Security in Vehicular Ad Hoc Networks

Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin (Sherman) Shen, University of Waterloo

ABSTRACT

Vehicular communication networking is a promising approach to facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. One of the ultimate goals in the design of such networking is to resist various malicious abuses and security attacks. In this article we first review the current standardization process, which covers the methods of providing security services and preserving driver privacy for Wireless Access in Vehicular Environments (WAVE) applications. We then address two fundamental issues, *certificate revocation* and *conditional privacy preservation*, for making the standards practical. In addition, a suite of novel security mechanisms are introduced for achieving secure certificate revocation and conditional privacy preservation, which are considered among the most challenging design objectives in vehicular ad hoc networks.

INTRODUCTION

The advancement and wide deployment of wireless communication technologies have revolutionized human lifestyles by providing the most convenience and flexibility ever in accessing Internet services and various types of personal communication applications. Recently, car manufacturers and telecommunication companies have been gearing up to equip each car with technology that allows drivers and passengers to communicate with each other as well as with the roadside infrastructure that may be located in some critical sections of the road, such as at every traffic light or any intersection or stop sign, in order to improve the driving experience and make driving safer. For example, Microsoft Corp.'s MSN TV and KVH Industries, Inc. have introduced an automotive vehicle Internet access system called TracNet, which can bring Internet service to any in-car video screen. It also turns the entire vehicle into an IEEE 802.11-based Wi-Fi hotspot, so passengers can use their wireless-enabled laptops to go online. Furthermore, by using such equipped communication devices, also known as onboard units (OBUs), vehicles can communicate with each other as well as with roadside units (RSUs) located at critical points on the road. A self-organized network can be formed by connecting the vehicles and RSUs, called a vehicular ad hoc network (VANET), and the RSUs are further connected to the backbone network. Increasing interest has been raised recently in the applications of roadside-to-vehicle communications (RVCs) and intervehicle communications (IVCs), aiming to improve driving safety and traffic management while providing drivers and passengers with Internet access. It is estimated that the market for vehicular communications will reach multiple billions of dollars by 2012.

In VANETs, RSUs can provide assistance in finding facilities such as restaurants and gas stations, and broadcast traffic-related messages such as maximum curve turning speed notifications to give drivers a heads up. On the other hand, VANETs can enable vehicles to communicate with each other so that drivers can have better awareness of what is going on in their driving environment and take early action to respond to an abnormal situation. For achieving this, an OBU regularly broadcasts routine traffic-related messages with information on position, current time, direction, speed, brake status, steering angle, turn signal, acceleration/deceleration, traffic conditions, and traffic events [1]. In addition, emergency messages can be generated and sent by OBUs in case of emergent braking, traffic jam, or any accident. For example, as shown in Fig. 1, whenever there is an accident on a highway, several lanes can be blocked. Drivers can experience a long delay. However, the delay can be mitigated if drivers are informed in advance so that they can follow detour route or change lanes to avoid a traffic jam.

Despite the advantages of a VANET, there are many challenges, especially in the aspects of security and privacy. As a special implementation of mobile ad hoc networks (MANETs), a VANET inherits all the known and unknown security weaknesses associated with MANETs, and could be subject to many security and privacy threats. It is obvious that any malicious behavior of users, such as a modification and replay attack with respect to the disseminated

