(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 111**

(51) Int. Cl.:
H04L 12/18 (2006.01)
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04744435 .1**
(96) Fecha de presentación : **30.06.2004**
(97) Número de publicación de la solicitud: **1645071**
(97) Fecha de publicación de la solicitud: **12.04.2006**

(54) Título: **Direccionamiento indirecto seguro.**

(30) Prioridad: **03.07.2003 EP 03101998**

(45) Fecha de publicación de la mención BOPI:
05.05.2011

(45) Fecha de la publicación del folleto de la patente:
05.05.2011

(73) Titular/es:
KONINKLIJKE PHILIPS ELECTRONICS N.V.
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es: **Kevenaar, Thomas, A., M.**

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCION

Direccionamiento indirecto seguro.

La invención se refiere a un procedimiento de comunicación de un fragmento de comunicación. La invención se refiere además al correspondiente dispositivo encaminador, dispositivo receptor, sistema, y señal que implementan este procedimiento.

En redes de comunicación a menudo se realiza la distinción entre unidifusión, multidifusión y difusión. Unidifusión es la situación en la que un dispositivo único (el dispositivo emisor) envía un mensaje a otro dispositivo único (el dispositivo receptor). En multidifusión, el dispositivo emisor envía un mensaje a varios dispositivos receptores (a más de uno, pero no a todos), mientras que en difusión, el dispositivo emisor envía un mensaje a todos los dispositivos en la red.

Aunque casi todas las redes contienen algoritmos de encaminamiento que soportan unidifusión, esto no siempre es el caso para multidifusión. Cuando los algoritmos de encaminamiento no soportan multidifusión y un dispositivo único todavía desea dirigirse a varios dispositivos, la multidifusión puede lograrse mediante unidifusión repetida.

Sin embargo, el dispositivo emisor no podría ni tendría permiso para realizar unidifusión repetida debido a, por ejemplo, limitaciones de potencia o de coste. Un ejemplo sería una red de control inalámbrica usada para controlar las luces en grandes espacios públicos. Aquí un único conmutador de luz barato, debe poder conmutar por ejemplo, más de 50 luces. Obviamente pueden encontrarse muchos más ejemplos de aplicación.

Puede encontrarse una solución a este problema en direccionamiento indirecto (IA), en el que un segundo dispositivo (el dispositivo encaminador) está disponible en la proximidad del dispositivo emisor. El dispositivo emisor enviará entonces un mensaje único al dispositivo encaminador que realizará, a continuación, unidifusión repetida.

Sin embargo, los problemas están relacionados con los aspectos de seguridad de IA. Por ejemplo, la aplicación que se ejecuta en el dispositivo emisor podría desear cifrar su mensaje usando una clave de cifrado K_G conocida solamente por miembros de un grupo G. Además el dispositivo emisor podría desear aplicar un código de integridad de mensaje (MIC) a partes de la comunicación tales como su propia dirección ID1 y la dirección de destino G en el mensaje usando también K_G. El resultado es que solamente los miembros de G (pero *no* el dispositivo encaminador) pueden leer el mensaje y los dispositivos de recepción pueden verificar si, en efecto, el mensaje está destinado a ellos y si se envió por el dispositivo emisor ID1.

Los protocolos de comunicación se describen comúnmente usando una pila a modo de OSI estratificada. Parte de esta pila son, de la parte inferior a la parte 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). Tramas intercambiadas entre capas iguales en dispositivos diferentes consisten en una *cabecera* y una *carga útil*. Una trama en el nivel *n* en la pila se envía físicamente como la carga útil de una trama en la capa n-1. Las abreviaturas para identificar algunos de los campos en estas cabeceras son las siguientes: SRC para la dirección de origen, DEST para la dirección de destino, e INF para el campo de información.

Una solución sencilla pero ineficaz al problema sería hacer que la capa de aplicación calcule un MIC en el mensaje, y en su dirección de destino y en su dirección de origen usando la clave de grupo K_G.

La capa NWK entonces añadirá también las direcciones NWK-DEST y NWK-SRC, puesto que habitualmente se requieren por los algoritmos de encaminamiento. Además podría calcular un MIC adicional en estas dos direcciones NWK. En comparación con las soluciones dadas anteriormente esta dará como resultado más sobrecarga (una o dos direcciones más) y un MIC adicional que debe enviarse lo que hace que esta solución sea menos eficaz. Un segundo inconveniente es que el nivel APL se ocupa de verificar la información de dirección, una tarea que pertenece de manera más natural a una capa más baja.

La solicitud de patente internacional WO00/62503 describe un aparato y un procedimiento para autenticar mensajes en una multidifusión usando etiquetas para determinar si el nodo de transmisión está en la multidifusión.

La solicitud de patente europea EP902569 describe un procedimiento y un sistema para el acceso de un cliente de punto extremo de unidifusión a una sesión de protocolo de Internet (IP) de multidifusión. El procedimiento comprende acumular en un servidor de pasarela información de directorio relacionada con la sesión de multidifusión, suministrar a un cliente de unidifusión la información del directorio, recibir en el servidor de pasarela del cliente de unidifusión una petición para unirse a una sesión seleccionada elegida a partir de la información de directorio, y unirse a la sesión solicitada en el servidor de pasarela en nombre del cliente de unidifusión, comprendiendo además conversión de dirección. Es un objetivo de la invención proporcionar un procedimiento que mejore la eficacia del direccionamiento indirecto al tiempo que se proporciona seguridad.

