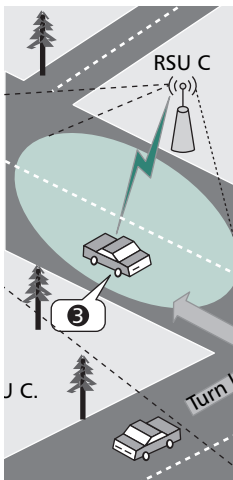# SECURITY IN SERVICE-ORIENTED VEHICULAR NETWORKS

HAOJIN ZHU, SHANGHAI JIAO TONG UNIVERSITY
RONGXING LU AND XUEMIN (SHERMAN) SHEN, UNIVERSITY OF WATERLOO
XIAODONG LIN, UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

The success of service delivery in vehicular networks depends on the underlying communication system to enable the user devices to connect to a large number of communicating peers and even to the Internet.

ABSTRACT

Service-oriented vehicular networks support diverse infrastructure-based commercial services including Internet access, real-time traffic concerns, video streaming, and content distribution. The success of service delivery in vehicular networks depends on the underlying communication system to enable the user devices to connect to a large number of communicating peers and even to the Internet. This poses many new research challenges, especially in the aspects of security, user privacy, and billing. In this article we first identify the key requirements of authentication, privacy preservation, and billing for service delivery in vehicular networks. We then review the existing industrial and academic efforts on service-oriented vehicular networks. We also point out two security challenges, minimizing vehicle-to-infrastructure authentication latency and distributed public key revocation, which are considered among the most challenging design objectives in service-oriented vehicular networks. A novel fast vehicle-to-infrastructure authentication based on a vehicle mobility prediction scheme and an infrastructure-based short-time certificate management scheme are then proposed to address these two challenges.

INTRODUCTION

With the advancement of wireless technology, vehicular communication networks, also known as vehicular ad hoc networks (VANETs), are emerging as a promising approach to increase road safety, efficiency and convenience [1]. The U.S. Federal Communication Commission (FCC) has allocated 75 MHz spectrum at 5.9 GHz for vehicle-to-vehicle (V2V) and vehicle-to-infra-structure (V2I) communications. The proposed vehicular communication technology, known as dedicated short-range communication (DSRC) [2], is currently being standardized by the IEEE. Many major car manufacturers have responded positively and are actively working together in bringing this promising technology to fruition.

Although the primary purpose of DSRC is to enable communication-based automotive safety applications like cooperative collision warning (CCW), the standard also provides for a range of commercial applications, thereby making DSRC technology more cost effective. For example, Internet access has become part of our daily lives, and there is a growing demand for accessing the Internet or information centers from vehicles. Therefore, roadside units (RSUs) can be deployed every few miles along the highway for users to download maps, traffic data, and multimedia files. Vehicles can use RSUs to report real-time traffic information and request location-based services such as finding restaurants, gas stations, or available parking space. Although third-generation (3G) networks or satellite techniques can be used to achieve this goal, RSUs have the advantage of low cost, easy deployment, and high bandwidth. We call these kinds of vehicular networks *service-oriented*, and they are expected to provide clear customer benefits and motivate commercial operators to invest in large-scale deployment of wireless infrastructures.

Figure 1 illustrates a typical service delivery scenario for future VANETs, which comprise three major domains: the vehicular internet-working, network provider, and content provider domains. In the vehicular internetworking domain, a vehicle gains access to the RSU via direct V2I communication when the vehicle is in the transmission coverage of the RSU, or multi-hop V2V and V2I communication when the vehicle is out of the RSU's overage. In the network provider domain, RSUs, which may be owned by a single or multiple network providers, can serve as Internet gateways to link users in vehicles and commercial service providers. The commercial service providers, which belong to the content provider domain, can maintain different service databases and provide corresponding services to customers.

