Hindawi Publishing Corporation
International Journal of Vehicular Technology
Volume 2012, Article ID 862368, 8 pages
doi:10.1155/2012/862368

Research Article

Efficient Noninteractive Secure Protocol Enforcing Privacy in Vehicle-to-Roadside Communication Networks

Fatty M. Salem, Maged Hamada Ibrahim, and I. I. Ibrahim

Department of Electronics, Communications and Computers, Faculty of Engineering, Helwan University, 1 Sherif Street, Helwan 11792, Egypt

Correspondence should be addressed to Fatty M. Salem, fatty4com@hotmail.com

Received 16 June 2012; Accepted 17 October 2012

Academic Editor: Cheng-Min Lin

Vehicular ad hoc networks (VANETs) have attracted extensive attentions in recent years for their promises in improving safety and enabling other value-added services. In this paper, we propose an efficient noninteractive secure protocol preserving the privacy of drivers in vehicle-to-roadside (V2R) communication networks with the ability of tracing malicious drivers only by a third trusted party (TTP), who is assumed to be fully trusted. Our proposed protocol can provide these complex requirements depending on symmetric cryptographic algorithms. The drivers can change the symmetric key used for message encryption with each message transmission and find noninteractively new values to be correctly used for verification and tracing in case of malicious behavior. The advantages of symmetric cryptographic algorithms over asymmetric algorithms are the faster processing speed and the shorter message length which makes it suitable for real-time applications such as V2R communications. An efficient key revocation scheme will be also described.

1. Introduction

The advancement and wide deployment of wireless communication technologies have revolutionized human's lifestyles by providing the best convenience and flexibility ever in accessing the internet services and various types of personal communication applications. Recently, vehicle manufactories and telecommunication industries gear up to equip each vehicle with the technology that allows the vehicle-to-vehicle (V2V) communications as well as the vehicle-to-roadside (V2R) communication. Roadside unit (RSU) is located in some critical sections of the road, such as at every traffic light or any intersection or any stop sign, in order to improve the driving experience and make driving safer.

The integration of V2V and V2R communications is beneficial because V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium areas and at locations where roadside units are not available.

In a safety application, it is important to guarantee the source authentication to prevent unauthorized entities from tampering with the broadcasted messages and from impersonating as legitimate participants in the network. However, authentication in this mobile environment poses a privacy risk to the users; hence, through authentication, the identity of the drivers must be preserved to protect their location privacy. In case of malicious activity, the sender of the disputed message must be traced and revoked only by the TTP who is assumed to be a trusted entity.

Additionally, as VANETs are characterized by the high mobility of vehicles, they require a very short message length to be broadcasted and processed in a timely manner.

A number of research contributions discuss vulnerabilities [3, 4], summarize security requirements, and design principles of the network [5], propose specific mechanisms [6–9].

Public key infrastructure (PKI) and certificates can provide a level of trust between users of public keys, but there are several disadvantages for using PKI and certificates in V2R communications: (1) long message lengths and long processing time, where the size of public keys should be long enough to prevent adversaries from attacking the algorithms and obtaining the associated private keys. In addition, most asymmetric algorithms use modular exponentiation which

in turn provides a slow processing speed; (2) PKI and certificates provide a constant public key for each entity which associates itself to its owner, and this will reveal the identity of drivers which leads to threat on the location privacy of the drivers.

In this paper, we propose an efficient secure protocol to preserve the privacy of the drivers in V2R communication networks based on symmetric cryptographic algorithms to reduce the overheads and the processing time.

Paper Organization. Section 2 reviews previous protocols in which preserving privacy is the main goal. In Section 3, we discuss the motivations and our contributions. In Section 4, we describe the existing technology required for our proposed protocol. Then, we will describe the model in Section 5. In Section 6, we describe our proposed protocol. Then, we evaluate the performance of the protocol in Section 7. Finally, we conclude this paper in Section 8.

2. Related Work

A dynamic key distribution system is proposed [4], where vehicles periodically request a new certificate from the certificate authority (CA). However, these requests place an additional load on the CA in addition to the network. The proposed approaches in [10–12] are based on issuing a temporary certificate from the remote certificate authority (RCA) when the local certificate authority (LCA) is not available. These approaches reduce the load on certificate authorities but require high communication cost between several central authorities and mobile users to certify the temporary certificate.

