Comunicaciones Privadas en Redes Ad-hoc Vehiculares

Alexandre Viejo, Francesc Sebé, Josep Domingo-Ferrer y Jesus Manjón

Departament d'Enginyeria Informàtica i Matemàtiques

Cátedra UNESCO de Privacidad de Datos

Universitat Rovira i Virgili

Av. Països Catalans, 26, Tarragona

{alexandre.viejo, francesc.sebe,josep.domingo,jesus.manjon}@urv.cat

Resumen

Presentamos un nuevo sistema que proporciona servicios a vehículos y permite comunicaciones coche-a-coche en redes ad-hoc formadas por vehículos (VANETs). Nuestra propuesta proporciona seguridad y privacidad a las comunicaciones siempre y cuando las señales de tráfico que utilizamos en el sistema sean de confianza. Dichas señales están facultadas para revocar identificadores y alertar a la red sobre usuarios que intentan enviar mensajes falsos para crear confusión y problemas. Nuestra propuesta mejora el estado del arte proporcionando privacidad a los usuarios que acceden a los proveedores de servicios. Además, aportamos un mecanismo para actualizar de forma segura los pseudónimos de los usuarios. Dicho mecanismo evita la necesidad de almacenar una serie de pseudónimos precalculados.

1. Introducción

Las redes ad-hoc móviles (MANETs) son una tecnología prometedora y emergente que permite el desarrollo de nuevas aplicaciones descentralizadas. Una MANET está formada por nodos móviles que se conectan entre sí de forma autoorganizada y sin infraestructuras preestablecidas.

Cuando los nodos móviles son vehículos (*e.g* coches, motos...), dicha MANET pasa a considerarse una red ad-hoc vehicular (VANET). En este caso, los nodos se mueven a altas velocidades. Además, el número de nodos que participan en la red es normalmente muy elevado. En consecuencia, las VANETs tiene que soportar una gran cantidad de nodos entrando y saliendo de la red.

Existe una gran cantidad de aplicaciones para las VANETs. Una de las más importantes es la posibilidad de diseminar mensajes de alerta para aquellos vehículos que pueden encontrarse con accidentes o situaciones peligrosas en general (*e.g* niebla, obstáculos...). Otras aplicaciones interesantes incluyen obtener información útil para los conductores como restaurantes cercanos, hoteles o estaciones de servicio. Además, pueden proporcionar diversión en forma de Internet, descargas de contenido multimedia o chat entre vehículos.

El uso de algunas de estas aplicaciones puede implicar la necesidad de autenticar a los vehículos. Este proceso debe realizarse de forma segura para evitar que posibles intrusos puedan dañar la red. Adicionalmente, el sistema debe preservar los derechos básicos en cuanto a privacidad. Esto significa que los protocolos de comunicación en uso deben proteger la privacidad de los usuarios. En particular, un adversario debe ser incapaz de obtener el patrón de movimiento de un usuario concreto.

Diseñar protocolos que proporcionen autenticación de usuarios preservando su privacidad es una tarea complicada y desafiante que merece esfuerzo de investigación.

Por último, hay que tener en cuenta que las propuestas exitosas en cuanto a seguridad y privacidad aplicadas a VANETs, no deben

depender de autoridades centralizadas o infraestructuras fijas. No obstante sí se puede suponer la existencia de ordenadores potentes y con suficiente energía en los vehículos.

En cualquier caso, la conexión a una autoridad central sí es realista en ciertas situaciones como la revisión periódica del vehículo.

1.1. Estado de la técnica

La privacidad en redes ad-hoc es una meta complicada de conseguir. En este tipo de redes los usuarios finales requieren servicios y envían información personal (*e.g.* identificadores, preferencias, etc.) a través de nodos que actúan normalmente como enrutadores y ocasionalmente como proveedores de servicios. Estos nodos no son de confianza y pueden comprometer la privacidad de los usuarios, analizando la información que estos reenvían a terceras personas. Este comportamiento permite a los intrusos acumular información de diversas fuentes e inferir información importante sobre un usuario específico. En redes móviles (MANETs o VANETs), este problema es incluso mayor. En este caso es posible rastrear los movimientos de un cierto usuario, lo cual implica conocimiento de los hábitos privados de dicho usuario.

