Autenticación y privacidad en redes vehiculares

Authentication and privacy in vehicular networks

J. M. de Fuentes Gª-Romero de Tejada, A. I. González-Tablas Ferreres, A. Ribagorda Garnacho
Grupo de Seguridad en las T.I., Departamento de Informática, Univ. Carlos III de Madrid
Avenida de la Universidad, 30, 28911 Leganés (Madrid).
Teléfono: 0034 91 624 94 22 Fax: 0034 91 624 91 29
{jfuentes, aigonzal, arturo}@ inf.uc3m.es

Resumen

Las redes vehiculares son redes de comunicación en la que participan esencialmente vehículos. Estas redes permiten, entre otras cosas, intercambiar datos para proporcionar más información al conductor y mejorar así la seguridad vial. La seguridad de dicha información resulta crucial, pues la vida de los pasajeros está en juego. De hecho, el envío de información falsa debería perseguirse, por lo que se hace necesario identificar al emisor. Sin embargo, a través de la red vehicular se podría efectuar un seguimiento (electrónico) del camino seguido por un vehículo, por lo que puede comprometerse la privacidad de sus ocupantes. En este artículo se presentan los principales mecanismos que se han propuesto para implementar este compromiso entre identificación y privacidad.

Palabras clave: Red vehicular, autenticación, privacidad, seudónimo.

Abstract

Vehicular ad-hoc networks (VANETs) are composed mainly by vehicles. These communication networks allow data interchanging. In this way, more and better information is provided to the driver, thus achieving a better road safety. Information security is critical in these scenarios, as human lives are at stake. Particularly, spreading false data should be prosecuted, so sender identification is needed. However, such identification could lead to tracking. In this way, privacy protection must be achieved. In this article, mechanisms to fulfill this identification-privacy tradeoff are analyzed.

Keywords: VANET, authentication, privacy, pseudonym.

1. Introducción

El transporte de personas y mercancías es, hoy día, una de las cuestiones más relevantes para el normal funcionamiento de la actividad social e industrial de los países desarrollados. Por este motivo, la eficiencia y la eficacia de los medios de transporte es un aspecto en constante evolución. En particular, la seguridad vial es un objetivo primordial en las políticas de

transportes de multitud de países industrializados. Destaca, por ejemplo, el proyecto *Vision Zero*[1] en Suecia, donde se quiere acabar con las víctimas por accidentes de tráfico para el año 2020.

Para la mejora de la seguridad vial resulta conveniente simplificar la toma de decisiones por parte del conductor. En particular, uno de los problemas que se detectan en la actualidad es la falta de información global desde el punto de vista del conductor. Éste toma sus decisiones utilizando los datos de los que dispone, que habitualmente se reducen a aquello que se encuentra dentro de su campo de visión. Sin embargo, esta información resulta muchas veces insuficiente para tomar la decisión óptima, es decir, aquella que proporcione la máxima seguridad no sólo para su propio vehículo sino para los demás. Así, si el vehículo delantero frena, sería interesante saber si esto se produce como consecuencia de una leve adecuación de velocidad en un tramo específico o bien por la ocurrencia inmediata de un accidente. En ambos casos, las respuestas por parte del conductor (y de aquéllos que circulan detrás de éste) deberían ser distintas desde el punto de vista de la seguridad vial.

Para contribuir a la resolución de esta necesidad, se está desarrollando una nueva tecnología de la información denominada **red vehicular o VANET** (del inglés, Vehicular Ad-hoc NETwork). Gracias a este nuevo tipo de red, los vehículos se convierten en nodos de comunicación que pueden compartir información sobre el estado de su entorno (p.e. estado del pavimento, velocidad a la que se circula, aviso de accidentes, etc.). A partir de esa información, el conductor tiene más elementos de juicio para dirigir el vehículo de manera más segura.

Como ejemplo práctico de aplicación desarrollada sobre una red vehicular, el proyecto *eCall*[2] persigue que el propio vehículo contacte con el centro de emergencias en el momento en

[1] http://www.monash.edu.au/muarc/reports/papers/visionzero.html
[2] http://www.esafetysupport.org/en/ecall_toolbox/

que se haya visto involucrado en un accidente. De esta manera, la gestión de la asistencia se realiza de manera mucho más eficaz, con la correspondiente disminución (previsible) del número de víctimas en carretera.

Las redes vehiculares son, por tanto, una valiosa integración de las tecnologías de la información en el área del transporte que proporciona numerosos beneficios. No obstante, existen numerosos riesgos que deben ser considerados en estas redes relacionados con la gestión de las identidades de los vehículos y las responsabilidades que se les pueden exigir. Para minimizar dichos riesgos, se pueden utilizar mecanismos de autenticación y protección de la privacidad adecuados a las redes VANET. Antes de entrar en detalle sobre este aspecto, se ilustrará brevemente cómo se establecen estas redes y qué tipo de informaciones entran en juego.