In service-oriented vehicular networks, the success of service provisioning models depends on the underlying communication system to enable the user devices to connect to a large
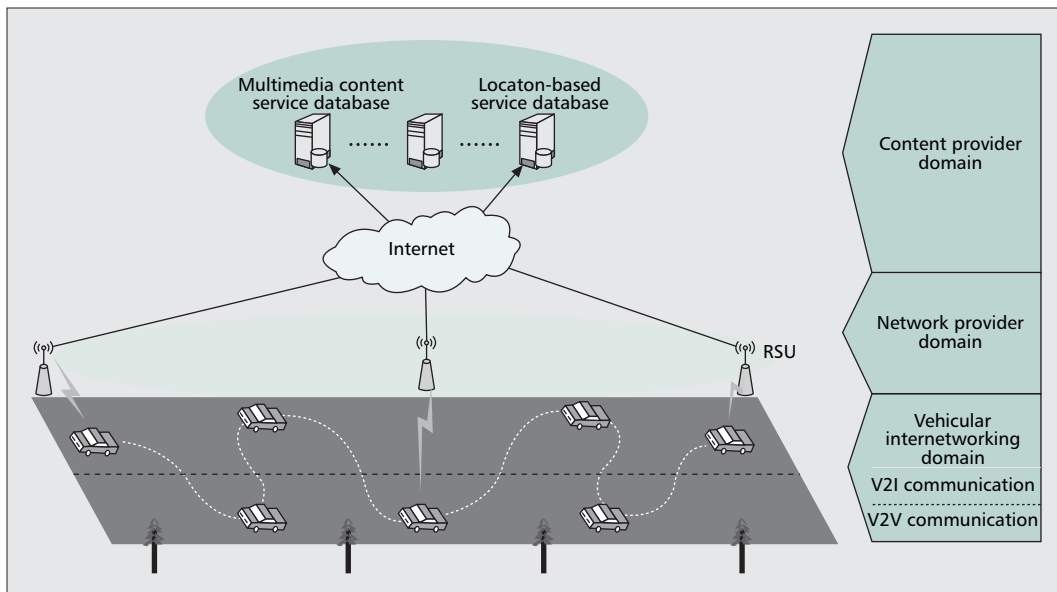
Figure 1. *System architecture of service-oriented vehicular networks.*

number of communicating peers and even to the Internet. This poses many new challenges, especially for security, user privacy, and billing for services in a highly mobile, and sometimes even multiple, service provider context. In particular, a series of security mechanisms on user authentication and content encryption should be well designed to provide a secure way to exchange information for the involved parties. Furthermore, anonymization services need to be provided in service-oriented VANETs to meet users' increasing demands for location privacy. In addition, a flexible billing model should be defined to reward the service providers as well as the forwarding vehicles.

In this article we first review the possible network architecture of service-oriented vehicular networks, and point out that hybrid V2I and V2V communication may be the anticipated network architecture in the future service-oriented vehicular networks. We then identify the basic security requirements, and discuss the related standards and possible solutions to achieve these security objectives. Finally, we propose two novel methods to address *long V2I authentication latency* and *public key certificate revocation* issues, which are identified as two crucial challenges in secure service-oriented vehicular network design.

NETWORK ARCHITECTURE OF SERVICE-ORIENTED VEHICULAR NETWORKS

From the transmission perspective, the service delivery in vehicular networks can be categorized into two cases: direct V2I communications and hybrid V2I and V2V communications. In an area where RSU density is high enough, as shown in Fig. 2a, vehicles can connect to the RSU directly. Even though direct V2I communication has the advantage in transmission reliability and wireless bandwidth, it suffers from limited transmission range. From an economical perspective, in the early stage of vehicular networks it is not cost
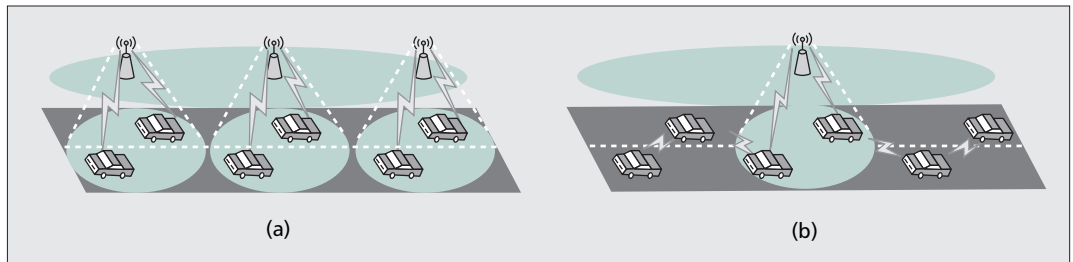
effective for the service operator to pursue full coverage because of the high deployment and maintenance costs. Alternatively, exploiting inter-vehicle transmission to broaden the service coverage range of the RSUs becomes a promising solution to provide broadband access in VANETs. As shown in Fig. 2b, intermediate nodes could forward traffic flows to the nearest RSU via multihop transmission, while the RSU provides Internet access for customers in vehicles.