0163-6804/08/$25.00 © 2008 IEEE

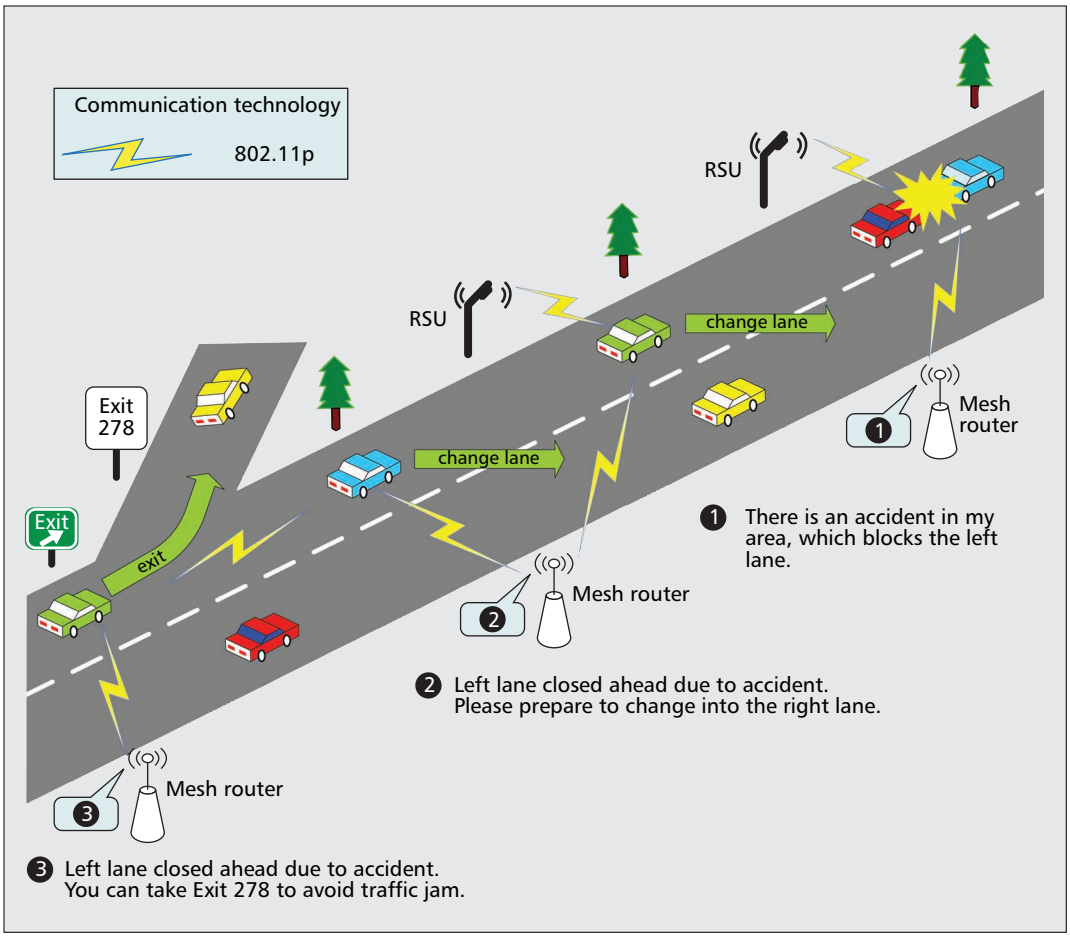

Figure 1. *An example of road emergency response operation under VANET.*

The IEEE 1609 WAVE communication standards, which are also known as Dedicated Short Range Communications protocols, have emerged recently to enhance the 802.11 to support wireless communications among vehicles for the roadside infrastructure.

messages, could be fatal to the other users. In addition, the issues in VANET security become more challenging due to the unique features of networks, such as the high-speed mobility of the network entity (or vehicle) and the extremely large amount of network entities. Furthermore, *conditional privacy preservation* must be achieved in the sense that user related privacy information, including the driver's name, license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in case of dispute such as a crime/car accident scene investigation, which can be used to look for witnesses. Therefore, it is critical to develop a suite of elaborate and carefully designed security mechanisms for achieving security and conditional privacy preservation in a VANET. Until recently, however, security and privacy issues of VANETs have been given little attention. It is notable that security and privacy concerns have formed the major barrier, preventing many drivers from employing state-of-the-art Internet connected automobile technologies.

In this article we first review IEEE 1609.2 and the Vehicle Safety Communications (VSC) project, which specify methods of securing Wireless Access in Vehicular Environments (WAVE) messages against various attacks, such as eavesdropping, modification, source spoofing, message modification, and replays [1, 2]. We then identify two fundamental issues, certificate revocation and conditional privacy preservation, which need to be addressed in order to make the standards practical. Furthermore, we propose a suite of novel security mechanisms in order to achieve secure certificate revocation and conditional privacy preservation, which are considered among the most challenging design objectives in VANETs.

IEEE 1609.2 Security and the VSC Project

The IEEE 1609 WAVE communication standards, which are also known as Dedicated Short Range Communications (DSRC) protocols, have emerged recently to enhance 802.11 to support wireless communications among vehicles for the roadside infrastructure [2]. The IEEE 1609.2 standard addresses the issues of securing WAVE messages against eavesdropping, spoofing, and other attacks. The components of the IEEE 1609.2 security infrastructure are shown in Fig. 2, and are based on industry standards for public key cryptography, including 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 necessary to support core

The VSC project proposes to maintain a list of short-lived anonymous certificates for the purpose of keeping the privacy of drivers, where the short-lived certificates are discarded once after being used. The scheme can provide a higher security assurance.