2. Caracterización de las redes vehiculares.

En términos generales, las redes vehiculares presentan dos características diferenciadoras con respecto a otros escenarios de red tradicional. Por un lado, abarcan una extensa área geográfica (la red de carreteras). Por otro lado, los vehículos se mueven a una velocidad muy elevada. Esta movilidad ocasiona que las conexiones vehiculares sean esporádicas (*ad-hoc*). Todas estas cuestiones han propiciado la creación de una nueva tecnología de comunicación, denominada **DSRC**[3] (*Dedicated Short-Range Communications*). En términos generales, se puede definir esta tecnología como una variante de las comunicaciones inalámbricas actuales (estándar 802.11) donde se establecen comunicaciones esporádicas de corto alcance.

En una red vehicular participan dos tipos de entidades, tal y como se refleja en la Figura 1. Por un lado, la mayor parte de los nodos son los propios vehículos, que llevan incorporado un

dispositivo de comunicaciones conocido como **OBU** (del inglés, *On-Board Unit*, unidad de comunicaciones a bordo). Por otro lado, las **RSU** (del inglés, *Road-Side Unit*, unidad al borde de la carretera) son dispositivos estacionarios de comunicación que se sitúan a lo largo de las carreteras.

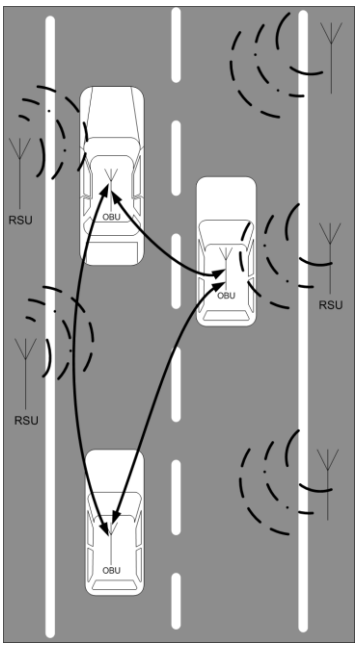

Figura 1. Arquitectura típica de una red vehicular

Las entidades descritas permiten establecer dos tipos de comunicaciones. Por una parte, se permite la interconexión entre los vehículos que circulan próximos. Esto hace posible la compartición de información sobre el entorno que se introdujo anteriormente. Por otra parte, se establece una comunicación entre el vehículo (a través de su OBU) y la RSU para que pueda existir un intercambio de datos desde y hacia otras entidades que presten sus servicios a través de las redes vehiculares. Esto hace posible, por ejemplo, la distribución de datos actualizados sobre el estado del tráfico desde la Dirección General de Tráfico.

[3] http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

3. Compromiso autenticación-privacidad en las redes vehiculares

Los intercambios de información que se acaban de describir presentan una serie de necesidades de seguridad que deben ser satisfechas. De hecho, la seguridad de la información juega, en este tipo de redes, un papel crucial. Dado que los datos que se reciban pueden afectar a la conducción y, por tanto, a la seguridad de los ocupantes, es imprescindible asegurar su veracidad. Es por ello que debe poderse perseguir (y aislar) a aquellos vehículos que difundan información errónea.

Así, en primer lugar, resulta conveniente contar con mecanismos que permitan **identificar** a los vehículos. En segundo lugar, es necesario poder disponer de herramientas para **autenticar** dichos vehículos en sus comunicaciones, es decir, tener la garantía de que el vehículo es quien dice ser, y los mensajes que éstos envíen. De esta forma, será posible identificar al vehículo que emitió un determinado mensaje y aplicar las medidas sancionadoras que correspondan (en caso de que dicho mensaje contenga información falsa). Por ejemplo, si un vehículo difunde a través de la VANET la existencia de un falso atasco con la intención de forzar a los demás vehículos a escoger otra ruta, debería identificarse al emisor para castigarle adecuadamente.

No obstante, la autenticación no debe lesionar la debida **privacidad** de los participantes. Si el vehículo que emite un mensaje quedara identificado dentro del mismo, sería posible efectuar el **seguimiento** de un vehículo, ya que se podrían trazar distintos mensajes enviados por éste [1]. Esto constituye un problema, en tanto que habitualmente se puede definir (con cierta fidelidad) una relación entre el vehículo y su conductor. De hecho, es habitual que el propietario del vehículo sea su conductor más frecuente. Por tanto, la identificación del vehículo se convierte indirectamente en la del conductor o propietario. Dado que el seguimiento afecta entonces no

sólo al vehículo sino también a una persona, entra en juego la protección de la privacidad. Esta necesidad es más acuciante si se tiene en cuenta que las RSU constituyen una infraestructura de comunicaciones que generalmente dispone y mantiene la administración regional. En estas circunstancias, las RSU podrían permitir la monitorización de las comunicaciones vehiculares por parte de dicha administración y, con ello, la replicación del fenómeno del *"*gran hermano*"* en la carretera [2].