The advancement of wireless technologies has made hybrid V2V and V2I transmission in service-oriented networks possible. For example, the IEEE 802.11p Wireless Access in the Vehicular Environment (WAVE) standard has been developed to support data exchange between high-speed vehicles, and between vehicles and RSUs. Furthermore, the network coding technique, which allows and encourages coding/mixing operations on intermediate forwarders and decoding on the recipients, has been introduced in VANETs to improve network throughput and minimize end-to-end delay [3]. Particularly, the coding-enabled wireless technique is suitable for the following services in VANETs:

- **Broadcast video streaming**: Service providers can broadcast the video streaming via roadside infrastructure (e.g., RSUs) to vehicles driving through. Drivers or passengers could also enjoy watching live news or football match, while the video data is conveyed by either from RSU directly or from other relay vehicles.
- **Content distribution**: Content distribution such as downloading digital maps is another promising application that should be supported by VANETs. What differentiates content distribution from other infotainment services is the quantity of information, which is usually very large. Therefore, it is difficult for vehicles to accomplish file downloading with a limited number of transactions with RSUs or other vehicles, and cooperative file distribution is inevitable in this case.

Figure 2. *Network architecture in service-oriented vehicular networks: a) high RSU density; b) low RSU density.*

In conclusion, we envision that in the near future the architecture of service-oriented vehicular networks will include hybrid V2V and V2I communication, which can achieve larger network coverage and better return on investment (ROI).

SECURITY REQUIREMENTS FOR SERVICE-ORIENTED VEHICULAR NETWORKS

To successfully deploy service-oriented vehicular networks, a number of security requirements must be satisfied.

Confidentiality: Confidentiality is necessary to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in a vehicular network environment to protect information traveling between different network entities including RSUs and forwarding vehicles, since an adversary may try to reveal the service content by eavesdropping. The confidentiality objective can be achieved by using end-to-end encryption, which requires the presence of mutual authentication and key agreement between the service requester and service provider.

Authentication: Similar to conventional systems, authentication techniques verify the identity of the vehicular nodes in communication and distinguish legitimate vehicular users from unauthorized users. In particular, the authentication in service-oriented vehicular networks includes two levels: authentication between vehicles (V2V authentication) to provide link-to-link security, and authentication between the vehicle and RSU as well as the service provider (V2I authentication) to ensure that accounting or billing can be performed correctly [4].

Privacy: Privacy issues for service provisioning in VANETs regard primarily preserving the anonymity of a vehicle and/or the privacy of its location. Privacy protection tries to prevent adversaries (e.g., another vehicle or an external observer) from linking the vehicle to the driver's name, license plate, speed, position, and traveling routes along with their relationships to compromise the sender's privacy [5].

Billing: Similar to authentication, there are also two billing issues: billing between vehicles and service providers (V2I billing), and billing between vehicles (V2V billing). The first billing issue takes place between users and service providers, and its major function is to charge service subscribers for the service they use. The second issue originates from conventional ad hoc networks and deals with intermediate node rewarding. To reward intermediate nodes, incentives for data forwarding must be considered.

In summary, security issues in service-oriented vehicular networks can be categorized into two major classes: security between vehicles, and security between vehicles and service providers or their operated infrastructure. In the following section we discuss possible solutions to achieve these security objectives.

RELATED STANDARDS AND POSSIBLE SECURITY SOLUTIONS

Many efforts have been made to address the security and privacy issues from both the standardization and academia point of view.

RELATED STANDARDS

The IEEE 1609.2 standard addresses the issues of securing WAVE messages against eavesdropping, spoofing, and other attacks and is positioned for providing V2V authentication and encryption [2]. It is based on industry standards for public key cryptography, including the support for elliptic curve cryptography (ECC), WAVE certificate formats, and hybrid encryption methods, in order to provide secure services for WAVE communications. The security infrastructure is also responsible for the administrative functions, which are necessary to support the core security functions, such as certificate revocation. However, this standard does not provide the support of user authentication and billing for any service-oriented applications.

AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

In [4] the key elements for a scalable solution of authentication, authorization, and accounting (AAA) that may be suitable for service delivery in VANETs are investigated. In [6] a novel AAA access control scheme for application services in VANETs is proposed based on IEEE 802.11i and the EAP-Kerberos model, where the authentication request is issued by the requesting vehicle and sent through the forwarding vehicles and the RSU, until reaching a centralized authentication server (e.g., RADIUS) that can grant access to the requesting mobile user. To realize fast and secure handoff in IEEE 802.11-based vehicular networks, an efficient pre-authentication scheme is proposed by reducing four-way handshake to two-way handshake between the RSU and requesting vehicles [7].

PRIVACY

The most widely adopted privacy preserving technique in vehicular networks is time-based pseudonyms. For example, in [5] the privacy of vehicles can be protected by introducing an electronic license plate (ELP), which is an anonymous key pair that can be changed frequently according to the driving speed and preloaded into a vehicle tamper-proof device (TPD). An alternative for providing anonymity in vehicular networks is the use of group signatures [8]. A group signature scheme allows one member of the group to sign a message such that other members of the group have the ability to verify that the message originated from a group member, but not to identify the actual sender.

