Protocolo de creación de evidencias en entornos vehiculares

J.M. de Fuentes, A.I. González-Tablas, A. Ribagorda, B. Ramos

Universidad Carlos III, Avda. Universidad 30, 28911 Leganés, España.
{jfuentes, aigonzal, arturo, benja1}@inf.uc3m.es
Teléfono: +34 91 624 94 22

Resumen Las redes vehiculares son un novedoso escenario de comunicación. Estas redes permiten el diálogo entre vehículos, y de estos con la infraestructura. Gracias a estas redes se puede proporcionar más información y nuevos servicios a conductores y pasajeros. Uno de esos nuevos servicios es la creación de evidencias sobre el comportamiento de un vehículo. Esto será útil, por ejemplo, para la correcta determinación de responsabilidad en un accidente o para justificar un comportamiento adecuado ante una sanción recibida. Utilizando las redes vehiculares se puede obtener la descripción de ese comportamiento a través de los vehículos del entorno. Con ello se impide que el propio vehículo describa su actuación de una forma modificada acorde con sus intereses. Para abordar este nuevo servicio es necesario garantizar la seguridad de la información intercambiada. En este trabajo se presenta un protocolo de creación de evidencias sobre el comportamiento de un vehículo, obteniendo los datos desde los cercanos. Se incluye el protocolo de verificación de las evidencias, así como el análisis de seguridad de la propuesta.
Palabras clave: Evidencia, VANET, testigos.

1. Introducción

El transporte terrestre mediante vehículos es, hoy día, una de las actividades humanas imprescindibles. Por este motivo, las inversiones para la mejora de todos los elementos implicados son cada vez más notables. Los avances en esta dirección están orientados a facilitar la tarea de conducción y proporcionar un mayor bienestar y seguridad a los conductores y pasajeros.

Como muestra del nivel de desarrollo de los transportes, la siniestralidad en las carreteras ha disminuido en un 44 % en los últimos 5 años en España [1]. No obstante, la sociedad de la información en la que actualmente estamos inmersos demanda un nuevo tipo de bienestar. Se debe proporcionar medios audiovisuales (música, vídeo) así como acceso a las fuentes de información (Internet) y a las nuevas formas de comunicación (correo electrónico, mensajería instantánea, etc.).

Para satisfacer estas necesidades, las tecnologías de la información y las comunicaciones están experimentando un fuerte desarrollo en el ámbito vehicular. En los últimos tiempos, las redes ad-hoc vehiculares (Vehicular Ad-hoc NETwork, VANET) se han sumado a las posibilidades de conectividad actuales (Wi-Fi,

GPRS, UMTS). Este nuevo tipo de redes están especialmente concebidas para interconectar vehículos entre sí y con las infraestructuras de comunicación que se desplieguen en las carreteras.

Gracias a estas nuevas posibilidades de comunicación intervehicular, surgen nuevas aplicaciones interesantes para la mejora del desarrollo del tráfico. Por ejemplo, los propios vehículos pueden advertir a sus seguidores acerca de incidencias en la vía o del estado de la circulación. Sin embargo, a pesar del grado de desarrollo alcanzado, existen situaciones del tráfico para las que las soluciones tradicionales no son suficientes. En la actualidad, por ejemplo, la determinación de responsabilidad ante un accidente se enfrenta a la falta de pruebas fehacientes que reflejen adecuadamente los hechos. Igualmente, los conductores no disponen de medios de prueba que acrediten que se actuó correctamente en el momento de una supuesta infracción. Las redes vehiculares pueden contribuir en esta dirección utilizando una característica inherente: los vehículos que presenciaron el hecho pueden ofrecer los datos que conocen para describir la situación en cuestión. De esta manera, se pueden construir evidencias relativas al comportamiento de un vehículo en un pasado reciente. Este tipo de elementos probatorios son de gran interés para todos los implicados en el transporte. Los conductores pueden, por primera vez, disponer de pruebas para defenderse de acusaciones inciertas o aclarar las circunstancias de un accidente. Así mismo, las aseguradoras evitan los fraudes derivados de partes de accidente con datos inciertos. Por su parte, las autoridades pueden simplificar el proceso de esclarecimiento de las circunstancias de un siniestro, así como la burocracia de la tramitación de sanciones.

En este trabajo se propone un protocolo para la creación de evidencias sobre el comportamiento de un vehículo obtenidas a través de aquellos que circulan en su entorno. Para construir esa evidencia, el solicitante podrá obtener el consenso a partir de los testimonios recogidos. Con ello se facilita su interpretación por parte del destinatario (que, generalmente, será un juez o autoridad competente). Además, se persigue el anonimato de los testigos frente al solicitante, con lo que se previenen posibles represalias derivadas de testimonios no favorables para este. Para la consecución de los aspectos de seguridad, el protocolo utiliza los servicios establecidos por el estándar IEEE 1609.2, de seguridad en redes vehiculares [2].

El resto del artículo se estructura como sigue. El apartado 2 describe el entorno vehicular y señala los aspectos relevantes del escenario y del estándar sobre el que se apoya la propuesta. El apartado 3 introduce el concepto de evidencia y detalla cómo se puede obtener en el ámbito vehicular. El apartado 4 desarrolla el protocolo de creación de evidencias que se propone. El apartado 5 se centra en el protocolo de verificación de las evidencias creadas. El apartado 6 expone el análisis de seguridad de la propuesta. El apartado 7 incluye los trabajos relacionados y, finalmente, el apartado 8 recoge las conclusiones y líneas futuras.

