A Robust Conditional Privacy-Preserving Authentication Protocol in VANET*

Chae Duk Jung[1], Chul Sur[2], Youngho Park[3], and Kyung-Hyune Rhee[3]

[1] Department of Information Security, Pukyong National University, 599-1, Daeyon3-Dong, Nam-Gu, Busan, 608-737, Republic of Korea
jcd0205@pknu.ac.kr
[2] Department of Computer Science, Pukyong National University
kahlil@pknu.ac.kr
[3] Division of Electronic, Computer & Telecommunication Engineering, Pukyong National University
{pyhoya,khrhee}@pknu.ac.kr

Abstract. Recently, Lu *et al.* proposed an efficient conditional privacy preservation protocol, named ECPP, based on group signature scheme for secure vehicular communications. However, ECPP dose not provide unlinkability and traceability when multiple RSUs are compromised. In this paper, we make up for the limitations and propose a robust conditional privacy-preserving authentication protocol without loss of efficiency as compared with ECPP. Furthermore, in our protocol, RSUs can issue multiple anonymous certificates to an OBU to alleviate system overheads for validity check of RSUs. In order to achieve these goals, we consider a universal re-encryption scheme as our building block.

Keywords: Vehicular Ad-hoc Network, Conditional Privacy, Authentication, Movement Tracking, Universal Re-encryption, Group Signature.

1 Introduction

In the near future, vehicles will be equipped with on-board processing and wireless communication modules, which enable vehicle-to-vehicle and vehicle-to-infrastructure communications based on short-range wireless technology, e.g., IEEE 802.11p [16]. That is called a vehicular ad-hoc network (VANET). VANET mainly consists of On-Board Units (OBUs) and Roadside Units (RSUs) [11], where OBUs are installed on vehicles to provide wireless communication capability, while RSUs are deployed to provide access point to vehicles within their radio coverages. By this organization, VANET can provide useful functions such as cooperative driving and probe vehicle data. For example, a vehicle can warn other vehicles about traffic accidents or traffic jam.

* This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2008-521-D00454).

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 35–45, 2009.

Considering the useful VANET applications, it is necessary to develop a suit of elaborate and carefully designed security mechanisms to make VANET applications viable [1,5,7,10,12,13,14,15,17]. Especially, the increasing demand for privacy protection has brought additional requirements related with privacy preservation in VANET such as anonymous message authentication. Therefore, conditional privacy preservation, which private information is not disclosed to other entities while the authorities should legally trace user-related information in case of a disputed event, becomes one of the main requirements for secure VANET.

Lin *et al.* [9] proposed a conditional privacy-preserving authentication protocol for VANET by integrating the techniques of group signature and identity-based signature. However, in [9], even though the authors reduced certificate revocation list (CRL) size, their protocol needs the management of certificate revocation information in OBUs. Hence, each vehicle must spend much time in message verification when the number of revoked vehicles is increased.

Recently, Lu *et al.* [8] proposed an efficient conditional privacy preservation protocol, named ECPP, which issues on-the-fly short-time anonymous certificate to OBUs by using a group signature scheme [2]. Since RSUs can check the validity of the requesting vehicle during the short-time anonymous certificate generation phase, such revocation check by an OBU itself of [9] is not required. ECPP provides unlinkability and traceability under the unrealistic assumption that most RSUs will not disclose any inner information without the authorization of the trusted authority. However, due to the fact that there exist a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection facilities against malicious attacks. Therefore, it is possible for an attacker to access RSUs and disclose the information in the RSUs. When multiple RSUs are compromised, an attacker is able to track the movement trace of a vehicle by using the information stored in the compromised RSUs [3], because each RSU stores unchanged pseudonyms for OBUs in ECPP. As a result, ECPP does not provide unlinkability of OBUs when some RSUs were compromised. Furthermore, since the trace protocol in ECPP is run by incorporating with an RSU which issued a certificate corresponding to a disputed message, it is impossible to trace OBUs belong to compromised RSUs. Consequently, ECPP does not provide unlinkability and traceability when multiple RSUs are compromised.

Moreover, even though ECPP runs mutual authentication between OBUs and RSUs, it requires validity check of RSUs by using up-to-date revocation list in anonymous certificate generation phase by considering an attacker who can disclose inner information in compromised RSUs.

As a result, it is necessary to design an efficient and robust conditional privacy-preserving authentication protocol that not only provides unlinkability and traceability even if multiple RSUs are compromised, but also reduces system overheads for validity check of RSUs in OBUs' anonymous certificate generation phase.

