(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 023 362**

(51) Int. Cl.:

G06F 8/65 (2008.01)
G06F 9/445 (2008.01)
H04W 4/40 (2008.01)
G06F 21/30 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.10.2017 E 22205812 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.03.2025 EP 4152144**

(54) Título: **Método de mejora de dispositivo montado en vehículo y dispositivo relacionado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.05.2025

(73) Titular/es:

SHENZHEN YINWANG INTELLIGENT TECHNOLOGIES CO., LTD. (100.00%)
Room 101, Huawei Headquarters Office Building
Huawei, Vanke City Community Bantian Street
Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

YANG, YANJIANG;
WEI, ZHUO;
LIN, HSIAO-YING;
LI, TIEYAN y
SHEN, JUNQIANG

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de mejora de dispositivo montado en vehículo y dispositivo relacionado

CAMPO TÉCNICO

Esta solicitud está relacionada con el campo de tecnologías montadas en vehículo, y en particular, con un método de mejora de dispositivo montado en vehículo y un dispositivo relacionado.

ANTECEDENTES

En el futuro, cada vehículo es un nodo de red en internet de vehículos y es sustancialmente el mismo que un dispositivo conectado a web tal como un ordenador o un teléfono móvil. Se estima que del 60 % al 70 % de llamadas de vehículo en Norteamérica son provocados por problemas de firmware/software. Por lo tanto, mejorar un firmware/software de un dispositivo montado en vehículo es una etapa indispensable. Un vehículo convencional de dispositivo montado en vehículo a mejorar se llama para mejora de firmware/software. Este tipo de método tiene desventajas de costes altos y un ciclo largo.

Por lo tanto, para un futuro dispositivo montado en vehículo, tiene que implementarse una mejora remota más flexible usando una tecnología por el aire (Over-The-Air, OTA), justo como la mejora remota realizada para un ordenador y un teléfono móvil actualmente. La mejora remota de firmware/software para un dispositivo montado en vehículo puede brindar muchos beneficios. Por ejemplo, esto ayuda a arreglar rápidamente errores clave de firmware/software, mejora la seguridad del vehículo, y añade una nueva función o rasgo a tiempo al vehículo durante toda la vida útil. Por lo tanto, en esta manera de OTA, se puede implementar mejora de firmware/software sin llamar al vehículo. Esto puede reducir muchos de costes para un fabricante de vehículos o minorista y también brinda comodidad al propietario de un vehículo.

Sin embargo, durante la mejora remota para un dispositivo montado en vehículo a mejorar, como algunos dispositivos montados en vehículo a mejorar tienen problemas tales como limitada capacidad de computación o limitado espacio de almacenamiento, la eficiencia en la mejora para los dispositivos montados en vehículo a mejorar es relativamente baja, afectando incluso a la mejora de todo el sistema montado en vehículo. Por lo tanto, un problema que tiene que resolverse urgentemente es cómo garantizar una mejora segura y eficiente de firmware/software para un dispositivo montado en vehículo.

El documento US 2014/0282470 A1 describe sistemas y métodos para transmisión de datos entre uno o más vehículos y un aparato de control (p. ej., servidor u otro dispositivo informático). En particular, dicho documento está relacionado con sistemas, métodos y productos de programa informático para transmisión por el aire de imágenes electrónicas (EI) entre uno o más vehículos y un subsistema de control.

COMPENDIO

Realizaciones de la presente invención proporcionan un método de mejora de dispositivo montado en vehículo y un vehículo inteligente, para resolver un problema que no se puede implementar mejora segura y eficiente de firmware/software para un dispositivo montado en vehículo. La invención se establece por las reivindicaciones anexas.

Según un primer aspecto, una realización de la presente invención proporciona un método de mejora de dispositivo montado en vehículo según la reivindicación 1. Según esta realización de la presente invención, en un lado de dispositivo de control montado en vehículo, se realiza procesamiento de verificación de seguridad en un paquete de mejora montado en vehículo requerido para mejorar un dispositivo montado en vehículo, para impedir que dispositivos montados en vehículo a mejorar que tienen diferentes capacidades de mejora participen en un proceso de verificación de seguridad, asegurando de ese modo que el dispositivo montado en vehículo se mejora de manera segura y eficientemente usando el paquete de mejora montado en vehículo.

En una implementación posible, el paquete de mejora montado en vehículo incluye una primera firma digital; y realizar, por parte del dispositivo de control montado en vehículo, verificación de seguridad en la pluralidad de archivos de mejora incluye: realizar, por parte del dispositivo de control montado en vehículo, verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital. En otras palabras, el paquete de mejora montado en vehículo se verifica usando una firma digital, asegurando de ese modo la validez del paquete de mejora montado en vehículo obtenido desde fuera de un dispositivo montado en vehículo por el dispositivo de control montado en vehículo.

En una implementación posible, el método incluye además: enviar, por parte del dispositivo de control montado en vehículo, información de autenticación de identidad a un servidor de mejoras; y si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo y el servidor de mejoras; y obtener, por parte de un dispositivo de

control montado en vehículo, un paquete de mejora montado en vehículo de un servidor de mejoras incluye: obtener, por parte del dispositivo de control montado en vehículo, el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro. En otras palabras, un canal seguro se establece entre el dispositivo de control montado en vehículo y el servidor de mejoras, para garantizar la confidencialidad del paquete de mejora montado en vehículo en un proceso de transmisión. En este caso, el paquete de mejora montado en vehículo no necesita ser encriptado adicionalmente. En una implementación posible, el paquete de mejora montado en vehículo se encripta usando una primera clave, y la primera clave es una clave simétrica; y el método incluye además: obtener, por parte del dispositivo de control montado en vehículo, la primera clave de un servidor de claves; y después de realizar, por parte del dispositivo de control montado en vehículo, verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital, el método incluye: desencriptar, por parte del dispositivo de control montado en vehículo, la pluralidad de archivos de mejora usando la primera clave si tiene éxito la verificación de firma digital. En otras palabras, el paquete de mejora montado en vehículo se encripta, y una clave de encriptación se almacena en un servidor de claves dedicado, asegurando de ese modo efectivamente la confidencialidad del paquete de mejora montado en vehículo en un proceso de transmisión.

En una implementación posible, enviar, por parte del dispositivo de control montado en vehículo, un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido incluye: dividir, por parte del dispositivo de control montado en vehículo, el archivo de mejora pretendido en una pluralidad de subarchivos de mejora; generar, por parte del dispositivo de control montado en vehículo, una pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y generar un primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando una segunda clave, donde la segunda clave es una clave de algoritmo simétrica; y enviar secuencialmente, por parte del dispositivo de control montado en vehículo al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC. En otras palabras, durante la transmisión del paquete de mejora montado en vehículo entre dispositivos montados en vehículo, un archivo de mejora se divide en una pluralidad de bloques de datos asociados usando un algoritmo preestablecido, y se realiza procesamiento de MAC en los bloques de datos asociados, de modo que el dispositivo de control montado en vehículo divide un archivo de mejora completo en una pluralidad de bloques de datos que se pueden transmitir por separado y en la que verificación de validez se puede realizar por separado. Adicionalmente, como la pluralidad de bloques de datos se asocian, un bloque de datos que tiene un problema de seguridad se puede localizar rápidamente usando un algoritmo relacionado. Por lo tanto, disminuye la carga de trabajo de computación y la complejidad de computación en una unidad de tiempo para un dispositivo montado en vehículo a mejorar que tiene una capacidad relativamente débil. Después de que ocurre un error de transmisión de archivo de mejora, una parte de error se puede encontrar tan rápidamente como sea posible, de modo que únicamente se solicita retransmitir la parte de error en vez del archivo de mejora entero. De esta manera, se garantiza además una mejora segura y eficiente para el dispositivo montado en vehículo.

En una implementación posible, el método incluye además: encriptar, por parte del dispositivo de control montado en vehículo, cada uno de la pluralidad de subarchivos de mejora usando una tercera clave; y generar, por parte del dispositivo de control montado en vehículo, una pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido incluye: generar, por parte del dispositivo de control montado en vehículo usando el algoritmo preestablecido, la pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora que se encriptan usando la tercera clave. La confidencialidad del paquete de mejora montado en vehículo además se garantiza mientras que se garantiza la validez del paquete de mejora montado en vehículo, impidiendo de ese modo que el paquete de mejora montado en vehículo de sea obtenido por una parte no autorizada.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora, una pluralidad de bloques de datos asociados mutuamente se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y la pluralidad de subarchivos de mejora llevan una segunda firma digital de la pluralidad de bloques de datos que se genera usando una cuarta clave, donde la cuarta clave es una clave asimétrica; realizar, por parte del dispositivo de control montado en vehículo, verificación de seguridad en la pluralidad de archivos de mejora incluye: comprobar, por parte del dispositivo de control montado en vehículo, la segunda firma digital de la pluralidad de bloques de datos; y enviar, por parte del dispositivo de control montado en vehículo, un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido incluye: generar, por parte del dispositivo de control montado en vehículo, un segundo MAC de la pluralidad de bloques de datos usando una quinta clave, donde la quinta clave es una clave de algoritmo simétrica; y enviar secuencialmente, por parte del dispositivo de control montado en vehículo al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el segundo MAC. En otras palabras, puede implementarse transmisión de bloque y firma del paquete de mejora montado en vehículo en un lado de desarrollador de mejora. Esto es, antes de obtenerse por el dispositivo de control montado en vehículo, se obtienen bloques de datos a través de división usando un algoritmo preestablecido y firmado. En este caso, el dispositivo montado en vehículo necesita comprobar primero la validez de los bloques de datos, y entonces realiza procesamiento

de MAC en bloques de datos comprobados como válidos. De esta manera, disminuye la carga de trabajo de computación y la complejidad de computación del dispositivo montado en vehículo a mejorar mientras se garantiza la validez del archivo de mejora montado en vehículo en un proceso de transmisión en vehículo. Por lo tanto, el dispositivo montado en vehículo se mejora de manera segura y eficientemente.

En una implementación posible, el algoritmo preestablecido incluye uno cualquiera de un algoritmo de cadena de hash, un algoritmo de árbol de hash, y un algoritmo de filtro de Bloom. El algoritmo preestablecido usa una función hash de los algoritmos anteriores, para dividir el archivo de mejora pretendido en una pluralidad de bloques de datos asociados mutuamente. De esta manera, durante el procesamiento de MAC, puede realizarse procesamiento de MAC únicamente en uno de la pluralidad de bloques de datos, y otros bloques de datos asociados pueden comprobarse usando un valor hash para asociación mutua.

En una implementación posible, el método incluye además: retransmitir, por parte del dispositivo de control montado en vehículo, un bloque de datos pretendido al dispositivo montado en vehículo a mejorar pretendido, donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos. En función de transmisión de bloques asociados, un bloque de datos en el que falla la verificación se puede localizar rápidamente, y cuando ocurre este tipo de error de transmisión, únicamente tiene que solicitarse de nuevo un bloque de datos correspondiente en vez del archivo de mejora entero, reduciendo de ese modo sobrecargas, mejorando la eficiencia de mejora y garantizando la seguridad de mejora.

Según un segundo aspecto, una realización de la presente invención proporciona un vehículo inteligente según la reivindicación 8.

En una implementación posible, el dispositivo de control montado en vehículo se configura específicamente para realizar verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital. En otras palabras, el dispositivo de control montado en vehículo del vehículo inteligente en esta realización de la presente invención necesita comprobar la validez de la pluralidad de archivos de mejora en el paquete de mejora montado en vehículo que se obtiene desde fuera del vehículo.

En una implementación posible, el dispositivo de control montado en vehículo se configura específicamente para:

enviar información de autenticación de identidad al servidor de mejoras, si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo y el servidor de mejoras, y obtener el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro; o el paquete de mejora montado en vehículo se encripta usando una primera clave, la primera clave es una clave simétrica, y el dispositivo de control montado en vehículo se configura específicamente para: obtener la primera clave de un servidor de claves, y después de que tiene éxito la verificación de firma digital realizada en la pluralidad de archivos de mejora usando la primera firma digital, desencriptar la pluralidad de archivos de mejora usando la primera clave. En otras palabras, el dispositivo de control montado en vehículo del vehículo inteligente en esta realización de la presente invención puede establecer un canal seguro a un extremo de servidor, para garantizar la seguridad de un proceso de obtener el paquete de mejora montado en vehículo.

En una implementación posible, el dispositivo de control montado en vehículo se configura específicamente para: dividir el archivo de mejora pretendido en una pluralidad de subarchivos de mejora, generar una pluralidad de bloques de datos asociados mutuamente usando un algoritmo preestablecido, generar un primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando una segunda clave, y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC, donde la segunda clave es una clave de algoritmo simétrica; y

el dispositivo montado en vehículo a mejorar se configura específicamente para: recibir secuencialmente la pluralidad de bloques de datos que llevan el primer MAC y que son enviados por el dispositivo de control montado en vehículo; realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

En otras palabras, después de verificar la validez del paquete de mejora montado en vehículo obtenido desde fuera del vehículo, el dispositivo de control montado en vehículo del vehículo inteligente en esta realización de la presente invención divide el archivo de mejora en bloques y realiza procesamiento de MAC dentro de vehículo, para garantizar la validez del archivo de mejora durante transmisión en vehículo. Adicionalmente, como el dispositivo montado en vehículo a mejorar puede recibir y comprobar bloques del archivo de mejora, un error se puede localizar rápidamente. Además, la complejidad de computación es relativamente baja para

comprobación de MAC. Por lo tanto, se puede garantizar que la comprobación y la mejora son relativamente fáciles para un dispositivo montado en vehículo a mejorar que tiene una capacidad de mejora relativamente débil en el vehículo. De esta manera, se garantiza la eficiencia y la seguridad de mejora de vehículo.

En una implementación posible, el dispositivo de control montado en vehículo se configura específicamente para:

encriptar cada uno de la pluralidad de subarchivos de mejora usando una tercera clave, y generar, usando el algoritmo preestablecido, la pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora que se encriptan usando la tercera clave; y
el dispositivo montado en vehículo a mejorar se configura específicamente para: cuando se verifican todos de la pluralidad de bloques de datos, desencriptar cada uno de la pluralidad de bloques de datos verificados secuencialmente usando la tercera clave, y combinar la pluralidad de bloques de datos que se desencriptan usando la tercera clave para mejora.

En otras palabras, para el dispositivo de control montado en vehículo del vehículo inteligente en esta realización de la presente invención, además se garantiza la confidencialidad del archivo de mejora a través de encriptación durante la transmisión del archivo de mejora en el vehículo.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora, una pluralidad de bloques de datos asociados mutuamente se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y la pluralidad de subarchivos de mejora llevan una segunda firma digital de la pluralidad de bloques de datos que se genera usando una cuarta clave, donde la cuarta clave es una clave asimétrica;

el dispositivo de control montado en vehículo se configura específicamente para: comprobar la segunda firma digital de la pluralidad de bloques de datos, generar un segundo MAC de la pluralidad de bloques de datos usando una quinta clave, y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el segundo MAC, donde la quinta clave es una clave de algoritmo simétrica; y
el dispositivo montado en vehículo a mejorar se configura específicamente para: recibir secuencialmente la pluralidad de bloques de datos que llevan el segundo MAC y que son enviados por el dispositivo de control montado en vehículo; realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la quinta clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

En otras palabras, después de verificar la validez del archivo de mejora dividido y firmado obtenido desde fuera del vehículo, el dispositivo de control montado en vehículo del vehículo inteligente en esta realización de la presente invención divide el archivo de mejora en bloques y realiza procesamiento de MAC dentro de vehículo, para garantizar la validez del archivo de mejora durante transmisión en vehículo. Adicionalmente, como el dispositivo montado en vehículo a mejorar puede recibir y comprobar bloques del archivo de mejora, un error se puede localizar rápidamente. Además, la complejidad de computación es relativamente baja para comprobación de MAC. Por lo tanto, se puede garantizar que la comprobación y la mejora son relativamente fáciles para un dispositivo montado en vehículo a mejorar que tiene una capacidad de mejora relativamente débil en el vehículo. De esta manera, se garantiza la eficiencia y la seguridad de mejora de vehículo.

Según un tercer aspecto, como ejemplo para un mejor entendimiento, se presenta un método de mejora de dispositivo montado en vehículo, que puede incluir:

recibir, por parte de un dispositivo montado en vehículo a mejorar pretendido, un archivo de mejora pretendido enviado por un dispositivo de control montado en vehículo, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad realizada por el dispositivo de control montado en vehículo y que se utiliza para mejorar al menos el dispositivo montado en vehículo a mejorar pretendido; y realizar, por parte del dispositivo montado en vehículo a mejorar pretendido, una mejora segura usando el archivo de mejora pretendido. En esta realización de la presente invención, el dispositivo montado en vehículo a mejorar pretendido recibe un archivo de mejora en el que el procesamiento de verificación de seguridad ya se ha realizado en un lado de dispositivo de control montado en vehículo, y realiza mejora de dispositivo usando el archivo de mejora, para impedir a dispositivos montados en vehículo a mejorar que tienen diferentes capacidades de mejora que participen en un proceso de verificación de seguridad, de garantizando ese modo que un dispositivo montado en vehículo a mejorar se mejora de manera segura y eficientemente usando el paquete de mejora montado en vehículo.

En una implementación posible del ejemplo para un mejor entendimiento, realizar, por parte del dispositivo montado en vehículo a mejorar pretendido, una mejora segura usando el archivo de mejora pretendido incluye:

usar, por parte del dispositivo montado en vehículo a mejorar pretendido, un modo de mejora de actualizaciones de sistema A/B, y realizar la mejora segura usando el archivo de mejora pretendido, donde el dispositivo montado en vehículo a mejorar es un primer dispositivo montado en vehículo a mejorar cuya capacidad de almacenamiento de recursos y/o capacidad de procesamiento superan un valor preestablecido o un primer dispositivo montado en vehículo a mejorar que se especifica por adelantado. Para un dispositivo montado en vehículo a mejorar que tiene una capacidad relativamente fuerte, se puede usar el modo de mejora de actualizaciones de sistema A/B para mejora.