INCENTIVE

In order to stimulate data forwarding in VANETs, incentive mechanisms including reputation-based and credit-based solutions can be adopted. Reputation-based schemes such as Confidant in [9] rely on the individual nodes to monitor neighboring nodes' traffic and keep track of each others' reputations so that uncooperative nodes can eventually be detected and excluded from the networks. Credit-based incentive schemes such as [10] introduce some form of virtual currency or e-cash to regulate the packet forwarding relationships among different nodes. A third party can be considered as existing that is responsible for e-cash issuing and clearance. In the context of service-oriented VANETs, this third party can be the service provider, and thus the data forwarding process can be also seen as data rewarding process.

In spite of the above research efforts, there are still many remaining issues. In the next two sections we focus on two important issues, reducing V2I authentication delay and distributed public key revocation, which are crucial to success of service oriented-networks.

REDUCING V2I AUTHENTICATION DELAY

As mentioned above, AAA-based IEEE 802.1x authentication can be a promising solution for authentication, authorization, and billing between vehicles and service providers. However, the full authentication described in IEEE 802.1x may require a long authentication delay up to 750~1200 ms, mostly due to the lengthy round-trip of signaling between the AAA server and the RSU [11]. Considering the highly frequent change of associated RSUs, authentications between vehicles and RSUs are expected to happen at high frequency. Therefore, it is difficult to apply the full authentication procedure, including RADIUS, to V2I re-association authentication due to its heavy operations and long delay times.

EXISTING FAST V2I AUTHENTICATION

To achieve global service continuity and enable users to gain fast access to various services, an efficient V2I authentication scheme is highly desired. Currently, there are a variety of strategies to reduce the handoff latency, including proactive key distribution and pre-authentication [12]. Proactive key distribution intends to achieve fast authentication in wireless environment by predistributing key materials one hop ahead of a mobile user for fast authentication, while a pre-authentication scheme requires a mobile user to perform the authentication before the associated RSU changes. Both schemes increase the load on the RSU and authentication server. We assume that the cost of performing a proactive key distribution or pre-authentication is $Cost_{auth}$, which includes the propagation cost of key context transfer between the RSUs or AAA signaling between the RSUs and AAA server. Given the number of one-hop neighboring RSUs $\mathcal{N}$ and the number of vehicles within the RSU's coverage range, $\mathcal{M}$, we can obtain the load on this RSU as $O(\mathcal{M} * \mathcal{N} * Cost_{auth})$. It is obvious that the cost will increase in line with traffic density as well as RSU density. In the following section we focus on reducing the proactive key distribution cost by taking advantage of vehicle mobility prediction.

FAST V2I AUTHENTICATION BASED ON VEHICLE MOBILITY PREDICTION

In VANETs drivers must follow traffic regulations and road instructions. For example, vehicles cannot wander on the road back and forth, and go off the road on purpose. Therefore, the movement pattern of vehicles becomes predictable. These unique characteristics in VANETs make mobility-prediction-based pre-authentication a promising fast authentication method that can significantly reduce authentication latency. First, a vehicle needs to successfully authenticate to an RSU in order to use any services, and the first authentication could be a lengthy full authentication procedure involved with a remote AAA server. Then the RSU with which the vehicle is associated predicts the possible future direction the vehicle will follow based on the following information:

- The traffic information broadcast by the vehicle, such as driving direction, acceleration/deceleration, velocity, position
- The RSU's surrounding area road map
- The RSU's neighboring RSUs distribution

After the RSU locates the next RSU that covers the area the vehicle will enter, the RSU can pre-establish a shared session key between the vehicle and its next associated RSU. Afterward, when the RSU association occurs, a symmetric-key-based user authentication process will take place locally between the vehicle and its new associated RSU, which is very fast.

Obviously, the accuracy of the direction prediction of a vehicle's movement is crucial to the success of the above fast authentication scheme. In VANETs each vehicle periodically broadcasts traffic-related information, such as driving direction, acceleration/deceleration, velocity, and position. We make use of such information as training data and design a mobility prediction scheme based on a multilayer perceptron (MLP) network, which has the ability to predict the possible future direction in which a vehicle will go. Since the scenario of driving at an intersection is much more complicated than the scenario of driving along the road, without loss of generality we chose the first one as a test environment. Specifically, we chose the physical location, 398 Westmount Rd. N, Waterloo, Ontario, Canada,

It can be considered that there exists a third party which is responsible for E-cash issuing and clearance. In the context of service-oriented VANETs, this third party can be the service provider, and thus the data forwarding process can be also seen as data rewarding process.

