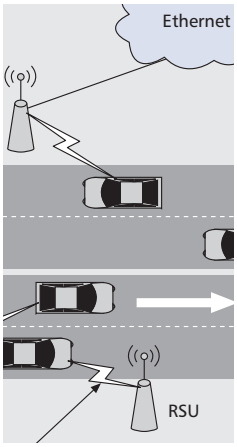
COMPLEMENTING PUBLIC KEY INFRASTRUCTURE TO SECURE VEHICULAR AD HOC NETWORKS

ALBERT WASEF AND RONGXING LU, UNIVERSITY OF WATERLOO
XIAODONG LIN, UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY
XUEMIN (SHERMAN) SHEN, UNIVERSITY OF WATERLOO



The authors propose a mechanism for mitigating the effect of DoS attacks in VANETs. Simulation results show that the complementary mechanisms together with PKI can efficiently secure VANETs.

ABSTRACT

Vehicular ad hoc networks are emerging as an effective technology for providing a wide range of safety applications to by-vehicle passengers. Ensuring secure operation is one of the prerequisites for deploying reliable VANETs. In this article we argue that public key infrastructure is the most viable mechanism for securing VANETs as it can meet most VANET security requirements. However, PKI cannot provide certain security requirements such as location privacy, efficient authentication, and distributed and fair revocation. To complement the security services provided by PKI, we introduce complementary security mechanisms that can meet the aforementioned security requirements. Since denial of service attacks have severe consequences on network availability, which is one of the VANET security requirements, we propose a mechanism for mitigating the effect of DoS attacks in VANETs. Simulation results show that the complementary mechanisms together with PKI can efficiently secure VANETs.

INTRODUCTION

Due to the foreseen impact of the vehicular ad hoc network (VANET) offering a variety of safety applications, extensive attention in industry and academia has been directed toward bringing VANETs into real life and standardizing network operation. As a result, IEEE developed the IEEE 1609 Wireless Access in Vehicular Environments (WAVE) standard for VANETs. Moreover, the American Society for Testing and Materials (ASTM) and IEEE have developed dedicated short-range communication (DSRC) as the basic vehicular communications technology, where DSRC has bandwidth of 75 MHz at 5.9 GHz frequency. Figure 1 shows the basic VANET network model, which mainly consists of vehicles or onboard units (OBUs), fixed infrastructure roadside units (RSUs) sparsely distributed all over the network, and a trusted authority (TA), which is responsible for providing security materials (certificates, keys, etc.) to all the entities in the network. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are two basic vehicular communication modes, which allow vehicles to communicate with each other or with RSUs, respectively.

In VANET safety-related applications, drivers may take life-critical actions based on messages received from other vehicles. However, any malicious behavior of a user, such as injecting false information, or modifying and replaying the disseminated messages, could be fatal to other users. In addition, users are very conservative about their privacy-related information. For example, users will not accept having their driving routes unconditionally accessed by the public. Therefore, security and privacy preservation are among the critical challenges in the deployment of VANETs. To satisfy the security and privacy requirements, it is prerequisite to elaborately design a suite of mechanisms to achieve security and privacy preservation for practical VANETs.

In this article we first identify the requirements to secure VANETs, and argue that public key infrastructure (PKI) is the most viable solution to secure VANETs. We also point out some limitations of PKI in securing VANETs. We then introduce a set of mechanisms to mitigate the limitations of PKI. Since denial of service (DoS) attacks have severe consequences on network availability, which is one of the VANET security requirements, we propose a novel mechanism that can mitigate the effect of this type of attacks.

SECURING VANETS

In order to secure VANETs, the following security requirements should be met [1]:

- Authentication: Entity authentication is required to ensure that the communicating entities are legitimate. In addition, data authentication is also a concern to ensure that the contents of the received data is neither altered nor replayed.
- Non-repudiation: Non-repudiation is necessary to prevent legitimate users from denying the transmission or contents of their messages.

