MLAS: Multiple Level Authentication Scheme for VANETs

T.W. Chim
Department of Computer Science
The University of Hong Kong
twchim@cs.hku.hk

S.M. Yiu
Department of Computer Science
The University of Hong Kong
smyiu@cs.hku.hk

Lucas C.K. Hui
Department of Computer Science
The University of Hong Kong
hui@cs.hku.hk

Victor O.K. Li
Department of Electrical and Electronic Engineering
The University of Hong Kong
vli@eee.hku.hk

ABSTRACT

The vehicular ad hoc network (VANET) is an emerging type of network which enables vehicles on roads to intercommunicate for driving safety. The basic idea is to allow arbitrary vehicles to broadcast ad hoc messages (e.g. traffic accidents) to other vehicles. However, this raises the concern of security and privacy. Messages should be signed and verified before they are trusted while the real identity of vehicles should not be revealed, but traceable by authorized party. Existing solutions either rely too heavily on a tamper-proof hardware device, or do not have an effective message verification scheme. In this paper, we propose a multiple level authentication scheme which still makes use of tamper-proof devices but the strong assumption that a long-term system master secret is preloaded into all tamper-proof devices is removed. Instead the master secret can be updated if needed to increase the security level. On the other hand, messages sent by vehicles are classified into two types - regular messages and urgent messages. Regular messages can be verified by neighboring vehicles by means of Hash-based Message Authentication Code (HMAC) while urgent messages can only be verified with the aid of RSUs nearby by means of a conditional privacy-preserving authentication scheme.

Keywords

Secure vehicular sensor network, message classification, authentication, batch verification, proxy re-encryption

1. INTRODUCTION

The vehicular ad hoc network (VANET) is an emerging type of network by which driving safety can be enhanced through inter-vehicle communications or communications with roadside infrastructure. It is an important element of the Intelligent Transportation Systems (ITSs) [10]. In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the backend. The OBUs and RSUs communicate using the Dedicated Short Range Communication (DSRC) protocol [8] over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g. the Internet). The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road condition, traffic accident information) to other nearby vehicles and RSU such that other vehicles may adjust their travelling routes and RSU may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. This paper focuses on inter-vehicle communications.

Like other communication networks, security issues have to be well-addressed. For example, the message from an OBU has to be integrity-checked and authenticated before it can be relied on. Otherwise, an attacker can modify a vehicle's safety message or even impersonate a vehicle to transmit a fake safety message. For example, a boy may impersonate an ambulance to request other vehicles to give way to him or request nearby RSUs to change traffic lights to green so that he can catch up an appointment with his girl friend. Besides, privacy is another issue that raises a lot of concern in recent years. A driver may not want others to know its travelling routes by tracing messages sent by its OBU. Someone may argue that in current road system, a vehicle can already be traced by means of its license plate number. However, most parts of VANET are automatic (e.g. the status of a vehicle will be broadcasted by its OBU periodically and automatically) and such an automatic messaging system should not leak a driver's privacy any easier than the current situation. Thus an anonymous communications protocol is needed. While being anonymous, a vehicle's real identity should be able to be revealed by a trusted party when necessary. For example, the driver who sent out fake messages causing an accident should not be able to escape by using an anonymous identity. Thus we call this kind of privacy conditional privacy.

Privacy-preserving authentication schemes have been discussed in the research community for a while. Examples include [13], [12] and [6]. However, all of them propose hav-

ASIACCS '11, March 22–24, 2011, Hong Kong, China.

ing the same treatment to all messages. This is obviously improper. Some messages are more urgent than others. In fact, in daily operation of a VANET, more than 90% of messages are regular (non-urgent) messages such as those about change of travelling speed and turning direction. Urgent messages only appear when there are accidents or unexpected road conditions. Therefore, adopting the same authentication scheme (and with the same security level) to both regular and urgent messages usually yields a waste of power. In this paper, we propose to first classify messages sent by a vehicle into regular messages and urgent messages. Regular messages refer to those that are sent periodically (every 500 msec according to the DSRC [8] standard). They are usually about the current status of a vehicle including its travelling speed, turning direction and brake application. Urgent messages, on the other hand, refer to those that are sent when there are critical road situations such as accidents and road blocking. Messages sent by a fire engine or an ambulance are also considered as urgent since slowing down their travelling speed can cause loss of human life or property. We then propose different treatments on the two kinds of messages. For regular messages, the receiving vehicle only needs to show that they were generated and sent by a trusted tamper-proof device while for urgent messages, we provide a mechanism for a trusted party to reveal the real identity of the sender. That is, attacks caused by a vehicle are accountable.

