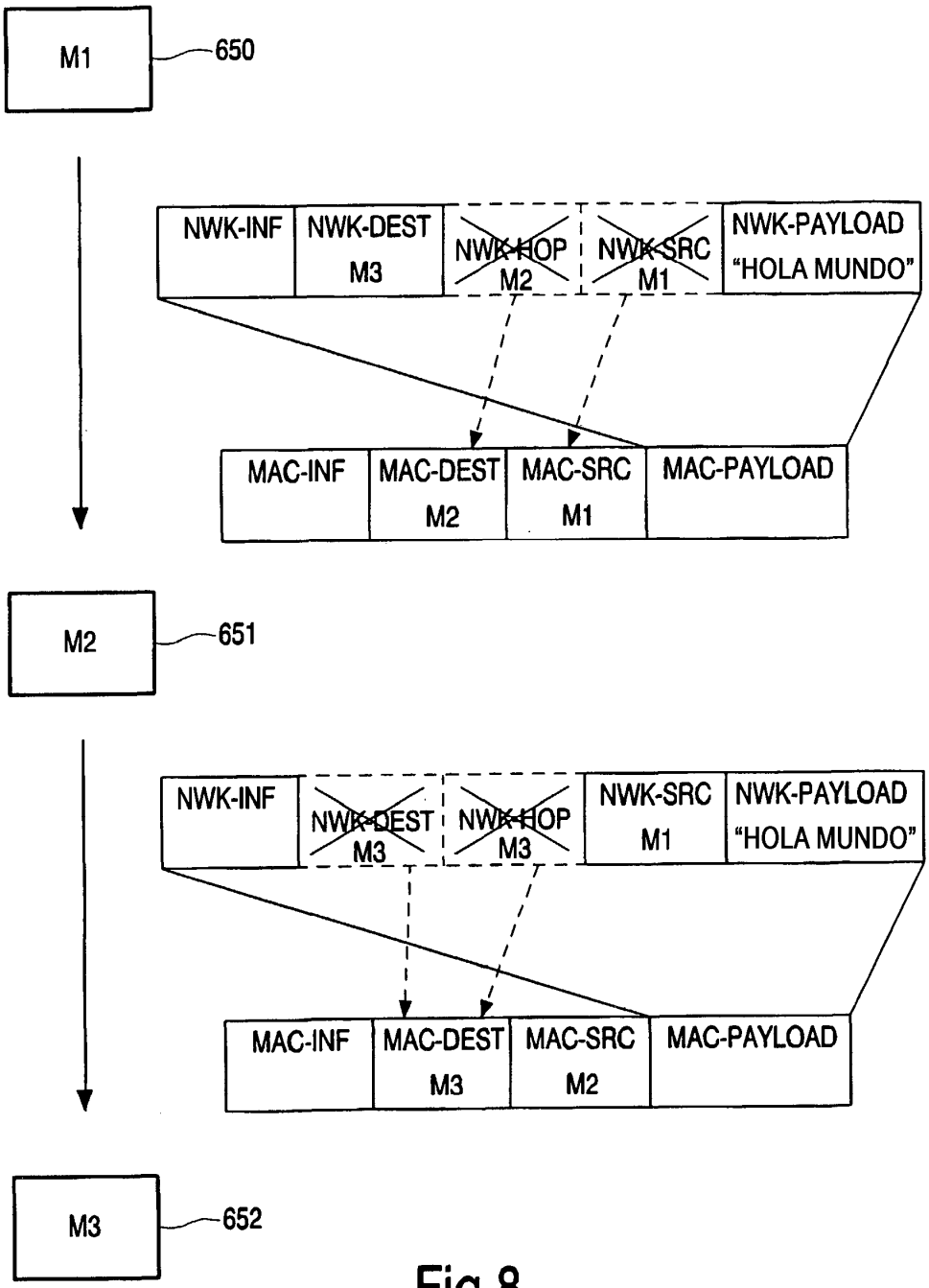
M1
650
NWK-INF
NWK-DEST
M3
NWK-HOP
M2
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
MAC-INF
MAC-DEST
M2
MAC-SRC
M1
MAC-PAYLOAD
M2
651
NWK-INF
NWK-DEST
M3
NWK-HOP
M3
NWK-SRC
M1
NWK-PAYLOAD
"HOLA MUNDO"
MAC-INF
MAC-DEST
M3
MAC-SRC
M2
MAC-PAYLOAD
M3
652

Fig.8

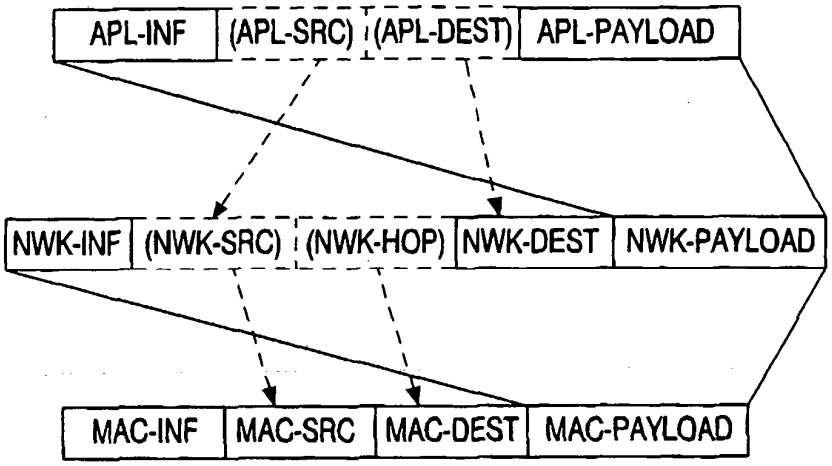
APL-INF
(APL-SRC)
(APL-DEST)
APL-PAYLOAD
NWK-INF
(NWK-SRC)
(NWK-HOP)
NWK-DEST
NWK-PAYLOAD
MAC-INF
MAC-SRC
MAC-DEST
MAC-PAYLOAD

Fig.9

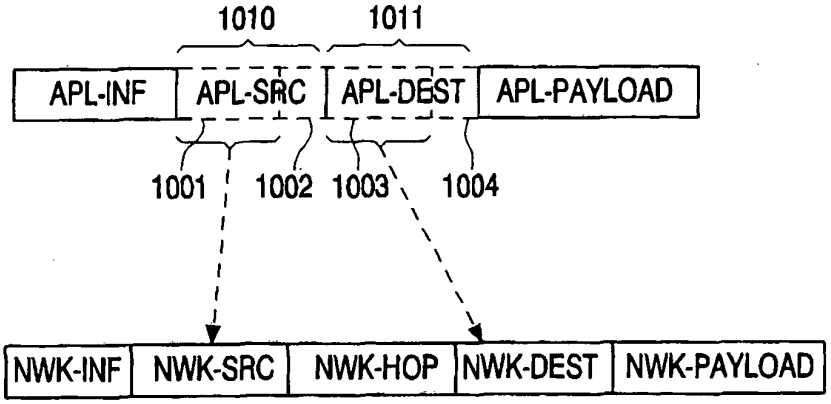
1010
1011
APL-INF
APL-SRC
APL-DEST
APL-PAYLOAD
1001
1002
1003
1004
NWK-INF
NWK-SRC
NWK-HOP
NWK-DEST
NWK-PAYLOAD

Fig.10