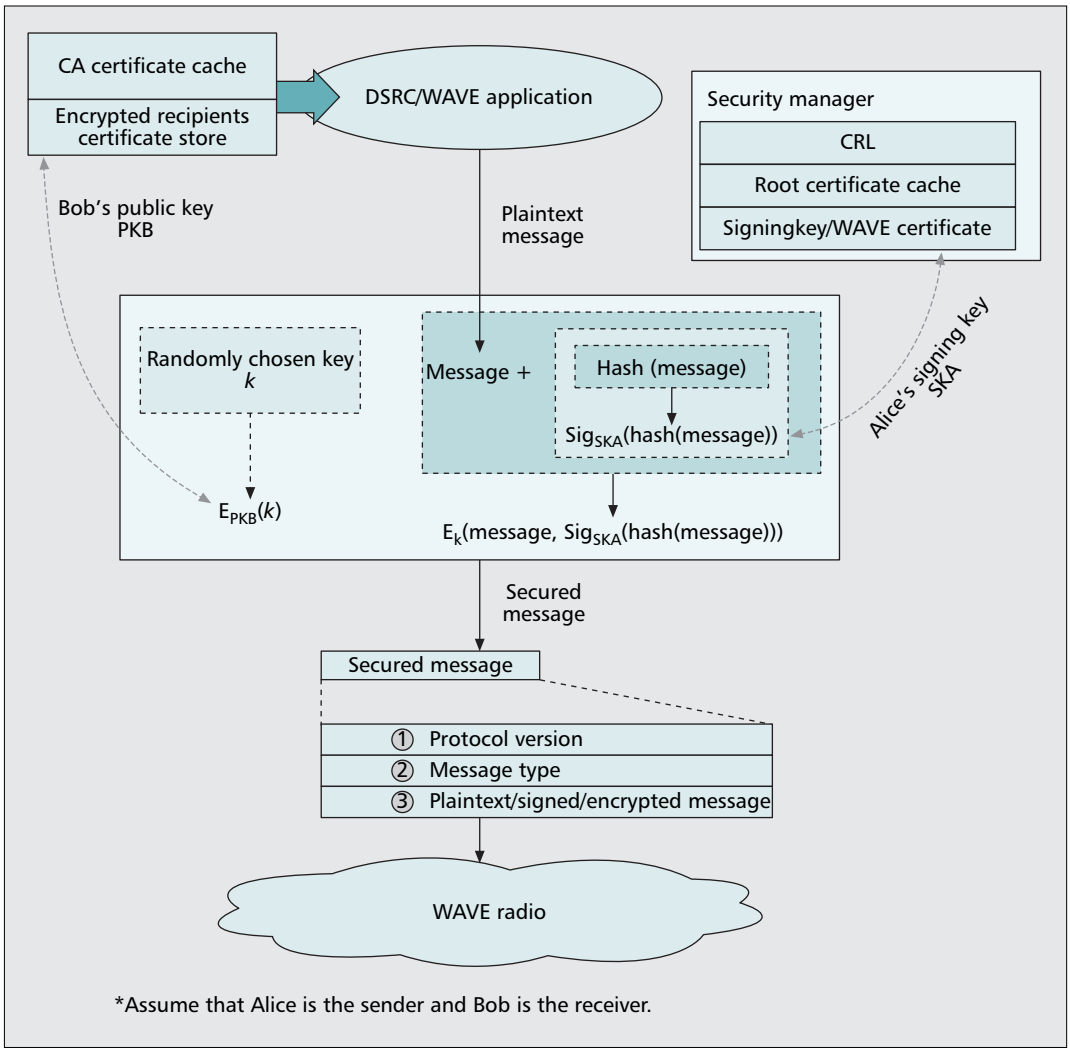

Figure 2. *The IEEE Std 1609.2 security services framework for creating and exchanging WAVE messages between WAVE devices.*

security functions such as certificate revocation. Note that certificate revocation is essential to any security system based on the public key infrastructure (PKI), which has not been addressed in the current IEEE 1609.2 by considering the unique features of vehicular networks. In addition, IEEE 1609.2 does not define driver identification and privacy protection, and has left a lot of issues open.

The Vehicle Safety Communications (VSC) project also evaluates the feasibility of supporting vehicle safety related applications through the DSRC standard [1]. The VSC project proposes to maintain a list of short-lived anonymous certificates for the purpose of keeping the privacy of drivers, where the short-lived certificates are discarded once they have been used. The scheme can provide higher security assurance because the certificates are blindly signed by the certificate authority (CA) in order to deal with any possible insider attack. An insider attack could simply be launched by the CA abusing its authority and mishandling driver information. A linkage marker is devised for the escrow authorities to associate each blindly signed anonymous certificate with a single vehicle. All compromised and expired vehicles have to be revoked by putting certificates belonging to those vehicles into the certificate revocation list (CRL). The disadvantage of this scheme is that the CRL may grow quickly such that it takes a long time to check through the whole CRL to see if a given certificate is valid or not. Another disadvantage lies in the fact that for achieving traceability, a unique electronic identity is assigned to each vehicle by which the identity of the vehicle owner can be inspected by the police and authorities in any dispute. Although this scheme can effectively meet the conditional anonymity requirement, it is far from efficient, and can hardly become a scalable and reliable approach because the ID management authority has to keep all the anonymous certificates for the vehicles in the administrative region. Once a malicious message is detected, the authority has to exhaustively search a very large database to find the identity related to the compromised anonymous certificate. In the following we introduce a more effective and efficient solution for achieving *certificate revocation* and *conditional privacy preservation*.

RSU-AIDED CERTIFICATE REVOCATION

A public key certificate links the public key to its owner's identity, which is certified and issued by a CA. With a public key certificate, various attacks, such as man-in-the-middle attacks and impersonation attacks, can be prevented. However, due to some unexpected reasons, a certificate of a user may need to be revoked. For example, once the private key corresponding to the public key specified in the certificate is identified as compromised, the certificate should be revoked to maintain system security.

In traditional PKI architecture, the most commonly adopted certificate revocation scheme is through CRL, which is a list of revoked certificates stored in central repositories prepared in CAs. Based on such centralized architecture, alternative solutions to CRL could be by way of a certificate revocation system (CRS), certificate revocation tree (CRT), the Online Certificate Status Protocol (OCSP) [3], and other methods. The common requirement for these schemes is high availability of the centralized CAs, where frequent data transmission with OBUs to obtain timely revocation information may cause significant overhead. Thus, with the high-speed mobility and extremely large amount of network entities in VANETs, the centralized CRL architecture may be far from realistic.

