SPA: Self-certified PKC-based Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks

Jianhong Zhang, Yuanbo Cui, Zhipeng Chen
College of Science, North China University of Technology
Beijing 100144, P.R.China

Abstract

As an important component of Intelligent Transportation Systems (ITS), vehicular ad hoc *networks can provide safer and more comfortable driving circumstance for the drivers. Pseudonyms certificate and group-oriented signature are two most widely adopted privacy-preserving technique in VANET. However, the two methods exists many efficiency flaws which affect their application. To overcome the above problems which exist in the above two methods. In this paper, we propose a novel privacy-preserving authentication protocols based on self-certified signature. And we show that our scheme can achieve conditional privacy-preserving and is proven be secure in the random oracle. Furthermore, the scheme has the following advantages: short length of the signature and low computation.*

Keywords: *VANETs, self-certified cryptography, anonymous authentication*

1: Introduction

To satisfy increasing requirement of enhancing transportation safety and efficiency, vehicular ad hoc network (VANET) emerges. It is a special kind of mobile ad hoc networks consisting of entities including the vehicles, also known as on-board units (OBUs), and the roadside units (RSUs). In a vehicular ad hoc network, the OBUs and RSUs, equipped with on-board sensory, processing, and wireless communication modules, can form a self-organized networks. In VANET, each vehicle can not only communicate with each other, i.e,vehicle-to-vehicle (V-2-V) communication, but also communicate with roadside unit, i.e., vehicle-to-infrastructure (V-2-I) communication. Therefore, compared with the traditional pure infrastructure-based network, the hybrid of V-2-V and V-2-I communications is promising since it can not only overcome the disadvantages of infrastructure-based network, but also overcome the disadvantage of non-infrastructure -based network. As for the development of VANETs, it is expected to serve as a general platform for the development of any vehicle centered applications [1] in the near future. However,before deploying VANET for practical application, security and privacy issues must be addressed. Otherwise, the VANET might be confronted with many potential attacks, for example, malicious attacks, route tracing,service abuses and sybil attack, and so on.

The most widely adopted privacy-preserving technique in VANET is divided into two types. one is based on pseudonyms certificate, during registration, each vehicle is supposed to pre-loaded a large number of pseudonyms certificates with pseudo identities in this type,and randomly chooses one of the available pseudonymous certificates for signing a

message at one time. However, when a vehicle is revoked, all the pseudo identities would be added into a CRL. Thus, certificate management and revocation are troublesome; the other is based on on group-oriented signature which is a combination of group signature(ring signature) and ID-based signature. Each vehicle is considered as a group member and can anonymously produce a message-signature. However, the length of group signature is much longer than one of ordinary signature and the computational cost of verifying group signature is high, and the revocation of member is the inherent problem in the group signature.

Self-certified public key cryptosystem was introduced by Girault[7]. In the self-certified public key system, certificate verification and management are not required and the key escrow problem can be eliminated. The idea is that certificate is replace by a witness and the public key is embedded in it. Anyone who holds a witness along with an attributive identity can recover the corresponding public key to verify signature. Thus, it leads in the reduction of communication, computation and storage amount.

To overcome the above problems in the privacy-preserving, we propose a novel privacy-preserving authentication protocols to address the security and privacy based on self-certified signature in this paper. And we show that our scheme can achieve conditional privacy preserving and is proven be secure in the random oracle. And the proposed scheme has the following advantages: short length of the signature and low computation.

2: Preliminaries

2.1: Objectives

To avoid reinventing the wheel, refer to [1] for a full discussion of the attack and security requirements to the interested reader. In the following, we focus on anonymity and liability.

1. Anonymity: it includes vehicle's identity anonymity and anonymous user authentication. vehicle's identity anonymity denotes that given a safety message with a valid signature, identifying the actual signer is computationally hard for everyone but the trusted authority. Malicious nodes cannot obtain the private information of the vehicles from the safety message. Anonymous user authentication indicates that the process of attempting to verify that a user is authentic and legitimate but does not reveal the real identity of the user.
2. Liability: If a malicious vehicle with OBU produces a fraudulent message. Then the authority must be able to open the corresponding signature to trace the actual identity of the vehicle. Our design objective is to make that TA can open a group signature with the TA's master key to compute the real identity of the sender.

