ATLANTIS PRESS

Advances in Engineering Research, volume 140

2nd International Conference on Electrical, Control and Automation Engineering (ECAE 2017)

A Secure and Efficient Scheme with Batch-Verification for Vehicular Ad-Hoc Network

Fuyuan Tan[1], Fei Tang[2], Wenjun Luo[3] and Zhong Hong[4]

[1]College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
[2]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China
[3]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China
[4]College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China

***Abstract*—Vehicular ad hoc network (VANET) is a special kind of Mobile ad hoc network (MANET) which can improve the traffic control systems. Due to the limitation of wireless communications, efficiency and bandwidth are two important issues need to be considered for its design. In this work, we design a secure and efficient scheme with batch-verification for vehicular ad hoc network. Compared to existing secure VANET-based authentication schemes, our scheme has higher efficiency and lower bandwidth.**

Keywords-VANET; security; efficiency; batch-verification

I. INTRODUCTION

With the increasing of the number of vehicles, traffic problems, such as traffic congestion, parking difficulty, traffic accidents and so on, frequently occur around us. Therefore, how to improve the traffic control systems to fit the new traffic environment is a very important problem. Based on such reality requirement background, researchers introduced the notion of vehicular ad hoc network (VANET) [10], [17]. As a special kind of mobile ad hoc network (MANET) [4], [20], VANET is hopeful to revolutionize the human driving experiences and improve the traffic control systems.

Generally, VANET contains three objects: trusted authority (TA), road side units (RSU), and on board unit (OBU). TA is a regional trusted authority which is responsible for issuing and maintaining authentication information of identity of each network node in VANET. OBU is installed in the vehicles as a trusted platform module which allows vehicle to communicate with RSUs or other vehicles through wireless channel. RSU is deployed along the roads which can communicate with TA through a secure transmission protocol, such as the wired channel and communicate with OBUs through wireless channel.

There are two central challenges in VANET, secure authentication [1], [9], [21] and privacy issues [6], [13]. Generally, the notion of secure authentication is that it is able to ensure the integrity of message and guarantee the authenticity of the message sender. However, on the other side, the driver of vehicle, i.e., message sender, does not want his or her private information, e.g., real identity, to be revealed during communications. Due to the limitations of wireless communications, efficiency and bandwidth undoubtedly are two important factors need to be seriously considered for the design of authentication protocol. According to the dedicated short range communications (DSRC) protocol [3] which can be used to application scenario of VANET, each vehicle should broadcast a traffic related message every 100-300ms. Assume that there has 100 vehicles in the area of an RSU, the RSU will receive over 20000-60000 messages within one minute. Therefore, on the premise of privacy preservation, how to improve the authentication efficiency and reduce the communication bandwidth is the core issue in VANET.

II. RELATED WORK

In recent years, privacy issues and security authentication have been extensively studied in the field of VANET.

The authentication schemes which are based on public key infrastructure (PKI), e.g., [16], [14] can be used to protect the real identities of users and ensure both the security authentication and integrity of message. In such schemes, TA preloads a large number of pseudonymous public-secret key pairs as well as the corresponding public certificates in each vehicle. According to the public certificates, each vehicle would be generated a short lifetime pseudo identity to protect the real identity. However, there has two shortcomings in PKI-based schemes [2], [15], [18]: First, a large number of public and secret keys as well as public certificates need to be preloaded into each vehicle, thus, the systems are need to equipped with massive storage device. Second, it is a tough work to update or revoke the public certificates.

In order to improve the efficiency of authentication, Zhang et al. [22] proposed an identity-based batch verification (IBV) scheme for the communications between RSUs and vehicles. In their scheme, identity-based cryptography was adopted to generate pseudo identities, so it decreases the costs of public certificates. In the mean time, it allows RSU to verify a bunch of messages from multiple vehicles at the same time through batch verification operation. In addition, the vehicle privacy was protected by pseudo identity, while TA has the ability to trace the real identity of the message sender from pseudo identity. In addition, Lo et al. [13], Liu et al. [10], Hu et al. [8], Xie et al. [19] proposed an identity-based authentication scheme for VANET, respectively.

In this work, we design a secure and efficient scheme with batch-verification for vehicular ad-hoc network. Compared to existing secure VANET-based authentication schemes, our scheme has higher efficiency and lower bandwidth.

III. PRELIMINARY

A. System Model

The system model of VANET is shown in the following Figure.