as shown in Fig. 3, as our test intersection. Eight hundred samples are collected, and each sample is a five-dimensional vector as presented below:

$$\langle \textit{Direction, Speed, Acceleration,} \\ \textit{Turn-Light, Traffic-Light} \rangle \quad (1)$$

where *Direction* denotes the direction a vehicle turns, such as east or west, and *Speed* denotes the velocity of a driving vehicle. *Acceleration* denotes whether a driving vehicle accelerates or decelerates. If the value of this field is positive, the vehicle is speeding up; otherwise, the vehicle is slowing down. The fourth field, *Turn-Light*, denotes signals of the turn light of a vehicle, particularly when a vehicle is going to turn at an intersection. As we define it, this field has five possible values, 0.2, 0.4, 0.6, 0.8, and 1, which denotes the flashing of a left-turn light, the flashing of a right-turn light, the flashing of a brake light, the flashing of both a left-turn light and a brake light, and the flashing of both a right-turn light and a brake light of the vehicle, respectively. The last field, *Traffic-Light*, indicates the color of the current traffic light: red, green, or yellow.

Since it is prohibited for a vehicle to make a U-turn at that intersection, the desired output of a vehicle's movement is turning left, turning right, or moving ahead. A three-layer perceptron of MLP is employed, and the number of neurons of the input layer is five, where each presents a feature in the five-dimensional vector. The num-ber of neurons of the hidden layer is 10, and the number of neurons of the output layer is three, where the biggest associated output on the neuron denotes the responding decision. The data set is divided into two parts, a training set with 600 samples and a testing set with 200 samples.

Table 1 presents the accuracy of the prediction. There are a total of 200 samples for testing. Seventy-one out of 200 vehicles made left turns at the intersection, and 68 samples are classified correctly; 65 out of 200 vehicles made right turns at the intersection, and 64 samples are classified correctly; 64 out of 200 vehicles went straight ahead at the intersection, and 64 are classified correctly. Thus, the total accuracy rate is 98.0 percent. The key reason the wrong prediction occurs is traffic violations. For example, some vehicles do not show their left-turn (right-turn) light when they turn left (right), or even indicate the wrong turn light.

The fast authentication process can be illustrated by Fig. 4. Suppose that the vehicle is originally associated with RSU A; RSU A will predict the vehicle mobility patterns and thus determine the possible next associated RSU (e.g., D in Fig. 4). The session key is transferred from A to D with the help of an authentication server. After obtaining the session key, RSU D can quickly authenticate a vehicle by performing symmetric-key-based user authentication and grant its access.

Based on the prediction accuracy rate, the expected authentication delay T can be formulated as follows:

$$T = T_1 \times p + (T_1 + T_2) \times q \\ = T_1 + T_2 \times q, \quad (2)$$

where p denotes the probability of correct prediction, and q is the probability of wrong prediction, which is equal to $1 - p$. T_1 denotes the authentication delay when the prediction is accurate, which means the delay of a symmetric-key-based user authentication process. T_2 denotes the authentication delay of a full IEEE 802.1x authentication process. In reality, T_2 is far larger than T_1. The final result of Eq. 2 shows that the expected authentication delay is linearly dependent on the accuracy of the prediction rate. The maximum is closely equal to T_2, and the minimum is equal to T_1. From the performance result in Table 1, our movement prediction scheme based on an MLP classifier can achieve very high accuracy; thus, the expected authentication delay is tightly close to the minimum delay T_1. Obviously, T_1 is the time for performing symmetric-key-based user authentication, which is usually very small.

DISTRIBUTED PUBLIC KEY REVOCATION

In service-oriented vehicular networks the security of V2V communication is based on public key certificates. However, how to efficiently revoke nodes' certificates represents a major challenge. A public key certificate links the public key to its owner's identity, which is certified and issued by a certification authority (CA). With public key certificates, various attacks, such as man-in-the-middle and impersonation attacks, can be prevented. However, due to misbehavior, a certificate of a user has to be revoked in order to limit the risk the certificate poses to the rest of the network.

	Turn left	Turn right	Go ahead	Total
Total number	71	65	64	200
Accurate number	68	64	64	196
Accurate rate	95.7	98.4	100	98.0