Las redes vehiculares, por tanto, afrontan el **compromiso autenticación-privacidad** desde lo más profundo de su esencia. Se trata de una cuestión central a la hora de diseñar y desarrollar la propia red. Por este motivo, numerosas contribuciones investigadoras se han referido a la creación de mecanismos que satisfagan este compromiso de forma que se cuente con credenciales electrónicas que permitan atestiguar la identidad del poseedor, sin que esto permita realizar un seguimiento sobre el vehículo ni derivar ningún dato sensible a partir de su mero uso. El principal mecanismo considerado en las propuestas actuales contempla la identificación de los vehículos a través de seudónimos temporales y la utilización de certificados de clave pública asociados a dichos seudónimos como credenciales.

4. Identificación de los vehículos

En la actualidad, fuera del contexto de las VANET, un vehículo ya es identificado en dos momentos distintos. Por un lado, el fabricante le asigna un número único (comúnmente conocido como **número de bastidor** o chasis) al finalizar su proceso de fabricación. Por otro lado, para que el vehículo entre en circulación debe obtenerse (al menos en España) una autorización administrativa. Esta autorización implica que su propietario se inscriba en un registro creado para este fin y conlleva, además, la emisión de **placas de matrícula** que se disponen en el vehículo.

Ambas identidades son cualitativamente distintas. En particular, el número de bastidor no cambia durante toda la vida del vehículo y, además, se dispone en el interior del vehículo. Sin embargo, la placa de matrícula puede cambiarse (tras la venta del vehículo, por ejemplo) y está diseñada para ser vista desde el exterior.

Con respecto al problema de seguimiento (y, por extensión, de privacidad) que se debe combatir en las redes vehiculares, la existencia de las placas de matrícula plantea un punto de partida común para todas las soluciones que se desarrollen: el seguimiento visual del vehículo es siempre posible, si se disponen de los medios (e.g. videocámaras) adecuados [3]. Por este motivo, un sistema electrónico de identificación que proporcionara un anonimato perfecto al comunicante no sería ni adecuado ni procedente, en tanto que siempre podría ser violado utilizando medios físicos. Las soluciones que se contemplen en el ámbito electrónico deberán proporcionar, al menos, el mismo nivel de privacidad que existe en la actualidad.

Tomando como referencia lo descrito sobre las placas de matrícula, en las redes vehiculares se ha propuesto una extensión natural de éstas, denominada **ELP** (del inglés *Electronic License Plate*, placa de matrícula electrónica) [4]. El ELP es, así, un identificador único emitido por una autoridad legal (que, por definición, se asume confiable). Sin embargo, el uso del ELP como identificador permanente en las comunicaciones jugaría en contra de la privacidad deseada. Si se empleara en dos mensajes emitidos en distintos lugares, ambos podrían ser relacionados y el seguimiento del vehículo se podría efectuar sin dificultad. Esto agravaría el problema de privacidad existente en la actualidad, en el que un observador apostado en el lateral de una carretera puede observar los vehículos que por allí circulan. Al llevarlo al plano

electrónico, este seguimiento podría hacerse (incluso en múltiples lugares a la vez) utilizando dispositivos electrónicos que podrían manejarse de manera remota.

Es preciso por tanto buscar otras soluciones que permitan identificar los vehículos y posibilitar su autenticación (o la autenticación de los mensajes que éstos envían) así como proteger su privacidad. La solución que más atención está acaparando en la literatura es la utilización de **seudónimos** [5]. Los seudónimos son, en realidad, nombres falsos que ocultan la identidad real. Una posible forma sería utilizar números aleatorios. Cualquier técnica es válida siempre que la autoridad legal pueda descubrir la identidad real asociada al seudónimo. De lo contrario, no podría llevarse a efecto el requisito de permitir la penalización a aquéllos que se comporten de manera incorrecta. Por otro lado, si un vehículo utilizase el mismo seudónimo todo el tiempo, sería fácil asociar dicho seudónimo con la identidad real del vehículo. Por tanto, para evitar este riesgo, es habitual considerar que un vehículo utilizará un conjunto de seudónimos diferentes a lo largo del tiempo.

5. Creación de credenciales electrónicas. Certificados basados en seudónimos

Uno de los mecanismos más extendidos para permitir la autenticación de una entidad en el plano electrónico son los **certificados de clave pública**. Dichos certificados son emitidos por una autoridad de certificación, y atestiguan que la clave pública que en ellos se contiene está asociada con la entidad titular del certificado. De esta credencial se deriva, al mismo tiempo, que ésta es la única entidad que dispone de la correspondiente clave privada.