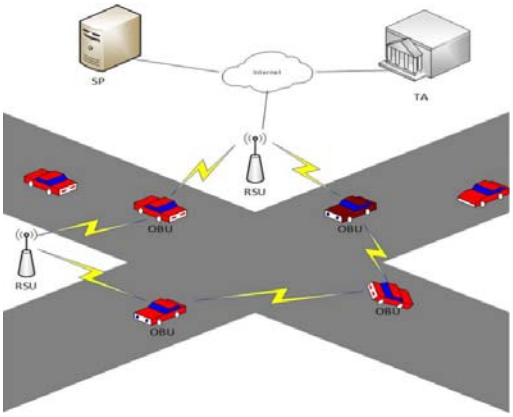

FIGURE I. SYSTEM MODEL OF VANET

There has four entities in VANET [10]: a trusted authority (TA), application service provider (SP), road side units (RSU), and on-board units (OBU) equipped on vehicles. Formally:

- TA could be the transportation management departments. The responsibilities of the TA are to generate system global security parameters and publish public/secret keys for all participants. We assume that TA is credible, available and never compromised all the time.
- SP provides application services for all participants in system. It is responsible for making further analysis and giving feedback to RSU after receiving traffic related information.
- RSU is a telecommunication device which is installed along roadside. According to DSRC protocol, RSUs and vehicles could communicate with each other. RSU, TA and SP could communicate by a safety cable channel. The main duty of RSU is to verify the validity of the message from vehicles.
- OBU is a wireless communication unit which is installed in each vehicle in VANET. It could communicate with RSUs or other OBUs by using DSRC protocol.

B. Security Requirement

A secure message authentication scheme for VANET should satisfy the following requirements [5], [7]:

- *Message integrity and authentication*: In VANET, after receiving messages, the receiver (RSU or vehicles) should ensure the integrity of the message as well as the authentication of the senders by verifying the signatures.
- *Identity privacy preserving*: The real identity of each vehicle should be kept anonymous from RSUs and other vehicles, which can only be known by the vehicle itself and TA. Any third party could not be able to expose the vehicle's real identity through analyzing messages sent by it.
- *Traceability*: When there has dispute, TA should have ability to trace the real identity of the sender according to the message.

C. Bilinear Map

Let G_1 and G_2 be two cyclic groups. Both orders of G_1 and G_2 are prime q. Assume that P is a generator of G_1. We say that $e: G_1 \times G_1 \to G_2$ is a bilinear map if it satisfies the following properties:

- *Bilinearity*: Given $P, Q \in G_1$, we have

$$e(P, Q+R) = e(P,Q)e(P,R)$$

In particularly, for any $a, b \in Z_q^*$, we have

$$e(aP, bQ) = e(P, bQ)^a = e(P, aQ)^b = e(P,Q)^{ab}$$

$$= e(abP, Q) = e(P, abQ).$$

- *Non-degeneracy*: $e(P,P) \neq 1$.
- *Computability*: For all $P, Q \in G_1$, $e(P,Q)$ can be computed efficiently.
- *Symmetric*: $e(P,Q) = e(Q,P)$ for all $P, Q \in G_1$.

D. Discrete Logarithm (DL) Problem

Given two random elements $P, Q \in G_1$, the DL problem is to find a which satisfies $Q = aP$.

IV. OUR PROPOSED SCHEME

A. System Setup

In this phase, TA generates and publishes some system parameters as follows:

- TA produces the parameters of bilinear map $\{G_1, G_2, q, P, e\}$.
- TA chooses three hash functions: $H: \{0,1\}^* \to Z_q^*$,

$$H_1: \{0,1\}^* \to Z_q^*, H_2: \{0,1\}^* \to G_1.$$

- TA chooses a random integer $s \in Z_q^*$ as the master secret key and computes $P_{pub} = sP$ as the system

public key. Then, TA publishes the system parameters $\{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2\}$.

- Each vehicle is assigned with a real identity *RID* and a password *PWD*. TA preloads *RID*, *PWD*, system parameters and the system master secret key s into each vehicle's tamper-proof device.