To tackle the problem, Raya *et al*. [4] proposed three certificate revocation protocols for VANETs: Revocation Using Compressed Certificate Revocation Lists (RC^2RL), Revocation of the Tamper-Proof Device (RTPD), and Distributed Revocation Protocol (DRP). RC^2RL uses a compression technique to reduce the overhead of distribution of the CRL. Instead of checking the status of a certificate, RTPD removes revoked certificates from their corresponding vehicles' certificate stores by introducing a tamper-proof device as a vehicle key and certificate management tool. In this case the vehicle possessing the revoked certificates is informed of the certification revocation incident by which the tamper-proof device automatically removes those revoked certificates. Different from RC^2RL and RTPD, a distributed certificate revocation mechanism is implemented in DRP to determine the status of a certificate. In DRP each vehicle is equipped with an attacker detection system, which enables a vehicle to identify any compromised peer. When a compromised or malicious vehicle is detected and located, its neighbors can work together to temporally revoke the compromised one. To design a suitable and efficient certificate revocation scheme, the following four observations are made:

- Although certificate revocation events are rare, the timely notification of such an event is crucial to a PKI-based security system, especially in a VANET environment with an extremely large amount of vehicles distributed across a wide area. In this case it is infeasible to assume that each vehicle can check the revocation status of the certificates they are using. Furthermore, there could be far fewer RSUs than vehicles. It is envisioned that RSUs will be sparse in a VANET, mainly located at every road intersection and freeway interchange along roads.
- The CRL could be very large, while the storage space at each individual OBU may be small. This results in the fact that the CRL available at an OBU could be incomplete or inaccurate.
- The movement of a vehicle can be predicted based on its broadcast traffic-related messages.
- IVC communications are performed locally, where a vehicle is more interested in the driving environment around it by listening to the broadcast messages from its neighboring vehicles. In this way an RSU can be used to assist certificate revocation checking by validating the status of a certificate from a passing vehicle based on its broadcast messages. If a revoked certificate is found, the RSU will notify all the other vehicles within its transmission range by broadcasting a warning message containing the revoked certificate just identified.

Therefore, we introduce a novel RSU-aided certificate revocation (RCR) mechanism for performing certificate revocation. As shown in Fig. 3, there are three types of network entities: the authority (denoted CA), RSUs, and vehicles. Their relationship is defined as follows. The CA manages the RSUs, and both of them are assumed to be trustworthy. The RSUs are connected to the Internet through either wired Ethernet or WiMAX, or any other networking technology. Furthermore, the CA provides each RSU a secret key, while the corresponding public key is an identity string containing the name of the RSU, the physical location, and the authorized message type. In this way an RSU can sign messages by using an identity-based signature [7].

Whenever a certificate is revoked, the CA will broadcast a certificate revocation notification to all the RSUs. Each RSU then checks the status of the certificates contained in all the messages broadcast by the passing vehicles. If a certificate has been confirmed as revoked, the RSU will broadcast a warning message such that all other approaching vehicles can update their CRLs and avoid communicating with the compromised vehicle. Since vehicle movement can be predicted based on its driving conditions (e.g., direction, speed, position), the RSU can further notify all neighboring RSUs of where the compromised vehicle may go. In addition, RSUs are normally sparsely located, so even if all the RSUs broadcast the corresponding warning message, only a limited number of vehicles will be notified. Thus, to speed up warning message dissemination, the warning message among vehicles can be forwarded through IVC communications, that is, forwarded by each vehicle, hop by hop, throughout its predefined lifetime.

However, a compromised vehicle may intentionally disable message broadcasting while it passes through an RSU to avoid being detected. This is also referred as a *silent attack*, which can easily be handled by granting every RSU the

To speed up the warning message dissemination, the warning message among vehicles can be forwarded through IVC communications, i.e., it can be forwarded by each vehicle hop-by-hop throughout its pre-defined lifetime.

If a vehicle discovers that a neighbor vehicle is using a certificate that has not been verified by an RSU for longer than a certain period of time, the corresponding messages will be disregarded. Thus, the security and safety of the VANET can be achieved with the least amount of effort.