En una implementación posible del ejemplo para un mejor entendimiento, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora; recibir, por parte de un dispositivo montado en vehículo a mejorar pretendido, un archivo de mejora pretendido enviado por un dispositivo de control montado en vehículo incluye: recibir secuencialmente:, por parte del dispositivo montado en vehículo a mejorar pretendido, una pluralidad de bloques de datos que llevan un primer MAC y que son enviados por el dispositivo de control montado en vehículo, donde la pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, el primer MAC es un código de autenticación de mensaje de la pluralidad de bloques de datos que se genera usando una segunda clave, y la segunda clave es una clave simétrica; y realizar, por parte del dispositivo montado en vehículo a mejorar pretendido, una mejora segura usando el archivo de mejora pretendido incluye: realizar secuencialmente, por parte del dispositivo montado en vehículo a mejorar pretendido, verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar, por parte del dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que se verifican secuencialmente para mejora. En otras palabras, durante la transmisión del paquete de mejora montado en vehículo entre dispositivos montados en vehículo, un archivo de mejora se divide en una pluralidad de bloques de datos asociados usando un algoritmo preestablecido, y se realiza procesamiento de MAC en los bloques de datos asociados, de modo que el dispositivo de control montado en vehículo divide un archivo de mejora completo en una pluralidad de bloques de datos que se pueden transmitir por separado y en la que verificación de validez se puede realizar por separado. Adicionalmente, como la pluralidad de bloques de datos se asocian, un bloque de datos que tiene un problema de seguridad se puede localizar rápidamente usando un algoritmo relacionado. Por lo tanto, disminuye la carga de trabajo de computación y la complejidad de computación en una unidad de tiempo para un dispositivo montado en vehículo a mejorar que tiene una capacidad relativamente débil. Después de que ocurre un error de transmisión de archivo de mejora, una parte de error se puede encontrar tan rápidamente como sea posible, de modo que únicamente se solicita retransmitir la parte de error en vez del archivo de mejora entero. De esta manera, se garantiza además una mejora segura y eficiente para el dispositivo montado en vehículo.

En una implementación posible del ejemplo para un mejor entendimiento, la pluralidad de subarchivos de mejora se encriptan usando una tercera clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar, por parte del dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que se verifican secuencialmente para mejora incluye: cuando se verifican todos de la pluralidad de bloques de datos, desencriptar, por parte del dispositivo montado en vehículo a mejorar pretendido, cada uno de la pluralidad de bloques de datos verificados secuencialmente usando la tercera clave, y combinar la pluralidad de bloques de datos que se desencriptan usando la tercera clave para mejora. La confidencialidad del paquete de mejora montado en vehículo además se garantiza mientras que se garantiza la validez del paquete de mejora montado en vehículo, impidiendo de ese modo que el paquete de mejora montado en vehículo de sea obtenido por una parte no autorizada.

En una implementación posible del ejemplo para un mejor entendimiento, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora; recibir, por parte de un dispositivo montado en vehículo a mejorar pretendido, un archivo de mejora pretendido enviado por un dispositivo de control montado en vehículo incluye: recibir secuencialmente:, por parte del dispositivo montado en vehículo a mejorar pretendido, una pluralidad de bloques de datos que llevan un segundo MAC y que son enviados por el dispositivo de control montado en vehículo, donde la pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, el segundo MAC es un código de autenticación de mensaje de la pluralidad de bloques de datos que se genera usando una quinta clave, y la quinta clave es una clave simétrica; y realizar, por parte del dispositivo montado en vehículo a mejorar pretendido, una mejora segura usando el archivo de mejora pretendido incluye: realizar secuencialmente, por parte del dispositivo montado en vehículo a mejorar pretendido, verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la quinta clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar, por parte del dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que se verifican secuencialmente para mejora. En otras palabras, puede implementarse transmisión de bloque y firma del paquete de mejora montado en vehículo en un lado de desarrollador de mejora. Esto es, antes de obtenerse por el dispositivo de control montado en vehículo, se obtienen bloques de datos a través de división usando un algoritmo preestablecido y firmado. En este caso, el dispositivo montado en vehículo necesita comprobar primero la validez de los bloques de datos, y entonces realiza procesamiento de MAC en bloques de datos

comprobados como válidos. De esta manera, disminuye la carga de trabajo de computación y la complejidad de computación del dispositivo montado en vehículo a mejorar mientras se garantiza la validez del archivo de mejora montado en vehículo en un proceso de transmisión en vehículo. Por lo tanto, el dispositivo montado en vehículo se mejora de manera segura y eficientemente.

En una implementación posible del ejemplo para un mejor entendimiento, el método incluye además: volver a obtener, por parte del dispositivo montado en vehículo a mejorar pretendido, un bloque de datos pretendido del dispositivo de control montado en vehículo, donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos. En función de transmisión de bloques asociados, un bloque de datos en el que falla la verificación se puede localizar rápidamente, y cuando ocurre este tipo de error de transmisión, únicamente tiene que solicitarse de nuevo un bloque de datos correspondiente en vez del archivo de mejora entero, reduciendo de ese modo sobrecargas, mejorando la eficiencia de mejora y garantizando la seguridad de mejora.

Según un cuarto aspecto, como ejemplo para un mejor entendimiento, se proporciona un aparato de mejora de dispositivo montado en vehículo. El aparato de mejora de dispositivo montado en vehículo tiene una función de implementar el método en una cualquiera de las anteriores realizaciones de método de mejora de dispositivo montado en vehículo. La función puede implementarse usando hardware o ejecutando correspondiente software por hardware. El hardware o software incluye uno o más módulos correspondientes a la función.

Según un quinto aspecto, como ejemplo para un mejor entendimiento, se proporciona un aparato montado en vehículo a mejorar. El dispositivo terminal tiene una función de implementar el método en una cualquiera de las anteriores realizaciones de método de mejora de dispositivo montado en vehículo. La función puede implementarse usando hardware o ejecutando correspondiente software por hardware. El hardware o software incluye uno o más módulos correspondientes a la función.

Según un sexto aspecto, como ejemplo para un mejor entendimiento, se proporciona un dispositivo de control montado en vehículo. El dispositivo de control montado en vehículo incluye un procesador, y el procesador se configura para apoyar al dispositivo de control montado en vehículo al realizar una correspondiente función en el método de mejora de dispositivo montado en vehículo proporcionado en el primer aspecto. El dispositivo de control montado en vehículo puede incluir además una memoria, y la memoria se configura para acoplarse al procesador y almacenar una instrucción de programa y datos que son necesarios para el dispositivo de control montado en vehículo. El dispositivo de control montado en vehículo puede incluir además una interfaz de comunicaciones para comunicación entre el dispositivo de control montado en vehículo y otro dispositivo o red de comunicaciones.

Según un séptimo aspecto, como ejemplo para un mejor entendimiento se proporciona un dispositivo montado en vehículo a mejorar pretendido. El dispositivo montado en vehículo a mejorar pretendido incluye un procesador, y el procesador se configura para apoyar al dispositivo montado en vehículo a mejorar pretendido a realizar una correspondiente función en el método de mejora de dispositivo montado en vehículo proporcionado en el tercer aspecto. El dispositivo montado en vehículo a mejorar pretendido puede incluir además una memoria, y la memoria se configura para acoplarse al procesador y almacenar una instrucción de programa y datos que son necesarios para el dispositivo montado en vehículo a mejorar pretendido. El dispositivo montado en vehículo a mejorar pretendido puede incluir además una interfaz de comunicaciones para comunicación entre el dispositivo montado en vehículo a mejorar pretendido y otro dispositivo o red de comunicaciones.

Según un octavo aspecto, como ejemplo para un mejor entendimiento, se proporciona un soporte de almacenamiento informático, configurado para almacenar una instrucción de software informático usado por el dispositivo de control montado en vehículo proporcionado en la sexto aspecto. La instrucción de software informático incluye un programa diseñado para implementar el anterior aspecto.

Según un noveno aspecto, como ejemplo para un mejor entendimiento, se proporciona un soporte de almacenamiento informático, configurado para almacenar una instrucción de software informático usado por el dispositivo montado en vehículo a mejorar pretendido proporcionado en el séptimo aspecto. La instrucción de software informático incluye un programa diseñado para implementar el anterior aspecto.

Según un décimo aspecto, como ejemplo para un mejor entendimiento, se proporciona un programa informático. El programa informático incluye una instrucción, y cuando el programa informático es ejecutado por un ordenador, el ordenador se habilita para realizar etapas del método de mejora de dispositivo montado en vehículo en cualquier implementación posible del primer aspecto.

Según un undécimo aspecto, como ejemplo para un mejor entendimiento, se proporciona un programa informático. El programa informático incluye una instrucción, y cuando el programa informático es ejecutado por un ordenador, el ordenador se habilita para realizar etapas del método de mejora de dispositivo montado en vehículo en cualquier implementación posible del tercer aspecto.

Según un duodécimo aspecto, como ejemplo para un mejor entendimiento, se proporciona un sistema de chip. El sistema de chip incluye un procesador, configurado para soportar un dispositivo montado en vehículo a mejorar pretendido o un dispositivo de control montado en vehículo al implementar una función relacionada con los anteriores aspectos, por ejemplo, recibir o procesar datos y/o información en los métodos anteriores. En un posible diseño, el sistema de chip incluye además una memoria, y la memoria se configura para almacenar una instrucción de programa; y datos que son necesarios para el dispositivo montado en vehículo a mejorar pretendido o el dispositivo de control montado en vehículo. El sistema de chip puede incluir un chip, o puede incluir un chip y otro dispositivo discreto.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIGURA 1 es un diagrama de una arquitectura de mejora de sistema montado en vehículo según una realización de la presente invención;
la FIGURA 2 es un diagrama estructural esquemático de un orquestador de OTA según una realización de la presente invención;
la FIGURA 3 es un diagrama estructural esquemático de un dispositivo montado en vehículo a mejorar según una realización de la presente invención;
la FIGURA 4 es otro diagrama de una arquitectura de mejora de sistema montado en vehículo según una realización de la presente invención;
la FIGURA 5 es un diagrama de flujo esquemático de un método de mejora de dispositivo montado en vehículo según una realización de la presente invención;
la FIGURA 6 es un diagrama estructural esquemático de un aparato de mejora montado en vehículo según una realización de la presente invención;
la FIGURA 7 es un diagrama estructural esquemático de un aparato montado en vehículo a mejorar según una realización de la presente invención;
la FIGURA 8 es un diagrama estructural esquemático de un dispositivo según una realización de la presente invención; y
la FIGURA 9 es un diagrama estructural esquemático de un vehículo inteligente según una realización de la presente invención.

DESCRIPCIÓN DE REALIZACIONES

A continuación se describen realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención.

En esta memoria descriptiva, las reivindicaciones y los dibujos adjuntos de esta solicitud, los términos "primero", "segundo", "tercero", "cuarto", etc. pretenden distinguir entre diferentes objetos, pero no indican un orden particular. Adicionalmente, los términos "que incluye" y "que tiene" y cualesquiera otras variantes del mismo pretenden cubrir una inclusión no exclusiva. Por ejemplo, un proceso, un método, un sistema, un producto o un dispositivo que incluye un serie de las etapas o unidades no se limita a las etapas o unidades enumeradas, pero opcionalmente incluye además una etapa o unidad no enumerada, u opcionalmente incluye además otra etapa o unidad inherente del proceso, el método, el producto o el dispositivo.

Mencionar una "realización" en esta memoria descriptiva significa que una característica, estructura o rasgo particular descrito con referencia a las realizaciones se puede incluir en al menos una realización de esta solicitud. La frase mostrada en diversas ubicaciones en esta memoria descriptiva puede no necesariamente referirse a una misma realización, y no es una realización independiente u opcional exclusiva de otra realización. Se entiende explícita e implícitamente por un experto en la técnica que las realizaciones descritas en esta memoria descriptiva pueden combinarse con otra realización.

Términos tales como "componente", "módulo" y "sistema" usados en esta memoria descriptiva se usan para indicar entidades relacionadas con ordenador, hardware, firmware, combinaciones de hardware y software, software, o software que se ejecuta. Por ejemplo, un componente puede ser, pero sin limitación a esto, un proceso que se ejecuta en un procesador, un procesador, un objeto, un archivo ejecutable, un hilo de ejecución, un programa y/o un ordenador. Según se muestra en las figuras, tanto un dispositivo informático como una aplicación que se ejecuta en un dispositivo informático pueden ser componentes. Uno o más componentes pueden residir dentro de un proceso y/o un hilo de ejecución, y un componente se puede localizar en un ordenador y/o distribuirse entre al menos dos ordenadores. Además, estos componentes se pueden ejecutar desde diversos medios legibles por ordenador que almacenan diversas estructuras de datos. Por ejemplo, los componentes pueden comunicarse usando un proceso local y/o remoto y sobre la base de, por ejemplo, una señal que tiene uno o más paquetes de datos (por ejemplo, datos de dos componentes que interactúan con otro componente en un sistema local, un sistema distribuido y/o por una red tal como internet que interactúan con otros sistemas usando la señal).

Primero, en esta solicitud se explican y se describen algunos términos, para facilitar el entendimiento para un experto en la técnica.

(1). Una tecnología por el aire (Over-the-air Technology, OTA) es una tecnología para realizar la mejora remota de firmware o software a través de una interfaz de aire en comunicación móvil.

(2). Un servicio de información montado en vehículo (Telematics) es un compuesto de telecomunicaciones (Telecommunications) y ciencias de la información (Informatics), y puede definirse literalmente como sistema de servicio que proporciona información usando un sistema informático integrado un vehículo tal como un automóvil, una aeronave, una embarcación, o un tren, tecnologías de comunicaciones inalámbricas, un aparato de navegación por satélite, o tecnologías de internet para intercambiar información tal como un texto o voz. En breve, el sistema de servicio conecta un vehículo a internet usando una red inalámbrica, y proporciona un vehículo propietario con diversa información necesaria para conducir y vivir.

(3). Una unidad de control electrónico (Electronic Control Unit, ECU) es un microcontrolador específico de vehículo desde una perspectiva de uso. Como un ordenador común, la unidad de control electrónico incluye circuitos integrados a gran escala tales como un microprocesador (CPU), una memoria (una ROM o una RAM), una interfaz de entrada/salida (I/O), un convertidor analógico-a-digital (A/D), un conformador y un controlador.

(4). Una unidad de control de vehículo (Vehicle control unit, VCU) también se puede denominar controlador de vehículo eléctrico integrado. La VCU es un controlador general de una cadena de trasmisión de vehículo eléctrico, es responsable de coordinar el funcionamiento de partes tales como un motor térmico, un motor de impulsión, un caja de engranajes, y una batería de energía, y tiene funciones de mejorar las prestaciones de potencia, prestaciones de seguridad y eficiencia económica de un vehículo. La VCU es una parte central de un sistema de control de vehículo eléctrico integrado y es un controlador central configurado para controlar arranque, funcionamiento, avance y retroceso, velocidad y parada de un motor de un vehículo eléctrico y controlar otro dispositivo electrónico del vehículo eléctrico. Como parte central de un sistema de control de un vehículo eléctrico puro, la VCU es responsable de tareas tales como intercambio de datos, gestión de seguridad, interpretación de intensión del conductor y gestión de corriente de alimentación. La VCU recoge una señal de un sistema de control de motor, una señal de un pedal de acelerador, una señal de un pedal de freno, y una señal de otra parte, determina una intensión de conducción de un conductor tras realizar análisis completo y genera una respuesta, y monitoriza acciones de controladores de partes de capa más baja. La VCU juega un papel en funciones tales como conducción normal del vehículo, regeneración y frenado de energía de batería, gestión de red, diagnosis y procesamiento de fallos y monitorización de estado de vehículo.

(6). Un bus de red de área de controlador (Controller Area Network, CAN) es un bus de campo aplicado más ampliamente en el mundo. Recibe mucha atención la alta fiabilidad y una fuerte capacidad de detección de errores del bus CAN, y por lo tanto el bus CAN se aplica ampliamente a un sistema de control de ordenador de vehículo y un entorno industrial con una temperatura ambiente de hash, fuerte radiación electromagnética y vibración intensa. El bus CAN es un bus de campo ampliamente aplicado y tiene una gran perspectiva de aplicación en campos tales como medición industrial y automatización de control e industrial. Un CAN es una red de bus de comunicaciones en serie. El bus CAN tiene las ventajas de ser fiable, en tiempo real y flexible en comunicación de datos. Para diseño transparente y ejecución flexible, una estructura del bus CAN se divide en una capa física y una capa de enlace de datos (que incluye una subcapa de control de enlace lógico LLC y una subcapa de control de acceso a medios MAC) según un modelo estándar ISO/OSI.

(7). Un código de autenticación de mensaje (Message Authentication Code, MAC) es una función de codificación para una fuente de señal. El MAC es similar a un algoritmo digest pero necesita usar una clave durante la computación, y por lo tanto el MAC depende de ambas de una clave usada e información cuyo MAC tiene que computarse. Realmente, el MAC se obtiene usualmente a través de construcción basada en el algoritmo digest.

(8). Un algoritmo de derivación de clave (Key Derivation Function, KDF) es una función de derivación de clave usada durante encriptación y desencriptación. Una función de la función de derivación de clave es derivar datos de clave de un puerto serie de bit secreto compartido. Durante la negociación de clave, la función de derivación de clave trabaja en una cadena de bits secreta obtenida en intercambio de clave, para generar una clave de sesión requerida o datos de clave requeridos para encriptación adicional.

(9). Criptología de clave pública (criptología asimétrica): La criptología de clave pública también se denomina criptología asimétrica. Un algoritmo de clave asimétrica significa que una clave de encriptación de un algoritmo de encriptación es diferente de una clave de desencriptación del algoritmo de encriptación, o una clave del algoritmo de encriptación no se puede deducir usando la otra clave. Un usuario que tiene criptología de clave pública tiene una clave de encriptación y una clave de desencriptación, y la clave de desencriptación no puede obtenerse usando la clave de encriptación. Adicionalmente, la clave de encriptación es pública. La criptología de clave pública se diseña en función de este principio, para usar información de asistencia (información de trampilla) como clave secreta. La seguridad de este tipo de criptología depende de la complejidad de computación de un problema en la

que se basa el tipo de criptología. Actualmente, la criptología de clave pública común incluye criptología de clave pública RSA, criptología de clave pública ElGamal, y criptología de curva elíptica.

(10). Criptología simétrica: La encriptación de clave simétrica también se denomina encriptación de clave dedicada. Para ser específicos, un remitente de datos y un receptor de datos usan necesariamente una misma clave para realizar operaciones de encriptación y desencriptación en un texto plano. Esto es, una clave de encriptación se puede deducir de una clave de desencriptación, y viceversa. En la mayoría de algoritmos simétricos, una clave de encriptación es la misma que la clave de desencriptación. Estos algoritmos también se denominan algoritmo de clave secreta o algoritmo de una clave, y requieren que un remitente y un receptor acuerden sobre una clave antes asegurar la comunicación. La seguridad de los algoritmos simétricos depende de la clave, y la filtración de la clave significa que cualquiera puede encriptar y desencriptar un mensaje. La clave tiene que mantenerse secreta siempre que la comunicación requiera confidencialidad.