Este objetivo se realiza mediante un procedimiento de comunicación de un fragmento de comunicación, comprendiendo el fragmento de comunicación una primera referencia de dirección de destino relativa a un grupo de al menos un dispositivo receptor, comprendiendo las etapas de: - añadir un dispositivo emisor un código de integridad de mensaje cifrado para proteger al menos parte del fragmento de comunicación, - transmitir el dispositivo emisor el fragmento de comunicación protegido a un dispositivo encaminador, - modificar el dispositivo encaminador, para al menos un

dispositivo receptor en el grupo de dispositivos de destino, la primera referencia de dirección de destino para obtener una dirección del al menos un dispositivo receptor, mientras que se mantiene el código de integridad de mensaje cifrado sin cambios, y posteriormente retransmitir el fragmento de comunicación protegido modificado al, al menos un, dispositivo receptor, - recibir el al menos un dispositivo receptor el fragmento de comunicación protegido modificado, - restaurar el al menos un dispositivo receptor el fragmento de comunicación protegido original para permitir la verificación del fragmento de comunicación protegido original usando el código de integridad de mensaje.

Por razones de seguridad, la información de direccionamiento debería protegerse con un MIC usando la clave K_G. Sin embargo, el dispositivo encaminador debe poder cambiar la información de direccionamiento para realizar unidifusión repetida. Obviamente, puesto que G está protegido por el MIC, no puede sustituirse simplemente por una dirección de destino para realizar unidifusión repetida: cuando el dispositivo receptor recibe el fragmento de comunicación con la dirección sustituida y comprueba el MIC, encontrará un desajuste porque la información protegida debería contener G y no el dispositivo receptor ID. Como resultado, probablemente ignorará el mensaje.

Por tanto, el dispositivo emisor indica el uso de direccionamiento indirecto, por ejemplo, fijando un campo de bit de IA especial en el mensaje. (Alternativamente, el dispositivo encaminador puede indicar el uso de direccionamiento indirecto, por ejemplo, fijando un campo de bit de IA especial en el mensaje, después de detectar, por ejemplo, porque la dirección de destino es una identidad de grupo, que se usa direccionamiento indirecto). Las direcciones MAC-DEST y MAC-SRC indican que se envía un mensaje del ID1 al ID2. Las direcciones NWK-DEST y NWK-SRC indican que el destino final del mensaje son todos los miembros en G (excepto posiblemente el propio ID1) y que ID1 envió el mensaje. El campo NWK-INF indica además que el mensaje se usa en el contexto de direccionamiento indirecto (IA=1) y la aplicación a ID1 cifró la cadena m usando la clave de grupo K_G (lo que se indica por $E_{KG}(m)$).

Al recibir el mensaje desde el dispositivo emisor, el dispositivo encaminador observa que es un mensaje de IA inspeccionando el bit de IA en el campo NWK-INF y realizará una unidifusión múltiple a todos los miembros del grupo G (excepto posiblemente el dispositivo emisor ID1). A partir de su información de encaminamiento (por ejemplo, tablas de encaminamiento), el dispositivo encaminador sabe que una forma de llegar al dispositivo receptor es enviándolo a nodos intermedios. El encaminador cambia, para cada dispositivo receptor, el campo NWK-DEST desde la entrada G hasta la dirección del dispositivo receptor ID, ya que los saltos intermedios no tienen constancia de una identidad de grupo G y los algoritmos de encaminamiento de unidifusión necesitan una dirección de dispositivo única, conocida, como destino final. Debe observarse además que, a causa de la sustitución, el MIC y la información protegida ya no concuerdan. El dispositivo receptor tras recibir el mensaje sustituirá la información modificada, por ejemplo, el dispositivo receptor ID por el ID de grupo, y se puede verificar posteriormente el MIC. El dispositivo receptor debería conocer la identidad de todos los dispositivos en G para realizar esta acción. Una solución alternativa es que el dispositivo emisor o el dispositivo encaminador copie la identidad del grupo G en algún lugar en el fragmento de comunicación, por ejemplo, en el campo NWK-INF en la trama NWK. De esta manera los dispositivos receptores no tienen que almacenar el enlace entre identidades de dispositivos e identidades de grupos y todavía pueden sustituir la identidad de grupo en el campo NWK-DEST antes de verificar el MIC. Además, de esta manera se soportan múltiples grupos solapados.

La ventaja de esta solución es que el dispositivo emisor solamente requiere almacenar una cantidad muy limitada de información, y enviar pocos fragmentos de comunicación y muy cortos. Las actividades del dispositivo encaminador (ID2) y los saltos intermedios son independientes del hecho de si el mensaje por el dispositivo emisor (en este caso, ID1) es seguro o no. Solamente los miembros del grupo y (naturalmente) el dispositivo encaminador necesitan tener constancia del direccionamiento indirecto; los nodos intermedios entre el dispositivo encaminador y los dispositivos receptores no tienen constancia del modo de direccionamiento indirecto. No es necesario confiar en el dispositivo encaminador con datos de aplicación.

Una implementación ventajosa del procedimiento según la invención se describe en la reivindicación 2. El uso de un único campo de bit de IA para indicar el uso del modo de direccionamiento indirecto es sencillo y eficaz.

Una implementación ventajosa del procedimiento según la invención se describe en la reivindicación 4. Usar una única clave común tanto para cifrar el contenido del mensaje como para generar o verificar el MIC da como resultado una implementación eficaz.

