(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 575 911**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.03.2008 E 08744059 (0)**

(97) Fecha y número de publicación de la concesión europea: **16.03.2016 EP 2137875**

(54) Título: **Gestión de certificado de segmento de vehículo usando esquemas de certificado compartido**

(30) Prioridad:

19.03.2007 US 918742 P
19.03.2008 US 51241

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.07.2016

(73) Titular/es:

TELCORDIA TECHNOLOGIES, INC. (100.0%)
1 Ericsson Drive 5G116
Piscataway, NJ 08854-4157, US

(72) Inventor/es:

ZHANG, TAO;
DI CRESCENZO, GIOVANNI;
PIETROWICZ, STANLEY;
VAN DEN BERG, ERIC y
WHITE, ROBERT G.

(74) Agente/Representante:

VILLAMOR MUGUERZA, Jon

DESCRIPCIÓN

Gestión de certificado de segmento de vehículo usando esquemas de certificado compartido

Campo de la invención

La presente invención se refiere en general a la gestión de certificado de segmento de vehículo. En particular, la invención se refiere al proceso de gestión de certificado y clave criptográfica anónimos.

Antecedentes de la invención

Definir un método para gestionar una solicitud de firma de certificado (CSR, *Certificate Signing Request*) 1609.2 u otros certificados anónimos para el sistema de integración de infraestructura de vehículo (VII, *Vehicle Infrastructure Integration*) es un reto técnico muy difícil, complejo y multifacético. Ningún método propuesto hasta la fecha ha satisfecho completamente todos los objetivos de diseño. Cada uno ofrece un equilibrio diferente de objetivos contrapuestos y estrechamente interrelacionados, que incluyen la privacidad del vehículo, seguridad del sistema, escalabilidad del sistema, robustez del sistema, mantenimiento del segmento del vehículo, baja complejidad, implementación práctica y operación ubicua.

Se conocen diversas categorías de aproximaciones para la gestión de claves y certificados anónimos. Una de esas categorías incluye esquemas de certificado combinatorio que son aproximaciones de clave compartida donde cada vehículo utiliza un pequeño número de claves y certificados que se extraen aleatoriamente desde un conjunto compartido de claves y certificados. Las claves del conjunto pueden crearse mediante un algoritmo de generación de claves. La privacidad se consigue debido a que cada clave y certificado se comparte por muchos vehículos. Sin embargo, el equilibrio entre escalabilidad, privacidad y comportamiento en esta categoría está limitado.

Otra categoría es un esquema de certificado no vinculado, de corta duración, en el que se asigna a cada vehículo un gran número de claves únicas. La privacidad se consigue debido a que cada vehículo puede usar uno de entre un gran número de certificados en cualquier momento.

Los esquemas básicos de certificado anónimo combinatorio, o esquemas combinatorios básicos, consiguen privacidad distribuyendo el mismo par de claves pública-privada y su certificado asociado a un gran número de vehículos. De ese modo, ninguna actividad relacionada con una clave y un certificado particular puede atribuirse a un solo vehículo debido a que el número de vehículos que originan potencialmente tal actividad es muy grande. Se presenta una corta descripción del esquema combinatorio básico estructurada en las tres frases siguientes: generación de clave, distribución de clave, y revocación y actualización de clave.

Generación de clave: La autoridad de certificación (CA, *Certificate Authority*) crea un conjunto de *N* ternas distribuidas de manera uniforme e independiente, conteniendo cada terna una clave pública, una clave privada secreta, y un certificado asociado.

Distribución de clave: Se proporcionará a cada vehículo un pequeño número (n) de claves, y sus certificados asociados elegidos de forma aleatoria e independiente a partir del grupo.

Revocación y sustitución de clave: Las claves y los certificados podrían ser utilizados en actividades maliciosas. Una vez que se detecta un certificado involucrado en actividades maliciosas, la CA revocará el certificado. La CA puede revocar un certificado publicándolo en una lista pública de revocación de certificado (CRL, *certificate revocation list*) que se distribuirá a todos los vehículos y otras entidades que necesiten comunicar con vehículos y que por lo tanto necesiten verificar certificados 1609.2. Se desechará cualquier señal de comunicación que use una clave revocada.

Cuando se revoca un certificado C, cada vehículo que comparte C solicitará eventualmente de la CA un nuevo par de clave y su certificado para reemplazar el certificado revocado. La CA usa el número de solicitudes de reposición de clave procedentes de cada vehículo para determinar si un vehículo es sospechoso de actividades maliciosas y si el vehículo debe continuar recibiendo claves y certificados anónimos nuevos. En particular, la CA solamente proporcionará claves y certificados anónimos a un vehículo que no haya solicitado más de *b* claves, donde *b* se refiere al umbral de reposición de clave. Cuando todos los certificados anónimos sobre un vehículo se han revocado y el vehículo deja de estar autorizado por la CA para recibir certificados anónimos nuevos, el vehículo tendrá que llevarse a estaciones de servicio para una investigación adicional y para obtener la re-autorización antes de que se le permita recibir nuevos certificados de nuevo.

Los esquemas combinatorios básicos reemplazan los certificados revocados mediante la revocación de cada clave *k* de mal comportamiento inmediatamente después de la detección y usa la misma clave *k'* nueva para reemplazar el certificado k revocado en cada vehículo que solicite un certificado de sustitución para *k*. Como alternativa, los certificados revocados pueden reemplazarse revocando *g*>1 certificados a la vez. La CA crea *g* certificados de sustitución (y sus certificados asociados) para reemplazar las *g* claves revocadas. Se proporcionará a cada vehículo que solicite la reposición de clave una clave extraída aleatoriamente con una probabilidad *p* del conjunto de claves de sustitución recién creadas y con una probabilidad *1-p* del grupo completo de *N* claves.

Se conocen técnicas para asociar los certificados anónimos asignados a un vehículo con información específica del vehículo (por ejemplo, el número de VIN), de modo que el equipo de a bordo (OBE, *on-board equipment*) no funcionará cuando se cambie a un vehículo diferente.

Los métodos de revocación y sustitución de certificado en los esquemas combinatorios básicos tienen limitaciones. Por ejemplo, si se usa el mismo certificado para reemplazar una clave revocada en todos los vehículos que tengan esa clave revocada, un atacante puede repetir su actividad maliciosa indefinidamente sin ser atrapado de la siguiente manera. En primer lugar, un vehículo envía un mensaje preparado maliciosamente usando una clave *k* dada. El sistema de VII detecta este mensaje y se revoca la clave *k*. En ese punto, es difícil detectar qué vehículo generó el mensaje preparado maliciosamente dado que varios vehículos se asignaron con la clave *k* y por tanto cualquiera de ellos podría haber actuado potencialmente de forma maliciosa. Después, todos los vehículos que compartían previamente la clave *k* actualizan esta clave y reciben una nueva clave *k'*. Ahora, el atacante sigue con su actividad maliciosa usando la nueva clave *k'*, obligando con ello a que esta nueva clave se revoque de nuevo. Este bucle podría continuar indefinidamente sin que el sistema de VII detecte qué vehículo está actuando maliciosamente.

Además, el método de los esquemas combinatorios básicos para revocar $g>1$ certificados a la vez y que proporciona a cada vehículo solicitante certificados seleccionados aleatoriamente, dará como resultado distribuciones impredecibles (incontrolables) de certificados entre los vehículos. Esto significa que la privacidad, escalabilidad y comportamiento del sistema de gestión de certificado se convertirán en desconocidos e inmanejables con el tiempo.

Las principales operaciones en el proceso de gestión de certificado anónimo son: 1) comprobación; 2) inicialización; 3) selección y rotación, y 4) revocación y sustitución de claves y certificados anónimos. La comprobación de claves y certificados anónimos puede llevarse a cabo tanto por proveedores de vehículos como por fabricantes de equipamiento original del vehículo (OEM, *original equipment manufacturers*) para asegurar el correcto funcionamiento de los componentes del software y el hardware de generación de clave y certificado.

La inicialización de claves y certificados anónimos incluye la interacción entre vehículos, distribuidores de vehículos, y OEM de vehículos, para permitir que los vehículos obtengan sus conjuntos iniciales de claves y certificados anónimos en directo. Una vez que un vehículo se inicializa con sus claves y certificados de larga duración, tal como los certificados 1609.2 CSR, el vehículo puede usar esas claves y certificados de larga duración para adquirir claves y certificados anónimos iniciales de la misma manera que adquirirá las claves y certificados anónimos posteriores.

La selección y rotación de claves y certificados anónimos incluye procedimientos usados por cada vehículo para seleccionar las claves y certificados anónimos para usar y decidir cómo y cuándo rotar (cambiar) los certificados anónimos que cada vehículo usa..

La revocación y sustitución de claves y certificados anónimos determina qué certificados anónimos deben ser revocados, revocando esos certificados de los vehículos y del sistema de VII, y proporcionando claves y certificados nuevos para reemplazar las claves y certificados revocados en los vehículos. Sin embargo, los métodos de revocación y sustitución de certificado en los esquemas de certificado combinatorio básico tienen varias limitaciones cruciales que necesitan superarse. En primer lugar, no soportan un número de moderado a alto de atacantes. En segundo lugar, darán como resultado distribuciones de probabilidad impredecibles e incontrolables de certificados entre los vehículos, dando como resultado una escalabilidad y un comportamiento del sistema impredecibles e incontrolables. En tercer lugar, carecen de algunos métodos necesarios para asegurar la operación continua del sistema de gestión de certificado. Por ejemplo, usan un umbral fijo de reposición de claves para determinar los vehículos a los que no debe permitirse que reciban nuevos certificados anónimos, pero no proporcionan un método para decrementar o restablecer los contadores de claves de reposición.

El documento WO 2008/112048 A1 divulga un método para autorizar y asignar pares de certificados y claves sin pérdida de privacidad. Se realiza un seguimiento del mal uso de los certificados.

El documento US 2005/0140964 A1 divulga un método de gestión de clave en redes de sensores distribuidos que incluye una técnica de revocación.

El objeto de la invención consiste en proporcionar un método de gestión que, en la revocación y sustitución de ternas de pares de certificados y claves, se equilibra entre objetivos de escalabilidad, privacidad y comportamiento.

Este objeto se lleva a cabo mediante las características de las reivindicaciones independientes.

Los términos que se definen a continuación se usan en todo el documento:

Certificado anónimo: un certificado asociado a un par de claves pública-privada que, cuando lo usan vehículos, no habilitará la identificación y el seguimiento de vehículos. En un esquema de certificado combinatorio, cada certificado anónimo se compartirá entre varios vehículos en el sistema de VII. El certificado se une a un mensaje firmado que se genera por el vehículo y que se usa para verificar la firma digital.

Clave anónima: un par de claves privada-pública que se comparte entre muchos vehículos en el sistema de VII y

que se usa para firmar mensajes. Las claves privadas anónimas son altamente confidenciales y cualquier compromiso de una clave anónima puede poner en peligro la integridad del sistema de VII.

Atacante: cualquier entidad que pueda estar usando claves y certificados anónimos para perjudicar, dañar o manipular el sistema de VII ya sea de forma maliciosa o ya sea de forma no intencionada.

Eliminación de atacante: el proceso de retirar o hacer que resulte inofensivo un atacante para el sistema de VII. Ejemplos de eliminación de atacante incluyen medidas preventivas del sistema, tal como el bloqueo de un vehículo (es decir, revocando completamente todos los certificados anónimos en un vehículo), y expulsando a un atacante del sistema mediante expiración del certificado.

Certificado: una forma electrónica de credencial que usa una firma digital de una autoridad digna de confianza para dar fe de la unión de una clave pública con una identidad y/o un conjunto de permisos.

Bloqueo: una acción emprendida por el sistema de VII para denegar solicitudes de certificados, típicamente debido a excesivos intentos de reposición de clave.

Aplicación privada: un servicio de valor añadido opcional seleccionado por el propietario u ocupante del vehículo que se entrega al hacer uso del sistema de VII.

Clave privada: un código de encriptación/desencriptación relacionado matemáticamente con una clave pública emparejada en un sistema criptográfico asimétrico. Una clave privada se mantiene en secreto y se usa para desencriptar información encriptada mediante su clave pública emparejada o información de firma como prueba de autenticidad o integridad.

Aplicación pública: un servicio obligatorio en el sistema de VII, generalmente para seguridad pública o movilidad mejorada, del que todos los vehículos participan al usar mensajes anónimos.

Clave pública: un código de encriptación relacionado matemáticamente con una clave privada emparejada en un sistema criptográfico asimétrico. Una clave pública se comparte y se usa para encriptar información que solamente puede desencriptarse por su clave privada emparejada. Es computacionalmente inviable deducir una clave privada a partir de una clave pública.

Segmento de vehículo: el conjunto de hardware y software instalado en cada vehículo que soporta funciones de VII.

Breve sumario de la invención

La presente invención proporciona ventajosamente técnicas para resolver algunos de los problemas de la gestión de certificado anónimo combinatorio abordando los aspectos críticos referentes a su factibilidad, escalabilidad y comportamiento. Se presentan métodos y procedimientos para gestionar claves y certificados criptográficos de identificación y anónimos IEEE 1609.2 y certificados anónimos en el sistema de integración de infraestructura de vehículo (VII), junto con métodos para la gestión de certificados de identificación y anónimos en una arquitectura de autoridad de certificación dividida diseñada para potenciar la privacidad del vehículo. Se proporcionan métodos novedosos para que los vehículos seleccionen con prudencia un certificado anónimo para su uso y para cambiarlo dinámicamente para mejorar la privacidad del vehículo. Se describe la operación y el fundamento matemático de cada técnica y los métodos de selección de certificado anónimo.

El método de la invención para la gestión de certificados y claves criptográficas para una pluralidad de vehículos comprende las etapas de generar un grupo de ternas usando un algoritmo de generación de clave, teniendo el grupo un número de ternas del tamaño del grupo de claves; distribuir a y asociar con cada vehículo de la pluralidad de vehículos un número pequeño de ternas elegidas aleatoriamente a partir del grupo de ternas; revocar una terna de las ternas elegidas cuando se detecta que la terna se ha usado en actividad maliciosa; y para cada vehículo asociado a la terna revocada, determinar si debe sustituirse la terna revocada usando uno o más perfeccionamientos.

Los perfeccionamientos pueden incluir una técnica de sustitución de clave probabilística que comprende las etapas de revocar un número c de ternas que se eligen aleatoriamente entre las ternas del grupo que no están revocadas actualmente, donde el número c es un número entero pequeño; seleccionar un número c1 de ternas nuevas generado de forma aleatoria e independiente usando el algoritmo de generación de claves, donde el número c1 es el número c más uno; designar un número c1 de ternas nuevas para reemplazar las ternas revocadas, y enviar la terna actualizada elegida al vehículo solicitante.

Un segundo perfeccionamiento puede ser una técnica de decremento de contador de reposición de clave que comprende para cada vehículo las etapas de crear un identificador anónimo y mantener un registro de reposición de claves asociado al identificador anónimo; incrementar un contador de reposición de claves en el registro de reposición de clave para el identificador anónimo según un número de claves que el vehículo solicite durante un periodo de tiempo; y decrementar el contador de reposición de claves para cada identificador anónimo en una cantidad si no se produjo ninguna petición de reposición de clave durante un periodo de tiempo previo, a menos que

el contador de reposición de claves sea igual a uno de un umbral de reposición de clave y sea cero, en el que cuando el contador de reposición de claves sea menor o igual que el umbral de reposición de claves para el vehículo, reemplazar la terna revocada para el vehículo.

