Gestión del riesgo inherente en la revocación de certificados de redes vehiculares

Carlos Gañán*, Jose L. Muñoz*, Francisca Hinarejos†, Andreu Isern† and Juanjo Alins*
*Universitat Politècnica de Catalunya (UPC) † Universitat de les Illes Balears (UIB)
{carlos.ganan,jlmunoz,juanjo}@entel.upc.edu {xisca.hinarejos,andreupere.isern}@uib.es

***Resumen*—Las redes vehiculares requieren de algún mecanismo para autenticar los mensajes, identificar a los vehículos legítimos y sacar de la red aquéllos que no presenten un comportamiento adecuado. La infrastructura de clave pública (PKI) puede proporcionar estos requisitos mediante el uso de certificados digitales. Sin embargo, la adopción de una PKI, conlleva la necesidad de gestionar no tan sólo la emisión de certificados sino también su revocación. El estándar IEEE 1609.2 apunta que la revocación de certificados en redes vehiculares debe depender del uso de Listas de Certificados Revocados (CRLs). En este artículo, analizamos los problemas derivados del uso de CRLs en este tipo de redes. Asimismo, proponemos un mecanismo para gestionar el riesgo inherente del uso de estas listas el cual mejora el uso tradicional de las CRLs. Ayudándose del canal de control de este tipo de redes, nuestro mecanismo es capaz de dar a conocer la frescura de los datos de revocación en tiempo real. Además, este mecanismo permite a los usuarios estimar el riesgo operacional que asumen al usar las CRLs.**

***Index Terms*—VANET, PKI, Revocation, Risk.**

I. Introducción

Durante la pasada década, las comunicaciones inalámbricas entre vehículos han captado la atención de la industria y de la comunidad científica por su potencial capacidad de contribuir en hacer más segura y cómoda la conducción. Este tipo de comunicaciones han estimulado la aparición de redes *ad hoc* entre vehículos, las llamadas VANETs. Las VANETs están formadas por nodos móviles capaces de comunicarse entre ellos (i.e. Comunicaciones Vehículo a Vehículo -V2V-) y con la infraestructura (i.e. Comunicaciones Vehículo a Infraestructura -V2I-). Para hacer este tipo de comunicaciones factible, los vehículos se equipan con unidad a bordo (OBUs) y a lo largo de la carretera se sitúan unidades fijas (RSUs). Mediante la tecnología inalámbrica de corto alcance basada en el estándar IEEE 802.11, se posibilita el uso de comunicaciones multisalto que permiten el intercambio de información entre los nodos de la red que no se encuentran en alcance directo [1].

Sin embargo, la propia naturaleza de estas redes junto con la alta movilidad de una gran cantidad de vehículos hacen necesaria la integración de medidas de seguridad primordiales tales como la autenticación, la integridad del mensaje, el no repudio, y la privacidad [2]. Sin seguridad, todos los usuarios serían potencialmente vulnerables al funcionamiento fraudulento de los servicios proporcionados por la VANET. De esta forma, es necesario expulsar de la red a los nodos que se ven comprometidos, defectuosos y/o ilegítimos. La solución básica para proporcionar estos requisitos es el uso de certificados digitales vinculados al usuario por un tercera parte de confianza. Estos certificados se pueden usar para firmar información. La mayoría de las soluciones existentes gestionan estos certificados mediante una Autoridad de Certificación (CA) [3]. De acuerdo con el estándar IEEE 1609.2 [4], la redes de vehículos dependerán de una infraestructura de clave pública (PKI). En una PKI, la CA emite certificados digitales autenticados para cada nodo de la red. Así, una gestion eficiente de estos certificados es crucial para un funcionamiento robusto y fiable de la PKI. Una parte crítica de cualquier esquema que gestione certificados digitales es la revocación de los mismos. En este sentido, el estándar plantea el uso de listas de certificados revocados (CRLs) y certificados de corta vida para proporcionar el servicio de revocación. Las CRLs se pueden ver como listas negras que enumeran qué certificados están revocados junto con la fecha de revocación y, opcionalmente, las razones por las cuales fueron revocados.