2.2: Bilinear map and security assumption

In this subsection, we briefly review the properties of the bilinear pairings.

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be three cyclic multiplicative group with the prime order q. Let g_1, g_2 be the generator of groups $\mathbb{G}_1$ and $\mathbb{G}_2$ An admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, which satisfies the following three properties:

- Bilinear: If $u \in \mathbb{G}_1, v \in \mathbb{G}_2$ and $a, b \in Z_q^*$, then $e(u^a, v^b) = e(u, v)^{ab}$;

- Non-degenerate: There exists a $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ such that $e(g_1, g_2) \neq 1$;
- Computable: If $u \in \mathbb{G}_1, v \in \mathbb{G}_2$, one can compute $e(u, v) \in \mathbb{G}_T$ in polynomial time.

The Weak Computational Diffie-Hellman Problem (WCDH):Let $\mathbb{G}_1$ be a multiplicative cyclic group of order q, g_1 is a generator of group $\mathbb{G}_1$. Z_q is a finite field. Given $k+1$ values $(g_1, g_1^a, g_1^{a^2}, \cdots, g_1^{a^k})$, where k is an integer and $a \in Z_q$, the goal of $k-$weak CDH problem is to compute $g_1^{a^{-1}}$.

The $k-$wCDH problem is $(t, \epsilon)-$hard, if there is no PPT algorithm $\mathcal{A}$ can solve the $k-$wCDH problem in time at most t with probability ϵ if

$$Adv_{k,\mathcal{A}} = Pr[g_1^{a^{-1}} \leftarrow \mathcal{A}(g_1, g_1^a, \cdots, g_1^{a^k}) : a \in_R Z_q] \geq \epsilon$$

The $k-$wCDH problem is a new hard problem. The hardness of the problem is based on the difficulty of solving Collusion Attack Algorithm with k traitors.

The $k+1$ Exponent Problem (EP) . Let $\mathbb{G}_1$ be a multiplicative cyclic group of order q, g_1 is a generator of group $\mathbb{G}_1$. Z_q is a finite field. Given $k+1$ values $(g_1, g_1^a, g_1^{a^2}, \cdots, g_1^{a^k})$, where k is an integer and $a \in Z_q$, its goal is to compute $g_1^{a^{k+1}}$.

The $k+1$EP is $(t, \epsilon)-$hard, if there is no PPT algorithm $\mathcal{A}$ can solve the $k+1$ EP in time at most t with probability ϵ if

$$Adv_{k,\mathcal{A}} = Pr[g_1^{a^{k+1}} \leftarrow \mathcal{A}(g_1, g_1^a, \cdots, g_1^{a^k}) : a \in_R Z_q] \geq \epsilon$$

The hardness of $k+1$ exponent problem is proved that it is polynomial time equal to the k-wCDHP.

The Extended $k+1$ Exponent Problem (EP) Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of order q, g_2 is a generator of group $\mathbb{G}_2$. Z_q is a finite field, ψ is a computable isomorphism from group $\mathbb{G}_2$ onto group $\mathbb{G}_1$ such that $\psi(g_2) = g_1$. Given $k+1$ values $(g_2, g_2^a, g_2^{a^2}, \cdots, g_2^{a^k})$ and a isomorphism map ψ, where k is an integer and $a \in Z_q$, its goal is to compute $g_1^{a^{k+1}}$.

The Extended $k+1$EP is $(t, \epsilon)-$hard, if there is no PPT algorithm $\mathcal{A}$ can solve the extended $k+1$ EP in time at most t with probability ϵ if

$$Adv_{k,\mathcal{A}} = Pr[g_1^{a^{k+1}} \leftarrow \mathcal{A}(g_2, g_2^a, \cdots, g_2^{a^k}, g_1 = \psi(g_2)) : a \in_R Z_q, \psi(\cdot)] \geq \epsilon$$

3: Our privacy-preserving authentication scheme

In the following, our privacy-preserving authentication protocol is proposed. The main idea in the scheme is based on self-certified signature. The system consists of two parties. i.e. the vehicle and the trusted authority (TA).