1536-1284/10/$25.00 © 2010 IEEE

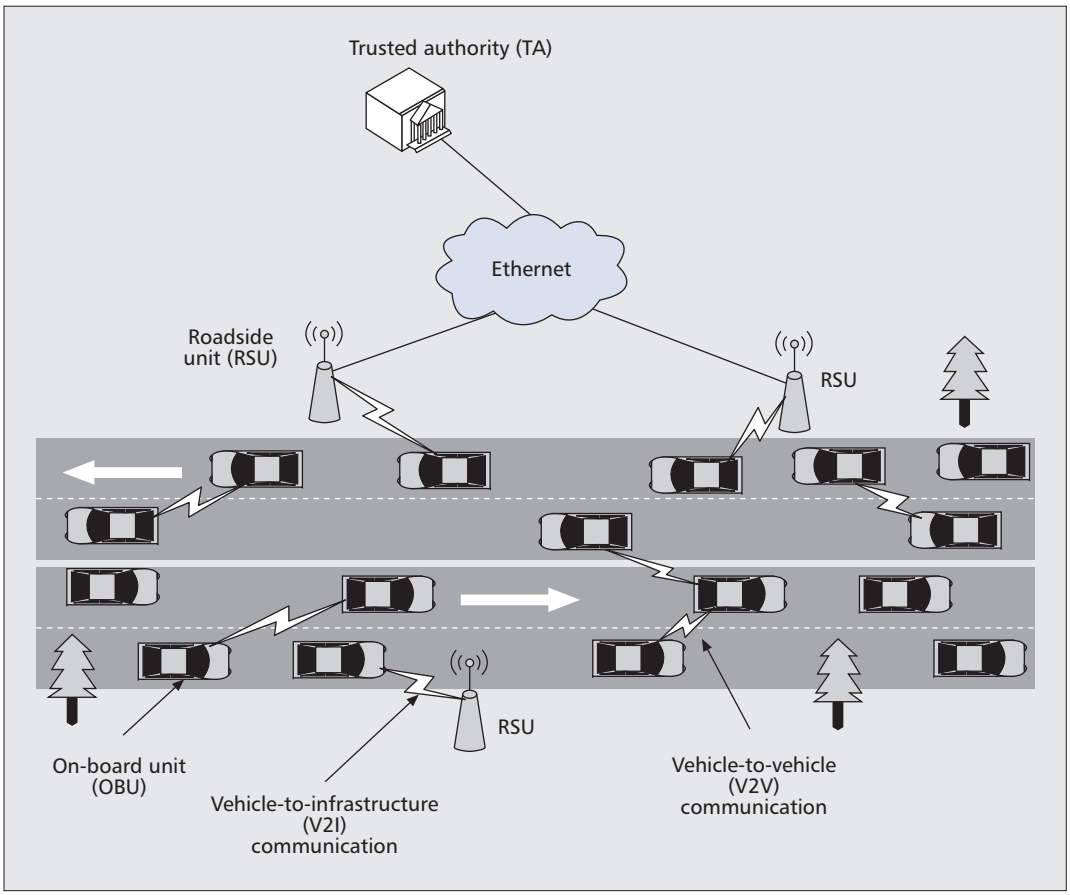


Figure 1. *Basic VANET network model.*

- Privacy: Preserving users' privacy is mainly related to preventing disclosure of their real identities and location information.
- Access control: Access control is necessary to define the operations that each entity in the network can perform. In addition, any misbehaving entity should be revoked from the network to protect the safety of other legitimate entities in the network. Moreover, any actions taken by that misbehaving entity should be repealed.
- Availability: Users may be frustrated if VANET services become temporarily unavailable due to attacks such as DoS attacks.

In this section, we argue that PKI is the most viable mechanism for securing VANETs as it can meet most VANET security requirements. In addition, we identify some limitations of PKI.

Employing PKI to Secure VANETs

The security requirements of data authentication and non-repudiation can be achieved by employing digital signatures. Implementing digital signatures can be achieved via asymmetric cryptography where each entity has a public/private key pair. Any entity can use its unique private key to generate a unique digital signature for an outgoing message. When a signed message is received, the recipient uses the sender's public key to verify the digital signature of the sender of the message. Successful digital signature verification implies that the content of the message is not altered, and only the sender can generate this message (i.e., achieving data authentication and non-repudiation). For entity authentication, the public key of each entity must be authentic to all the entities in the network. Therefore, securing VANETs requires PKI, where a TA generates an authentic certificate for each entity in the network binding the entity's public key to its identity.

Access control can be achieved by defining the permitted actions for each entity in the attributes of its certificate. Furthermore, revocation can be achieved by employing certificate revocation lists (CRLs), which contain the certificate identities of misbehaving nodes. Before verifying any received message, each node checks whether or not the sender is included in the up-to-date CRL.

Intuitively, complete privacy preservation can achieve users' privacy. However, it is a double-edged sword and shown to be unsuitable for VANETs, since an attacker could abuse it to cover malicious behaviors. Therefore, conditional privacy preservation is of vital importance to secure vehicular communications, which can be achieved by employing anonymous certificates. Since anonymous certificates do not contain any information about the real identity of the certificate holder, vehicles can authenticate each other while preserving their privacy, and only the TA has the ability to identify the real identity of a vehicle from its anonymous certificate.