In [13], vehicles are organized into groups and only group leader broadcasts messages, while the remaining members maintain silence in order to hamper linkability between pseudonyms. However, given the high volume of messages required for safety information, silent periods would not be suitable.

The protocol introduced in [14] provides anonymous message authentication and conditional privacy preservation by periodically changing the signing key. However, three disadvantages have been identified: (1) each vehicle has to take a large storage space to store a huge number of anonymous key pairs; (2) it may be very time consuming for the authority to trace for any awkward certificate due to the long revocation list; (3) once some vehicle's anonymous keys are revoked, it takes a long time for each vehicle to update the certificate revocation list.

The proposed protocol in [15] is based on the group signature technique. Compared with the protocol in [14], vehicles do not require storing a huge number of anonymous keys in its storage units, and the top authority can efficiently track the targeted vehicle. However, although the revocation list is shorter and easily updated, the time for safety message verification grows linearly with the number of revoked vehicles in the revocation list. Thus, each vehicle has to spend more time on safety message verification when the scale of revocation list is large. Once the safety message is time-aware, this solution may not be feasible due to the heavy verification process.

In [16], it is a noninteractive ID-based scheme which takes use of members' identities to establish a secure trust relationship between communicating vehicles, and of a blind signature-based scheme for vehicle-to-roadside device communication which allows authorized vehicles to anonymously interact with their roadside units. They claimed that their scheme is secure, but authors in [17] found that it suffers from the parallel session attack and the leakage of each vehicle's secret key. This makes the secret keys in the system insecure. Thus, the system is broken.

It is proposed in [18] a non-interactive secure VANET protocol which achieves anonymity and traceability; the protocol uses the idea of traceable linkable democratic group signatures introduced in [19]. However, the protocol requires a high computation complexity due to the extensive dependency on cryptographic proofs-of-knowledge.

Authors of [20] define a system where vehicles change pseudonyms in a certain region pointed by the system, this region should be where a lot of vehicles are within the communication range [21]. The disadvantage of this approach is emerged when there are not enough vehicles changing pseudonyms within the region. To overcome this problem, the protocol in [22] proposes self-assigned digital pseudonyms, taking a set of measures while changing pseudonyms which are (1) synchronizing pseudonym change; (2) introducing silent periods; (3) changing pseudonyms when vehicles are in the region.

In [23], the authors are concerned with how to achieve efficient and robust pseudonym-based authentication. They designed mechanisms that reduce the security overhead for safety beaconing and retain robustness for transportation safety. This approach enables vehicle onboard units to generate their own pseudonyms, without affecting the system security.

In the contribution of [1], a non-interactive secure VANET protocol is given that provides authentication and preserves privacy among drivers; the drivers can change their public keys frequently and find noninteractively the new token corresponding to the changed public keys set. In case of malicious activity, only the TTP can identify the drivers of disputed messages. The protocol can provide these fundamental requirements with a low overhead and short processing time for a small number of groups in the network. However, as the protocol depends on a multiprime RSA algorithm, for a large number of groups in the network, the size of transmitted messages will be affected.

The authors aimed to improve the efficiency of the protocol in [1], proposing a non-interactive secure protocol [2], providing security and privacy for intervehicle communication (IVC) networks; the protocol uses the standard RSA encryption, and the transmitted message is independent of the number of groups, which provides a constant low overhead for any given number of groups in the network.

In [24], an interactive anonymous random key set-based authentication protocol is proposed; the protocol preserves user privacy under the zero-trust policy, in which no central authority is trusted with the user privacy. However, the

period of reusing the key is restricted to prevent correlation from being made.

When using general purpose automatic survey (GPAS) system based on VANETs [25], some compromised nodes may try to take advantage of GPAS to utilize their personal benefits or to destroy the survey system. Therefore, to ensure system security, it is required to identify the adversary model in GPAS. Specifically, even if one node has not gone to the target region, it may still overhear the survey request and generate one response, breaching the spatial condition. Meanwhile, with multiple pseudonyms, one node may generate multiple survey responses and sign them with different certificates.

Besides vulnerabilities versus attacks against traffic safety and driver privacy, a large-scale VANET in a metropolitan area raises scalability and management challenges. The paper in [26] employs identity-based group signatures (IBGSs) to divide a large-scale VANET into easy-to-manage groups and establish liability in vehicular communications while preserving privacy. The proposed protocol has the disadvantage of the high computation complexity due to the realization of the system in bilinear groups.