2. El entorno vehicular

El entorno vehicular, como escenario de comunicación, afronta numerosos retos que no se habían planteado hasta el momento. En primer lugar, los vehículos

(que serán nodos de comunicación) se desplazan a una alta velocidad (incluso por encima de los 100 km/h) y con distintos itinerarios. Esto provoca que las redes se formen con un conjunto de nodos muy volátil. Por otro lado, pueden concentrarse numerosos vehículos en una misma área (por ejemplo, en un semáforo o en un atasco), lo que da lugar a redes con un elevado número de nodos.

Las comunicaciones vehiculares se establecen generalmente ad-hoc, siendo los nodos los propios vehículos o la infraestructura de comunicaciones (si existe) situada a lo largo de la vía. Los elementos de comunicación de la infraestructura se sitúan longitudinalmente a la vía, generalmente aprovechando los elementos de balizamiento o señalización vertical tradicional. Dada la extensión de la red de carreteras, no se puede asumir la existencia de dicha infraestructura en todo punto de la red viaria. Este hecho limita fuertemente las suposiciones sobre los servicios accesibles desde el vehículo. Desde el punto de vista de la seguridad, es importante destacar que no se dispone de terceros de confianza (autoridades de sellado de tiempo o de certificación) permanentemente accesibles.

2.1. El estándar IEEE 1609.2

Las características especiales que se han descrito han motivado la creación de una variante del estándar IEEE 802.11 de comunicación inalámbrica. Esta se conoce como WAVE (Wireless Access in Vehicular Environments). La familia de estándares IEEE 1609 define la arquitectura y los servicios necesarios para posibilitar las comunicaciones vehiculares.

En particular, la norma IEEE 1609.2 define los servicios de seguridad para aplicaciones de este entorno [2]. Las características de esta norma, en lo relativo a la propuesta que se presenta, son las siguientes:

- *Modelos de comunicación.* Se recogen dos tipos de comunicación. El primero permite la oferta de servicios al resto de vehículos y su aceptación por parte de estos. El segundo se basa en el intercambio de mensajes cortos (WSM, Wave Short Messages). Mientras que la intención de aquéllos es establecer una sesión entre comunicantes, los WSM pueden utilizarse esporádicamente.
- *Algoritmos criptográficos.* Se establece la utilización de ECIES (para cifrado asimétrico), ECDSA (para firma) y AES en modo CCM (para cifrado simétrico). Para compartir la clave simétrica, se debe realizar un ensobrado digital con ECIES.
- *Certificación.* Los nodos disponen de certificados de clave pública. Para comprobar su estado se utilizan listas de certificados revocados (CRL).
- *Tipos de mensajes.* Los mensajes pueden viajar en claro, firmados o cifrados. Así mismo, es posible enviar mensajes cifrados y firmados.
- *Datos accesibles.* Se asume que cualquier unidad de comunicaciones WAVE conoce su posición y el tiempo actual (y una estimación del error cometido). Para firmar, se asume que se dispone de la clave criptográfica, los certificados asociados, una implementación de los algoritmos de firma y un generador de números aleatorios criptográficamente seguro.

- *Aseguramiento adicional de las aplicaciones.* Las aplicaciones pueden prevenir los ataques de repetición utilizando sellos de tiempo (*time stamps*). Además, se permite que las aplicaciones no envíen mensajes firmados cuando el margen de error en el tiempo o posición actual sea demasiado grande.
- *Aspectos de privacidad.* El estándar no aborda ningún mecanismo para conseguir el envío anónimo de mensajes autenticados. Por otra parte, el estándar se centra en proteger los datos contenidos en los mensajes y no contempla el anonimato en los encabezados de los paquetes. Por ello, pueden producirse pérdidas de privacidad derivadas de la revelación de cierta información estática (e.g. direcciones IP fijas, etc.)

3. Evidencias electrónicas en el ámbito vehicular

Antes de abordar cómo crear evidencias en el ámbito vehicular es preciso, en primera instancia, determinar qué es una evidencia electrónica. Tras abordarlo en el primer apartado, el segundo describe para qué pueden servir y el tercero qué elementos mínimos se necesitan para su creación.

3.1. Evidencias electrónicas. Definición y requisitos

El término "evidencia electrónica" dispone de numerosas definiciones en la literatura. En el contexto de este trabajo, dicho término se refiere a *"cualquier registro generado por, o almacenado en, un sistema computacional que puede ser utilizado como prueba en un proceso legal"* [3].

Partiendo de esta definición, se habla de evidencia cuando se cree que las conclusiones derivables de esa información son indiscutibles y que, por tanto, el juez aceptará la evidencia como prueba [4]. Para que dicha aceptación sea posible y a pesar de la heterogeneidad legislativa existente, se establecen habitualmente cuatro principios para la admisibilidad de las pruebas [5]:

- Autenticidad y Confiabilidad, es decir, que la prueba sea auténtica y contenga datos fiables.
- Suficiencia, es decir, que sea completa para acreditar el hecho.
- Conformidad con las leyes, especialmente, que se haya obtenido sin violar otros derechos.

Estos principios constituyen requisitos necesarios para que la evidencia tenga peso como prueba en un proceso judicial. El juez o magistrado es (habitualmente) el encargado de verificar el cumplimiento de dichos principios, así como de valorar la relevancia de lo aportado dentro del proceso en curso. Por este motivo, para la utilización de evidencias electrónicas en procesos policiales o judiciales debe extremarse la corrección técnica en todo el proceso de custodia.