De las descripciones anteriores acerca del algoritmo de clave simétrica y el algoritmo de clave asimétrica, se puede aprender lo siguiente: Se usa una misma clave para ambas de encriptación de clave simétrica y desencriptación de clave simétrica, o es fácil deducir una clave de desencriptación de una clave de encriptación. Adicionalmente, el algoritmo de clave simétrica tiene características tales como fácil procesamiento de encriptación, rápida encriptación y desencriptación, una clave relativamente corta, y una historia de desarrollo larga, y el algoritmo de clave asimétrica tiene características tales como lenta encriptación y desencriptación, una clave larga, y una historia de desarrollo corta.

(11). Se usa el protocolo de seguridad de capa de transporte (Transport Layer Security, TLS) para proporcionar confidencialidad e integridad de datos entre dos programas de aplicación. El protocolo incluye dos capas: el protocolo de registro de TLS (TLS Record) y el protocolo de saludo de TLS (TLS Handshake). El protocolo de seguridad de capa de transporte (TLS) se usa para garantizar la confidencialidad y la integridad de datos entre dos programas de aplicación de comunicaciones.

Primero, se proporciona un problema técnico que se tiene que resolver en esta solicitud y un escenario de aplicación. En la técnica anterior, un dispositivo convencional montado en vehículo se llama para mejora de firmware/software. Para ser específicos, un vehículo se llama a una ubicación especificada tal como un taller de reparación de automoción o un 4S Store, para mejorar firmware/software usando los siguientes métodos cuyas implementaciones específicas son la siguiente solución 1 y solución 2.

Solución 1: Usando una interfaz de grupo conjunto de acción de prueba (Joint Test Action Group, JTAG) o una interfaz de modo de depuración en segundo plano (Background Debugging Mode, BDM), realizar escritura online o realizar escritura después de desensamblar un dispositivo montado en vehículo. Específicamente, se puede incluir una manera 1 y una manera 2.

Manera 1: Primero descargar software a mejorar a un programador usando un ordenador personal (personal computer, PC), conectar el programador a un dispositivo de programación, colocar una placa de circuito impreso (Printed Circuit Board, PCB) de un sistema de control de vehículo electrónico en el dispositivo de programación y alinear la placa de circuito impreso con una interfaz de descarga, y finalmente encender el programador y escribir el software.

Manera 2: Conectar líneas de datos de descarga de programa de un PC y un microordenador de un chip a una PCB de un sistema de control de vehículo electrónico en serie, y utilizar el PC para descargar directamente un programa al microordenador de un chip.

La manera 1 y la manera 2 anteriores tienen problemas de requerir un experto en la técnica, costes más altos y operación bastante incómoda.

Solución 2: Realizar escritura flash en función de una diagnosis a bordo (On-Board Diagnostic, OBD) de un bus CAN.

Etapa 1. Entrar un modo de renovación de un estado de funcionamiento normal de programa de aplicación de un sistema de vehículo electrónico (interrupción o diagnosis por desencadenante).

Etapa 2. Comprobar una memoria de un chip de controlador de vehículo electrónico, y determinar si un programa de aplicación correcto está almacenado en la memoria.

Etapa 3. Si no hay programas de aplicación correctos en la memoria, descargar software de programa de aplicación de un dispositivo de diagnóstico, transmitir la software de programa de aplicación a través del bus CAN, y renovar un programa de aplicación en un flash (un módulo de renovación se configura para iniciar y guiar la escritura de software).

La solución 2 tiene problemas de requerir un experto en la técnica y un ciclo largo.

Además de la solución 1 y la solución 2 anteriores, actualmente, se implementa mejora remota para algunos vehículos. Sin embargo, la mejora remota se implementa generalmente principalmente para un dispositivo montado en vehículo que tiene una capacidad de computación relativamente fuerte y espacio de almacenamiento relativamente grande. En otras palabras, actualmente, un método de mejora seguro y eficiente de firmware/software no se puede proporcionar para un dispositivo montado en vehículo que tiene una capacidad de computación relativamente débil o espacio de almacenamiento relativamente pequeño. Por lo tanto, cómo implementar mejora segura y eficiente de firmware/software para dispositivos montados en vehículo a mejorar que tienen diferentes capacidades de mejora en un sistema montado en vehículo es un problema técnico que realmente se tiene que resolver en esta solicitud.

Para facilitar el entendimiento de las realizaciones de la presente invención, sobre la base de las descripciones anteriores, a continuación se describe primero una arquitectura de sistema de mejora montada en vehículo aplicada a las realizaciones de la presente invención. La FIGURA 1 es un diagrama de una arquitectura de mejora de sistema montado en vehículo (una arquitectura 1 por abreviar) según una realización de la presente invención. Un método de mejora de dispositivo montado en vehículo proporcionado en esta solicitud puede aplicarse a la arquitectura de sistema. La arquitectura de sistema incluye un servidor de mejoras, un dispositivo de control montado en vehículo, y una pluralidad de dispositivos montados en vehículo a mejorar tales como una HMI (human-machine interface, interfaz humano-máquina), un BMS (battery management system, sistema de gestión de batería), una ECU 1 y un ECU 2. El dispositivo de control montado en vehículo puede incluir una unidad de telemática y una unidad de orquestador de OTA (OTA Orchestrator) que se configuran para gestionar y ayudar en un proceso de mejora de la pluralidad de dispositivos montados en vehículo a mejorar. En la arquitectura de sistema, la mejora remota para un dispositivo montado en vehículo puede incluir los siguientes procesos básicos: liberación de paquete de mejora, obtención de paquete de mejora, transmisión en vehículo de paquete de mejora y mejora y confirmación.

El servidor de mejoras se configura para obtener un paquete de mejora montado en vehículo desencriptado de un desarrollador.

La telemática en el dispositivo de control montado en vehículo es responsable de la comunicación con el exterior. En esta solicitud, la telemática es responsable de comunicar con el servidor de mejoras y un servidor de claves, para implementar una tarea de obtener el paquete de mejora montado en vehículo y realizar algunas acciones de transmitir el paquete de mejora montado en vehículo (enviar el paquete de mejora montado en vehículo al orquestador de OTA).

El orquestador de OTA en el dispositivo de control montado en vehículo es responsable de la comunicación con los dispositivos montados en vehículo a mejorar en el vehículo. En esta solicitud, el paquete de mejora montado en vehículo pasa a través la telemática y una unidad/módulo de gestión, y finalmente llega en un dispositivo montado en vehículo a mejorar pretendido. Una función principal del orquestador de OTA es gestionar y ayudar en un proceso de mejora de los dispositivos montados en vehículo. Específicamente, el orquestador de OTA necesita tener las siguientes funciones: entrega y gestión de claves; gestión de proceso OTA; ayudar a otro dispositivo montado en vehículo a mejorar que tiene una capacidad más débil en una operación que requiere una gran carga de trabajo de computación, por ejemplo, verificar integridad y autenticidad de un paquete de mejora, o transcodificar (transcoding); y servir como nodo de respaldo de otro dispositivo montado en vehículo a mejorar que tiene una capacidad más débil, para restauración cuando falla la mejora. El orquestador de OTA es un entidad lógica y se puede desplegar físicamente en cualquier unidad o módulo potente tal como la telemática, una pasarela, o un VCU. Una estructura del orquestador de OTA puede mostrarse en la FIGURA 2. La FIGURA 2 es un diagrama estructural esquemático de un orquestador de OTA según una realización de la presente invención. El orquestador de OTA puede incluir una CPU de procesador, una memoria volátil RAM relacionada, una memoria no volátil ROM relacionada y un almacenamiento seguro configurado para almacenar una clave, por ejemplo, una clave estática que se comparte con un dispositivo montado en vehículo. El orquestador de OTA incluye además una memoria configurada para almacenar un programa de gestión OTA, y el programa de gestión OTA se usa para gestionar un proceso de mejora; e incluye además una interfaz de red que puede comunicar con otro dispositivo montado en vehículo a través de un bus CAN u otra red en vehículo. Se puede entender que, si el orquestador de OTA se implementa en la telemática, el orquestador de OTA requiere además una interfaz de red para comunicar con una red externa. Esto es, el orquestador de OTA necesita tener una capacidad de computación relativamente fuerte y una cantidad de recursos relativamente grande, para ayudar a un dispositivo montado en vehículo a completar mejora remota y ser de confianza para otro dispositivo montado en vehículo. Desde el punto de vista de división de arquitectura lógica, el orquestador de OTA divide la arquitectura en una parte de comunicación fuera del vehículo y una parte de comunicación en el vehículo. Dispositivos de la parte en el vehículo tienen que realizar únicamente una operación de criptología simétrica, en vez de una operación de criptología de clave pública. Si se tiene que realizar una operación de clave pública, la operación de clave pública se asigna al orquestador de OTA, para reducir la carga de trabajo de computación y la complejidad de computación de un dispositivo a mejorar en el vehículo.

Para los dispositivos montados en vehículo a mejorar, una composición de uno cualquiera de los dispositivos montados en vehículo a mejorar puede mostrarse en la FIGURA 3. La FIGURA 3 es un diagrama estructural esquemático de un dispositivo montado en vehículo a mejorar según una realización de la presente invención. El dispositivo montado en vehículo a mejorar puede incluir un microcontrolador (Micro controller), un controlador de CAN (CAN controller), y un transceptor (Transceiver). El dispositivo montado en vehículo a mejorar se comunica con una red en vehículo tal como un bus CAN usando el transceptor (transceiver). El controlador de CAN se configura para implementar el protocolo de CAN, y el microcontrolador se configura para implementar procesamiento de computación relacionado antes y después de la mejora. Por ejemplo, el microcontrolador puede implementar un método de mejora de dispositivo montado en vehículo realizado por el dispositivo montado en vehículo a mejorar en esta solicitud. Con referencia al diagrama estructural esquemático anterior, en esta solicitud, un dispositivo montado en vehículo a mejorar pretendido recibe, en función de la red en vehículo tal como el bus CAN usando un transceptor (Transceiver), un archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo, y realiza mejora segura usando el archivo de mejora pretendido y el microcontrolador (Micro Controller). Para una función más específica, consúltense descripciones acerca de una función relacionada con el dispositivo montado en vehículo a mejorar en subsiguientes realizaciones.

Del diagrama estructural esquemático del dispositivo montado en vehículo a mejorar se puede aprender que el bus CAN se usa comúnmente en vehículos actuales, pero el bus CAN afecta al ancho de banda. En consecuencia, en algunos escenarios de mejora, no se puede lograr la máxima eficiencia de mejora para mejora remota de firmware/software para un dispositivo montado en vehículo.

La FIGURA 4 es otro diagrama de una arquitectura de mejora de sistema montado en vehículo (una arquitectura 2 por abreviar) según una realización de la presente invención. A diferencia de la arquitectura de mejora de sistema proporcionada en la FIGURA 1, esta arquitectura de mejora de sistema montado en vehículo incluye además un servidor de claves.

Un servidor de mejoras se configura para obtener, de un desarrollador, un paquete de mejora montado en vehículo encriptado por el desarrollador.

El servidor de claves se configura para: cuando el paquete de mejora montado en vehículo se encripta por el desarrollador, obtener una clave del desarrollador a través de un canal seguro, almacenar la clave, y finalmente proporcionar la clave a un dispositivo de control montado en vehículo.

Se puede entender que, para otros aspectos tales como funciones específicas del dispositivo de control montado en vehículo y una pluralidad de dispositivos montados en vehículo a mejorar, consúltense descripciones acerca de entidades de función o unidades en la arquitectura de mejora de sistema montado en vehículo correspondientes a la FIGURA 1. En esta memoria no se describen de nuevo detalles.

Se puede entender además que, la arquitectura de mejora de sistema montado en vehículo en esta solicitud puede incluir además el desarrollador. Después de desarrollar y probar un programa de mejora (firmware/software), el desarrollador entrega el paquete de mejora montado en vehículo al servidor de mejoras. El paquete de mejora montado en vehículo entregado tiene que firmarse usando una firma digital. Opcionalmente, antes de ser firmado usando la firma digital, el paquete de mejora montado en vehículo puede además encriptarse. Si el paquete de mejora montado en vehículo no se encripta, la arquitectura es la arquitectura de sistema de la FIGURA 1; si el paquete de mejora montado en vehículo se encripta, la arquitectura es la arquitectura de sistema de la FIGURA. 2. Correspondientes realizaciones se tienen que detallar en las siguientes descripciones.

Cabe señalar que, la arquitecturas de mejora de sistema montado en vehículo en la FIGURA 1 y la FIGURA 2 son meramente dos ejemplos de implementaciones de las realizaciones de la presente invención. Una arquitectura de sistema de comunicaciones en las realizaciones de la presente invención incluye, pero no se limita a esto, las anteriores arquitecturas de sistema.

A continuación se analiza específicamente y resuelve el problema técnico proporcionado en esta solicitud usando realizaciones del método de mejora de dispositivo montado en vehículo proporcionado en esta solicitud.

La FIGURA 5 es un diagrama de flujo esquemático de un método de mejora de dispositivo montado en vehículo según una realización de la presente invención. El método puede aplicarse a la arquitectura de mejora de sistema montado en vehículo en la FIGURA 1 o la FIGURA 4. Con referencia a la FIGURA 5, a continuación se describe el método desde una perspectiva de interacción entre un dispositivo de control montado en vehículo y un dispositivo montado en vehículo a mejorar pretendido. El método puede incluir las etapas S501 a S505.

Etapa S501. El dispositivo de control montado en vehículo obtiene un paquete de mejora montado en vehículo.

Etapa S502. El dispositivo de control montado en vehículo realiza verificación de seguridad en una pluralidad de archivos de mejora.

Etapa S503. El dispositivo de control montado en vehículo envía un archivo de mejora pretendido al dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora.

Etapa S504. El dispositivo montado en vehículo a mejorar pretendido recibe el archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad realizada por el dispositivo de control montado en vehículo y que se utiliza para mejorar el dispositivo montado en vehículo a mejorar.

Etapa S505. El dispositivo montado en vehículo a mejorar pretendido realiza mejora segura usando el archivo de mejora pretendido.

Específicamente, el paquete de mejora montado en vehículo incluye la pluralidad de archivos de mejora, y cada archivo de mejora se usa para mejorar al menos un dispositivo montado en vehículo a mejorar. En otras palabras, un dispositivo montado en vehículo a mejorar en un sistema montado en vehículo puede corresponder a uno o más archivos de mejora.

Antes de que el dispositivo de control montado en vehículo realice la etapa S501, el paquete de mejora montado en vehículo se libera. Generalmente, después de desarrollar y probar un programa de mejora, un desarrollador del paquete de mejora montado en vehículo (firmware/software) entrega el paquete de mejora montado en vehículo a un servidor de mejoras. En una implementación posible, el paquete de mejora montado en vehículo incluye una primera firma digital. Se asume que el paquete de mejora montado en vehículo es M e información de versión es ver (por ejemplo, toda información de metadatos (meta-data) tal como un nombre de programa, un número de versión nueva y un número de versión antigua). En esta realización de la presente invención, las siguientes dos maneras de firma digital se pueden proporcionar durante la liberación del paquete de mejora montado en vehículo: el desarrollador firma digitalmente el paquete de mejora, o el servidor de mejoras firma digitalmente el paquete de mejora, como se muestra en la FIGURA 6. La FIGURA 6 es un diagrama esquemático de dos tipos de firmas digitales según una realización de la presente invención. Se incluye un caso 1 y un caso 2.

Caso 1: $\sigma=Sign_D(M||ver)$ indica que el desarrollador firma digitalmente M||ver, y sirve como primera firma digital en esta solicitud.

Caso 2: $\sigma=Sign_S(M||ver)$ indica que el servidor de mejoras firma digitalmente M||ver, y sirve como primera firma digital en esta solicitud.

Un algoritmo firma digital usado en los dos maneras anteriores de firmar no se limita específicamente en esta solicitud. Opcionalmente, un canal seguro puede establecerse entre el desarrollador y el servidor de mejoras para transferir información, y el canal seguro puede ser un canal de red o puede ser un canal físico tal como una carta registrada. En conclusión, cuando se libera el paquete de mejora montado en vehículo, el servidor de mejoras actualiza el paquete de mejora montado en vehículo [M, ver, σ], y libera externamente información acerca de un paquete de mejora montado en vehículo actualizado o nuevo.

Esta solicitud proporciona dos arquitecturas de mejora de sistema montado en vehículo: la arquitectura 1 sin un servidor de claves mostrado en la FIGURA 1, y una arquitectura 2 que incluye un servidor de claves mostrado en la FIGURA 4.

En la arquitectura 1, el paquete de mejora montado en vehículo no se encripta. El servidor de mejoras necesita realizar autenticación en información de identidad del dispositivo de control montado en vehículo, establecer un canal seguro al dispositivo de control montado en vehículo después de que la autenticación tiene éxito, y obtener el paquete de mejora montado en vehículo a través del canal seguro. El proceso es un proceso en el que un orquestador de OTA en el dispositivo de control montado en vehículo obtiene un paquete de mejora del servidor de mejoras usando una unidad de telemática.

Específicamente, el dispositivo de control montado en vehículo envía información de autenticación de identidad al servidor de mejoras. Si la información de autenticación de identidad es autenticada por el servidor de mejoras, el canal seguro se establece entre el dispositivo de control montado en vehículo y el servidor de mejoras; y el dispositivo de control montado en vehículo obtiene, del servidor de mejoras a través del canal seguro, el paquete de mejora montado en vehículo que se requiere para mejora.

En una implementación específica, el orquestador de OTA consulta al servidor de mejoras, o el servidor de mejoras empuja un mensaje de actualización al orquestador de OTA. El paquete de mejora puede obtenerse específicamente en las siguientes etapas.

1. El orquestador de OTA (OTA orchestrator) obtiene información de versión actual del dispositivo montado en vehículo a mejorar pretendido. La información puede obtenerse consultando el dispositivo montado en vehículo a mejorar pretendido o consultando una base de datos mantenida por el orquestador de OTA (se asume que el orquestador de OTA mantiene información básica de firmware/software de todos los dispositivos montados en vehículo).
2. El orquestador OTA determina si se requiere mejora. Si se requiere mejora, el orquestador de OTA puede elegir avisar al propietario de un vehículo para realizar la mejora. Si el propietario de vehículo acepta, la mejora procede.
3. El orquestador de OTA inicia autenticación al servidor de mejoras, establece un canal seguro al servidor de mejoras, y transmite un paquete de datos a través del canal seguro.
4. El orquestador de OTA informa la información de versión actual del dispositivo montado en vehículo al servidor de mejoras, y si el servidor de mejoras acepta, el orquestador de OTA descarga un paquete de mejora [M, ver, σ, {M'}]. M es el paquete de mejora montado en vehículo; ver representa información de versión, que incluye toda información de metadatos (meta-data) tal como un nombre de programa, un número de nueva versión, y un correspondiente número de versión antigua; $\sigma=Sign_D(M||ver)$ o $\sigma=Sign_S(M||ver)$ es la primera firma digital, y M' representa un archivo de restauración; y {M'} indica que M' es opcional y es eficaz únicamente cuando el dispositivo montado en vehículo a mejorar pretendido es un dispositivo de capacidad débil.
5. El orquestador de OTA realiza verificación sobre autenticidad de la primera firma digital σ, y si falla la verificación, el orquestador de OTA abandona la mejora. Opcionalmente, si es necesario, el orquestador de OTA también realiza verificación en M'. Se asume que M' también lleva una firma digital.