Dado que se espera que el tamaño de la VANETs crezca de manera exponencial y que para proporcionar privacidad cada vehículo dispondrá de una gran número de certificados temporales (llamados seudónimos), las CRLs serán de gran tamaño. Así, la distribución de las CRLs estará sujeta a grande retardos. Además, durante el despliegue inicial de estas redes, las RSUs no estarán uniformemente distribuidas lo que dificultará el acceso a las autoridades de confianza. Por ello, la manera en que las CRLs se distribuyen debe de ser mejorada para asegurar que la revocación se lleva a cabo en estos entorno propenso a retardos. Ya se han propuesto diversos mecanismos para mejorar la distribución de CRLs en estas redes (e.g. [3], [5]). Estas propuestas intentan hacer más eficiente la distribución de estas listas, ya sea mediante la reducción de su tamaño o mediante el uso de comunicaciones V2V. Sin embargo, ninguna de estas propuestas trata el problema de la falta de información sobre certificados que han sido revocados durante el intervalo de validez de la CRL.

En este contexto, cada CRL contiene un gran número de certificados revocados que difiere significativamente de la CRL emitida previamente. El número de nuevos certificados revocados variará dependiendo del tiempo que haya transcurrido desde la publicación de la última CRL. Estos nuevos certificados revocados son desconocidos al usuario (en parte) durante el intervalo de validez de la CRL actual y (en su totalidad) durante el tiempo que se esté operando con una CRL desactualizada ya sea porque no hay conexión con la infraestructura o porque todavía no ha sido de bajarse la nueva CRL debido a su gran tamaño. Durante estos periodos, un vehículo podría estar operando con otra entidad cuyo certificado ha sido revocado sin ser consciente de ello. Es en estas situaciones, cualquier usuario está asumiendo cierto riesgo de operar con un certificado revocado.

En este artículo, proponemos un mecanismo para dar a conocer este riesgo a cada usuario. La idea principal consiste

en aprovecharse del canal de control de las VANETs para comunicar de forma periódica este riesgo. Así cada usuario, dependiendo de su actitud de cara al riesgo podrá decidir si opera o no durante los intervalos en los que la información de revocación está desactualizada. De esta manera, sin incrementar el overhead en las comunicaciones, somos capaces de enviar información muy valiosa para los usuarios de la red acerca del servicio de revocación.

II. Problemas derivados del uso de CRLs en VANETs

Cuando una autoridad de certificación (CA) invalida el certificado de un determinado vehículo, ésta debe incluir el número de serie del certificado en cuestión en la CRL. Una vez hecho esto, la CA distribuye la CRL de manera que los vehículos de la red puedan identificar y desconfiar del vehículo cuyo certificado a sido revocado. La distribución debería llevarse a cabo de forma rápida y eficiente, de manera que todos los vehículos sean conscientes de los certificados revocados en todo momento.

Sin embargo, la distribución de la CRL por sí misma ya presenta un serio desafío debido a su gran tamaño. Dado que la CRL es una lista que contiene los números de serie de todos los certificados emitidos por una determinada CA que han sido revocados y no han expirado todavía, su distribución causa una gran sobrecarga a la red. Además, el tamaño de la CRL aumenta de manera espectacular con que una porción pequeña de OBUs se revoquen, ya que cada uno gestiona un gran número de certificados temporales. Para tener una idea de cómo de grande una CRL en estas redes puede llegar a ser, considerad el caso donde un 1 % del total de OBUs en los Estados Unidos son revocados. Recordad que en una VANET, cada vehículo no sólo dispone de un único certificado de identidad, sino también de decenas de seudónimos (certificados temporales). El número de seudónimos puede variar dependiendo del grado de privacidad y anonimato que se pretenda conseguir. De acuerdo con los autores en [6], una OBU debe disponer de suficientes seudónimos para poder cambiar de seudónimo cada minuto mientras se conduce. Esto da lugar a unos 43,000 seudónimos por año, suponiendo una media de dos horas de conducción diaria. Sólo en los EE.UU., habían más de 255 millones de vehículos registrados en el 2008, de los cuales más de 137 millones era de pasajeros [7]. En este caso, la CRL contendría alrededor de 100 billones de certificados revocados. Asumiendo que los certificados pueden ser identificados por un número de serie de 16 bytes (el tamaño de un bloque AES), el tamaño de la CRL sería de 1,7 TB aproximadamente. Sólo la cantidad de memoria necesaria para almacenar esta CRL haría imposible el despliegue del servicio de revocación. Es por ello, que el tamaño de la CRL debe reducirse.

El tamaño de la CRL puede reducirse usando CAs regionales, las cuales en vez de gestionar toda la CRL gestionan partes de la misma según determinadas regiones geográficas. En estos casos aparece un compromiso entre el tamaño de la región geográfica que gestiona la CA y el tamaño de la CRL, al mismo tiempo que aumenta la complejidad de gestión de la PKI a nivel global. Lo que supondría menor complejidad de gestión sería tener una única región, como sería todo el país de los EE.UU, con una única CA responsable de cada certificado y de cada seudónimo. Sin embargo, una única región da lugar a CRLs de varios terabytes. Por lo tanto, es necesario dividir la información de la CRL en función de diferentes áreas regionales. Siguiendo con nuestro ejemplo de los EE.UU., si la CRL se divide por ciudades (i.e., 10,015 ciudades conforme el la oficina de censo americana), el tamaño de la CRL se reduce a unos 170 Mbytes.