3.2. Usos previstos de las evidencias vehiculares

Para satisfacer, en el ámbito vehicular, las exigencias planteadas en el apartado anterior, se debe conocer qué se pretende acreditar a través de las evidencias. Por ello, algunos de sus usos previstos son los siguientes:

1. Acreditación espacio-temporal, demostrar que un determinado vehículo se encontraba en un determinado lugar en un momento concreto.
2. Demostración de correcto comportamiento, por ejemplo, ante una sanción por exceso de velocidad, siempre que esta se notifique inmediatamente.
3. Determinación de las circunstancias de un accidente, por ejemplo, si se activó o no el intermitente en un cambio de carril que provocó una colisión.

3.3. Elementos necesarios para crear evidencias vehiculares

Para construir estas evidencias se necesita obtener, de acuerdo al principio legal de *suficiencia* antes introducido, cuantos datos sean necesarios para acreditar el suceso. Así, además del momento de la evidencia, será necesario recabar datos adicionales, tales como información de posicionamiento (GPS, etc.) o datos procedentes de los sensores incorporados en el vehículo. Todas estas fuentes de datos son susceptibles de falsificación. Los sistemas de posicionamiento son susceptibles de ataques basados en la alteración de la señal (e.g. *jamming* [6]), entre otros. Por su parte, la seguridad física de las redes sensoriales en los vehículos no es muy elevada. Aunque se han propuesto algunas medidas de protección, estas no han sido globalmente implementadas en los sistemas de automoción [7]. De esta manera, se hace posible que el propietario de un vehículo manipule los datos para así dibujar una falsa realidad más propicia a sus intereses.

Afortunadamente, se pueden paliar estas deficiencias utilizando las redes vehiculares, pues los propios vehículos del entorno pueden servir como fuente de datos. Se necesita que dichos vehículos (que llamaremos *testigos*) sean mayoritariamente *participativos* y *honestos*. Se requiere que los testigos participen (es decir, ofrezcan su testimonio al solicitante) para que se dispongan de los datos externos que permitan crear las evidencias. Por otro lado, se requiere que sean honestos para que los datos que ofrezcan no hayan sido maliciosamente manipulados en origen. Dicha honestidad no asegura que los testimonios describan fielmente la realidad: siguen siendo posibles errores sensoriales derivados de las propias técnicas de medición utilizadas. Sin embargo, habitualmente es posible cuantificar el grado de incertidumbre propio de cada medida, lo que permite dar la credibilidad adecuada a cada testimonio.

Para cerrar el ciclo de custodia de la evidencia, una vez obtenidos los datos es preciso almacenarlos de forma fiable. Los vehículos deben disponer de capacidad computacional para realizar tareas criptográficas (esencialmente firma digital, para asegurar origen e integridad). Además, deben disponer de una fuente fiable de tiempo para añadir información temporal a la evidencia. Todas estas cualidades se integran en los dispositivos Hardware Security Module (HSM) que ya se han propuesto en el ámbito vehicular [8].

En esta sección se han abordado los requisitos esenciales para crear evidencias en el entorno vehicular. Se necesita disponer de fuentes confiables de datos, así como un almacenamiento seguro para dicha información. Es preciso diseñar un protocolo que permita la transferencia de dicha información entre los testigos y el solicitante, aspecto que se abordará en el siguiente apartado.

4. Protocolo de creación de evidencias vehiculares

Teniendo en cuenta las peculiaridades del entorno vehicular (apartado 2) y los aspectos particulares sobre evidencias electrónicas (apartado 3), en este apartado se propone un protocolo para crear evidencias electrónicas en este contexto. Para ello, primeramente se introduce la filosofía subyacente del protocolo propuesto. Posteriormente se enuncian las suposiciones necesarias para implantarlo y finalmente se presenta el protocolo en sí mismo.

4.1. Idea general del protocolo

El protocolo persigue la creación de evidencias sobre el comportamiento reciente de un vehículo. Sin embargo, como ya se ha dicho, el vehículo en cuestión puede manipular los datos para obtener una descripción de la situación más favorable para sus intereses. Por este motivo, se recurre a la obtención distribuida de los datos desde los vehículos del entorno. Debido a la alta movilidad de los vehículos, un protocolo de intercambio de información demasiado extenso podría provocar la pérdida de conectividad del solicitante con los vehículos aptos para ser testigos. Por este motivo, el protocolo requiere únicamente dos transferencias de datos: petición de información (solicitud) y envío de estimaciones (respuesta). Estas fases aparecen representadas en la Figura 1.

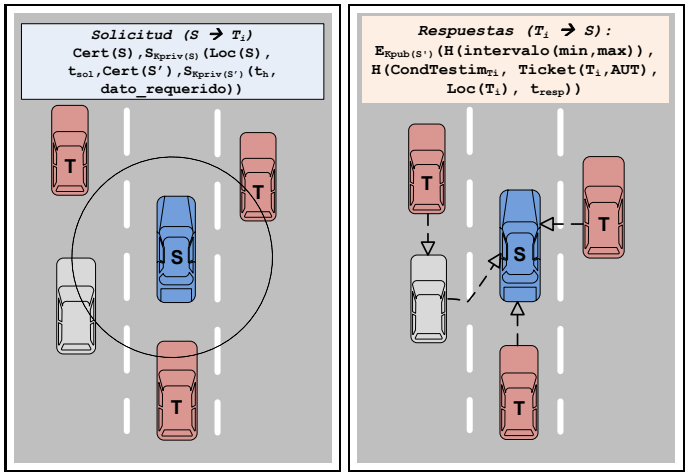

Figura 1. Fases del protocolo de creación de evidencias.