En la arquitectura 2, el paquete de mejora montado en vehículo se encripta en el servidor de mejoras. Por lo tanto, puede no ser necesario establecer un canal seguro dedicado entre el dispositivo de control montado en vehículo y el servidor de mejoras. Adicionalmente, después de que el dispositivo de control montado en vehículo realiza verificación en el paquete de mejora montado en vehículo usando la primera firma, el paquete de mejora montado en vehículo además tiene que desencriptarse usando una primera clave. En esta realización, los archivos de mejora se encriptan por el desarrollador. Un beneficio adicional de encriptar los archivos de mejora por el desarrollador es que el desarrollador no necesita considerar la credibilidad del servidor de mejoras. Por lo tanto, se protege aún más la confidencialidad de los archivos de mejora.

Específicamente, el paquete de mejora montado en vehículo se encripta usando la primera clave. La primera clave es una clave simétrica. El dispositivo de control montado en vehículo obtiene la primera clave del servidor de claves. Después de que el dispositivo de control montado en vehículo realiza verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital, si tiene éxito la verificación de firma digital, el dispositivo de control montado en vehículo desencripta la pluralidad de archivos de mejora usando la primera clave.

Después de desarrollar y probar un programa de mejora, el desarrollador del paquete de mejora montado en vehículo (firmware/software) entrega los archivos de mejora al servidor de mejoras. Este proceso es correspondiente a la arquitectura mostrada en la FIGURA 4. A diferencia de la arquitectura 1, esta arquitectura necesita un servidor de claves adicional.

Se asume que los archivos de mejora son M y ver representa información de versión, que incluye toda información de metadatos (meta-data) tal como un nombre de programa, un número de versión nueva, y un correspondiente número de versión antigua. El desarrollador selecciona cualquier clave K (la primera clave), y encripta M usando K, de modo que se obtiene C=E(K, M). En esta memoria E(K, .) representa encriptación basada en K, por ejemplo, encriptación de grupo.

Como se ha descrito anteriormente, para la primera firma digital, hay dos escenarios: el desarrollador firma digitalmente el paquete de mejora, o el servidor de mejoras firma digitalmente el paquete de mejora. En ambos casos, el desarrollador necesita enviar la clave K de los archivos de mejora encriptados al servidor de claves a través de un canal seguro, y el canal para transmitir los archivos de mejora encriptados no requiere protección. Un canal secreto entre el desarrollador y el servidor de claves puede establecerse usando muchos métodos, por ejemplo, usando la TLS. Esto no se limita específicamente en esta solicitud.

En una implementación específica, el proceso es un proceso en el que el orquestador de OTA obtiene un paquete de mejora del servidor de mejoras y obtiene, del servidor de claves, una clave para desencriptar software de mejora. Específicamente, después de enterarse de que hay un nuevo paquete de mejora para un dispositivo montado en vehículo, el orquestador de OTA inicia el proceso. El orquestador de OTA puede aprender el mensaje consultando el servidor de mejoras o el servidor de mejoras empuja información al orquestador de OTA. El paquete de mejora puede obtenerse en las siguientes etapas.

1. El orquestador de OTA obtiene información de versión actual del dispositivo montado en vehículo a mejorar pretendido. La información puede obtenerse consultando el dispositivo montado en vehículo a mejorar pretendido o consultando una base de datos mantenida por el orquestador de OTA (se asume que el orquestador de OTA mantiene información básica de firmware/software de todos los dispositivos montados en vehículo).
2. El orquestador OTA determina si se requiere mejora. Si se requiere mejora, el orquestador de OTA puede elegir avisar al propietario de un vehículo para realizar la mejora. Si el propietario de vehículo acepta, la mejora procede.
3. El orquestador de OTA descarga un paquete de mejora [C, ver, σ, {C'}] del servidor de mejoras. Cabe señalar que C′ representa un archivo firmado encriptado usando una firma digital y para ser usado para restauración cuando falla la mejora; y {C'} indica que C′ es opcional y es eficaz únicamente cuando el dispositivo montado en vehículo a mejorar pretendido es un dispositivo de capacidad débil.
4. El orquestador de OTA realiza verificación sobre autenticidad de σ (esto es, realizar verificación sobre autenticidad de la primera firma digital), y si falla la verificación, el orquestador de OTA abandona la mejora. Si es necesario, el orquestador de OTA también realiza verificación sobre C′.
5. El orquestador de OTA inicia autenticación al servidor de claves, establece un canal seguro al servidor de claves, y obtiene una clave de desencriptación K (esto es, la primera clave) del paquete de mejora a través del canal seguro. Si es necesario, el orquestador de OTA también necesita obtener una clave de desencriptación para desencriptar C′.
6. El orquestador de OTA desencripta C usando K para obtener los archivos de mejora M; y si es necesario, el orquestador de OTA también necesita desencriptar C′ para obtener M' (M' es un archivo usado para restauración cuando falla la mejora).

En una implementación posible, si también tiene que protegerse la confidencialidad de los archivos de mejora, después de obtener el paquete de mejora, el orquestador de OTA no desencripta C pero divide C en n partes: C_1, C_2..., y C_n, y entonces usa C_1, C_2..., y C_n en subsiguientes métodos de procesamiento que son en función de una cadena de hash, un árbol de hash, y un filtro de Bloom. El orquestador de OTA también necesita transferir la clave K compartida al dispositivo montado en vehículo a mejorar pretendido a través de un canal secreto, de modo que el dispositivo montado en vehículo a mejorar pretendido realiza desencriptación.

En la etapa S502, el dispositivo de control montado en vehículo necesita realizar verificación de seguridad en la pluralidad de archivos de mejora en el paquete de mejora montado en vehículo obtenido del servidor de mejoras. En una implementación posible, el paquete de mejora montado en vehículo incluye la primera firma digital, y el orquestador de OTA del dispositivo de control montado en vehículo realiza verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital. Para ser específicos, después de que el dispositivo de control montado en vehículo obtiene el paquete de mejora montado en vehículo, a diferencia de la técnica anterior en la que un paquete de mejora se envía directamente a un correspondiente dispositivo montado en vehículo a mejorar para mejora, primero se realiza verificación de seguridad (por ejemplo, verificación de autenticidad) en la pluralidad de archivos de mejora en el paquete de mejora montado en vehículo en un lado de dispositivo de control montado en vehículo, un archivo de mejora en el que tiene éxito la verificación de seguridad se somete entonces a transcodificación (transcoding), y un archivo de mejora transcodificado se envía a un correspondiente dispositivo montado en vehículo a mejorar para mejora segura. Cabe señalar que, la transcodificación en esta solicitud significa que se realiza procesamiento de asociación hash, usando un algoritmo (un algoritmo de cadena de hash, un algoritmo de árbol de hash, o un algoritmo de filtro de Bloom), en cada uno de una pluralidad de subarchivos de mejora obtenido a través de división, y se realiza procesamiento de MAC en uno o más nodos en una cadena de hash, un árbol de hash o un filtro de Bloom, para implementar además transmisión segura de segmento de paquete de datos que es aplicable a una red en vehículo. De esta manera, disminuye una gran cantidad de operaciones de verificación de seguridad que tienen que ser realizadas por el dispositivo montado en vehículo a mejorar. En otras palabras, carga de trabajo de computación, complejidad de computación y similares disminuyen durante la verificación de seguridad realizada por un único dispositivo montado en vehículo a mejorar.

En la etapa S503, diferentes dispositivos montados en vehículo a mejorar pueden corresponder a únicamente algunos archivos de mejora en el paquete de mejora montado en vehículo. Por lo tanto, el dispositivo de control montado en vehículo necesita enviar el archivo de mejora pretendido en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora al dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido. Se puede entender que tamaños y contenido de subarchivos de mejora en el archivo de mejora pretendido pueden ser diferentes.

En una implementación posible, el dispositivo de control montado en vehículo divide el archivo de mejora pretendido en una pluralidad de subarchivos de mejora (que también pueden entenderse como pluralidad de segmentos); genera una pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y genera un primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando una segunda clave; y envía secuencialmente, al dispositivo

montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC. La segunda clave es una clave de algoritmo simétrica.

Específicamente, durante la transmisión del paquete de mejora montado en vehículo entre dispositivos montados en vehículo, el dispositivo de control montado en vehículo divide, usando un algoritmo preestablecido, un archivo de mejora en una pluralidad de bloques de datos asociados, y realiza procesamiento de MAC en los bloques de datos asociados, de modo que el dispositivo de control montado en vehículo divide un archivo de mejora completo en una pluralidad de bloques de datos que se pueden transmitir por separado y en los que se puede realizar por separado verificación de validez. Adicionalmente, como la pluralidad de bloques de datos se asocian, un bloque de datos que tiene un problema de seguridad se puede localizar rápidamente usando un algoritmo relacionado. El algoritmo preestablecido incluye uno cualquiera del algoritmo de cadena de hash, el algoritmo de árbol de hash, y el algoritmo de filtro de Bloom. En esta solicitud, el dispositivo de control montado en vehículo divide el archivo de mejora pretendido en la pluralidad de subarchivos de mejora para evitar enviar el archivo de mejora pretendido al dispositivo montado en vehículo a mejorar de uno en uno, de modo que el dispositivo montado en vehículo a mejorar puede por separado recibir y proceso los subarchivos de mejora. Por lo tanto, "secuencialmente" en esta solicitud puede incluir "uno después otro", o puede indicar "una pluralidad de subarchivos de mejora después de otra pluralidad de subarchivos de mejora", por ejemplo, primero enviar dos subarchivos de mejora, luego enviar otros dos subarchivos de mejora, etc.; o puede indicar primero enviar un subarchivo de mejora, luego enviar otro dos subarchivos de mejora, etc. Esto es, el dispositivo de control montado en vehículo meramente necesita dividir el archivo de mejora pretendido en una pluralidad de subarchivos de mejora y enviar los subarchivos de mejora al dispositivo montado en vehículo a mejorar en lotes. Una manera específica de dividir el archivo de mejora pretendido y enviar secuencialmente los subarchivos de mejora al dispositivo montado en vehículo a mejorar no se limita específicamente en esta solicitud. En esta solicitud, para resolver problemas de una capacidad débil e insuficientes recursos de almacenamiento de un dispositivo montado en vehículo y ancho de banda de red en vehículo limitado, el orquestador de OTA desplegado es capaz de transcodificar (transcoding) el paquete de mejora montado en vehículo. Con la función de transcodificación del orquestador de OTA, el dispositivo montado en vehículo no necesita realizar una operación de criptología de clave pública, reduciendo de ese modo la carga de trabajo del dispositivo montado en vehículo. Por lo tanto, disminuye la carga de trabajo de computación y la complejidad de computación en una unidad de tiempo para un dispositivo montado en vehículo a mejorar que tiene una capacidad relativamente débil. Adicionalmente, después de que ocurre un error de transmisión de archivo de mejora, una parte de error se puede encontrar tan rápidamente como sea posible, de modo que únicamente se solicita retransmitir la parte de error en vez del archivo de mejora entero. De esta manera, se garantiza además una mejora segura y eficiente para el dispositivo montado en vehículo.

En una implementación posible, el dispositivo de control montado en vehículo divide el archivo de mejora pretendido en una pluralidad de subarchivos de mejora, encripta (para garantizar confidencialidad) y transcodifica (para garantizar la autenticidad) la pluralidad de subarchivos de mejora, y envía secuencialmente subarchivos de mejora encriptados y transcodificados al dispositivo montado en vehículo a mejorar pretendido. Específicamente, el dispositivo de control montado en vehículo encripta cada uno de la pluralidad de subarchivos de mejora usando una tercera clave, genera, usando el algoritmo preestablecido, la pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora que se encriptan usando la tercera clave, y envía secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC. En otras palabras, esta realización de la presente invención difiere de la realización anterior de la presente invención en que el dispositivo de control montado en vehículo necesita encriptar la pluralidad de subarchivos de mejora antes de transcodificar, para garantizar la confidencialidad de la pluralidad de subarchivos de mejora, y entonces transcodifica los subarchivos de mejora encriptados.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora, una pluralidad de bloques de datos asociados mutuamente se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y la pluralidad de subarchivos de mejora llevan una segunda firma digital de la pluralidad de bloques de datos que se genera usando una cuarta clave, donde la cuarta clave es una clave asimétrica; el dispositivo de control montado en vehículo comprueba la segunda firma digital de la pluralidad de bloques de datos; el dispositivo de control montado en vehículo genera un segundo MAC de la pluralidad de bloques de datos usando una quinta clave, donde la quinta clave es una clave de algoritmo simétrica; y el dispositivo de control montado en vehículo envía secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el segundo MAC. En otras palabras, puede implementarse transmisión de bloque y firma del paquete de mejora montado en vehículo en un lado de desarrollador de mejora. Esto es, antes de obtenerse por el dispositivo de control montado en vehículo, se obtienen bloques de datos a través de división usando un algoritmo preestablecido y firmado. En este caso, el dispositivo montado en vehículo necesita comprobar primero la validez de los bloques de datos, y entonces realiza procesamiento de MAC en bloques de datos comprobados como válidos. La carga de trabajo de computación y la complejidad de computación en la comprobación de MAC son mucho menores que los de un caso de firma. Por lo tanto, la carga de trabajo de computación y la complejidad de computación del dispositivo montado en vehículo a mejorar pueden disminuir mientras se garantiza la validez del archivo de mejora

montado en vehículo en un proceso de transmisión en vehículo. Por lo tanto, el dispositivo montado en vehículo se mejora de manera segura y eficientemente.

En la etapa S504, el dispositivo montado en vehículo a mejorar pretendido recibe el archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo. El archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad realizada por el dispositivo de control montado en vehículo y que se utiliza para mejorar al menos el dispositivo montado en vehículo a mejorar pretendido. Específicamente, este proceso es un proceso de transmisión segura en vehículo del paquete montado en vehículo.

En la etapa S505, el dispositivo montado en vehículo a mejorar pretendido realiza mejora segura usando el archivo de mejora pretendido. En una implementación posible, cuando el dispositivo montado en vehículo a mejorar es un primer dispositivo montado en vehículo a mejorar cuya capacidad de almacenamiento de recursos y/o capacidad de procesamiento supera un valor preestablecido o un primer dispositivo montado en vehículo a mejorar que se especifica por adelantado, por ejemplo, un dispositivo que tiene una capacidad de procesamiento relativamente fuerte o una capacidad de almacenamiento relativamente fuerte, o un dispositivo especificado, un modo de mejora de actualizaciones de sistema A/B (A/B System Updates) se usa para el dispositivo montado en vehículo a mejorar pretendido. Para ser específicos, el dispositivo montado en vehículo a mejorar pretendido tiene un región A y un región B, un programa a mejorar (firmware o software) se ejecuta en la región A y un nuevo programa de mejora se escribe en la región B, y el programa se ejecuta en la región B después de completarse la mejora. Esto no afecta al funcionamiento normal de un sistema de versión antigua en un proceso de mejora montado en vehículo. Por ejemplo, un dispositivo de fuerte capacidad o un dispositivo de clave usa un método de mejora de actualizaciones de sistema A/B; un dispositivo de capacidad débil usa el orquestador de OTA como nodo de respaldo, para realizar restauración cuando la mejora falla. Cuando la mejora tiene éxito, el dispositivo montado en vehículo borra el paquete de mejora y notifica al orquestador de OTA. El orquestador de OTA borra el paquete de mejora, actualiza la base de datos, y notifica al propietario del vehículo de la mejora exitosa. Como alternativa, el orquestador de OTA puede elegir notificar al servidor de mejoras. Adicionalmente, el orquestador de OTA puede además elegir ordenar al dispositivo montado en vehículo a mejorar pretendido que realice testimonio remoto, para testimoniar que la mejora tiene éxito.

En una implementación posible, el dispositivo montado en vehículo a mejorar pretendido recibe secuencialmente la pluralidad de bloques de datos que llevan el primer MAC y que son enviados por el dispositivo de control montado en vehículo. La pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, el primer MAC es un código de autenticación de mensaje de la pluralidad de bloques de datos que se genera usando una segunda clave, y la segunda clave es una clave simétrica. En otras palabras, la segunda clave es una clave compartida. Por lo tanto, únicamente se tiene que realizar verificación de autenticidad entre el dispositivo a mejorar pretendido y el dispositivo de control montado en vehículo usando la clave simétrica simple. Esto reduce la carga de trabajo de computación y la complejidad de computación del dispositivo a mejorar pretendido. De esta manera, una mejora segura y eficiente puede requerir únicamente una carga de trabajo de computación relativamente pequeña y una complejidad de computación relativamente baja incluso para un dispositivo "débil" montado en vehículo a mejorar que tiene una capacidad de computación relativamente débil o espacio de almacenamiento relativamente pequeño.

En una implementación posible, el dispositivo montado en vehículo a mejorar pretendido realiza secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; y cuando se verifican todos de la pluralidad de bloques de datos, el dispositivo montado en vehículo a mejorar pretendido combina la pluralidad de bloques de datos verificados secuencialmente para mejora. Para ser específicos, después de recibir la pluralidad de subarchivos de mejora que se encriptan usando la segunda clave, transcodificados usando el algoritmo preestablecido, y enviados por el dispositivo de control montado en vehículo, el dispositivo a mejorar pretendido necesita comprobar el primer MAC usando la segunda clave, y realiza comprobación de valor de asociación en la pluralidad de bloques de datos usando un rasgo de los bloques de datos asociados mutuamente generados usando el algoritmo preestablecido. Después de que se decodifican y verifican todos los bloques de datos, esto es, la verificación en todas los bloques de datos tiene éxito, el dispositivo a mejorar pretendido combina la pluralidad de subarchivos de mejora en un archivo completo para mejora.