Usando el protocolo 802.11a para comunicarles con las RSU en el radio de alcance, los vehículos podrían obtener un throughput de entre 10-30 Mbps dependiendo de su velocidad y de la congestión de la carretera [8]. Por lo tanto, en el mejor de los casos, un vehículo tardaría más de 45 segundos en bajarse la parte de CRL correspondiente a la región en la que se encuentra. Bajo condiciones de no congestión, cualquier vehículo debería ser capaz de tener conexión con la infraestructura durante más de 45 segundos, y, por lo tanto, de descargarse la CRL. En escenarios donde los vehículos no fuesen capaces de mantener un enlace permanente con la infraestructura durante esta cantidad de tiempo, técnica tales como filtros de Bloom o códigos de fuente digital pueden ser usadas para obtener la información de revocación. Así, aunque el problema de tener CRLs de enorme tamaño se mitiga mediante el uso de tales técnicas, las restricciones que impone en la distribución afectan a la frescura de la información de revocación.

El hecho de necesitar un tiempo considerable para descargarse la CRL acarrea que estas listas no puedan ser emitidas muy frecuentemente, por lo que su intervalo de validez debe ser acortado. Este intervalo de validez determina directamente la frecuencia con la que un vehículo debe actualizar la información de revocación. Por lo tanto, este intervalo es crítico e impacta en el consumo de ancho de banda. En este contexto, aparece otro compromiso entre la frescura de la información de revocación, y el ancho de banda consumido para descargar las CRLs. Periodos de validez largos disminuyen la sobrecarga de la red a costa de tener información de revocación desactualizada. Por contra, periodos de validez cortos aumentan la sobrecarga de la red, pero los usuarios disponen de información fresca acerca de los certificados revocados. Dado que las CRLs no pueden ser emitidas cada vez que un nuevo certificado es revocado, los vehículos tienen que operar con información de revocación que no siempre es completa (de hecho la mayor parte del tiempo no lo es). Consiguientemente, los usuarios asumen cierto riesgo cuando confían en que un certificado que no está en el CRL que tienen no está revocado.

III. Mecanismo para la gestión del riesgo inherente en la revocación de certificados

En la sección anterior hemos mostrado que el enorme tamaño de las CRLs en las VANETs fuerza a aumentar el intervalo de emisión de las mismas. Tradicionalmente, las CRLs se emiten de forma periódica. La forma típica de asegurar la frescura de los datos es mediante el uso de sellos temporales. De hecho, las CRLs siempre incluyen un par de sello temporales:

- `thisUpdate`: instante en el cual se emitió la CRL,
- `nextUpdate`: instante en el que se emitirá la próxima CRL.

Así, si `nextUpdate-thisUpdate = 1 hour` significa que una nueva CRL se emite cada hora, siendo éste su intervalo

de emisión. Obviamente, el intervalo de emisión debe ser más corto que el periodo de validez medio de los certificados. De esta forma, las OBUs almacenan en su cache la CRL durante el periodo de validez de la misma, y resuelven las peticiones de estado de los certificados de manera local. Cuando la CRL expira (`currentTime = nextUpdate`), las OBUs deben contactar con la CA (o con alguna entidad de la red que posea la información de revocación emitida por la CA) para actualizar la información de revocación.

El problema en las VANETs es que las CRLs no pueden emitirse muy a menudo con tal de evitar una sobrecarga en la red excesiva. Es por ello, que las VANETs solo pueden ser securizadas hasta cierto punto. Los usuarios dentro de la red vehicular tienen que lidiar con un cierto grado de inseguridad que no puede ser eliminado totalmente. En este contexto, se debe estimar el nivel de seguridad en relación a una potencial amenaza. Esta inseguridad siempre existirá y es inherente a la infraestructura de clave pública global. Además, en las VANETs está inseguridad es incluso mayor no por su gran escalar sino también por las restricciones en la emisión de la CRL. La seguridad total es inalcanzable, incluso bajo la hipótesis quimérica de que la información de revocación pudiese ser distribuida de forma instantánea a todo el mundo. Una clave privada podría haber sido comprometida mucho antes de que este hecho sea conocido y el correspondiente certificado fuese revocado. Esto no puede ser gestionado por los esquemas de revocación tradicionales, pero debe de ser tenido en cuenta cuando se analiza el riesgo inherente de la PKI.