Intuitively, complete privacy preservation can achieve users' privacy. However, it is a double-edged sword and shown to be unsuitable for VANET, since an attacker could abuse it to evade the malicious behaviors.

There is a necessity for mechanisms that can accelerate the authentication in PKI to ensure reliable VANETs. Therefore, besides PKI, additional security mechanisms providing location privacy, distributed and fair revocation, and efficient authentication are required to efficiently secure VANETs.

Limitations of PKI

PKI has some limitations in securing VANETs.

Privacy — Although anonymous certificates in PKI can guarantee identity privacy, they cannot support location privacy. If a vehicle changes its certificate between two observation points controlled by an attacker while moving in the same lane and with the same speed on the road, an attacker can correlate the certificates used by that vehicle and hence track the vehicle. In addition, the anonymity set is defined as the set of vehicles changing their anonymous certificates between two observation points launched by an attacker. If the anonymity set size of a vehicle changing its certificate is one, an attacker is capable of tracking it. Accordingly, a mechanism for ensuring location privacy is needed to overcome this PKI limitation.

Revocation — To revoke a vehicle in PKI, a CRL has to be issued by the TA (i.e., centralized revocation) and broadcast by the infrastructure RSUs. The network scale of VANETs is expected to be very large. Hence, the distribution of CRLs is prone to long delays. In addition, during the early deployment of VANETs, it is expected that RSUs will be sporadically distributed in the network. In practice, revocation of misbehaving vehicles should take place as fast as possible to prevent these vehicles from jeopardizing the safety of other vehicles.

Fair revocation is also a concern to avoid revoking innocent vehicles. For example, if vehicle A broadcasts disputed message M due to an unintentional misoperation, and other vehicles immediately report M to the TA, vehicle A will be revoked by the TA. Obviously, this is unfair to vehicle A. Therefore, revocation policies in VANETs should be further explored from coarse-grained to fine-grained.

Efficient Authentication — According to DSRC, each vehicle has to broadcast a message, which includes its current position, speed, and other telematic information, every 300 ms. In such a scenario each vehicle may receive a large number of signed messages every 300 ms. The ability for each vehicle to check CRL for a large number of certificates and verify the senders' signatures on the received messages in a timely manner forms an inevitable challenge to VANETs, especially in the context of PKI where these processes may take a long time. Hence, there is a necessity for mechanisms that can accelerate the authentication in PKI to ensure reliable VANETs.

Therefore, besides PKI, additional security mechanisms providing location privacy, distributed and fair revocation, and efficient authentication are required to efficiently secure VANETs.

Complementing PKI to Efficiently Secure VANETs

In this section we present a set of mechanisms complementing the security services offered by PKI for VANETs.

Complementing Privacy

We address the problem of location privacy in order to complement the privacy provided by PKI.

Location Privacy — Several works in the literature has addressed the problem of location privacy in VANETs. Sampigethaya *et al*. [2] proposed to use random silent periods where each vehicle opts to remain silent for a random period to protect its location privacy. This method is suitable for VANET applications excluding safety applications, as safety applications require vehicles to periodically transmit safety messages.

Freudiger *et al*. [3] used Cryptographic MIX-zones (CMIX) to provide location privacy. In CMIX an RSU at a selected road intersection establishes a group key with the vehicles entering the intersection. The group key shared between all the vehicles in the intersection is used to encrypt all the communications in that intersection to create a CMIX. In addition, all the vehicles in the CMIX are forced to change their certificates. As a result of the forced certificate change and random direction change of each vehicle at road intersections, an attacker on the roadside cannot link a certificate to a particular vehicle, hence providing location privacy.

We have proposed achieving location privacy by using random encryption periods (REPs) [4], where a vehicle changing its certificate surrounds itself with an encrypted communication zone using group communications until it ensures that all the conditions to be tracked are violated. Only unrevoked vehicles in this zone can decrypt the communication using the shared group key. In this way an outsider attacker[1] will not be able to capture the messages broadcast by the vehicles as the outsider attacker does not have the group key. The encrypted communications zone continues until sufficient ambiguity about which vehicle changed its certificate is created to confuse the attacker. To evaluate REP, we simulate a Manhattan mobility model using Matlab, where vehicles arrive according to a Poisson process at a rate of 50 vehicles/s. In the simulation each street consists of four lanes (two in each direction). Figure 2 shows a comparison of the ratio between the anonymity sets of different sizes and the total number of anonymity sets for the case without and with REP, and with CMIX. It should be noted that as the size of the anonymity set increases, the probability of tracking a vehicle decreases. It can be seen that without using REP, the anonymity sets of size one are 100 percent of the total anonymity sets. Also for CMIX, only 18.18 percent of the total anonymity sets achieves set size greater than one, while 81.82 percent of the anonymity sets still have size one at the end of the simulation.