Es importante observar que no todos los vehículos disponen de esa información. En otras palabras, no todos los vehículos del entorno son aptos para ser testigos. En la Figura 1, el vehículo azul (marcado con 'S') es el solicitante de la evidencia, mientras que los rojos (marcados con 'T') son posibles testigos. El vehículo blanco no dispone de información sobre el solicitante y representa

los vehículos del entorno que participan como intermediarios en la comunicación debido a la lejanía de los comunicantes.

Un aspecto interesante del protocolo es que se autoriza al solicitante a crear una evidencia que contenga el dato consensuado tomando en consideración los datos procedentes de los testigos. Gracias a esto, se simplifica la interpretación de la evidencia, siendo más clara la circunstancia que se quiere demostrar y su relevancia para el proceso en el que se utilice. Para hacer posible la construcción de ese consenso, el testigo envía, junto con sus estimaciones acerca del hecho considerado (e.g. velocidad del solicitante), un *token* especial. Este token contiene en su interior las condiciones bajo las cuales el solicitante puede construir el consenso utilizando el dato aportado por el testigo. Dichas condiciones expresan, entre otras cosas, quién era el solicitante y cuáles fueron las estimaciones enviadas. Así, el solicitante no podrá (legítimamente) crear un consenso apoyado por el testigo utilizando un dato que no se ajuste a las estimaciones que este hizo.

Finalmente, debe destacarse que el protocolo crea una única evidencia autocontenida (e.d. contiene toda la información necesaria para verificarla). Esta cualidad incrementará su confiabilidad ante la autoridad a la que se presente.

4.2. Suposiciones sobre el entorno

Para que el protocolo propuesto sea factible en el entorno vehicular es preciso que existan cuatro requisitos mínimos, derivados de las necesidades expuestas para la creación de evidencias vehiculares (apartado 3.3):

- Existencia de una Autoridad de Certificación. El estándar IEEE 1609.2 exige que la autenticación de las entidades se realice mediante certificados. Por este motivo, se exige que exista una Autoridad de Certificación que se ocupe de la gestión de dichos certificados.
- Incorporación de una plataforma confiable en el vehículo. Es preciso contar con un almacenamiento confiable con capacidades criptográficas y una fuente fiable de tiempo. Se necesita, por tanto, un dispositivo HSM en el vehículo.
- Incorporación de sensores en el vehículo. El vehículo debe disponer de sensores (vídeo, radar, etc.) para conocer el estado de su entorno (estado de la vía, obstáculos, etc.). A través de los sensores es posible reconocer el comportamiento de otros vehículos, lo que servirá como fuente principal de datos para este protocolo [9]. Dichos datos son almacenados en el citado HSM.
- Mayoría honesta y atacantes no colaborativos. Los testigos deberán ser mayoritariamente honestos, lo que permitirá aislar los testimonios que difieran significativamente de las estimaciones de la mayoría. Los atacantes, por su parte, deben operar de manera independiente, es decir, no colaboran para construir un falso testimonio común.

Además de lo anterior, es conveniente que los vehículos utilicen las redes vehiculares para comunicarse datos útiles sobre el estado del tráfico. Existen dos paradigmas para llevar a cabo esta comunicación. Por un lado, los vehículos pueden enviar periódicamente mensajes de reporte de estado (*beaconing*).

El cometido de esos mensajes es ofrecer a los vehículos del entorno información sobre las circunstancias propias (posición, velocidad, estado, etc.). Por otro lado, gracias a la conducción cooperativa (e.g. Cooperative Cruise Control), los vehículos se agrupan en función de sus parámetros de conducción (e.g. destino, velocidad deseada). Ambas formas de comunicación son interesantes para este trabajo ya que permiten que el resto de vehículos conozcan más detalles sobre el comportamiento del vehículo solicitante.

Finalmente, a fin de preservar la identidad real de los participantes, se asume que los vehículos emplean seudónimos para su identificación. Estos deben poder ser resolubles por la Autoridad, a fin de obtener la identidad real de los implicados en caso necesario [10]. Además, se asume que los vehículos cambian periódicamente de seudónimo, para evitar su trazabilidad.

4.3. Notación

Para describir el protocolo se utilizará la notación siguiente. En primer lugar, los roles posibles son:

- S, el vehículo que solicita la creación de la evidencia (solicitante).
- T_i, vehículo (testigo) que tiene datos sobre el comportamiento reciente de S.
- AUT, la autoridad legal a la que se presentará la evidencia.

Las funciones criptográficas se denotan de la forma siguiente:

- H(M), función resumen sobre 'M'. Incluye también el mensaje resumido (M).
- S_K(M), firma de 'M' con la clave K y el algoritmo ECDSA. Incluye también el mensaje a firmar (M).
- E_K(M)/D_K(M), cifrado/descifrado asimétrico de 'M' con la clave K y el algoritmo ECIES.
- SE_K(M), cifrado simétrico de 'M' con la clave K y el algoritmo AES-CCM.
- Verify(F,Cert(X)), verificación del mensaje firmado 'F' utilizando la clave contenida en el certificado Cert(X).

Finalmente, los datos intercambiados se denotan como sigue:

- ID(X), el identificador (seudónimo) del vehículo X.
- Cert(X), certificado de clave pública del vehículo X.
- intervalo(a,b), expresión de los valores contenidos en el intervalo [a,b], independientemente de la naturaleza de a y b.
- t_i, marca de tiempo del momento i.
- Loc(X), coordenadas del lugar actual del vehículo X.

