(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 945 060**

(51) Int. CI.:

H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.11.2018 PCT/FR2018/052984**

(87) Fecha y número de publicación internacional: **06.06.2019 WO19106273**

(96) Fecha de presentación y número de la solicitud europea: **27.11.2018 E 18825753 (9)**

(97) Fecha y número de publicación de la concesión europea: **22.02.2023 EP 3718280**

(54) Título: **Técnica de procesamiento de mensajes enviados por un dispositivo comunicante**

(30) Prioridad:

01.12.2017 FR 1761549

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.06.2023

(73) Titular/es:

ORANGE (100.0%)
111, quai du Président Roosevelt
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

LAVEDRINE, RÉMI

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Técnica de procesamiento de mensajes enviados por un dispositivo comunicante

La invención se relaciona con el campo general de las telecomunicaciones.

La invención se refiere más particularmente a una técnica de procesamiento de mensajes enviados por un dispositivo comunicante. Más precisamente, estos mensajes son enviados por medio de una puerta de enlace de acceso con destino a un dispositivo receptor.

La técnica de procesamiento se ubica en el campo de los dispositivos comunicantes u objetos conectados.

Por dispositivo comunicante u objeto conectado, se entiende un dispositivo capaz de intercambiar informaciones con otros dispositivos. En estos dispositivos, se distinguen aquellos que intercambian informaciones por medio de una red de comunicación administrada por un operador de red, con, según los casos, otro dispositivo, un terminal de comunicación o incluso un equipo informático de la red de comunicación. La red de comunicación puede basarse en tecnologías de redes móviles celulares denominadas 2G, 3G, 4G, 5G, así como las tecnologías de redes de baja potencia y largo alcance LPWA (para «*Low Power Wide Area*») tales como la red LoRa.

Desde el punto de vista del usuario, la comunicación por medio de redes denominadas de largo alcance se diferencia de la comunicación por medio de redes denominadas de bajo alcance (tales como Bluetooth, Bluetooth Low Energy, WiFi, Zigbee, ZWave, etc.) por las siguientes ventajas:

- independencia frente a un equipo intermedio para acceder a una red de comunicación extendida;

- seguridad: la mayoría de las tecnologías de largo alcance integran intrínsecamente características de seguridad, tales como una autenticación, un cifrado, las cuales ofrecen una garantía de seguridad nativa para las aplicaciones implementadas en esta red;

- facilidad de configuración y de utilización: no hay necesidad de configurar una clave de seguridad o de realizar un emparejamiento, operaciones que pueden resultar extremadamente complejas para el usuario cuando el dispositivo no integra una pantalla o dispone de periféricos de entrada/salida limitados, o bien para usuarios que no están habituados a utilizar este tipo de tecnologías.

Se constata que estos dispositivos comunicantes son hasta ahora poco seguros y se están convirtiendo en el objetivo de ataques. Es posible que algunos dispositivos comunicantes presenten uno o más fallos de seguridad, susceptibles de permitir que un individuo malintencionado tome el control a distancia, por ejemplo, mediante la instalación en el dispositivo comunicante de un software malicioso, (en inglés «*malware*»), con el fin de operar actividades malintencionadas, tales como el robo de datos, o un ataque de denegación de servicio, por ejemplo (DDoS para «*Distributed Denial of Service attack*» en inglés). Tales ataques de denegación de servicio se dirigen a dispositivos receptores a los cuales los dispositivos comunicantes envían datos.

Las publicaciones de patente US2010/153394 A1 y US2008/0177843 A1 se ubican en el campo del filtrado de correos electrónicos no deseados.

Uno de los objetivos de la técnica propuesta es remediar las deficiencias/desventajas del estado de la técnica y/o ofrecer mejoras en el mismo.

Según un primer aspecto, se propone un procedimiento de procesamiento de mensajes enviados por un dispositivo comunicante. El procedimiento comprende:

- una verificación mediante un dispositivo de seguridad de que un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor es un mensaje por transmitir, siendo el mensaje transmitido al dispositivo receptor cuando la verificación es positiva;

- una recepción mediante el dispositivo de seguridad de una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado,

los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante e identificador de producto que los del dispositivo comunicante que ha emitido el dicho mensaje están bloqueados por el dispositivo de seguridad durante la dicha verificación.

Por tanto, esto permite proteger los dispositivos receptores frente a dispositivos comunicantes susceptibles de presentar un fallo de seguridad. En efecto, se está volviendo común que terceros malintencionados tomen el control de dispositivos comunicantes debido a su bajo nivel de seguridad. Por tanto, la implementación de este procedimiento permite aumentar la seguridad general controlando rápidamente los comportamientos malintencionados de los dispositivos comunicantes. Una detección de un comportamiento malintencionado por el dispositivo receptor permite implementar directamente un bloqueo mediante el dispositivo de seguridad de mensajes posteriores transmitidos por

otros dispositivos comunicantes. Por tanto, el dispositivo de seguridad implementa para los dispositivos comunicantes de los cuales es encargado las medidas necesarias para la protección del dispositivo receptor.

El dispositivo receptor se ubica en las partes de la red, denominadas en segundo plano («*back-end*» en inglés). Por tanto, está previsto para recibir datos procedentes de dispositivos comunicantes que se ubican en las partes de la red, denominados frontal («*front-end*» en inglés). El dispositivo receptor puede, por ejemplo, proporcionar un servicio a partir de los datos recibidos. El dispositivo de seguridad también está posicionado en la parte frontal y permite proteger la parte de segundo plano de la red.

El procedimiento de procesamiento es particularmente muy adecuado para ser implementado para los dispositivos comunicantes, los cuales disponen en general de poca potencia de procesador, pero los cuales comprenden interfaces con la red de comunicación extendida, la red de Internet. Debido a estas interfaces las cuales permiten tomar el control a distancia, estos dispositivos comunicantes se convierten en el objetivo de ataques.