En este contexto, proponemos un mecanismo que es capaz de gestionar este riesgo inherente a la información de revocación y de comunicárselo a los usuario de la red vehicular. Este mecanismo puede entenderse como un mecanismo para el control del riesgo. Tradicionalmente, se asume implícitamente que todo los vehículos deberían obtener la CRL más reciente. Sin embargo, en las VANETs esto puede ser altamente ineficiente dado el tamaño de las CRLs. En su lugar, los usuarios (o en su defecto los programadores de las aplicaciones) deberían establecer requisitos de frescura de la información de revocación para determinar la política de actualización de las CRLs. Requisitos de frescura más estrictos darán lugar a un menor riesgo, pero incurrirán en una sobrecarga de la red alta. Por ejemplo, una aplicación de seguridad viaria debe operar con datos de revocación tan frescos como sea posible. Sin embargo, otras aplicaciones como las de entretenimiento podrían operar con riesgos más altos.

A continuación describimos las diferentes fases del mecanismo para gestionar el riesgo:

1. *Estimación del riesgo*: Durante esta fase la CA calcula el riesgo de operar con la CRL cacheada,
2. *Transmisión del riesgo*: Periódicamente, cada CA regional comunica el riesgo estimado a la correspondiente RSU, que a su vez lo difunde a los nodos vehiculares bajo su cobertura.

III-A. Risk Calculation

Como se ha comentado en la sección previa, los nodos vehiculares operan con una CRL cacheado mientras ésta es valida. En este sentido, la CA emite CRLs ligadas a dos sellos temporales:

- *thisUpdate.* Instante en el que se publicó la CRL,
- *nextUpdate.* Instante en el que una CRL actualizada se publicará.

Usando estos dos sellos temporales, los vehículos podrían intentar estimar el riesgo de operar con la CRL cacheada. Sin embargo, estos sellos temporales constituyen un criterio pobre para evaluar este riesgo. Los vehículos podrían calcular el tiempo que ha pasado desde la publicación de la CRL y compararlo con el instante en que se espera que se publique una nueva CRL. Con esta comparación, se podría obtener una idea de la frescura de la información de revocación pero no se puede inferir el riesgo de confiar como completa tal información. Dependiendo de la tasa de revocación de certificados, el riesgo después de transcurrir cierta cantidad de tiempo desde la publicación de la CRL variará. Por lo tanto, para estimar este riesgo no es suficiente con conocer el tiempo que ha transcurrido sino también la tasa de revocación. Esta tasa sólo es conocida por la CA correspondiente. Por lo tanto, la CA es la única entidad de la red que puede estimar el riesgo. Así, ésta será la encarga de estimar el riesgo y de publicarlo en cada instante.

Usando la teoría de grupos clásica y un análisis probabilístico, se puede calcular la probabilidad de considerar un certificado como válido cuando el estado real conocido por la CA en el instante t es de revocado (ver detalles en [9]):

$$\rho(t) = Prob(Cert \in \mathcal{U}) = \frac{p(t-t_0)}{(1-p)T_c + p(t-t_0)}, \qquad (1)$$

donde T_c es el tiempo de vida medio de un certificado, p es el porcentaje medio de certificados revocados y $\mathcal{U}$ es el conjunto de certificados revocados que no constaban en la CRL previa.

La figura 1 representa la evolución de $\rho(t)$ durante tres actualizaciones consecutivas de la CRL. Como era de esperar, esta probabilidad es cero en los instantes de publicación de una nueva CRL donde todos los certificados revocados por la CA son introducidos en la CRL. Por contra, esta probabilidad es máxima justo antes de publicar una nueva CRL, dado que el número de certificados revocados desconocidos es máximo en ese instante. Cabe destacar, que este máximo (así como la pendiente de la función $\rho(t)$) varía dependiendo del porcentaje de certificados revocados (p). Como se puede observar en la figura, cuando este porcentaje es mayor ($p_2 > p_3 > p_1$) esta probabilidad aumenta más rápidamente.

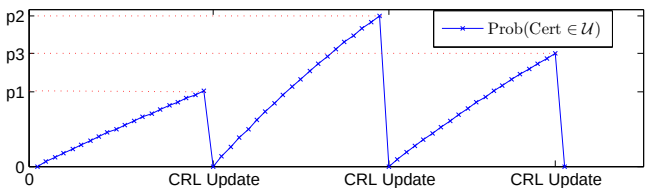

Figura 1. Evolución de la probabilidad $\rho(t)$.