En una implementación posible, la pluralidad de subarchivos de mejora se encriptan usando una tercera clave; cuando se verifican todos de la pluralidad de bloques de datos, el dispositivo montado en vehículo a mejorar pretendido desencripta cada uno de la pluralidad de bloques de datos verificados secuencialmente usando la tercera clave; y el dispositivo montado en vehículo a mejorar pretendido combina la pluralidad de bloques de datos que se desencriptan usando la tercera clave para mejora. En otras palabras, esta realización de la presente invención difiere de la realización anterior de la presente invención en que el dispositivo montado en vehículo a mejorar pretendido necesita realizar verificación en los subarchivos de mejora encriptados y transcodificados antes de desencriptar la pluralidad de subarchivos de mejora que se verifican, y combina la pluralidad de subarchivos de mejora para mejora después de que la desencriptación tiene éxito.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora; y el dispositivo montado en vehículo a mejorar pretendido secuencialmente recibe la pluralidad de bloques de datos que llevan el segundo MAC y que son enviados por el dispositivo de control montado en vehículo. La pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando el algoritmo preestablecido, el segundo MAC es un código de autenticación de mensaje de la pluralidad de bloques de datos que se genera usando una quinta clave, y la quinta clave es un algoritmo simétrico. El dispositivo montado en vehículo a mejorar pretendido realiza secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la quinta clave; y cuando se verifican todos de la pluralidad de bloques de datos, el dispositivo montado en vehículo a mejorar pretendido combina la pluralidad de bloques de datos verificados secuencialmente para mejora. En otras palabras, puede implementarse transmisión de bloque y firma del paquete de mejora montado en vehículo en un lado de desarrollador de mejora. Esto es, antes de obtenerse por el dispositivo de control montado en vehículo, se obtienen bloques de datos a través de división usando un algoritmo preestablecido y firmado. En este caso, el dispositivo montado en vehículo necesita comprobar primero la validez de los bloques de datos, y entonces realiza procesamiento de MAC en bloques de datos comprobados como válidos. La carga de trabajo de computación y la complejidad de computación en la comprobación de MAC son mucho menores que los de firma. Por lo tanto, la carga de trabajo de computación y la complejidad de computación del dispositivo montado en vehículo a mejorar pueden disminuir mientras se garantiza la validez del archivo de mejora montado en vehículo en un proceso de transmisión en vehículo. Por lo tanto, el dispositivo montado en vehículo se mejora de manera segura y eficientemente.

Además, cuando el dispositivo montado en vehículo a mejorar pretendido realiza una operación de mejora, si falla la verificación en un bloque de datos pretendido en la pluralidad de bloques de datos en el dispositivo montado en vehículo a mejorar pretendido, el dispositivo de control montado en vehículo retransmite el bloque de datos pretendido al dispositivo montado en vehículo a mejorar pretendido. En otras palabras, el dispositivo montado en vehículo a mejorar pretendido vuelve a obtener el bloque de datos pretendido del dispositivo de control montado en vehículo. Combinación y mejora se realizan únicamente cuando se verifican todos los bloques de datos. En esta realización de la presente invención, como el archivo de mejora pretendido se divide en una pluralidad de bloques de datos, cuando falla la verificación en uno o más bloques de datos, únicamente se tiene que descargar de nuevo el uno o más bloques de datos en lugar del archivo de mejora entero pretendido, reduciendo de ese modo sobrecargas y mejorando la eficiencia de mejora.

A continuación se describe la verificación de autenticidad entre el dispositivo de control montado en vehículo y el dispositivo a mejorar pretendido, esto es, cómo el dispositivo de control montado en vehículo transcodifica el archivo de mejora pretendido del paquete de mejora montado en vehículo usando un algoritmo preestablecido.

En una implementación específica, después de verificar la autenticidad del paquete de mejora montado en vehículo, el orquestador de OTA empieza el proceso en un momento apropiado, por ejemplo, en un estado estacionado, o el orquestador de OTA puede elegir pedir al propietario del vehículo que confirme la mejora de nuevo. El orquestador de OTA realiza división y procesamiento de transcodificación en el paquete de mejora montado en vehículo, y transfiere secuencialmente subarchivos de mejora transcodificados al dispositivo montado en vehículo a mejorar pretendido. Esta solicitud proporciona tres métodos de transcodificación independientes: una solución basada en cadena de hash, una solución basada en árbol de hash y una solución basada en filtro de Bloom. A continuación se describen procesos de transmisión en vehículo de paquete de mejora en función de los tres métodos de transcodificación. Primero, se asume que el orquestador de OTA comparte una clave k con el dispositivo montado en vehículo a mejorar pretendido. La k compartida puede ser estática o puede ser generada temporalmente por el orquestador de OTA y el dispositivo montado en vehículo a mejorar pretendido.

Método 1: Método de transcodificación basado en cadena de hash

1. El orquestador de OTA divide un archivo de mejora M en n partes: M_1, M_2..., y M_n.
2. Forma una cadena de hash usando M_1, M_2..., y M_n de la siguiente manera, donde H(.) representa una función hash criptográfica:

$$h_n=H(M_n)$$

$$h_i=H(M_i, h_{i+1})$$

$$h_2=H(M_2, h_3)$$

3. El orquestador OTA calcula v=MAC(k, M_1||ver, h_2) usando la clave compartida k (la segunda clave). En esta memoria, el MAC es un código de autenticación de mensaje (message authentication code) estándar, es decir, el primer MAC.

4. Empezando desde la primera parte, el orquestador de OTA transfiere secuencialmente M_i al dispositivo montado en vehículo a mejorar pretendido. Para la primera parte, el orquestador de OTA necesita transferir v, M_1, ver, y h_2; para las partes restantes, el orquestador de OTA necesita transferir únicamente M_i y h_{i+1}.
5. El dispositivo montado en vehículo a mejorar pretendido realiza secuencialmente verificación en M_i usando la clave compartida k. Si falla la verificación en una parte, el dispositivo montado en vehículo a mejorar pretendido puede pedir retransmisión. Después de recibir y verificar todas las partes, el dispositivo montado en vehículo a mejorar pretendido combina todas las partes en el archivo de mejora completo M.

Método 2: Método de transcodificación basado en árbol triple

1. El orquestador de OTA divide un archivo de mejora M en n partes: M_1, M_2..., y M_n.
2. Forma un árbol binario usando M_1, M_2..., y M_n. Como se muestra en la figura: un nodo hoja representa datos, cada nodo intermedio incluye un valor de un nodo de raíz que puede obtenerse en función de un valor de un subnodo del nodo intermedio usando hash, por ejemplo, $h_1=H(M_1||ver||M_2)$, y $h_5=H(h_1||h_2)$.
3. El orquestador de OTA calcula el valor del nodo de raíz usando la clave compartida k (la segunda clave). Como se muestra en la figura, por ejemplo, $v=MAC(k, h_5||h_6)$, es decir, el primer MAC.
4. Empezando desde M_1 y M_2, el orquestador de OTA transfiere dos partes al dispositivo montado en vehículo a mejorar pretendido cada vez. Para las primeras dos partes, el orquestador de OTA necesita transferir v, $M_1||ver$, M_2, h_2, y h_6; para las partes restantes, el orquestador de OTA necesita transferir dos pedazos de datos y datos de verificación de asistente correspondiente a los dos pedazos de datos. En la figura, datos de verificación de asistente de M_1 y M_2 son h_2 y h_6; datos de verificación de asistente de M_3 y M_4 están en blanco, porque la verificación en M_3 y M_4 se puede realizar usando h_2; datos de verificación de asistente de M_5 y M_6 son h_4; y datos de verificación de asistente de M_7 y M_8 están en blanco.
5. El dispositivo montado en vehículo a mejorar pretendido realiza verificación en una de cada dos partes usando la clave compartida k. Si la verificación en dos partes falla, el dispositivo montado en vehículo a mejorar pretendido puede pedir retransmisión. Después de recibir y verificar todas las partes, el dispositivo montado en vehículo a mejorar pretendido combina todas las partes en el archivo de mejora completo M.

Método 3: Método de transcodificación basado en filtro de bloom

Un filtro de Bloom es una estructura de datos eficiente en almacenamiento que se utiliza para determinar si datos existen datos en un conjunto. Un ejemplo es de la siguiente manera:

Se establece una distribución F (filtro de Bloom) con una longitud de ℓ, en la que un valor de cada elemento se establece inicialmente a 0. Se seleccionan t funciones hash H_1, H_2..., y H_t. Cada función hash es una correlación desde el conjunto a {1, 2..., ℓ}. Para ser específicos, cada elemento del conjunto se correlaciona a cualquier valor en {1, 2..., ℓ}. Un método para añadir un elemento e en el conjunto al filtro de Bloom es de la siguiente manera: calcular $H_i(e)$, y modificar una ubicación dirigida por $H_i(e)$ en F a 1. Un método para determinar, en función de F, si un elemento e' existe en el conjunto es calcular todos los valores hash de e', y únicamente cuando todas ubicaciones dirigidas por todos los valores hash en F son 1, determinar que el elemento existe en el conjunto.

Usar el filtro de Bloom para determinar si el elemento existe en el conjunto tiene los siguientes rasgos:

Se puede determinar que el elemento no está en el conjunto siempre que una ubicación indicada por un valor hash del elemento en F sea 0; si las ubicaciones indicadas por todos los valores hash del elemento son 1, aunque se puede determinar que el elemento está el conjunto, existe falso positivo, y una probabilidad de falso positivo es $(1-e^{-t\frac{n}{\ell}})^t$, donde n es una cantidad de elementos que se añaden al filtro de Bloom.

El tiempo para añadir un elemento o determinar si un elemento está en el conjunto es un constante.

Un proceso de transmisión en vehículo de paquete de mejora basado en transcodificación de filtro de Bloom es de la siguiente manera:

1. El orquestador de OTA divide un archivo de mejora M en n partes: M_1, M_2..., y M_n.
2. El orquestador de OTA establece un filtro de Bloom F y añade M_1, M_2..., y M_n a F, y calcula v=MAC(k, F), es decir, el segundo MAC, usando la clave compartida k (la segunda clave).

3. Transferir F y v al dispositivo montado en vehículo a mejorar pretendido, y transferir secuencialmente M_i.

4. El dispositivo montado en vehículo a mejorar pretendido realiza primero verificación en F usando la clave compartida k, y puede pedir retrasmitir F y v si falla la verificación; cuando se recibe cada M_i, determina si M_i está en F, y si M_i no está en F, pide retrasmitir M_i; y finalmente, combina todos recibidos M_1, M_2..., y M_n en el archivo de mejora completo M.

Para las anteriores tres maneras, se asume que la confidencialidad (confidencialidad) del archivo de mejora no tiene que protegerse durante comunicación en vehículo. Si la confidencialidad del archivo de mejora tiene que protegerse, el orquestador de OTA necesita obtener primero un texto cifrado C_i al encriptar cada M_i (usando la tercera clave en esta solicitud), y sustituye M_i con C_i en el anterior método basado en cadena de hash, método basado en árbol de hash o método basado en filtro de Bloom. En otras palabras, se realiza encriptación usando la tercera clave, como se ha descrito anteriormente. Después de recibir cada parte, el dispositivo montado en vehículo a mejorar pretendido encripta C_i para obtener M_i después de verificarse la autenticidad. Cabe señalar que la clave para encriptación es preferiblemente diferente de la clave usada en el MAC. Por ejemplo, si la k compartida es suficientemente larga, k puede dividirse en dos claves diferentes; de otro modo, pueden generarse dos claves en función de k usando una función de derivación de clave.

Las anteriores tres maneras de dividir y transcodificar el archivo de mejora por el orquestador de OTA tienen los siguientes beneficios: El dispositivo montado en vehículo a mejorar pretendido no necesita realizar verificación en la firma digital pero realiza únicamente una operación de criptología simétrica, esto es, calcular el MAC y hash. Adicionalmente, la operación de criptología simétrica es mucho más eficiente que la operación de criptología de clave pública. Es más, el dispositivo montado en vehículo a mejorar es capaz de realizar verificación de segmento en la validez de cada segmento, y por lo tanto puede detectar un segmento inválido o erróneo a tiempo, para pedir al orquestador de OTA que retrasmita el segmento, en lugar de retransmitir el archivo de mejora entero. Si se realiza transcodificación común en vez de transcodificación de segmento, esto es, si se usa un MAC en lugar de una firma digital, el dispositivo montado en vehículo a mejorar pretendido no puede localizar con precisión una ubicación de error, y necesita pedir al orquestador de OTA que retrasmita el archivo de mejora entero. Por lo tanto, según esta realización de la presente invención, no únicamente se puede localizar con precisión una ubicación de error, se puede reducir la carga de trabajo de computación y la complejidad de computación del dispositivo a mejorar en el vehículo, de modo que el dispositivo montado en vehículo a mejorar se puede mejorar de manera segura y eficiente.

En la descripción anterior, el orquestador de OTA divide el archivo de mejora. En otra realización, un desarrollador de paquete de mejora puede realizar división. Específicamente, el método basado en cadena de hash se usa como ejemplo.

1. El desarrollador de paquete de mejora divide un archivo de mejora M en n partes: M_1, M_2... y M_n.
2. Formar una cadena de hash usando M_1, M_2..., y M_n de la siguiente manera, donde H(.) representa una función hash criptográfica:

$$h_n=H(M_n)$$

$$h_i=H(M_i, h_{i+1})$$

$$h_2=H(M_2, h_3)$$

3. Calcular $\sigma=Sign_D(M||ver, h2)$ usando una clave privada de firma. La firma es la segunda firma digital en esta solicitud, y la clave privada de firma es la cuarta clave.
4. Usar [M, ver, σ] como paquete de mejora y entregar el paquete de mejora al servidor de mejoras. Opcionalmente, M_1, M_2..., y M_n pueden encriptarse además para garantizar la confidencialidad del paquete de mejora montado en vehículo. Consúltense las descripciones anteriores relacionadas acerca de encriptar el archivo de mejora y garantizar la confidencialidad del archivo de mejora. En esta memoria no se describen de nuevo detalles.

Cuando el orquestador de OTA necesita obtener el paquete de mejora del servidor de mejoras, empezando desde la primera parte, el servidor de mejoras transfiere secuencialmente M_i al dispositivo montado en vehículo a mejorar pretendido. Para la primera parte, el servidor de mejoras necesita transferir σ, M_1, ver, y h_2; para restante partes, el servidor de mejoras necesita transferir únicamente M_i y h_{i+1}.

Para la primera parte M_1, el orquestador de OTA necesita realizar verificación en la firma digital σ; para las partes restantes M_i, el orquestador de OTA necesita realizar verificación únicamente en $h_i=H(M_i, h_{i+1})$.

Después de recibir y verificar todas las partes, el orquestador de OTA realiza transcodificación como se ha descrito anteriormente, esto es, calcula $v=MAC(k, M_1||ver, h_2)$ usando la clave compartida k (la quinta clave en esta solicitud). El MAC es el segundo MAC. Para subsiguiente paquete de mejora transmisión en vehículo, los

procesos de mejora y confirmación son los mismos que los del método 1, método 2 y método 3. Adicionalmente, para la manera de transcodificación basada en árbol de hash y la manera de transcodificación basada en filtro de Bloom, consúltese esta realización de la presente invención y el anterior método 2 y método 3. En esta memoria no se describen de nuevo detalles.

En esta realización de la presente invención, después de completarse la verificación de autenticidad en el paquete de mejora montado en vehículo en el dispositivo de control montado en vehículo (opcionalmente, puede realizarse además verificación de confidencialidad antes de la verificación de autenticidad), el dispositivo de control montado en vehículo necesita transmitir la pluralidad de archivos de mejora en los que tiene éxito la verificación de autenticidad (opcionalmente, se puede incluir verificación de confidencialidad), a un correspondiente dispositivo montado en vehículo a mejorar en el sistema montado en vehículo. Un remitente y un receptor para transmisión se cambian, esto es, la transmisión fuera de vehículo del paquete de mejora montado en vehículo se convierte en transmisión en vehículo del paquete de mejora montado en vehículo. Por lo tanto, tiene que realizar de nuevo la verificación de autenticidad o incluso la verificación de confidencialidad. Adicionalmente, según esta realización de la presente invención, verificación de firma que requiere gran carga de trabajo de computación y alta complejidad de computación se implementa en un lado de dispositivo de control montado en vehículo, y verificación de MAC que requiere pequeña carga de trabajo de computación y baja complejidad de computación todavía se implementa en el dispositivo montado en vehículo a mejorar. Esto no únicamente garantiza una alta eficiencia de mejora de un dispositivo montado en vehículo a mejorar que tiene una capacidad débil, sino que también garantiza la seguridad dentro y fuera de un vehículo en un proceso de mejora montado en vehículo.

En función de las descripciones anteriores, se puede entender que esta solicitud proporciona los siguientes puntos técnicos clave.

Un primer punto es autenticidad (Authenticity) del paquete de mejora montado en vehículo: El dispositivo montado en vehículo a mejorar comprueba la autenticidad del paquete de mejora. Para garantizar la autenticidad del paquete de mejora, una firma digital para el paquete de mejora tiene que ser proporcionada por el desarrollador o el servidor de mejoras (package server). Cuando el paquete de mejora llega al orquestador de OTA, el orquestador de OTA ayuda al dispositivo montado en vehículo a mejorar a realizar verificación en la firma digital. Entonces, el orquestador de OTA realiza una operación de transcodificación (Transcoding). Una criptología simétrica se usa en la operación de transcodificación para proporcionar verificación de autenticidad de paquete de mejora para el dispositivo montado en vehículo a mejorar. Se asume que el orquestador de OTA comparte una clave con cada dispositivo montado en vehículo a mejorar. La clave puede ser entregada por el orquestador de OTA por adelantado, y un proceso de entrega específico está más allá del alcance de esta solicitud. El paquete de mejora se divide en una pluralidad de partes a través de la operación de transcodificación (Transcoding), y se transmite al dispositivo montado en vehículo a mejorar parte por parte. Específicamente, se proporciona una operación de transcodificación basada en cadena de hash, una operación de transcodificación basada en árbol de hash, y una operación de transcodificación basada en filtro de Bloom. Ventajas de una operación de transcodificación parte-por-parte y una tecnología de transmisión parte-por-parte son de la siguiente manera: Una limitación de capacidad de computación en un dispositivo montado en vehículo y una limitación de ancho de banda en una red de comunicaciones en vehículo se toman en plena consideración. Después de que ocurre un error de transmisión de paquete de mejora, el dispositivo montado en vehículo puede encontrar una parte que sufre el error de transmisión, de modo que se solicita retransmitir únicamente la parte de error en vez del paquete de mejora entero.