Los certificados constan, por tanto, de dos informaciones principales: la identidad del titular y el material criptográfico asociado. En las redes vehiculares se han propuesto diferentes

alternativas para crear cada uno de esos datos. A continuación se describen ambas cuestiones por separado.

5.1. Identidad contenida en el certificado

Según lo visto anteriormente, la mayoría de las propuestas actuales asumen que la identidad de los vehículos sea representada por seudónimos temporales. De esta manera la identidad contenida en el certificado no revela ningún dato sensible sobre el titular. Sin embargo, debe seguir siendo posible relacionar en algún momento dichos seudónimos con las identidades reales de los vehículos para poder exigir responsabilidades a sus propietarios en el caso de que así sea necesario. Para prevenir posibles abusos de la autoridad, se suele proponer que exista una separación de roles que deban cooperar para llevar a cabo la resolución de la identidad [6]. Así, se distingue entre la **autoridad legal** y la **autoridad de certificación**. La primera se encarga de gestionar el registro de los vehículos de cara a autorizar su circulación y permitir la emisión de las placas de matrícula. La segunda se encarga de la gestión de los seudónimos temporales y de sus correspondientes certificados. Ambas entidades aparecen reflejadas en la Figura 2, donde también se pueden observar los distintos datos que conoce cada entidad. La autoridad legal conoce las identidades reales de los vehículos y sus propietarios, mientras que la autoridad de certificación conoce qué seudónimo se asigna a cada vehículo. De esta manera, se necesita la cooperación de ambas para resolver la identidad del conductor. Gracias a esta separación de roles, se minimiza la posibilidad de que las diferentes entidades involucradas colaboren para resolver la identidad de un vehículo sin que sea estrictamente necesario.

5.2. Creación de las claves públicas y privadas

Además de la creación de los seudónimos, es necesario crear las claves públicas y privadas que permitirán la autenticación del poseedor del certificado en las VANET. Excepcionalmente, si se utiliza **criptografía basada en identidad**, se puede utilizar el identificador (el seudónimo, en este caso) como clave pública [7]. Si no se utiliza esta técnica, la identidad y las claves deben generarse por separado.

Se han propuesto dos alternativas principales para generar dichas claves: la **creación centralizada** o **distribuida**. La creación centralizada consiste en delegar todo el proceso en la autoridad de certificación. El vehículo, periódicamente, accede a dicha entidad para obtener no sólo nuevos certificados, sino también las correspondientes claves privadas. Por su parte, en la creación distribuida es cada vehículo el que genera las claves [8]. Cuando necesita obtener nuevos certificados, se envía a la autoridad de certificación el seudónimo escogido y la clave pública que se quiere introducir en el certificado.

Ambas alternativas son posibles gracias al componente confiable que se asume alojado en el vehículo. Dicho componente se denomina **TPM** (del inglés, *Trusted Platform Module*) y proporciona tanto almacenamiento confiable como capacidades criptográficas [9]. En ambos casos, el TPM se utiliza para custodiar y utilizar el material criptográfico. Sin embargo, en la versión distribuida tiene una mayor responsabilidad, pues también se encarga de crear dicho material.

Si se analizan ambas alternativas, la versión distribuida presenta notables ventajas. Es más escalable, en tanto que se delega parte del procesamiento en los vehículos. Además, la clave privada nunca abandona el vehículo, lo que redunda en un mayor nivel de seguridad. Sin

embargo, el correcto funcionamiento del TPM es ahora más crítico. Si fuera posible alterar este componente, se podría conseguir que varios vehículos acordaran un conjunto de seudónimos y claves. De esta manera, distintas entidades podrían obtener certificados iguales y, como resultado, serían indistinguibles.

6. Obtención y utilización de los certificados

6.1. Obtención inicial y actualización

Una vez creados, los seudónimos deben utilizarse durante un período corto de tiempo. De hecho, el punto óptimo sería utilizarlos una sola vez, dado que así la dificultad para realizar un seguimiento sería elevada. Esto implica la necesidad de obtener nuevos certificados de forma periódica. Una interesante solución se basa en aprovechar los procesos de fabricación y autorización administrativa para cargar un conjunto inicial de certificados en el vehículo. Posteriormente, se podrían introducir nuevos certificados aprovechando las inspecciones técnicas que los vehículos deben efectuar periódicamente.

6.2. Políticas de cambio de seudónimos

El proceso del cambio de seudónimo que se usa en cada momento no puede realizarse arbitrariamente. Es preciso encontrar un momento adecuado para realizarlo de manera que se consiga mantener la privacidad. Considérese un tramo de vía en el que sólo circulan dos vehículos. Si sólo uno de ellos efectúa el cambio de seudónimo, su eficacia será nula. Cualquier observador externo podrá deducir que el nuevo seudónimo corresponde al vehículo que lo cambió.