The protocol in [27] presents signature-seeking drive (SSD), which is a secure incentive framework that stimulates cooperative dissemination of advertising messages among vehicular users in a secure way. The SSD employs the concept of virtual cash to charge and reward the provision of advertising service as an incentive for users in the network. The protocol in [28] adopted proxy signature cryptography to authenticate vehicles and RSUs and to delegate the RSU to issue short-lived certificates only for authenticated vehicles. However, these protocols depend on the PKI which suffers from the long processing time and the computational costs.

3. Motivations and Contributions

We argue that a number of security services must be provided which could be complex by the inherent nature of the network. Moreover, due to the high mobility of VANETs, and,hence, the short time available for the communication between vehicles and RSUs, time sensitivity is an additional challenge because it prohibits the use of security protocols that have high overhead or require a large number of rounds to accomplish the communication.

The contribution of this paper is to introduce an efficient non-interactive secure protocol preserving privacy of the drivers in V2R communications depending on symmetric cryptographic algorithms to reduce the complexity, the processing time, and the transmission overhead. In addition, tracing malicious drivers should be reachable only by the TTP who is assumed to be fully trusted in the system model, and key revocation of malicious drivers will be obtained in an efficient manner.

4. Existing Technology

Tamper-Resistant Hardware. A hardware, such as a smart card [29], that contains cryptographic keys and algorithms, is considered secure if it has the following properties [30]: (1) read-proof hardware: that is, a hardware that prevents an attacker from reading or accessing its contents; (2) tamper-proof hardware: that is, a hardware that prevents an attacker from changing its contents; (3) self-destructing capability: that is, a hardware that can destroy its contents if an attacker tries to access it. These properties are also defined as a set of security requirements for a cryptographic module [31]. This module should protect private keys from unauthorized disclosure or modification. Similarly, this module should protect public keys against unauthorized modification. The requirements also refer to the Over-the-Air Rekeying (OTAR) [32] protocol if key generation and delivery over the air is desired between the trusted entity (TTP in our network) and the mobile node.

5. The Model

Now, we aim to describe the communication, the adversary, and the system model.

5.1. Communication Model. In the communication model, when the TTP connects with any driver in the network during the setup algorithm, all messages are exchanged through a private and authenticated channel. In the communication among vehicles and between a vehicle and roadside infrastructure, all entities have access to a public channel such that these communications will be over an insecure channel.

5.2. Adversary Model. In the adversary model, we study authentication and privacy protection of the vehicle operators under a malicious adversary, which means that this adversary can see and learn all information sent to or from the corrupted node, and this adversary may also cause corrupted nodes to deviate from the specified protocol in any way.

5.3. System Model. Entities in VANET are classified into three categories.

Network vehicles have the ability to communicate through an open medium. Network vehicles have the lowest security level.

While we might hope that most drivers in the system could be trusted to follow the specified protocol, some drivers will attempt to maximize their gains, regardless of the cost to the system. A greedy driver might try to convince the neighboring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his destination.

Road side infrastructure is the set of RSUs. RSUs are agents of the authority which are deployed at the road sides. An RSU can be a powerful device or a comparatively simple one. RSU is of a semitrust with the medium security level.

In our work, we assume that an RSU is authorized to create safety application messages transmitted to the vehicles on the road, and hence, we can assume that any RSU is an

honest but curious entity. RSUs are not authorized to identify the identity of the sender.

Third trusted party is responsible for management in VANETs. It holds all the secrets and has responsibilities to trace and then revoke malicious drivers in the network. The TTP has the highest security level. The TTP is assumed to be fully trusted and cannot be compromised.

6. The Protocol

Our proposed protocol depends on symmetric cryptographic algorithm, hash function, and simple X-OR operations.

6.1. Description of Our Protocol. The protocol is composed of four algorithms: Setup, Send, Verify, and Trace. These algorithms are described as follows.

Setup. Initially, the TTP generates four secret values, which are sec1, sec2, sec3, and sec4, and generates a symmetric key S that is common among all entities in the V2R network. Then, the TTP stores the value va1 $=$ sec1 $\oplus$ sec2 $\oplus$ sec3, and the symmetric key S on the tamper resistant hardware of the RSUs, where $\oplus$ denotes X-OR.