Un tercer perfeccionamiento puede ser una técnica de umbral de reposición de clave dinámico que comprende las etapas de para cada vehículo crear un identificador anónimo y mantener un registro de reposición de claves asociado al identificador anónimo; si el vehículo está asociado a la terna revocada, añadir una marca en contra del vehículo; elegir un umbral basado en la marca, el número pequeño de ternas asociadas al vehículo, y el grupo de claves, y si la marca es menor que el umbral, reemplazar la terna revocada.

Un cuarto perfeccionamiento puede ser una técnica de aislamiento de ataque geográfico que comprende las etapas de compilar una lista de vehículos a los que se distribuyó la terna revocada; y para cada vehículo de la lista de vehículos, si el vehículo ha dado prueba de estar en una posición geográficamente diferente de un RSE que registró la terna revocada, retirar el vehículo de la lista y reemplazar la terna revocada.

Un quinto perfeccionamiento puede ser una técnica de prueba de posición geográfica que comprende las etapas de compilar una lista de vehículos a los que se distribuyó la terna revocada; solicitar para cada vehículo de la lista de vehículos una prueba de posición desde un RSE y, si la prueba de posición muestra que el vehículo está en una posición geográficamente diferente de un RSE que registró la terna revocada, retirar el vehículo de la lista y reemplazar la terna revocada.

Breve descripción de los dibujos

La invención se describe adicionalmente en la descripción detallada a continuación, mediante referencia a los dibujos considerados a título de realizaciones no limitativas de la invención, en los que los mismos números de referencia representan partes similares en todos los dibujos. Como debe entenderse, sin embargo, la invención no se limita a las disposiciones y modalidades precisas representadas. En los dibujos:

la figura 1 es un diagrama de flujo de una primera realización;

la figura 2 ilustra la densidad de vida útil del vehículo;

la figura 3 ilustra la vida útil esperada del vehículo;

la figura 4 es un diagrama de flujo de una segunda realización;

la figura 5 es un diagrama de flujo de una tercera realización;

la figura 6 es un diagrama de flujo de una cuarta realización, y

la figura 7 es un diagrama de flujo de una quinta realización.

Descripción detallada de la invención

Los esquemas de certificado combinatorio o esquemas combinatorios básicos incluyen aproximaciones de clave compartida donde cada vehículo usa un número pequeño de claves y certificados que se extraen aleatoriamente desde un conjunto compartido de ternas, o claves y certificados. La privacidad se logra debido a que cada clave y certificado se comparte por muchos vehículos. Se proporcionan realizaciones de la invención que habilitan esquemas de certificado combinatorio para manejar un número significativamente más alto de atacantes mientras se mantiene una alta privacidad y un bajo impacto sobre vehículos inocentes. Esas realizaciones pueden implementarse individualmente o en diversas combinaciones para potenciar el esquema combinatorio básico.

Sustitución de clave probabilística

El objetivo de esta realización es conseguir dos propiedades simultáneamente: impedir que una actividad maliciosa repetida continúe indefinidamente sin ser detectada y mantener la distribución de probabilidad de los certificados entre vehículos con el paso del tiempo. Esta estrategia de revocación y sustitución de certificado anónimo permite la detección de vehículos repetitivamente maliciosos, mantiene la misma distribución de probabilidad de los certificados anónimos sobre los vehículos y solamente acarrea unos pequeños gastos extra.

Esta realización es una estrategia de reposición de clave inteligente para superar dos limitaciones críticas de esquemas de certificados combinatorios básicos. La realización puede implementarse como un perfeccionamiento para un esquema combinatorio básico. En primer lugar, esta nueva estrategia de reposición de clave permite que la CA aísle probabilísticamente a un atacante de forma rápida a medida que continúa el proceso de reposición de clave situando implícitamente un atacante entre un conjunto diferente de vehículos inocentes en cada ronda de reposición de claves, obligando de ese modo al atacante a tener la mayor homogeneidad entre los conjuntos de vehículos a los que se repuso la clave. En segundo lugar, mantiene la distribución uniforme de los certificados anónimos entre todos los vehículos, lo que ayuda a asegurar que el sistema de gestión de certificados tiene un comportamiento predecible (y por tanto controlable) con el paso del tiempo a medida que los vehículos entran y salen del sistema.

Según esta estrategia, siempre que se revoca una terna o clave *k*, la CA elegirá también revocar un número, por ejemplo un "número *c*" o *c* ternas o claves *k(1), ... k(c)* adicionales, que se eligen aleatoriamente entre las claves que se encuentran en la versión actual del conjunto y que no estén actualmente revocadas, para algún número entero pequeño *c≥1* (aquí, elegir un número *c* pequeño es solamente relevante con respecto a la evaluación de comportamiento). Además, la CA selecciona *c*+1 nuevas claves *k', k'(1), ..., k'(c)* generadas de forma aleatoria e independiente usando el algoritmo de generación de clave, y designa esas claves para reemplazar las claves revocadas en la estructura del esquema. Por último, tras recibir una petición del vehículo para actualizar ya sea la clave *k* o ya sea una de las c claves *k(i)* revocadas adicionales, la CA actualizará cualquiera de esas claves usando la modificación probabilística siguiente con respecto a la estrategia previa.

La CA elige de forma aleatoria e independiente una entre las nuevas claves *k', k'(1), ..., k'(c)* y envía esta clave elegida como la nueva clave al vehículo que la solicitó. Se consiguen dos propiedades principales de este procedimiento de actualización de clave que se discuten a continuación; ninguna de estas propiedades se logra mediante esquemas básicos de certificado combinatorio.

La primera propiedad consiste en que la distribución estacionaria de claves entre vehículos se mantiene. De manera más concreta, la estrategia anterior mantiene las siguientes invariables: 1) en cualquier momento, el grupo de claves contiene *N* claves que se eligen de forma aleatoria e independiente según el algoritmo de generación de clave asociado; 2) cada vehículo está dotado de y asociado a *n* claves distribuidas de manera uniforme e independiente del conjunto de claves que están en la versión actual (actualizada) del grupo de claves de tamaño *N*. Estas y otras invariables relativas mantenidas mediante la estrategia anterior son de importancia crucial para preservar el análisis de los parámetros de comportamiento diversos asociados con el esquema de certificado incluso tras múltiples revocaciones de claves y por lo tanto a lo largo de la vida útil del esquema.

La segunda propiedad de esta estrategia de revocación de clave es que ayuda a descubrir rápidamente qué vehículo es responsable de un comportamiento o una actividad repetidamente maliciosos, según se expone a continuación.

Eliminación de atacante mediante una prueba de clave vinculada

Se supone que la actividad maliciosa desde un vehículo llega en forma de uno o más mensajes particulares, cada uno de ellos firmado usando un par de claves particular y se supone además que esta actividad maliciosa es detectable. Con ello, dado un mensaje particular enviado por un vehículo, existe un procedimiento que establece si éste contiene actividad maliciosa. Un procedimiento para descubrir todos los atacantes que enviaron mensajes que contienen actividad maliciosa puede llevarse a cabo de la siguiente manera.

En primer lugar, para cualquier terna o clave que está asociada a un mensaje que contiene actividad maliciosa, se registra una lista de atacantes candidatos. La lista contiene la lista de vehículos a los que se distribuyó esta terna. Para reducir esta lista, todos los vehículos que han actualizado esta terna revocada y han dado prueba de estar en una posición geográficamente diferente de la zona geográfica del equipo de carretera (RSE, *RoadSide Equipment*) que grabó el mensaje con actividad maliciosa, se retiran de la lista.

Alternativamente, según se muestra en las técnicas de contador de reposición de clave y de umbral de reposición de clave a continuación, se puede mantener un conjunto de todos los conjuntos de ternas o claves distribuidas a los vehículos. Para cada conjunto del número de claves revocadas, un contador en el conjunto puede actualizarse. En cualquier momento, si existe una terna que tiene una lista con un solo vehículo en la misma, o un solo contador de reposición de clave actualizado, entonces el vehículo se declarará el único candidato de actividad maliciosa con clave k. Para todas las ternas o claves de actividad maliciosa restantes, se consideran todas las listas asociadas a ellas, y se cuenta el número de apariciones de identidades del vehículo en ellas. Es decir, para cada vehículo v, y en cualquier momento, se define ml(v) como igual al número de listas a las que pertenece este vehículo en este momento. Aquí, el número ml(v) indica el "nivel malicioso" de este vehículo en particular. Se pueden distinguir tres casos:

Si existe un vehículo tal que ml(v)>2n, este vehículo es un "fuerte candidato para actividad maliciosa repetida".

Si existe un vehículo tal que n<=ml(v)<2n, este vehículo es un "candidato para actividad maliciosa repetida".

Si existe un vehículo tal que 2<ml(v)<n, este vehículo es un "candidato débil para actividad maliciosa repetida".

Obsérvese que el parámetro de umbral establecido anteriormente igual a 2n puede tener que cambiarse según configuraciones concretas variables de los parámetros n, N y V.

La figura 1 es un diagrama de flujo que ilustra la sustitución de clave probabilística. Inicialmente, se llevan a cabo los procesos de esquema combinatorio básico (no representados) de modo que un vehículo obtiene un número pequeño de ternas elegidas aleatoriamente a partir de un grupo de ternas, y cuando se detecta actividad maliciosa, la terna asociada a la actividad maliciosa se revoca, y se hace necesario determinar si debe reemplazarse la terna revocada para un vehículo en particular. En la etapa S1 de esta sustitución de clave, se revocan *c* ternas; estas ternas se eligen aleatoriamente entre las ternas del grupo que no estén actualmente revocadas. En la etapa S2, se

seleccionan c+1 nuevas ternas, generadas de forma aleatoria e independiente. Las nuevas c+1 ternas se destinan a reemplazar las c ternas revocadas en la etapa S3. Un vehículo solicita una terna actualizada en la etapa S4 y en la etapa S5 se elige una terna entre las c+1 ternas y se envía al vehículo solicitante.

Opcionalmente, pueden llevarse a cabo las siguientes etapas opcionales. Para cada terna revocada, una lista de vehículos a los que se distribuyó la terna revocada puede compilarse en la etapa S6 y todos los vehículos inocentes, es decir, los vehículos que tienen actualizada la terna revocada y han dado prueba de estar en una posición geográficamente diferente de un RSE que registró la terna revocada, pueden retirarse de la lista en la etapa S7.

Decremento de contador de reposición de clave

Una aproximación esencial y efectiva para detectar si un vehículo puede estar haciendo un mal uso de sus certificados anónimos consiste en mantener un seguimiento y un análisis de cuántas veces el vehículo ha solicitado nuevos certificados durante periodos de tiempo dados. Las formas en las que se mantienen tales contadores de reposición de clave para los vehículos son esenciales para la escalabilidad de los esquemas de certificados anónimos y el impacto sobre vehículos inocentes. Esta realización es un forma inteligente de decrementar dinámicamente los contadores de reposición de clave de vehículo dependiendo de las actividades de reposición de clave del vehículo para reducir significativamente el impacto negativo acumulativo de la revocación de certificado sobre vehículos inocentes. La realización puede implementarse como un perfeccionamiento en un esquema combinatorio básico.

Esta realización reduce significativamente el número de vehículos inocentes bloqueados y mejora la vida útil del vehículo, es decir, el tiempo antes de que un vehículo sea bloqueado, y por lo tanto permite que los esquemas combinatorios básicos manejen un número significativamente más alto de atacantes mientras mantienen los mismos niveles de privacidad e impacto sobre vehículos inocentes. Una estrategia de decremento de contador de reposición de clave apropiadamente diseñada resulta también necesaria para permitir que los esquemas de certificado combinatorio sigan funcionando con el paso del tiempo debido a que, sin ningún método de decremento de contador de reposición de clave diseñado apropiadamente, los contadores de reposición de clave crecerán indefinidamente y harán eventualmente que esos contadores de reposición de clave no puedan usarse.

En esta realización, no se realizan suposiciones inherentes en relación con el número de atacantes o bien con el número de certificados que usan en sus ataques. Se puede combinar con cualquiera de las otras realizaciones. Se realiza la suposición de que la CA de asignación mantiene un registro de cada conjunto de pares de claves pública-privada y de sus certificados asociados. A continuación se proporciona una descripción de cómo podría implementarse esta realización.

Cuando se inicializa un vehículo, la CA de asignación crea un identificador anónimo (AID, *anonymous identifier*). La CA de asignación selecciona n>0 pares de claves pública-privada anónimos y sus certificados asociados, es decir, ternas, y las envía de forma segura al vehículo. La CA de asignación mantiene un registro de reposición de clave con un contador de reposición de clave (RC, *Rekey Counter*) asociado a cada identificador anónimo. La CA de asignación incrementa el contador de reposición de clave asociado para cada vehículo según el número de claves que el vehículo solicite durante un periodo de tiempo específico. No se concederán peticiones de reposición de clave a vehículos cuando su RC exceda el umbral de reposición de clave (RT, *Rekey Threshold*).

La CA de asignación decrementa el RC para cada AID en una cantidad específica si no ha existido ninguna solicitud de reposición de clave durante el periodo de tiempo anterior. Si el RC es igual al RT, entonces la CA de asignación no decrementa el RC. Una vez que el vehículo ha alcanzado el límite de RT, se bloquea de forma efectiva hasta que se haya sometido a una inspección y se haya autorizado a recibir claves adicionales. La CA de asignación no decrementará el RC por debajo de cero (0) con independencia de cuánto tiempo haya estado el vehículo sin solicitar reposición de clave. Esto mantiene el RC asociado a cada AID entre 0 y el valor de RT.

El método mejora la vida útil del vehículo al decrementar el RC del vehículo si no existiera ninguna solicitud de reposición de clave en el periodo de tiempo anterior. Por el contrario, el esquema combinatorio básico permite que el RC crezca con el paso del tiempo provocando que los vehículos se bloqueen a una velocidad más rápida. Sin embargo, la efectividad de esta realización para incrementar la vida útil del vehículo en relación con el esquema combinatorio básico se reduce a medida que incrementa el número de atacantes. Esto se debe a que un número mayor de atacantes cubrirá una fracción mayor de vehículos inocentes que un número menor de atacantes.

Motivación para el método

Un atacante provocará que sus claves se revoquen. Cada clave que se revoque se mantendrá también por vehículos inocentes. Sin embargo, muy pocos vehículos inocentes comparten más de una o dos claves con un atacante particular. Esto significa que si existen pocos atacantes, los atacantes podrán bloquearse en su totalidad antes que los vehículos inocentes que comparten alguna de sus claves. Con el paso del tiempo, el efecto acumulativo de los atacantes provocará que los vehículos inocentes se bloqueen. Un vehículo inocente puede tener solamente una clave revocada cada dos meses debido a la actividad de un atacante, pero esto significa que después de dos años el vehículo se bloqueará si el RT es menor de doce.