Talking about tamper-proof devices, some existing schemes also assume the existence of them. However, their security assumption is too strong to be accepted. They assume that a long-term master secret key is preloaded into all tamper-proof devices and all security functions rely on it. In this sense, once one of the temper-proof devices is cracked and the system master secret is leaked to an attacker, the whole system will be compromised. In this paper, we use tamper-proof devices with a weaker security assumption. We still need a system master secret for security functions. However, instead of preloading them into tamper-proof devices permanently, we propose to transmit them to vehicles in a secure way. Also the system master secret can be updated when any tamper-proof device is proved to be compromised. This can help to raise the security level of the system. Through security analysis, we show that our schemes achieve the goals of authenticity, conditional privacy preserving and traceability.

The remainder of this paper is organized as follows. Related works are presented in Section 2. The system model and the problem statement are described in Section 3. Our schemes are presented in details in Section 4. The security analysis of our scheme is given in Sections 5. Finally, Section 6 concludes the paper.

2. RELATED WORK

In terms of integrity-checking and authentication, digital signature in conventional public key infrastructure (PKI) [7] is a well accepted choice. However, requiring a vehicle to verify the PKI signatures of other vehicles by itself as in works like [9] induces two problems as mentioned in [12]. First, the computation power of an OBU is not strong enough to handle all verifications in a short time, especially in places where the traffic density is high. Second, to verify a message from an unknown vehicle involves the transmission of a public key certificate which causes heavy message overhead. Therefore, one possible approach is to let the nearby RSU to help a vehicle to verify the message of another.

Related problems have been addressed in some recent works [12, 13, 11, 5]. In [13], the IBV protocol was proposed for vehicle-to-RSU communications. The RSU can verify a large number of signatures as a batch using three *pairing* operations (see works like [13] and [6] for what a pairing operation is). However, their work relies heavily on a tamper-proof hardware device, installed in each vehicle, which preloads the system-wide secret key. Once one of these devices is cracked, the whole system will be compromised. On the other hand, by actual implementation, we found that batch verification is not as efficient as they argue. Finally, the IBV protocol is not designed for vehicle-to-vehicle communications. In a more recent work [12], the RAISE protocol was proposed for vehicle-to-vehicle communications. The protocol is software-based. It allows a vehicle to verify the signature of another with the aid of a nearby RSU. To notify other vehicles whether a message from a certain vehicle is valid, a hash value of 128 bytes needs to be broadcasted. There can be tens up to thousands of signatures within a short period of time, thus the notification messages induce a heavy message overhead. In another recent work, SPECS [6], some security and privacy-enhancing communications schemes were proposed. Of particular interest, a group communications protocol was defined. After a simple handshaking with any RSU, a group of known vehicles can verify the signature of each other without any further support from RSUs. A common group secret is also developed for secure communications among group members.

Regarding conditional privacy preserving, some recent works such as [5] propose to achieve the goal by using group signature schemes. That is, each vehicle in the system is assigned a group private key. When a vehicle wants to broadcast a message, it signs the message using its group private key. Verifiers such as RSUs can then verify its signature using a common group public key. In this way, a signature can be properly verified but at the same time, the real identity of the signer can be hidden. Only if necessary, a trusted party can use a private key to reveal the real identity of the signer. Though conditional privacy preserving can be achieved, we argue that such group signature schemes are complicated and inefficient.

3. PROBLEM STATEMENT

This section explains our system model, assumptions and security requirements.