Garantizar la privacidad de los usuarios a veces entra en conflicto con los requisitos de seguridad. Por ejemplo, un sistema que ofrece servicios requiere que los usuarios se autentifiquen para asegurar el correcto pago por dichos servicios. Otro ejemplo ocurre cuando un cierto usuario se comporta de forma inadecuada en la red. El sistema debe ser capaz de identificar a dicho usuario para poder tomar medidas contra él. Las medidas que adoptemos para regular estas situaciones pueden afectar la privacidad de los usuarios. En [8] los autores proponen que todos los nodos que participan en la red se registren. Esta solución viola por completo las normas de privacidad. En [10] los autores presentan un protocolo que permite a los nodos de una MANET reconocerse cuando se encuentran de nuevo. Este esquema proporciona autenticación segura contra atacantes pasivos. El problema es que permite a los usuarios cambiar libremente su identidad, con lo que no es un protocolo válido para para MANETs seguras.

Las VANETs son un caso especial de MANETs y tienen requisitos similares. Existen algunos proyectos de investigación relacionados con VANETs: Carisma [7], FleetNet [5] y Vehicle Safety Communications (VSC) [9], entre otros. No obstante, solamente el proyecto VSC proporciona seguridad, pero considera la privacidad como un problema menor. En [6], los autores ofrecen una visión general en cuanto a seguridad y privacidad en VANETs.

En [4] se encuentra un resumen reciente de amenazas a la privacidad que deben ser tratadas al trabajar con VANETs. Este trabajo realizado por un investigador de BMW da la lista de requisitos para obtener privacidad en este entorno. El autor proporciona unos primeros pasos hacia una solución global. Su propuesta se basa en que cada coche debe mantener una lista de pseudónimos que pueden ser mapeados a una identidad real en situaciones especiales. El pseudónimo en uso debe cambiar periódicamente para evitar ser traceado. No obstante, el autor reconoce que un observador que siga a un cierto vehículo durante suficiente tiempo podrá relacionar los diferentes pseudónimos inutilizando así el intento de anonimización. Aunque el autor proporciona ciertas contramedidas contra este comportamiento, el problema continua abierto.

Otro problema detectado en esta propuesta es la presencia de proveedores de servicios que son capaces de mapear pseudónimos a identidades reales. Esto se hace para que un usuario con ciertos derechos pueda acceder a determinados servicios o enviar determinados mensajes. En consecuencia, sólo los nodos relacionados con dichos proveedores pueden conocer la identidad de los usuarios mientras que el resto de nodos de la red no será capaz de tracear a un determinado usuario. No obstante, consideramos que garantizar la honestidad de los proveedores es difícil sino imposible en entornos reales. Además, y aunque sea un problema menor, esta propuesta requiere una gran cantidad de pseudónimos. Este punto debe ser solucionado también.

1.2. Contribución y estructura del artículo

Presentamos un esquema que proporciona servicios a vehículos y comunicaciones en VANETs. Estas comunicaciones implican la transmisión de mensajes para una amplia lista de receptores (uno-a-muchos) o para un único receptor (vehículo-a-vehículo).

Un usuario que utilice nuestro sistema de comunicación necesita un pseudónimo válido, firmado por la autoridad de tráfico. Si un usuario se comporta de forma dañina, su pseudónimo queda marcado como 'revocado' y sus mensajes pierden toda credibilidad. Un usuario debe cambiar frecuentemente su pseudónimo para evitar ser traceado por terceras personas. Dichos pseudónimos no pueden ser mapeados a identidades reales.

Nuestra propuesta proporciona comunicaciones seguras y privacidad mientras las señales de tráfico utilizadas sean de confianza. Dichas señales pueden revocar pseudónimos y avisar a la red sobre malos comportamientos. Nuestro esquema mejora la propuesta presentada en [4], ofreciendo privacidad a los usuarios que acceden a los proveedores de servicios. Además solucionamos la necesidad de grandes cantidades de pseudónimos introduciendo la actualización dinámica de pseudónimos. Por último, mientras las señales no se vean comprometidas, nuestra propuesta evita que intrusos puedan tracear las localizaciones de los usuarios.