El perfeccionamiento actual reduce el RC de los vehículos para los que no han existido solicitudes de reposición de clave durante un periodo de tiempo. Un vehículo inocente podría seguir adelante varios meses antes de tener una clave revocada por actividad del atacante. A estos vehículos se les reducirán sus RC de modo que cuando experimenten revocación de clave debido a la actividad del atacante, estarán mejor capacitados para resistir el efecto sin bloquearse. Son posibles otras opciones para implementar un decremento, por ejemplo rebajando el contador en una cantidad fija por unidad de tiempo (correspondiente a las revocaciones esperadas por unidad de tiempo para un vehículo inocente). El beneficio potencial de un algoritmo de decremento más elaborado es un área que podría estudiarse adicionalmente.

Vida útil esperada del vehículo

Sea N (tamaño del grupo de claves) el número de ternas o claves anónimas en el grupo; sea n el número de certificados anónimos mantenidos por cada vehículo a la vez; y establézcase b como el umbral de reposición de clave, RT.

Considérese un vehículo que acaba de introducirse en el sistema con su RC establecido en cero. Se calcula el número esperado de periodos de tiempo antes de que el vehículo se bloquee si existen m atacantes por periodo.

La función de distribución de probabilidad para el RC del vehículo en el periodo t se calcula recurrentemente de la siguiente manera.

Sea S(k, t) la probabilidad de que el RC del vehículo sea igual a k en el periodo t.

El vehículo se introdujo con un contador de reposición de clave establecido en 0 de modo que S(0, 0)=1 y S(k, 0)=0 si k>0.

Para t=1 y $0 \leq k \leq b$ se tiene S(k, 1)=P(k) donde se define P(k)=B(k, mn/N), la probabilidad binomial de k apariciones en m pruebas con probabilidad n/N.

Para t>1 se tiene:

$$S(0,t)=S(0,t-1)P(0)+S(1,t-1)P(0).$$

Para 0<k<b-1 se tiene:

$$S(k,t) = S(k+1,t-1)\,P(0) + \sum_{i=0}^{k-1} S(i,t-1)\,P(k-i)$$

Para k=b-1 se tiene:

$$S(b-1,t) = \sum_{i=0}^{b-1} S(i,t-1)\,P(b-1-i)$$

Para k=b se tiene:

$$S(b,t) = 1 - \sum_{i=0}^{b-1} S(i,t)$$

S(b, t)-S(b, t-1) es la función de densidad de probabilidad de la vida útil del vehículo, de modo que el valor medio de la distribución viene dado por:

$$\sum_{t=1}^{\infty} t\left(S(b,t) - S(b,t-1)\right)$$

Si hacemos que el intervalo de tiempo sea de meses, entonces la figura 2 muestra la densidad de vida útil del vehículo para m=1.000, b=10, n=5 y N=10.000.

En este caso, nuestro método da como resultado una vida útil esperada del vehículo de 153 meses. Por el contrario, en el esquema combinatorio básico, la vida útil esperada del vehículo con esos mismos parámetros es solamente de seis meses, de modo que este método mejora significativamente la vida útil del vehículo.

La figura 3 muestra la vida útil esperada del vehículo como una función de m, el número de atacantes por periodo de tiempo. En ese caso, el periodo de tiempo es de un mes.

Obsérvese que el método es más efectivo cuanto menor sea el número de atacantes. Para un número mayor de

atacantes por mes, el método puede extenderse incrementando el RT. Esto permite que los atacantes reciban más claves pero minimiza el impacto de bloqueo de vehículos inocentes.

Análisis de ataque a gran escala

En un ataque a gran escala que esté basado en las claves desde muchos vehículos comprometidos, una capacidad de detección de intrusión asociada a la CA de asignación puede calcular el RT requerido que se necesita para mantener un nivel establecido de bloqueo del vehículo inocente. Esto limitará el daño colateral del ataque y permitirá que el sistema siga funcionando a niveles casi normales. La penalización es que puede llevar más tiempo retirar el número de vehículos que están operando como atacantes en el sistema.

Debe apreciarse que una unidad con mal comportamiento que no sea un vehículo, se eliminará de forma inmediata puesto que hace un mal uso de sus claves. Por ejemplo, tales unidades podrían ser ordenadores portátiles que se han programado para usar claves anónimas. El proceso de reposición de clave requiere que el vehículo tenga una clave de identificación de modo que a los impostores de vehículos no se les podrá reponer la clave.

En caso de ataque a gran escala, el decremento de RC por periodo puede necesitar hacerse mayor de modo que el sistema pueda retornar más rápidamente a la normalidad tras el ataque. De hecho, el periodo de tiempo de reposición de clave podría acortarse en combinación con el RT incrementado y el decremento de RC para responder a eventos sobre el terreno mientras gestiona la crisis.

La figura 4 es un diagrama de flujo que ilustra el decremento del contador de reposición de clave. Inicialmente, los procesos de esquema combinatorio básico se llevan a cabo según se ha descrito anteriormente. En la etapa RC1, se crea un identificador anónimo para cada vehículo y se asocia un registro de reposición de claves a este identificador anónimo. En la etapa RC2, un contador de reposición de clave en el registro de reposición de claves se incrementa según un número de claves que el vehículo solicita durante un periodo de tiempo. Se realiza una comprobación en la etapa RC3 para determinar si las solicitudes de reposición de clave se produjeron durante un periodo de tiempo anterior. Si no se produjo ninguna solicitud de reposición de clave (RC3=NO), el valor del contador de reposición de clave se compara con un umbral de reposición de clave en la etapa RC4. Si el contador de reposición de clave es menor que el umbral de reposición de clave (RC4=SÍ), el contador de reposición de clave se compara con cero en la etapa CR5. Si el contador de reposición de clave es mayor que cero (RC5=SÍ), el contador de reposición de clave se decrementa en una cantidad en la etapa RC6. En la etapa RC7, la terna revocada para el vehículo se reemplaza y el proceso se termina.

Si el contador de reposición de clave es igual al umbral de reposición de clave (RC4=NO) o el contador de reposición de clave es cero (RC5=NO), el contador de reposición de clave no se decrementa y el proceso se termina.

Umbral de reposición de clave dinámica

Esta realización utiliza un modelo matemático para eliminar atacantes de forma anónima y proporciona una novedosa aproximación que permite que el sistema de VII controle el número de vehículos inocentes que pueden ser acusados incorrectamente de actividad maliciosa. Estos objetivos se alcanzan estableciendo y ajustando dinámicamente el umbral de reposición de clave en base a criterios de comportamiento objetivo, por ejemplo, relación de eliminación de falso atacante, y número total de certificados mal usados para la población de vehículos. El método hace un seguimiento del número de certificados mal usados por cada vehículo de una manera anónima sacando ventaja del hecho de que el conjunto de *n* certificados mantenidos por un vehículo es un seudónimo de vehículo relativamente único o “ID anónimo”.

Después de que uno o más certificados han sido detectados como involucrados en actividades maliciosas, la CA necesita revocar esos certificados. Además, la CA necesita conocer qué vehículos están involucrados en actividades maliciosas de modo que detendrá la previsión de certificados anónimos a esos vehículos para impedir que los atacantes ataquen el sistema de VII indefinidamente. Sin embargo, la CA podría permitir que los vehículos inocentes pasen a compartir certificados anónimos con los atacantes para seguir recibiendo certificados anónimos que reemplacen sus certificados revocados.

El esquema combinatorio básico usa un umbral de reposición de clave fijo, *b*, para decidir qué vehículos son atacantes y por tanto no se les debe asignar ya certificados anónimos. Según se ha expuesto anteriormente, la CA hace un seguimiento del número de solicitudes de cada vehículo usando su contador RC de reposición de claves. Una vez que el RC para un vehículo excede el umbral de reposición de claves (RT) fijo *b*, se considera que el vehículo es un atacante (es decir, hace mal uso de sus certificados anónimos) y no debe permitirse que reciba ya nuevos certificados anónimos.

Este esquema básico tiene al menos las siguientes limitaciones críticas. Una, bloqueará un número excesivamente grande de vehículos inocentes incluso para un número relativamente pequeño de atacantes, lo que hará que la aplicación pública de VII deje de funcionar y creará también una carga de trabajo excesiva en las estaciones de servicio que necesitarán examinar esos vehículos “bloqueados” y volver a autorizarlos para que reciban certificados anónimos de nuevo.

Dos, los RC crecerán con el paso del tiempo según se detecte que los nuevos certificados anónimos están siendo mal usados. Eventualmente, los RC para todos o la mayor parte de los vehículos estarán por encima del RT *b*. No existe ningún método para decrementar o restablecer dinámicamente los RC con el paso del tiempo. Tres, es difícil determinar un valor de RT fijo que sea apropiado para un sistema de VII a escala nacional durante un largo periodo de tiempo.

Por lo tanto, es necesario desarrollar un método para establecer y ajustar dinámicamente el RT. Debería establecerse de manera que cumpla los objetivos de gestión de certificado crítico, tales como el nivel de escalabilidad, el nivel de privacidad, y el comportamiento, por ejemplo la proporción de vehículos inocentes acusados erróneamente. El RT deberá ajustarse para responder al entorno del sistema cambiante, tal como el número de atacantes detectados en el sistema, para reducir el impacto de los atacantes sobre vehículos inocentes.

Se describe una realización que toma como entrada los certificados mal usados detectados y establece y ajusta dinámicamente el RT para que cumpla con los criterios de sistema dados y usa el RT dinámico para detectar atacantes de una manera anónima, es decir sin identificar los vehículos. La realización puede implementarse a modo de un perfeccionamiento en un esquema combinatorio básico. Pueden usarse también los mismos métodos descritos en esta realización para detectar certificados mal usados. Además, el método se extiende fácilmente al caso en que los certificados o marcas negras duran poco tiempo.

Esta sección analiza también la efectividad de la realización de detección anónima propuesta cuando existen doscientos millones de vehículos, v = 200.000.000.

Para el análisis matemático en esta sección, se supone que los certificados mal usados se detectan de forma inmediata y sin error. Cada certificado mal usado se marca en negro inmediatamente después de su detección. El marcado en negro permite la revocación de los certificados, pero la revocación inmediata del certificado es una alternativa. Adicionalmente, se supone que la CA sólo necesita saber los v conjuntos de certificados anónimos que se han asignado a los vehículos en cualquier momento. La CA, sin embargo, no conoce a qué vehículos se han asignado los certificados. Es posible que la CA cuente el número de certificados revocados dentro de cada conjunto de certificados (que representa un vehículo).

Intuitivamente, si el número de certificados marcados en negro para un vehículo es relativamente alto, es probable que sea un vehículo con mal comportamiento. Resulta deseable detectar los vehículos con mal comportamiento tan rápido como sea posible, sin impactar en demasiados vehículos inocentes. Los esquemas para la detección de vehículos con mal comportamiento se presentan a continuación con el análisis de comportamiento.

Esquema de detección 1: Esquema de umbral

Cada vez que se detecta que un certificado está siendo mal usado, la CA pone una marca negra contra cada vehículo que comparte ese certificado. Una observación importante es que, estadísticamente, un atacante tendrá más marcas negras que un vehículo inocente y que las marcas negras contra el atacante crecerán más rápidamente que las marcas negras para vehículos inocentes.

El fundamento matemático para la observación es de la siguiente manera. Para un vehículo inocente, la probabilidad de tener b certificados con marcas negras después de que un total de mt certificados se han marcado en negro, es:

$$((1-(1-n/N)^{mt})^b \approx (1-e^{-ct})^b$$

donde $c = mn / N$.

Para un atacante que ha usado exactamente k certificados marcados en negro, esta probabilidad es más alta: puesto que los certificados mal usados se detectan y se marcan en negro de forma inmediata, la probabilidad de tener b certificados marcados en negro después de que un total de mt certificados han sido marcados en negro, es $((1-(1-n / N)^{mt})^{b-k} \simeq (1-e^{-ct})^{b-k}$.

Alternativamente, con probabilidad de $((1-(1-n / N)^{mt})^b \simeq (1-e^{-ct})^b$, un atacante que haga un mal uso de k certificados tiene $b+k$ marcas negras.

Así que de hecho, es probable que un atacante tenga más marcas negras que un vehículo inocente. Cuántas más de ellas depende de cuántos certificados use mal.

Ahora supóngase que un vehículo tiene b certificados con marcas negras. ¿Qué probabilidad hay de tener b o más certificados con marcas negras revocados si el vehículo es de hecho inocente? Ignorando un posible límite máximo sobre el número de eventos de reposición de clave por vehículo, esta probabilidad es

$$p(b) = \sum_{k=b}^{\infty} (1-e^{-ct})^k = e^{ct}(1-e^{-ct})^b \qquad (1)$$

lo que se denomina *valor-p* de observación de *b* revocaciones para un vehículo. Este valor p se reduce con *b*: cuanto mayor es *b,* menor es la probabilidad de que el vehículo sea inocente.

Un método de detección para vehículos con mal comportamiento puede elaborarse como método de umbral, lo que de hecho es una prueba de hipótesis estadística. Se está probando la hipótesis H_0: el vehículo usó todos sus certificados correctamente, frente a la alternativa general H_1: el vehículo hizo un mal uso de uno o más de sus certificados. Una estadística de prueba *T* suficiente es el número de certificados que se han marcado en negro para el vehículo en cuestión. Esta prueba es un método de umbral (de hecho, es una prueba de proporción de probabilidad generalizada): se acepta H_0 si $T < t$, y se rechaza, es decir se detecta que un vehículo ha tenido un mal comportamiento, si $T \geq t$. Se puede elegir un umbral t_α de modo que la probabilidad de declarar falsamente que un vehículo ha tenido un mal comportamiento sea α.

Supóngase que un vehículo está monitorizado. Se elige t_α resolviendo: $p(t_\alpha) = \alpha$, o

$$p(t_\alpha) = e^{ct}(1-e^{-ct})^{t_\alpha} = \alpha$$

$$t_\alpha = \log(e^{-ct}\alpha)/\log(1-e^{-ct})$$

Obsérvese que $t_\alpha(mt,n,N,\alpha)$ depende de los parámetros α, *mt, n y N*. Cuantos más certificados son revocados (es decir, para *mt* más alto), el umbral es más alto.

Para $\alpha = 0{,}05$, $mt = 1000$, $n = 5$, $N = 10.000$, y por tanto $ct = 0{,}5$, se obtiene el umbral $t_\alpha = \log(e^{-ct}\alpha)/\log(1-e^{-ct}) = 3{,}75$. Para mantener un cinco por ciento de probabilidad de etiquetado erróneo del vehículo como de mal comportamiento, el vehículo con mal comportamiento se marca después de que tenga cuatro o más certificados marcados en negro.

Cuando existen doscientos millones de vehículos ($v = 200.000.000$), prueba $v = 200.000.000$ hipótesis H_0: el vehículo *i* es inocente, es decir, ha usado todos sus certificados correctamente, frente a las alternativas respectivas H_{i1}: el vehículo *i* ha hecho un mal uso de uno o más de sus certificados. Supóngase que todos menos un número pequeño relativo m_1 de los vehículos son inocentes (es decir, $m_0 = v - m_1$ hipótesis nulas H_{i0} son verdaderas). Entonces de media $(v - m_1)$ se plantearán α falsas alarmas y (como máximo) m_1 verdaderas. El número de falsas alarmas es de hecho un distribución binomial $(v - m_1, \alpha)$. Por lo tanto, la probabilidad de al menos una falsa alarma es $(1 - (1-\alpha)^{v-m1})$. Además, la relación esperada de falsas alarmas respecto al total de alarmas es de aproximadamente $(v-m_1)\alpha/(v-m_1)\alpha + m_1)$, lo que es casi 1. De ese modo, ¡casi todas las alarmas planteadas serán de hecho falsas alarmas!