Complementing Revocation

We study distributed and fair revocation in order to complement the revocation provided by PKI.

Distributed Revocation — Raya *et al*. [5] addressed the problem of local revocation where they proposed an eviction technique consisting of the fol-

[1] *An outsider attacker is one who does not possess any authentic security credentials (e.g., certificates, keys).*

lowing components: localized misbehavior detection system (MDS) and local eviction of attackers by voting evaluators (LEAVE). MDS and LEAVE enable the neighboring vehicles of a misbehaving vehicle to locally quarantine the misbehaving vehicle until a centralized revocation decision is issued by the TA. In addition, Raya *et al*. employed game theory to model the local revocation of an accused vehicle as a game between the neighboring vehicles of the accused vehicle [6]. Moreover, they developed a local revocation game for VANETs considering the high mobility of the vehicles.

We have proposed an efficient decentralized revocation (EDR) protocol for VANETs, which enables a group of neighboring vehicles to completely revoke a nearby misbehaving vehicle [7]. The EDR protocol is based on a secret sharing scheme, where a master secret key is divided mathematically into a number of shadows (or simply parts), and the shadows are probabilistically distributed to all the vehicles. When a vehicle misbehaves, one of its neighboring vehicles acts as a revocation coordinator and sends a revocation of the misbehaving vehicle request to the neighboring vehicles. Each vehicle of the neighboring vehicles uses its shadow to calculate a revocation share and forwards it to the revocation coordinator. The revocation shares are calculated in such a way that it is infeasible to recover the shadows used in calculating the revocation shares. Then the revocation coordinator combines all the shares to generate a revocation message to completely remove the misbehaving vehicle from the network. EDR is independent of the RSUs and the TA, which makes it suitable for the early deployment phase of VANETs, where a non-uniform RSU distribution is expected. Also, EDR distributes the revocation load to all the vehicles, thus avoiding overwhelming the TA. Moreover, it achieves fast revocation of misbehaving vehicles, thus decreasing the time window in which a misbehaving vehicle can broadcast malicious messages. EDR can be used as a standalone revocation protocol or integrated with the CRL technique to compensate for the absence of RSUs in some areas.

We conduct Network Simulator-2 (NS-2) simulation for revocation scenarios, using EDR and the centralized revocation employing CRL, triggered by a vehicle at three different locations: location1, location2, and location3 corresponding to initial distances of 2.7 km, 4.7 km, and 10.3 km, respectively, from the TA at the beginning of the simulation. The revocation process is triggered every 10 s during the simulation, and the corresponding revocation delay is measured. Figure 3 shows the conventional CRL revocation delay T_{CRL} and the EDR revocation delay T_{EDR} in milliseconds vs. the simulation time. The CRL revocation delay T_{CRL} is the delay between sending a revocation request to the TA from one of the neighboring vehicles of a misbehaving vehicle until the new CRL is broadcast in the geographic area containing the misbehaving vehicle. The EDR revocation delay T_{EDR} is the delay from the moment the revocation coordinator issues a revocation request until the revocation message of the misbehaving vehicle is broadcast in the geographic area containing the misbehaving vehicle. It can be seen from Fig. 3 that T_{EDR} is almost the same for the three locations, and is confined within the range of 21–35 ms. This is due to the fact that the proposed protocol is independent of the TA. On the other hand, it can be seen that T_{CRL} increases with distance from the TA. Consequently, the delay saving of the proposed EDR protocol compared to conventional CRL revocation increases with distance from the TA. It should be noted that T_{EDR} and T_{CRL} correspond to the vulnerability window a misbehaving vehicle has until it is revoked for EDR and CRL, respectively. During the vulnerability window, the misbehaving vehicle can still jeopardize the safety of neighboring vehicles. It can be seen that EDR has a smaller vulnerability window than the CRL technique, which increases the safety level in VANETs.