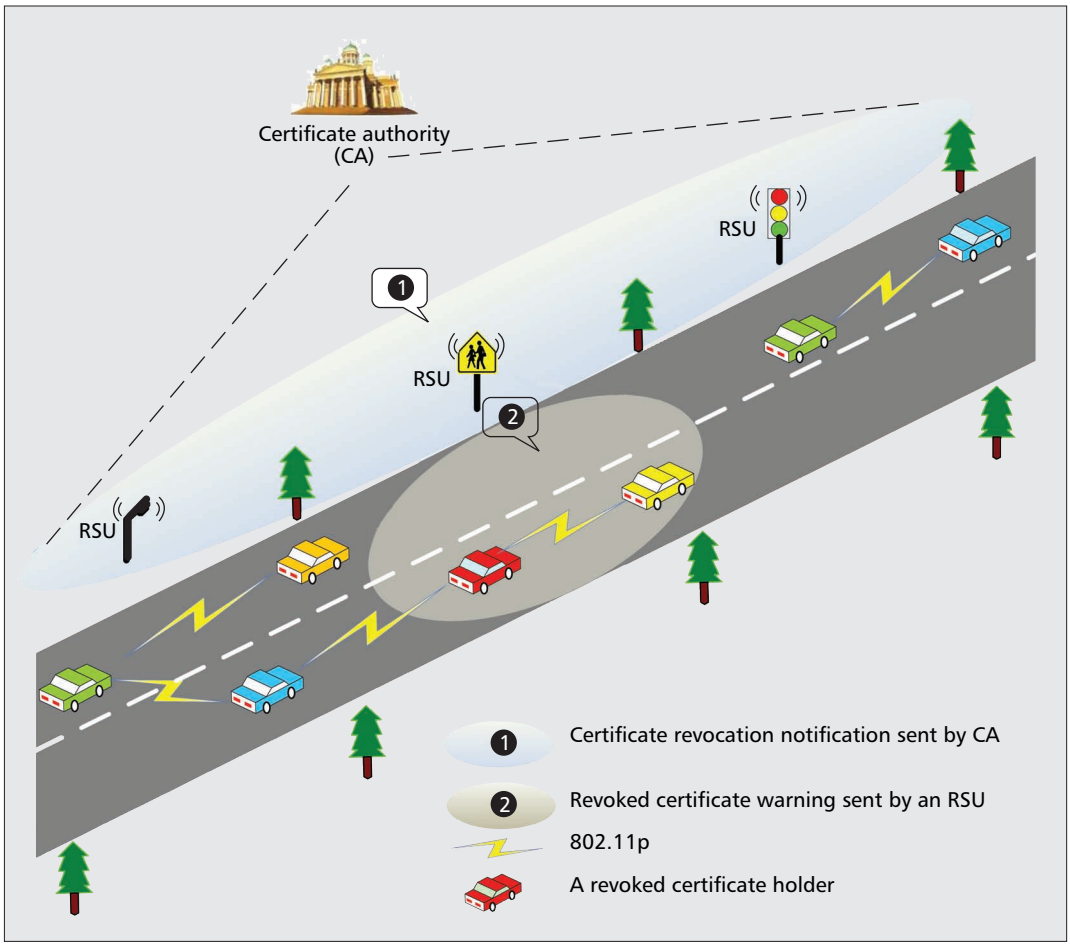

Figure 3. *The RSU-aided certificate revocation scheme.*

privilege of signing the certificate of each vehicle. In this case, whenever a vehicle passes through an RSU, the vehicle asks the RSU to sign its certificate, where the signature serves as evidence that can demonstrate its authenticity and legitimacy to other vehicles. If a vehicle discovers that a neighbor vehicle is using a certificate that has not been verified by an RSU for longer than a certain period of time, the corresponding messages will be disregarded. Thus, the security and safety of the VANET in terms of resisting compromised vehicles can be achieved with the least amount of effort.

Conditional Privacy Preservation

Privacy preservation is another important design requirement for VANETs, where the *source privacy* of safety messages is envisioned to emerge as a key security issue because some privacy- sensitive information, such as the driver's name, license plate, position, and driving route, could be intentionally deprivatized so that the personal privacy of the driver is jeopardized. Therefore, the safety message's authentication with *source privacy preservation* is critical for a VANET to be considered for practical implementation and commercialization. In particular, the *privacy preservation* in VANETs should be conditional, where senders are anonymous to receivers while traceable by the CA. With traceability, the CA can reveal the source identity of a message once a dispute occurs to the safety message.

In spite of its ultimate importance, conditional privacy preservation has not been well studied. In [4] Raya *et al.* proposed a security protocol based on anonymous key pairs, hereafter referred to as anonymous credentials. By installing a large number of short-lived anonymous credentials (probably 43,800) in a vehicle and randomly selecting one of them to sign each message, the vehicle's anonymity requirement can be met. Also, a unique electronic identity is devised and can be used by the police to associate the identities of vehicle owners with launched messages. However, this protocol may be inefficient when the CA would like to identify the sender of a malicious message since the CA needs to keep the anonymous credentials of all the vehicles in an administrative region (which could be a province or a whole country). Once a malicious message is detected, the CA has to exhaustively search a very large credential database (probably 43,800 × million cars) to find the identity related with the compromised anonymous credential, which incurs tremendous complexity for identity and credential management. In addition, since compromised or expired vehicles have to be revoked, all credentials belonging