El dispositivo de seguridad puede estar coubicado con una puerta de enlace de acceso a la red de comunicación. Esta puerta de enlace de acceso permite a los dispositivos comunicantes acceder a la red de comunicación y, por lo tanto, transmitir datos al dispositivo receptor, el cual se ubica en la parte de segundo plano de la red.

En un modo de realización particular, la puerta de enlace de acceso implementa las funciones del dispositivo de seguridad.

Por tanto, el procedimiento de procesamiento aprovecha la detección de un comportamiento malintencionado de un dispositivo comunicante por el dispositivo receptor para neutralizar las posibles transmisiones de otros dispositivos comunicantes de un mensaje del mismo tipo. Estos otros dispositivos comunicantes son dispositivos con el mismo identificador de producto y, por lo tanto, proporcionados por el mismo fabricante.

No se requiere ninguna modificación en los dispositivos comunicantes, siendo el procedimiento de procesamiento implementado en la red, esencialmente en la parte frontal de la red.

Los diferentes modos o características de realización mencionados más adelante pueden agregarse de manera independiente o en combinación entre sí, al procedimiento de procesamiento, tal como se definió anteriormente.

En un modo de realización particular, el procedimiento de procesamiento comprende además una neutralización del dispositivo comunicante, para el cual se ha recibido la notificación.

Por tanto, el dispositivo comunicante que ha emitido el mensaje se encuentra neutralizado. Aunque controlado a distancia por un tercero malintencionado, el dispositivo comunicante no puede afectar más al dispositivo receptor. Se puede tratar de diferentes niveles de neutralización. En un modo de realización particular, los accesos a la red de comunicación del dispositivo comunicante están desactivados: no se pueden enviar más mensajes al dispositivo receptor. En otro modo de realización, el dispositivo comunicante está fuera de uso, por ejemplo, bloqueando el inicio de su sistema operativo.

En un modo de realización particular del procedimiento de procesamiento, los mensajes posteriores del mismo tipo que el mensaje para el que se recibió la notificación, emitidos por los dispositivos comunicantes proporcionados por el mismo fabricante y con un identificador de producto diferente al del dispositivo comunicante que ha emitido el dicho mensaje son bloqueados por el dispositivo de seguridad durante la dicha verificación.

Por tanto, la toma de control a distancia por un tercero malintencionado de dispositivos comunicantes del mismo fabricante es rápidamente contenida, los mensajes emitidos por estos dispositivos se encuentran directamente bloqueados por el dispositivo de seguridad, antes de llegar al dispositivo receptor.

En un modo de realización particular, el procedimiento de procesamiento comprende la obtención por el dispositivo de seguridad de al menos un mensaje por transmitir.

Por tanto, es posible configurar el dispositivo de seguridad con un conjunto de mensajes autorizados para un identificador de producto determinado. También es posible una vez finalizado el ataque autorizar de nuevo la transmisión del mensaje, el cual había sido indicado como bloqueado.

Según un segundo aspecto, se propone un dispositivo de seguridad destinado para procesar un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor, comprendiendo el dicho dispositivo de seguridad un módulo de procesamiento dispuesto para:

- verificar que el dicho mensaje es un mensaje por transmitir;

- transmitir el dicho mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;

- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de mensajes posteriores del mismo tipo que el mensaje para el cual se

recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante e identificador de producto que los del dispositivo comunicante que ha emitido el dicho mensaje.

Las ventajas indicadas para el procedimiento de procesamiento según el primer aspecto se transponen directamente al dispositivo de seguridad.

En un modo de realización particular del dispositivo de seguridad, el módulo de procesamiento está dispuesto además para bloquear los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por los dispositivos comunicantes proporcionados por el mismo fabricante e identificador de producto diferente a los del dispositivo comunicante que ha emitido el dicho mensaje.

Según un tercer aspecto, se propone un sistema de seguridad que comprende:

- un dispositivo de seguridad destinado para procesar un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor, comprendiendo el dicho dispositivo de seguridad un módulo de procesamiento dispuesto para:

- verificar que el dicho mensaje es un mensaje por transmitir;

- transmitir el dicho mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;

- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo identificador de fabricante e identificador de producto que los del dispositivo comunicante que ha emitido el dicho mensaje;

- un dispositivo receptor, dispuesto para recibir el dicho mensaje enviado por el dispositivo comunicante y transmitido por el dispositivo de seguridad y para enviar la dicha notificación al dispositivo de seguridad.

Las ventajas indicadas para el procedimiento de procesamiento según el primer aspecto se transponen directamente al sistema de seguridad.

Según un cuarto aspecto, se propone un programa para un dispositivo de seguridad, que comprende instrucciones de código de programa destinadas para controlar la ejecución de aquellas de las acciones del procedimiento de procesamiento anteriormente descrito implementadas por el dispositivo de seguridad, cuando ese programa es ejecutado por ese dispositivo y un soporte de registro legible por un dispositivo en el cual se registra un programa para un dispositivo.

Las ventajas indicadas para el procedimiento de procesamiento según el primer aspecto se transponen directamente al programa para un dispositivo de seguridad y al soporte de registro.

La técnica de procesamiento de mensajes enviados por un dispositivo comunicante se comprenderá mejor con la ayuda de la siguiente descripción de modos de realización particulares, con referencia a los dibujos adjuntos en los cuales:

- la Figura 1 representa los dispositivos comunicantes en su entorno en un modo de realización particular;

- la Figura 2 ilustra las etapas de un procedimiento de procesamiento según un modo particular de realización;

- La Figura 3 representa un dispositivo de seguridad en un modo de realización particular.