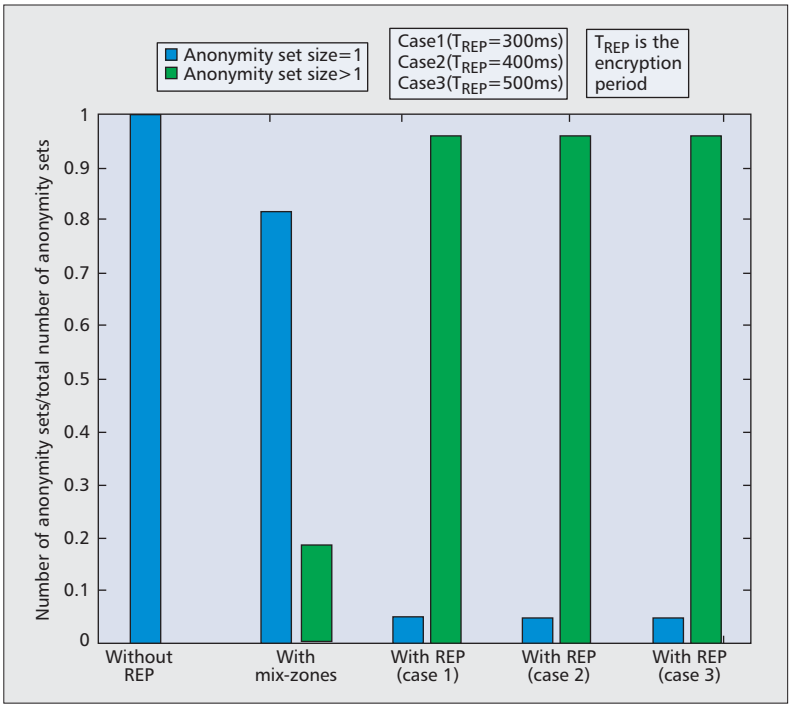


Figure 2. *The impact of REP on the anonymity set size for the Manhattan mobility model.*

Fine-Grained Revocation Policy in VANETs — We have proposed an efficient privacy-preserving communication scheme with blacklists, named PPCB, for vehicular communications [8]. Briefly stated, in PPCB each vehicle maintains a blacklist which records all *identifiers* of other vehicles that are temporarily locally blocked by the vehicle. Here, the identifier does not refer to the real identity; instead, it is one kind of local link information. The vehicle can use it to check whether another vehicle could contact it within a time period. At the same time, the local blacklist cannot be shared with other vehicles, so unlinkability can still be provided, which is fair to another vehicle *B* if *B* only does one misoperation occasionally. In order to identify the real malicious vehicles, the TA will periodically collect blacklists from all vehicles. From these blacklists, the TA can reveal the real identities of these suspicious vehicles. If the same real identity appears in the blacklists

more than a threshold, the TA will revoke the vehicle; otherwise, the vehicle's behavior is recognized as malfunctioning, not malicious.

Complementing Authentication Efficiency

In order to complement the authentication capabilities provided by PKI, we introduce mechanisms to accelerate the main processes of the authentication, which are the revocation status check and signatures verification processes, respectively.

Accelerating the Revocation Status Check Process — In a certificate-based authentication system such as PKI, the authentication of a received message is performed by checking that the sender's certificate is not included in the current CRL and verifying the sender's signature. Since the number of vehicles in VANETs is in millions, and each vehicle possesses a number of certificates to protect its identity privacy, the size of the CRL maybe very large, which could result in long delays to check the revocation status of a sender.