A tenor de este hecho, se han propuesto **diferentes políticas de cambio**. Por ejemplo, una posibilidad es cambiarlo en función de la velocidad [5]. A mayor velocidad, mayor ritmo de cambio de seudónimos. Con esto se consigue aumentar la incertidumbre, incluso si el observador abarca un tramo largo de la vía.

Por otra parte, se ha propuesto mantener periodos de silencio (e.d. ausencia de comunicaciones) de duración aleatoria [10]. Esto dificulta que un tercero pueda adivinar cuándo se producirá el siguiente cambio de seudónimo. Sin embargo, resulta conveniente hacer coincidir esos silencios con aquéllos de otros vehículos. De lo contrario, se caería en el escenario del ejemplo de partida. Para abordar esta cuestión, se propone la creación de **contextos mixtos** [11]. Estos son zonas de la carretera en donde no se sitúa ninguna infraestructura de comunicaciones (e.d. RSU). Se dice, por tanto, que el contexto mixto es un área no monitorizada. Cuando el vehículo entra en dicho contexto, se detienen todas sus comunicaciones. De esta manera, si múltiples vehículos se encuentran a la vez en dicha zona, resulta complejo para un observador externo retomar el seguimiento cuando éstos abandonen el área.

La eficacia de las políticas de cambio de seudónimo está condicionada a que éste sea su único medio de identificación. En otras palabras, si existen otros factores que permiten identificar electrónicamente (al mismo tiempo) al vehículo, el uso de seudónimos no aportará ventaja alguna para la protección de su privacidad. A este respecto, es preciso tener en cuenta que la red vehicular, como la mayoría de las redes de comunicación actuales, se ha diseñado como una pila de protocolos que ofrecen distintos servicios. Cada una de las capas de la pila exige una identificación distinta, por lo que será necesario cambiar junto con el seudónimo los identificadores en todas las capas [12].

No obstante, incluso tomando esta precaución existen características inherentes al funcionamiento de los dispositivos de comunicación (e.d. la OBU) que, con los medios adecuados para detectarlas, permiten la identificación del comunicante. Un ejemplo es la **huella electromagnética** (en inglés, *radio frequency fingerprinting*), un cierto patrón que se mantiene en los distintos envíos de información que emite un dispositivo [13]. Esta característica debe tenerse en cuenta de cara a la evaluación de la eficacia de los métodos de cambio de seudónimo.

7. Revocación de certificados

La gestión de la identidad implica no sólo su creación sino también su revocación en caso necesario. El proceso de revocación debe iniciarse cuando se ha perdido la confianza en la identidad emitida. Esto sucede, habitualmente, cuando se ha perdido el control (por pérdida o robo) de la clave privada asociada a la identidad. Sin embargo, en el ámbito vehicular, el mal comportamiento de un vehículo en el funcionamiento de la red puede ser motivo de revocación.

Para ilustrar esta cuestión, pongamos dos ejemplos de mal comportamiento. En primer lugar, considérese un automóvil que envía información acerca de un accidente inexistente, con el fin de simular una situación de tráfico denso y obtener así una vía menos transitada. Por otro lado, supóngase que un vehículo no participa en el encaminamiento de mensajes dentro de la red vehicular. Ambas cuestiones afectan al normal funcionamiento de la VANET y, por tanto, deben ser evitadas. La revocación constituye el primer mecanismo de defensa, en tanto que permite aislar a los vehículos que no son confiables.

Los ejemplos anteriores ilustran las dos fases principales de la revocación derivada del mal comportamiento: la **detección** de éste y la **defensa** frente al mismo. A continuación se

exploran ambas fases por separado. La Figura 2 describe gráficamente el procedimiento completo que se sigue durante la revocación y que se explicará detenidamente en los apartados siguientes.