System model and assumptions: Recall that a vehicular network consists of on-board units (OBUs) installed on vehicles, road-side units (RSUs) along the roads, and a trusted authority (TA). We focus on the inter-vehicle communications over the wireless channel. We assume the followings:
1) The TA is trusted and is online periodically and when needed for updating system master secret key. RSUs and TA communicate through a secure fixed network. To avoid being a single point of failure or a bottleneck, redundant TAs which have identical functionalities and databases are installed.
2) The RSUs have higher computation power than OBUs.
3) The RSU to Vehicle Communication (RVC) range is at least twice of the Inter-Vehicle Communication (IVC) range. In this way, all vehicles receiving the same message as the RSU are in the feasible range to receive the notification from the RSU.

4) There exists a conventional public key infrastructure (PKI) for the distribution of system master secret. We will talk about the details in Section 4.1.
5) The real identity of any vehicle is only known by the TA and itself but not by others.

Security requirements: We aim at designing a scheme to satisfy the following security requirements:
1) *Message integrity and authentication*: Whenever a vehicle sends a message, any other vehicle should be able to verify that the message is indeed sent and signed by an authorized tamper-proof device without being modified by anyone. At the same time, any RSU and TA together should be able to verify that the message is indeed sent and signed by a registered vehicle without being modified by anyone. They can then inform other vehicles the verification result.
2) *Identity privacy preserving*: The real identity of a vehicle should be kept anonymous from other vehicles and a third-party should not be able to reveal a vehicle's real identity by analysing multiple messages sent by it.
3) *Traceability and revocability*: Although a vehicle's real identity should be hidden from other vehicles, if necessary (e.g. in case of urgent messages), the TA should have the ability to obtain a vehicle's real identity.

4. OUR SOLUTIONS - MLAS

In this section, we discuss our solution - Multiple Level Authentication Scheme (MLAS) for VANETs in details. Our scheme contains six basic modules and we will describe them one by one.

Throughout this section, we denote the process of encrypting plaintext M with public key PK to obtain ciphertext C as $C = AS\_ENC_{PK}(M)$. We denote the HMAC value generated on message M using the secret key K as $HMAC_K(M)$. For the process of signing message M by TA with its private key TSK to obtain signature σ, we denote it as $\sigma = TSIG_{TSK}(M) = TSK \times H(M)$ where $H(.)$ is a MapToPoint hash function [4] which in turns relies on hash functions like SHA-3 [1] since SHA-1 or MD-5 have been proved to be useless in providing the reasonable level of security recently. The receiver can then verify σ by checking whether $\hat{e}(\sigma, P) = \hat{e}(H(M), TRID)$ where P is a public parameter while $TRID = TSK \times P$ is the public key corresponding to TSK.

4.1 Setup by TA

During system startup, TA chooses the groups $\mathbb{G}$ (with P as the generator) and $\mathbb{G}_\mathbb{T}$ that satisfy the bilinear map properties:
1) *Bilinear*: $\forall P, Q, R \in \mathbb{G}$ and $\forall a, b \in \mathbb{Z}$, $\hat{e}(Q, P+R) = \hat{e}(P+R, Q) = \hat{e}(P, Q) \cdot \hat{e}(R, Q)$. Also $\hat{e}(aP, bP) = \hat{e}(P, bP)^a = \hat{e}(aP, P)^b = \hat{e}(P, P)^{ab}$.
2) *Non-degenerate*: There exists $P, Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_\mathbb{T}}$.
3) *Computable*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}$.

TA gives itself an identity $TRID$ and a secret key TSK. $TRID$ is assumed to be known by everyone in the system. TA assigns each RSU R_i an identity $RRID_i$ and a secret key RSK_i. $RRID_i$ as well as the location of the RSU are made public in advance (e.g. stored in a local map database).

During the first registration of a vehicle, TA assigns each vehicle V_i a real identity $VRID_i = xP$ where x is a random number, and a tamper-proof device with activation password $VPWD_i$. Note that TA does not need to keep the value of x after generating $VRID_i$. TA then issues a set of n credentials $Cr_{i1}, Cr_{i2}, ..., Cr_{in}$ for V_i. Here n is a system parameter and can be adjusted according to the security level required. Each credential Cr_{ix} is of the format $< Cr\_Num_{ix}, TSIG_{TSK}(Cr\_Num_{ix}) >$ where Cr_Num_{ix} is actually a re-encryption key (corresponding to the credential key Cr_Key_{ix}). Recall that a proxy re-encryption scheme is similar to a traditional symmetric or asymmetric encryption scheme with the addition of a delegation function. The message sender (TA in our case) can generate a re-encryption key based on his/her own secret key and the key of the delegated user (vehicle in our case). A proxy (RSU in our case) can then use this re-encryption key to translate a ciphertext (system master key in our case) into a special form such that the delegated user can use his/her private key to decrypt the ciphertext. A representative proxy re-encryption scheme is [2]. Back to the credential, $TSIG_{TSK}(Cr\_Num_{ix})$ represents TA's signature on Cr_Num_{ix} such that an RSU can verify its validity using the publicly-known TA identity $TRID$.