Un segundo punto es la confidencialidad (Confidentiality) del paquete de mejora montado en vehículo: Un atacante puede analizar contenido del paquete de mejora usando una tecnología de ingeniería inversa. Por lo tanto, tiene que protegerse la confidencialidad del paquete de mejora montado en vehículo. Se proporcionan soluciones de protección basadas en los siguientes dos casos:

a. Si un paquete de mejora no se encripta en un servidor de mejoras, cuando una telemática montada en vehículo obtiene el paquete de mejora, el servidor de mejoras necesita realizar autenticación de identidad en la telemática montada en vehículo y establecer un canal seguro, para enviar el paquete de mejora a través del canal seguro.

b. Si un paquete de mejora se encripta (usando una clave simétrica) en un servidor de mejoras, una telemática montada en vehículo necesita obtener la clave de encriptación de un servidor de claves, y otras etapas son las mismas que las del caso a.

Un último punto es una política de mejora basada en capacidad: Diferentes dispositivos montados en vehículo tienen diferentes capacidades de computación y recursos de almacenamiento. Por ejemplo, una telemática montada en vehículo, una pasarela y un VCU usualmente tienen una capacidad relativamente fuerte, pero la mayoría de dispositivos montados en vehículo (ECU) tienen una capacidad de procesamiento relativamente débil. Por lo tanto, se proporciona la política de mejora basada en capacidad. Para ser específicos, un modo de mejora de actualizaciones de sistema A/B tiene que usarse para un dispositivo de fuerte capacidad o de clave, mientras que para un dispositivo de capacidad débil, una versión antigua de firmware o software del

dispositivo montado en vehículo a mejorar puede respaldarse con la ayuda del orquestador de OTA, para realizar restauración cuando la mejora falla.

Lo anterior describe en detalle el método en las realizaciones de la presente invención. A continuación se proporciona un aparato relacionado en las realizaciones de la presente invención.

La FIGURA 6 es un diagrama estructural esquemático de un aparato de mejora montado en vehículo según una realización de la presente invención. El aparato de mejora montado en vehículo se aplica a un sistema montado en vehículo, y el sistema montado en vehículo incluye un dispositivo de control montado en vehículo y uno o más dispositivos montados en vehículo a mejorar. El aparato de mejora montado en vehículo 10 puede ser el dispositivo de control montado en vehículo en el anterior sistema, y el aparato 10 puede incluir una unidad de obtención de paquete de mejora 101, una unidad de gestión de mejora 102, y una unidad de transmisión de mejora 103. Al continuación se describen específicamente las unidades.

La unidad de obtención de paquete de mejora 101 se configura para obtener un paquete de mejora montado en vehículo, donde el paquete de mejora montado en vehículo incluye una pluralidad de archivos de mejora, y cada archivo de mejora se usa para mejorar al menos un dispositivo montado en vehículo a mejorar.

La unidad de gestión de mejora 102 se configura para realizar verificación de seguridad en la pluralidad de archivos de mejora.

La unidad de transmisión de mejora 103 se configura para enviar un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora.

En una implementación posible, el paquete de mejora montado en vehículo incluye una primera firma digital; y la unidad de gestión de mejora se configura específicamente para realizar verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital.

En una implementación posible, el aparato 10 incluye además:

una unidad de autenticación de identidad, configurada para enviar información de autenticación de identidad al servidor de mejoras; y
una unidad de establecimiento de canal, configurada para: si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo y el servidor de mejoras; y
la unidad de obtención de paquete de mejora se configura específicamente para obtener el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro.

En una implementación posible, el paquete de mejora montado en vehículo se encripta usando una primera clave, y la primera clave es una clave simétrica; y el aparato incluye además:

una unidad de obtención de clave, configurada para obtener la primera clave de un servidor de claves; y
el aparato 10 incluye además:
una unidad de desencriptación, configurada para: después de realizarse la verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital, desencriptar, para el dispositivo de control montado en vehículo, la pluralidad de archivos de mejora usando la primera clave si tiene éxito la verificación de firma digital.

En una implementación posible, la unidad de transmisión de mejora 103 se configura específicamente para:

divide el archivo de mejora pretendido en una pluralidad de subarchivos de mejora; generar una pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y generar un primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando una segunda clave, donde la segunda clave es una clave de algoritmo simétrica; y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC.

En una implementación posible, el aparato 10 incluye además:

una unidad de encriptación, configurada para encriptar cada uno de la pluralidad de subarchivos de mejora usando una tercera clave; y
la unidad de transmisión de mejora 103 se configura específicamente para:

dividir el archivo de mejora pretendido en la pluralidad de subarchivos de mejora; generar, para el dispositivo de control montado en vehículo usando el algoritmo preestablecido, la pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora que se encriptan usando la tercera clave, y generar el primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando la segunda clave, donde la segunda clave es una clave de algoritmo simétrica; y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora, una pluralidad de bloques de datos asociados mutuamente se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y la pluralidad de subarchivos de mejora llevan una segunda firma digital de la pluralidad de bloques de datos que se genera usando una cuarta clave, donde la cuarta clave es una clave asimétrica;

la unidad de gestión de mejora 102 se configura específicamente para comprobar, para el dispositivo de control montado en vehículo, la segunda firma digital de la pluralidad de bloques de datos; y
la unidad de transmisión de mejora 103 se configura específicamente para: generar un segundo MAC de la pluralidad de bloques de datos usando una quinta clave, donde la quinta clave es una clave de algoritmo simétrica; y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el segundo MAC.

En una implementación posible, el algoritmo preestablecido incluye uno cualquiera de un algoritmo de cadena de hash, un algoritmo de árbol de hash, y un algoritmo de filtro de Bloom.

En una implementación posible, el aparato 10 incluye además:

una unidad de retransmisión, configurada para retrasmitir un bloque de datos pretendido al dispositivo montado en vehículo a mejorar pretendido, donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos.

Cabe señalar que, para una función de cada unidad funcional del aparato de mejora montado en vehículo 10 descrito en esta realización de la presente invención, consúltense descripciones relacionadas en las realizaciones de método mostradas de la FIGURA 1 a la FIGURA 6. En esta memoria no se describen de nuevo detalles.

La FIGURA 7 es un diagrama estructural esquemático de un aparato montado en vehículo a mejorar según una realización de la presente invención. El aparato montado en vehículo a mejorar 20 se aplica a un sistema montado en vehículo, y el sistema montado en vehículo incluye un dispositivo de control montado en vehículo y uno o más dispositivos montados en vehículo a mejorar. El aparato montado en vehículo a mejorar 20 puede ser el dispositivo montado en vehículo a mejorar en el anterior sistema, y el aparato 20 puede incluir una unidad de recepción 201 y una unidad de mejora 202. Al continuación se describen específicamente las unidades.

La unidad de recepción 201 se configura para recibir un archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad realizada por el dispositivo de control montado en vehículo y que se utiliza para mejorar al menos el dispositivo montado en vehículo a mejorar pretendido.

La unidad de mejora 202 se usa para realizar la mejora segura usando el archivo de mejora pretendido.

En una implementación posible, la unidad de mejora 202 se configura específicamente para:

usar un modo de mejora de actualizaciones de sistema A/B, y realizar la mejora segura usando el archivo de mejora pretendido, donde el dispositivo montado en vehículo a mejorar es un primer dispositivo montado en vehículo a mejorar cuya capacidad de almacenamiento de recursos y/o capacidad de procesamiento supera un valor preestablecido o un primer dispositivo montado en vehículo a mejorar que se especifica por adelantado.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora; y la unidad de recepción 201 se configura específicamente para:

recibir secuencialmente la pluralidad de bloques de datos que llevan el primer MAC y que son enviados por el dispositivo de control montado en vehículo, donde la pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, el primer MAC es un código de autenticación de mensaje

de la pluralidad de bloques de datos que se genera usando una segunda clave, y la segunda clave es una clave simétrica; y
la unidad de mejora 202 se configura específicamente para:

realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

En una implementación posible, la pluralidad de subarchivos de mejora se encriptan usando una tercera clave; y
la unidad de mejora 202 se configura específicamente para:

realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; cuando se verifican todos de la pluralidad de bloques de datos, desencriptar cada uno de la pluralidad de bloques de datos verificados secuencialmente usando la tercera clave; y combinar la pluralidad de bloques de datos que se desencriptan usando la tercera clave para mejora.

En una implementación posible, la unidad de recepción 201 se configura específicamente para:

recibir secuencialmente la pluralidad de bloques de datos que llevan un segundo MAC y que son enviados por el dispositivo de control montado en vehículo, donde la pluralidad de bloques de datos son una pluralidad de bloques de datos asociados mutuamente que se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, el segundo MAC es un código de autenticación de mensaje de la pluralidad de bloques de datos que se genera usando una quinta clave, y la quinta clave es un algoritmo simétrico; y
la unidad de mejora 202 se configura específicamente para:

realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la quinta clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

En una implementación posible, el aparato 20 incluye además:

una unidad de retransmisión, configurada para volver a -obtener un bloque de datos pretendido del dispositivo de control montado en vehículo, donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos.

Cabe señalar que, para una función de cada unidad funcional del aparato montado en vehículo a mejorar 20 descrito en esta realización de la presente invención, consúltense descripciones relacionadas en las realizaciones de método mostradas de la FIGURA 1 a la FIGURA 6. En esta memoria no se describen de nuevo detalles.

La FIGURA 8 es un diagrama estructural esquemático de un dispositivo según una realización de la presente invención. Ambos del aparato montado en vehículo a mejorar 10 y el aparato montado en vehículo a mejorar 20 pueden implementarse en una estructura en la FIGURA 8. El dispositivo 30 incluye al menos un procesador 301, al menos una memoria 302, y al menos una interfaz de comunicaciones 303. Adicionalmente, el dispositivo puede incluir además componentes de finalidad general tales como una antena, y en esta memoria no se describen detalles.

El procesador 301 puede ser una unidad de procesamiento central de finalidad general (CPU), un microprocesador, un circuito integrado de aplicación específica (Application-Specific Integrated Circuit, ASIC), o uno o más circuitos integrados para controlar la ejecución del programa de la solución anterior.

La interfaz de comunicaciones 303 se configura para comunicar con otro dispositivo tal como un servidor de mejoras, un servidor de claves, o un dispositivo en vehículo o con una red de comunicaciones.

La memoria 302 puede ser una memoria de solo lectura (Read Only Memory, ROM) u otro tipo de dispositivo de almacenamiento estático capaz de almacenar información estática e instrucciones, o una memoria de acceso aleatorio (Random Access Memory, RAM) u otro tipo de dispositivo de almacenamiento dinámico capaz de almacenar información e instrucciones, o puede ser una memoria de solo lectura programable borrable eléctricamente (Electrically Erasable Programmable Read-Only Memory, EEPROM), una memoria de solo lectura de disco compacto (Compact Disc Read-Only Memory, CD-ROM) u otro almacenamiento de disco óptico,

almacenamiento de disco óptico (que incluye un disco compacto, un disco láser, un disco óptico, un disco versátil digital, un disco Blu-ray, o algo semejante), un soporte de almacenamiento en disco magnético u otro dispositivo de almacenamiento magnético, o cualquier otro medio que se puede usar para llevar o almacenar código de programa esperado en una instrucción o forma de estructura de datos y que puede ser accedido por un ordenador, pero sin limitación a esto. La memoria puede existir independientemente, y se conecta al procesador usando un bus. Como alternativa, la memoria puede integrarse con el procesador.

La memoria 302 se configura para almacenar código de programa de aplicación para ejecutar la solución anterior, y el procesador 301 controla la ejecución. El procesador 301 se configura para ejecutar el código de programa de aplicación almacenado en la memoria 302.

Cuando el dispositivo mostrado en la FIGURA 8 es el aparato de mejora de dispositivo montado en vehículo 10, se puede usar código almacenado en la memoria 302 para realizar el método de mejora de dispositivo montado en vehículo proporcionado en la FIGURA 2, por ejemplo, obtener un paquete de mejora montado en vehículo, donde el paquete de mejora montado en vehículo incluye una pluralidad de archivos de mejora, y cada archivo de mejora se usa para mejorar al menos un dispositivo montado en vehículo a mejorar; realizar verificación de seguridad en la pluralidad de archivos de mejora; y enviar un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora.

Cabe señalar que, para una función de cada unidad funcional del aparato de mejora de dispositivo montado en vehículo 10 descrito en esta realización de la presente invención, consúltense descripciones relacionadas de las etapas S502 y S503 en la realización de método mostrada en la FIGURA 5. En esta memoria no se describen de nuevo detalles.

Cuando el dispositivo mostrado en la FIGURA 8 es el aparato montado en vehículo a mejorar 20, el código almacenado en la memoria 302 se puede usar para realizar el método de mejora de dispositivo montado en vehículo proporcionado en la FIGURA. 9, por ejemplo, recibir un archivo de mejora pretendido enviado por un dispositivo de control montado en vehículo, donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad realizada por el dispositivo de control montado en vehículo y que se utiliza para mejorar al menos el dispositivo montado en vehículo a mejorar pretendido; y realizar la mejora segura usando el archivo de mejora pretendido.

Cabe señalar que, para una función de cada unidad funcional del aparato montado en vehículo a mejorar 20 descrito en esta realización de la presente invención, consúltense descripciones relacionadas de las etapas S504 y S505 en la realización de método mostrada en la FIGURA 5. En esta memoria no se describen de nuevo detalles.

La FIGURA 9 es un diagrama estructural esquemático de un vehículo inteligente según una realización de la presente invención. El vehículo inteligente 40 incluye un dispositivo de control montado en vehículo 401 y al menos un dispositivo montado en vehículo a mejorar 402.

El dispositivo montado en vehículo 401 se configura para obtener un paquete de mejora montado en vehículo, realizar verificación de seguridad en una pluralidad de archivos de mejora en el paquete de mejora montado en vehículo, y enviar un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido, donde cada archivo de mejora se usa para mejorar al menos un dispositivo montado en vehículo a mejorar, y el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora.

El dispositivo montado en vehículo a mejorar 402 se configura para recibir el archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo, y realizar la mejora segura usando el archivo de mejora pretendido, donde el dispositivo montado en vehículo a mejorar es el dispositivo montado en vehículo a mejorar pretendido.

En una implementación posible, el dispositivo de control montado en vehículo 401 se configura específicamente para realizar verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital.

En una implementación posible, el dispositivo de control montado en vehículo 401 se configura específicamente para:

enviar información de autenticación de identidad al servidor de mejoras, si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo y el servidor de mejoras, y obtener el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro; o

el paquete de mejora montado en vehículo se encripta usando una primera clave, y la primera clave es una clave simétrica; y el dispositivo de control montado en vehículo (401) se configura específicamente para:

obtener la primera clave de un servidor de claves, y después de que tiene éxito la verificación de firma digital realizada en la pluralidad de archivos de mejora usando la primera firma digital, desencriptar la pluralidad de archivos de mejora usando la primera clave.

En una implementación posible, el dispositivo de control montado en vehículo 401 se configura específicamente para:

dividir el archivo de mejora pretendido en una pluralidad de subarchivos de mejora, generar una pluralidad de bloques de datos asociados mutuamente usando un algoritmo preestablecido, generar un primer código de autenticación de mensaje MAC de la pluralidad de bloques de datos usando una segunda clave, y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el primer MAC, donde la segunda clave es una clave de algoritmo simétrica; y
el dispositivo montado en vehículo a mejorar 402 se configura específicamente para:

recibir secuencialmente la pluralidad de bloques de datos que llevan el primer MAC y que son enviados por el dispositivo de control montado en vehículo; realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la segunda clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

En una implementación posible, el dispositivo de control montado en vehículo 401 se configura específicamente para:

encriptar cada uno de la pluralidad de subarchivos de mejora usando una tercera clave, y generar, usando el algoritmo preestablecido, la pluralidad de bloques de datos asociados mutuamente de la pluralidad de subarchivos de mejora que se encriptan usando la tercera clave; y
el dispositivo montado en vehículo a mejorar 402 se configura específicamente para:

cuando se verifican todos de la pluralidad de bloques de datos, desencriptar cada uno de la pluralidad de bloques de datos verificados secuencialmente usando la tercera clave, y combinar la pluralidad de bloques de datos que se desencriptan usando la tercera clave para mejora.

En una implementación posible, el archivo de mejora pretendido incluye una pluralidad de subarchivos de mejora, una pluralidad de bloques de datos asociados mutuamente se generan de la pluralidad de subarchivos de mejora usando un algoritmo preestablecido, y la pluralidad de subarchivos de mejora llevan una segunda firma digital de la pluralidad de bloques de datos que se genera usando una cuarta clave, donde la cuarta clave es una clave asimétrica;
el dispositivo de control montado en vehículo 401 se configura específicamente para:

comprobar la segunda firma digital de la pluralidad de bloques de datos, generar un segundo MAC de la pluralidad de bloques de datos usando una quinta clave, y enviar secuencialmente, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos que llevan el segundo MAC, donde la quinta clave es una clave de algoritmo simétrica; y
el dispositivo montado en vehículo a mejorar 402 se configura específicamente para:

recibir secuencialmente la pluralidad de bloques de datos que llevan el segundo MAC y que son enviados por el dispositivo de control montado en vehículo; realizar secuencialmente verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido usando la quinta clave; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados secuencialmente para mejora.

Cabe señalar que, para el dispositivo de control montado en vehículo 401 y el dispositivo montado en vehículo a mejorar 402 del vehículo inteligente 40 descrito en esta realización de la presente invención, consúltense descripciones relacionadas del dispositivo de control montado en vehículo y el dispositivo montado en vehículo a mejorar en la realización de método mostrada en la FIGURA 5. En esta memoria no se describen de nuevo detalles.

Se puede entender que, el vehículo inteligente 40 puede además integrarse con funciones de un sistema de conducción inteligente, un sistema de servicio de vida, un sistema de protección de seguridad, un sistema de servicio de posicionamiento, un sistema de servicio cabina, y similares usando ordenador, detección moderna,

convergencia de información, comunicaciones, artificial inteligencia, control automático, y otras tecnologías. Esto no se limita específicamente en esta solicitud, y en esta memoria no se describen detalles.

Una realización de la presente invención proporciona además un soporte de almacenamiento informático. El soporte de almacenamiento informático almacena un programa, y cuando es ejecutado, el programa realiza algunas o todas la etapas descritas en una cualquiera de las realizaciones de método anteriores.

Una realización de la presente invención proporciona además un programa informático. El programa informático incluye una instrucción, y cuando el programa informático es ejecutado por un ordenador, el ordenador se habilita para realizar algunas o todas de las etapas de uno cualquiera de los métodos de mejora de dispositivo montado en vehículo.