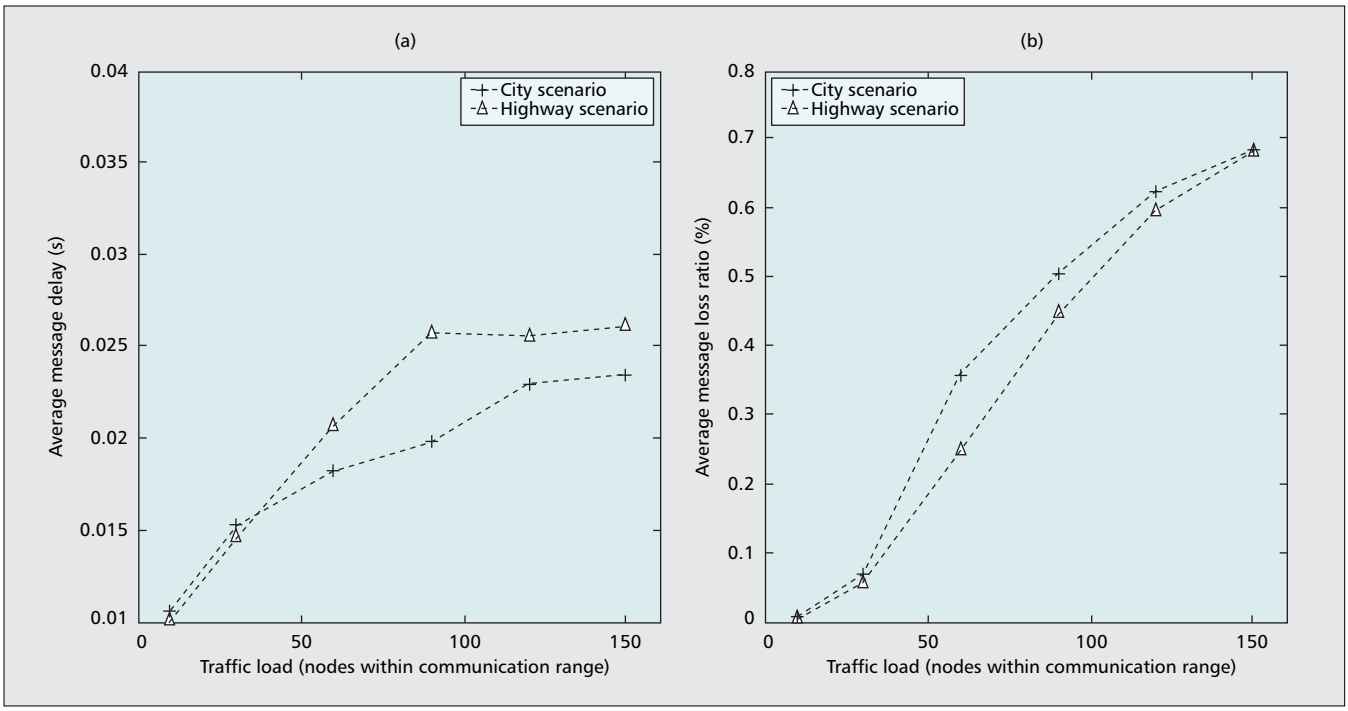

Figure 4. *Impact of traffic load on: a) message end-to-end delay; b) message loss ratio.*

to those revoked vehicles have to be released in the CRL, which tremendously increases the size of the CRL and makes the dissemination of the CRL intractable.

State-of-the-art progress in solving the problem was recently made to achieve conditional privacy preservation in VANETs by integrating the techniques of group signature and identity-based signature (GSIS) [5]. Based on these signatures, the GSIS protocol not only meets the security and conditional anonymity requirements for VANETs, but also simplifies certificate and ID traceability management. In particular, the GSIS protocol can significantly reduce the size of the CRL and minimize the effort of deploying PKI for RSUs. This is achieved by dividing the security problem into two categories: the communications between OBUs, as well as between OBUs and RSUs, due to their different security requirements. In the first category a short group signature scheme [6] is employed to secure messages launched by OBUs, where messages can be securely and anonymously signed by senders, while the identities of senders can be recovered by authorities. As for the second category, a signature scheme using identity-based cryptography (IBC) [7] is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity, where the signature and certificate management overhead can be tremendously reduced. OBUs installed in emergency vehicles will be treated the same as RSUs since it is unnecessary to protect the privacy of both RSUs and OBUs installed in emergency vehicles. In addition, the identity of each RSU as its public key is a concatenation of the name of the RSU, the operation region, and the authorized message types. With such a design an RSU replication attack, where a compromised RSU is relocated to launch any malicious attack, can be mitigated by the fact that any OBU receiving the messages can check the physical location and message type to see if the message sender is working in the authorized domain.

To verify the efficiency of the proposed security protocol GSIS for IVC applications, we conduct a simulation with ns-2. In order to properly estimate the practical road environment and vehicular traffic, two different types of road systems are considered. The first is by way of the mobility model generation tool introduced in [8], which is specialized to generate realistic city traffic scenario files for vehicles in ns-2. This tool makes use of the publicly available Topologically Integrated Geographic Encoding and Referencing (TIGER) database from the U.S. Census Bureau, where detailed street maps of each city and town in the United States of America are given. The map adopted in the study is a real city traffic environment in Houston, Texas. Each vehicle is first randomly scattered on one intersection of roads and repeatedly moves toward another randomly selected intersection along the paths in the map. Each vehicle drives at a randomly fluctuated speed in a range of ±5 mi/h centered at a road speed limit that ranges from 35–75 mi/h along different streets. The second type of road system considered in the study is a traffic scenario on a straight bidirectional six-lane highway, where the vehicles drive at speeds within the range of 100 ± 10 mi/h. The transmission range of each vehicle is 300 m. In both cases an RSU is allocated every 500 m along each road, which sends messages every 300 ms.

