Message Authentication for Vehicular Ad Hoc Networks

Shaik Patta Abdul Khayum, Dr.K.V. Subba Reddy Institute of Technology, abdulkhayumsafa@gmail.com,
C.Md Gulzar, Assoc.professor in Dept of CSE

Abstract—Vehicular Ad Hoc Networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. The proposed EMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, EMAP has a modular feature rendering it integrable with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL.

I.INTRODUCTION

Vehicular ad-hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and Vehicular ad-hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol1 (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

II.PROPOSED WORK

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. The Public Key Infrastructure (PKI) is the most viable technique to achieve these security requirements [4],[10]. PKI employs Certificate Revocation Lists (CRLs) to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long. There are some works addressing the problem of distributing the large-size CRL in VANETs. In [12], Raya *et al.* introduce RC2RL (Revocation using Compressed Certificate Revocation Lists), where the traditional CRLs, issued by the TA, are compressed using Bloom filters to reduce its size prior to broadcasting. Papadimitratos *et al.* [13] propose to partition the CRL into small pieces and distribute each piece independently. Laberteaux *et al.* [14] use car to car communication to speed up the CRL broadcasting. Haas *et al.* [6] develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to re-produce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which is used to check the revocation status of other entities, still suffers from the expected large size exactly as that in the traditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL.

Fig. 1. Hash chain

Also, the authors propose using bloom filter, which is some kind of lookup hash tables, to perform CRL checking for the received certificates. To minimize the false-positives in the bloom filter, the authors proposed that each vehicle has to check before sending its certificate whether this certificate will trigger a false positive or no. If yes, then it uses another certificate.

In this paper, we propose an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using

a CRL. EMAP employs keyed Hash Message Authentication Code (HMAC) in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs. In addition, EMAP is free

from the false positive property which is common for lookup hash tables as it will be indicated in the next section.

Bilinear Pairing

The bilinear pairing [20] is one of the foundations of the proposed protocol. Let G1 denote an additive group of prime order q, and G2 a multiplicative group of the same order. Let P be a generator of G1, and ˆe : G1 ?G1 → G2 be a bilinear mapping with the following properties:

1)Bilinear:

$$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}, \text{ for all } P, Q \in \mathbb{G}_1 \text{ and } a, b \in_R \mathbb{Z}_q.$$

2) Non-degeneracy: ˆe(P,Q) _= 1G2.

3) Symmetric: ˆe(P,Q) = ˆe(Q, P), for all P,Q , G1.

4) Admissible: the map ˆe is efficiently computable.

Hash Chains

A hash chain [24] is the successive application of a hash function h : {0, 1}∗ → Z∗q with asecret value as its input. A hash function is easy and efficient to compute, but it is computationally infeasible to invert. Fig. 1 shows the application of a hash chain to a secret value v, where v0 = v, vi = h(vi−1) ▫ 1 ≤ i ≤ j.

Search Algorithms

The WAVE standard does not consider a specific mechanism for searching CRLs to check the revocation status of certificates. The most common search algorithms [25] include non-optimized

search algorithms such as linear search algorithm, and optimized search algorithms such as binary search algorithm and lookup hash tables.

System Model

As shown in Fig. 2, the system model under consideration consists of the followings.

• A Trusted Authority (TA), which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network;

• Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA;

• On-Board Units (OBUs), which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

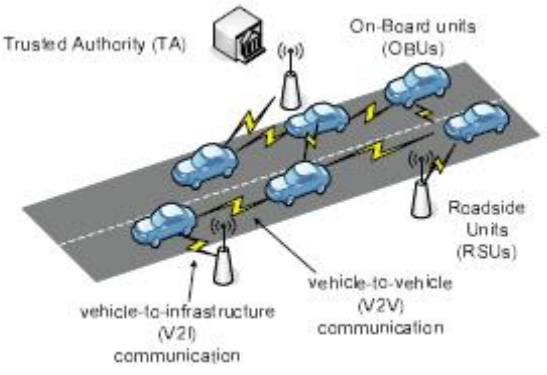

Fig. 2. The system model

Message Authentication

Since we adopt a generic PKI system, the details of the TA signature on a certificate and an OBU signature on a message are not discussed in this paper for the sake of generality. We only

focus in how to accelerate the revocation checking process, which is conventionally performed by checking the CRL for every received certificate.

Revocation

The revocation is triggered by the TA when there is an OBUu to be revoked. The certificates of OBUu must be revoked. In addition, the secret key set RSu of OBUu and the current secret

key Kg are considered revoked. Hence, a new secret key K˜g should be securely distributed to all the non-revoked OBUs. Also, each non-revoked OBU should securely update the compromised keys in its key sets RS and RP.

Forward secrecy: Since the values of the hash chain included in the revocation messages are released to non-revoked OBUs starting from the last value of the hash chain, and given the fact that a hash function is irreversible, a revoked OBU cannot use a hash chain value vj−ver+1 received in a previous revocation process to get the current hash chain value vj−ver. Consequently, a revoked OBU cannot update its secret key set (RS).

Resistance to replay attacks: Since in each message an OBU includes the current time stamp in the revocation check value REVcheck = HMAC(Kg, PIDu||Tstamp), an attacker cannot record REVcheck at time Ti and replay it at a later time Ti+1 to pass the revocation checking process as the receiving OBU compares the current time Ti+1 with that included in the revocation check.