Una implementación ventajosa del procedimiento según la invención se describe en la reivindicación 5. El dispositivo receptor intenta sustituciones múltiples de la referencia de dirección de destino mediante los grupos de los que es miembro el dispositivo emisor. De esta manera, el dispositivo receptor puede encontrar la identidad de grupo para la que el MIC coincide. Esto alivia la necesidad de añadir la identidad de grupo en el fragmento de comunicación, optimizando por tanto la longitud del fragmento de comunicación.

Una implementación ventajosa del procedimiento según la invención se describe en la reivindicación 6. Esta implementación permite al dispositivo receptor restaurar el fragmento de comunicación sin información local o sin tener que realizar múltiples intentos para encontrar la identidad de grupo coincidente almacenando o copiando la primera referencia de dirección de destino original en el fragmento de comunicación protegido modificado.

El dispositivo encaminador, el dispositivo receptor, el sistema, y la señal según la invención están caracterizados tal como se describe en las reivindicaciones 7 a 10.

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

la figura 1 muestra una vista en despiece ordenado de un mensaje en la capa MAC para una pila de protocolo de cuatro capas,

la figura 2 muestra un ejemplo esquemático de direccionamiento indirecto,

la figura 3 muestra un ejemplo detallado de direccionamiento indirecto, y

la figura 4 muestra los formatos de mensaje en el nivel MAC durante el direccionamiento indirecto

En todas las figuras, los mismos números de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos se implementan normalmente en software, y como tal representan entidades de software, tales como módulos u objetos de software.

Los protocolos de comunicación se describen comúnmente usando una pila a modo de OSI estratificada. Una pila a modo de ejemplo comprende, de la parte inferior a la parte 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). Las tramas intercambiadas entre capas iguales en dispositivos diferentes consisten en una *cabecera* y una *carga útil* y una trama en el nivel *n* en la pila se envía físicamente como la carga útil de una trama en la capa n-1. Por tanto, considerando las tres capas superiores en esta pila de protocolo de cuatro capas, la figura 1 ilustra un mensaje 100 enviado por la capa MAC.

En muchos casos existe una estrecha relación entre las direcciones en la capa APL y en la capa NWK que hacen posible excluir la información de dirección duplicada en la capa APL para llegar a una solución eficaz. La información de dirección en la capa NWK habitualmente no puede excluirse porque se requiere por los algoritmos de encaminamiento. Debido a que las direcciones APL habitualmente son iguales a las direcciones NWK o pueden derivarse fácilmente, no siempre están presentes para reducir el tamaño del mensaje.

Los campos INF contienen información para un dispositivo de recepción sobre las diferentes capas sobre qué tipo de información está presente en el resto del mensaje y cómo debería tratarse. Por ejemplo, el campo MAC-INF podría indicar que la CARGA ÚTIL DE MAC está cifrada. Esto mostrará al dispositivo de recepción que primero debe descifrar la carga útil antes de ocuparse de ella adicionalmente. Asimismo, el campo NWK-INF podría indicar que la trama recibida se genera en el contexto de direccionamiento indirecto y debería tratarse en consecuencia.

El direccionamiento indirecto se representa esquemáticamente en la figura 2. ID1, dispositivo 201 emisor, miembro del grupo G= {ID1, ID3, ID4, ID5}, envía un mensaje 211 que contiene la dirección de destino final G, su propia dirección ID1 y una cadena m (es decir, la información real que va a enviarse al grupo) a ID2, el dispositivo 202 encaminador. Cuando ID2 recibe el mensaje y observa que el mensaje procedente de ID1 está destinado al grupo G, retransmitirá el mensaje a ID3 203, ID4 204 e ID5 205 cuyas direcciones encontró, por ejemplo, en una tabla 212 de emparejamiento.

Como medida de seguridad, la aplicación que se ejecuta en ID1 que genera la cadena m, podría desear cifrar m usando una clave de cifrado K_G conocida solamente por miembros de G. Además podría desear aplicar un código de integridad de mensaje (MIC) a su propia dirección ID1 y la dirección de destino G en el mensaje también usando K_G. El resultado de estas medidas de seguridad es que sólo los miembros de G (aunque *no* el dispositivo encaminador) pueden leer el mensaje y los dispositivos de recepción pueden verificar si, en efecto, el mensaje está destinado a ellos y si se envió por ID1.

Puesto que ID1 no confía en el dispositivo encaminador ID2, ID2 no tiene acceso a la clave K_G. Sin embargo, el nodo encaminador debería poder cambiar la información de direccionamiento en el nivel NWK para realizar unidifusión repetida. Puesto que G está protegido por el MIC, simplemente no puede sustituirse por ID3, ID4 e ID5 para realizar unidifusión repetida: cuando los dispositivos de recepción ID3, ID4 e ID5 comprueban el MIC, encontrarán un desajuste porque la información protegida debería contener G y no ID3, ID4 o ID5, respectivamente. Como resultado, ignorarán el mensaje.

Como se ilustra en la figura 3, ID1 conoce la clave de grupo de cifrado K_G, la identidad del grupo G (aunque no necesariamente las direcciones de todos los miembros del grupo) y la dirección de su dispositivo encaminador ID2. El dispositivo encaminador ID2 conoce o puede recuperar las direcciones de todos los miembros de G.