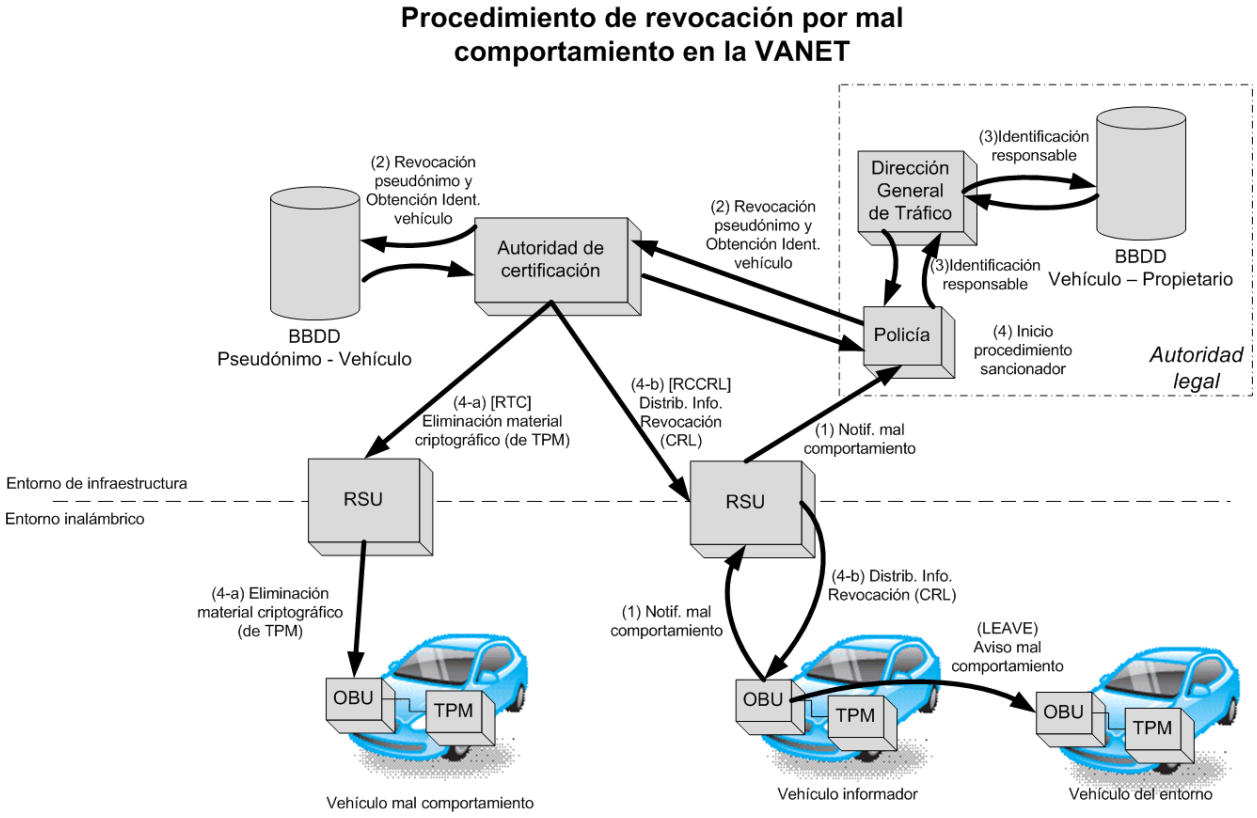

Figura 2. Procedimiento completo de revocación

7.1. Detección de comportamientos indeseados

La detección de comportamientos incorrectos está fuertemente condicionada por la propia naturaleza de la red vehicular y, más concretamente, por la manera en que se gestiona la identidad en este escenario. Tal y como se ha descrito hasta el momento, existe una entidad encargada de gestionar los certificados que sirven para identificar y autenticar a cada vehículo. Sin embargo, no existe una forma escalable de que los vehículos conozcan, a priori, otros datos acerca de los demás. Esto sería relevante, por ejemplo, para establecer medidas de confianza sobre los datos reportados por otro vehículo, en función de comportamientos anteriores. No

existe, por tanto, un modelo global para la gestión de la confiabilidad (o reputación) que merece un vehículo concreto. De hecho, no sería eficiente que cada vehículo almacenara la reputación sobre todos los demás vehículos, puesto que en realidad sólo se encontrará con una pequeña cantidad de ellos y durante un corto intervalo de tiempo. Tampoco se podría centralizar dicha reputación, dado que por la propia naturaleza de la red vehicular no se puede asumir una conectividad permanente a entidades externas.

En estas circunstancias, los comportamientos no deseados se detectan de forma local e independiente por parte de los propios vehículos. Los mecanismos propuestos se basan en que el receptor del mensaje mida la coherencia de la información ofrecida por un vehículo, con respecto a lo manifestado por los demás y lo que él mismo conoce a través de sus sensores.

Una vez que se detecta un comportamiento no adecuado, la respuesta debe ser escalonada. El envío puntual de información incorrecta no puede suponer la pérdida absoluta de confianza en el nodo emisor. Por ello, se ha propuesto un esquema de aislamiento progresivo en función de la persistencia del mal comportamiento [14]. Este esquema se implementa a través del protocolo **LEAVE**. Éste propone un sistema de votación en el que participan los vehículos que circulan alrededor del potencial malhechor. Una vez que se ha detectado el comportamiento inadecuado, los votantes emiten mensajes de advertencia al resto de vehículos (Figura 2). Si el comportamiento malicioso persiste, se procede a avisar a la autoridad legal para que revoque dicha identidad (Figura 2, mensaje 1). Es importante destacar que sólo la autoridad es capaz de revocar la identidad de cualquier vehículo.

7.2. Acciones de defensa frente al mal comportamiento

Una vez que se ha decidido revocar el certificado de un vehículo, la autoridad contacta con la entidad de gestión de seudónimos para resolver la identidad del vehículo implicado (Figura 2, mensaje 2). Además, se obtiene la identidad del propietario para procesar las notificaciones administrativas que pudieran derivarse (Figura 2, mensaje 3).