The performance metrics used in the simulation are the average message delay and average message loss ratio, which are denoted $avgD_{msg}$ and $avgLR$, respectively, and expressed as follows:

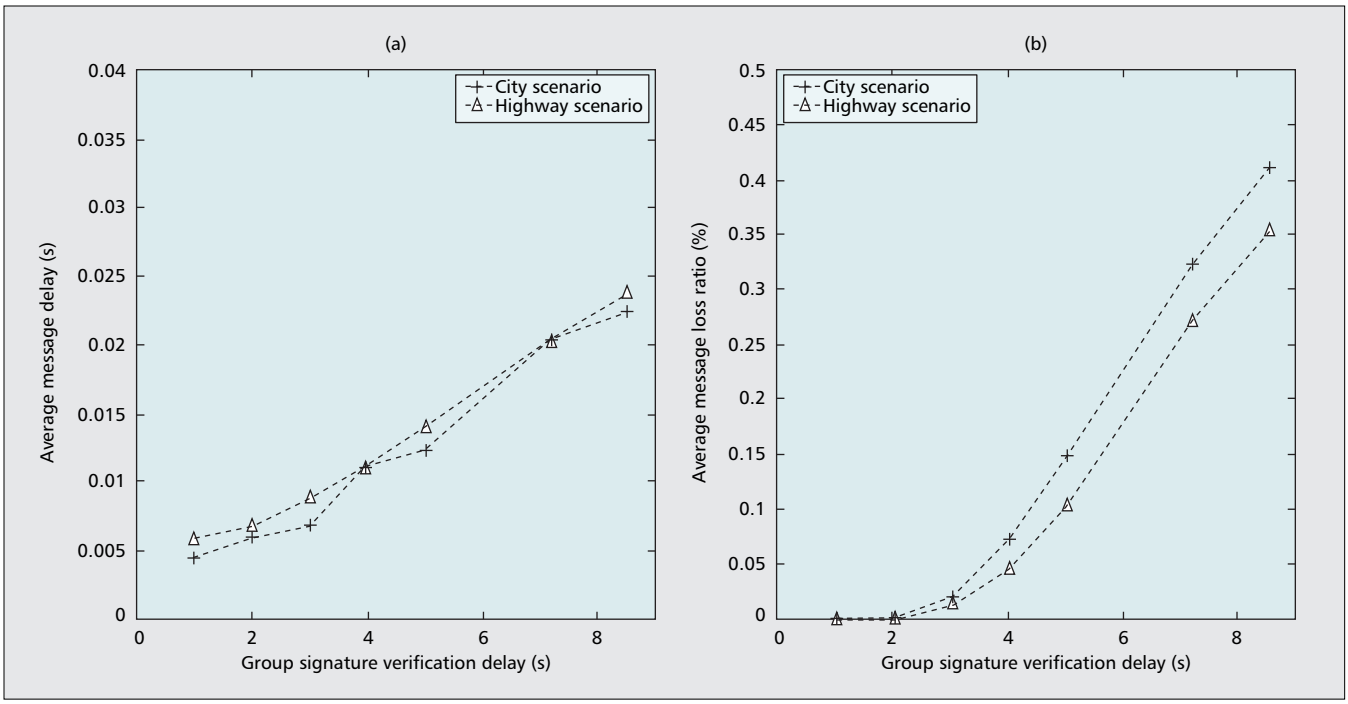

Figure 5. *Impact due to signature verification latency on: a) message end-to-end delay; b) message loss ratio.*

$$avgD_{msg} = \frac{1}{N_D \cdot M_{sent\_n} \cdot K_n} \sum_{n \in D} \sum_{m=1}^{M_{sent\_n}} \sum_{k=1}^{K_n} \begin{Bmatrix} T_{sign}^{n\_m} + T_{transmission}^{n\_m\_k} + T_{verify}^{n\_m\_k} \\ \cdot (L_{n\_m\_k} + 1) \end{Bmatrix}, \quad (1)$$

where D is the sample district in the simulation, N_D is the number of vehicles in D, M_{sent_n} is the number of messages sent by vehicle n, K_n is the number of vehicles within the one-hop communication range of vehicle n, $T_{Sign}^{n\_m}$ is the time taken by vehicle n to sign message m, $T_{transmission}^{n\_m\_k}$ is the transmission delay of message m sent by vehicle n and received by transmission vehicle k, $T_{verify}^{n\_m\_k}$ is the time taken by vehicle k to verify message m sent by vehicle n, and $L_{n\_m\_k}$ is the length of the queue in vehicle k when message m sent by vehicle n is received.

$$avgLR = \frac{1}{N_D} \sum_{n=1}^{N_D} \frac{M_{consumed}^{n}}{\sum_{k=1}^{K_n} M_{arrived}^{n}}, \quad (2)$$

where $M_{consumed}^{n}$ is the number of messages consumed by vehicle n in the application layer, and $M_{arrived}^{n}$ is the number of messages received by vehicle n in the MAC layer. In the following two sets of experiments are conducted to analyze the impacts of having different traffic loads and cryptographic algorithm processing speeds. Different from any previously reported study, this study takes the average number of neighboring vehicles within the communication range of each vehicle as the traffic load, which serves as the upper bound on the number of packets a vehicle could receive within a dissemination cycle (i.e., predefined broadcast traffic-related message period). Furthermore, the delay induced by any cryptographic operation is considered in the ns-2 simulation through the measurement of cryptographic library Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). In this study the group signature signing delay and verification delay are 3.6 ms and 7.2 ms, respectively, while the delay by an identity-based signature verification is 3.6 ms. We only consider the message loss caused by the security protocol rather than the wireless transmission channel. Note that the message will be lost if the queue is full when the message arrival rate is higher than the message verification rate.