4.4. Descripción del protocolo

A continuación se expone el protocolo de creación de evidencias, junto con una breve explicación del cometido de los mensajes.

Fase 1. Solicitud de datos

En este mensaje, el solicitante envía un mensaje firmado (Signed WSM) indicando la información que se requiere (dato_ requerido) y el tiempo de la misma (t_h). Debido al cambio periódico de seudónimos, es posible que el actual del solicitante (S) fuera distinto del que se usaba en el momento al que se refieren los datos requeridos (S'). A través de este mensaje, el solicitante demuestra que esa era su identidad en el momento de los hechos.

$S \rightarrow T_i$: Cert(S),$S_{Kpriv(S)}$(Loc(S), t_{sol}, Cert(S'), $S_{Kpriv(S')}$(t_h, dato_ requerido))

El mensaje se envía a todos los vehículos que se encuentren en un entorno razonable del solicitante (*geocasting*), utilizando para ello los datos de localización proporcionados por este. Con ello se evita la propagación de la solicitud a vehículos que no pueden disponer de dicha información (por estar situados demasiado lejos del solicitante).

Fase 2. Envío de respuestas

La segunda fase tiene como objetivo enviar las respuestas (testimonios) desde los vehículos testigos al solicitante. Esta fase solo tiene lugar si la información ha sido recibida de forma íntegra, lo que se asegura verificando las firmas de la solicitud. Igualmente, se verifica que tanto la localización como el tiempo de la solicitud toman valores razonables. En [11] se describe una forma de realizar estas comprobaciones. Si resultan satisfactorias, se realizan los siguientes pasos:

2.a. Estimación del dato basado en información del exterior.

Cada uno de los testigos estima cuál es el valor del dato requerido por el solicitante. Para ello, utiliza las informaciones que se le han proporcionado desde el exterior sobre el solicitante (beaconing, Cooperative Cruise Control). Usando estas fuentes de información, se crea un intervalo posible.

T_i : beaconing(S') x Coop. Cruise Control(S') $\Rightarrow$ intervalo_ posible

2.b. Contraste de hipótesis.

Utilizando como entrada el intervalo obtenido en el paso anterior (intervalo_ posible), se utiliza el conocimiento propio (sobre la propia situación y sobre el solicitante) para establecer si el intervalo anterior es razonable. Para ello se emplean las mediciones obtenidas desde los propios sensores (radar, vídeo, ordenador a bordo, etc.). Supongamos que el solicitante desea que los testigos acrediten su velocidad. El intervalo_ posible (del paso anterior) es (100,120). Si el testigo circulaba en t_h a 110 y los sensores detectan que ese vehículo fue adelantado, el subintervalo de velocidades (110,120) queda descartado.

T_i : intervalo_ posible x informacion_sensores $\Rightarrow$ intervalo(min,max)

El diseño de este cálculo es una tarea compleja, pues requiere otorgar credibilidad a múltiples fuentes de datos. En [12] y [13] se analizan diversas técnicas para abordar esta cuestión.

2.c. Envío de respuesta.

Si el intervalo construido en el paso anterior contiene algún valor, se procede a enviar la respuesta. La respuesta contiene tras partes. La primera va dirigida al solicitante y contiene la estimación sobre el dato_ requerido. Dicha estimación está cifrada (por confidencialidad) utilizando la clave del solicitante en el momento de los hechos (e.d. K_{pub}(S')). La segunda parte va dirigida a la Autoridad

a la que se presente la evidencia. Esta parte (denotada como Ticket) contiene la clave $K_{Testim(Ti)}$:

Ticket(T_i,AUT) = $E_{Kpub(AUT)}$(Cert(T_i), $S_{Kpriv(Ti)}$($K_{Testim(Ti)}$))

$K_{Testim(Ti)}$ se utiliza para cifrar las condiciones bajo las que el solicitante puede crear un consenso utilizando el dato proporcionado por el testigo. Dichas condiciones cifradas conforman el token $CondTestim_{Ti}$. El solicitante podrá usar dicho token para reflejar que el consenso alcanzado está avalado por las observaciones efectuadas por el testigo.

$CondTestim_{Ti} = SE_{KTestim(Ti)}$(ID($T_i$), ID(S'), intervalo(min,max), t_h, t_{resp})

Es preciso destacar que gracias a esta distribución de la información, la identidad del testigo queda oculta para el solicitante. Esto resulta especialmente beneficioso en caso de que el testimonio no resulte favorable para el solicitante, lo que podría originar represalias contra aquel. La respuesta definitiva es:

$T_i \rightarrow$ S: $E_{Kpub(S')}$(H(intervalo(min,max)), H($CondTestim_{Ti}$, Ticket (T_i,AUT), Loc(T_i), t_{resp}))

Fase 3. Generación de evidencia.

El solicitante verifica que la información espacio-temporal del testigo es razonable, así como la integridad de la estimación recibida. Si es así, calcula el dato de consenso entre todos los testigos, es decir, datoConsenso $\in$ $intervalo_{Ti}$ $\forall$ i. Si no es posible dicho consenso, se busca el valor que esté contenido en la mayor cantidad posible de observaciones de los testigos.

Usando ese dato, se crea la evidencia definitiva (EV(S)), incluyendo los tokens de autorización de los distintos testigos. Para n testigos, la evidencia queda:

EV(S) = Cert(S), $S_{Kpriv(S)}$(datoConsenso, t_h, t_{evid}), (Ticket(T_1,AUT), $CondTestim_{T1}$,(...), Ticket(T_n,AUT), $CondTestim_{Tn}$)

5. Protocolo de verificación de la evidencia

En esta sección se presenta el protocolo de verificación asociado a la evidencia creada. La notación empleada es la misma que la expuesta en el apartado 4.3. Excepto la Fase 1, todas se realizan sobre cada uno de los testimonios contenidos en la evidencia. La verificación se supera si todas las fases se superan.