Este ejemplo apunta la necesidad de ejercer *control de multiplicidad*. En una aproximación, puede reducirse drásticamente α de modo que la probabilidad de tener incluso una falsa alarma en la monitorización de $v = 200.000.000$ vehículos está controlada al nivel original $\alpha_{FWER}=0{,}05$. De esta manera, la tasa de error respecto a la familia *(FWER, Family Wise Error Rate)* está controlada en α_{FWER}. Para $v = 200.000.000$, esto conduce a $\alpha = 2{,}5\cdot10^{-10}$ (!). Esto ya no es práctico; por ejemplo, para $mt = 1000$, $n = 5$, $N = 10.000$ y por tanto $ct = 0{,}5$, se obtiene el umbral $t_\alpha = \log(e^{-ct}\alpha)/(\log(1 - e^{-ct}) = 24{,}3$. Esto podría detectar y etiquetar un vehículo con mal comportamiento si tiene 25 o más marcas negras. Sin embargo, este umbral conservador conduce a muchas (demasiadas) detecciones perdidas.

En la siguiente sección, se presenta una aproximación alternativa a la comprobación múltiple, que consigue mejores equilibrios entre el número de falsas alarmas y detecciones perdidas.

Esquema de detección 2: Control de tasa de descubrimiento falsa

En los últimos años, una aproximación alternativa a la comprobación múltiple ha alcanzado popularidad; en vez de controlar la tasa de error respecto a la familia tal como se ha descrito anteriormente, se usa un criterio de control diferente. El criterio es la tasa de descubrimiento falsa (FDR, *False Discovery Rate*). La FDR se define de la siguiente manera. Supóngase que se está comprobando *v* hipótesis nulas H_{i0}, $i = 1,..., v$ tal como se ha definido anteriormente. Entonces la tabla 1 proporciona una visión general de los errores.

Tabla 1. Número de errores cometidos cuando se comprueban *v* hipótesis nulas

Descripción de amenaza de privacidad & confidencialidad	Declarado no significativo	Declarado significativo	Total
Hipótesis nulas verdaderas	*U*	*V*	$m_0 = v - m_1$
Hipótesis nulas no verdaderas	*T*	*S*	$m_1 = v - m_0$

Total	*v* - *R*	*R*	*v*

La FDR es la proporción esperada de errores cometidos al rechazar falsamente hipótesis nulas. En términos de variables aleatorias listadas en la tabla 1, la FDR puede definirse matemáticamente como:

$$\mathbf{FDR} = E(V/V+S) = E(V/R)$$

En Controlling the False Discovery Rate: A Practical and Powerful Approach to Multiple Testing. Journal of the Royal Statistical Society,, Serie B, Vol. 57, núm. 1, pp. 289-300, 1995, Benjamini y Hochberg definen un procedimiento (procedimiento de B-H) para controlar la FDR bajo un nivel específico *q**. Consideran las estadísticas de prueba para las *v* hipótesis de prueba T_i, *i* = 1,..., *v,* y calculan sus valores *p* correspondientes $P_i=p(T_i)$ usando el cálculo del valor *p,* (1), anterior. Si las pruebas están ordenadas por el tamaño de sus valores *p,* $P_{(1)} \leq P_{(2)} \leq ... \leq P_{(v)}$, en orden creciente, este ordenamiento induce un ordenamiento equivalente sobre las estadísticas de prueba en orden decreciente: $T_{(1)} \geq T_{(2)} \geq \ldots \geq T_{(v)}$. En consecuencia, el procedimiento de B-H para controlar la FDR resulta:

- Sea *k* el *i* mayor para el que $P_{(i)} \leq \frac{i}{v} q^*$;
- Rechazar todas las $H_{o(i)}$, *i* = 1,..., *k.*

Se ha demostrado que este procedimiento garantiza que:

$$FDR = E(V/R) \leq \frac{m_0}{v} q^* \leq q^*$$

Obsérvese que el procedimiento no incorpora el número de hipótesis nulas verdaderas m_0. Si éste es grande, esto hace que la diferencia sea pequeña. Pero si el conocimiento (o una estimación) de m_0 (o de m_0 / v) está disponible, entonces el procedimiento puede hacerse más potente reemplazando el $q^* \; por \; \frac{v}{m_0} q^*$ original o su estimación.

Entonces, el procedimiento garantiza aún el control de la FDR a nivel *q**, mientras que rechaza más hipótesis nulas falsas. Incorporar el conocimiento acerca de m_0 / v subyace también en la base del incremento de potencia en el método de control de FDR del procedimiento de B-H.

El procedimiento de B-H se conoce como procedimiento de 'configuración'. Se implementa al comparar $P_{(i)} \leq \frac{i}{v} q^*$, empezando con $P_{(v)}$ y siguiendo linealmente hacia $P_{(1)}$ hasta que el algoritmo se detiene. Puesto que el método es secuencial, el umbral real en el que se rechazan hipótesis nulas es una variable aleatoria y por lo tanto el método es un método de umbral 'adaptativo' o aleatorio.

Por el contrario, Storey J., Taylor J.S., y Siegmund D., Strong Control, Conservative Point Estimation and Simultaneous Conservative Consistency of False Discovery Rates: a Unified Approach. Journal of the Royal Statistical Society, Serie B, Vol. 66, núm. 1, pp. 187-205, 2004, consideran un procedimiento de control de FDR basado en un umbral a fijo para valores p para rechazar hipótesis nulas. El procedimiento se basa en una estimación conservadora de la FDR correspondiente al rechazo con un umbral α fijo, $FDR_\lambda(\alpha)$. Aquí, λ es un parámetro de sintonización, para el que se proporciona un algoritmo de selección/estimación. Resulta interesante comparar el método de control de FDR de umbral fijo con los métodos de umbral fijo considerados anteriormente. Puesto que el número de hipótesis *v* es grande, la FDR es aproximadamente:

$$FDR = E(V/R) \approx E(V)/E(R)$$

Sea $\pi_0 = m_0 / v$. El requisito de control de la FDR a un nivel específico $FDR \leq q^*$ implica entonces:

$$\alpha \leq \frac{(1-\pi_0)q^*}{\pi_0(1-q^*)}$$

Para los parámetros: número de vehículos con mal comportamiento m_1 = 1000, *v* = 200.000.000 y *q** = 0,5 (una falsa alarma por cada alarma verdadera), se obtiene un umbral de $\alpha \leq 10^{-5} / (1-10^{-5}) \approx 10^{-5}$ para los valores p, lo que se traduce en un umbral de $t_{10\text{-}5} = \log(e^{-ct}\, 10^{-5}) \log(1-e^{-ct})$ para las estadísticas de prueba. Para mt = 1000, *n* = 5, *N* = 10.000 y por tanto *ct* = 0,5, se obtiene el umbral $t_{10\text{-}5}$ = 12,9.

Obsérvese que dado el número total de marcas negras *mt*, el número de vehículos con mal comportamiento está acotado superiormente por *mt,* y acotado inferiormente por mt/t_{α}.

Con alrededor de 1000 vehículos con mal comportamiento, para obtener una proporción de una falsa detección por cada detección verdadera, necesita detectarse si el número de certificados marcados en negro para un vehículo es 13 o más alto. Esto afecta de hecho a un equilibrio entre la aproximación de prueba simple que detecta alrededor de 4 vehículos y la aproximación derivada de FWER que detecta alrededor de 25 vehículos.

La figura 5 es un diagrama de flujo que ilustra un umbral de reposición de clave dinámica. Inicialmente, los procesos del esquema combinatorio básico se llevan a cabo según se ha descrito anteriormente. Para cada vehículo, se crea un identificador anónimo y un registro de reposición de clave asociado al identificador anónimo se mantiene en la etapa D1. Si el vehículo está asociado a una terna revocada (D2=SÍ), se añade una marca contra el vehículo en la etapa D3. Se elige un umbral en la etapa D4, estando el umbral basado en la marca, en el pequeño número de ternas asociadas al vehículo y en el tamaño del grupo de claves. Si la marca es menor que el umbral (D5=SÍ), la terna revocada se reemplaza en la etapa D6, y el proceso termina.

Si el vehículo no está asociado a una terna revocada (D2=NO), o si la marca es mayor que el umbral (D5=NO), entonces el proceso termina.

Análisis de los esquemas de detección propuestos

Actualmente se está analizando el comportamiento de los esquemas de detección propuestos de forma detallada: para varios números de atacantes, las modalidades de ataque y el número de vehículos monitorizados. Nuestros resultados preliminares muestran que:

- Según aumentan las marcas negras para todos los vehículos, se requerirá un RT mayor para conseguir los mismos criterios de comportamiento objetivo.

- Con más atacantes, el tiempo medio (número de marcas negras) hasta la detección incrementa.

- Con menos vehículos monitorizados, el umbral de detección y el tiempo medio para la detección disminuyen, lo que sugiere que las técnicas de localización geográfica deberán ayudar a incrementar la escalabilidad.

Este último fenómeno proporciona también la siguiente reflexión: separar los certificados marcados en negro en “familias” que contengan un subconjunto de atacantes puede incrementar la efectividad y la velocidad con las que el método propuesto detecta atacantes, incrementando con ello su escalabilidad y comportamiento. Tal separación puede hacerse mediante separación espacial o temporal de certificados marcados en negro. Mantener las familias de marcas negras en valores menores ayuda a mantener los umbrales de detección más bajos, y por lo tanto facilita una detección más rápida.

Bajo ataques a gran escala (un número grande de atacantes simultáneos), la separación temporal puede resultar difícil, dado que es probable que los certificados posteriores marcados en negro correspondan a diferentes atacantes. La separación espacial puede ser aún factible.

Aislamiento de ataque geográfico

Esta realización proporciona una solución al problema de “uno afecta a muchos”, por el que un atacante afecta a todos los demás vehículos que comparten el certificado usado durante el ataque, puesto que todos se consideran atacantes candidatos y han de pasar por un procedimiento de reposición de clave. Según esta solución, se define un número de zonas geográficas y la búsqueda de un atacante se concentra en la zona geográfica donde se detectó el primer mal uso del certificado. La búsqueda se extiende en cuanto a cobertura lentamente hasta que se identifica al atacante, suponiendo que el efecto debido a que un vehículo conduzca a través de zonas diferentes sea insignificante. En varios escenarios prácticos, este método convierte el efecto de “uno afecta a muchos” en un efecto de “uno afecta a ninguno”.

La realización puede ser implementada como un perfeccionamiento respecto a un esquema combinatorio básico. El objetivo de esta realización es crear una técnica novedosa que resuelva el siguiente problema de “uno afecta a muchos”. Supóngase que un atacante usa una clave anónima y su certificado asociado para enviar mensajes maliciosos. Tras el descubrimiento de actividad maliciosa en estos mensajes, el certificado se revoca y se añade a la lista de revocación de certificados. Como consecuencia, puesto que otros diversos vehículos comparten el mismo certificado, estos vehículos se ven afectados dado que se consideran atacantes candidatos y tienen que pasar por un procedimiento de reposición de clave. Al observar que los atacantes muestran implícitamente su localización en sus mensajes, y que un número muy grande de vehículos que comparten las claves del atacante estarán en ubicaciones completamente distintas, es posible observar que estos últimos vehículos no estuvieron involucrados en los ataques y por tanto no se verán afectados, y no se les requerirá reposición de clave. En varios escenarios prácticos, este método convierte el efecto de “uno afecta a muchos” en un efecto de “uno afecta a ninguno”.

Todas las estrategias de actualización de clave discutidas anteriormente requieren un procedimiento que lleve a cabo una investigación sobre qué vehículo, entre varios candidatos, fue el responsable de uno o más mensajes generados maliciosamente. Puesto que este procedimiento es caro en términos de varios recursos, resulta claramente deseable minimizar el número de vehículos inocentes que se requieren para pasar por la investigación. Esto es crucial para evitar la siguiente negación sutil de ataque de servicio: un atacante malicioso corrompe continuamente múltiples vehículos, obligando a un número mucho mayor de vehículos a generar peticiones de actualización de clave a la CA de asignación, que puede verse potencialmente desbordada con tales peticiones.

Por ejemplo, según el esquema combinatorio básico tal como se ha descrito anteriormente, para todos y cada uno de los mensajes m maliciosamente generados desde un vehículo (asociado a una clave k dada), existe un promedio de Vn/N vehículos que se van a ver sometidos al procedimiento de investigación anterior. Además, la versión del esquema combinatorio básico potenciado con sustitución de clave probabilística, que es esencial para detectar vehículos repetidamente maliciosos, incrementa adicionalmente el número de vehículos sometidos a investigación en un factor c (pequeño) multiplicativo. Al igual que para los valores prácticos de los parámetros V, n, N y c, los números pueden ser bastante altos. La técnica novedosa que sigue basada en CRL basadas en localización, reduce potencialmente, en una cantidad muy grande, el número de vehículos afectados.

El problema que se está considerando aparece intensamente conectado al problema del anonimato en el diseño de un esquema de certificado, tal como se explica ahora. Si se propone un esquema que satisfaga propiedades de anonimato deseables, entonces el número de remitentes potenciales de cualquier mensaje dado es muy grande, y por lo tanto el número de vehículos que pueden ser atacantes candidatos debido a un mensaje malicioso dado puede ser también grande. A la inversa, si buscamos formas de reducir el número de vehículos sometidos a una investigación, se acabará más probablemente con métodos que reduzcan el anonimato de los vehículos con respecto a un mensaje dado. Por lo tanto, necesitamos buscar aproximaciones que conlleven una pérdida mínima de anonimato, o minimicen el impacto de esta pérdida. En efecto, el perfeccionamiento que sugerimos tiene alguna pérdida intrínseca de anonimato como sería el caso de cualquier esquema de certificado donde los vehículos necesitan enviar mensajes a RSE dependientes de la ubicación, poniendo por lo tanto de relieve constantemente su posición geográfica aproximada.

Considérese un mensaje generado maliciosamente desde un vehículo en una posición geográfica (x, y) y asociado a una clave *k*. Debido al diseño del esquema, conocemos que existe una media de Vn/N vehículos a los que se distribuyó la clave k y que por tanto van a ser declarados atacantes candidatos con referencia a ese mensaje malicioso. Sin embargo, se espera que el número de tales vehículos que tienen posición geográfica cercana a (x, y) sea mucho más pequeño y parece inútil requerir que se declaren atacantes candidatos vehículos con una posición geográfica “suficientemente alejada” de (x, y).