Una vez calculada la función $\rho(t)$, debemos estimar la consecuencias de operar con un certificado revocado para finalmente calcular el riesgo. Estas consecuencias variarán dependiendo de la causa de revocación del certificado. Los certificados PKIX/X.509 y la especificación de la CRL define nueve causas diferentes de revocación de un certificado de clave pública (véase Tabla I).

Código	Texto	w_i	Descripción
(1)	keyCompromise	9	Clave privada comprometida
(2)	cACompromise	10	Autoridad de Certificación comprometida
(3)	affiliationChanged	1	Nombre u otra información ha cambiado
(4)	superseded	1	Certificado sobre-emitido
(5)	cessationOfOperation	2	Certificado no necesario
(6)	certificateHold	3	Certificado en espera
(7)	removeFromCRL	0	Certificado pasa de estar en espera a ser válido
(8)	privilegeWithdrawn	5	Privilegios han sido eliminados
(9)	aACompromise	10	Autoridad de atributos comprometida

Cuadro I
CÓDIGO DE REVOCACIÓN, PESOS w_i Y DESCRIPCIÓN.

Hemos definido una serie de pesos w_i para cada posible causa de revocación. Estos pesos nos permitirán dar más importancia a aquellos certificados que fueron revocados debido a un uso malicioso o a un compromiso de clave. Los valores de estos pesos son puramente intuitivos ya que hay causas de revocación que suponen una amenaza (y por tanto un riesgo) mayor para los usuarios de la VANET que otras causas. Por ejemplo, el compromiso de la clave privada de la CA es mucho más dañino y tiene consecuencias potencialmente más desastrosas que el hecho de sobre-emitir un certificado.

Para calcular el valor de las consecuencias $Q(t)$, la CA debe calcular la ratio de certificados revocados por cada causa determinada $r_i(t)$ y calcular la media ponderada. Así, el valor de las consecuencias $Q(t)$ puede expresarse como:

$$Q(t) = \frac{\sum_{i=1}^{9} w_i r_i(t)}{\sum_{i=1}^{9} w_i}. \quad (2)$$

Una vez la CA ha estimado las consecuencias de operar con los certificados que han sido revocados recientemente, ésta puede calcular el riesgo como:

$$Risk(t) = Q(t) \cdot \rho(t). \quad (3)$$

Cabe denotar que este riesgo incrementa con el paso del tiempo de la misma forma que lo hace la probabilidad de operar con un certificado revocado desconocido. Así, el riesgo será cero cuando una nueva CRL es emitida (aunque siempre existe un cierto riesgo inherente que ni la CA puede estimar) y éste crece hasta que cualquier certificado revocado conocido haya expirado. En ese instante, el riesgo alcanza su valor máximo ya que todos los certificados revocados son desconocidos.

III-B. Transmitiendo el riesgo estimado

El mecanismo para la gestión del riesgo de la información de revocación que proponemos se aprovecha de la capa física de las VANETs para transmitir el valor estimado del riesgo a los vehículos. La capa física de las VANETs se basa en el protocolo dedicado de comunicacsión de corto alcance (DSRC) [1]. DSRC dispone de una banda de 75 MHz en la frecuencia de los 5.9 GHz con siete canales que no se solapan. Dos tipos de canales diferentes se definen en DSRC. El primer tipo de canal es el canal de control, llamado CCH, el cual es un canal único reservado para mensaje cortos, de aplicaciones de alta prioridad y mensajes de control del sistema [4]. Durante la duración del CCH, cada nodo difunde una baliza que proporciona información sobre el vehículo en cuestión. El otro tipo de canal es el canal de servicio, o SCH, el cual se divide en seis subcanales diferentes de 10 MHz que dan soporte a una amplia gama de aplicaciones y de transferencia de datos. Durante los intervalos de transmisión del CCH, no se transmite nada por el SCH y vice versa.

El mecanismo de gestión de riesgo usa el canal CCH para transmitir el riesgo desde la RSUs a los vehículos. Primeramente, la CA calcula el riesgo y se lo transmite a las RSUs por un canal seguro cableado. Cada nodo de la VANET monitoriza el canal CCH durante los periodos designados como intervalos de control. El periodo de tiempo para un intervalo CCH entero se denomina Sync Interval (véase Figura 2). Entre intervalos de emisión del CCH, los nodos pueden cambiar al canal SCH para participar de aplicaciones tales como la descarga de ficheros.

Figura 2. CCH/SCH temporización.