La figura 1 representa un entorno en el cual se implementa el procedimiento de procesamiento en un modo de realización particular. El entorno representado comprende los dispositivos 11, 21, 31, 12, 22 comunicantes que acceden a una red 1 de comunicación por medio de una puerta 40 de enlace de acceso. Un dispositivo u objeto comunicante o conectado, es un objeto adecuado para intercambiar informaciones por medio de una red de comunicación, con, según el caso, otro objeto, un terminal de comunicación o incluso un equipo 60 informático de la red de comunicación. Por tanto, en la continuación, se designa por dispositivo comunicante, tanto los objetos físicos conectados a la red como las aplicaciones de software «virtualizadas» asociadas con algunos de estos objetos. Tales dispositivos comunicantes pueden ser designados por el acrónimo IoT, para el inglés «*Internet of Things*», en francés «Internet de las cosas».

El dispositivo 11, 21, 31, 12, 22 comunicante puede ser cualquier tipo de terminal que permita transmitir datos, tal como un teléfono móvil, un teléfono inteligente («*smartphone*» en inglés), una tableta, un objeto conectado.

Por tanto, un dispositivo comunicante u objeto conectado puede corresponder a un terminal móvil, un reloj adaptado para transmitir informaciones a un terminal móvil a través de una red de comunicación extendida, tal como la red de Internet, un detector de humo adaptado para comunicarse con un terminal móvil remoto con el fin de señalar la presencia de humo en una casa, una caja de control médico, una caja de geolocalización. En la figura 1, se representan

los termostatos 11, 21, 31 y los detectores 12, 22 de movimiento. Se recuerda, en este caso, que se trata de un ejemplo de entorno y que no se adjunta ninguna limitación al tipo de estos dispositivos comunicantes, ni a su número.

Estos dispositivos comunicantes son adecuados para transmitir datos a un dispositivo informático remoto, denominado en la continuación dispositivo receptor, por medio de una red 1 de comunicación. Estos datos se transmiten en mensajes.

Estos mensajes se envían por medio de la puerta 40 de enlace de acceso. Esta puerta de enlace de acceso depende de la red de acceso. La red de acceso corresponde por ejemplo a una red de comunicación móvil de tipo GSM, EDGE, 3G, 3G+ o 4G (también denominada LTE para «*Long Term Evolution*»). La red de acceso también puede corresponder a una red inalámbrica de tipo WiFi según la norma IEEE 802.11. La red de acceso también puede corresponder a una red de baja potencia y largo alcance LPWA (para «*Low Power Wide Area*») tal como la red LoRa.

En el modo de realización representado, el dispositivo 11, 21, 31, 12, 22 comunicante envía datos a un servidor 60 como dispositivo receptor. Este servidor 60 está dispuesto para proporcionar un servicio a partir de datos recibidos. Este servicio puede corresponder, por ejemplo, a un servicio de salud, un servicio de asistencia personal, un servicio de localización. No se adjunta ninguna limitación al número de dispositivos receptores.

El dispositivo comunicante se identifica por un identificador único. Este identificador corresponde por ejemplo a un identificador único de tipo IEEE EUI-48 (para «*Extended Unique Identifier*»). Este identificador único es un número codificado en 48 bits que permite identificar especialmente el fabricante, el producto y el número de serie.

Para una red de tipo de largo alcance y baja potencia, por ejemplo, LoRA, este identificador único puede corresponder, por ejemplo, al identificador único del dispositivo DevEUI.

Para una red de comunicación móvil, este identificador único es un identificador memorizado en un elemento de seguridad (o «Elemento Seguro») del dispositivo comunicante durante la fase de configuración de este último.

En la figura 1 también se representa un dispositivo 50 de seguridad. En el modo de realización particular que se describe, este último recibe todos los mensajes enviados con destino a un dispositivo receptor mediante los dispositivos comunicantes que acceden a la red de comunicación por medio de la puerta 40 de enlace de acceso. Está ubicado en el corte de los mensajes enviados por los dispositivos comunicantes antes de la transmisión de los mensajes verificados hacia el dispositivo receptor. El dispositivo 50 de seguridad está dispuesto para verificar que un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor es un mensaje por transmitir. Un mensaje por transmitir es un mensaje denominado autorizado. Un mensaje que no debe transmitirse es bloqueado por el dispositivo de seguridad y es un mensaje denominado no autorizado. Esta verificación se detalla posteriormente. En particular, en el entorno representado en la figura 1, el dispositivo de seguridad transmite al servidor 60 los mensajes que le están destinados. Por tanto, el dispositivo de seguridad transmite los mensajes en función del dispositivo receptor al cual están destinados. El dispositivo de seguridad ubicado en la parte frontal de la red protege entonces una pluralidad de dispositivos receptores.

En este modo de realización particular, el dispositivo de seguridad está asociado a una puerta de enlace de acceso. El dispositivo de seguridad y la puerta de enlace de acceso pueden coubicarse. El dispositivo de seguridad también se puede integrar en la puerta 40 de enlace de acceso.

En la figura 1, se representa un único dispositivo de seguridad. No se adjunta ninguna limitación a esta representación.

La figura 3 ilustra de manera esquemática un dispositivo 50 de seguridad en un modo de realización particular.

El dispositivo 50 de seguridad, tal como se representa en la figura 3, comprende especialmente:

- un procesador 51 para ejecutar instrucciones de código de módulos de software;

- una zona 52 de memoria, dispuesta para memorizar un programa que comprende instrucciones de código para implementar las etapas del procedimiento de procesamiento;

- una memoria 53 de almacenamiento, dispuesta para almacenar datos utilizados durante la implementación del procedimiento de procesamiento;

- un módulo 54 de comunicación, que forma una interfaz de comunicación con una red de comunicación, dispuesto para comunicarse con dispositivos de una red de comunicación;

- un módulo 55 de procesamiento, dispuesto para verificar que un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor es un mensaje por transmitir, siendo el mensaje transmitido al dispositivo receptor cuando la verificación es positiva;

- una memoria 56 de almacenamiento, dispuesta para memorizar los mensajes que deben ser bloqueados.