Our Contribution. In this paper, we propose a robust conditional privacy-preserving authentication protocol based on universal re-encryption scheme [4] and identity-based group signature scheme [2]. To efficiently resolve the problem

resulted from certificate revocation in traditional PKI, the proposed protocol employs the concept of shot-time anonymous certificate. Besides, even though multiple RSUs are compromised, in contract to ECPP, the proposed protocol provides unlinkability and traceability without loss of efficiency as compared with ECPP. Furthermore, to reduce system overheads for validity checks of RSUs in OBUs' anonymous certificate generation phase, RSUs issue multiple anonymous certificates to an OBU based on universal re-encryption scheme.

The rest of the paper is organized as follows. In Section 2, we describe our design objectives and define conditional privacy level for secure VANET. We outline our system architecture in Section 3. Section 4 presents the proposed conditional privacy-preserving authentication protocol. In Section 5, the security and efficiency of the proposed protocol are analyzed. Finally, we conclude the paper in Section 6.

2 Security Requirements

In this paper, we aim at achieving the following objectives:

- **Authentication.** The origin of the messages should be authenticated to guard against impersonation attack. Also, even though an attacker compromises some RSUs, the attacker cannot forge a signature on safety message in a compromised RSU's communication range.
- **Anonymity.** The identities of vehicles should be hidden from normal message receivers during the safety message authentication process. Moreover, even if an attacker obtains inner information of compromised RSUs, the attacker cannot disclose real identities of OBUs.
- **Unlinkability.** When an adversary has collected several safety messages that have different pseudonyms from an OBU, the OBU should be still not traceable. Moreover, even though the adversary compromised RSUs, it also cannot link information stored in the RSUs as the same OBU.
- **Traceability.** The authority should be able to trace the sender of a safety message by revealing the identity in case of any disputed situation such as liability investigation. In addition, even if multiple RSUs are compromised, the authority should be able to trace real identities of pseudonyms in anonymous certificates without assistance of compromised RSUs.

Following the above goals, we modify the definition of conditional privacy level in [8] as Table 1.

Note that, ECPP does not provide unlinkability of an OBU since the compromised RSUs store the same pseudonym for same OBU. Moreover, since the trace protocol in ECPP is run by the trust authority with an RSU (certificates generator), it is impossible to trace real identities of OBUs belong to damaged RSUs. As a result, ECPP provides Level 1 Privacy in Table 1.

Table 1. Definition of Conditional Privacy Level

	Authentication	Anonymity	Unlinkability	Traceability
Level 1 Privacy	O	O	×	×
Level 2 Privacy	O	O	O	×
Level 3 Privacy	O	O	O	O

3 System Model

In this section, we describe our system model, in which communication nodes are either membership manager, RSUs, or OBUs as follows:

- **Membership Manager** is public agencies or corporations with administrative powers in a specific field; for example, city or state transportation authorities. The membership manager establishes and manages system parameters and system roles for secure VANET. In addition, the membership manager should be able to reveal the identities of safety message senders in the case of disputed traffic events.
- **RSUs** belong to the membership manager. When an RSU receives a request message for certificate issue from an OBU, it checks the validity of the OBU with the membership manager. If the OBU is legal, the RSU issues multiple anonymous certificates to the OBU by using universal re-encryption scheme and group signature scheme.
- **OBUs** periodically send a safety message by using its own short-time anonymous certificate. When an OBU needs anonymous certificates, it requests certificate issue to a nearby RSU. If the OBU is legitimated, it is able to get new multiple short-time anonymous certificates from the RSU.

To make our model more clear, we assume the followings:

- Each OBU has a unique electronic identity, e.g., ELP (Electronic License Plate).
- OBUs change its own shot-time anonymous certificates within 1 minute (min) as a result of [12].
- Membership manager can inspect all RSUs at high level and detect compromised RSUs.

Our protocol consists of the following 5-phases:

1. Setup: The membership manager sets up its own master key and system parameters based on identity-based group signature scheme [2] and universal re-encryption scheme [4]
2. Registration: The membership manager assigns MAC keys to OBUs and group signing keys to RSUs, respectively. At the same time, the membership manger stores the pairs ⟨OBU's real ID, MAC key⟩ in his secure storage.