De esta manera, cada CA regional envía a las RSUs que gestiona un mensaje autenticado M que contiene el valor del riesgo y un sello temporal.

$$CA \rightarrow RSUs : M = [Risk, TimeStamp]_{Sign_{CA}}$$

Cada CAs regional debe tener un enlace cableado para comunicar el riesgo a las RSUs correspondientes. El sello temporal permite que los vehículos verifiquen la frescura del mensaje y al mismo tiempo comprobar en qué instante fue calculado el riesgo. De esta forma se evitan ataques potenciales de falsificación y de repetición. El tamaño de este mensaje es de 72 bytes:

- 64 bytes para la firma ECDSA-256 de la CA.
- 4 bytes para el sello temporal representado los segundos UTC desde la época ('1970-01-01 00:00:00' UTC).
- 4 bytes para representar el valor del riesgo.

Durante el intervalo CCH, las RSUs difunden este mensaje a los vehículos. No obstante, no en todos los intervalos CCH se envía el mensaje M. Dependiendo de la tasa de revocación de certificados, cada CA regional establece su política de emisión de dicho mensaje, de manera que no se incurra en una sobrecarga sin sentido por la difusión del valor del riesgo. Normalmente, los certificados se revocarán con una tasa inferior a los $100ms$. Por ejemplo, si se están revocando certificados con una tasa media de 1 certificado por minuto, la CA tendrá que establecer la tasa de emisión del riesgo a un mensaje por minuto como máximo. Por otra parte, los vehículos que no estén en el alcance de ninguna RSU, pueden aprovecharse de las comunicaciones V2V para obtener el mensaje M. Como el mensaje está firmado por la CA, cualquier vehículo puede actuar como repositorio y transmitir el mensaje sin posibilidad de falsificar su contenido. Las OBUs deben comprobar la autenticidad y frescura del mensaje M, y descartarlo en cualquier otro caso. Una vez se ha autenticado, las OBUs son conscientes del riesgo que están asumiendo al operar en ese momento en la VANET confiando en la información contenida en la CRL cacheada. De forma indirecta, el valor del riesgo también proporciona una idea de cuantos certificados revocados son desconocidos. Dependiendo de los requisitos de frescura de aplicación y la actitud hacia del riesgo del usuario, los nodos pueden decidir si deben de

operar en la red o deben contactar con la CA para descargarse información de revocación más reciente.

IV. Evaluación

En este sección se evalúa la eficiencia del mecanismo propuesto para gestionar el riesgo inherente a la información de revocación. La evaluación se lleva a cabo mediante la plataforma NCTUns [10], que fue elegida por su librería avanzada del estándar IEEE 802.11p, y su capacidad de integración con cualquier herramienta de redes de Linux.

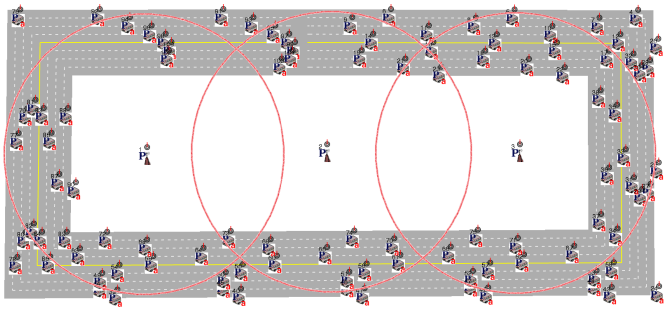

Figura 3. Escenario de simulación.

El escenario de referencia se representa en la Figura 3. Éste consiste de 4 vías de doble carril formando un rectángulo de 1000x500m. Se colocan tres RSUs en el interior del rectángulo cada 300 metros. Dada la colocación y el rango de cobertura de las misma, hay zonas de las vías que no entran en cobertura de ninguna de las tres RSUs.

La Tabla II resume los valores de los parámetros de configuración del escenario de referencia. Cabe destacar que hemos escogido el modelo de propagación Nakagami ya que varios estudios empíricos han mostrado que este modelos de propagación radio es adiente para la simulación de un entorno vehicular [11].

Parámetro	Valor
Área	1000x500m
Número de RSUs	3
Número de OBUs	100
Radio de transmisión de las RSUs	300m
MAC	IEEE 802.11p
Modelo de propagación	Nakagami

Cuadro II
Parámetros de configuración del escenario de referencia.