The TTP picks a unique secret key ps_i for each driver i which belongs to V2R network and computes some initial values for each driver to be used for verification and tracing, and these values are

$$\begin{aligned} A_i &= ps_i \oplus t_i \oplus v_i \oplus \text{sec1},\\ B_i &= t_i \oplus \text{sec2},\\ C_i &= v_i \oplus \text{sec3},\\ D_i &= u_i \oplus v_i,\\ E_i &= u_i \oplus \text{sec4},\\ F_i &= l_i, \end{aligned} \tag{1}$$

where the values v_i, u_i, and l_i are unique for each driver generated by the TTP, but the value t_i can be associated with more than one participant. The previous initial values are initiated such that the following conditions must be satisfied:

$$\begin{aligned} Ps_i \oplus v_i \oplus \text{sec3} &= \text{con1},\\ u_i \oplus v_i \oplus t_i \oplus \text{sec2} &= \text{con2},\\ 1_i \oplus v_i \oplus \text{sec3} &= \text{con3},\\ u_i \oplus l_i \oplus \text{sec4} &= \text{con4}, \end{aligned} \tag{2}$$

where con1, con2, con3, and con4 are constants chosen by the TTP and known for the RSUs.

At the end of the SETUP algorithm, the TTP provides each driver with a tamper-resistant hardware that contains the following data: $Ps_i, A_i, B_i, C_i, D_i, E_i, F_i$, and the common symmetric key S. This tamper-resistant hardware should be installed securely inside the vehicle of the driver.

Send. The driver changes the secret key used for the message encryption and the initial values to avoid associating certain values with a vehicle and a location, and hence, violating drivers' privacy. So, the driver will compute his own information as follows.

First, the driver computes the new secret key to satisfy, $Ps_i' = H(m)$, where $H(m)$ is the one-way hash function of the message m.

It is obvious that the new secret key can be formulated as $Ps_i' = Ps_i \oplus K$, where k is defined as a secret for each message transmission.

The driver can find his new values from

$$\begin{aligned} A_i' &= Ps_i \oplus t_i \oplus v_i \oplus \text{sec1} \oplus k,\\ B_i' &= t_i \oplus \text{sec2} \oplus k,\\ C_i' &= v_i \oplus \text{sec3} \oplus k,\\ D_i' &= u_i \oplus v_i \oplus k,\\ E_i' &= u_i \oplus \text{sec4} \oplus k,\\ F_i' &= l_i \oplus k. \end{aligned} \tag{3}$$

The message m will be encrypted using the new computed secret key Ps_i':

$$c1 = E_{Ps_i'}(m). \tag{4}$$

Then, the new values used for verification and tracing must be encrypted using the common secret key S:

$$c2 = E_s(A_i' || B_i' || C_i' || D_i' || E_i' || F_i'), \tag{5}$$

where $\|$ denotes concatenation, and the cryptographic algorithm used for encryption to produce the ciphertexts c_1 and c_2 is a symmetric key encryption algorithm. The encryption should use cipher block chaining (CBC) mode.

Since the symmetric key S is stored in a tamper-resistant hardware, intruders and any member of V2R network neither know the value of this key nor have access to it. Only the TTP has access to the memory location where this key is stored. Encrypting the values used for verification and tracing using the symmetric key S indicates that the message was generated by a tamper-resistant hardware provided by the TTP during the SETUP algorithm.

At the end of the SEND algorithm, the message to be broadcasted to the RSU is $c1 \| c2$.

Verify. Now, the RSU aims to authenticate if the transmitter is a participant in the V2R network as follows.

The RSU will decrypt the ciphertext c_2 using the symmetric key S, getting

$$D_s(c2) = A_i' || B_i' || C_i' || D_i' |||| E_i' || F_i'. \tag{6}$$

It can find the new symmetric key to decrypt the message m by computing

$$A_i' \oplus B_i' \oplus C_i' \oplus \text{val} = Ps_i \oplus K = Ps_i'. \tag{7}$$

Then, RSU checks if $Ps_i' = H(m)$, if it is satisfied, it verifies that the transmitted data will be correctly used to trace the driver in case of malicious activities, by checking the following conditions:

$$\begin{aligned} Ps_i' \oplus C_i' &= \text{con1}, \\ B_i' \oplus D_i' &= \text{con2}, \\ C_i' \oplus F_i' &= \text{con3}, \\ E_i' \oplus F_i' &= \text{con4}. \end{aligned} \tag{8}$$

If these conditions are satisfied, then, the RSU accepts the message. Otherwise, it rejects the message.