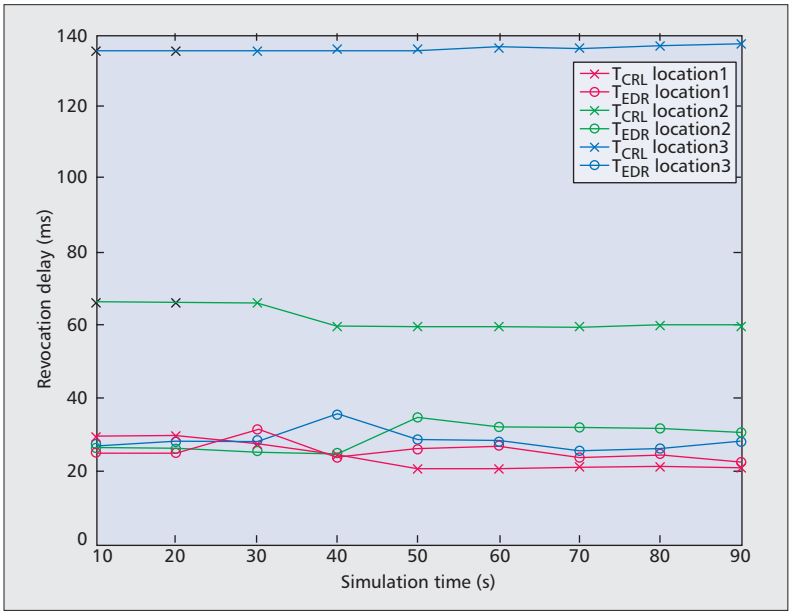


Figure 3. *The revocation delay for different revocation scenarios.*

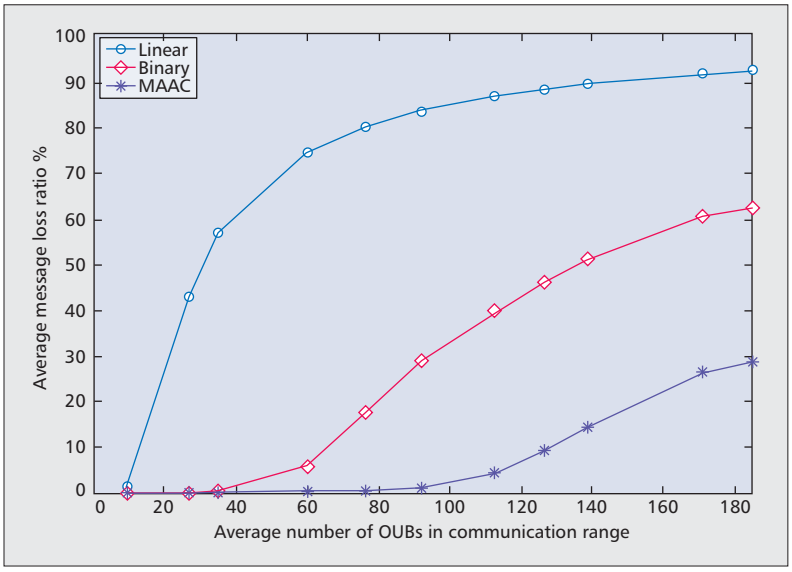


Figure 4. *Comparison of message loss ratios for different schemes.*

We have proposed the Message Authentication Acceleration (MAAC) protocol for VANETs [9], which replaces the time-consuming CRL checking process by an efficient revocation check process. The revocation check process uses a fast keyed hash message authentication code (HMAC), which deterministically generates a fixed size unique output for an arbitrary block of data using some secret key. HMAC is easy and efficient to calculate but computationally infeasible to invert. In MAAC, the key used in calculating the HMAC is a group key shared only between unrevoked vehicles. When a vehicle broadcasts a message, it appends to the message an HMAC, calculated using the shared group key, as proof that it has not been previously revoked. The recipient vehicle calculates its own HMAC on the received messages using its group key and compares the received HMAC with the calculated one. If a match occurs, the sender is not previously revoked since the secret key is shared only between unrevoked vehicles and vice versa. Thus, MAAC can avoid the need to check the CRL, hence alleviating the effect of the long delay to check the revocation status of senders. Through simulations, it is demonstrated that MAAC can accelerate the message authentication.

A direct impact of improving the authentication efficiency in MAAC is improving the message loss ratio is incurred due to the authentication computation overhead. To evaluate the improvement in message loss ratio, we conduct simulations using NS-2 for a city street scenario. The simulation area is 7.4 km × 7.4 km, and the maximum speed of the vehicles is 60 km/h. We are interested in the average message loss ratio, which is defined as the average ratio between the number of messages dropped every 300 ms, due to the message authentication delay, and the total number of messages received every 300 ms by a vehicle. Figure 4 shows the average message loss ratio vs. average number of vehicles within the communication range of each vehicle for message authentication employing CRL linear check, CRL binary check, and MAAC, respectively, for a CRL containing 20,000 certificates. It can be seen that the message loss ratio increases with the number of vehicles within communication range for all the schemes under consideration. Also, message authentication employing MAAC significantly decreases the message loss ratio compared to that employing either the linear or binary CRL revocation status check. The reason for the superiority of MAAC is that it incurs the minimum revocation status check delay compared to the linear and binary CRL revocation check processes.