ID1 envía el mensaje 301 al encaminador 302 ID2 que, en el nivel MAC, se parecerá al mensaje 401 en la figura 4 en el que, en comparación con la figura 1, los campos que no son pertinentes en la explicación actual se omiten por motivos de claridad. Las direcciones MAC-DEST y MAC-SRC indican que un mensaje se envía de ID1 a ID2. Las direcciones NWK-DEST y NWK-SRC indican que el destino final del mensaje son todos los miembros de G (excepto posiblemente el propio ID1) y que el mensaje se envió por ID1. El campo NWK-INF indica además que se refiere a un mensaje en el contexto de direccionamiento indirecto (IA=1) y la aplicación en ID1 cifró la cadena m usando la clave de grupo K_G (lo que se indica por $E_{KG}(m)$) en CARGA ÚTIL DE APL. Un fondo gris oscuro en un mensaje significa que su contenido está protegido por un MIC usando K_G. Como solución alternativa, la aplicación en el dispositivo emisor ID1 puede decidir no cifrar m sino sólo añadir un MIC. En este caso, $E_{KG}(m)$ en el mensaje 401 será sustituido por m.

Al recibir el mensaje desde el dispositivo 301 emisor ID1, el dispositivo 302 encaminador ID2 observa que es un mensaje de IA inspeccionando el bit de IA en el campo NWK-INF y realizará una unidifusión múltiple a todos los miembros de G 303, 304, 305 (de nuevo, excepto posiblemente ID1). En una implementación alternativa, al recibir un mensaje desde un dispositivo emisor, el dispositivo encaminador, en lugar de comprobar el bit de IA en el campo NWK-INF, también puede comprobar el campo NWK-DEST para concluir que el dispositivo emisor envió un mensaje de IA.

A continuación, el dispositivo encaminador sustituye en el campo NWK-DEST el valor G por ID3, ID4 y ID5, respectivamente, ignorando en este caso la falta de concordancia resultante entre la información protegida por el MIC y el propio MIC. Se permite al encaminador realizar otras modificaciones a la información protegida siempre y cuando los dispositivos receptores puedan deshacer las modificaciones antes de verificar el MIC.

Como ejemplo, se describe el mensaje de unidifusión desde ID2 a ID4. A partir de su información de encaminamiento (por ejemplo, tablas de encaminamiento), ID2 sabe que una forma de llegar a ID4 es enviándolo a ID7 después de lo cual podrían seguir múltiples saltos, como se indica en la figura 3. El mensaje que ID2 envía a ID7 en el nivel MAC entonces se parecerá al mensaje 402 en la figura 4. En el campo NWK-DEST la entrada G se sustituye por ID4, debido a que los saltos intermedios no tienen constancia de una identidad de grupo G y los algoritmos de encaminamiento de unidifusión necesitan una dirección de dispositivo única, conocida como destino final. A causa de esta sustitución, el MIC y la información protegida ya no concuerdan lo que se indica por el fondo gris claro/rayado del campo NWK-DEST.

Después de posiblemente más saltos, un mensaje 313 termina finalmente en ID4. Si la penúltima dirección de salto era ID8 (véase la figura 3), el mensaje se parece al mensaje 403. Si ID4 conoce la identidad de todos los dispositivos en G puede recibir un mensaje de (indicado por ID1→{G} en la figura 3), entonces, inspeccionando el campo NWK-SRC en el mensaje recibido, ID4 puede obtener la identidad de grupo G. Antes de verificar el MIC en el mensaje usando la K_G, sustituirá ID4 en el campo NWK-DEST por G.

Aunque esta solución es muy eficaz en situaciones sencillas, habrá problemas en situaciones más complicadas. Podría ser, por ejemplo, que tanto ID1 como ID4 sean un miembro de G pero también de un grupo diferente G' en el que ID1 es también un dispositivo emisor. Tras la recepción de un mensaje, ID4 no está seguro de si debería sustituir ID4 en el campo NWK-DEST por G o por G' porque tendrá almacenado ID1 → {G, G'}. Claramente ID4 puede probar todas las identidades de grupo en la lista perteneciente a ID1 hasta que un MIC recalculado coincida con el MIC en el mensaje. Una solución alternativa es que ID copie la identidad de grupo G en la trama NWK, por ejemplo, en el campo NWK-INF. De esta manera los dispositivos receptores no tienen que almacenar el enlace entre identidades de dispositivo e identidades de grupo y todavía pueden sustituir la identidad de grupo en el campo NWK-DEST antes de verificar el MIC. El coste es que, en este caso, los mensajes que van a enviarse serán más largos.

Como solución alternativa a almacenar G en la trama NWK, el dispositivo receptor puede intentar sustituciones múltiples de la referencia de dirección de destino mediante los grupos de los que el dispositivo receptor y el dispositivo emisor son un miembro. De esta manera, el dispositivo receptor puede encontrar la identidad de grupo para la que el MIC coincide. Esto alivia la necesidad de añadir la identidad de grupo en el fragmento de comunicación, optimizando, por tanto, la longitud del fragmento de comunicación.

Las ventajas del procedimiento según la invención son tal como se resumen a continuación. El dispositivo emisor solamente requiere almacenar una cantidad muy limitada de información. Las actividades del dispositivo encaminador (ID2) y los saltos intermedios son independientes del hecho de si el mensaje por el dispositivo emisor (en este caso, ID1) es seguro o no. Solamente los miembros del grupo y (naturalmente) el dispositivo encaminador tienen constancia de un grupo G. Existe solamente un bit de sobrecarga en los mensajes (el bit de IA en el campo NWK-INF). Los dispositivos receptores tienen que almacenar los enlaces entre ID de dispositivo e ID de grupo, lo que puede realizarse eficazmente. No es necesario confiar en el dispositivo encaminador con datos de aplicación.