System Initialization: The trusted parties (TA) set up the system as follows. Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be three multiplicative cyclic groups of the same prime order q. $g_2 \in \mathbb{G}_2$ is a generators of group $\mathbb{G}_2$. ψ is a computable isomorphism from group $\mathbb{G}_2$ onto group $\mathbb{G}_1$ such that $\psi(g_2) = g_1$. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear map. The trusted authority (TA) randomly chooses $\alpha \in Z_q^*$ as master key, then computes the corresponding public key $MPK = g_2^\alpha$. In addition, TA also chooses two collision-resistant hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, and $H_2 : \{0,1\}^* \rightarrow Z_q$. The TA also maintains a member list ML which is kept secret. We will define this list later. Finally, publish the system parameters

$$params = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_2, \psi, MPK, H_1, H_2)$$

Vehicle registration: Assume that each vehicle is associated with a real identity, *e.g.*, the driving license number. To join to a VANET , a vehicle $\mathcal{V}$ with real identity ID_v must interactively communicate with TA by a confidential channel by the following steps:

1. A vehicle $\mathcal{V}$ first chooses a $x \in Z_q$ as his private key sk_v and compute the corresponding public key $pk_v = e(g_1, g_2)^x$.
2. Then it computes a zero-knowledge proof ZKP_0 of private key $V = g_2^{\alpha x}$ and sends (ID_i, V, pk_v, ZKP_0) to TA.
3. The TA verifies the validity of $e(V, g) = pk_v^{\alpha}$ and the zero-knowledge proof ZKP_0. If they hold, then the TA computes

$$W'_v = (V^{1/\alpha} H_1(ID_V))^{1/\alpha}$$

   and returns W' to the vehicle, and keeps (ID_i, W'_v) in the his database.
4. Upon receiving (ID_i, W'_v) , the vehicle first checks whether it is valid by the following equation:

$$e(\psi(W'_v), MPK)e(\psi(H_1(ID_v)^{-1}), g_2) = pk_v$$

   If it is valid, then (ID_i, W'_v) is the membership certificate of the vehicle $\mathcal{V}$, and it is added into the local database.

Anonymous authentication For a vehicle-generated message, it consists of five fields: message-ID, payload,Timestamp, TTL and signature. According to DSRC ,Message-ID defines the message type, and the payload may include the information on the vehicle's position, direction, speed, traffic events, event time and so on, whose length is 100 bytes. A timestamp indicates of time of producing the signature, which is used to prevent replay attacks. The TTL field is Time To Live and determines how long the message is allowed to remain in the VANET. Refer to [1] for the detail description.

To produce a signature on message m, the vehicle $\mathcal{V}$ computes as follows:

1. First, it randomly chooses $l \in Z_q$ to compute $W = \psi(W'_v)^l$ and $R = \psi(H_1(ID_v))^l$ in order to conceal the membership certificate W'_v and his identity ID_v of the vehicle $\mathcal{V}$.
2. then randomly choose $r \in Z_q$ to compute

$$u = (g_1)^r, t = \frac{1 - rH_2(m||u||R||W)}{lx}$$

   .
3. Finally, the resultant anonymous signature on message m is $\sigma = (W, R, u, t)$.

Verifying After receiving a signature σ on message m, a verifier can execute the following process for each signature:

1. Firstly, the vehicle parses σ into (W, R, u, t) and computes $h_2 = H_2(m||u||R||W)$;
2. then check

$$e(W^t, MPK)e(u^{h_2} R^{-t}, g_2) = e(g_1, g_2)$$

Doubtable message Tracing In the future, if the dispute appears, a produced signature σ on a message m by the vehicle $\mathcal{V}$ is found fraudulent. Then the TA can adopt the following way to trace the real identity of the vehicle $\mathcal{V}$.