Específicamente, podemos pensar en dividir el país entero, o cualquiera que sea el zona geográfica completa de interés, en un número (por ejemplo, 100) de zonas geográficas relativamente grandes y considerar solamente atacantes candidatos en la misma zona geográfica donde se observó el ataque. En este caso, el número de zonas y sus tamaños relativos se eligen de modo que, en cualquier momento dado, el número de vehículos que cambian de zona es de un orden mucho más bajo con respecto al número de vehículos que permanecen en la misma zona. Por lo tanto, la idea básica es que solamente se necesita investigar los vehículos que requieren que su clave *k* se actualice mientras están en la misma zona geográfica en la que se observó el ataque. Se espera que esto reduzca significativamente el número de vehículos involucrados en este procedimiento y no contribuya a ninguna pérdida de privacidad debido a que los vehículos restantes no son candidatos originadores del mensaje generado maliciosamente que ya se había deducido mediante el conocimiento de la ubicación del RSE que recibió ese mensaje.

Ahora se van a proporcionar más detalles sobre cómo esta técnica modifica la prueba de clave vinculada de atacante malicioso descrita anteriormente, durante la fase de eliminación de atacante. La prueba resultante se denomina prueba de clave vinculada dependiente de la geografía.

Descubrimiento de atacante malicioso

Al igual que anteriormente, se supone que la actividad maliciosa procedente de un vehículo llega en forma de uno o más mensajes, cada uno de ellos firmado usando un par de claves particular. Además, suponemos que esta actividad maliciosa es detectable eficazmente; es decir, dado un mensaje particular enviado por un vehículo, existe un procedimiento eficaz que establece si contiene actividad maliciosa.

En primer lugar, para cualquier terna que esté asociada a un mensaje que contenga actividad maliciosa, se registra una lista de atacantes candidatos, que contiene la lista de vehículos a los que se distribuyó esta terna. Para reducir esta lista, retiramos de la lista todos los vehículos que hayan actualizado esta terna revocada mientras hablan con un RSE en un zona geográfica que es diferente de la zona geográfica que registró la actividad maliciosa si tal actividad fue descubierta muy recientemente, o suficientemente distante de la zona que registró el mensaje con actividad maliciosa, si tal actividad no fue descubierta recientemente (es decir, si la zona es inalcanzable por un vehículo en la cantidad de tiempo (distancia en el tiempo) desde el momento en que la actividad maliciosa fue registrada por primera vez).

En cualquier momento, si existe una terna *k* que tenga una lista con un solo vehículo en la misma, entonces se declara este vehículo como el único candidato para actividad maliciosa con terna *k.* Para todas las restantes ternas de actividad maliciosa, se consideran todas las listas asociadas a las mismas y se cuentan las apariciones de identidades de vehículo en las mismas. Es decir, para cada vehículo v, y en cualquier momento, definimos ml(v) como igual al número de listas a las que pertenece el vehículo v en ese momento. En este caso, el número ml(v) indica el "nivel malicioso" de ese vehículo v en particular. Se pueden distinguir tres casos:

Si existe un vehículo v tal que ml(v) > 2n, se declara que el vehículo v es un "fuerte candidato para actividad maliciosa repetida".

Si existe un vehículo v tal que n ≤ ml(v) ≤ 2n, se declara que el vehículo v es un "candidato para actividad maliciosa repetida".

Si existe un vehículo *v* tal que 2 < ml(v) < n, se declara que el vehículo v es un "débil candidato para actividad maliciosa repetida".

El parámetro de umbral anterior, establecido actualmente como igual a 2n, puede tener que cambiarse según configuraciones variables concretas de los parámetros n, N, V.

La figura 6 es un diagrama de flujo que ilustra aislamiento de ataque geográfico. Inicialmente, los procesos de esquema combinatorio básico se realizan tal como se ha descrito anteriormente. En la etapa G1, se compila una lista de vehículos a los que se distribuyó la terna revocada. En la etapa G2, se comprueba cada vehículo de la lista de vehículos. Si un vehículo ha dado prueba de estar en una posición geográficamente diferente del RSE que registró la terna revocada (G2=SÍ), el vehículo se retira de la lista en la etapa G3, y su terna revocada se reemplaza en la etapa G4. A continuación, el proceso se termina.

Si el vehículo no tiene la prueba dada (G2=NO), el proceso se termina.

Análisis de la prueba de clave vinculada dependiente de la geografía

La técnica de aislamiento de ataque geográfico no afecta a las propiedades de anonimato o imposibilidad de vinculación del esquema combinatorio básico. Ahora se analizan las propiedades de eliminación de atacante mejoradas.

Se empieza analizando el caso de un solo vehículo malicioso y a continuación se pasa al caso de múltiples vehículos maliciosos simultáneos.

Caso 1 – Vehículo malicioso único: Más formalmente, supóngase que un vehículo en particular hace uso de una de sus ternas k anónimas para alguna actividad maliciosa que se ha detectado por un RSE. Como consecuencia, se revoca la terna k, así como ternas k(1),... k(c) adicionales. En ese punto, es difícil detectar qué vehículo generó el mensaje malicioso dado que a varios vehículos se les asignó la terna k y por lo tanto cualquiera de ellos podría haber actuado potencialmente de forma maliciosa.

Sin embargo, a diferencia de en el esquema combinatorio básico, no todos los vehículos que previamente compartían la terna k reciben la misma nueva terna k' con la terminación de su petición de actualización, dado que cada uno de ellos puede recibir cualquiera de las nuevas ternas k'(i) adicionales con alguna probabilidad. Ahora, si el vehículo previamente malicioso continúa su actividad maliciosa usando la nueva terna k', obligando con ello a esta nueva terna a ser revocada de nuevo, el conjunto S(k) de vehículos que comparten k' con el vehículo malicioso es muy diferente del conjunto S(k') de vehículos que previamente compartían k con el vehículo malicioso. Como resultado, el vehículo malicioso puede ser identificado como uno de los vehículos en la intersección de los dos conjuntos S(k), S(k').

Además, el efecto de intersección continuará indefinidamente en presencia de actividad maliciosa repetida, hasta que se detecte que un solo vehículo es el que ha actuado maliciosamente. Más formalmente, se observa que debido al procedimiento de asignación de reposición de clave aleatoria para la terna k' y para las c ternas k'(1),..., k'(c) adicionalmente revocadas junto con la terna k, el conjunto de vehículos que son potencialmente originadores de la actividad maliciosa repetida se reduce en un factor multiplicativo igual a 1/(c+1) después de cada ronda de actualizaciones de terna desde la CA. En este punto, mediante una "ronda de actualizaciones de terna" quiere indicarse la suposición del peor caso de que la CA actualice todos los vehículos que comparten la terna *k* usada durante la actividad maliciosa. Puesto que el conjunto original de vehículos potencialmente maliciosos tenía un tamaño medio igual a *Vn/N,* el vehículo malicioso se detectará dentro de un número de rondas de actualizaciones de terna igual de media a log(Vn/N)/log(c+1) (los logaritmos son de base 2).

La tabla 2 evalúa el número de rondas esperado de actualizaciones de terna requeridas para descubrir el vehículo malicioso que mantiene vigente su actividad maliciosa tras cada actualización de terna, bajo la suposición de que el vehículo malicioso espera que todas las actualizaciones de terna se realicen en una ronda por parte de la CA antes de continuar con su actividad maliciosa. Aquí, consideramos los valores típicos de V=200.000.000, n=6, y unas pocas instancias razonables de los parámetros N y c.

Tabla 2. Número esperado de rondas de actualización de clave para identificar un vehículo malicioso

Tamaño del grupo (N)	c = 1	c = 3	c = 7	c = 15
10000	16,8	8,4	5,6	4,2
5000	17,8	8,9	5,9	4,4
2500	18,8	9,4	6,2	4,7

Si se abandona la suposición del peor caso de que el vehículo malicioso espera a que todas las actualizaciones de ternas se realicen en una ronda por parte del CA antes de continuar con su actividad maliciosa, y se supone que el vehículo malicioso es suficientemente afortunado para esperar a que la mayor parte de una fracción q (por ejemplo, q=14) de todas las actualizaciones de clave se realicen, entonces todas las entradas de la tabla anterior deberán multiplicarse por q, reduciendo con ello significativamente estos números a constantes muy pequeñas en la mayor parte de los escenarios prácticos. Generalizando esta idea, podemos definir una tasa de *actualización de clave,* indicada como *u,* para cada vehículo, y usar en nuestro análisis la observación crucial de que el valor *u* es, para la mayor parte de los vehículos no atacantes, significativamente menor que para los vehículos atacantes.

Además, si consideramos que la técnica de aislamiento geográfico reduce significativamente el tamaño de la lista de atacantes candidatos para cualquier clave asociada a actividad maliciosa, entonces obtenemos que el vehículo malicioso podrá ser detectado dentro de un número de rondas de actualizaciones de clave igual por término medio a log (L)/log (c+1) (los logaritmos son de base 2), donde L es la longitud de esta lista original, según se ha reducido debido a aislamiento geográfico.

Los detalles de cómo se lleva a cabo la identificación real de un vehículo detectado como malicioso, dependen de los detalles de inicialización de la identificación y de las claves y certificados anónimos en la inicialización del vehículo y de la fase de preventa. Se presentan dos variantes principales para este procedimiento de inicialización de clave. La primera variante considera el caso de una CA de autorización que certifica cada clave de identificación y emite un conjunto de claves anónimas para cualquier vehículo específico. En ese caso, la CA de autorización conoce qué claves han sido asignadas al vehículo identificado. De ese modo, el sistema de detección de intrusión (IDS, *Intrusion Detection System*) solo necesitará comunicar a las CA de autorización la secuencia de claves actualmente vinculadas a la actividad maliciosa, y la CA de autorización contestará con (la lista de) los vehículos a los que se proporcionó un número suficientemente grande de esas claves.

La segunda variante considera el caso de una generación conjunta de claves anónimas desde la CA de autorización (que conoce la identidad del vehículo pero no qué claves anónimas se han asignado al mismo) y la CA de asignación (que conoce qué claves anónimas se han asignado a un vehículo pero no su identidad). En este caso, el sistema de IDS necesitará que la CA de asignación comunique la secuencia de claves actualmente vinculadas a actividad maliciosa a la CA de autorización que de nuevo contestará con (la lista de) los vehículos a los que se proporcionó un número suficientemente grande de esas claves. Obsérvese que se confía en la CA de asignación para proporcionar una secuencia correcta de claves, sin pérdida de generalidad puesto que la CA de asignación goza de la confianza de la CA de autorización para llevar a cabo correctamente también un número de otras funciones.

Caso 2 – Múltiples vehículos maliciosos: El análisis anterior ha supuesto la existencia de un solo vehículo que envía mensajes generados maliciosamente. Un escenario mucho más realista podría incluir múltiples vehículos que, en cualquier momento, están enviando simultáneamente mensajes maliciosamente computados, potencialmente desde diferentes localizaciones geográficas. De hecho, el escenario del peor caso es un ataque a gran escala en el que cada terna del grupo es utilizada por uno o más vehículos para enviar mensajes maliciosos. Según describimos ahora con mayor detalle, realizando un número de suposiciones razonables sobre la distribución de vehículos y sobre la distribución de atacantes, el análisis de este escenario aparentemente más involucrado sigue desde una extensión cuidadosa del análisis previo para un solo vehículo atacante.

Además de los parámetros *N, n, b, c, L, t, V, u* ya definidos, se considera el número de RSE o zonas geográficas *g* del país. Cada zona geográfica puede tener una densidad más baja o más alta de vehículos, con valores potencialmente variables según el momento del día o al día del año. El presente se centra principalmente en dos escenarios, uno de baja densidad de vehículos para el que usamos el parámetro *ld,* y uno de alta densidad de vehículos para el que usamos el parámetro *hd*, donde se espera que $ld << V/g$ y $hd >> V/g$. Se usará el parámetro *a* para indicar el número de ataques o de atacantes, y se considerará $\alpha > 1$ o incluso $a > N$, que modelan ataques a gran escala.

Empezaremos analizando el éxito en la eliminación de un atacante bajo muchos escenarios interesantes, según diferentes suposiciones en relación con los factores siguientes: el mayor o menor número de mensajes maliciosos enviados en cualquier ataque dado; la cantidad de tiempo transcurrido entre dos mensajes maliciosos cualesquiera enviados con respecto a cualquier ataque dado; las zonas geográficas donde se localiza cada atacante; la baja o alta densidad de vehículos en esas zonas geográficas donde se localiza el ataque.

Escenario (a): En este escenario, se hacen las siguientes suposiciones; los atacantes pueden enviar solamente un único mensaje para realizar su ataque; las zonas geográficas donde cada atacante se ubica están distribuidas de manera independiente y uniforme en el país y tienen una baja densidad de vehículos.

En este caso, al final de la técnica de aislamiento geográfico, los vehículos que, en el momento del ataque, estaban fuera de cualquiera de las zonas geográficas donde ocurrió el ataque, tienen ya probada su inocencia al proporcionar una posición diferente como prueba de la posición geográfica. Sin embargo, para cada zona geográfica donde ocurrió un ataque, existe al menos una terna revocada y una lista de *L* atacantes candidatos que tienen la misma terna que la involucrada en el ataque, y que estaban en la misma zona geográfica en el momento del ataque. Dados los parámetros *n, N, ld,* el valor esperado de *L-1* para cada ataque específico es $(ld\text{-}1)(1\text{-}(1 - 1/N)^n)$, que puede aproximarse como $(ld*n)/N$, que puede considerarse más pequeño que *20n/V/gN* si se supone que *ld<20V/g.* Obsérvese que puede elegirse *n, N* de modo que *20nV/gN* sea mucho más pequeño que 1. Se querría calcular el valor esperado de la suma de *L(i).1* para todo *i,* donde *L(i)* es la longitud de la lista de atacantes candidatos asociados al $i^{-ésimo}$ ataque en la misma zona geográfica. Esto puede ser calculado multiplicando *20nV/gN* veces el número esperado de atacantes en la misma zona geográfica. Este último número puede analizarse mediante una variación del problema clásico de "*balls into bins*" (problema consistente en asignar entrantes a receptores), puesto que estamos suponiendo que las zonas geográficas donde se ubica cada atacante están distribuidas de manera independiente y uniforme en el país.

A partir de este análisis, obtenemos que con probabilidad de al menos $(1\text{-}1/g)^{10}$, el número de atacantes es como máximo *6a/g+10 log g. Finalmente, se observa que 20nV/gN (6a/g+10 log g)* es aún menor que uno (1) para valores adecuados de *n, N* y valores prácticos de *g* e incluso para valores muy grandes de *a,* incluyendo una *a* más pequeña que *g* veces una constante no muy grande. Se observa que la elección de *n* y *N* puede estar limitada por consideraciones de privacidad del vehículo. También, el tamaño del grupo, *N,* no es fácilmente ajustable una vez que ha empezado la operación del sistema.

El análisis anterior implica que en este escenario, la lista de atacantes candidatos, de media, contiene el atacante único. El análisis puede extenderse para mostrar que esto se mantiene con alta probabilidad.

Escenario (b): En este escenario, se empieza haciendo las mismas suposiciones que en el escenario (a), y solamente se hace la siguiente modificación: en vez de suponer las zonas geográficas donde se ubica cada atacante distribuidas de manera independiente y uniforme por el país, se supone que los atacantes se eligen de manera independiente y uniforme entre todos los vehículos.