It is evident that these conditions could not be satisfied if the driver is not a participant in the V2R network. Furthermore, the value k must be used in all equations to produce the new values $A_i', B_i', C_i', D_i', E_i'$, and F_i' to verify the previous conditions correctly, this value k is the key used to trace the drivers of disputed message. Additionally, no entity can encrypt his chosen message m', where the new secret key used to encrypt the message is generated from $Ps_i' = H(m)$, which guarantees data integrity.

Trace. This algorithm can be executed only by the TTP as follows.

First, the TTP performs the VERIFY algorithm to authenticate the sender, and if it is verified, the TTP will compute

$$\begin{aligned} T1 &= \text{con1} \oplus Ps_i' \oplus \text{sec3} = v_i' = v_i \oplus k, \\ T2 &= \text{con2} \oplus v_i' \oplus \text{sec2} = u_i \oplus t_i \oplus k, \\ T3 &= B_i' \oplus \text{sec2} = t_i \oplus k, \\ T4 &= E_i' \oplus \text{sec4} = u_i \oplus k, \end{aligned} \tag{9}$$

then

$$\begin{aligned} T5 &= \text{T2} \oplus \text{T3} = u_i, \\ T4 &\oplus \text{T5} = k. \end{aligned} \tag{10}$$

Hence, the secret key $Ps_i = Ps_i' \oplus k$ will be known, which is a unique key for each driver in the network. So, the TTP can trace and then revoke this driver.

It is obvious that these computations cannot be executed without the knowledge of the four secrets sec1, sec2, sec3, and sec4, which are known only for the TTP.

6.2. Key Revocation. Timely access to revocation information is a particularly hard problem in VANETs. Different aspects of revocation were discussed in [23, 33] without a complete solution provided. It proposes the distribution of certificate revocation lists (CRLs) and short-lived certificates, but does not elaborate how to achieve this. Short-lived certificates are also proposed in [7].

But short lifetimes open some vulnerability issues; such an approach is not appropriate for a life-critical VANETs environment. Moreover, certificates have to be refreshed frequently to keep the vulnerability window very small. This could create high loads both on the CA and on the network. In addition, it is not feasible to search a revocation list since it may cause high communication latencies and additional processing time.

In this paper, we assumed a secure tamper-resistant hardware, this hardware contains the common symmetric key S. We showed in previous sections that in order to authenticate the driver and verify that the values would be correctly used in the TRACE algorithm, these values must be encrypted using the common symmetric key S.

Based on the assumption of using a secure tamper-resistant hardware, we propose the following method that allows vehicles to identify values that are not encrypted by the symmetric key S. When the TTP traces malicious driver, to revoke this member, the TTP performs a secure communication with the tamper-resistant hardware of the vehicle which sent the disputed message. Such secure communications should be implemented as Over-the-Air Rekeying (OTAR) specification protocol [32]. This secure communication allows the TTP to access the memory locations where symmetric key S is stored and zeroing these memory locations (maintenance role). Therefore, this tamper-resistant hardware will not be able to encrypt its new values. So, the VERIFY algorithm will fail.

By using the current technology and our proposed technique, we avoided the computational cost and additional processing delay of searching in a list of all revoked keys. Additionally, just zeroing the tamper-resistant hardware of a revoked member does not add any computational or communication costs on the TTP. Moreover, we avoided revealing the identities of revoked members, hence maintaining their anonymity, *backward unlinkability*.

7. Performance Analysis

Now we aim to evaluate the performance of our proposed protocol in terms of privacy preserving, load on the TTP, overheads, invocations, and processing time.

7.1. Privacy Preserving and Security. We aim to discuss the privacy of the drivers in our proposed protocol. The drivers can generate the new secret key for an infinite number of messages. Hence, each vehicle has a large set of secret keys used to encrypt the message; the new key depends on the message itself. Hence, if we assume using MD5 hash function (digest size of 128 bits), the probability to relate messages which are sent by the same driver is $1/2^{128}$, which is a negligible probability. Furthermore, it is obvious that identifying the sender of the message is constrained by knowing the four secret values of the TTP, which is infeasible following the one-wayness security of the X-OR operation.

When implementing DES, 3DES, AES, Blowfish, and RC4 in MATLAB 7.0 software, it is clear that the avalanche effect (a desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text; in particular,

Table 1: Comparison based on avalanche effect.

Technique	1-bit variation in key keeping plaintext constant	1 bit variation in plaintext keeping key constant
DES	30	34
3DES	37	33
AES	64	71
Blowfish	37	23
RC4	0	1

Table 2: Number of innovations of our proposed protocol.