La Sección 2 describe el nuevo esquema y cómo la privacidad y la seguridad se consigue en este escenario. Las conclusiones y el trabajo futuro se resumen en la Sección 3.

2. Nuestra propuesta

Nuestro escenario supone una VANET formada por: i) varias señales de tráfico instaladas en una cierta área; ii) los coches que viajan por el área cubierta con la red. Las señales de tráfico se consideran nodos estáticos en la VANET y son gestionadas por la autoridad de tráfico (la DGT). Consideramos que las señales son nodos de confianza, lo que implica que no guardan información relacionada con los usuarios ni realizan ninguna actividad dañina para la red. Cada señal guarda en un dispositivo a prueba de manipulación la clave privada utilizada por la autoridad de tráfico (SK_t). La clave pública asociada es conocida y aceptada como válida por todos los nodos.

Cada vehículo esta equipado con un dispositivo a prueba de manipulación (similar a una tarjeta inteligente) que no puede ser desinstalado del vehículo. Este dispositivo proporciona memoria segura y computación segura. Su cometido es que el usuario no pueda manipular el identificador del vehículo.

Nuestra propuesta abraza dos tipos de aplicaciones en VANETs: *transmisión de mensajes* y *provisión de servicios*.

2.1. Transmisión de mensajes

Los nodos participantes en una VANET pueden enviar una gran variedad de mensajes a otros nodos utilizando dos paradigmas diferentes: vehículo-a-vehículo o uno-a-todos (un vehículo o una señal de tráfico hacen broadcast de un cierto mensaje).

Existen dos tipos de mensaje asociados al paradigma vehículo-a-vehículo:

- Comunicaciones privadas entre dos usuarios específicos. Proporcionamos seguridad a estas transmisiones estableciendo una clave de sesión entre las dos partes. Para ello utilizamos el protocolo Diffie-Hellman [2] (o su versión autenticada [3]).
- Mensajes de alerta que son relevantes para un único receptor. Por ejemplo, un vehículo frena de repente y avisa al coche situado detrás de él para evitar una colisión. Este tipo de transmisión sólo requiere autenticación de la fuente. No se requiere confidencialidad.

Los mensajes uno-a-todos incluyen alertas sobre accidentes o otra información útil para los conductores. Las señales de tráfico utilizan este tipo de comunicación para informar a toda la red sobre un usuario deshonesto. Además, todos los vehículos utilizan *broadcast* periódicamente para intercambiar mensajes llamados *hello_beacons*, que contienen

información correspondiente a la gestión de la propia red. Este tipo de mensajes son esenciales para conocer la existencia de nodos activos en la VANET.

Todos los mensajes enviados por las señales de tráfico vía *broadcast* son de confianza (están correctamente firmados) y no llevan pseudónimo.

En referencia a los pseudónimos utilizados por los vehículos, un pseudónimo Id_{node} contiene un valor aleatorio v, un sello temporal que indica el momento en se generó dicho pseudónimo y las dos claves públicas del nodo (PK^s_{node}, PK^e_{node}) utilizadas para firmar y cifrar, respectivamente. Un pseudónimo más viejo que un cierto tiempo preestablecido (*e.g.* un día) es considerado como inválido. Finalmente, un pseudónimo debe estar firmado con SK_t para ser válido:

$$Id_{node} \leftarrow$$

$$\{v||timestamp||PK_{s,node}||PK_{e,node}\}_{SK_t}$$

La tarjeta inteligente del vehículo contiene su Id_{node} actual y las claves secretas $SK_{s,node}$, $SK_{e,node}$.