Next, TA pre-loads $VRID_i$, $VPWD_i$, all the n credentials $Cr_{i1}, Cr_{i2}, ..., Cr_{in}$ as well as the corresponding credential keys Cr_Key_{i1}, Cr_Key_{i2}, ..., Cr_Key_{in} into V_i's tamper-proof device. Besides, TA also stores the mapping $[VRID_i : Cr\_Num_{i1}, Cr\_Num_{i2}, ..., Cr\_Num_{in}]$ into its database (for real identity tracing in the future). Note that each credential represents V_i's authorized identity. However, no one except TA can reveal V_i's real identity based on the credential. It is true that RSUs can trace V_i's path based on the credentials if they are used frequently and at different locations. However, in our scheme, V_i only uses its credential explicitly occasionally (only when it wants to obtain the updated system master key s).

4.2 Master Key Transmission and Updating

TA randomly picks $s \in \mathbb{Z}_q$ as the initial system master key and computes $P_{pub} = sP$ as a public parameter. TA can update s and the corresponding P_{pub} if there is a need and the most updated s being encrypted using TA's public key (i.e. $AS\_ENC_{TRID}(s)$) is broadcasted to all RSUs while the most updated P_{pub} is made public. All RSUs store $AS\_ENC_{TRID}(s)$ locally. Note that since s is encrypted using TA's public key, RSUs cannot know its value either.

Whenever there is a need (e.g. when any vehicle is proved to be compromised), TA can update the system master key s into s'. TA transmits the encrypted new master key $AS\_ENC_{TRID}(s')$ to all RSUs. Again all the RSUs store $AS\_ENC_{TRID}(s')$ locally. All RSUs broadcast a master key update message to all in-range vehicles. The vehicles can thus repeat the same procedure as that for obtaining the initial system master key s (to be described in the next sub-section) to obtain the new one.

Our MLAS scheme supports vehicle revocation. TA maintains a revocation list which contains credential numbers of all revoked vehicles (e.g. those vehicles which have been proved to have committed any kind of attack to the system). This revocation list is then broadcasted to all RSUs. Having this mechanism, RSUs will not re-encrypt and send the system master secret to revoked vehicles in order to protect the system.

4.3 Vehicle Startup and Requesting for Master Key

When vehicle V_i starts, the driver inputs the real identity $VRID_i$ and password $VPWD_i$ (assigned by TA in Section 4.1) to activate the tamper-proof device. Here only simple hardware checking is involved. If either the real identity or the password is, or both are incorrect, the tamper-proof device refuses to perform further operations.

V_i's tamper-proof device then picks a credential Cr_{ix} (and the corresponding credential key Cr_Key_{ix}), where $x \in [1, n]$, from its pool at random. Assume that there is an RSU R_j nearby (recall that its identity $RRID_j$ is known by all vehicles in advance by means of a local map database). V_i's tamper-proof device encrypts Cr_{ix} using $RRID_j$ (i.e. $AS\_ENC_{RRID_j}(Cr_{ix})$). R_j decrypts and verifies the validity of Cr_{ix} (by checking TA's signature on the credential number using $TRID$). If it is valid, R_j re-encrypts $AS\_ENC_{TRID}(s)$ into a form that is decryptable by the credential key Cr_Key_{ix} using the re-encryption key Cr_Num_{ix}. V_i's tamper-proof device can thus decrypt using Cr_Key_{ix}, obtain and store s locally. As Cr_Key_{ix} is pre-loaded into the tamper-proof device and no interface is provided for outputting it, even the driver cannot obtain s successfully.