Es evidente para un experto en la técnica que modificaciones menores realizadas a las soluciones presentadas anteriormente aún constituyen las mismas soluciones.

Por ejemplo, para reducir adicionalmente el tamaño del mensaje desde el dispositivo emisor ID1 al dispositivo encaminador ID2, la identidad del encaminador (ID2) podría omitirse si queda clara a partir del contexto. Al recibir un mensaje desde ID1, el encaminador podría deducir a partir del contexto que debe retransmitir el mensaje al grupo G. Esto reduce aún más la cantidad requerida de almacenamiento en el dispositivo emisor y la longitud del mensaje que va a enviar el dispositivo emisor.

Como segundo ejemplo, para reducir adicionalmente el tamaño del mensaje desde el dispositivo emisor ID1 al dispositivo encaminador ID2, la identidad del dispositivo emisor ID1 puede omitirse de la definición de grupo en el dispositivo encaminador (en este caso G= {ID1,ID3,ID4,ID5}), si el dispositivo encaminador está actuando solamente como encaminador para un único dispositivo en G (en este caso ID1),

Son posibles alternativas. En la descripción anterior, "que comprende" y "comprendiendo" no excluyen otros elementos o etapas, "un" o "una" no excluyen una pluralidad, y un procesador único u otra unidad también puede llevar a cabo las funciones de varios medios mencionados en las reivindicaciones.

REIVINDICACIONES

1. Procedimiento de comunicación de un fragmento (211) de comunicación, comprendiendo el fragmento de comunicación una primera referencia de dirección de destino relativa a un grupo de al menos un dispositivo (203) receptor, comprendiendo las etapas de:

- añadir un dispositivo (201) emisor un código de integridad de mensaje cifrado para proteger al menos parte del fragmento de comunicación,

- transmitir el dispositivo emisor el fragmento de comunicación protegido a un dispositivo (202) encaminador,

- modificar el dispositivo encaminador, para al menos un dispositivo receptor en el grupo de dispositivos de destino, la primera referencia de dirección de destino para obtener una referencia de dirección del al menos un dispositivo receptor, mientras que se mantiene el código de integridad de mensaje cifrado sin cambios, y posteriormente retransmitir el fragmento (213) de comunicación protegido modificado al, al menos un, dispositivo receptor,

- recibir el al menos un dispositivo receptor el fragmento de comunicación protegido modificado,

- restaurar el al menos un dispositivo receptor el fragmento de comunicación protegido original para permitir una verificación del fragmento de comunicación protegido original usando el código de integridad de mensaje.

2. Procedimiento según la reivindicación 1, en el que el fragmento de comunicación comprende un campo de bit de IA para indicar si se usa el direccionamiento indirecto.

3. Procedimiento según la reivindicación 1, en el que el dispositivo emisor y el al menos un dispositivo receptor comparten una clave de cifrado común, y donde el código de integridad de mensaje cifrado sólo puede calcularse y verificarse usando la clave de cifrado común.

4. Procedimiento según la reivindicación 3, en el que la clave de cifrado común se usa para cifrar el contenido del mensaje.

5. Procedimiento según la reivindicación 1, en el que el al menos un dispositivo receptor restaura el fragmento de comunicación protegido original sustituyendo la primera referencia de dirección de destino por cada una de las identidades de grupo de grupos que comprenden el dispositivo emisor para determinar para cuál de las identidades de grupo el código de integridad de mensaje coincide.

6. Procedimiento según la reivindicación 1, en el que

- el dispositivo encaminador, en la etapa de modificar la primera referencia de dirección de destino, almacena la primera referencia de dirección de destino en el fragmento de comunicación protegido modificado, y

- el al menos un dispositivo receptor restaura el fragmento de comunicación protegido original usando la primera referencia de dirección de destino almacenada en el fragmento de comunicación protegido modificado para permitir la verificación del código de integridad de mensaje.

7. Dispositivo (202) encaminador que se dispone para encaminar un fragmento (211) de comunicación de un dispositivo emisor a un dispositivo receptor, comprendiendo el fragmento de comunicación una primera referencia de dirección de destino relativa a un grupo de al menos un dispositivo receptor, comprendiendo el dispositivo encaminador:

- medios (223) de recepción que se disponen para recibir el fragmento de comunicación, que comprenden una primera referencia de dirección relativa a un grupo de al menos un dispositivo receptor, estando el fragmento de comunicación al menos parcialmente protegido por un código de integridad de mensaje cifrado,

- medios (224) de modificación que se disponen para modificar el fragmento de comunicación, sustituyendo la primera referencia de dirección de destino por una referencia de dirección relativa al, al menos un, dispositivo receptor, mientras se mantiene el código de integridad de mensaje cifrado original, y

- medios (225) de transmisión para transmitir el fragmento (213) de comunicación modificado al, al menos un, dispositivo receptor.

8. Dispositivo (203) receptor que se dispone para recibir un fragmento (213) de comunicación modificado procedente de un dispositivo transmisor a través de un dispositivo encaminador, comprendiendo el fragmento de comunicación modificado un código de integridad de mensaje cifrado y una referencia de dirección del dispositivo receptor y que se deriva de un fragmento (211) de comunicación que comprende una primera referencia de dirección de destino relativa a un grupo de al menos un dispositivo receptor, comprendiendo el dispositivo receptor:

- medios (226) de recepción que se disponen para recibir el fragmento de comunicación modificado,

caracterizado porque el dispositivo receptor comprende además

- medios (227) de restauración que se disponen para restaurar el fragmento de comunicación original que se usaba para calcular el código de integridad de mensaje cifrado modificando la referencia de dirección del dispositivo receptor para obtener la primera referencia de dirección de destino, y

- medios (228) de verificación que se disponen para verificar el código de integridad de mensaje cifrado.