Cualquier mensaje *hello_beacon* enviado por un coche contiene su pseudónimo, su posición (coordenadas GPS) y ciertos datos, todo ello firmado con $SK_{s,node}$:

$$hello\_beacon \leftarrow$$

$$\{Id_{node}, posicion, timestamp, datos\}_{SK_{s,node}}$$

Un mensaje enviado vía broadcast por un usuario es válido si Id_{node} es un pseudónimo válido, la firma con $SK_{s,node}$ es correcta e Id_{node} no ha sido marcado como 'revocado'.

2.1.1. Obtención de un pseudónimo

Si una señal de tráfico recibe un *hello_beacon* que posee un Id_{node} que ha expirado (sello temporal caducado), la señal insta a dicho nodo a actualizar su pseudónimo.

El procedimiento es el siguiente:

1. El nodo genera dos parejas de claves:

   $$(SK'_{s,node}, PK'_{s,node})$$

   $$(SK'_{e,node}, PK'_{e,node})$$

2. El nodo genera un nuevo

   $$Id' \leftarrow$$

   $$\{v'||timestamp'||PK'_{s,node}||PK'_{e,node}\}_{SK_{s,node}}$$

   (Destacamos que el nuevo valor aleatorio, el nuevo sello temporal y la nueva clave pública se firman con la clave secreta antigua del propio nodo).

3. El nodo envía el siguiente mensaje cifrado a la señal de tráfico

   $$\{Id_{node}||Id'\}_{PK_t}$$

4. La señal de tráfico descifra el mensaje, verifica su contenido (en particular se asegura que Id_{node} no ha sido revocado por un mal comportamiento anterior) y genera el mensaje firmado:

   $$Id'_{node} \leftarrow$$

   $$\{v'||timestamp'||PK'_{s,node}||PK'_{e,node}\}_{SK_t}$$

5. Id'_{node} es enviado al vehículo cifrado bajo $PK'_{e,node}$

6. El vehículo descifra el mensaje y obtiene su nuevo pseudónimo Id'_{node}.

Cada coche producido en la fábrica recibe un identificador inicial. Dicho identificador viene firmado con SK_t pero no es un pseudónimo válido. El identificador inicial será reemplazado por uno válido la primera vez que el coche contacte con una señal de tráfico.

Podría suceder que un coche que necesite obtener un nuevo pseudónimo no pueda acceder a ninguna señal de tráfico. En este caso, la única posibilidad es esperar hasta encontrar una. No obstante, esta situación es difícil que se dé.

2.1.2. *Broadcast* de mensajes coche-a-todos

Un usuario que quiere enviar una alerta a la red selecciona el mensaje a enviar, concatena el sello temporal y su pseudónimo y firma el mensaje entero utilizando su clave privada.

Un posible ejemplo de esta situación se daría cuando un coche, atrapado en un atasco, alerta a los coches cercanos sobre esta situación.

Al recibir el mensaje, los otros coches verifican la validez del pseudónimo. El mensaje se considera válido si el pseudónimo no ha sido revocado.

Las señales de tráfico tienen dos maneras de decidir si un usuario es deshonesto o no:

1. Se considera que un mensaje es falso si hay al menos i (parámetro de seguridad) mensajes de diferentes usuarios informando que un cierto mensaje es falso.

2. La segunda opción se basa en la posibilidad de que las señales de tráfico reciban información directamente de la autoridad de tráfico sobre situaciones peligrosas en la carretera. Un usuario que envíe información contradictoria con la fuente oficial será considerado como deshonesto.

Una vez una señal detecta a un usuario deshonesto, notifica a toda la red dicha situación mediante *broadcast*.

2.1.3. Transmisión de mensajes vehículo-a-vehículo

Este tipo de transmisión se utiliza para establecer comunicaciones seguras entre vehículos. Un coche que recibe un *hello_beacon* de otro coche puede solicitar un enlace seguro con la otra parte. Los dos coches intercambian sus pseudónimos y construyen un secreto compartido utilizando el protocolo Diffie-Hellman (o su versión autenticada).