3. Multiple Anonymous Certificates Generation: When an OBU requests anonymous certificates for given time period, it generates and transmits a request message including new pseudonym and MAC value to a nearby RSU. After validity check for the OBU, the RSU issues multiple short-time anonymous certificates to the OBU. Finally, the OBU verifies the issued certificates and checks the validity of the RSU by using RL (Revocation List).
4. Safety Message Authentication: OBUs periodically sign traffic information by using conventional digital signature scheme under its own shot-time signing key, and then broadcast a traffic information attached with the signature and the short-time anonymous certificate. Before accepting received traffic information, each receiver verifies the signature with sender's certificate.
5. OBU's Real ID Trace: In case of problematic happening, the membership manager traces the real identity of generator of a safety message by using its own private key.

4 Proposed Protocol

In this section, we propose a robust conditional privacy-preserving authentication protocol based on universal re-encryption [4] and identity-based group signature [2] for secure VANET. Table 2 describes the notations used in the proposed protocol.

Table 2. Notations

Notation	Description
GS_{mk}	master key of group signature
GS_{pk}	public key of group signature
GS_{params}	system parameters of group signature
sk_{MM}, pk_{MM}	private/public key pair of membership manager
H, H_0	cryptographic hash functions
K_i	MAC key for OBU_i
$H_K()$	MAC function under key K
ID_i	OBU_i's real identity, i.e., ELP
ID'_i	pseudonym of OBU_i
$ID'_{i,\cdot}$	short-time pseudonym of OBU_i
$Cert_{i,\cdot}$	short-time anonymous certificate of OBU_i
$sk_{i,\cdot}, pk_{i,\cdot}$	OBU_i's short-time private/public key pair
$GSig()$	group signature function
$Sig()$	ordinary digital signature function
$E(), D()$	encryption and decryption function of universal re-encryption
$Re()$	re-encryption function of universal re-encryption
t	validity period for shot-time certificate

4.1 Setup

The membership manager generates the required bilinear groups and system parameters as it is in [2]. Given security parameter k, the membership

manager chooses a k-bit prime number p, bilinear map groups (G_1, G_2) of order p. The membership manager randomly picks generators $g_1 \in G_1$ and $g_2 \in G_2$. Let $\hat{e} : G_1 \times G_2 \rightarrow G_T$ be a bilinear pairing. The membership manager selects $\gamma \in Z_p^*$ and sets $GS_{pk} = g_2^{\gamma}$. After that, the membership manager chooses secure cryptographic hash functions $H : \{0,1\}^* \rightarrow Z_p^*$ and $H_0 : \{0,1\}^* \rightarrow G_2^2$. The system parameter GS_{params} and master key GS_{mk} of the membership manager are set up as follows:

$$GS_{params} = (G_1, G_2, G_T, \hat{e}, p, g_1, g_2, H, H_0, GS_{pk}),\ GS_{mk} = \gamma$$

In addition, the membership manager selects its own private key $sk_{MM} \in Z_p^*$ and computes public key $pk_{MM} = g^{sk_{MM}}$, where g is a generator for the underlying group for the ElGamal cryptosystem.

4.2 Registration

In registration phase, the membership manager issues a group signing key to each RSU for generating anonymous certificates and a MAC key to each OBU. All OBUs need to be registered with the trusted membership manager and preloaded with public system parameters and their own MAC key before joining VANET. Thus, the membership manager randomly chooses MAC key K_i and then transmits K_i to OBU_i over a secure channel. In addition, the membership manager stores the pair $\langle ID_i, K_i \rangle$ in its own secure storage. To generate a group signing key, the membership manager selects $x_j \in Z_p^*$ such that $\gamma + x_j \neq 0$, and then sets $A_j = g_1^{1/\gamma + x_j}$. After that, the membership manager sends (A_j, x_j) to RSU_j as the group signing key over a secure channel.

4.3 Multiple Anonymous Certificates Generation

When an OBU_i wants to get new multiple anonymous certificates for given time period from a nearby RSU_j, OBU_i and RSU_j run anonymous certificate generation protocol as follows.

Step 1. An OBU_i encrypts its own real identity ID_i based on universal re-encryption under the membership manager's public key to generate a new pseudonym ID_i'. At the same time, the OBU_i randomly selects a short-time validity period t and multiple signing keys $sk_{i,1}, \ldots, sk_{i,n}$, and then computes corresponding public keys (note that, each public key is formed by signature scheme in safety message authentication phase). Finally, the OBU_i computes MAC value $MAC_{ID_i'} = H_{K_i}(ID_i' || PK || t)$ and transmits $\langle ID_i', PK, t, MAC_{ID_i'} \rangle$ to a nearby RSU_j for obtaining n anonymous certificates, where PK is a set of public keys.