El módulo 54 de comunicación corresponde a un módulo de emisión/recepción el cual depende de la tecnología de acceso por radio.

El procedimiento de procesamiento implementado por el dispositivo 50 de seguridad se describirá ahora en relación con la figura 2.

En la continuación, se ubica en el nivel del dispositivo 11 comunicante.

El dispositivo 11 comunicante envía un mensaje M1-MSG1 con destino al servidor 60, como dispositivo receptor, por medio de la puerta 40 de enlace de acceso. Este último transmite el mensaje recibido al dispositivo 50 de seguridad.

El dispositivo 50 de seguridad verifica (E1) que el mensaje MSG1 enviado por el dispositivo 11 comunicante con destino a un dispositivo 60 receptor es un mensaje por transmitir para este tipo de dispositivo comunicante. Para esto, el dispositivo 50 de seguridad compara el mensaje MSG1 con los mensajes memorizados en la memoria 56 de almacenamiento.

Cuando la verificación es positiva, el mensaje MSG1 se transmite hacia su destino, el dispositivo 60 receptor.

El dispositivo 60 receptor verifica (F1) si el mensaje MSG1 es un mensaje emitido por un dispositivo comunicante malintencionado. Esta detección puede basarse en análisis efectuados en una secuencia de mensajes recibidos desde un dispositivo comunicante, las correlaciones entre los mensajes recibidos de diferentes dispositivos comunicantes, análisis temporales en una secuencia de mensajes. No se adjunta ninguna limitación a la forma en que el dispositivo 60 receptor detecta que el mensaje MSG1 es un mensaje que debe ser bloqueado o no. A título ilustrativo, el mensaje MSG1 es un mensaje «seguro». El dispositivo 60 receptor procesa entonces este mensaje MSG1.

En la continuación, el dispositivo 11 comunicante envía un mensaje M2-MSG2 con destino al servidor 60 por medio de la puerta 40 de enlace de acceso. Este último transmite el mensaje recibido al dispositivo 50 de seguridad.

El dispositivo 50 de seguridad verifica (E1) que el mensaje MSG2 enviado por el dispositivo 11 comunicante con destino a un dispositivo 60 receptor es un mensaje por transmitir. Para esto, el dispositivo 50 de seguridad compara el mensaje MSG2 con los mensajes memorizados en la memoria 56 de almacenamiento. El mensaje MSG2 no es considerado como un mensaje que debe ser bloqueado para este tipo de dispositivo comunicante. Siendo la verificación positiva, el mensaje MSG2 es transmitido (mensaje O2-MSG2) hacia su destino, el dispositivo 60 receptor.

El dispositivo 60 receptor detecta (F1) que el mensaje MSG2 es un mensaje emitido por un dispositivo comunicante malintencionado. Este dispositivo se ha vuelto malintencionado, por ejemplo, debido a una toma de control a distancia de un tercero malintencionado.

El dispositivo 60 receptor envía entonces al dispositivo 50 de seguridad una notificación O3-NOK(MSG2) que indica que el mensaje transmitido debe ser bloqueado para este tipo de dispositivo comunicante.

Esta notificación es recibida (E2) por el dispositivo 50 de seguridad y el mensaje MSG2 se memoriza en la memoria 56 de almacenamiento. Esta notificación indica al dispositivo 50 de seguridad que los mensajes posteriores del mismo tipo que el mensaje MSG2 para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante y con el mismo identificador de producto que los del dispositivo 11 comunicante que ha emitido este mensaje deben ser bloqueados por el dispositivo 50 de seguridad durante la verificación (E1).

En un modo de realización particular, ilustrado en la figura 2, el dispositivo 50 de seguridad envía un mensaje M3-Revoke de neutralización del dispositivo 11 comunicante, para el cual se ha recibido la notificación O3-NOK(MSG2).

Se puede tratar de diferentes niveles de neutralización. En un modo de realización particular, los accesos a la red de comunicación del dispositivo 11 comunicante están desactivados: no puede enviar más mensajes a los dispositivos receptores. En otro modo de realización, el dispositivo comunicante queda fuera de uso, por ejemplo, bloqueando el inicio de su sistema operativo. El dispositivo 11 comunicante ya no puede enviar ningún dato y ya no representa un riesgo para los otros dispositivos y la red de comunicación. El dispositivo 60 receptor no procesa más los mensajes procedentes de este dispositivo 11 comunicante revocado.

De regreso a la figura 2, ahora se ubica en el nivel del dispositivo 21 comunicante, el cual es un producto proporcionado por el mismo fabricante y del mismo tipo que el dispositivo 11 comunicante.

El dispositivo 21 comunicante envía un mensaje M4-MSG2 con destino al servidor 60 por medio de la puerta 40 de enlace de acceso. A título ilustrativo, este mensaje M4 transita por esta puerta 40 de enlace de acceso. Queda entendido que, en otros ejemplos, el mensaje M4 podría transitar por medio de otra puerta de enlace de acceso, asociada al mismo dispositivo 50 de seguridad. La puerta 40 de enlace de acceso transmite el mensaje recibido al dispositivo 50 de seguridad.

El dispositivo 50 de seguridad verifica (E1) que el mensaje MSG2 enviado por el dispositivo 21 comunicante con destino a un dispositivo 60 receptor es un mensaje por transmitir. Para esto, el dispositivo 50 de seguridad compara el mensaje MSG2 con los mensajes memorizados en la memoria 56 de almacenamiento. El mensaje MSG2 es emitido

por un dispositivo comunicante proporcionado por el mismo fabricante y con el mismo identificador de producto que los del dispositivo 11 comunicante en el origen de la notificación O3-NOK(MSG2). Por lo tanto, es bloqueado por el dispositivo 50 de seguridad y no se transmite con destino al dispositivo 60 receptor. Por tanto, este último está protegido contra los ataques que resultan de la toma del control de dispositivos comunicantes proporcionados por el mismo fabricante y correspondientes a un producto determinado.