B. Pseudo Identity Generation

First of all, vehicle V_i takes as inputs it's own *RID* and *PWD* into tamper-proof device. Then, the tamper-proof device checks the values of *RID* and *PWD*, if one of the values is incorrect, the tamper-proof device refuses the request. Otherwise, it generates the pseudo identity for V_i as follows:

$$PID_i^1 = r_i P \tag{1}$$

$$PID_i^2 = RID \oplus H(r_i P_{pub}) \tag{2}$$

where $r_i \in Z_q^*$ is a random integer chosen by the tamper-proof device. The pseudo identity of the vehicle V_i is $PID_i = (PID_i^1, PID_i^2)$.

C. Extract

After the pseudo identity of V_i was generated, tamper-proof device then computes responding secret key $sk_i = (K_i, s_i)$ as follows:

$$K_i = k_i P \tag{3}$$

$$s_i = k_i + H_1(PID_i^1 \| PID_i^2 \| K_i) \times s \pmod q \tag{4}$$

where $k_i \in Z_q^*$ is a random integer, $K_i \in G_1$ and $s_i \in Z_q^*$. Finally, the tamper-proof device stores up $\{PID_i, sk_i\}$.

D. Message Signing

To ensure the integrity of message and authenticity of sender, messages sent by the vehicle V_i should be signed before broadcasting. To sign a message m_i, the vehicle V_i computes:

$$U_i = s_i H_2(PID_i^1 \| PID_i^2 \| st_i \| m_i) \tag{5}$$

where st_i is a current timestamp of the message signing. Then, vehicle V_i broadcasts the tuples $\{PID_i, m_i, st_i, K_i, U_i\}$.

E. Message Verification

When a RSU or vehicle receives the tuples $\{PID_i, m_i, st_i, K_i, U_i\}$, assume that the receiving time is vt and Δt is the predefined endurable transmission delay. If $vt - st_i \le \Delta t$, the RSU or vehicle calculates:

$$h_{i,1} = H_1(PID_i^1 \| PID_i^2 \| K_i) \tag{6}$$

$$h_{i,2} = H_2(PID_i^1 \| PID_i^2 \| st_i \| m_i) \tag{7}$$

where $h_{i,1} \in Z_q^*$, $h_{i,2} \in G_1$, $K_i \in G_1$. Then checks whether the following equation holds:

$$e(U_i, P) = e(K_i, h_{i,2}) e(h_{i,1} P_{pub}, h_{i,2}) \tag{8}$$

If holds, RSU or vehicle accepts the message. Otherwise, rejects it.

F. Batch Verification

Given n tuples: $\{PID_1, m_1, st_1, K_1, U_1\}$, $\{PID_2, m_2, st_2, K_2, U_2\}$, ..., $\{PID_n, m_n, st_n, K_n, U_n\}$ which are sent by n different vehicles, if $vt - st_i \le \Delta t$ for all $i (1 \le i \le n)$, the receiver verifies their validity as follows:

$$e(\sum_{i=1}^n U_i, P) = e(\sum_{i=1}^n K_i, h_{i,2}) e(\sum_{i=1}^n h_{i,1} P_{pub}, h_{i,2}) \tag{9}$$

If holds, RSU or vehicle then accepts the n messages. Otherwise, rejects it.

For purpose of overcoming the attack emphasized by Liu etal. [11], we would replace the above batch equation with the following equation, where $\alpha_i \in_R \{0,1\}^l$ are randomly chosen for $i = (0, 1, 2, ..., n)$. Ordinarily l = 80 is enough for normal schemes in VANETs:

$$e(\sum_{i=1}^n \alpha_i U_i, P) = e(\sum_{i=1}^n \alpha_i K_i, h_{i,2}) e(\sum_{i=1}^n \alpha_i h_{i,1} P_{pub}, h_{i,2}) \tag{10}$$

If (10) holds, it means that these distinct n signatures are valid.

V. SECURITY ANALYSIS

In this section, we show the security of our proposed scheme.

1) Message authentication and integrity: In VANET, the message from a vehicle or RSU should be ensured that this message can not be modified or forged by attackers. The message authentication and integrity depends on the correctness of the verification equation.

2) Identity privacy preserving: In our scheme, each vehicle V_i has a pseudo identity PID_i which contains a random chosen r_i. Without r_i and s, any malicious adversary cannot recover the real identity of from its pseudo identity due to the hardness of the CDH problem. Hence, the identity privacy is preserved.