Fase 1. Verificación de firma de EV(S)

En primer lugar, se comprueba la firma sobre la evidencia, para asegurar su origen e integridad.

AUT : Verify(EV(S),Cert(S))

Fase 2. Descifrado de Ticket y obtención de condiciones del testimonio

El Ticket contiene la clave de protección de las condiciones del testimonio, por lo que es necesario obtenerla.

AUT : $D_{Kpriv(AUT)}$(Ticket(T_i,AUT)), con lo que se obtiene (Cert(T_i), $S_{Kpriv(Ti)}$ ($K_{Testim(Ti)}$)).

Si la verificación de la firma sobre $K_{Testim(Ti)}$ es correcta, se utiliza dicha clave para obtener las condiciones bajo las que se facilitó el testimonio:

AUT : $SE_{KTestim(Ti)}$($CondTestim_{Ti}$), obteniendo (ID(T_i), ID(S'), intervalo(min,max), t_h, t_{resp})

Fase 3. Verificación del estado de los certificados

La autoridad comprueba que los certificados eran válidos (no caducados ni revocados) en los momentos en que se utilizaron (t_{resp} para el testigo, t_{evid} para el solicitante).

Fase 4. Verificación del cumplimiento de las condiciones del testimonio

4.a Verificación de identidades

Debe comprobarse que el solicitante coincide con el autorizado por el testigo (a pesar de que puede haber cambiado de seudónimo). También debe comprobarse que el testigo y el solicitante son entidades distintas, así como los distintos testigos entre sí. Igualmente, los usos previstos de las evidencias exigen obtener la identidad real del solicitante, por lo que deberá resolverse el seudónimo. Para realizar estas operaciones, la autoridad que reciba la evidencia deberá contactar con la entidad encargada de la gestión de los seudónimos.

4.b Dato y momento legítimos

Se debe verificar que el dato consensuado está contemplado en las estimaciones del testigo. Además, se debe comprobar que el momento al que se refieren los testimonios es el momento del dato consensuado. También se comprueba que t_{evid} sea posterior (y no muy lejano) a t_h.

6. Análisis de seguridad

Tras la presentación de los protocolos propuestos, es necesario realizar un análisis de seguridad sobre la propuesta. En este trabajo resulta especialmente importante analizar si se satisfacen las propiedades necesarias para su admisibilidad como prueba (Sección 3.1). Si bien el cumplimiento del principio de *suficiencia* es responsabilidad del solicitante (que debe requerir los datos necesarios), el resto de principios dependen de la realización del protocolo descrito.

6.1. Autenticidad de la evidencia

Es preciso garantizar que la evidencia es auténtica. Para ello, se discutirá acerca de la integridad y el no repudio de la información en juego, así como la autenticación de las entidades participantes.

La *integridad* de la solicitud puede comprobarse gracias a las firmas incluidas. La integridad de los testimonios es también verificable gracias al uso de funciones resumen. De esta manera, es posible comprobar alteraciones maliciosas sobre los mensajes producidas por un intermediario. En lo referente al *no repudio*, en emisión está garantizado (tanto en los testimonios como en la evidencia) gracias al uso de firmas digitales. Sin embargo, el no repudio en recepción no está contemplado al no ser necesario en el contexto del protocolo.

Por lo que respecta a la *autenticación* de las entidades, tanto el solicitante como los testigos utilizan los certificados impuestos por el estándar. Sin embargo, la certificación conlleva ciertos problemas que deben ser considerados. En primer lugar, desde el punto de vista del testigo, si el certificado del solicitante

es revocado con anterioridad a la solicitud, es posible que no disponga de esa información. Esto origina que los testigos pueden participar en una ejecución inútil del protocolo, puesto que la evidencia creada carecerá de valor probatorio (al no ser confiable el solicitante). Esta amenaza está motivada por la compleja distribución de la información del estado de los certificados. Para paliarlo se podría utilizar un protocolo específico para la distribución de esta información [14].

6.2. Confiabilidad de la evidencia

Se debe asegurar que la evidencia contiene datos confiables. Gracias al uso de testigos (y bajo el supuesto de mayoría honesta), se consigue una fuente de datos presumiblemente imparcial. El consenso alcanzado por el solicitante se verifica utilizando los elementos de información contenidos en la propia evidencia. Sin embargo, desde el punto de vista del solicitante existen dos problemas que el protocolo actual no soluciona. En primer lugar, un testigo deshonesto podría dar una estimación al solicitante distinta de la incluida en CondTestim_{Ti}. De esta manera, el solicitante puede crear una evidencia que carezca de valor al no ajustarse (involuntariamente) a las supuestas estimaciones del testigo. Esta desventaja para el solicitante también puede manifestarse en que se reciban varios testimonios desde el mismo testigo, empleando distintos seudónimos. La comprobación por parte de la autoridad revelará este hecho y restará credibilidad a la evidencia, aunque en principio no debería ser causa de anulación.

Ambas cuestiones constituyen amenazas presentes, aunque de impacto presumiblemente limitado. Para su realización sería necesario alterar la plataforma confiable, o crear un componente alternativo que llevara a cabo el ataque. Además, no parece existir una motivación clara para este comportamiento, ya que requiere un procesamiento no despreciable para obtener un dudoso beneficio.