Con esta suposición diferente, las zonas con alta densidad de vehículos podrían tener listas mayores de atacantes candidatos. Al igual que en el escenario (a), obtenemos aún que el valor esperado de *L-1* para cada ataque específico puede ser aproximadamente de $(ld*N)/N$, que puede considerarse menor que *20nV/gN* (y, por lo tanto, puede hacerse mucho más pequeño que 1) si se supone que *ld<20N/g.* Sin embargo, el cálculo del número esperado de atacantes en la misma zona geográfica es diferente y puede analizarse mediante una variación del análisis anterior, usando un problema de "*balls into bins*" con una distribución de colocación no uniforme. A partir de este análisis se obtiene que con probabilidad de al menos $(1\text{-}1/g)^{10}$, el número de atacantes es como máximo de *6ld*a/V+10 log g.* Finalmente, se observa que *20nV/gN (6ld*a/V + 10 log g)* es aún menor que 1, para valores adecuados de *n, N* y valores prácticos de *g* e incluso para valores muy grandes de *a*, incluyendo *a* menor que *g* multiplicada por una constante no muy grande. Se observa que los valores de *n*, *N* pueden estar limitados por niveles de privacidad objetivo y que *N* puede ser difícil de ajustar mientras el sistema está funcionando.

El análisis anterior implica que incluso en este escenario, la lista de atacantes candidatos, de media, contiene el atacante solo. También, este análisis puede extenderse para mostrar que esto se mantiene con probabilidad alta.

Escenario (c): En este escenario, se supone que los atacantes realizan cada uno de sus ataques enviando al menos *2n* certificados maliciosos; estos mensajes se envían en intervalos de tiempo no muy largos entre sí; las zonas geográficas donde está ubicado cada atacante no están necesariamente distribuidas de manera independiente y uniforme en el país ni tienen una alta densidad de vehículos.

En este caso, al final de la técnica de aislamiento geográfico, los vehículos que estaban fuera de cualquiera de las zonas geográficas donde ocurrió un ataque, en el momento del ataque, se han descartado ya como atacantes candidatos. Esto supone que la fracción de vehículos que cambian de zonas geográficas respecto a todos los vehículos de la zona, es insignificante. Puesto que se supone que un ataque contiene al menos *2n* mensajes maliciosos y que esos mensajes se envían en una distancia corta en el tiempo entre sí, puede aislarse un zona geográfica simple dentro de la cual ocurrió el ataque. Esta puede ser una sola zona cubierta por un RSE, o incluso la unión de muy pocas de esas zonas. Ahora, para cada zona geográfica donde ocurrió un ataque, existen al menos *2n* ternas revocadas (puesto que el ataque afecta al menos a *2n* mensajes) por cada uno de los *a* ataques. Cada uno de los *a* atacantes puede elegir cómo asignar las *2n* ternas de ataque entre las *n* ternas que se asignaron originalmente a este atacante y hasta *2n* claves nuevas obtenidas después de las operaciones de reposición de clave, donde el objetivo es el de maximizar el número de vehículos honestos que comparten 2*n* ternas con cualquiera de entre los *a* atacantes. Mientras que es fácil apreciar que con una alta probabilidad la secuencia de *2n* ternas identifica unívocamente a su atacante asociado, podría ocurrir que tales *a* secuencias pudiera estar asociada

a más *a* vehículos, en cuyo caso un vehículo honesto podría considerarse un atacante candidato.

Ahora, considérese un vehículo honesto en la misma zona geográfica. Se calcula un límite superior para la probabilidad de que ocurra que este vehículo esté asociado a al menos *2n* entre las ternas atacantes en la misma zona geográfica, de la siguiente manera: este evento ocurre si (a) las *n* ternas distribuidas originalmente al vehículo honesto están compartidas por los vehículos atacantes (antes o después de las *2n* operaciones de reposición de clave) y si las *n* ternas distribuidas al vehículo honesto después de las operaciones de reposición de clave se comparten por cualquiera de los vehículos atacantes (b) debido a la estrategia de reposición de clave probabilística usada, o (c) debido a que pasa a ser alguna de las otras claves distribuidas a los vehículos atacantes.

Se observa que la probabilidad de que ocurra (a) es como máximo de $(2an / N)^n$; la probabilidad de que ocurra (b) es como máximo de (11(c + 1))n, debido a la estrategia de reposición de clave probabilística y la posibilidad de que ocurra (c) es como máximo de $(2an / N)^n$. Sobre todo, la probabilidad de que un vehículo honesto dado se declare como un fuerte candidato para actividad maliciosa repetida es $(2an/(c+1)N)^n + (2an / N)^{2n}$. Puesto que se considera una zona de alta densidad de vehículos, en la misma zona geográfica existen alrededor de *hd* vehículos y la probabilidad de que exista al menos un vehículo honesto en esa zona que sea declarado como un fuerte candidato para actividad maliciosa repetida es $hd((2an / (c+1)N)^n + (2an / N)^{2n})$. Se observa que para cualquier *hd*, *a*, existen valores adecuados de *c, n, N* de tal modo que esta cantidad es muy pequeña. Según lo anterior, se observa que los valores de *n, N* pueden estar también limitados por niveles de privacidad objetivo.

Si se considera además la idea de la discusión de la tabla 1 (anterior), puede usarse la observación de que la tasa de actualización de clave *u* es, para la mayor parte de los vehículos no atacantes, significativamente más pequeña que para los vehículos atacantes. Más específicamente, suponiendo que cada reposición de clave realizada por un atacante se lleva a cabo mediante como máximo una fracción q (por ejemplo, q=1/4) de vehículos que comparten la misma clave revocada, y que tales eventos son independientes a través de cada reposición de clave, se obtiene que el número esperado de vehículos honestos en la misma zona geográfica que se declaran fuertes candidatos para actividad maliciosa repetida es igual a $hd((2 a qn/(c+1)N)^n + (2aqn/N)^{2n})$.

<u>*Escenarios adicionales:*</u> El escenario más importante que no se ha considerado aún se produce cuando los atacantes llevan a cabo cada uno de sus ataques enviando uno solo, o muy pocos certificados maliciosos, y las zonas geográficas que albergan cada atacante no están necesariamente distribuidas de manera independiente y uniforme en el país, y tienen una alta densidad de vehículos.

Están considerándose ideas preliminares para resolver este difícil problema, en base a una ralentización artificial y gradual de la tasa de reposición de clave de vehículos honestos, hasta incluso no permitir ninguna reposición de clave en absoluto en caso de emergencia de ataques a gran escala. El impacto negativo de atacantes que envían uno solo, o muy pocos certificados maliciosos necesita estudiarse y comprenderse adicionalmente, también en combinación con una elección apropiada para la selección de la clave y el certificado anónimos y las estrategias de rotación.

<u>Prueba de posición geográfica</u>

La realización proporciona una solución más perfeccionada al problema de “uno afecta a muchos”. Se permite que cada vehículo pruebe su inocencia probando su posición geográfica en el momento en que se detectó un mal uso del certificado. Una prueba de posición geográfica consiste en una emisión de firma dependiente del tiempo y específica del vehículo por parte de un RSE a un vehículo.

La realización puede implementarse como un perfeccionamiento respecto a un esquema combinatorio básico. El objetivo de esta realización es el de diseñar una técnica novedosa que proporcione una solución más precisa al problema de “uno afecta a muchos”. La realización de aislamiento de ataque geográfico descrita anteriormente proporciona una técnica basada en aislamiento geográfico de los atacantes, específicamente al observar que los atacantes ponen implícitamente de relieve su localización en sus mensajes, y que un número muy grande de vehículos que comparten las claves de los atacantes estarán en localizaciones completamente diferentes. Los últimos vehículos pueden reconocerse fácilmente como no involucrados en los ataques y no resultarán afectados. Efectivamente, la realización geográfica descrita anteriormente considera zonas geográficas grandes y descarta como insignificante el impacto de los vehículos que se mueven entre zonas.

El análisis formal ilustra que en varios escenarios prácticos, se obtiene un efecto de “uno afecta a ninguno”. Este principio está mejor refinado en las realizaciones siguientes mediante una técnica novedosa denominada prueba de localizaciones geográficas, mediante la que obtenemos un efecto muy similar incluso en presencia de un número muy grande y muy *móvil* de atacantes en cualquier zona geográfica *pequeña.*

Según se ha expuesto, todas las estrategias de sustitución de clave anteriores requieren un procedimiento que realiza una investigación de qué vehículo, entre diversos candidatos, fue el responsable de uno o más mensajes generados maliciosamente. Ahora se potencian estos procedimientos para solicitar que cada vehículo candidato pruebe su inocencia, por ejemplo, mostrando pruebas apropiadas que desvinculen el tráfico de comunicación del vehículo candidato o su posición de las del tráfico de comunicación del vehículo malicioso. Según se ilustra con detalle a continuación, este procedimiento puede ser caro en términos de diversos recursos, incluyendo tiempo

computacional, y por tanto resulta claramente deseable minimizar el número de vehículos inocentes a los que se pide que se sometan al mismo.

La motivación por dicha técnica es de la siguiente manera. Considérese un mensaje generado maliciosamente desde un vehículo en una posición geográfica (x, y) y asociado a una clave k. Debido al diseño del esquema, se sabe que existirá una media de Vn/N vehículos a los que se distribuyó la clave k y que se están sometiendo por tanto a un procedimiento de investigación. Puesto que se espera que el número de tales vehículos que tienen una ubicación geográfica cercana a (x, y) sea mucho más pequeño, parece inútil requerir a los vehículos que tienen una posición geográfica "suficientemente alejada" de (x, y) en el momento del ataque que se sometan al procedimiento de investigación.

Específicamente, considerando la movilidad del vehículo, podría pensarse en mantener visualizada un "zona geográfica candidata", por simplicidad, tal como un círculo con centro en (x, y) y radio creciente con el tiempo. Entonces, la idea básica podría ser que la CA solamente necesita investigar los vehículos que soliciten que se actualice su clave k mientras están en la zona geográfica candidata en ese momento, donde la zona se actualiza con el tiempo teniendo en cuenta los posibles movimientos del vehículo malicioso. Podría parecer que esta técnica reduce significativamente el número de vehículos involucrados en el procedimiento de investigación y no contribuye a ninguna pérdida de privacidad debido a que los vehículos que no son originadores candidatos del mensaje generado maliciosamente se han deducido ya por el conocimiento de la localización del RSE que recibió este mensaje malicioso.

Sin embargo, existe otra razón potencial de por qué esta técnica puede no reducir el número de vehículos que deberían someterse al procedimiento de investigación. Algunos vehículos pueden permanecer sin uso durante el periodo de tiempo en el que el zona geográfica candidata se expande, hasta que esta zona incluya eventualmente vehículos que están muy alejados del sitio real de la actividad maliciosa.

Se prefiere por lo tanto usar una técnica que permita a un vehículo probar su posición y su estado en cualquier momento, tras la petición. Específicamente, en vez de considerar todos los vehículos a los que se distribuyó una clave particular como atacantes candidato, podría considerarse solo aquellos a los que se distribuyó esa clave particular y que no pueden probar que en el momento del ataque estaban en una posición geográfica diferente. En este punto, un vehículo solicita periódicamente a un RSE una prueba de posición, es decir, una firma con fecha y hora de una encriptación del vehículo de alguna información de identificación. Además, al solicitar un procedimiento similar siempre que el vehículo esté encendido (ON) o apagado (OFF), el vehículo puede proporcionar también, a petición, una prueba de inactividad del vehículo durante un intervalo de tiempo específico.

Ahora vamos a proporcionar más detalles sobre cómo llevar a cabo este procedimiento durante la etapa de uso de clave anónima, y la fase de eliminación de atacante.

Etapa de uso de clave anónima

Recuérdese que en cualquier punto, cada vehículo tiene *n* ternas, cada una de las cuales contiene una clave privada, una clave pública y un certificado, estando cada terna ya sea sin revocar aún o ya sea teniendo pendientes peticiones de actualización.

Al final de cada intervalo de tiempo de una duración t predefinida, cada vehículo pide al RSE que escucha una "prueba de posición" "específica del tiempo" y "específica del vehículo"; es decir, un certificado que proporciona seguridad de que el vehículo solicitante está en las zonas geográficas cubiertas por este RSE. Puede realizarse un protocolo para este tipo de prueba de posición combinando primitivas criptográficas bien conocidas. Como ejemplo, la petición podría contener un compromiso con una encriptación, usando la clave de identificación del vehículo de un momento aleatorio, y el propio momento: la respuesta del RSE podría ser una firma con fecha y hora, usando la clave pública del RSE, de la petición del vehículo.

Etapa de eliminación de atacante

Una prueba de posición para este vehículo consiste en la petición del vehículo, la respuesta del RSE, la clave de compromiso asociada al compromiso en la petición, la clave pública de identificación del vehículo y la aleatoriedad asociada a la encriptación calculada en la petición del vehículo.

Se observa que son posibles variantes de esta técnica. Por ejemplo, el vehículo podría enviar una encriptación de estos valores que puede desencriptarse solamente por la CA de autorización que puede referirse más tarde al contenido de la encriptación para la CA de asignación sin revelar la identidad del vehículo.

La figura 7 es un diagrama de flujo que ilustra una prueba de posición geográfica. Inicialmente, se realizan procesos de esquema combinatorio básico según se ha descrito anteriormente. En la etapa PG1, se compila una lista de vehículos a los que se distribuyó la terna revocada. En la etapa PG2, para cada vehículo de la lista de vehículos, se solicita una prueba de posición desde el RSE. La prueba de posición se comprueba en la etapa PG3 y, si la prueba de posición ilustra que dicho vehículo está en una posición geográficamente diferente del RSE que registró la terna revocada (PG3=SÍ), el vehículo se retira de la lista en la etapa PG4. En la etapa PG5 se sustituye la terna revocada.

Si la prueba de posición no ilustra una posición geográficamente diferente (PG3=NO), entonces el proceso se termina.

Mientras que la presente invención se ha descrito en realizaciones particulares, se apreciará que la presente invención no debe entenderse como limitada por tales realizaciones, sino interpretada según las reivindicaciones a continuación.

REIVINDICACIONES

1. Método para la gestión de claves y certificados criptográficos para una pluralidad de vehículos, comprendiendo dicho método las etapas de:

generar un grupo de ternas de clave pública, clave privada y certificado asociado, usando un algoritmo de generación de claves, teniendo dicho grupo un número de ternas del tamaño del grupo de clave; y

distribuir a y asociar con cada vehículo de dicha pluralidad de vehículos una pluralidad de ternas elegidas aleatoriamente a partir de dicho grupo de ternas;

revocar una terna de dichas ternas elegidas cuando se detecta que dicha terna se ha usado en actividad maliciosa, y

para cada vehículo asociado a dicha terna revocada, determinar si debe reemplazarse dicha terna revocada usando uno o más perfeccionamientos.

2. Método según la reivindicación 1, en el que un primer de dichos perfeccionamientos comprende las etapas de:

revocar un número c de ternas que se eligen aleatoriamente entre las ternas del grupo que no están actualmente revocadas, donde dicho número c es un número entero de uno o más;

seleccionar un número cl de nuevas ternas generadas de manera aleatoria e independiente usando el algoritmo de generación de claves, donde dicho numero cl es el número c más uno;

designar el número cl de nuevas ternas para reemplazar el número c de ternas revocadas, y

cuando un vehículo solicite una terna actualizada, elegir dicha terna actualizada entre el número cl de nuevas ternas y enviar dicha terna elegida actualizada al vehículo solicitante.