A partir de ese momento, se debe hacer efectiva la revocación propiamente dicha, para lo cual dos procedimientos distintos pueden utilizarse. Por un lado, el protocolo **RTC** (del inglés, *Revocation of the Trusted Component*) permite que la autoridad contacte directamente con el componente confiable (e.d. TPM) del vehículo [14]. Recuérdese que es este componente el que alberga la identidad del vehículo que, en este caso, quiere revocarse. Así, se envía un comando que ordena al TPM que borre todas las identidades (seudónimos) del vehículo, junto con sus materiales criptográficos asociados (Figura 2, mensaje 4-a). Para evitar ataques de suplantación (e.d. que una entidad distinta de la autoridad de certificación actúe en su nombre) el comando es firmado por la autoridad y el TPM verifica la firma antes de su ejecución. RTC es una solución eficaz para el problema pero requiere dos precondiciones que deben considerarse. Por un lado, se necesita conocer la última localización del vehículo cuya identidad se quiere revocar. De lo contrario, el comando de revocación debería enviarse a todas las RSU simultáneamente, lo cual afectaría gravemente al rendimiento global de la red. Por otro, requiere que exista una comunicación confiable entre la autoridad y los vehículos. De hecho, si un atacante tiene capacidad de interceptar esta comunicación, el protocolo RTC no puede ejecutarse.

Para los casos en que RTC no puede ejecutarse, se hace necesario distribuir la información de revocación a los demás vehículos (Figura 2, mensaje 4-b). Sin embargo, existen

multitud de vehículos y éstos, además, pueden tener múltiples identidades (seudónimos). Por este motivo, las técnicas tradicionales de gestión y distribución de listas de certificados revocados (denominadas **CRL**, del inglés *Certificate Revocation List*) no son adecuadas para el entorno vehicular, en tanto que la lista sería inmanejable.

Se han propuesto dos alternativas complementarias para resolver, de manera eficiente, la distribución de CRL. En primer lugar, se propone **comprimir** la lista de certificados [14]. Esta compresión se hace utilizando una herramienta probabilística denominada filtros Bloom. Éstos permiten caracterizar a un conjunto de forma que se pueda conocer, con elevada probabilidad, si un elemento está contenido en dicho grupo. Gracias a los filtros, la información necesaria que se debe incluir en la lista de revocación se reduce considerablemente. Además de lo anterior, la CRL se divide en numerosos trozos, con lo que se simplifica su distribución. Cada trozo es verificable por separado, por lo que se garantiza la autenticidad de los datos enviados.

La segunda alternativa relacionada con la distribución se inspira en el funcionamiento biológico de las epidemias [15]. Cada vehículo que recibe la información actualizada de revocación se convierte en *portador* de la información. Cuando se encuentra con otros vehículos que no disponen de dichos datos, se produce la *infección* (Figura 2, mensaje 5). Este método aprovecha la potencialidad de las comunicaciones inter-vehiculares, descentralizando así la labor de distribución.

8. Proporcionando no repudio en emisión respetando la privacidad

En algunas aplicaciones de las redes vehiculares, es necesario garantizar, más allá de la autenticación, que el emisor del mensaje no pueda negar que envió éste. Este requisito, conocido como **no repudio en emisión**, se lleva a la práctica habitualmente mediante la **firma**

electrónica. Éste es el mismo mecanismo que se emplea en las aplicaciones que requieren que un mensaje (p.e. un aviso de accidente) sea avalado por un número mínimo de entidades distintas (a través de sus firmas) para ser creíble. Sin embargo, utilizar una firma tradicional lesionaría la privacidad del vehículo firmante, en tanto que se utilizaría su identificador permanente y, por tanto, dos mensajes distintos firmados por el mismo vehículo podrían ser relacionados. De nuevo, el problema del seguimiento se haría posible. La técnica que se propone en las redes vehiculares para abordar esta necesidad son las **firmas en grupo** [8]. Esencialmente, se trata de un tipo de firma en el que la entidad que verifique la firma puede estar segura de que el mensaje procedía de una entidad, sin conocer su identidad real. Sólo una entidad autorizada (de nuevo, sería la autoridad legal) podría revelar la identidad del firmante.

Los procedimientos necesarios para hacer posible este tipo de firmas son muy similares a los que ya se han descrito para la creación de certificados basados en seudónimos. La única diferencia sustancial es que la creación de las claves pública-privada no puede realizarse de manera distribuida. Es la autoridad de certificación quien establece una serie de parámetros que permiten derivar estas claves cumpliendo con las propiedades que se acaban de describir.