4.4 Message Signing by Vehicle

Recall that messages sent by vehicles can be classified into two types:

1) Regular messages: These messages are sent regularly (every 500 msec according to the DSRC standard). They include warning messages about travelling speed, turning direction and brake application.

2) Urgent messages: These messages are sent only occasionally. They include emergency messages about about road accidents or bad road conditions.

No matter which of the two types a message belongs to, to sign a message M_i, V_i's tamper-proof device first picks a credential Cr_{ix} from its pool at random and computes the pseudo identity $VPID_i = (VPID_{i1}, VPID_{i2}) = (rP, Cr\_Num_{ix} \oplus H(rP_{pub}))$ where r is a random nonce and $H(.)$ is a MapToPoint hash function. V_i's tamper-proof device also computes the signing key $(VSK_{i1}, VSK_{i2}) = (sVPID_{i1}, sH(VPID_{i1}))$. It then signs the message M_i to form the signature $\sigma_i = (\sigma_{i1}, \sigma_{i2}) = (HMAC_s(M_i), VSK_{i1} + \sigma_{i1} VSK_{i2}))$. The pseudo identity $VPID_i$, the original message M_i and the signature σ_i are then broadcasted.

4.5 Message Verification by Vehicle or RSU

For a type 1 regular message, the receiving vehicle simply re-computes $HMAC_s(M_i)$ using the stored s and M_i to see whether it is equal to σ_{i1} received. If yes, there is a very high probability that the sender is a valid vehicle since only valid tamper-proof devices can obtain s from the system.

By the time vehicle V_j receives the message from V_i, a nearby RSU should be able to overhear the message as well due to our assumptions on communication ranges. This RSU then samples some type 1 messages broadcasted in the air and verifies them using the procedure follows. Here the sample size is a system parameter which depends on the system security requirement.

Without loss of generality, assume that the type 1 message received is M_i and the corresponding signature is $\sigma_i = \sigma_{i1}, \sigma_{i2})$. RSU then checks whether $\hat{e}(\sigma_{i2}, P) = \hat{e}(VPID_{i1} + \sigma_{i1} H(VPID_{i1}), P_{pub})$.

Note that in case an RSU overhears more than one type 1 messages at about the same time, it can verify them in a batch by checking whether $\hat{e}(\sum_{i=1}^{n} \sigma_{i2}, P) = \hat{e}(\sum_{i=1}^{n} VPID_{i1} + \sigma_{i1} H(VPID_{i1}), P_{pub})$.

In case the two sides are not equal, it means at least one signature in the batch is invalid. RSU can then adopt the binary search technique as discussed in [6] to locate which signature(s) is (are) invalid. It can then forward that signature(s) together with the pseudo identity (identities) concerned to TA for further investigation.

After verification, RSU notifies all vehicles in its range the result. This can be done by means of fix-sized bloom filters since which have been shown to be efficient in [6]. The treatments of type 2 messages are the same as that of type 1 messages except that RSU will verify all of them (instead of taking samples). This is because urgent messages tend to be more important and may have serious impact to human life or property. However, when there is an accident, it is likely that a large number of vehicles will generate similar urgent messages on it. The RSU can thus first filter the received messages instead of verifying all of them. For example, the RSU can first investigate the contents of the urgent messages and for those with similar contents, it only verifies a threshold number (which in turn depends on the reliability requirement of the system) of them. In this way, the RSU can be a bit more relaxed even when the urgent messages come in a burst.

4.6 Real Identity Tracking and Revocation

To reveal the real identity of the sender of a message, TA is the only authorized party that can perform the tracing. Given vehicle V_i's pseudo identity $VPID_i$, TA first reveals the credential number used by V_i (i.e. Cr_Num_{ix}) by computing $VPID_{i2} \oplus H(sVPID_{i1}) = Cr\_Num_{ix} \oplus H(rP_{pub}) \oplus H(srP) = Cr\_Num_{ix}$.

TA can then search through its database to see which vehicle real identity $VRID_i$ the credential Cr_Num_{ix} belongs to.

5. SECURITY ANALYSIS

We analyse our schemes to show that they are secure with respect to the security requirements listed in Section 3. Formal proofs will be given in the full paper.