Operation	Symmetric encryption	Symmetric decryption	Hash function	Bit X-OR
Send	2	—	1	7
Verify	—	2	1	5
Trace	—	2	1	8

a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts) is highest in AES. It is medium in DES, 3DES, and Blowfish. It is smallest in RC4. Therefore, if one desires a good avalanche effect, AES is the best option as shown in Table 1. Hence, we recommend AES (advanced encryption standard) as the symmetric key encryption of our proposed protocol.

Brute forcing AES-128 is unlikely to be practical in the foreseeable future. According to NIST, assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{255} keys per second), then it would take that machine approximately 149 thousand billion (149 trillion) years to crack a 128-bit AES key.

7.2. Load on the TTP. As the drivers need not to issue a new value from the TTP with each message transmission as these values could be computed by the member himself without any dependence on the TTP, we can eliminate the load on the TTP and on the network that overloaded on the CA when executing any of the protocols [4, 10–12].

7.3. Overheads. It is evident that the messages to be transmitted through the network are $c1 \| c2$, which are the ciphertexts of a symmetric cryptographic algorithm.

Using the AES algorithm as our proposed symmetric cryptographic algorithms, then, the size of the produced ciphertext will be 128 bits. As a result, the overall overhead will be 256 bits (32 bytes). Additionally, the message itself need not to be transmitted through the network. Hence, it is a very low overhead compared to other existing protocols aiming to achieve the security requirements of VANETs.

7.4. Invocations and Processing Time. It is evident that the proposed protocol requires a very simple computation to be executed and, hence, very small processing time due to dependency on the symmetric cryptographic algorithms. We show in Table 2 the number of invocations of our proposed protocol. Additionally, TRACE algorithm will be executed only in case of malicious activity, but it does not add any computational or communication costs during regular communications.

Table 3: Number of invocations of similar methods.

Operation	Invocations of protocol [1]	Invocations of protocol [2]
RSA encryption	2	2
RSA decryption	2	2
DSA signature	1	1
DSA signature verification	1	1
Modular exponentiation	2	4

Table 4: Listing some of cryptochips.

Cryptochip	IPSec-AES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
SafeXcel-1841	2000	1220	1250
SafeXcel-1841	3200	1400	1440

The proposed protocol in [1, 2] allows the network members to change their own set of keys frequently with each message transmission without any load on the TTP. However, these protocols depend on PKI which suffers from the computational costs. The number of innovations required for executing these protocols is shown in Table 3.

As the cryptographic algorithms take a significant amount of time if the algorithms are implemented in software, current advancements in technologies provide hardware cryptographic coprocessors for use in securing financial applications, e-commerce, and SSL (secure socket layer) transactions. These coprocessors [34, 35] accelerate the algorithms used to implement IPSec and SSL VPNs, allowing vendors to create multifunctional security appliances with a single security coprocessor. Some of crypto chips supporting symmetric and asymmetric encryption algorithms are shown in Table 4.

8. Conclusion

In this paper, we introduced a noninteractive secure protocol preserving privacy of the drivers in V2R communication networks. Our protocol is based on symmetric key cryptographic algorithm, hash function, and simple X-OR operations. The privacy of the drivers can be preserved by the frequent change of the symmetric key and the initial values used for verification and tracing. The dependence on symmetric cryptographic algorithm provides the minimum overheads, minimum complexity, minimum processing time, and with no load on the TTP during the communication between vehicles and RSUs when broadcasting safety application messages, which proves the practicality and effectiveness of our proposed protocol in V2R communication networks.

In case of malicious activities, the only one who has the right to trace and revoke the driver of disputed message is the TTP who is assumed to be fully trusted. In addition, we propose an efficient way to revoke malicious drivers which

avoids the computational cost and additional processing delay of searching in a list of all revoked keys and avoids revealing the identities of revoked members, hence, maintaining their anonymity.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

References

[1] F. M. Salem, M. H. Ibrahim, and I. I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *Proceedings of the 6th International Conference on Networking and Services (ICNS '10)*, pp. 156–161, Cancun, Mexico, March 2010.

[2] F. M. Salem, M. H. Ibrahim, and I. I. Ibrahim, "Non-interactive secure and privacy preserving protocol for inter-vehicle communication networks," in *Proceedings of the 7th International Conference on Information Technology—New Generations (ITNG '10)*, pp. 108–113, Las Vegas, Nev, USA, April 2010.