■ **Table 1.** *The performance of movement prediction.*
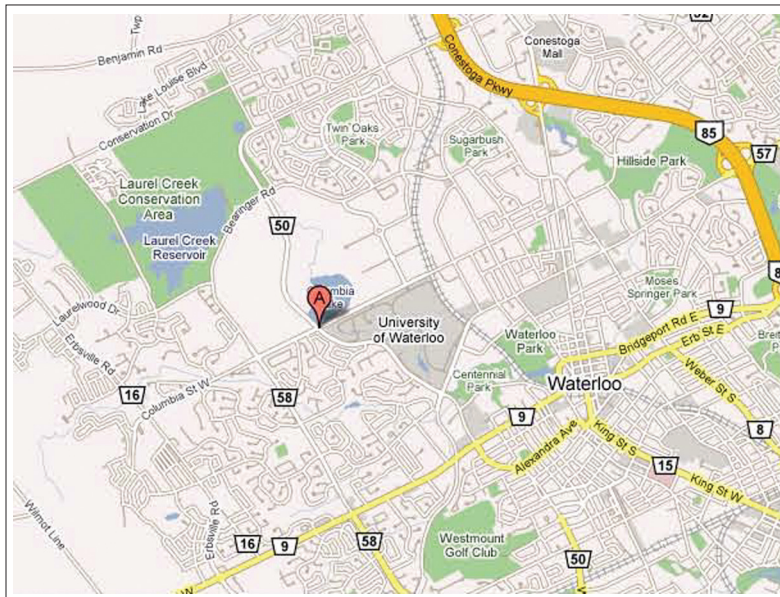
■ **Figure 3**. *The considered environment for the mobility prediction experiment.*

For example, an attacker could impersonate a legal vehicle to request services from an RSU, or a revoked node could generate unwanted traffic flows (denial-of-service [DoS] attacks). To mitigate situations such as those described above, an efficient public key revocation scheme is required.
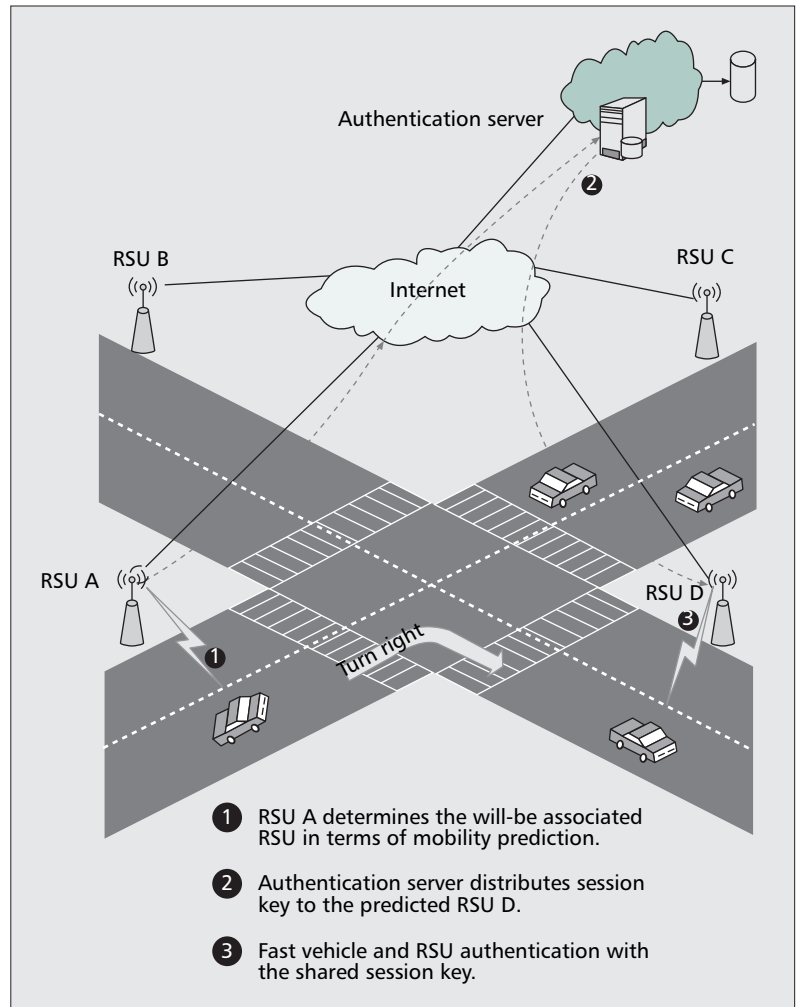
In traditional public key infrastructure (PKI) architecture, the most commonly adopted certificate revocation scheme is through a certificate revocation list (CRL), which is a list of revoked certificates stored in central repositories prepared in CAs. In the context of VANETs, the CA adds the identification of the revoked certificate(s) to a CRL. The CA then publishes the updated CRL to all VANET participants, instructing them not to trust the revoked certificate. The CA employs a set of infrastructures (e.g., RSUs) to broadcast this CRL to all mobile nodes as they pass. RSU-based CRL revocation may be challenging in certain areas (e.g., rural regions) where not enough RSUs are deployed or maintained. In these areas a vehicle may rarely encounter an RSU, and thus there may be a long delay until the vehicle receives the updated CRL, which may cause a potential threat to the security of vehicular networks.