3) Traceability: Given a pseudo identity $PID_i = (PID_i^1, PID_i^2)$ of vehicle V_i, TA can recover the real identity RID as follows:

$$\begin{aligned} & PID_i^2 \oplus H(sPID_i^1) \\ &= PID \oplus H(r_i P_{pub}) \\ &= RID \oplus H(s \cdot r_i P) \oplus H(r_i P_{pub}) \\ &= RID \end{aligned}$$

Therefore, TA can trace the real identity of the malicious vehicle V_i.

4) Replaying attack: In our scheme, we make use of st_i to present the timestamp of the message signing phase and vt to present the timestamp of the signature verification phase, Δt to stand for the predefined endurable transmission delay. If and only if $vt - st_i \le \Delta t$, the message will be considered for the verification. Therefore, our scheme can avoid the replaying attack from malicious user.

5) Master private key: In our scheme, the master secret key s is only used in the Extract algorithm to generate vehicle's secret key s_i. In the Message Signing algorithm, vehicle will make use of s_i to sign messages. Therefore, the master secret key is kept secretly in the signing phase.

VI. COMPARISONS

In this section, we compare our scheme to existing efficient VANET-based authentication schemes of [22], [12], [13], [8], [19] from the aspects of security, computation overhead, and bandwidth, respectively.

A. Security

As shown in the Table 1, the scheme of [22] can not avoid replaying attack and does not satisfy the security of "master secret key is kept secretly" which means that the scheme makes use of the master secret key to sign messages directly. Schemes in [12] and [13] can not avoid replaying attack. Schemes in [8] and [19] always use master secret key to sign messages directly. Our proposed scheme satisfies all of the security issues.

TABLE I. SECURITY COMPARISON

Schems	Auth and inte	Priv pres	Trac	Rep att	MSK kept secretly
[22]	√	√	√	×	×
[12]	√	√	√	×	√
[13]	√	√	√	×	√
[8]	√	√	√	√	×
[19]	√	√	√	√	×
Ours	√	√	√	√	√

(where "Auth and inte" means "authentication and integrity", "Priv pres" means "privacy preservation", "Trac" means "traceability", "Rep att" means "replaying attack", and "MSK kept secretly" means the master secret key is only used in the extract algrorithm to create vehicle's secret key.)

B. Computational Overhead

Computational overhead is one of the most important issues in VANET, which directly influences the value of traffic related message. We adopted the same items to Tzeng et al's [17] scheme and only take the dominated steps into account, such as T_{par} denotes the time for performing one bilinear pairing operation, and T_{mul} as the time for performing one point multiplication operation on G_1. The following results are gotten: T_{par} is 4.5ms, and T_{mul} is 0.6ms.

We compared our proposed scheme with the existing schemes proposed by Zhang et al's [22], Liu et al's [12], Lo et al's [13], Hu et al's [8] and Xie et al's [19]. From the data statistics in Table 2, [22]'s scheme needs 14.7 ms to verify a single message and needs (14.1+0.6n) ms to verify *n* messages. [12]'s scheme needs 10.2 ms to verify a single message and needs (9.6 + 0.6n) ms to verify *n* messages. [13]'s scheme needs 4.5 ms to verify a single message and needs (2.7 + 1.8n) ms to verify *n* messages. [19]'s scheme needs 26.1 ms to verify a single message and needs nearly (23.7 + 2.4n) ms to verify *n* messages. [8]'s scheme needs 1.2 ms to verify a single message or *n* messages. Our proposed scheme needs 1.2 ms to verify a single message and needs (0.6+0.6n) ms to verify *n* messages. However, we can see that the scheme [22], [8], [19] are not secure owing to using the master private key secretly.

According to the above analysis, the efficiency and bandwidth of our scheme are ideal on the basis of the premise of security.

TABLE II. COMPUTATION COST COMPARISON

Schemes	Verifying a single message	Verifying n messages
[22]	$3T_{par} + 2T_{mul}$	$3T_{par} + (n+1)T_{mul}$
[12]	$2(T_{par} + T_{mul})$	$2T_{par} + (n+1)T_{mul}$
[13]	T_{par}	$3(n+1.5)T_{mul}$
[8]	$2T_{mul}$	$2T_{mul}$
[19]	$5T_{par} + 6T_{mul}$	$5T_{par} + 4(n+0.5)T_{mul}$
Ours	$2T_{mul}$	$(n+1)T_{mul}$

VII. CONCLUSION

Vehicular ad hoc network (VANET) has the properties of short delay requirement and frequent communications, and hence the high computation efficiency and low communication bandwidth are two very important factors for VANET. In this work, we proposed a secure and efficient scheme with batch-verification for vehicular ad hoc network. Comparing existing VANET-based authentication schemes, our scheme has better security and performance simultaneously.