En un modo de realización particular, el dispositivo 50 de seguridad envía un mensaje M5-Revoke de neutralización del dispositivo 21 comunicante. Como se describió anteriormente para la neutralización del dispositivo 11 comunicante, se puede tratar de diferentes niveles de neutralización. El dispositivo 21 comunicante ya no puede enviar ningún dato y ya no representa un riesgo para los otros dispositivos y la red de comunicación.

En este modo de realización, un mensaje MSG2 emitido por un dispositivo comunicante proporcionado por el mismo fabricante, pero con un identificador de producto diferente no se bloquea y se transmite al dispositivo 60 receptor. En este caso, se señala que un mensaje MSG2 emitido por un dispositivo comunicante proporcionado por un fabricante diferente tampoco está bloqueado y se transmite al dispositivo 60 receptor.

En otro modo de realización, los mensajes posteriores del mismo tipo que el mensaje MSG2 para el que se recibió la notificación O3-NOK(MSG2), emitidos por los dispositivos comunicantes proporcionados por el mismo fabricante, pero con un identificador de producto diferente al del dispositivo comunicante que ha emitido este mensaje son bloqueados por el dispositivo 50 de seguridad durante la verificación (E1).

A título ilustrativo, se ubica en el nivel del dispositivo 12 comunicante, proporcionado por el mismo fabricante que el dispositivo 11 comunicante (termostato). Sin embargo, este dispositivo 12 comunicante (detector de movimiento) es un producto de otro tipo.

El dispositivo 12 comunicante envía un mensaje MSG2 con destino al servidor 60 por medio de la puerta 40 de enlace de acceso. A título ilustrativo, este mensaje MSG2 transita por esta puerta 40 de enlace de acceso. Se entiende que, en otros ejemplos, el mensaje MSG2 podría transitar por medio de otra puerta de enlace de acceso, asociada al mismo dispositivo 50 de seguridad. La puerta 40 de enlace de acceso transmite el mensaje recibido al dispositivo de seguridad.

El dispositivo 50 de seguridad verifica (E1) que el mensaje MSG2 enviado por el dispositivo 12 comunicante con destino a un dispositivo 60 receptor es un mensaje por transmitir. Para esto, el dispositivo 50 de seguridad compara el mensaje MSG2 con los mensajes memorizados en la memoria 56 de almacenamiento. El mensaje MSG2 es emitido por un dispositivo comunicante proporcionado por el mismo fabricante, pero con un identificador de producto diferente al del dispositivo 11 comunicante en el origen de la notificación O3-NOK (MSG2). Por lo tanto, es bloqueado por el dispositivo 50 de seguridad y no se transmite con destino al dispositivo 60 receptor. Por tanto, este último está protegido contra los ataques que resultan de la toma de control de dispositivos comunicantes proporcionados por el mismo fabricante, aunque correspondientes a un producto diferente.

En un modo de realización particular, el dispositivo 50 de seguridad envía un mensaje de neutralización del dispositivo comunicante 12. Tal como se ha descrito anteriormente para la neutralización del dispositivo 11 comunicante, se puede tratar de diferentes niveles de neutralización. El dispositivo 12 comunicante ya no puede enviar ningún dato y ya no representa un riesgo para los otros dispositivos y la red de comunicación.

En los modos de realización descritos anteriormente, la memoria 56 de almacenamiento memoriza los mensajes, tales como el mensaje MSG2, para los cuales se ha recibido una notificación (E2) por el dispositivo 50 de seguridad. Estos mensajes son mensajes que deben ser bloqueados por el dispositivo 50 de seguridad. En el estado inicial, se dice que todos los mensajes se transmiten. La memoria 56 de almacenamiento se enriquece de manera gradual en función de los mensajes para los cuales se recibe una notificación.

En un modo de realización particular, la memoria 56 de almacenamiento también memoriza los mensajes por transmitir. Se supone que estos mensajes son «seguros» o autorizados. Por tanto, es posible memorizar un conjunto de mensajes susceptibles de ser emitidos por dispositivos comunicantes proporcionados por un mismo fabricante y con el mismo identificador de producto. Este conjunto de mensajes se obtiene, por ejemplo, del fabricante. El dispositivo 50 de seguridad y su memoria 56 de almacenamiento se configuran con este conjunto de mensajes. En un modo de realización particular, el conjunto de mensajes, tal como el configurado por el fabricante es recibido por medio de una interfaz de comunicación. En este modo de realización particular donde la memoria 56 de almacenamiento memoriza los mensajes por transmitir, el mensaje MSG2 es eliminado del conjunto de mensajes «seguros» para este tipo de dispositivo comunicante en la recepción de la notificación O3-NOK(MSG2), con el fin de ser bloqueado por el dispositivo 50 de seguridad. Por tanto, la verificación (E1) comprende una comparación del mensaje MSG1, MSG2 recibido con el fin de verificar si pertenece al conjunto de mensajes por transmitir.

Del mismo modo que el dispositivo receptor ha solicitado un bloqueo del mensaje MSG2 por medio de la notificación O3-NOK(MSG2), el dispositivo 60 receptor puede solicitar al dispositivo 50 de seguridad que el mensaje MSG2 sea de nuevo considerado como un mensaje por transmitir. Por tanto, el dispositivo 50 de seguridad obtiene al menos un mensaje por transmitir. Esto permite regresar a un funcionamiento normal, una vez se resuelve el fallo de seguridad que afecta los dispositivos comunicantes.

En un modo de realización particular, el dispositivo 60 receptor también puede solicitar el bloqueo del mensaje MSG2 para este tipo de dispositivo comunicante a otros dispositivos de seguridad.