9. Sistema (200) para comunicación que comprende un dispositivo (201) emisor, un dispositivo (202) encaminador, y un dispositivo (203) receptor según las reivindicaciones 7 y 8.

10. Señal para un direccionamiento indirecto seguro, que comprende un fragmento (213) de comunicación procedente de un dispositivo transmisor a través de un dispositivo encaminador, comprendiendo el fragmento de comunicación un código de integridad de mensaje cifrado y una referencia de dirección de un dispositivo receptor, en el que el código de integridad de mensaje cifrado está protegiendo un fragmento de comunicación protegido original que comprende una primera referencia de dirección de destino relativa a un grupo de al menos un dispositivo (203) receptor para permitir al dispositivo receptor restaurar el fragmento de comunicación protegido original modificando la referencia de dirección del dispositivo receptor para obtener la primera referencia de dirección de destino para permitir la verificación del fragmento de comunicación protegido original usando el código de integridad de mensaje.

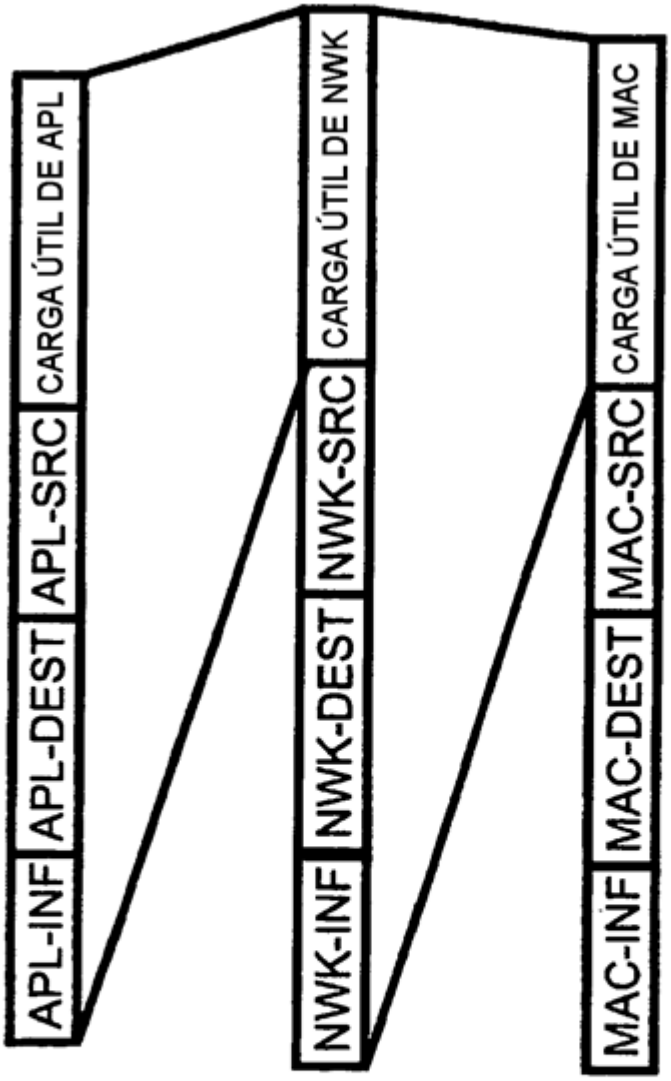
APL-INF
APL-DEST
APL-SRC
CARGA ÚTIL DE APL
NWK-INF
NWK-DEST
NWK-SRC
CARGA ÚTIL DE NWK
MAC-INF
MAC-DEST
MAC-SRC
CARGA ÚTIL DE MAC
100