ACKNOWLEDGEMENT

The authors would like to thank anonymous reviewer for their helpful comments and suggestions. The work is supported by the National Natural Science Foundation of China (No. 61702067), the Natural Science Foundation of Chongqing (No. cstc2017jcyjAX0201), and the Science and Technology Research Project of Chongqing Municipal Education Commission (No. KJ1600445).

REFERENCES

[1] Ahmedzaid F, Bai F, Bai S, et al. Vehicle safety communications applications (vsc-a) final report: appendix volume 3 security. Global Positioning System, 2011.

[2] Bhattacharya A K, Das A, Roychoudhury D, Lyer A, Bhattacharya D.Autonomous certification with list-based revocation for secure v2v communication. International Conference on Information Systems Security, Springer, 2012: 208-222.

[3] Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[4] Eissa T, Razak S A, Ngadi M A. A novel lightweight authentication scheme for mobile ad hoc networks. Arabian Journal for Science and Engineering, 2012, 37(8): 2179-2192.

[5] Engoulou R G, Bellaiche M, Pierre S, Quintero A. VANET security surveys. Computer Communications, 2014, 44(5): 1-13.

[6] Gamage C, Gras B, Crispo B, Tanenbaum A S. An identity-based ring signature scheme with enhanced privacy. Securecomm and Workshops 2006, IEEE, 2006: 1-5.

[7] He D, Zeadally S, Xu B, Huang X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[8] Hu X, Wang J, Xu H, Liu Y, Zhang X. Secure and pairing-free identity-based batch verification scheme in vehicle ad-hoc networks. International Conference on Intelligent Computing, Springer, 2016: 11-20.

[9] Jenefa J, Anita E A M. A Signature-based secure authentication framework for vehicular ad hoc networks. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2016, 10(2): 378-383.

[10] Lin X, Lu R, Zhang C, Zhu H, Ho P, Shen X. Security in vehicular ad hoc networks. IEEE communications magazine, 2008, 46(4): 88-95.

[11] Liu J K, Yuen T H, Man H A, et al. Improvements on an authentication scheme for vehicular sensor networks[J]. Expert Systems with Application, 2014, 41(5):2559-2564.

[12] Liu Y, He Z, Zhao S, Wang L. An efficient anonymous authentication protocol using batch operations for VANETs. Multimedia Tools and Applications, Springer, 2016, 75(24): 17689-17709.

[13] Lo N W, Tsai J L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1319- 1328.

[14] Lu R, Lin X, Zhu H, Ho P H, Shen X. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. INFOCOM 2008, IEEE, 2008: 1229-1237.

[15] Rabadi N M, Mahmud S M. Drivers' anonymity with a short message length for vehicle-to-vehicle communications network. The 5th IEEE Consumer Communications and Networking Conference, IEEE, 2008: 132-133.

[16] Raya M, Hubaux J P. Securing vehicular ad hoc networks. Journal of Computer Security, 2007, 15(1): 39-68.

[17] Tzeng S, Hong S, Li T, Wang X, Huang P H, . Enhancing security and privacy for identity-based batch verification scheme in VANET. IEEE Transactions on Vehicular Technology, 2015, 66(4): 1-12.

[18] Vaidya B, Makrakis D, Mouftah H. Effective public key infrastructure for vehicle-to-grid network. Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications. ACM, 2014: 95-101.

[19] Xie Y, Wu L, Zhang Y, Shen J. Efficient and secure authentication scheme with conditional privacy-preserving for VANETs. Chinese Journal of Electronics, 2016, 25(5): 950-956.

[20] Ying L, Yang S, Srikant R. Optimal delay-throughput tradeoffs in mobile ad hoc networks. IEEE Transactions on Information Theory, 2008, 54(9): 4119-4143.

[21] Zhang C, Lin X, Lu R, Ho P H, Shen X. An efficient message authentication scheme for vehicular communications. IEEE Transactions on Vehicular Technology, 2008, 57(6): 3357-3368.

[22] Zhang C, Lu R, Lin X, Ho P H, Shen X. An efficient identity-based batch berification scheme for vehicular sensor networks. INFORCOM 2008, IEEE, 2008: 246-250.