Se comprende que esta técnica de procesamiento permite mejorar la seguridad de una red de comunicación, protegiendo los dispositivos receptores ubicados en segundo plano de dispositivos comunicantes que serían el objeto de un ataque malintencionado. Tales dispositivos se encuentran aislados y no pueden continuar sus ataques. Además, esta neutralización también puede extenderse a los otros dispositivos del mismo tipo, o incluso a los dispositivos del mismo fabricante.

No se adjunta ninguna limitación a estos diferentes modos de realización y el experto en la técnica es capaz de definir otros que neutralicen en las partes frontales de la red de comunicación, los dispositivos comunicantes en los cuales un tercero malintencionado ha tomado el control con el fin de proteger los dispositivos receptores que se ubican en las partes de la red en segundo plano. En este caso, se señala que la puerta de enlace de acceso también puede contribuir a la neutralización de los dispositivos comunicantes detectando los comportamientos malintencionados. Por tanto, la coubicación del dispositivo de seguridad con la puerta de enlace de acceso permite bloquear rápidamente los mensajes emitidos por los dispositivos comunicantes que han pasado bajo el control de un tercero malintencionado.

La técnica de procesamiento se implementa por medio de componentes de software y/o hardware. En este sentido, el término “módulo” puede corresponder en este documento tanto a un componente de software como a un componente de hardware o a un conjunto de componentes de hardware y/o software, capaces de implementar una función o un conjunto de funciones, según lo cual se ha descrito anteriormente para el módulo en cuestión.

Un componente de software corresponde a uno o más programas de ordenador, uno o más subprogramas de un programa, o de manera más general a cualquier elemento de un programa o de un software. Un tal componente de software se almacena en la memoria, luego se carga y ejecuta mediante un procesador de datos de una entidad física y es susceptible de acceder a los recursos de hardware de esta entidad física (memorias, soportes de registro, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc.).

Del mismo modo, un componente de hardware corresponde a cualquier elemento de un conjunto de hardware (o hardware). Se puede tratar de un componente de hardware que se puede programar o no, con o sin procesador integrado para la ejecución del software. Se trata, por ejemplo, de un circuito integrado, una tarjeta inteligente, una tarjeta electrónica para la ejecución de un firmware (firmware), etc.

En un modo de realización particular, el módulo 55 de procesamiento está dispuesto para implementar aquellas de las etapas del procedimiento de procesamiento descrito anteriormente, implementadas por el dispositivo de seguridad. Se trata, de preferencia, de módulos de software que comprenden instrucciones de software para ejecutar aquellas de las etapas (o de las acciones) del procedimiento de procesamiento descrito anteriormente, implementadas por un dispositivo de seguridad. Por lo tanto, la invención también se refiere a:

- un programa para un dispositivo de seguridad, que comprende instrucciones de código de programa destinadas para controlar la ejecución de aquellas etapas (o de las acciones) del procedimiento de procesamiento descrito anteriormente, cuando el dicho programa es ejecutado por este dispositivo de seguridad;

- un soporte de registro legible por un dispositivo de seguridad en el cual se registra el programa para un dispositivo de seguridad.

Los módulos de software pueden ser almacenados o transmitidos por un soporte de datos. Este último puede ser un soporte de hardware de almacenamiento, por ejemplo, un CD-ROM, un disquete magnético o un disco duro, o un soporte de transmisión, tal como una señal eléctrica, óptica o de radio, o una red de telecomunicación.

Por tanto, el módulo 55 de procesamiento está configurado para:

- verificar que un mensaje enviado por un dispositivo comunicante con destino a un dispositivo receptor es un mensaje por transmitir;

- transmitir este mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;

- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante e identificador de producto que los del dispositivo comunicante que ha emitido este mensaje.

En un modo de realización particular, el módulo de procesamiento está además dispuesto para bloquear los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por los dispositivos comunicantes proporcionados por el mismo fabricante y de identificador de producto diferente a los del dispositivo comunicante que ha emitido el dicho mensaje.

Un sistema de seguridad comprende:

- un dispositivo 50 de seguridad destinado para procesar un mensaje enviado por un dispositivo 11, 21, 31, 12, 22 comunicante con destino a un dispositivo 60 receptor, comprendiendo el dicho dispositivo de seguridad un módulo 55 de procesamiento dispuesto para:

- verificar que este mensaje es un mensaje por transmitir;

- transmitir este mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;

- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por los dispositivos comunicantes proporcionados por el mismo fabricante e identificador de producto que los del dispositivo comunicante que ha emitido el dicho mensaje;

- un dispositivo receptor, dispuesto para recibir el dicho mensaje enviado por el dispositivo comunicante y transmitido por el dispositivo de seguridad y para enviar esta notificación al dispositivo de seguridad.

REIVINDICACIONES

1. Procedimiento de procesamiento que comprende:
- una verificación (E1) mediante un dispositivo (50) de seguridad de que un mensaje enviado por un dispositivo (11, 21, 31, 12, 22) comunicante con destino a un dispositivo (60) receptor es un mensaje por transmitir, siendo el mensaje transmitido al dispositivo receptor cuando la verificación es positiva;
- una recepción (E2) mediante el dispositivo de seguridad de una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado,
los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante que el del dispositivo comunicante que ha emitido el dicho mensaje están bloqueados por el dispositivo de seguridad durante la dicha verificación, siendo el dicho fabricante identificado por identificadores únicos de los dispositivos comunicantes.

2. Procedimiento de procesamiento según la reivindicación 1, que comprende una neutralización del dispositivo comunicante, para el cual se recibió la notificación.

3. Procedimiento de procesamiento según la reivindicación 1, en el cual los mensajes posteriores del mismo tipo que el mensaje para el que se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante y con el mismo identificador de producto que los del dispositivo comunicante que ha emitido el dicho mensaje son bloqueados por el dispositivo de seguridad durante la dicha verificación.