Step 2. The RSU_j checks the valid period t since a long period will cause the risk of continued circulation of an invalid certificate by an attacker. If t is short valid period, RSU_j transmits the received message to the membership manager

for checking a validity of OBU_i. The membership manager decrypts the received pseudonym ID'_i for getting real identity ID_i and searches MAC key K_i corresponding to ID_i. If $MAC_{ID'_i}$ is valid and the OBU_i is legal, the membership manager sends the permission message and up-to-date RL (=$\{A_1, \ldots, A_{N_R}\}$, Revocation List for revoked RSUs) to the RSU_j.

Step 3. If the RSU_j receives the permission message from the membership manager, it repeatedly executes a re-encryption algorithm in [4] with the pseudonym ID'_i to obtain n pseudonyms $ID'_{i,1}, \ldots, ID'_{i,n}$ for OBU_i. Then, the RSU_j computes each $\sigma_l = GSig(ID'_{i,l}||pk_{i,l}||t)$ by using group signature scheme [2] under its own group signing key and forms each anonymous certificate $Cert_{i,l} = \{ID'_{i,l}, pk_{i,l}, t, \sigma_l\}$, where $l = 1, \ldots, n$. Finally, the RSU_j transmits multiple anonymous certificates $Cert_{i,1}, \ldots, Cert_{i,n}$ and RL to the OBU_i.

Step 4. The OBU_i checks the validity of the RSU_j by using revocation checking procedure in [2] with RL. If RSU_j is not revoked, the OBU_i verifies received certificates by using GS_{pk}. Finally, the OBU_i accepts issued certificates if all the checks are valid.

4.4 Safety Message Authentication

OBU_i signs a traffic information m by using a conventional digital signature scheme such as ECDSA under its own short-time signing key $sk_{i,l}$ for generating signature σ_m. Then, the OBU_i forms the safety message $Msg = \{m, \sigma_m, Cert_{i,l}\}$ and broadcasts Msg. Upon receiving a safety message, each receiver first checks the validity of $Cert_{i,l}$ by using GS_{pk}. If the $Cert_{i,l}$ is valid, the receiver retrieves $pk_{i,l}$ from the $Cert_{i,l}$ and verifies σ_m using the $pk_{i,l}$. If σ_m is valid, the traffic information can be accepted, otherwise discarded.

4.5 OBU's Real ID Trace

In case of any disputed situation, it is necessary to extract a real identity of generator of the broadcasted safety message by the membership manager. Since pseudonyms $ID'_{i,l} = Re(ID'_i)$ of OBU_i are computed by re-encryption scheme of [4] with $ID'_i = E_{pk_{MM}}(ID_i)$, the pseudonyms were formed as ciphertexts for OBU's real identity under the pubic key of the membership manager. Note that, due to the property of universal re-encryption, the membership manager can output real identities from pseudonyms in the safety message by using its own private key sk_{MM}.

5 Discussion

5.1 Security

We analyze how the proposed protocol satisfies the security requirements stated in Section 2.

- **Authentication.** Since the signature is generated by a conventional digital signature scheme with respect to a pseudonym and a corresponding public key, which was proven to secure against adaptive chosen message attack, no adversary can launch a forgery attack and an impersonation attack to an OBU.
- **Anonymity.** Since OBUs' real identities are encrypted under pk_{MM} and re-encrypted ciphertexts are used as pseudonyms, an attacker who compromised multiple RSUs cannot disclose a real identity from pseudonyms in certificates without knowing sk_{MM} due to the property of universal re-encryption.
- **Unlinkability.** An eavesdropper cannot link the safety messages since most safety message consists of different pseudonyms and public keys independently. Even though multiple RSUs are compromised, the attacker does not obtain any information from the compromised RSUs since each OBU generates and transmits different pseudonyms to RSUs in certificate generation.
- **Traceability.** In dispute cases, the membership manager is able to trace a real identity of OBU_i corresponding pseudonym $ID'_{i,\cdot}$ by using its own private key sk_{MM}. Even if some RSUs are compromised, the membership manager is able to trace OBUs since the trace procedure in the proposed protocol is executed by the membership manager without cooperations with RSUs.

As a result, the proposed protocol provides Level 3 Privacy in Table 1.

5.2 Efficiency

In this section, we compare the proposed protocol with ECPP to show that our protocol provides reasonable efficiency in terms of OBU's computational costs and RSU valid serving ratios. For fairness in comparisons, we selected a bilinear pairing of 80-bit security level as the same security measures of ECPP as follows; degree $k = 6$, $|G_1| = 160$ bits and $|q| = 1024$ bits. Table 3 shows the measures to estimate and to compare our protocol with ECPP. Note that ECPP_M is ECPP's multiple certificates issue type as given in Table 4.