FIG.1

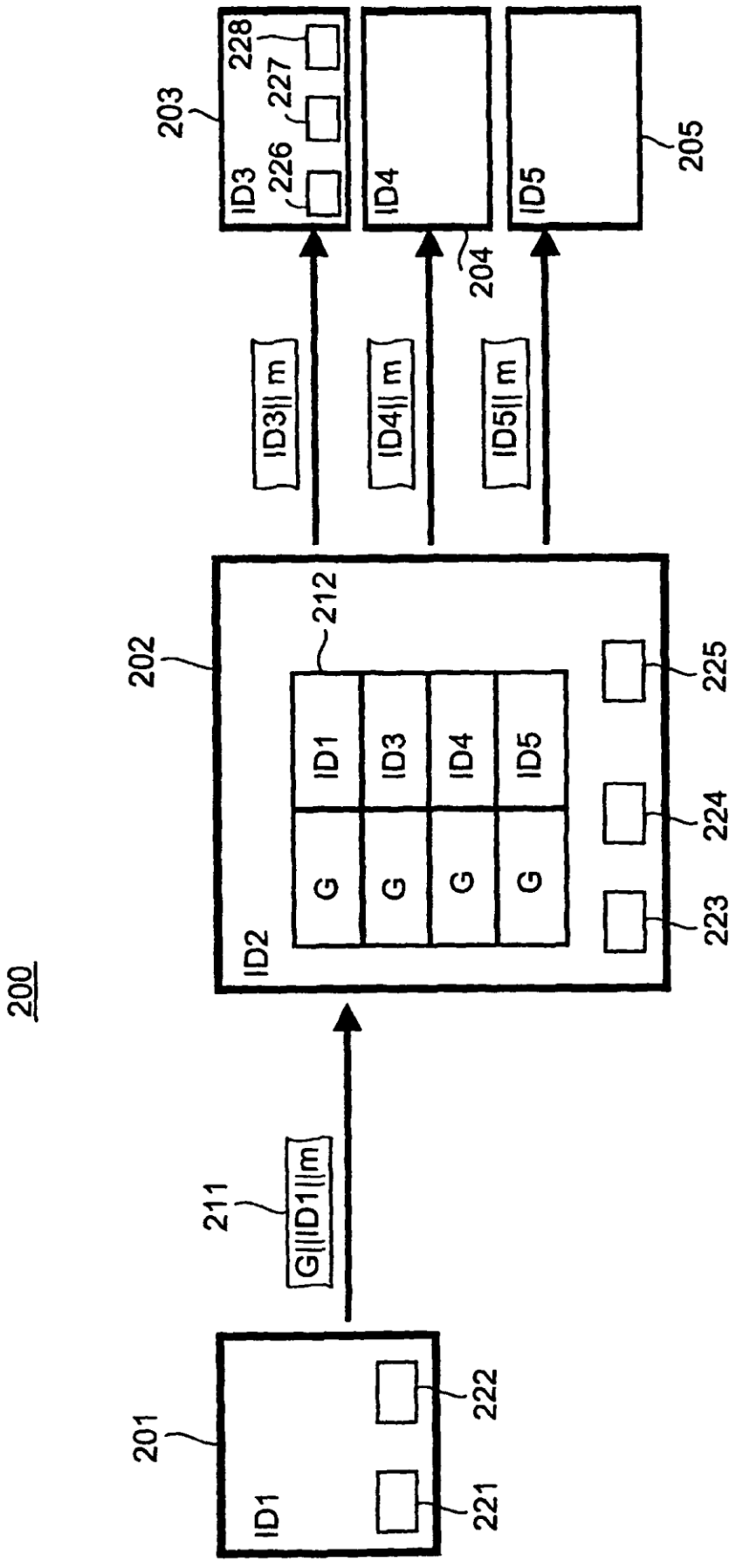
200
201
ID1
221
222
211
G||ID1||m
202
ID2
212
G
ID1
G
ID3
G
ID4
G
ID5
223
224
225
ID3||m
ID4||m
ID5||m
203
ID3
226
227
228
204
ID4
ID5
205

FIG.2

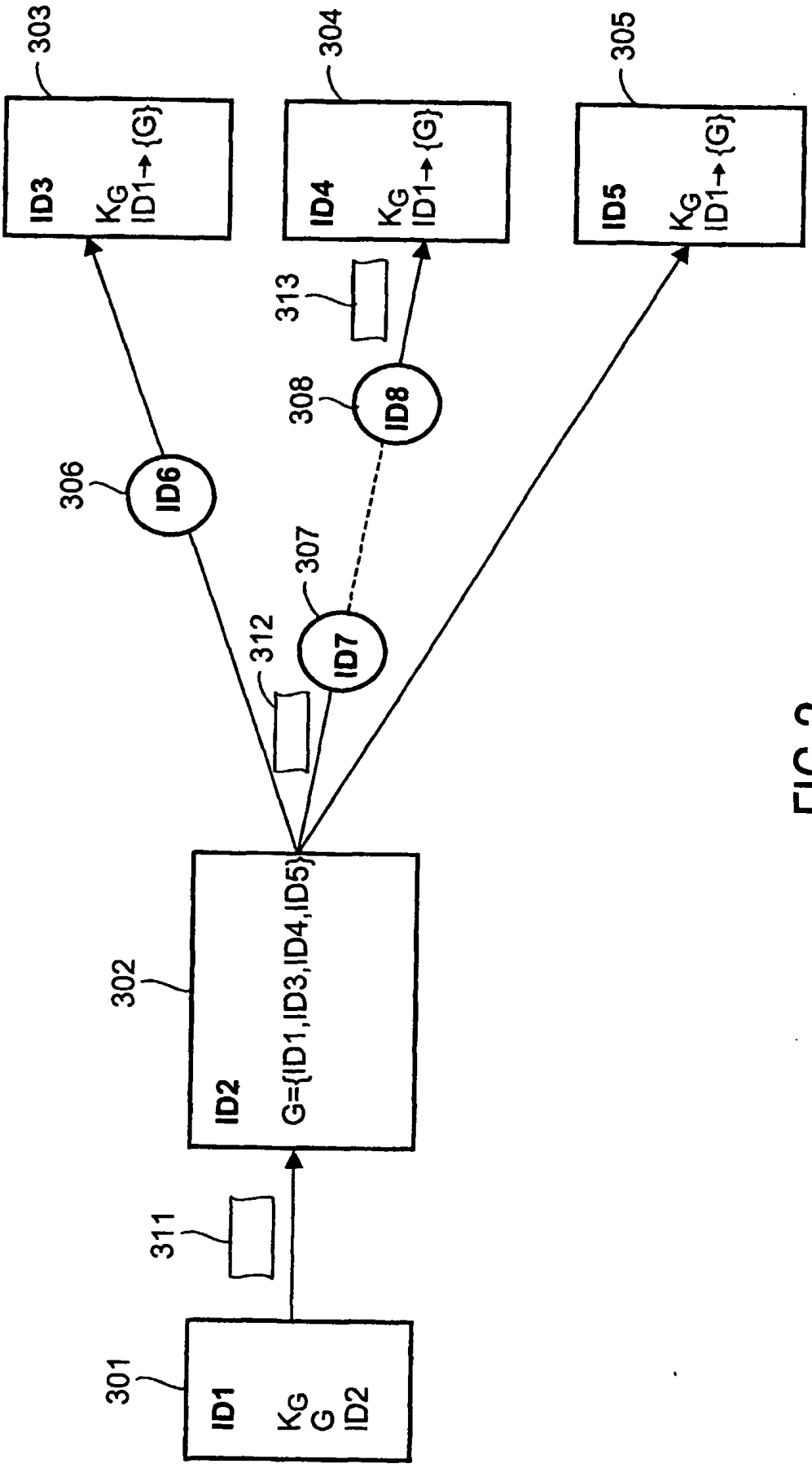
303
304
305
ID3
K_G
ID1→{G}
ID4
K_G
ID1→{G}
ID5
K_G
ID1→{G}
313
308
ID8
306
ID6
307
ID7
312
302
ID2
G={ID1,ID3,ID4,ID5}
311
301
ID1
K_G
G
ID2