Además, este paradigma de comunicación se utiliza también cuando un coche desea avisar a otro sobre una determinada situación que solamente le afecta a él. La Figura 1 muestra un ejemplo de esta situación donde un coche frena de repente y avisa al coche situado detrás. En este caso la confidencialidad no es necesaria, con lo que la fuente envía el mensaje firmado pero sin cifrar. Este proceso proporciona autenticación y evita que usuarios deshonestos envíen mensajes falsos.

Figura 1: Ejemplo de una transmisión vehículo-a-vehículo

2.2. Provisión de servicios

Las VANETs ofrecer ciertos servicios a los usuarios como peajes electrónicos, acceso a Internet o repostado en gasolineras. Estos servicios requieren un pago por parte del usuario pero no su autenticación. Por tanto, debemos proporcionar un sistema de pago seguro que no revele la identidad del usuario.

Para ello, proponemos el uso de los cheques electrónicos en su modalidad fuera de línea presentada en [1]. Este esquema proporciona privacidad perfecta a los usuarios honestos mientras que permite al proveedor de servicios verificar inmediatamente si un cheque es válido o no. Si un usuario intenta gastar más de una vez el mismo cheque, el sistema es capaz de obtener la identidad real del usuario y aplicar las medidas oportunas.

3. Conclusiones y trabajo futuro

En este trabajo hemos presentado un nuevo esquema que preserva la privacidad de los usuarios de VANETs mientras las señales de tráfico utilizadas se mantengan seguras y sean de confianza.

Nuestra propuesta consigue su objetivo sin comprometer las funcionalidades de la red y mejora las propuestas actuales presentes en la literatura. Específicamente, nuestro esquema proporciona comunicación vehículo-a-vehículo, acceso privado a proveedores de servicios y actualización privada de pseudónimos.

En el futuro mejoraremos este esquema para obtener seguridad y privacidad en escenarios con señales de tráfico deshonestas.

Descargo y agradecimientos

Los autores son responsables de las ideas expresadas en este artículo, que no reflejan necesariamente la posición de la UNESCO ni comprometen a dicha organización. Este trabajo ha sido financiado en parte por el Ministerio

de Educación y Ciencia a través del proyecto SEG2004-04352-C04-01 "PROPRIETAS" y por la Generalitat de Catalunya mediante la ayuda 2005 SGR 00446. Agradecemos a Agusti Solanas sus comentarios sobre un borrador de este artículo.

Referencias

[1] D. Chaum, B. Den Boer, E. Van Heyst, S. Mjolsnes and A. Steenbeek, *Efficient offline electronic checks (extended abstract)*, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Springer-Verlag, 1990.

[2] W. Diffie, M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, vol. 22(6), pp. 644-654, 1979.

[3] W. Diffie, P.C. van Oorschot, M.J. Wiener, *Authentication and authenticated key exchanges*, Designs, Codes and Cryptography, vol. 2, pp. 107-125, 1992.

[4] F. Dötzer, *Privacy issues in vehicular ad hoc networks*, Privacy Enhancing Technologies-PET'2005, Lecture Notes in Computer Science, vol. 3856, pp. 197-209, 2006.

[5] W. Franz, R. Eberhardt and T. Luckenbach, *Fleetnet - internet on the road*, Proceedings of the 8th World Congress on Intelligent Transportation Systems, 2001.

[6] J.P. Hubaux, S. Capkun and J. Luo, *Security and privacy of smart vehicles*, IEEE Security & Privacy, pp. 49-55, 2004.

[7] T. Kosch, *Local danger warning based on vehicle ad-hoc networks: Prototype and simulation*, Proceedings of 1st International Workshop on Intelligent Transportation, 2004.

[8] J. Newsome, E. Shi, D. Song and A. Perrig, *The Sybil attack in sensor networks: analysis & defenses*, Proceedings of the third international symposium on Information processing in sensor networks, ACM Press, pp. 259-268, 2004.

[9] Vehicle Safety Communications Consortium, *Vehicle Safety Communications (VSC) Project.* `http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm`

[10] A. Weimerskirch and D. Westhoff, *Zero common-knowledge authentication for pervasive networks*, Selected Areas in Cryptography, pp. 73-87, 2003.