CRL DISTRIBUTION BASED ON V2V TRANSMISSION

In [13] it is suggested to take advantage of V2V communications to speed up the CRL propagation process. A CRL update could be initialized by the RSUs, which broadcast the CRL update to each passing vehicle. Each receiving vehicle, in turn, transmits the updated CRL to every vehicle it encounters. This CRL propagation process is performed in an opportunistic way similar to epidemic routing, where each *infected* vehicle carries the updated CRL until it meets and forwards the updated CRL to the next uninfected vehicle. V2V-based CRL propagation can be regarded as a natural extension of traditional CRL distribution [13, 14]. However, if a large number of CRL distributions occur and are broadcast through the whole network, it can cause network congestion or hamper the provision of other high-priority services. In the next section, we will introduce a novel RSU-based short-time certificate scheme to avoid public key revocation.

RSU-BASED SHORT-TIME CERTIFICATE MANAGEMENT SCHEME

An alternative method to realize public key certificate revocation is using short-time certificates [15]. Based on the hierarchy network architecture of vehicular networks, we proposed a novel RSU-based short-time certificate management scheme in [15]. Each vehicle applies a long-term certificate from the CA and then updates a temporal short-time certificate whenever passing an RSU. To minimize the CRL distribution cost, CRL lists are distributed only to each RSU rather than to vehicles. The CRL distribution can thus be avoided since a vehicle is refused another short-time certificate from the RSU if it is on the revocation list. Another benefit of the RSU-based short-time certificate is that it can enhance user privacy by providing the driver with a new temporary identification whenever he/she passes an RSU.
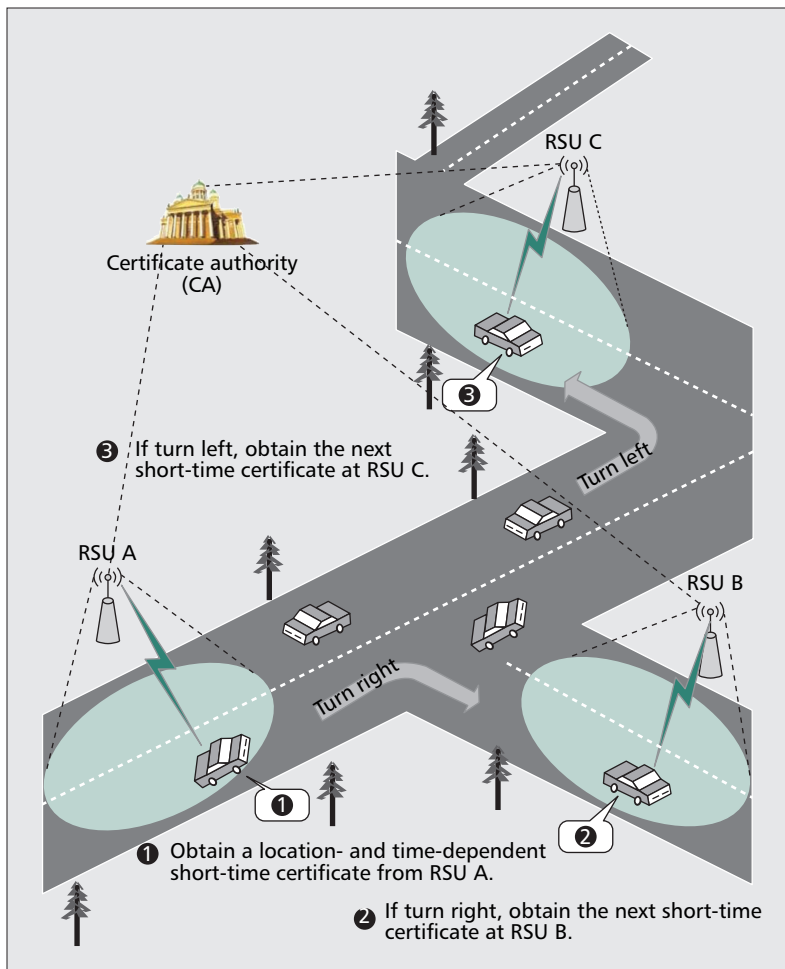

① RSU A determines the will-be associated RSU in terms of mobility prediction.

② Authentication server distributes session key to the predicted RSU D.

③ Fast vehicle and RSU authentication with the shared session key.