Una amenaza propia de este tipo de firmas es lo que se denomina habitualmente ***Sybil attack***. Esta amenaza consiste en que un único nodo utiliza, al mismo tiempo, múltiples identidades. De esta manera, un solo nodo podría firmar un mismo mensaje varias veces y el receptor no podría distinguir si dichas firmas proceden de entidades distintas. Para evitar esta amenaza en las redes vehiculares existen dos mecanismos. Por un lado, el propio componente confiable proporciona seguridad en este sentido, puesto que custodia los datos sensibles sin que sea posible alterarlos ni utilizar varias entidades al mismo tiempo. Por otro lado, en caso de que

no se disponga de este tipo de mecanismos, se proponen las **firmas en grupo enlazadas al mensaje** (en inglés, *Message-Linkable Group Signatures*) [16]. Las propiedades de este mecanismo aseguran que, dadas dos firmas sobre un mismo mensaje, es posible decidir si éstas proceden de dos entidades distintas, manteniendo al mismo tiempo el anonimato de las mismas. Al igual que sucedía en el caso anterior, la entidad autorizada podría revelar la identidad real de los firmantes.

9. Conclusiones

Las redes vehiculares proporcionan un nuevo y prometedor marco para la realización de nuevas aplicaciones que, entre otras cuestiones, permitirán mejorar la gestión del tráfico y la seguridad vial. Sin embargo, son también un escenario donde múltiples abusos pueden llevarse a cabo. Así por ejemplo, un vehículo podría distribuir datos falsos a través de la red, confundiendo al resto de vehículos. Por otro lado, un observador podría trazar el camino seguido por un vehículo, comprometiendo la privacidad de sus ocupantes (si existe alguna forma de conocer su identidad).

Todas estas cuestiones resaltan la necesidad de una adecuada gestión de la identidad, la creación de mecanismos de autenticación de los participantes, así como la protección de la privacidad. De hecho, estos asuntos constituyen temas centrales en el desarrollo de las redes vehiculares y deben abordarse en primera instancia para que el desarrollo futuro de estas nuevas redes sea satisfactorio.

En este trabajo se han revisado los principales mecanismos que permiten autenticar a un vehículo protegiendo al mismo tiempo la privacidad. Se han analizado los certificados de clave pública basados en seudónimos, al ser la alternativa más extendida. Además, se han examinado

las dificultades y mecanismos asociados al proceso de revocación. Finalmente, se han presentado algunos mecanismos para proporcionar la garantía de no repudio en emisión respetando, al mismo tiempo, la debida privacidad.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación (España), dentro del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2008-2011, bajo el contrato TIN2009-13461 (proyecto E-SAVE).

Referencias

[1] Gerlach, M. (2005). VaNeSe - An approach to VANET security. *V2VCOM.*

[2] Raya, M., Hubaux, J.-P. (2005). The Security of Vehicular Ad Hoc Networks, *Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, ACM.

[3] Parno, B., & Perrig, A. (2005) Challenges in Securing Vehicular Networks. *Workshop on Hot Topics in Networks (Hotnets-IV)*.

[4] Hubaux, J.-P., & Capkun, S. (2004). The security and privacy of smart vehicles. *IEEE Security and Privacy magazine*, 2 (3), 49-55.

[5] Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. *IEEE Wireless Communications*, 13 (5), 8-15.

[6] Lin, X., Sun, X., Ho, P.-H., & Shen, X. (2007). GSIS: A Secure and Privacy-Preserving Protocol for vehicular communications. *IEEE Transactions on vehicular technology*, 3442-3457.

[7] Sun, J., Zhang, C., & Fang, Y. (2007). An ID-Based framework achieving privacy and non-repudiation in vehicular ad-hoc networks. *Military Communications Conference (MILCOM)* (pp. 1-7). Orlando, Florida, USA: IEEE.

[8] Callandriello, G., G. Papadimitratos, P., Lloy, A., & Hubaux, J.-P. (2007). Efficient and Robust Pseudonymous Authentication in VANET. *International Workshop on Vehicular Ad Hoc Networks* (pp. 19-28). Montreal, QC, Canada: ACM.

[9] Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., & Raya, M. (2007). Architecture for Secure and Private Vehicular Communications. *7th International Conference on ITS*, (pp. 1-6).

[10] Sampigethava, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2006). CARAVAN: Providing Location Privacy for VANET. *International workshop on Vehicular ad hoc networks.* ACM.

[11] Gerlach, M. (2006). Assessing and Improving Privacy in VANETs. *Workshop on Embedded Security in Cars (ESCAR)*.

[12] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communication Magazine*.

[13] Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications Magazine*, 46 (11), 110-118.

[14] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., & Hubaux, J.-P. (2007). Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 25 (8), 1557-1568.

[15] Laberteaux, K. P., Haas, J. J., & Hu, Y.-C. (2008). Security Certificate Revocation List Distribution for VANET. *International Conference on Mobile Computing and Networking* (pp. 88-89). ACM.

[16] Domingo-Ferrer, J., & Wu, Q. (2009). Safety and privacy in vehicular communications. *Lecture Notes in Computer Science*, 173-189.