Table 3. Cryptographic operation time and protocol execution time (implemented on Pentium IV 3.0 GHz, $N_R = |RL|$)

Cryptographic operation time	Time(ms, millisecond)	
$\hat{e}$ bilinear pairing operation	4.5	
point multiplication on G_1	0.6	
exponentiation on Z_q	2.1	
Protocol execution time	**ECPP_M(ms)**	**Our Protocol(ms)**
time for n certificates issue	$20.4+14.4n$	$6.3+18.6n$
time for n certificates verification	$17.1n$	$17.1n$
time for validity check of RSU	$9N_R$	$9N_R$
total time for n certificates generation	$20.4+31.5n + 9N_R$	$6.3+35.7n+9N_R$

Table 4. Modification to multiple-ECPP

Phase	ECPP	ECPP$_M$
public key generation	$x \in Z_q^*,\ Y = xP$	$\forall\ i \leq n, x_i \in Z_q^*,\ Y_i = x_iP$
certificate check	check $Cert$	check $\forall\ i \leq n, Cert_i$
RSU validity check	$\times$	revocation check (by using RL)

To measure the valid number of requesting certificates n_V at once per vehicle, we assume that all OBUs in an RSU range request n_V anonymous certificates to the RSU and the average speed of vehicles varies from 10 m/s $\sim$ 40 m/s (or 36 km/hr $\sim$ 144 km/hr). Therefore, n_V depends on vehicle density d that is computed by 2-second rule which drivers maintain as much distance between vehicles, as the vehicle would travel in 2 s. That is, we have $d = R_{range} \times N_L/(v \times 2)$ where R_{range} is RSU's valid coverage, N_L is the number of lane and v is vehicle speed. Since $T_R \geq T_G \times d$ where $T_R (= R_{range}/v)$ is passing time through an RSU range and $T_G (= 6.3 + 18.6n_V)$ is the time overhead for generating n_V certificates, n_V can be measured as follow:

$$n_V \leq \frac{T_R}{18.6 \times d} - 0.3 = \frac{R_{range}}{v \times 18.6 \times d} - 0.3$$

Therefore, each OBU can request about 10 $\sim$ 50 anonymous certificates to an RSU depending on vehicle density.

Figure 1 shows computational costs of our protocol, ECPP$_M$ and ECPP with different N_R and different n. Then, we can observe that our protocol has reasonable efficiency to ECPP$_M$ in the matter of OBU's computational costs. Furthermore, when compromised RSUs are increasing, both our protocol and ECPP$_M$ which are multiple certificates issue protocols have more efficiency than single certificate issue protocol such as ECPP.

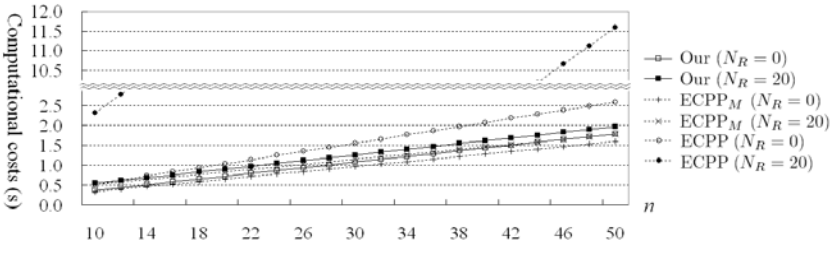

Fig. 1. Computational costs of OBU

Let $|R|_n$ be the minimal number of passed RSUs for n min, and ρ_n be the probability for each OBU to issue a request for n min. Therefore, an OBU could request n certificates to an RSU among $|R|_n$ RSUs. Then, we have $\rho_n = 1/|R|_n$ (note that, since $|R|_n$ is a minimal value, we consider that ρ_n is maximal

probability). When we assume that an RSU is allocated every 500 meter on the road, $|R|_1$ and ρ_1 are (10 m/s × 60 s)/500 m=1.2 and 0.8, respectively. In addition, we have $|R|_n = n \times |R|_1$. As a result, ρ_n can be measured as follow:

$$\rho_n = \frac{1}{|R|_n} = \frac{1}{n \times |R|_1} = \frac{1}{n}\rho_1 = \frac{0.8}{n}$$

By following Lu *et al.*'s analysis method [8], RSU valid serving ratios of the proposed protocol with ECPP_M for $n \geq 10$ are 100% where 10 m/s $\leq v \leq$ 40 m/s, $100 \leq d \leq 400$.