FIG.3

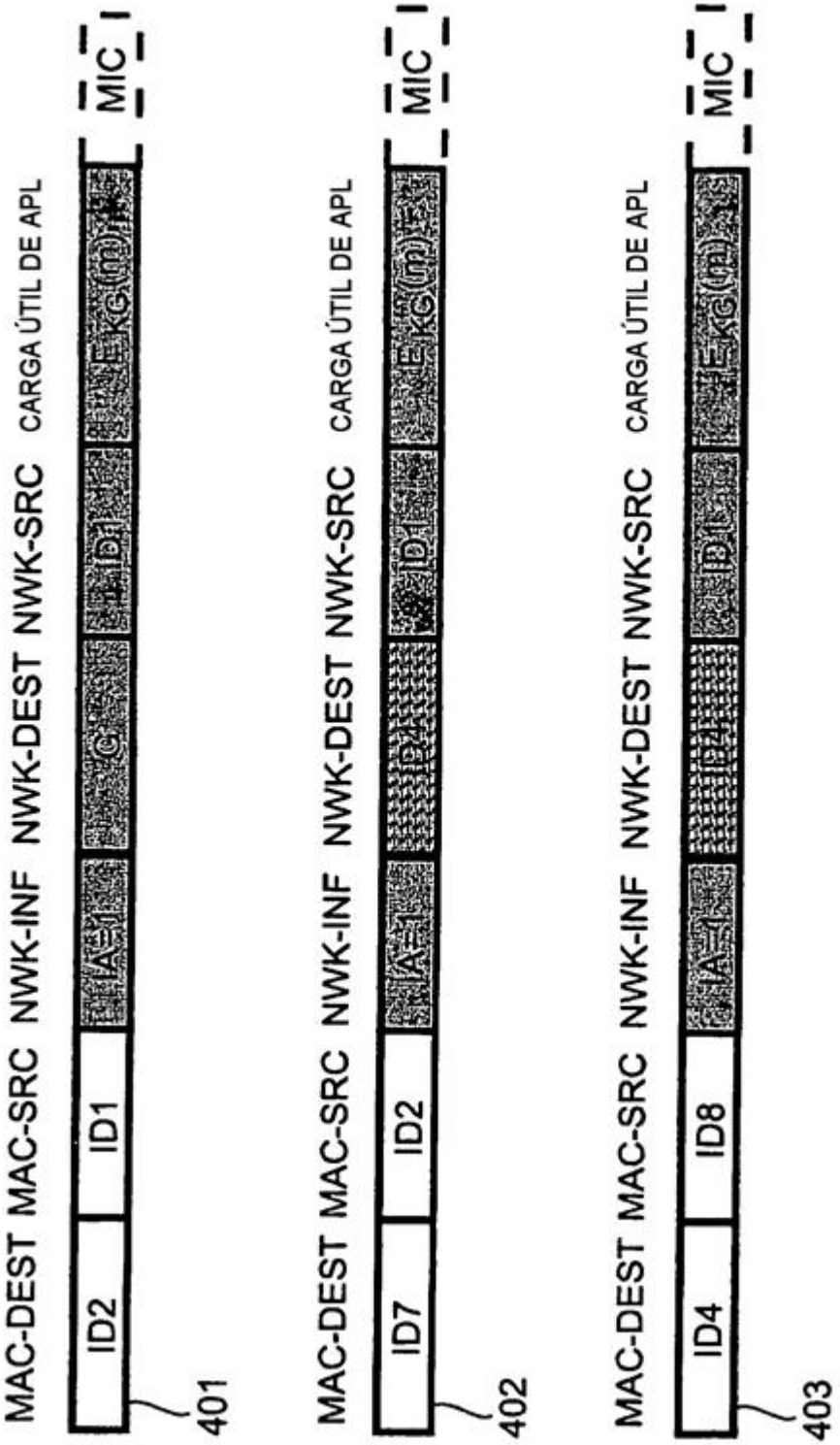
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
CARGA ÚTIL DE APL
ID2
ID1
MIC
401
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
CARGA ÚTIL DE APL
ID7
ID2
MIC
402
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
CARGA ÚTIL DE APL
ID4
ID8
MIC
403

FIG.4