En las realizaciones anteriores, la descripción de cada realización tiene enfoques respectivos. Para una parte que no se describe en detalle en una realización, consúltense las descripciones relacionadas en otras realizaciones.

En las varias realizaciones proporcionadas en esta solicitud, debe entenderse que el aparato divulgado puede implementarse de otras maneras. Por ejemplo, la realización de aparato descrita es meramente un ejemplo. Por ejemplo, la división de unidad es meramente división funcional lógica y puede ser otra división en una implementación real. Por ejemplo, una pluralidad de unidades o componentes puede combinarse o integrarse en otro sistema. Además, los acoplamientos mutuos o los acoplamientos directos o las conexiones de comunicación mostrados o discutidos se pueden implementar a través de algunas interfaces. Las conexiones de comunicación o acoplamientos indirectos entre los aparatos o unidades se pueden implementar de forma eléctrica u otras.

Las unidades anteriores descritas como partes separadas pueden o no estar físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, se pueden localizar en una posición o se pueden distribuir en una pluralidad de unidades de red. Se pueden seleccionar algunas o todas las unidades en función de los requisitos reales para lograr los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de esta solicitud se pueden integrar en una unidad de procesamiento, o cada una de las unidades puede existir físicamente sola, o dos o más unidades se integran en una unidad. La unidad integrada se puede implementar en forma de hardware, o se puede implementar en forma de unidad funcional de software.

Cuando la unidad integrada anterior se implementa en forma de una unidad funcional de software y se vende o utiliza como producto independiente, la unidad integrada se puede almacenar en un soporte de almacenamiento legible por ordenador. Sobre la base de este tipo de entendimiento, las soluciones técnicas de esta solicitud, esencialmente, o la parte que contribuye a la técnica anterior, o todas o algunas de las soluciones técnicas, se pueden implementar en forma de producto de software. El producto de software informático se almacena en un soporte de almacenamiento e incluye varias instrucciones para dar instrucciones a un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de red) para realizar todas o una parte de las etapas de los métodos descritos en las realizaciones de esta solicitud. El soporte de almacenamiento anterior incluye: cualquier medio que pueden almacenar código de programa, tal como una unidad de memoria USB, un disco duro extraíble, un disco magnético, un disco óptico, una memoria de solo lectura (Read Only Memory, ROM por abreviar), o una memoria de acceso aleatorio (Random Access Memory, RAM por abreviar).

Las realizaciones anteriores meramente pretenden describir las soluciones técnicas de esta solicitud, pero no limitar esta solicitud.

REIVINDICACIONES

1. Un método de mejora para un dispositivo montado en vehículo, aplicado a un vehículo, en donde el vehículo comprende un dispositivo de control montado en vehículo y uno o más dispositivos montados en vehículo a mejorar, y el método comprende:

obtener (S501), por parte del dispositivo de control montado en vehículo, un paquete de mejora montado en vehículo, en donde el paquete de mejora montado en vehículo comprende una pluralidad de archivos de mejora;
realizar (S502), por parte del dispositivo de control montado en vehículo, verificación de seguridad en la pluralidad de archivos de mejora; y
enviar (S503), por parte del dispositivo de control montado en vehículo, un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido, en donde el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora;
en donde enviar (S503), por parte del dispositivo de control montado en vehículo, un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido que se va a mejorar usando el archivo de mejora pretendido comprende:

dividir, por parte del dispositivo de control montado en vehículo, el archivo de mejora pretendido en una pluralidad de bloques de datos asociados usando un algoritmo preestablecido;
realizar procesamiento de código de autenticación de mensaje, MAC, en los bloques de datos asociados; y
enviar por separado, por parte del dispositivo de control montado en vehículo al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos.

2. El método según la reivindicación 1, en donde el paquete de mejora montado en vehículo comprende una primera firma digital; y realizar (S502), por parte del dispositivo de control montado en vehículo, verificación de seguridad en la pluralidad de archivos de mejora comprende:

realizar, por parte del dispositivo de control montado en vehículo, verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital.

3. El método según la reivindicación 2, en donde el método comprende además:

enviar, por parte del dispositivo de control montado en vehículo, información de autenticación de identidad a un servidor de mejoras; y
si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo y el servidor de mejoras; y
obtener (S501), por parte del dispositivo de control montado en vehículo, un paquete de mejora montado en vehículo comprende:
obtener, por parte del dispositivo de control montado en vehículo, el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro.

4. El método según la reivindicación 2, en donde el paquete de mejora montado en vehículo se encripta usando una primera clave, y la primera clave es una clave simétrica; y donde el método comprende además:

obtener, por parte del dispositivo de control montado en vehículo, la primera clave de un servidor de claves; y
después de realizar, por parte del dispositivo de control montado en vehículo, verificación de firma digital en la pluralidad de archivos de mejora usando la primera firma digital, el método comprende:
desencriptar, por parte del dispositivo de control montado en vehículo, la pluralidad de archivos de mejora usando la primera clave si tiene éxito la verificación de firma digital.

5. El método según una cualquiera de las reivindicaciones 1 a 4, en donde el algoritmo preestablecido comprende uno cualquiera de un algoritmo de cadena de hash, un algoritmo de árbol de hash y un algoritmo de filtro de Bloom.

6. El método según una cualquiera de las reivindicaciones 1 a 5, en donde el método comprende además:
retransmitir, por parte del dispositivo de control montado en vehículo, un bloque de datos pretendido al dispositivo montado en vehículo a mejorar pretendido, en donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos.

7. El método según una cualquiera de las reivindicaciones 1 a 6, en donde el dispositivo montado en vehículo a mejorar pretendido comprende una primera región y una segunda región, un archivo actual del dispositivo

montado en vehículo a mejorar pretendido se ejecuta en la primera región, y el archivo de mejora pretendido se escribe en la segunda región.

8. Un vehículo inteligente (40), en donde el vehículo inteligente (40) comprende un dispositivo de control montado en vehículo (401) y al menos un dispositivo montado en vehículo a mejorar (402), en donde:

el dispositivo de control montado en vehículo (401) se configura para obtener un paquete de mejora montado en vehículo, realizar verificación de seguridad en una pluralidad de archivos de mejora en el paquete de mejora montado en vehículo, y enviar un archivo de mejora pretendido a un dispositivo montado en vehículo a mejorar pretendido (402) que se va a mejorar usando el archivo de mejora pretendido, en donde cada archivo de mejora se usa para mejorar al menos un dispositivo montado en vehículo a mejorar (402), y el archivo de mejora pretendido es un archivo de mejora en el que tiene éxito la verificación de seguridad en la pluralidad de archivos de mejora, en donde el dispositivo de control montado en vehículo (401) se configura específicamente para: dividir el archivo de mejora pretendido en una pluralidad de bloques de datos asociados usando un algoritmo preestablecido; realizar procesamiento de código de autenticación de mensaje, MAC, en los bloques de datos asociados; y enviar por separado, al dispositivo montado en vehículo a mejorar pretendido, la pluralidad de bloques de datos; y

el dispositivo montado en vehículo a mejorar (402) se configura para recibir el archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo (401), y realizar la mejora segura usando el archivo de mejora pretendido, en donde el dispositivo montado en vehículo a mejorar (402) es el dispositivo montado en vehículo a mejorar pretendido (402), en donde el dispositivo montado en vehículo a mejorar (402) se configura específicamente para: recibir la pluralidad de bloques de datos asociados enviados por el dispositivo de control montado en vehículo (401); realizar verificación en la pluralidad de bloques de datos en función del algoritmo preestablecido; y cuando se verifican todos de la pluralidad de bloques de datos, combinar la pluralidad de bloques de datos verificados para mejora.

9. El vehículo inteligente (40) según la reivindicación 8, en donde el dispositivo de control montado en vehículo (401) se configura específicamente para:

realizar verificación de firma digital en la pluralidad de archivos de mejora usando una primera firma digital.

10. El vehículo inteligente (40) según la reivindicación 9, en donde el dispositivo de control montado en vehículo (401) se configura específicamente para:

enviar información de autenticación de identidad a un servidor de mejoras, si la información de autenticación de identidad es autenticada por el servidor de mejoras, establecer un canal seguro entre el dispositivo de control montado en vehículo (401) y el servidor de mejoras, y obtener el paquete de mejora montado en vehículo del servidor de mejoras a través del canal seguro.

11. El vehículo inteligente (40) según la reivindicación 9, donde el paquete de mejora montado en vehículo se encripta usando una primera clave, y la primera clave es una clave simétrica; y el dispositivo de control montado en vehículo (401) se configura específicamente para:

obtener la primera clave de un servidor de claves; y después de que tiene éxito la verificación de firma digital realizada en la pluralidad de archivos de mejora usando la primera firma digital, desencriptar la pluralidad de archivos de mejora usando la primera clave.

12. El vehículo inteligente (40) según una cualquiera de las reivindicaciones 8 a 11, el dispositivo de control montado en vehículo (401) se configura además para:

retrasmitir un bloque de datos pretendido al dispositivo montado en vehículo a mejorar pretendido, en donde el bloque de datos pretendido es un bloque de datos en el que la verificación falla en el dispositivo montado en vehículo a mejorar pretendido en la pluralidad de bloques de datos.

13. El vehículo inteligente (40) según una cualquiera de las reivindicaciones 8 a 12, en donde el dispositivo montado en vehículo a mejorar pretendido comprende una primera región y una segunda región, un archivo actual del dispositivo montado en vehículo a mejorar pretendido se ejecuta en la primera región, y el archivo de mejora pretendido se escribe en la segunda región.

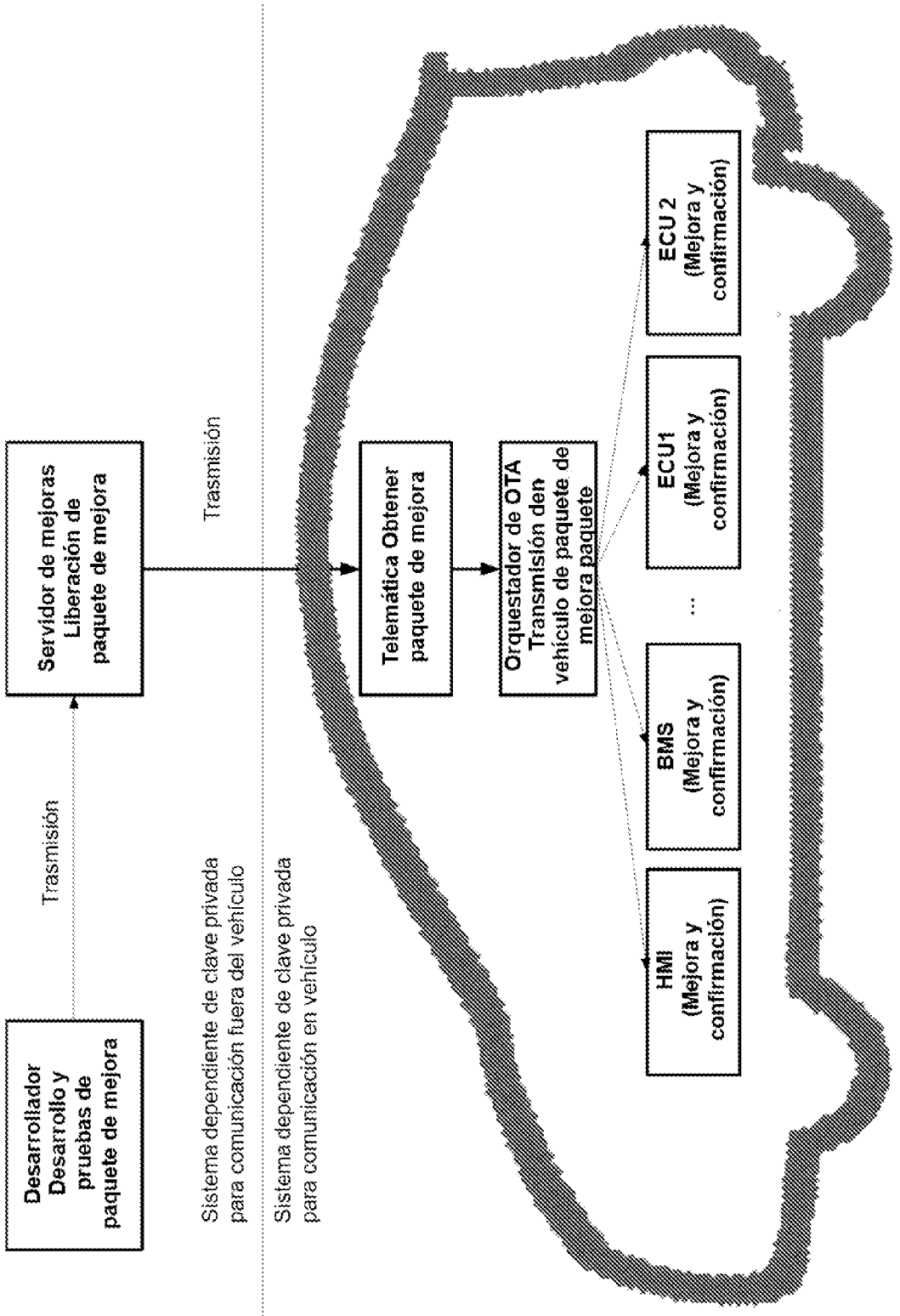
Desarrollador
Desarrollo y pruebas de paquete de mejora
Trasmisión
Servidor de mejoras
Liberación de paquete de mejora
Trasmisión
Sistema dependiente de clave privada para comunicación fuera del vehículo
Sistema dependiente de clave privada para comunicación en vehículo
Telemática Obtener paquete de mejora
Orquestador de OTA
Transmisión den vehículo de paquete de mejora paquete
HMI (Mejora y confirmación)
BMS (Mejora y confirmación)
...
ECU1 (Mejora y confirmación)
ECU 2 (Mejora y confirmación)

FIG. 1

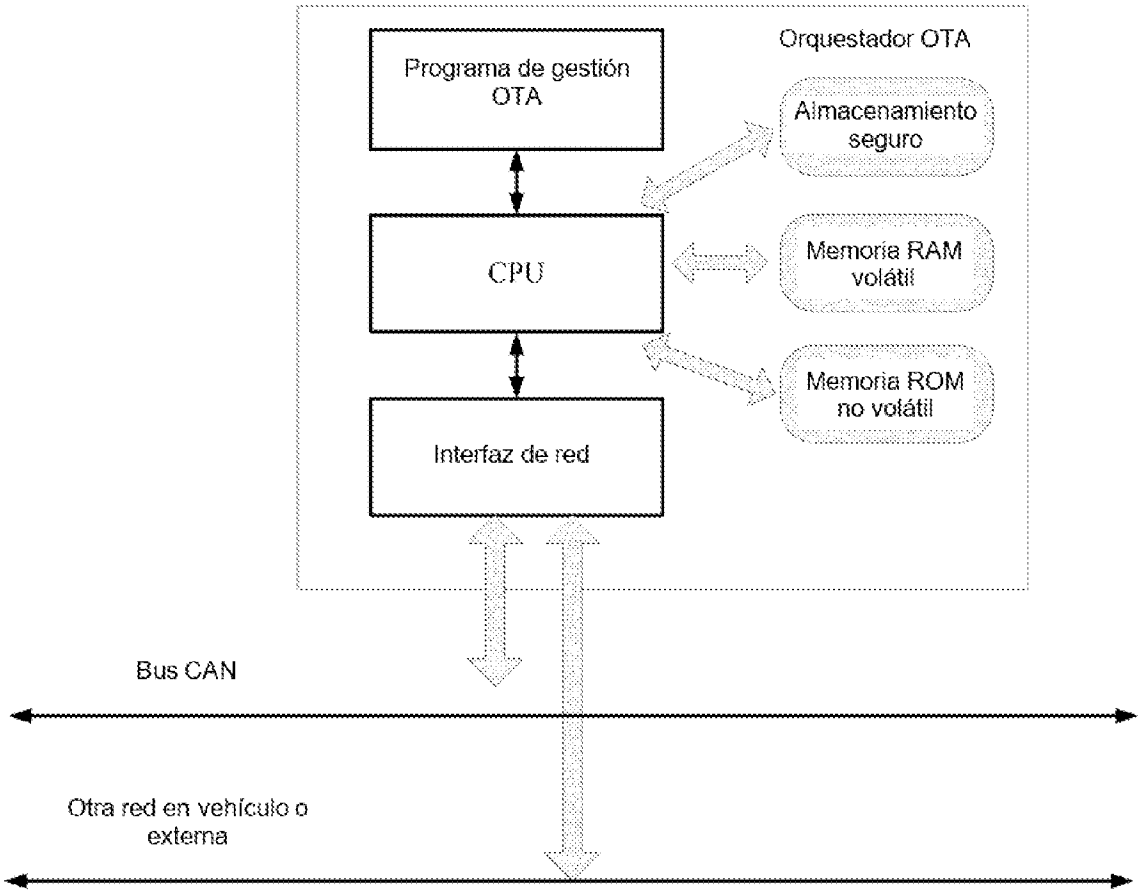
Orquestador OTA
Programa de gestión OTA
Almacenamiento seguro
CPU
Memoria RAM volátil
Memoria ROM no volátil
Interfaz de red
Bus CAN
Otra red en vehículo o externa