4. Procedimiento de procesamiento según la reivindicación 1 o 2, en el cual los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante y con un identificador de producto diferente al del dispositivo comunicante que ha emitido el dicho mensaje son bloqueados por el dispositivo de seguridad durante la dicha verificación.

5. Procedimiento de procesamiento según la reivindicación 1, que comprende una obtención mediante el dispositivo de seguridad de al menos un mensaje por transmitir.

6. Dispositivo (50) de seguridad destinado para procesar un mensaje enviado por un dispositivo (11,21,31,12,22) comunicante con destino a un dispositivo (60) receptor, comprendiendo el dicho dispositivo de seguridad un módulo (55) de procesamiento dispuesto para:
- verificar que el dicho mensaje es un mensaje por transmitir;
- transmitir el dicho mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;
- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por un mismo fabricante que el del dispositivo comunicante que ha emitido el dicho mensaje, siendo el dicho fabricante identificado por identificadores únicos de los dispositivos comunicantes.

7. Dispositivo de seguridad según la reivindicación 6, en el cual el módulo de procesamiento está además dispuesto para bloquear los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante y del mismo identificador de producto de los del dispositivo comunicante que ha enviado el dicho mensaje.

8. Dispositivo de seguridad según la reivindicación 6 o 7, en el cual el módulo de procesamiento también está dispuesto para bloquear los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por el mismo fabricante y de identificador de producto diferente de los del dispositivo comunicante que ha emitido el dicho mensaje.

9. Sistema de seguridad que comprende:
- un dispositivo (50) de seguridad destinado para procesar un mensaje enviado por un dispositivo (11,21,31,12,22) comunicante con destino a un dispositivo (60) receptor, comprendiendo el dicho dispositivo de seguridad un módulo (55) de procesamiento dispuesto para:
- verificar que el dicho mensaje es un mensaje por transmitir;
- transmitir el dicho mensaje cuando la verificación es positiva y bloquearlo cuando la verificación es negativa;
- recibir una notificación emitida por el dispositivo receptor indicando que el mensaje transmitido debe ser bloqueado, con el fin de bloquear durante la verificación de los mensajes posteriores del mismo tipo que el mensaje para el cual se recibió la notificación, emitidos por dispositivos comunicantes proporcionados por un mismo fabricante que el del dispositivo comunicante que ha emitido el dicho mensaje, siendo el dicho fabricante identificado por identificadores únicos de los dispositivos comunicantes;
- un dispositivo receptor, dispuesto para recibir el dicho mensaje enviado por el dispositivo comunicante y transmitido por el dispositivo de seguridad y para enviar la dicha notificación al dispositivo de seguridad.

10. Programa para un dispositivo de seguridad, que comprende instrucciones de código de programa destinadas para controlar la ejecución de aquellas de las acciones del procedimiento de procesamiento según una de las reivindicaciones 1 a 5 implementadas por el dispositivo, cuando el dicho programa es ejecutado por el dicho dispositivo.

11. Soporte de registro legible por un dispositivo de seguridad en el cual se registra el programa según la reivindicación 10.