[3] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Professional*, vol. 6, no. 1, pp. 24–29, 2004.

[4] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV '05)*, 2005.

[5] P. Papadimitratos, V. Gligor, and J. P. Hubaux, "Securing vehicular communications—assumptions, requirements, and principles," in *Proceedings of the Workshop on Embedded Security in Cars (ESCAR '06)*, 2006.

[6] M. Gerlach, "VaneSe—an approach to VANET security," in *Proceedings of the Vehicle-to-Vehicle Communications (V2VCOM '05)*, 2005.

[7] M. Jakobsson and S. Wetzel, "Efficient attribute authentication with applications to ad hoc networks," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04)*, pp. 38–46, October 2004.

[8] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, 2006.

[9] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Proceedings of the European Wireless*, 2002.

[10] B. Askwith, M. Merabti, Q. Shi, and K. Whiteley, "Achieving user privacy in mobile networks," in *Proceedings of the 13th Annual Computer Security Applications Conference (ACSAC '97)*, pp. 108–116, December 1997.

[11] D. Samfat and R. Molva, "A method providing identity privacy to mobile users during authentication," in *Proceedings of the Workshop on Mobile Computing Systems and Applications*, pp. 196–199, December 1994.

[12] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, 2004.

[13] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: providing location privacy for VANET," in *Proceedings of the Conference on Embedded Security in Cars (ESCAR '05)*, 2005.

[14] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[15] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[16] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[17] J.-S. Chou and Y. Chen, "A secure anonymous communication scheme in vehicular ad hoc networks from pairings," http://eprint.iacr.org/2010/028.pdf.

[18] M. H. Ibrahim, "Noninteractive, anonymously authenticated, and traceable message transmission for VANETs," *International Journal of Vehicular Technology*, vol. 2009, Article ID 702346, 14 pages, 2009.

[19] M. H. Ibrahim, "Resisting traitors in linkable democratic group signatures," *International Journal of Network Security*, vol. 9, no. 1, pp. 51–60, 2009.

[20] P. Wex, J. Breuer, A. Held, T. Leinmüller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proceedings of the IEEE 67th Vehicular Technology Conference-Spring (VTC '08)*, pp. 2800–2804, May 2008.

[21] F. Doetzer, "Privacy issues in vehicular ad hoc networks," in *Proceedings of the 5th international conference on Privacy Enhancing Technologies (PET '05)*, Lecture Notes in Computer Science, pp. 197–209, 2005.

[22] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04)*, pp. 29–37, New York, NY, USA, October 2004.

[23] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET'07) in conjunction with ACM MobiCom*, pp. 19–28, September 2007.

[24] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proceedings of the 8th International Symposium on Autonomous Decentralized Systems (ISADS '07)*, pp. 344–351, March 2007.

[25] C. A. Nataraj, "Problems and their solutions when using GPAS based on VANETs," in *Proceedings of the International Conference on Information and Computer Networks (ICICN '12)*, 2012.

[26] B. Qin, Q. Wu, J. Domingo-Ferrer, and L. Zhang, "Preserving security and privacy in large-scale," in *Proceedings of the 13th International Conference on Information and Communications Security (ICICS '11)*, pp. 121–135, 2011.

[27] S. -B. Lee, J. -S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," *Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2715–2728, 2012.

[28] H. K. Choi, I. H. Kim, and J. C. Yoo, "Secure and efficient protocol for vehicular ad hoc network with privacy preservation," *Eurasip Journal on Wireless Communications and Networking*, vol. 2011, Article ID 716794, 2011.

[29] Smart Card Alliance, http://www.smartcardalliance.org.

[30] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin, "Algorithmic tamper-proof (ATP) security: theoretical

foundations for security against hardware tampering," in *Proceedings of the Theory of Cryptography Conference (TCC '04)*, vol. 2951 of *Lecture Notes in Computer Science*, pp. 258–277, Berlin, Germany, 2004.

[31] FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, U.S. Department of Commerce, 1994.

[32] Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB-102.AACA, January 1996, Telecommunications Industry Association.

[33] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proceedings of the 7th International Conference on Intelligent Transport Systems Telecommunications (ITST '07)*, pp. 339–344, June 2007.

[34] SafeNet Inc Data sheet for SafeXcel 1841 security co-processor.

[35] SafeNet Inc Data sheet for SafeXcel 1842 security co-processor.