Resistance to colluding attacks: For a colluding attack, a legitimate OBU colludes with a revoked OBU by releasing the current secret key K˜g such that the revoked vehicle can use this key to pass the revocation check process by calculating the correct HMAC values for the transmitted messages. All the security materials of an OBU are stored in its tamper-resistant

HSM. In addition, all the keys update processes in Algorithms 3-5 are executed in the HSM,which means that the new secret key K˜g is stored in the HSM, and it cannot be transmitted in clear under any circumstances.

III. PERFORMANCE EVALUATION

Computation Complexity of Revocation Status Checking

We are interested in the computation complexity of the revocation status checking process which is defined as the number of comparison operations required to check the revocation status of an OBU. Let Nrev denote the total number of revoked certificates in a CRL. To check the revocation status of an OBUu using the linear search algorithm, an entity has to compare the certificate identity of OBUu with every certificate of the Nrev certificates in the CRL, i.e., the entity performs one-to-one checking process. Consequently, the computation complexity of employing the linear search algorithm to perform a revocation status checking for an OBU isO(Nrev).

Authentication Delay

We compare the message authentication delay employing the CRL with that employing EMAP to check the revocation

status of an OBU. As stated earlier, the authentication of any message
is performed by three consecutive phases: checking the sender's revocation status, verifying the sender's certificate, and verifying the sender's signature.

End-to-end delay

To further evaluate EMAP, we have conducted ns-2 [31] simulation for the city street scenario shown in . The adopted simulation parameters are given in Table I. We select the dissemination of the road condition information by an OBU every 300 msec to conform with the DSRC standards. The mobility traces adopted in this simulation are generated using TraNS. We are interested in the end-to-end delay, which is defined as the time to transmit a message from the sender to the receiver.

Message Loss Ratio

The average message loss ratio is defined as the average ratio between the number of messages dropped every 300 msec, due to the message authentication delay, and the total number of messages received every 300 msec by an OBU. It should be noted that we are only interested in the message loss incurred by OBUs due to V2V communications. According to DSRC, each OBU has to disseminate a message containing information about the road condition every 300 msec. In order to react properly and instantly to the varying road conditions, each OBU should verify the messages received during the last 300 msec before disseminating a new message about the road condition. Therefore, we chose to measure the message loss ratio every 300 msec.

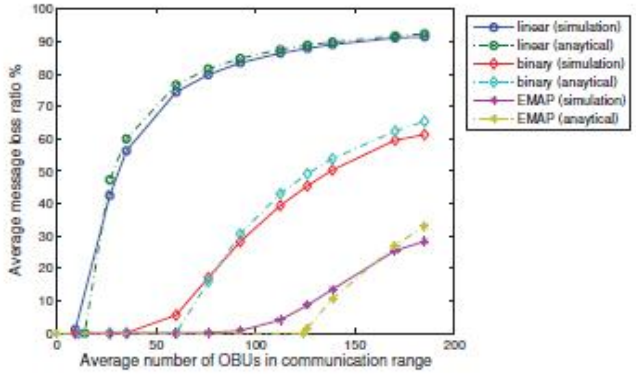

Fig. 6. Comparison between message loss ratio for different schemes

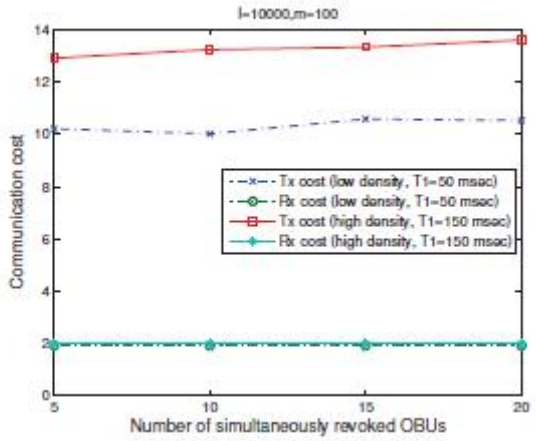

Fig. 7. Communication cost of updating Kg in EMAP

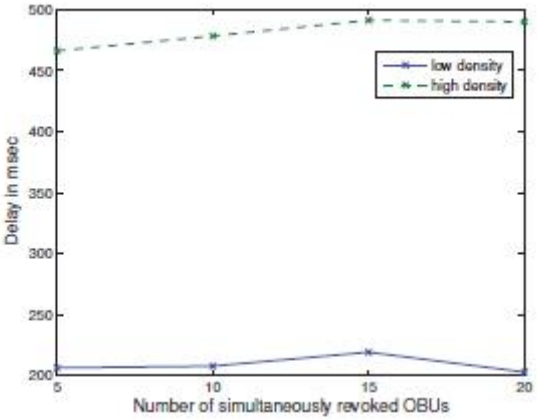

Fig. 8. Incurred delay to obtain K˜g in EMAP

REFERENCES

[1] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: a position paper," *Proc. Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland*, July 2006.

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," *Proc. Embedded Security in Cars (ESCAR)*, November 2005.

[3] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," *IEEE Trans. on Vehicular Technology*, vol. 59, pp. 533–549, 2010.

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

[5] "US bureau of transit statistics." [Online]. Available: http://en.wikipedia.org/wiki/Passenger vehicles in the United States

[6] J. J. Haas, Y. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," *Proc. 6th ACM international workshop on VehiculAr InterNETworking*, pp. 89–98, 2009.

[7] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, 2006.

[8] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[9] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," *Proc. IEEE GLOBECOM'09*, 2009.

[10] J. P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, pp. 49–55, 2004.

[11] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," *Proc. SECON '09*, pp. 1–9, 2009.