Accelerating the Signature Verification Process — To accelerate the signature verification process in VANETs, we have developed an efficient online/offline signature scheme[10]. The online/offline signature can divide the signature generation procedure in two phases. The first phase is executed offline (which is irrelevant to the message to be signed), and the second phase is performed online (after the message to be signed is

given). Since the online/offline signature casts costly computations executed in the offline phase, the online phase is typically very fast. However, the signature verification in existing online/offline signature schemes is comparatively slow. For example, the typical online/offline RSA signature requires an additional modular exponentiation operation $g^{m \cdot r} \bmod n$ in the verification phase. Different from these previously reported schemes, our online/offline Rabin signature is efficient in both signing and verification phases (i.e., the online phase only requires four modular multiplications [Mu] and one modular square [Sq], and the verification algorithm also only requires $6Mu + 3Sq$. Therefore, it can accelerate the authentication process in VANETs.

Table 1 presents the measured running time for 1024-bit RSA signature, the online/offline RSA signature, and the online/offline Rabin schemes [10], which are tested on an Intel Pentium III 1.4 GHz machine. From the table, we can see the fast verification of the online/offline Rabin scheme makes it more suitable for the efficient authentication required in VANETs.

Signature	RSA (e = 65,537)	Online/offline RSA (e = 65,537)	Online/offline Rabin
(Online) signing	52.235 ms	0.002 ms	0.011 ms
Verification	0.811 ms	54.023 ms	0.020 ms

Table 1. *Measured running time.*

Mitigating the Effect of DoS Attacks

An outsider attacker can launch a DoS attack by continuously broadcasting invalid signatures to exhaust other legitimate vehicles and prevent them from processing other messages received from legitimate users. The effect of this kind of attack is devastating to the network, and it may completely hinder the vehicular communication.

In this section we propose a mechanism for mitigating the effect of this kind of DoS attacks as follows.

The Proposed Mechanism

In order to mitigate the effect of the aforementioned type of DoS attacks, we propose that each vehicle keeps tracking of all the invalid signatures received in period ΔT. Then each vehicle calculates the invalid signature ratio as the ratio between the number of invalid signatures in ΔT and the total number of received messages in ΔT. When the invalid signatures ratio in a vehicle reaches a threshold predefined by the TA during system initialization, the vehicle starts to append HMAC to all outgoing signed messages. The HMAC is calculated on every outgoing message using a group key, which can be efficiently established in a VANET using the technique proposed in [9] shared between the unrevoked vehicles. Upon receiving a message, each vehicle calculates HMAC on the received message using its group key, and compares the calculated with the received HMAC. If there is a match, the vehicle continues to verify the signature on the message. If a mismatch occurs, the vehicle drops the message immediately. When the ratio of invalid signatures falls below the threshold in a vehicle, it stops appending the HMAC to outgoing messages.

The delay of using the Secure Hash Algorithm-1 (SHA-1) as the HMAC function is 0.42 μs. However, the delay of verifying a signature using the Elliptic Curve Digital Signature Algorithm (ECDSA), which has been adopted by the WAVE standard, is 2.4 ms. Figure 5 shows the

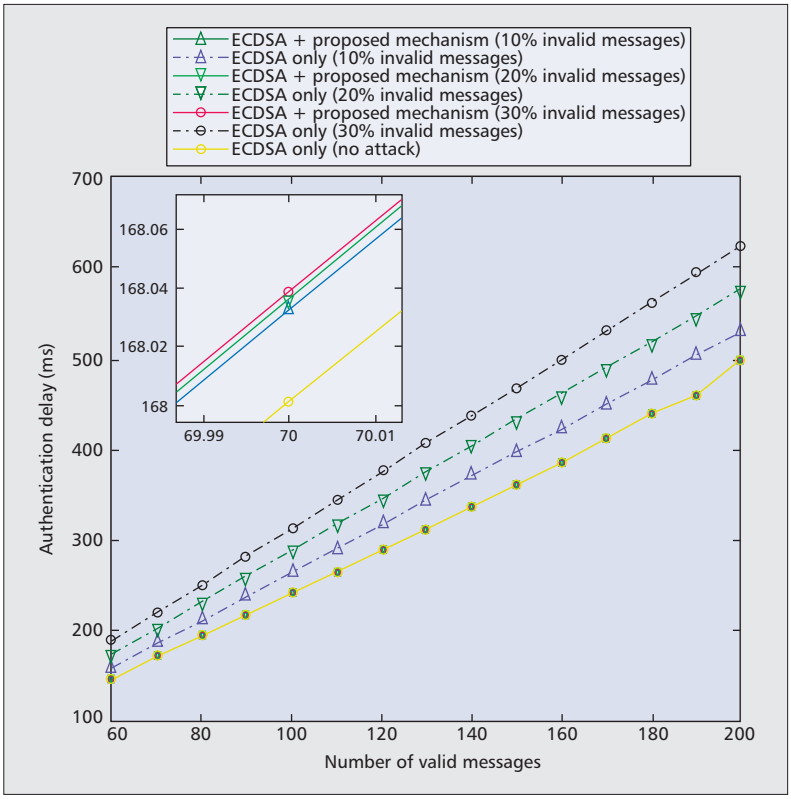


Figure 5. *Authentication delay under different scenarios.*

authentication delay in milliseconds vs. the number of valid messages for three scenarios:

- DoS attack where ECDSA and the proposed mechanism are employed for authentication.
- DoS attack where ECDSA only is employed for authentication.
- There is no attack (i.e., all the messages are valid), where ECDSA is employed for authentication.

In the DoS attack scenarios we consider an attacker contaminating the communicated messages by adding a number of invalid messages to be equal to 10, 20, and 30 percent of the number of valid messages, respectively. It can be seen that the invalid messages in the DoS attack scenario where ECDSA and the proposed mechanism are employed have a slight effect on the authentication delay compared to the scenario where there is no DoS attack. However, the invalid messages in the DoS attack scenario where only ECDSA is employed have a significant impact on the authentication delay. In addition, appending HMAC to the messages enables the vehicles to more quickly detect and drop the invalid signatures than in the case where only signatures are appended to the messages and the

The presented solutions for location privacy can protect the location privacy of vehicles against outsiders. How to protect the location privacy of vehicles against legitimate insiders in traditional certificate-based PKI is still an open research issue.

recipients have to verify the signatures. Consequently, the proposed mechanism can mitigate the effect of DoS attacks.

Conclusion and Open Research Issues

In this article, we have presented a number of security mechanisms to complement the PKI security services for privacy, efficient authentication, and revocation. Furthermore, we have proposed a mechanism for efficiently mitigating the effect of a DoS attack.

The presented solutions for location privacy can protect the location privacy of vehicles against outsiders. How to protect the location privacy of vehicles against legitimate insiders in traditional certificate-based PKI is still an open research issue. Also, mitigating the impact of DoS attacks launched by insider attackers is an important research issue as insider attackers can generate authentic signatures, and it will be difficult for other vehicles to detect this type of DoS attack. In addition, the problem of efficiently distributing the revocation information (e.g., CRL) to the vehicles in VANETs is a challenging issue as the network scale is very large. Another challenging topic is building a global reputation-based system while supporting privacy preservation because preserving the privacy of users requires frequent identity changes. Consequently, linking the reputation of a user to all its identities may contradict preserving the privacy of that user.

References

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

[2] K. Sampigethaya *et al.*, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE JSAC*, vol. 25, no. 8, 2007, pp. 1569–89.

[3] J. Freudiger and M. Raya, "Mix-Zones for Location Privacy in Vehicular Networks," *Proc. WiN-ITS*, Aug. 2007.

[4] A. Wasef and X. Shen, "REP: Location Privacy for VANETs using Random Encryption Periods," *ACM Mobile Net. Apps.*, vol. 15, no. 1, 2010, pp. 172–85.

[5] M. Raya *et al.*, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE JSAC*, vol. 25, 2007, pp. 1557–68.

[6] M. Raya *et al.*, "Revocation Games in Ephemeral Networks," *Proc. 15th ACM CCS*, 2008, pp. 199–210.

[7] A. Wasef and X. Shen, "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 58, no. 9, 2009, pp. 5214–24.

[8] R. Lu *et al.*, "PPCB: Privacy-Preserving Communications with Blacklists for Vehicular Communications," Tech. Rep. BBCR 2009-12, Univ. Waterloo, Canada, Dec. 2009.

[9] A. Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," *Proc. IEEE GLOBECOM '09*, 2009.

[10] R. Lu *et al.*, "Accelerating Authenticated Emergence Message Propagation to Mitigate Chain-Reaction Accidents in Highway Traffic," *Proc. CHINACOM '09*, 2009.

Biographies

ALBERT WASEF [S'09] (awasef@bbcr.uwaterloo.ca) received a B.Sc.(1998) degree and an M.Sc.(2003) from El Menoufia University, Egypt, both in electrical communications engineering. He 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 working with the Broadband Communications Research (BBCR) Group. His research interest includes wireless network security, privacy preservation in vehicular networks, and group communications.

RONGXING LU [S'09] (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 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. degree in information engineering from Beijing University of Posts and Telecommunications, China, in 1998 and a Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

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 served 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.