Figure 4. *An example of V2I fast authentication based on vehicle mobility prediction.*

The short-time certificate issuing process can be illustrated in Fig. 5. The vehicle sends a certificate request to RSU A to obtain the first short-time certificate. This short-time certificate can be updated at the next RSU, either *B* or *C*, depending on different routes. The validity time is determined by the maximum distance $\mathcal{D}_{max}$ between the RSU and its neighboring RSUs. We assume $\mathcal{V}$ as the expected average speed of this vehicle, so the validity time of this short-time certificate is $T_{valid} = \mathcal{D}_{max}/\mathcal{V} + \sigma$. Here, the parameter σ stands for the relaxing factor, which allows the certificate not to be revoked before the vehicle approaches the next RSU at a higher probability. The short-time certificate is not only time-dependent but also location-based. This means the short-time certificate is only valid in the neighboring area of a specific RSU, which can include all the possible routes to neighboring RSUs. Since all the short-time certificates are valid for a short period, the challenging public key revocation issue can be avoided.

CONCLUSION

Vehicular networks have been envisioned to play an important role in the future wireless communication service market. Service-oriented vehicular

■ Figure 5. *Location- and time-dependent short-time certificate.*

[3] S. Lee *et al.*, "Content Distribution in VANETs Using Network Coding: The Effect of Disk I/O and Processing O/H," *Proc. SECON '08*, 2008.

[4] E. Coronado and S. Cherkaoui, "An AAA Study for Service Provisioning in Vehicular Networks," *Proc. IEEE Conf. Local Comp. Net.*, 2007.

[5] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," *Proc. SASN*, 2005.

[6] H. Moustafa, G. Bourdon, and Y. Gourhant, "AAA in Vehicular Communication on Highways Using Ad Hoc Network Support: A Proposed Architecture," *Proc. VANET '05*, Sept. 2005.

[7] J. Hur, C. Park, and H. Yoon, "An Efficient Pre-Authentication Scheme for IEEE 802.11-Based Vehicular Networks," *IWSEC '07, LNCS4752*, 2007, pp.121–36.

[8] X. Lin *et al.*, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Trans. Vehic. Tech.*, vol. 56, no. 6, 2007, pp. 3442–56.

[9] E. Fonseca and A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS," NEC Network Labs, TR NLE-PR-2006-19, Mar. 2006.

[10] S. B. Lee *et al.*, "Secure Incentives for Commercial ad Dissemination in Vehicular Networks," *Proc. MobiHoc '07*, Sept. 2007.

[11] A. Alimian and B. Aboba, "Analysis of Roaming Techniques," IEEE 802.11-04/0377rl; http://www.drizzle.com/aboba/IEEE

[12] A. Mishra *et al.*, "Proactive Key Distribution Using Neighbor Graphs," *IEEE Wireless Commun.*, vol. 11, no. 1, 2004, pp. 26–36.

[13] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security Certificate Revocation List Distribution for VANET," *Proc. VANET '08*, San Francisco, CA, Sept. 2008.

[14] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," *Proc. VANET '08*, San Francisco, CA, Sept. 2008.

[15] R. Lu *et al.*, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *Proc. INFOCOM '08*, Phoenix, AZ, Apr. 15–17, 2008.

BIOGRAPHIES

HAOJIN ZHU (zhu-hj@cs.sjtu.edu.cn) received his B.Sc. degree (2002) from Wuhan University, China, his M.Sc. (2005) degree from Shanghai Jiao Tong University, China, both in computer science, and his Ph.D (2009) in electrical and computer engineering from the University of Waterloo, Canada. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His current research interests include wireless network security and applied cryptography.

RONGXING LU (rxlu@bbcr.uwaterloo.ca) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

XIAODONG LIN (xiaodong.lin@uoit.ca) received a Ph.D. in electrical and computer engineering from the University of Waterloo in June 2008 and a Ph.D. in information engineering from the Beijing University of Posts and Telecommunications, China, in June 1998. He is currently an assistant professor with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

XUEMIN (SHERMAN) SHEN [F] (xshen@bbcr.uwaterloo.ca) received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He serves as an Area Editor for *IEEE Transactions on Wireless Communications* and Editor-in-Chief for *Peer-to-Peer Networks and Applications*. He is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.

networks, which rely on both V2I and V2V communications, can be regarded as a combination of infrastructure-based broadband wireless networks and ad hoc networks. In this article we have discussed the key security requirements, and pointed out that existing solutions may face the challenges of long V2I authentication delay and public key revocation issues. The proposed V2I fast authentication scheme based on vehicle mobility prediction and an RSU-aided short-time certificate scheme can successfully address the authentication latency and public key certificate revocation issue. Our further research will focus on how to seamlessly integrate security at the V2I and V2V levels to obtain a general security platform for the service-oriented VANETs. We will also investigate the security performance by simulating in more realistic scenarios.

REFERENCES

[1] Communications for High-Speed Moving Objects: IEEE 802.16e, IEEE 802.20 and 5.9 GHz DSRC; http://www.researchandmarkets.com/reports/c50922

[2] IEEE Std. 1609.2-2006, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages," 2006.