3. Método según la reivindicación 2, que comprende además las etapas de:

para cada terna revocada, compilar una lista de vehículos a los que se distribuyó la terna revocada, y

retirar de la lista todos los vehículos que hayan actualizado la terna revocada y hayan dado prueba de estar en una posición geográficamente diferente de un equipo de carretera, RSE, que registró la terna revocada.

4. Método según la reivindicación 1, en el que un segundo de dichos perfeccionamientos comprende las etapas de:

para cada vehículo:

crear un identificador anónimo y mantener un registro de reposición de clave asociado a dicho identificador anónimo;

incrementar un contador de reposición de clave en dicho registro de reposición de clave para dicho identificador anónimo según un número de claves que dicho vehículo solicita durante un periodo de tiempo, y

decrementar el contador de reposición de clave para cada identificador anónimo en una cantidad si no ha ocurrido ninguna reposición de clave durante un periodo de tiempo previo, a menos que dicho contador de reposición de clave sea igual a un umbral de reposición de clave y a cero,

en el que, cuando el contador de reposición de clave es menor o igual que el umbral de reposición de clave para dicho vehículo, reemplazar dicha terna revocada para el citado vehículo.

5. Método según la reivindicación 1, en el que un tercero de dichos perfeccionamientos comprende las etapas de:

para cada vehículo:

crear un identificador anónimo y mantener un registro de reposición de claves asociado a dicho identificador anónimo;

si dicho vehículo está asociado a dicha terna revocada, añadir una marca en contra del vehículo;

elegir un umbral en base a dicha marca, al número de ternas asociadas a dicho vehículo, y al tamaño del grupo de claves, y

si dicha marca es menor que el citado umbral, reemplazar dicha terna revocada.

6. Método según la reivindicación 5, estando además dicho umbral basado en al menos uno de entre un periodo de tiempo y una localización geográfica.

7. Método según la reivindicación 1, en el que un cuarto de dichos perfeccionamientos comprende las etapas de:

compilar una lista de vehículos a los que se distribuyó la terna revocada; y

para cada vehículo de dicha lista de vehículos, si dicho vehículo ha dado prueba de estar en una posición geográfica diferente de un equipo de carretera, RSE, que registró la terna revocada, retirar dicho vehículo de la lista,

y reemplazar dicha terna revocada.

8. Método según la reivindicación 1, en el que un quinto de dichos perfeccionamientos comprende las etapas de:

compilar una lista de vehículos a los que fue distribuida la terna revocada;

para cada vehículo de dicha lista de vehículos, solicitar una prueba de posición desde un equipo de carretera, RSE, y si dicha prueba de posición ilustra que dicho vehículo está en una posición geográficamente diferente de un equipo de carretera, RSE, que registró la terna revocada, retirar dicho vehículo de la lista, y reemplazar dicha terna revocada.

9. Método según la reivindicación 8, en el que dicha prueba de posición comprende dicha petición del vehículo, una respuesta del citado equipo de carretera, RSE, una clave de liberación de compromiso asociada a un compromiso en dicha petición del vehículo, una clave pública asociada a dicho vehículo, y una aleatoriedad asociada a una encriptación calculada en dicha petición del vehículo.

10. Medio legible con ordenador que tiene un código de programa legible con ordenador para operar en un ordenador para gestión de claves y certificados criptográficos para una pluralidad de vehículos, implementando el código cuando se ejecuta un método que comprende:

generar un grupo de ternas de clave pública, clave privada y certificado asociado usando un algoritmo de generación de claves, teniendo dicho grupo un número de claves del tamaño del grupo de claves;

distribuir a y asociar con cada vehículo de dicha pluralidad de vehículos algunas ternas elegidas aleatoriamente a partir de dicho grupo de ternas;

revocar una terna de dichas ternas seleccionadas cuando se detecta dicha terna como usada en actividad maliciosa, y

para cada vehículo asociado a dicha terna revocada, determinar si se debe reemplazar dicha terna revocada usando uno o más perfeccionamientos.

11. Código de programa legible con ordenador según la reivindicación 10, en el que el código implementa el método de una de las reivindicaciones 1 a 9.

12. Código de programa legible con ordenador según la reivindicación 11, cuando depende de una de las reivindicaciones 4 a 6, estando dicho umbral basado en al menos uno de entre un periodo de tiempo y una localización geográfica.

13. Código de programa legible con ordenador según la reivindicación 10, en el que un cuarto de dichos perfeccionamientos comprende:

compilar una lista de los vehículos a los que se distribuyó la terna revocada, y

para cada vehículo de dicha lista de vehículos, si dicho vehículo ha dado prueba de estar en una posición geográficamente diferente de un equipo de carretera, RSE, que registró la terna revocada, retirar dicho vehículo de la lista, y reemplazar dicha terna revocada.

14. Código de programa legible con ordenador según la reivindicación 10, en el que un quinto de dichos perfeccionamientos comprende:

compilar una lista de vehículos a los que se distribuyó la terna revocada;

para cada vehículo de dicha lista de vehículos, solicitar una prueba de posición desde un equipo de carretera, RSE, y si dicha prueba de posición ilustra que dicho vehículo está en una posición

geográficamente diferente de un equipo de carretera, RSE, que registró la terna revocada, retirar dicho vehículo de la lista, y reemplazar dicha terna revocada.

15. Código de programa legible con ordenador según la reivindicación 14, en el que dicha prueba de posición comprende dicha petición del vehículo, una respuesta desde dicho equipo de carretera, RSE, una clave de liberación de compromiso asociada a un compromiso en dicha petición del vehículo, una clave pública asociada a dicho vehículo, y una aleatoriedad asociada a una encriptación calculada en dicha petición del vehículo.

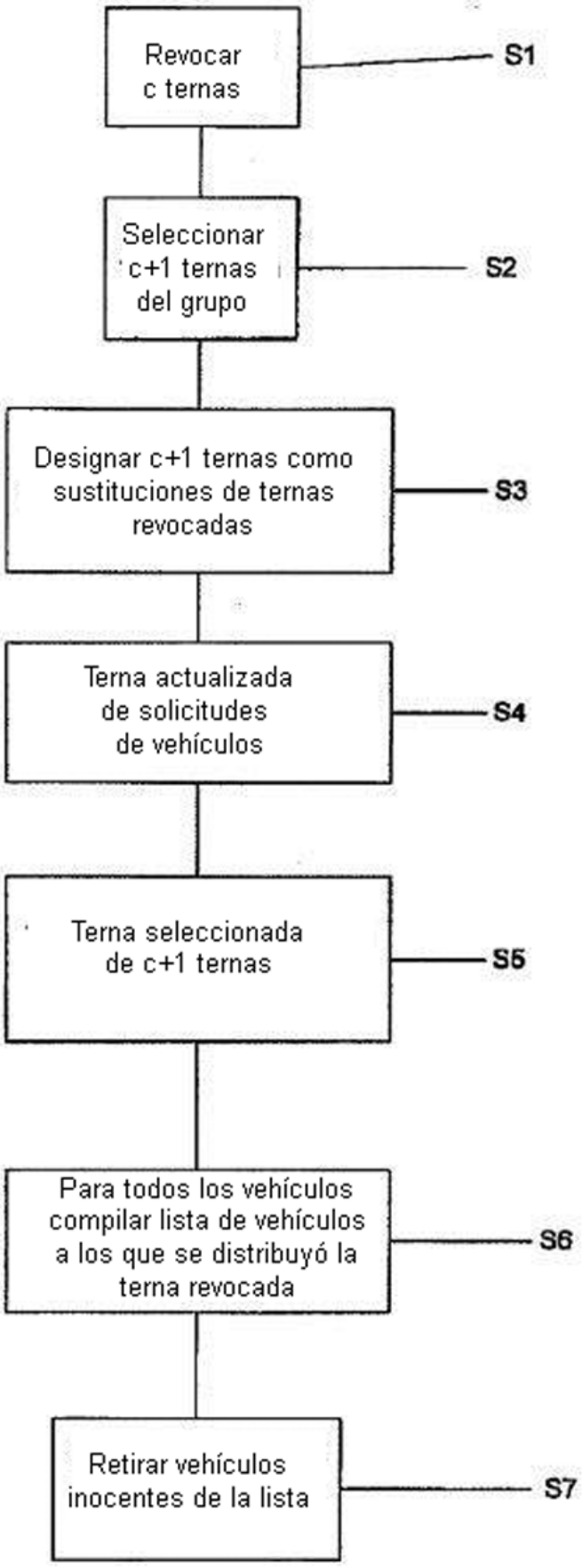
Revocar c ternas
S1
Seleccionar c+1 ternas del grupo
S2
Designar c+1 ternas como sustituciones de ternas revocadas
S3
Terna actualizada de solicitudes de vehículos
S4
Terna seleccionada de c+1 ternas
S5
Para todos los vehículos compilar lista de vehículos a los que se distribuyó la terna revocada
S6
Retirar vehículos inocentes de la lista
S7