Por otra parte, la frescura de los testimonios se comprueba en la verificación de la evidencia. Dado que el HSM dispone de una fuente fiable de tiempo, vehículos no presentes no tienen capacidad para crear testimonios "a posteriori". Estas marcas de tiempo protegen también al protocolo de ataques de repetición.

6.3. Conformidad con las leyes. Privacidad

La evidencia debe obtenerse sin violación de otros derechos. En este contexto, la privacidad es el derecho más amenazado. De hecho, a nivel conceptual, el solicitante pide a los testigos que le confirmen cuál fue su comportamiento en el pasado. La trazabilidad (del solicitante) es una necesidad en el protocolo. Sin embargo, esta violación de privacidad (inherente al protocolo) se ve compensada por el beneficio obtenido, la evidencia creada. Además, las estimaciones sobre su comportamiento se encuentran cifradas, por lo que se evita que el resto de vehículos conozcan más datos sobre el solicitante. Por su parte, la identidad de los testigos se encuentra protegida. Como ya se dijo, permanecen anónimos frente al solicitante. Además, según la descripción del protocolo de verificación, no es necesario resolver la identidad del testigo, con lo que se evita su trazabilidad por parte de la autoridad.

6.4. Otras amenazas posibles y riesgo de materialización

En primer lugar, la *disponibilidad* de las capacidades de comunicación de los vehículos puede quedar comprometida si el protocolo de creación de evidencias se utiliza frecuentemente. De hecho, todas las fases de dicho protocolo conllevan un cierto procesamiento criptográfico, por lo que es posible realizar un ataque de denegación de servicio mediante inundación de solicitudes. La utilidad de este tipo de ataque vendría determinada por la finalidad de la evidencia. Si, por ejemplo, se pretende obtener una evidencia que acredite una circunstancia tras la ocurrencia de un accidente, la parte culpable intentará evitar la creación de pruebas. Como contramedida, el protocolo requiere tan solo dos mensajes, para evitar en lo posible la sobrecarga del medio.

Los vehículos intermediarios también pueden afectar al desarrollo del protocolo. Si no se propaga la solicitud, o si no se encaminan adecuadamente los testimonios, el protocolo de creación pierde efectividad. Para disminuir el riesgo de esta amenaza se podría utilizar un mecanismo de prevención de comportamientos no colaborativos [15].

Por otro lado, el token de autorización del consenso $\mathrm{CondTestim}_{Ti}$ es el resultado de cifrar las condiciones válidas de consenso con una clave simétrica ($\mathrm{K}_{Testim(Ti)}$). Si dicha clave se reutiliza en varias respuestas consecutivas a un mismo solicitante, es posible realizar un *ataque de texto en claro conocido*. No obstante, asumiendo que los vehículos están en movimiento, es improbable que se produzcan los intercambios necesarios para comprometer la clave. En cualquier caso, se recomienda que la clave $\mathrm{K}_{Testim(Ti)}$ cambie periódicamente.

7. Trabajos relacionados

El aseguramiento de las comunicaciones vehiculares se ha abordado de forma extensa en la literatura [16]. No obstante, y hasta donde se ha desarrollado esta investigación, la creación de evidencias en el entorno vehicular ha sido escasamente abordada. Las propuestas más relevantes se centran en la reconstrucción de accidentes. En [17] se aborda este problema utilizando la plataforma confiable (la citada HSM) como elemento de registro de datos, a modo de "caja negra". Tras la ocurrencia del accidente, los vehículos implicados envían mensajes de advertencia, utilizando sus propias mediciones sensoriales como fuente de datos. Como ya se ha dicho, dichas fuentes podrían ser manipuladas, por lo que podría cuestionarse la validez de las evidencias que se pudieran derivar.

Por otra parte, en [18] se aborda la reconstrucción de accidentes utilizando datos propios y aquellos recibidos en las comunicaciones intervehiculares. Aunque nuestro enfoque es similar, en el presente trabajo se asume que los vehículos pueden obtener datos del estado de su entorno, lo que enriquece el proceso. Además, las aplicaciones objetivo de la presente propuesta se extienden más allá de la reconstrucción de accidentes.

La generación de evidencias ha sido también abordada dentro del marco de seguridad propuesto por Lin *et al.* [19]. Este marco se centra en proporcionar

seguridad y privacidad, junto con la debida trazabilidad en caso necesario. Para ello utilizan criptografía basada en identidad y firmas en grupo. Si bien esta última herramienta podría incorporarse a la propuesta que se presenta, para la autenticación se ha preferido utilizar certificados de clave pública, siguiendo las directrices marcadas por el estándar de seguridad en redes vehiculares.

Finalmente, las propuestas de creación de grupos podrían verse como un medio para la selección de testigos. Este tipo de técnicas han sido extensivamente abordadas, e incluso se han propuesto mejoras destinadas a mejorar la eficiencia de la comunicación dentro del grupo. De forma significativa, Raya *et al.* [20] abordan la agregación de valores de los miembros de un grupo. A pesar de ello, el contexto de uso de la presente propuesta requiere contactar con los vehículos aptos para ser testigos, es decir, aquellos que disponen de información sobre el comportamiento pasado del solicitante. Teniendo en cuenta la volatilidad de los grupos formados, es posible que no todos los testigos formen parte del grupo en el momento en que se solicita la creación de la evidencia. Por este motivo, no parece adecuado utilizar la formación de grupos para la selección de testigos.