In Fig. 4 it can be seen that with the increase of traffic load (i.e., the number of vehicles within the communication range), the message end-to-end delay does not vary a lot (around 22 ms), which is smaller than the maximum allowable message end-to-end transmission latency of 100 ms defined in [1]. In addition, the message loss ratio increases with the traffic load. It is notable that the loss ratio reaches as high as 68 percent when the traffic load is up to 150. However, such a traffic load can only be experienced when the road is in a severe traffic jam according to the relationship between the communication range and the intervehicle distance [1]. In this situation it is acceptable if a large number of messages are lost because most of the messages are repeatedly sent by each vehicle. Normal traffic conditions are experienced when the traffic load is below 50, where 20 percent loss ratio is achieved.

Another important factor that affects the performance of a security protocol is the latency taken by the cryptographic operations in the protocol. In the second experiment a normal traffic load in a city is considered, where on average 60 vehicles are within the communication range of a vehicle. Simulation results are

shown in Fig. 5. It can be seen that the message end-to-end delay and loss ratio increase when the cryptographic operation cost becomes larger. Also, the message loss ratio is significantly increased after the signature verification latency reaches a certain value. Furthermore, the performance under various road systems are very close. This demonstrates the stability and insensitivity of the proposed security protocol to different road systems and traffic loads.

Conclusions and Future Work

In this article a comprehensive review and state-of-the-art progress on industry standardization for security assurance and privacy preservation in VANETs have been presented. The solutions for achieving secure certificate revocation and conditional privacy preservation based on the PKI have been provided, which are the most imminent issues and functional blocks for creating a VANET with market readiness. For our future research, we plan to develop a suite of security mechanisms that not only preserve security and conditional privacy, but also provide fast anonymous authentication and privacy tracking with minimized secret storage and minimum cryptographic overhead.

For our future research, we plan to develop a suite of security mechanisms, which not only preserve the security and conditional privacy, but also provide fast anonymous authentication and privacy tracking with minimized secret storage and minimum cryptographic overhead.

References

[1] U.S. Dept. of Transportation, "National Highway Traffic Safety Administration, Vehicle Safety Communications Project — Final Report," Apr. 2006, http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm

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

[3] P. Wohlmacher, "Digital Certificates: A Survey of Revocation Methods," *Proc. ACM Wksp. Multimedia*, Los Angeles, CA, Oct. 2000, pp. 111–14.

[4] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *J. Computer Security*, Special Issue on Security, *Ad Hoc and Sensor Networks*, vol. 15, no. 1, 2007, pp. 39–68.

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

[6] D. Boneh, X. Boyen, and Hovav Shacham. "Short Group Signatures," *Proc. Advances in Cryptology — CRYPTO 2004*, Santa Barbara, CA, Oct. 2004, pp. 41–55.

[7] P. S. L. M. Barreto *et al.*, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," *Proc. Advances in Cryptology — ASIACRYPT 2005*, Taj Coromandel, Chennai, India, Dec. 2005, pp. 515–32.

[8] A. K. Saha and D. B. Johnson, "Modeling Mobility for Vehicular Ad Hoc Networks," *Proc. 1st Int'l. Wksp. Vehic. Ad Hoc Networks*, Philadelphia, PA, Oct. 2004, pp. 91–92.

Biographies

Xiaodong Lin (xdlin@bbcr.uwaterloo.ca) is currently working toward his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada, where he is a research assistant in the Broadband Communications Research (BBCR) Group. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Rongxing Lu (rxlu@bbcr.uwaterloo.ca) received B.Sc. and M.Sc. degrees in computer science from Tongji University, China, in 2000 and 2003, respectively. In 2006 he received a Ph.D. degree in computer science from Shanghai Jiao Tong University, China. Currently, he is a post-doctoral fellow at the University of Waterloo, Canada. His current research interests include wireless network security and cryptography. He is the co-recipient of the IEEE ICC 2007 Computer and Communications Security Symposium Best Paper Award.

Chenxi Zhang (c14zhang@engmail.uwaterloo.ca) received his B.Eng. and M.Eng. degrees from the Computer Science and Technology Department at the Harbin Institute of Technology, China, in 2003 and 2005, respectively. He is currently a Ph.D. student in the Department of Electrical and Computer Engineering at the University of Waterloo. His research interests include wireless network security and vehicular network security.

Haojin Zhu (h9zhu@bbcr.uwaterloo.ca) received a B.Eng. degree from Wuhan University, China, in 2002 and an M.Sc degree from Shanghai Jiao Tong University, China, in 2005, all in computer science. He is currently pursing his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo. His current research interests include wireless network security and applied cryptography.

Pin-Han Ho (pinhan@bbcr.uwaterloo.ca) received his Ph.D. from the ECE Department at Queen's University in 2002. He joined the ECE Department at the University of Waterloo as an assistant professor in 2002. His current research interests cover a wide range of topics in wired and wireless communication networks. He is the recipient of the Early Researcher Award in 2005, and Best Paper Awards at SPECTS '02, ICC '05 Optical Networking Symposium, and ICC '07 Computer and Communications Security Symposium.

Xuemin (Sherman) Shen (xshen@bbcr.uwaterloo.ca) is a professor of electrical and computer engineering and University Research Chair at the University of Waterloo. He received his Ph.D. in electrical engineering from Rutgers University, New Jersey, in 1990. His research interests include wireless/internet interworking, radio resource and mobility management, WLAN/WiMAX, UWB wireless communications, wireless ad hoc and sensor networks, and wireless network security.