Figura 1

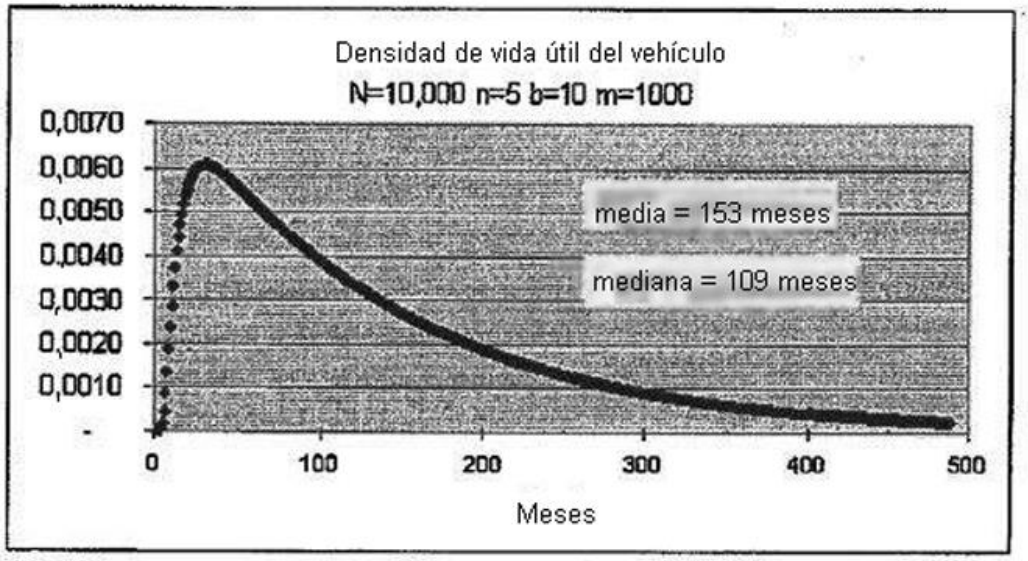

Figura 2

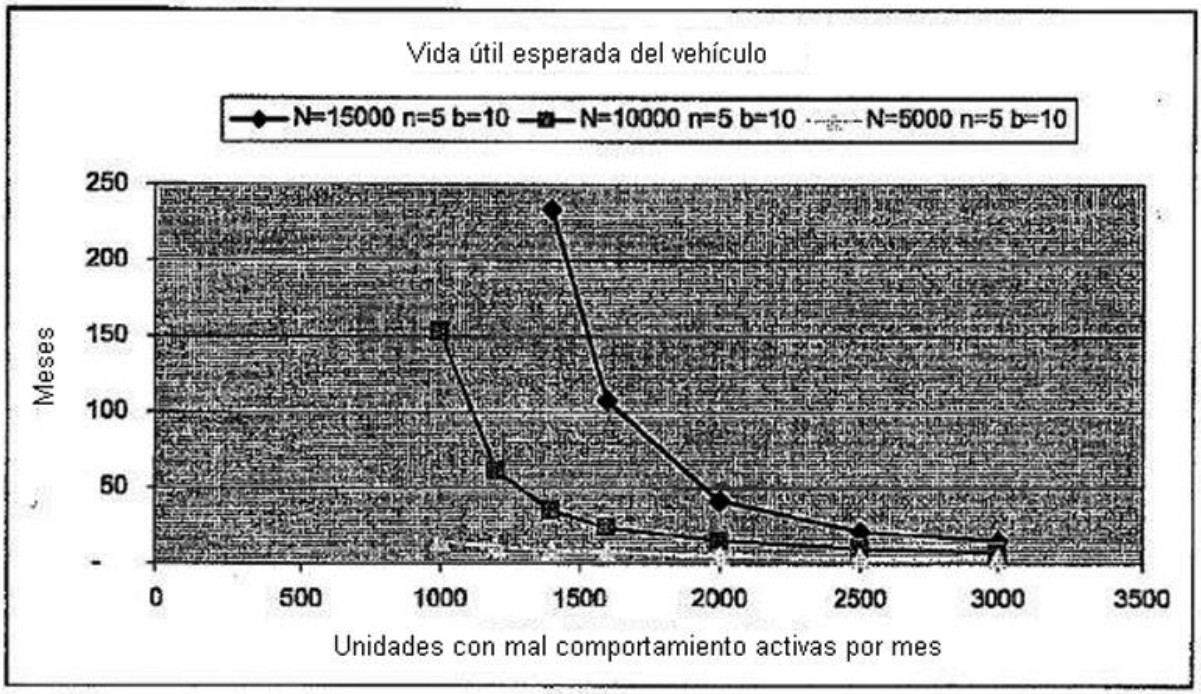

Figura 3

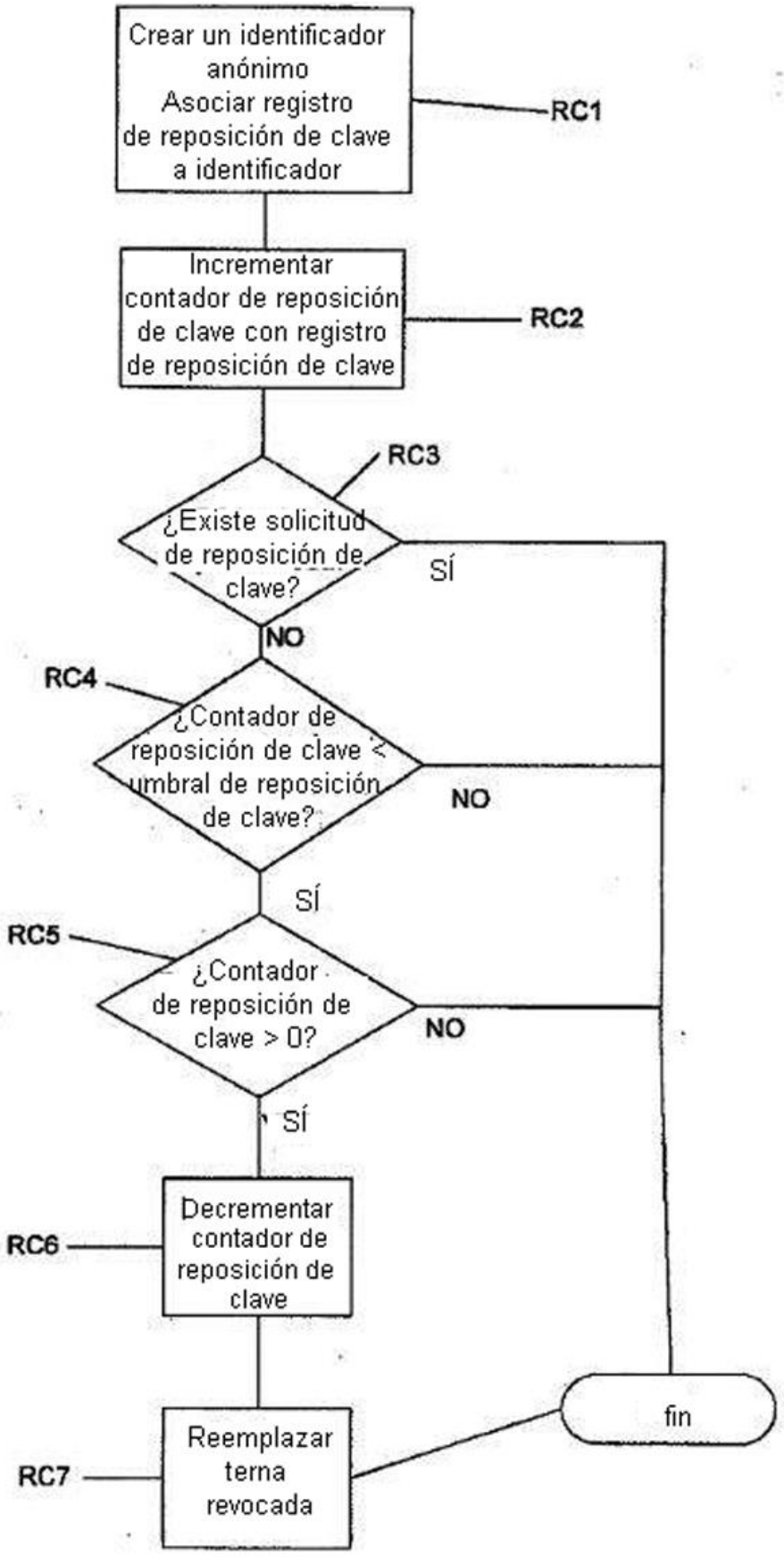
Crear un identificador anónimo
Asociar registro de reposición de clave a identificador
RC1
Incrementar contador de reposición de clave con registro de reposición de clave
RC2
RC3
¿Existe solicitud de reposición de clave?
SÍ
NO
RC4
¿Contador de reposición de clave < umbral de reposición de clave?
NO
SÍ
RC5
¿Contador de reposición de clave > 0?
NO
SÍ
Decrementar contador de reposición de clave
RC6
Reemplazar terna revocada
RC7
fin

Figura 4

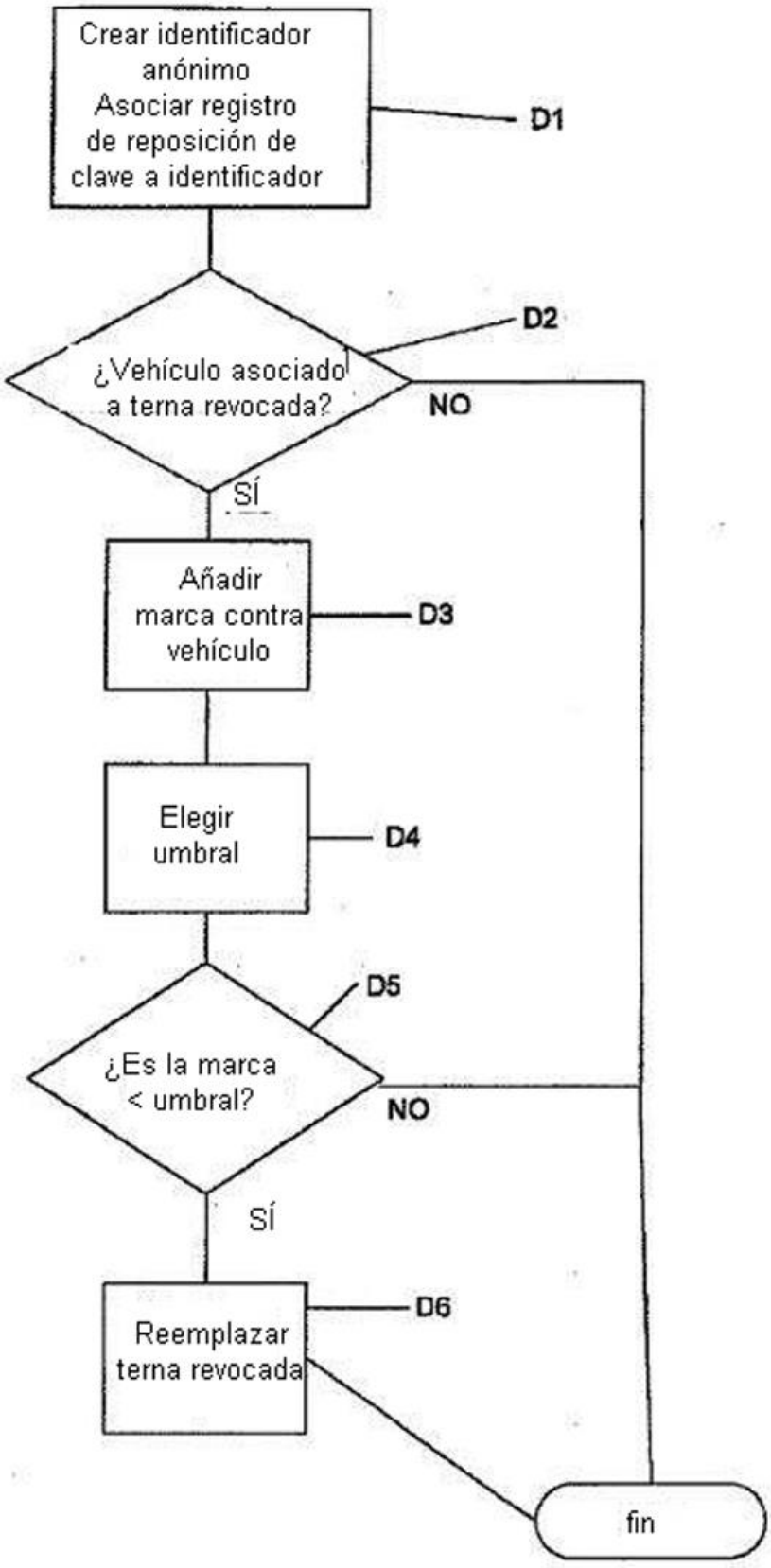
Crear identificador anónimo Asociar registro de reposición de clave a identificador
D1
¿Vehículo asociado a terna revocada?
D2
NO
SÍ
Añadir marca contra vehículo
D3
Elegir umbral
D4
¿Es la marca < umbral?
D5
NO
SÍ
Reemplazar terna revocada
D6
fin

Figura 5

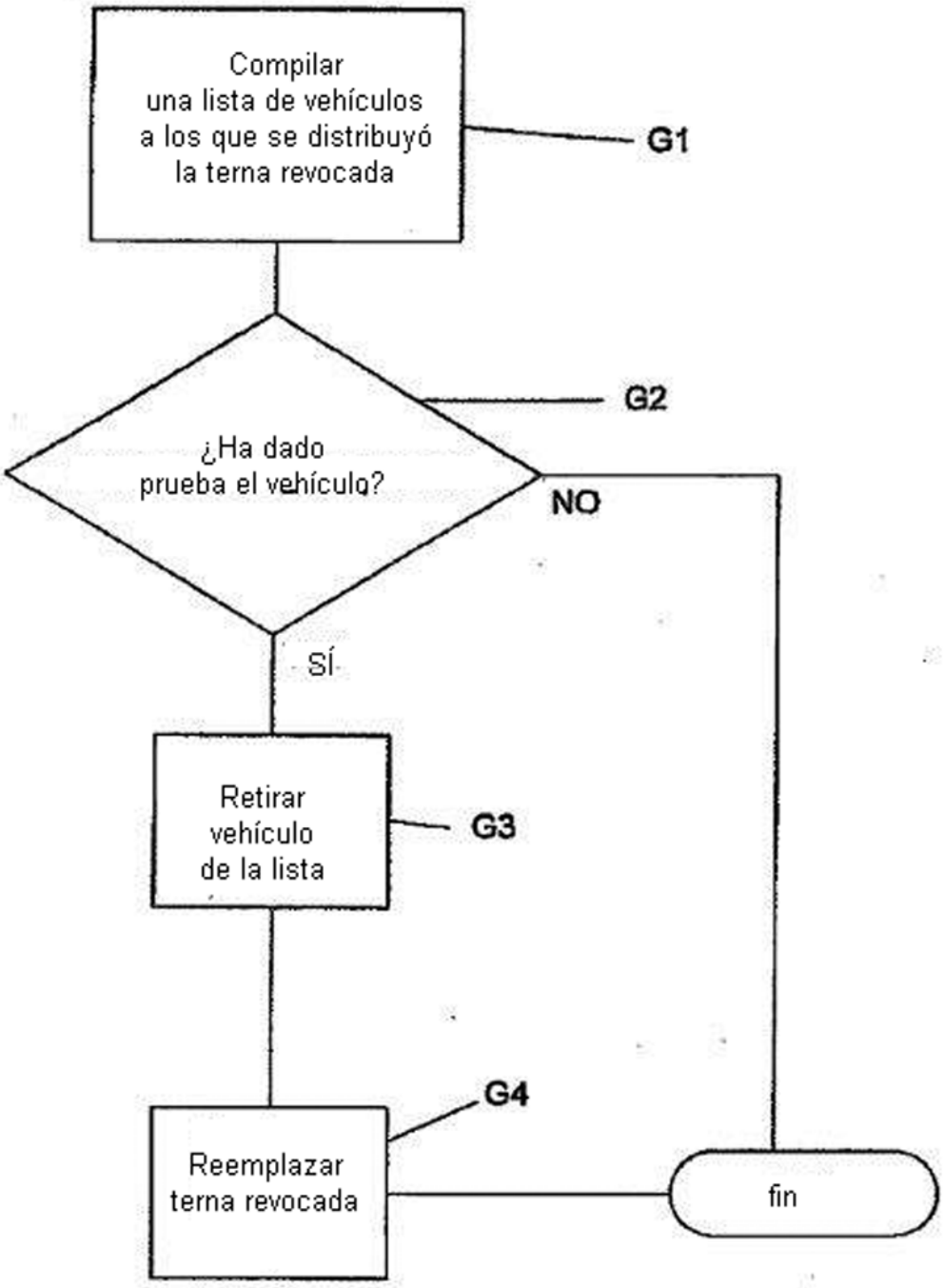
Compilar una lista de vehículos a los que se distribuyó la terna revocada
G1
¿Ha dado prueba el vehículo?
G2
NO
SÍ
Retirar vehículo de la lista
G3
Reemplazar terna revocada
G4
fin

Figura 6

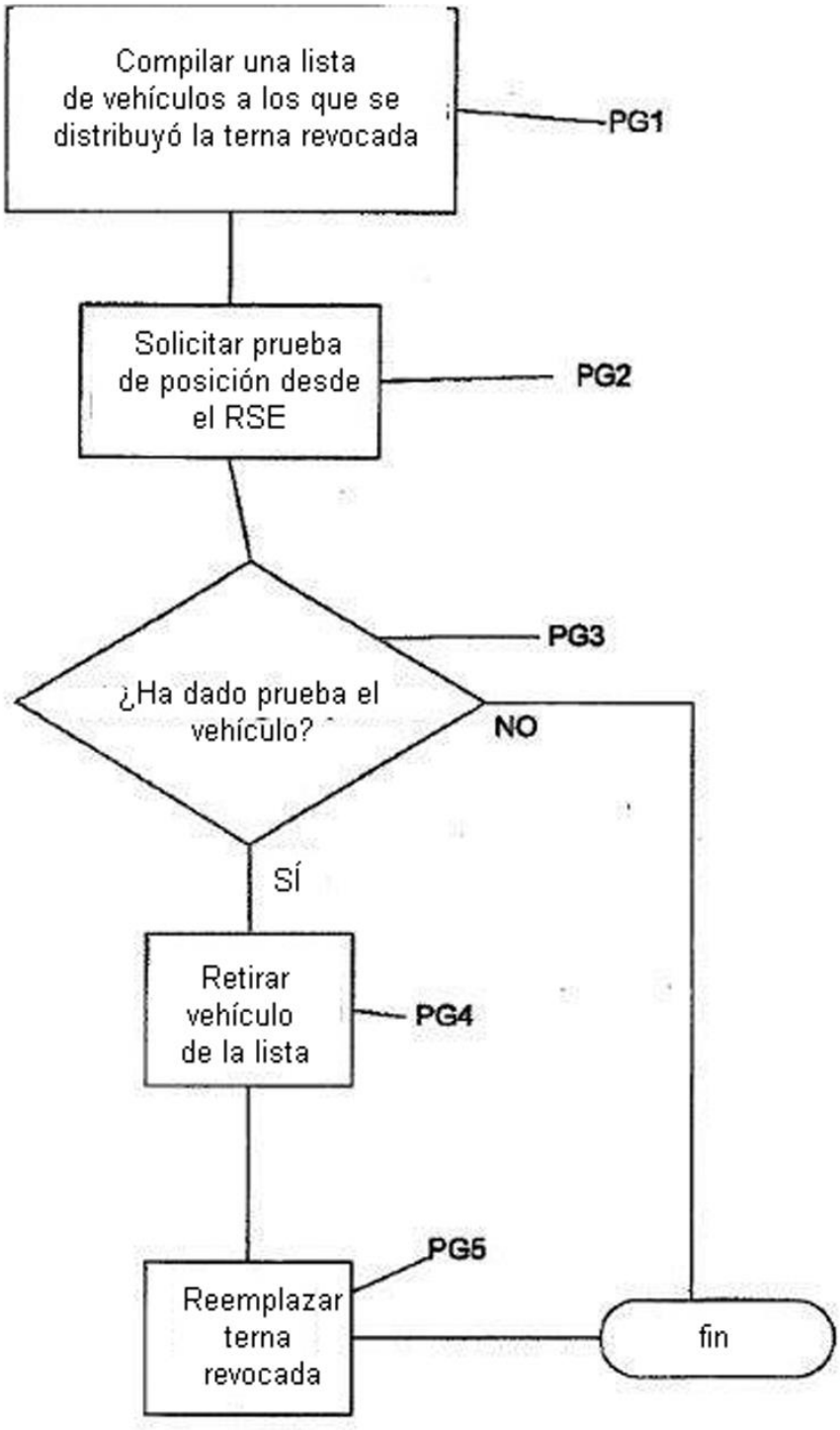
Compilar una lista de vehículos a los que se distribuyó la terna revocada
PG1
Solicitar prueba de posición desde el RSE
PG2
¿Ha dado prueba el vehículo?
PG3
NO
SÍ
Retirar vehículo de la lista
PG4
Reemplazar terna revocada
PG5
fin

Figura 7