Finally, we show the valid serving ratio of the membership manager for OBUs' requests. In our protocol, the main operation of the membership manager is to decrypt OBUs' pseudonyms at each n min, so the membership manager's performance always depends on the size of n. Then, S_{MM}, the valid serving ratio of the membership manager, can be defined by

$$S_{MM} = \begin{cases} 1, & \text{if } \frac{T_{ms}}{T_{MM} \cdot (T_{avg}/n) \cdot N_{OBU}} \geq 1 \text{ ;} \\ \frac{T_{ms}}{T_{MM} \cdot (T_{avg}/n) \cdot N_{OBU}} & \text{otherwise.} \end{cases}$$

where T_{ms} is a total time for a day, T_{MM} is time overhead for authenticating an OBU, T_{avg} is an average driving time per day and N_{OBU} is the number of OBUs.

From above equation, we can observe that the membership manager can efficiently process multiple certificates requests in most cases where $T_{MM} = 2.1$ ms and $T_{avg} = 120$ min. As a result, the proposed multiple anonymous certificates generation protocol is feasible.

6 Conclusion

In this paper, we have proposed a robust conditional privacy-preserving authentication protocol based on universal re-encryption scheme and identity-based group signature scheme for secure VANET. Compared with ECPP, the proposed protocol can provide unlinkability and traceability even if an attacker compromise multiple RSUs. Furthermore, to avoid frequent certificate requests and to reduce computational overhead for validity check of RSUs in certificate generation phase, RSUs can issue multiple anonymous certificates to an OBU. We have demonstrated, through the performance evaluation, that the proposed protocol has similar performance to ECPP in terms of OBU's computational costs and RSU valid serving ratios.

References

1. Blum, J., Eskandarian, A.: The threat of intelligent collisions. IT Professional, pp 6(1), 22–29 (2004)
2. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: CCS 2004, pp. 168–177 (2004)

3. Freudiger, J., Raya, M., Felegyhazi, M.: Mix-Zones for Location Privacy in Vehicular Networks. In: WiN-ITS 2007 (2007)
4. Golle, P., Jakobsson, M., Juels, A., Syverson, P.F.: Universal re-encryption for mixnets. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 163–178. Springer, Heidelberg (2004)
5. Hubaux, J.-P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security and Privacy Magazine 2(3), 49–55 (2004)
6. Kamat, P., Baliga, A., Trappe, W.: Secure, pseudonymous, and auditable communication in vehicular ad hoc networks. Security Comm. Networks (1), 233–244 (2008)
7. Luo, J., Hubaux, J.-P.: A survey of Inter-Vehicle Communication Technical Report. EPFL Technical Report IC/2004/24 (2004)
8. Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: ECPP: Efficient Conditional Privacy Preservation Protocol for secure Vehicular Communications. In: IEEE INFOCOM 2008, pp. 1903–1911 (2008)
9. Lin, X., Sun, X., Shen, X.: GSIS: a secure and privacy preserving protocol for vehicular communications. IEEE Transaction on Vehicular Technology 56(6), 3442–3456 (2007)
10. Parno, B., Perrig, A.: Challenges in securing vehicular networks. HotNets-IV (2005)
11. Peng, Y., Abichar, Z., Chang, J.M.: Roadside-aided Routing (RAR) in Vehicular Networks. IEEE ICC 2006 8, 3602–3607 (2006)
12. Raya, M., Hubaux, J.-P.: The Security of Vehicular Ad Hoc Networks. In: SASN 2005, pp. 11–21 (2005)
13. Raya, M., Hubaux, J.-P.: Security Aspects of Inter-Vehicle Communications. In: STRC (2005)
14. Raya, M., Hubaux, J.-P.: Securing Vehicle Ad Hoc Networks. Journal of Computer Security 15(1), 39–68 (2007)
15. Ren, K., Lou, W., Deng, R.H., Kim, K.: A Novel Privacy Preserving Authentication and Access Control Scheme in Pervasive Computing Environments. IEEE Transaction on Vehicular Technology 55(4), 1373–1384 (2006)
16. Varsheney, U.: Vehicular mobile commerce. IEEE Computer Magazine Online (2004)
17. Xu, Q., Mak, T., Ko, J., Sengupta, R.: Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages. IEEE Transaction on Vehicular Technology 56(2), 499–518 (2007)