FIG. 2

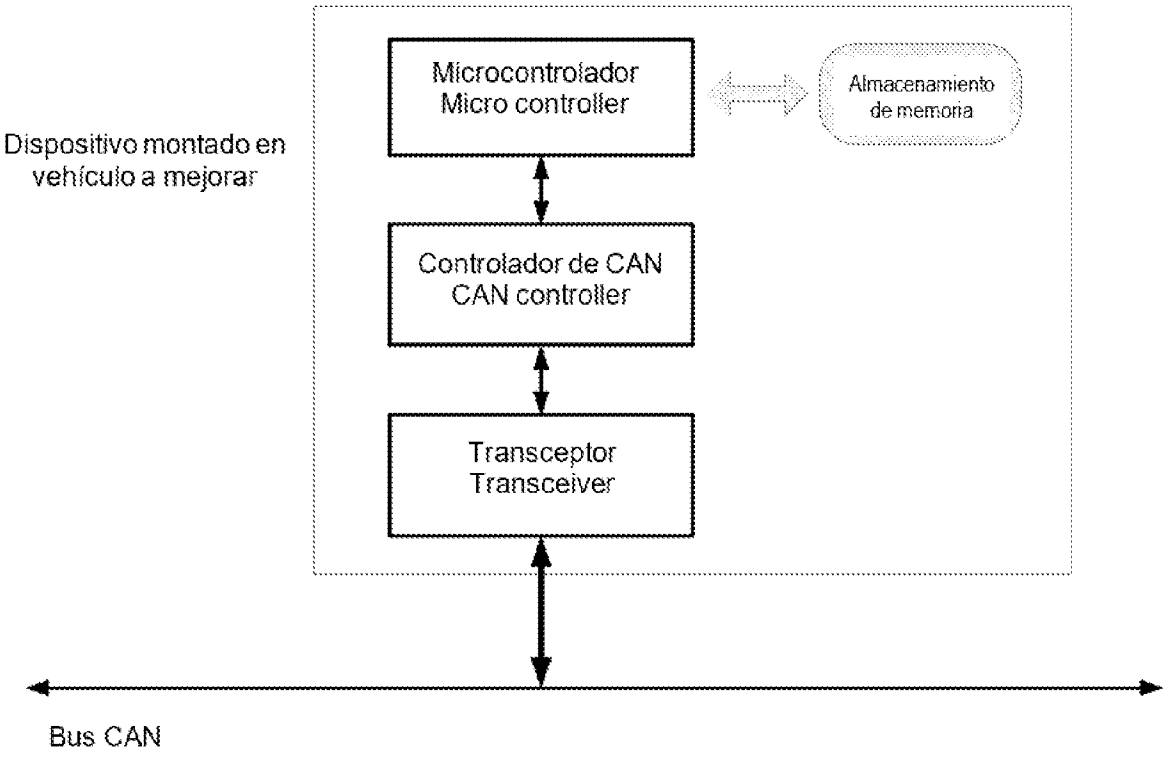
Dispositivo montado en vehículo a mejorar
Microcontrolador
Micro controller
Almacenamiento de memoria
Controlador de CAN
CAN controller
Transceptor
Transceiver
Bus CAN

FIG. 3

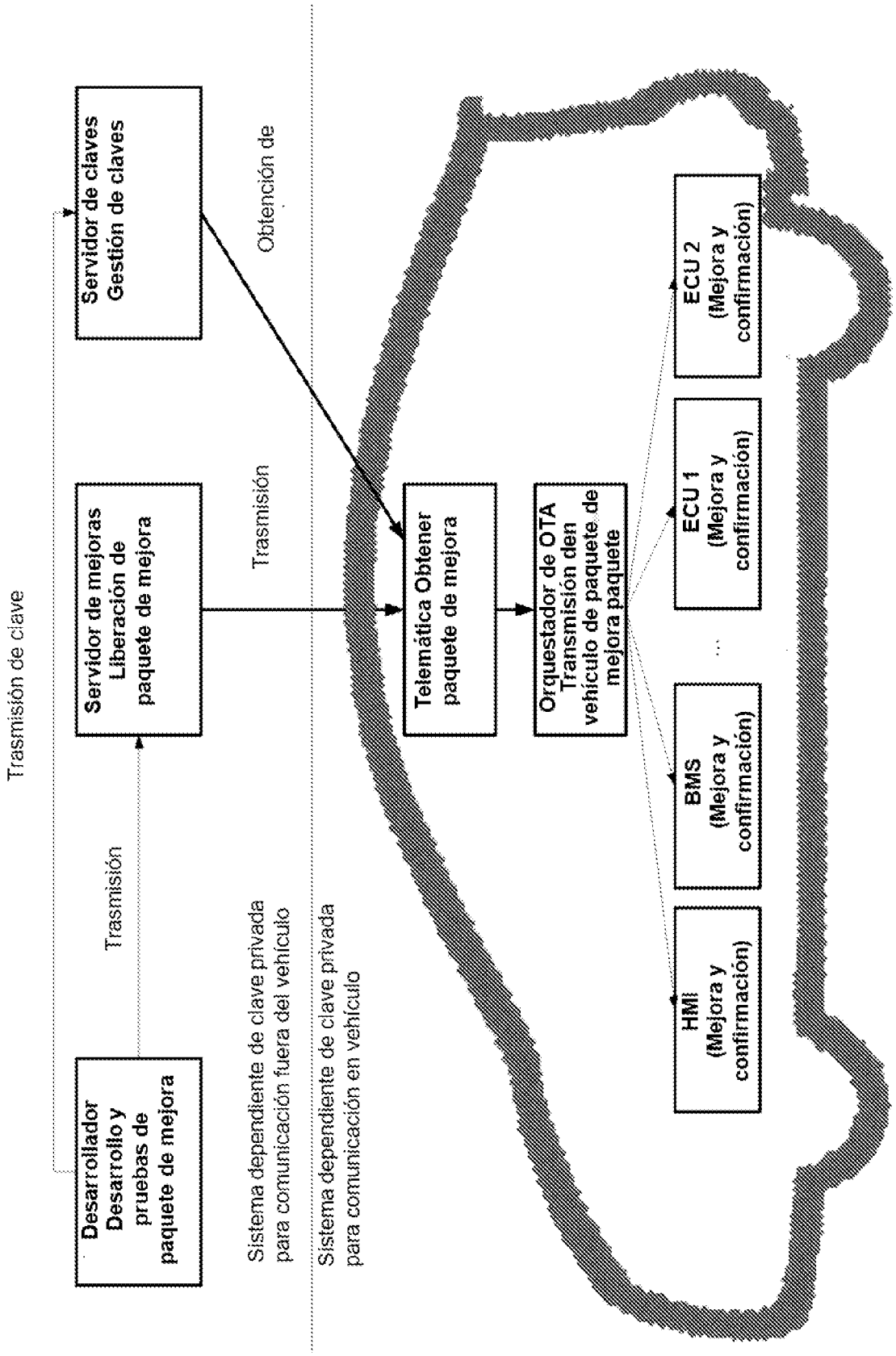
Trasmisión de clave
Desarrollador Desarrollo y pruebas de paquete de mejora
Trasmisión
Servidor de mejoras Liberación de paquete de mejora
Trasmisión
Servidor de claves Gestión de claves
Obtención de
Sistema dependiente de clave privada para comunicación fuera del vehículo
Sistema dependiente de clave privada para comunicación en vehículo
Telemática Obtener paquete de mejora
Orquestador de OTA Transmisión den vehículo de paquete de mejora paquete
HMI (Mejora y confirmación)
BMS (Mejora y confirmación)
...
ECU 1 (Mejora y confirmación)
ECU 2 (Mejora y confirmación)

FIG. 4

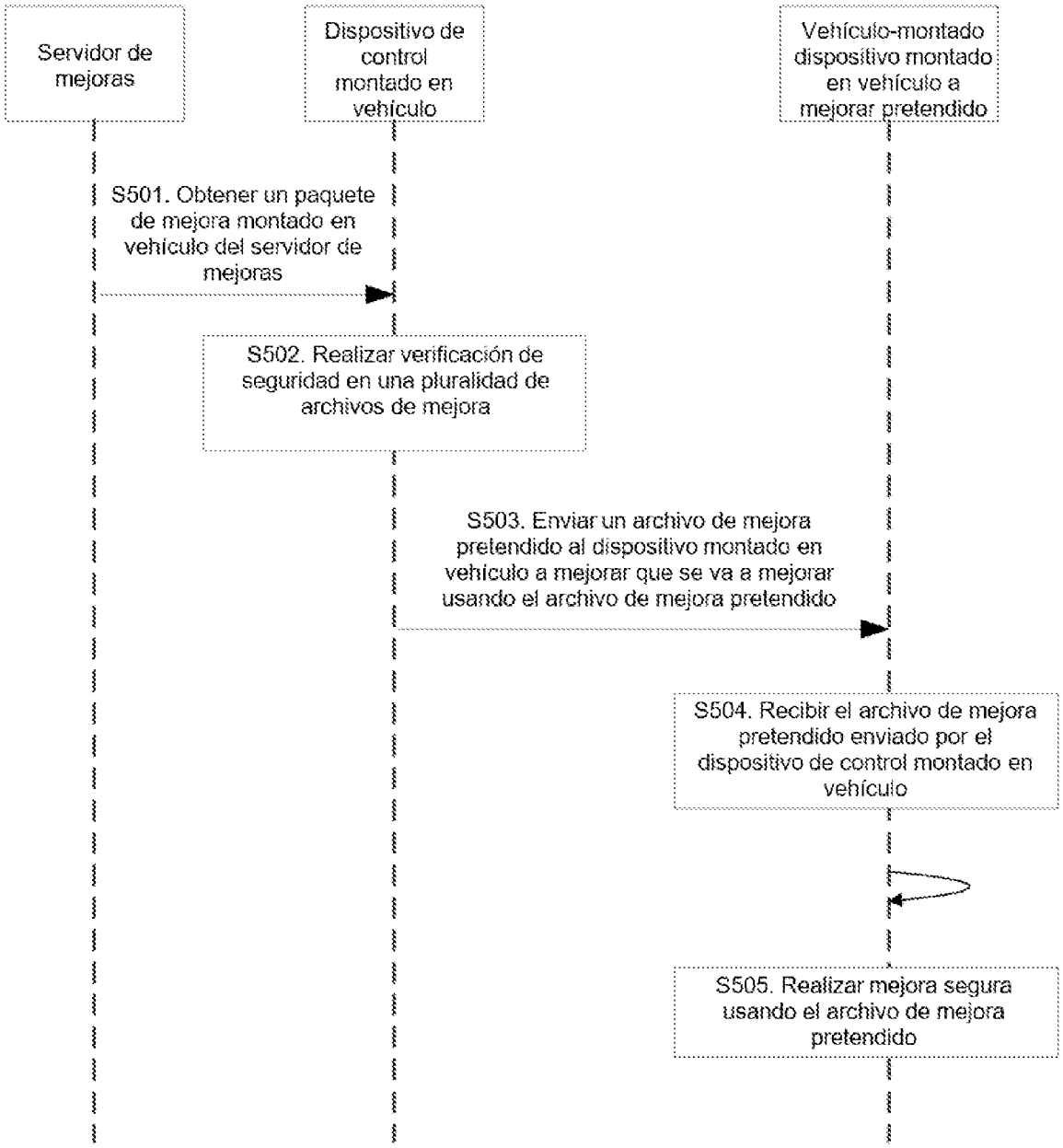
Servidor de mejoras
Dispositivo de control montado en vehículo
Vehículo-montado dispositivo montado en vehículo a mejorar pretendido
S501. Obtener un paquete de mejora montado en vehículo del servidor de mejoras
S502. Realizar verificación de seguridad en una pluralidad de archivos de mejora
S503. Enviar un archivo de mejora pretendido al dispositivo montado en vehículo a mejorar que se va a mejorar usando el archivo de mejora pretendido
S504. Recibir el archivo de mejora pretendido enviado por el dispositivo de control montado en vehículo
S505. Realizar mejora segura usando el archivo de mejora pretendido

FIG. 5

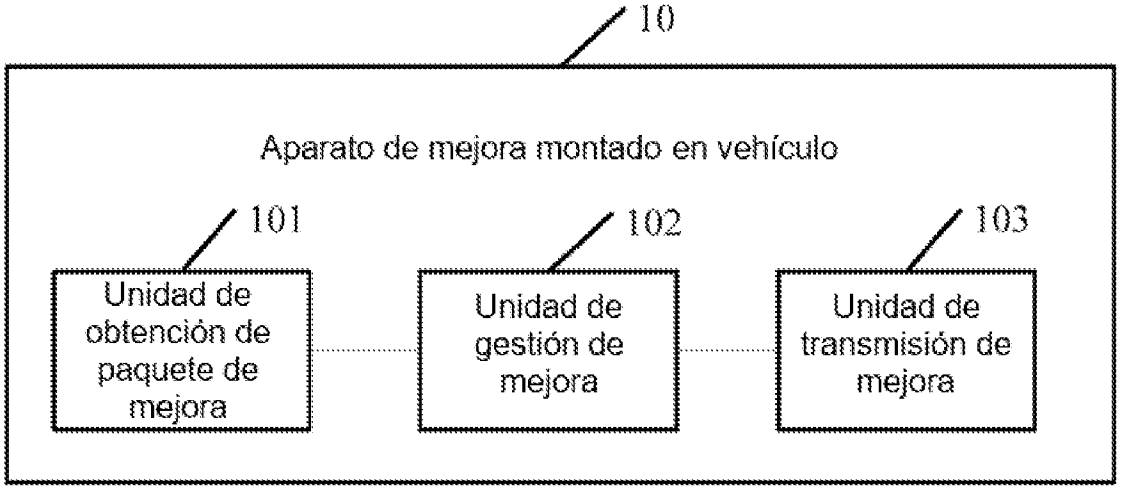
10
Aparato de mejora montado en vehículo
101
Unidad de obtención de paquete de mejora
102
Unidad de gestión de mejora
103
Unidad de transmisión de mejora

FIG. 6

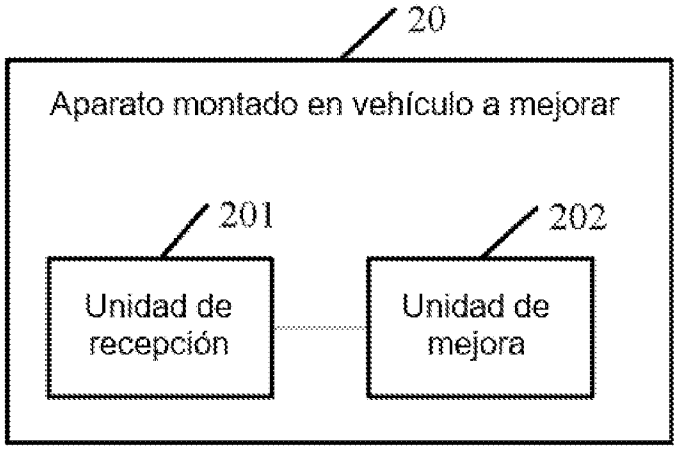
20
Aparato montado en vehículo a mejorar
201
Unidad de recepción
202
Unidad de mejora

FIG. 7

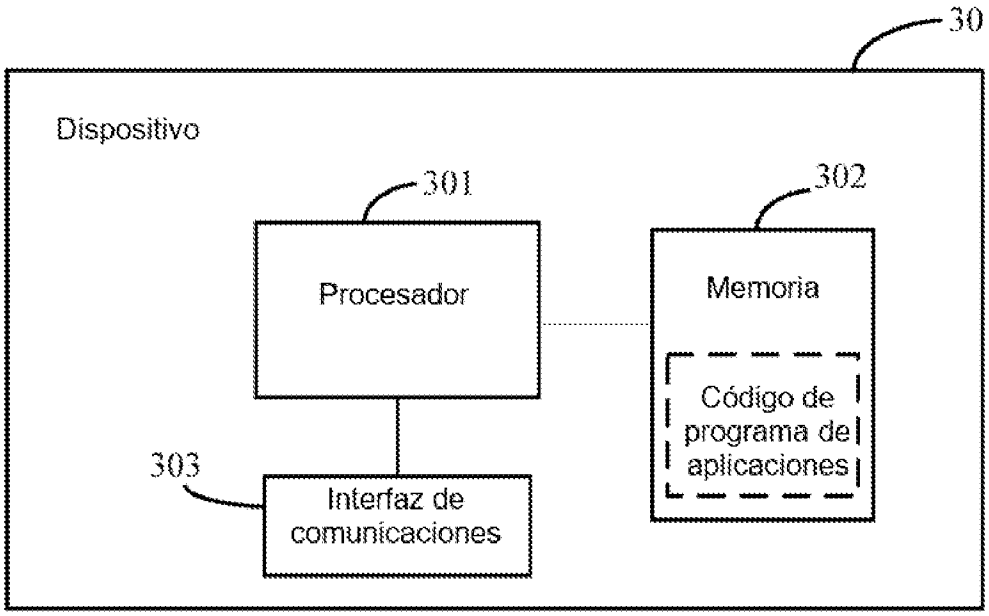
30
Dispositivo
301
Procesador
302
Memoria
Código de programa de aplicaciones
303
Interfaz de comunicaciones

FIG. 8

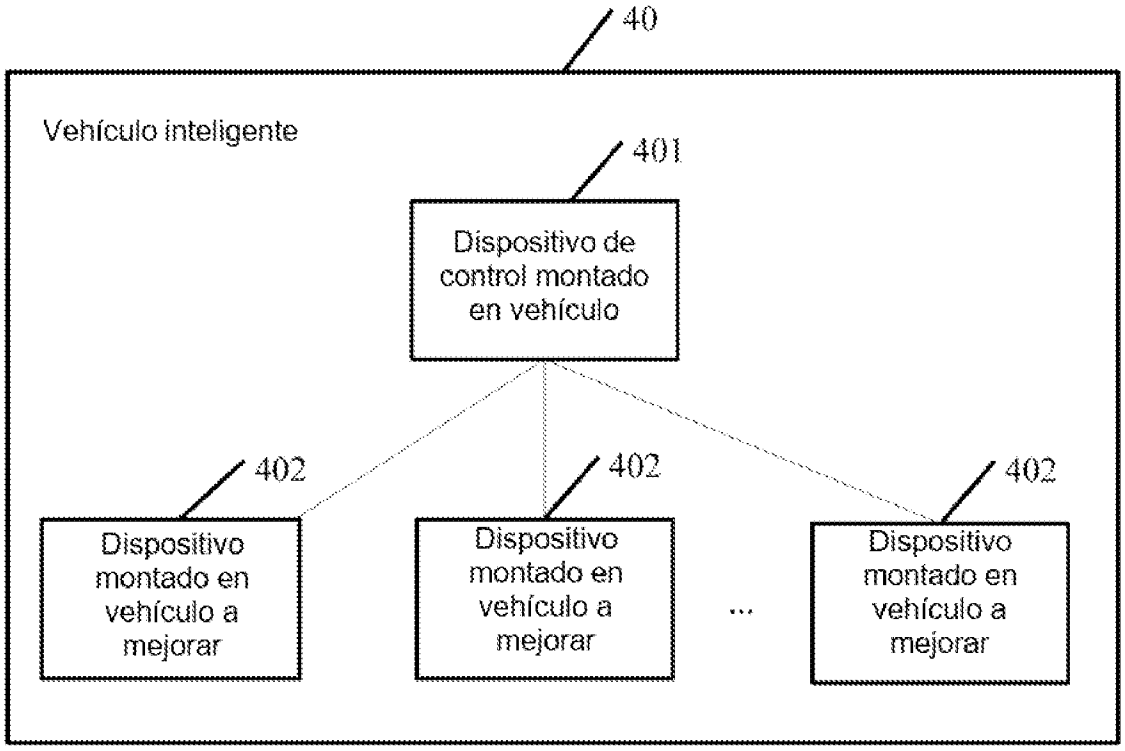
40
Vehículo inteligente
401
Dispositivo de control montado en vehículo
402
Dispositivo montado en vehículo a mejorar
402
Dispositivo montado en vehículo a mejorar
...
402
Dispositivo montado en vehículo a mejorar

FIG. 9