8. Conclusiones y trabajo futuro

En este trabajo se ha presentado un protocolo para la creación de evidencias sobre el comportamiento de un vehículo utilizando datos procedentes de algunos vehículos del entorno. Gracias a esta nueva forma de creación de evidencias se obtiene una descripción de la realidad tal y como la observaron los vehículos cercanos, que actúan como testigos. De esta manera, se evita que los datos de la evidencia provengan de los sensores del propio vehículo, que podrían ser maliciosamente modificados según los intereses de su propietario. El protocolo propuesto sólo requiere de dos transferencias de información (solicitud y respuestas), lo cual resulta clave para su idoneidad en este escenario.

Además de este protocolo de creación, se ha descrito el correspondiente protocolo de verificación de la evidencia. El análisis de seguridad sobre la propuesta ha mostrado que se satisfacen las propiedades adecuadas para el contexto de utilización del protocolo. Se han detectado, sin embargo, algunas carencias de seguridad derivadas del comportamiento potencialmente deshonesto de los testigos participantes. El trabajo futuro estará centrado, en primer lugar, en incorporar mecanismos frente a los problemas detectados. Igualmente, está previsto incluir mecanismos basados en incentivos para fomentar la participación, de forma que las solicitudes estén condicionadas a la satisfacción de un cierto pago. Así, se pueden diseñar pagos positivos a aquellos testigos que ofrezcan un testimonio valioso. Igualmente, los pagos negativos pueden servir para evitar testimonios deshonestos. Esta medida puede extenderse también a la labor de los intermediarios. Por otro lado, se pretende incorporar un mecanismo de agregación que permita reducir el número de respuestas (testimonios) que recibe el solicitante, garantizando al mismo tiempo la seguridad de la información en juego.

Agradecimientos

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

Referencias

1. DIRECCIÓN GENERAL DE TRÁFICO (España), *"Accidentes mortales en carretera. Año 2008"*, Observatorio Nacional de Seguridad Vial, 2009.
2. *IEEE Trial-Use Std. for Wireless Access in Vehicular Environments. Security Services for Applications and Management Messages* (1609.2). IEEE CS, 2006.
3. CANO, J.J., "Introducción a la informática forense". En: *Revista Asociación Colombiana de Ing. de Sistemas (ACIS)*.2006, núm. 96, pp. 64-73.
4. LÓPEZ-SILVES, A., *"Las evidencias electrónicas"*, TyD Consultores, [s.f.].
5. LLANEZA, P.; LÁZARO, F., "Evidencias electrónicas: de la información a la prueba electrónica". En: *Rev. Seg. en Informática y Com. (SIC)*,2009, núm. 83, pp. 92-97.
6. XU, W. *et al.*, "The feasibility of launching and detecting jamming attacks in wireless networks". En: *Proc. MobiHoc'05*,ACM, 2005.
7. WOLF, M.; WEIMERSKIRCH, A.; PAAR, C., "Security in automotive bus systems". En: *Proc. 2nd Workshop on Embedded Security in Cars (ESCAR)*, 2004.
8. KARGL, F. *et al.*, "Secure vehicular communication systems: implementation, performance, and research challenges". En: *IEEE Communications*, 2008, v. 46, n. 11.
9. GOLLE, P.; GREEN, D.; STADDON, J., "Detecting and correcting malicious data in VANETs". En: *Proc. 1st ACM Intl. Workshop on VANETs*. 2004, pp.29-37.
10. PAPADIMITRATOS, P. *et al.*, "Architecture for Secure and Private Vehicular Communications", En: *Proc. 7th Intl. Conf. on ITS*, 2007, pp.1-6.
11. NAI-WEI, L.; HSIAO-CHIEN, T., "Illusion Attack on VANET Applications. A Message Plausibility Problem".En: *Globecom Workshops*, IEEE CS, 2007, pp. 1-8.
12. WEX, P. *et al.*, "Trust Issues for Vehicular Ad Hoc Networks". En: *Vehicular Technology Conf.*, 2008. IEEE CS, pp. 2800-2804.
13. RAYA, M. *et al.*, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks". En: *INFOCOM 2008. 27th Conf. on Computer Comm.*. IEEE CS, 2008.
14. RAYA, M.; PAPADIMITRATOS, P.; HUBAUX, J.-P., "Securing vehicular communications". En: *Wireless Comm.*, IEEE CS. 2006, vol.13, núm.5, pp.8-15.
15. BUTTYÁN, L.; HUBAUX, J.-P., *"Security and cooperation in wireless networks"*, Cambridge University Press, 2007.
16. RAYA, M.; HUBAUX, J.-P., "Security aspects of inter-vehicle communications". En: *Proc. 5th. Swiss Transport Research Conf.*, 2005.
17. RAHMAN, S.U.; HENGARTNER, U., "Secure crash reporting in vehicular Ad hoc networks". En: *Proc. 3rd Intl. Conf. on Security and Privacy in Comm. Networks*. IEEE CS, 2007, pp.443-452.
18. YOUNG, C-P.; CHANG, B.; LIN, J-J.; FANG, R-Y., "Cooperative collision warning based highway vehicle accident reconstruction". En: *Proc. 8th Intl. Conf. on Intelligent Systems Design and Applications*,2008.
19. LIN, X.; SUN, X.; HO, P-H.; SHEN, X., "GSIS: A secure and privacy-preserving protocol for vehicular communications". En: *IEEE Transactions on vehicular technology*, vol. 56, núm. 6, Noviembre 2007.
20. RAYA, M.; AZIZ,A.; HUBAUX, J.-P., "Efficient secure aggregation in VANETs". En: *Proc. 3rd Intl. workshop on VANETs*. 2006. pp.67-75.