1) *Message integrity and authentication*: For all messages sent by vehicles, the signature σ_i on message M_i by vehicle V_i is composed of VSK_{i1} and VSK_{i2}. VSK_{i1} is defined as $sVID_{i1}$ where s is only known by tamper-proof devices since it is encrypted on its way and requires a pre-loaded credential key for decryption. Due to the difficulty of solving the discrete logarithm problem, there is no way for outside attackers to reveal s from the public parameter $P_{pub} = sP$. Thus an outside attacker cannot forge a signature easily. It is true that an inside attacker (e.g. a compromised tamper-proof device) knows the value of s. However, once it launches attacks and is discovered, all its preloaded credentials will be revoked. Thus it cannot obtain the updated system master key s anymore. Hence, an inside attacker cannot forge a signature also in the long run.

2) *Identity privacy preserving*: The pseudo identity of any vehicle is an ElGamal-type ciphertext, which is secure under the chosen plaintext attacks [3]. Also the random nonce r and the random selection of credentials make the pseudo identity of a vehicle different in different messages. This

makes tracing the location of a particular vehicle over time difficult.

3) *Traceability and revocability*: Section 4.6 shows that TA is able to trace a vehicle's real identity, thus traceability is satisfied. Also TA can revoke a vehicle from future usage, thus revocability is also satisfied.

6. CONCLUSIONS

We proposed a multiple level authentication scheme which still makes use of tamper-proof devices but the strong assumption that a long-term system master secret is preloaded into all tamper-proof devices is removed. Instead of preloading by factories, the system master secret can be updated and securely transmitted to a tamper-proof device when there is a need. On the other hand, messages sent by vehicles are classified into two types - regular messages and urgent messages. Regular messages can be verified by neighboring vehicles by means of Hash-based Message Authentication Code (HMAC) while urgent messages can only be verified with the aid of RSUs nearby by means of a conditional privacy-preserving authentication scheme. In the future, we will evaluate our scheme using simulations. We will also extend our scheme to a group communications scenario. Finally we will consider other secure applications in VANETs as well.

7. REFERENCES

[1] SHA-3 Project by NIST. http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. In *Proceedings of the 12th Annual Network and Distributed Systems Security Symposium (NDSS)*, 2005.

[3] J. Baek, B. Lee, and K. Kim. Secure Length-Saving ElGamal Encryption under the Computational Diffie-Hellman Assumption. *Lecture Notes in Computer Science - Information Security and Privacy, Vol. 1841*, pages 49 – 58, 2000.

[4] D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. In *Proceedings of Asiacrypt '01*, pages 514 – 532, 2001.

[5] B. K. Chaurasia, S. Verma, and S. M. Bhasker. Message broadcast in VANETs using Group Signature. In *Proceedings of the IEEE WCSN '09*, pages 131 – 136, Dec. 2008.

[6] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li. SPECS: Secure and Privacy Enhancing Communications for VANET. In *Proceedings of the ADHOCNETS '09*, Sept. 2009.

[7] R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. *IETF RFC2459*, 1999.

[8] H. Oh, C. Yae, D. Ahn, and H. Cho. 5.8 GHz DSRC Packet Communication System for ITS Services. In *Proceedings of the IEEE VTC '99*, pages 2223 – 2227, Sept. 1999.

[9] P. P. Tsang and S. W. Smith. PPAA: Peer-to-Peer Anonymous Authentication. In *Proceedings of ACNS '08*, pages 55 – 74, 2008.

[10] F. Wang, D. Zeng, and L. Yang. Smart Cars on Smart Roads: an IEEE Intelligent Transportation Systems Society Update. *IEEE Pervasive Computing, Vol. 5, No. 4*, pages 68 – 69, 2006.

[11] A. Wasef and X. Shen. PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks. In *Proceedings of the IEEE ICC '08*, pages 1458 – 1463, May 2008.

[12] C. Zhang, X. Lin, R. Lu, and P. H. Ho. RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks. In *Proceedings of the IEEE ICC '08*, pages 1451 – 1457, May 2008.

[13] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen. An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks. In *Proceedings of the IEEE INFOCOM '08*, pages 816 – 824, Apr. 2008.