1. the trusted party first checks the validity of the signature σ on message m by the verifying algorithm.
2. Then it looks up its local database to execute the following process

For $i = 1$ to n {

find (ID_i, W_i');
if $e(R, W_i') = e(W, H_1(ID_i))$ in the signature $\sigma = (W, R, u, t)$ then
break;
else $i = i + 1$
}
If $i <= n$ then
Output the real identity ID_i of the vehicle;
else
Output failure;

Once a vehicle is found compromised, the TA adds the information (ID_i, W_i') of the compromised OBU to the member revocation list ML, and sends ML to all RSUs. Then these RSUs periodically broadcasts the ML to the passing by vehicles. If the life span T of the compromised OBU's key is expired, the RSU stop informing other OBUs of the compromised OBU since the message signed by an expired group key will be discarded immediately. Thus, the number of revoked vehicles exist in the ML is restraint and the signature verification time will not grows long.

4: Security analysis

In this section, we show that our authentication scheme satisfies the above all privacy requirements and security requirements. In the following, we will show that our scheme satisfies unforgeability.

Lemma1. An attacker cannot forge the signature of a message to cheat other vehicles and make that it can pass the verification of the honest vehicle.

The Lemma 1 shows that our scheme satisfies unforgeability which can ensure that an illegal vehicle cannot produce a message-signature which is accepted by other vehicles. It implies that the attacker cannot cheat other vehicles by forging a new signature on a new message or by tampering a given message-signature or by replaying the expired message-signature. At the same time, it means that only a signer can produce its own message-signature. Thus, the property can achieve authentication of identity, integrity of message, non-repudiation of the signer and message's authenticity.

5: Conclusion

Security and privacy are two important issues in VANETs. To increase efficiency under balancing security and privacy issues, we propose a novel privacy-preserving authentication protocols based on self-certificate signature. Because our scheme doesn't group signature and pseudonyms certificate, it should adapt to large-scale VANETs by adopting batch verification technique of signatures. It is a solving problem to dynamically join and leave in VANETs.

Acknowledgments.

This work was supported partly by Supported by Beijing Natural Science Foundation (No:4122024) and the New Star Plan Project of Beijing Science and Technology (NO:2007B001).

References

[1] Rongxing Lu et.al, A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs. IEEE Transactions on Intelligent Transportation Systems 13(1): 127-139 (2012)

[2] Lei Zhang, Qianhong Wu, Bo Qin, and Josep Domingo-Ferrer,APPA: Aggregate Privacy-Preserving Authentication in Vehicular Ad Hoc Networks,ISC2011,LNCS 7001, pp. 293-308, (2011).

[3] Zhang, C., Lu, R., Lin, X., Ho, P., Shen, X.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: IEEE INFOCOM 2008, pp.246-250, (2008).

[4] Liqun Chen , Siaw-Lynn Ng, and Guilin Wang,Threshold Anonymous Announcement in VANETs,IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL.29(3), pp.605-612, (2011).

[5] Chenxi Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen. An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks. ICC 2008,pp 15-17, (2008)

[6] S. Goldwasser, S. Micali and R. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal of computing, 17(2), pp. 281-308, (1988).

[7] Marc Girault, Self-certifed public key, In EUROCRYPT'91, LNCS 547, pp. 490-497, (1991).

[8] David P, Jacque S. Security arguments for digital signatures and blind signatures. Journal of Cryptology, vol.13(3):361-396, (2000).

Authors

Jianhong Zhang received his Ph.D. degrees in Cryptography from Xidian University, Xi'an, Shanxi, in 2004 and his M.S. degree in Computer Software from Guizhou University, Guiyang, Guizhou, in 2001. He was engaging in postdoctoral re-search at Peking University from October 2005 to December 2007. He has been an Assistant Processor of College of Sciences, North China University of Technology, Beijing China, since 2001. His research interests include computer networks, cryptography, electronic commerce security, computer software.