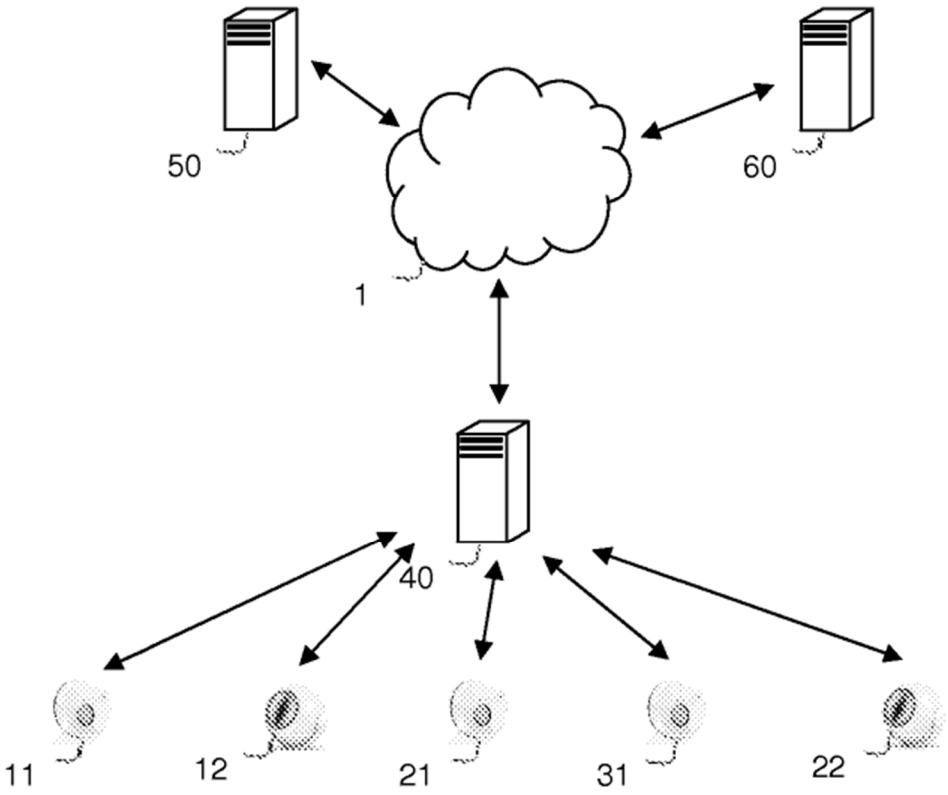
50
60
1
40
11
12
21
31
22

Fig. 1

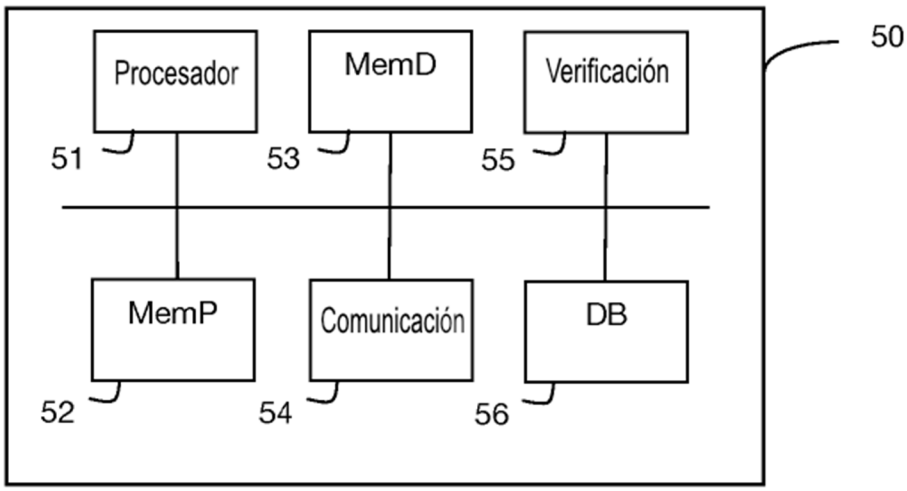
Procesador
MemD
Verificación
MemP
Comunicación
DB
50
51
53
55
52
54
56

Fig. 3

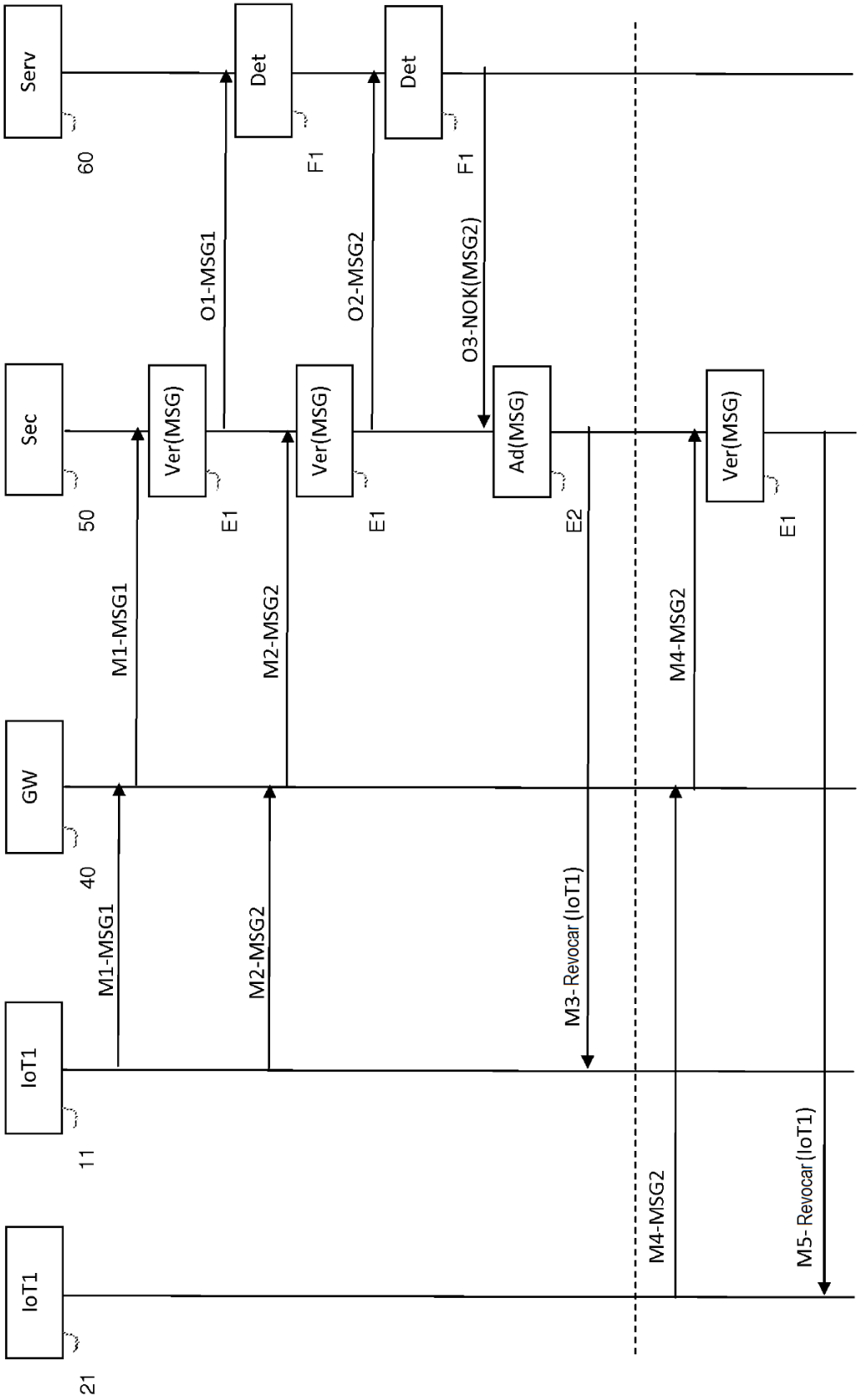
Serv
60
Det
F1
Det
F1
O1-MSG1
O2-MSG2
O3-NOK(MSG2)
Sec
50
Ver(MSG)
E1
Ver(MSG)
E1
Ad(MSG)
E2
Ver(MSG)
E1
M1-MSG1
M2-MSG2
M4-MSG2
GW
40
M1-MSG1
M2-MSG2
M3- Revocar (IoT1)
M4-MSG2
M5- Revocar (IoT1)
IoT1
11
IoT1
21

Fig. 2