En primer lugar, evaluamos la sobrecarga introducida en la red por el mecanismo de gestión del riesgo propuesto. Con este fin, configuramos las RSUs de manera que transmiten el mensaje M que contiene el valor del riesgo cada segundo. La figura 4 muestra el throughput de entrada en el canal CCH de un vehículo escogido al azar. Como era de esperar, el vehículo recibe mensajes de la RSU más próxima cada 100 ms, y cada segundo recibe el mensaje M lo que supone un incremento del throughput de 72 bytes. Así, la sobrecarga que se introduce en la red es de un 4 % en media en el canal CCH. Cabe denotar que esta sobrecarga será mucho menor en un escenario más realista, dado que raramente la CA establecerá un política de emisión del riesgo tan conservadora. Emitir el riesgo cada segundo supondría que en la red vehicular se están revocando certificados con una tasa increíblemente alta o que las aplicaciones que se están usando requieren de datos de revocación de tan recientes como fuese posible.

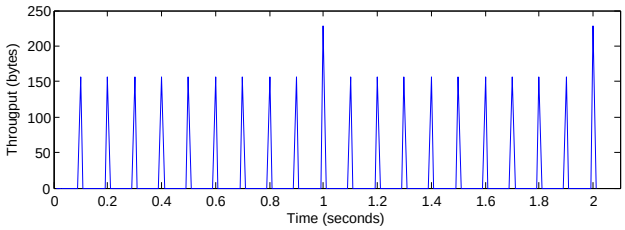

Figura 4. Caudal del canal CCH de un vehículo aleatorio.

Una vez hemos mostrado que la sobrecarga que el mecanismo que gestiona el riesgo es leve, a continuación evaluamos los beneficios de su uso. Para ellos, definimos tres perfiles de usuarios con actitudes hacia el riesgo diferentes:

- Aversos: usuarios que sólo operan si $Risk(t) \leq 0{,}3$.
- Neutrales: usuarios que sólo operan si $Risk(t) \in [0{,}3, 0{,}5]$.
- Amantes: usuarios que sólo operan si $Risk(t) \leq 0{,}9$.

Configuramos cada una de las 100 OBUs para seguir unos de estos tres perfiles de manera uniforme. Acto seguido, estimamos la evaluación del riesgo de operar en la red dada una política de emisión de CRL periódica. Como no disponemos de datos de revocación de una red vehicular, usamos la información de revocación contenida en la CRL de una CA real, GoDaddy. Godaddy es el actual proveedor de certificados SSL líder del mercado, Mediante la CRL de Godaddy, obtenemos el número diario de certificados revocados diariamente. Usando esta información calculamos la probabilidad de usar un certificado revocado $\rho(t)$. De la misma CRL somos capaces de obtener también las causas de revocación. La figura 5 muestra la ratio de certificados revocados según el tipo de causa. Este análisis abarca más de 300.000 certificados. Como se observa en la figura, la principal causa de revocación es el cese de operación, es decir, que un certificado que fue emitido con un determinado propósito ya no es necesario. El resto de causas son bastante menos probables. Usando los pesos definidos en la tabla I obtenemos el valor de las consecuencias de la CRL de Godaddy, i.e., $Q = 0{,}12$.

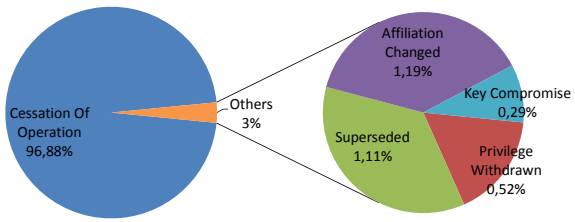

Figura 5. Causas de revocación de los certificados analizados.

Seguidamente, calculamos la función $Risk(t)$ para los siete días que dura la simulación. Como se puede ver en la figura 6, el riesgo es cero en los instantes de actualización de la CRL (en el caso de GoDaddy la CRL se actualiza cada 24 horas), y después éste crece conforme el número de certificados revocados.

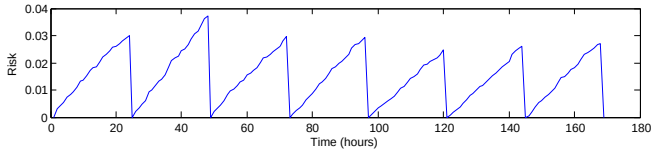

Figura 6. Riesgo de usar un certificado revocado desconocido.

Finalmente, lanzamos el escenario de simulación con un horizonte temporal de 7 días, y calculamos el tiempo durante el cual los vehículos pueden operar en la red de acuerdo a la actitud hacia el riesgo programada en la OBU. La figura 7 muestra el tiempo medio que un vehículo opera en la red de acuerdo con cada perfil. Los resultados muestran que los usuarios adversos al riesgo operan durante menos tiempo que aquellos que tienen una actitud más agresiva y arriesgan más. Cabe destacar que la relación entre los diferentes perfiles no es directamente proporcional, ya que el riesgo aumenta de acuerdo al número de revocaciones cuyo crecimiento no es lineal. También vale la pena observar que debido a que algunas zonas de la carretera no están cubiertas por ninguna RSU, hay usuarios que aún teniendo el mismo perfil de riesgo son capaces de operar durante más tiempo. Debido a esta misma razón, algunos usuarios de la red operan incluso cuando se ha sobrepasado su umbral de riesgo, dado que no son capaces de recibir el valor de riesgo ni de una RSU ni de ningún vehículo a su alcance.

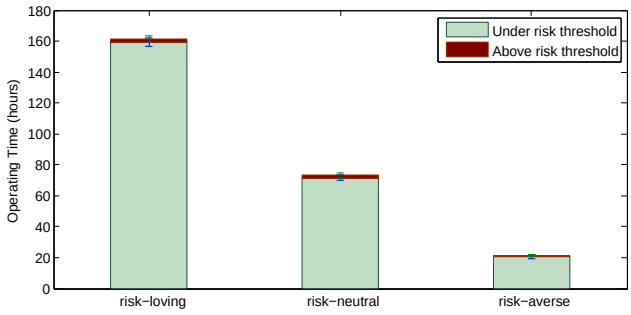

Figura 7. Tiempo de operación medio para cada tipo de perfil de riesgo.

V. Conclusiones

En este artículo se han analizado las limitaciones de la adopción de CRLs para gestionar el servicio de revocación en redes vehiculares. Se ha mostrado que la implantación de CRLs será factible siempre y cuando se utilicen CAs regionales conjuntamente con técnicas para reducir el tamaño de la CRL y optimizar su distribución No obstante, la frescura de los datos de revocación contenidos en la CRL debe ser gestionada de forma paralela para reducir la sobrecarga introducida en la red durante la distribución de las mismas.

Para dar a conocer a los usuarios la frescura de los datos de revocación, hemos propuesto un mecanismo capaz de gestionar el riesgo inherente a estos datos. Hemos mostrado que el riesgo propio de PKI vehicular no puede ser eliminado completamente, pero puede ser analizado y controlado. Mediante el servicio de revocación, las CA pueden controlar el riesgo y satisfacer los diferentes requisitos de frescura de la aplicaciones de la red vehicular. Con el mecanismo propuesto, los usuarios reciben periódicamente información acerca de la frescura de la CRL que está en vigor en un momento dado. De esta manera, las aplicaciones con requisitos de frescura más altos operarán con riesgo inferior pero a costa de sobrecargar la red tanto en ancho de banda como computacionalmente.

Acknowledgments

Este trabajo está subvencionado por el Ministerio de Ciencia y Educación bajo los proyectos CONSOLIDER-ARES (CSD2007-00004) y TEC2011-26452 "SERVET", y por la Generalitat de Catalunya bajo la subvención 2009 SGR 1362.

Referencias

[1] *IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments*, May 2008.

[2] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, ser. SASN '05, 2005, pp. 11–21.

[3] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Telecommunications, 2007. ITST '07. 7th International Conference on ITS*, Jun. 2007, pp. 1 –6.

[4] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, pp. 1–105, 2006.

[5] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, ser. VANET '08, 2008, pp. 86–87.

[6] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for vanet," in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, ser. VANET '09. New York, NY, USA: ACM, 2009, pp. 89–98.

[7] B. of Transportation Statistics U.S. Department of Transportation, "Number of u.s. aircraft, vehicles, vessels, and other conveyances," http://www.bts.gov/publications/national_transportation_statistics/html/table_01_11.html, 2009, [Online; accessed 31-July-2011].

[8] D. N. Cottingham, I. J. Wassell, and R. K. Harle, "Performance of ieee 802.11a in vehicular contexts," in *In Proc. IEEE VTC*. Spring, 2007.

[9] J. L. Muñoz, O. Esparza, C. Gañán, and J. Parra-Arnau, "Pkix certificate status in hybrid manets." in *WISTP*, ser. Lecture Notes in Computer Science, vol. 5746. Springer, 2009, pp. 153–166.

[10] S. Y. Wang and C. L. Chou, "Nctuns tool for wireless vehicular communication network researches," *Simulation Practice and Theory*, vol. 17, pp. 1211–1226, 2009.

[11] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta, "Empirical determination of channel characteristics for dsrc vehicle-to-vehicle communication," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ser. VANET '04. New York, NY, USA: ACM, 2004, pp. 88–88.