ISSN 2277-2685
IJESR/October 2014/ Vol-4/Issue-10/569-573
Aspari Nagaraju et al./ International Journal of Engineering & Science Research

EMAP: EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

Aspari Nagaraju*[1],Om Prakash[2], K. Prasanth Kumar[3]

[1]M.Tech Pursuing, JJ Institute of Information Technology, Maheshwarm, R.R. Dist, Telangana, India.

[2]Asst. Prof, JJ Institute of Information Technology, Maheshwarm, R.R. Dist, Telangana, India.

[3]HOD, JJ Institute of Information Technology, Maheshwarm, R.R. Dist, Telangana, India.

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 ðHMACÞ, where the key used in calculating the HMAC is shared only between nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient.

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 infrastructure Road-Side Units (RSUs). Vehicle-to Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs.

Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission.

RELATED WORK

In VANETs, the primary security requirements are identified as entity authentication, message integrity, nonrepudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [4, 12]. PKI employs 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.

In [12], Hubaux identify the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In [4], Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to

VANETs. In this approach, each vehicle needs to preload a huge pool of anonymous certificates. The number of the loaded certificates in each vehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it.

PRELIMINARIES

In this section, we introduce the bilinear pairing, hash chains, and search algorithms that can be employed for checking a CRL.

- **Bilinear Pairing**

The bilinear pairing [2] is one of the foundations of the proposed protocol. LetGG1 denote an additive group of prime order q, and GG2 a multiplicative group of the same order. Let P be a generator ofGG1, and ^ e:G G1GG1!GG2 be a bilinear mapping with the following properties.

- **Hash Chains**

A hash chain [6] is the successive application of a hash function h: f0;1g!ZZq with a secret value as its input. A hash function is easy and efficient to compute, but it is computationally infeasible to invert.

- **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 [7] include nonoptimized search algorithms such as linear search algorithm, and optimized search algorithms such as binary search algorithm and lookup hash tables.

The binary search algorithm works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted (with respect to the certificate's identity) database of the revoked certificates included in previous CRLs and the recently received CRL. The main idea of the binary search algorithm is to cancel out half of the entries under consideration after each comparison in the search process.

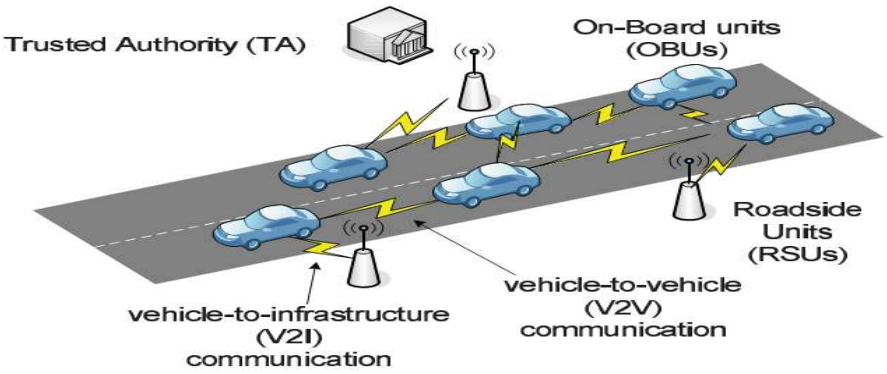


Fig 1: The system model

EXPEDITE MESSAGE AUTHENTICATION PROTOCOL

The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

- **System Model**

As shown in Fig. 2, the system model under consideration consists of the following: A Trusted Authority, 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.OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

- **System Initialization**

The TA initializes the system by executing Algorithm 1. Algorithm 1.System initialization

1: Select two generatorsP;Q2GG1 of order q,

2: for i 1;ldo

3: Select a random number ki 2ZZq

4: Set the secret key
K

---

i ¼kiQ2GG1

5: Set the corresponding public key Kþi ¼1kiP2GG1

6: end for

7: Select an initial secret key Kg 2GG2.to be shared between all the non-revoked OBUs

8: Select a master secret keys2ZZq

9: Set the corresponding public key P¼sP

10: Choose hash functions H: f0;1g!GG1 and h: f0;1g!ZZq

11: Select a secret valuev2ZZq and set v¼v

12: for i 1;jdo .to obtain a set V of hash chain values

13: Set vi
¼hðvi

1Þ

14: end for

15: for all OBUu in the network, TA do

16: for i 1;mdo

17: Select a random numbera2½1;l

18: Upload the secret key
K

---

a ¼kaQand the corresponding public key Kþa ¼1ka Pin HSMu which is the HSM embedded in OBUu

19: end for

20: Generate a set of anonymous certificates CERTufcertiuðPIDiu, PKiu; sigTAðPIDiukPKiu ÞÞj1————————————————i————————————————Cg. for privacy-preserving authentication

21: Upload CERTuin HSMuofOBUu

22: end for

23: Announce H, h, P, Q, and Pto all the OBUs

SECURITY ANALYSIS

In this section, we analyze the security of the proposed protocol against some common attacks.

- Resistance to Forging Attacks

- Forward Secrecy
- Resistance to Replay Attacks
- Resistance to Colluding Attacks

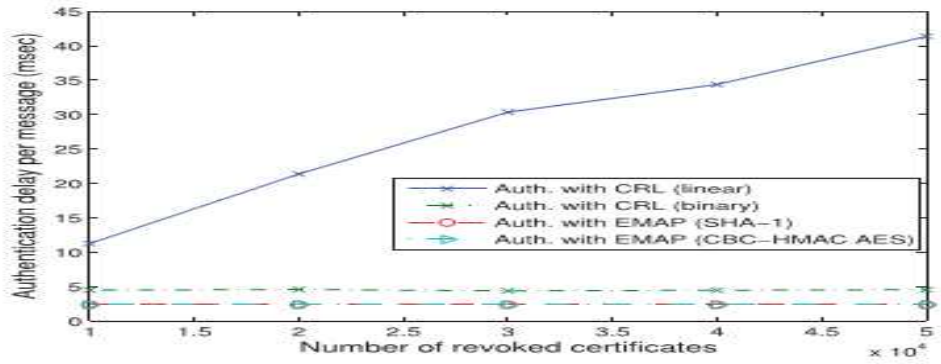
PERFORMANCE EVALUATION

- **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.

- **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.



(a) Authentication delay per message

Fig 2: Authentication delay

- **End-to-End Delay**

To further evaluate EMAP, we have conducted ns-2 [3] simulation for the city street scenario shown in Fig. We select the dissemination of the road condition information by an OBU every 300 msec to conform with the DSRC standards.

- **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.

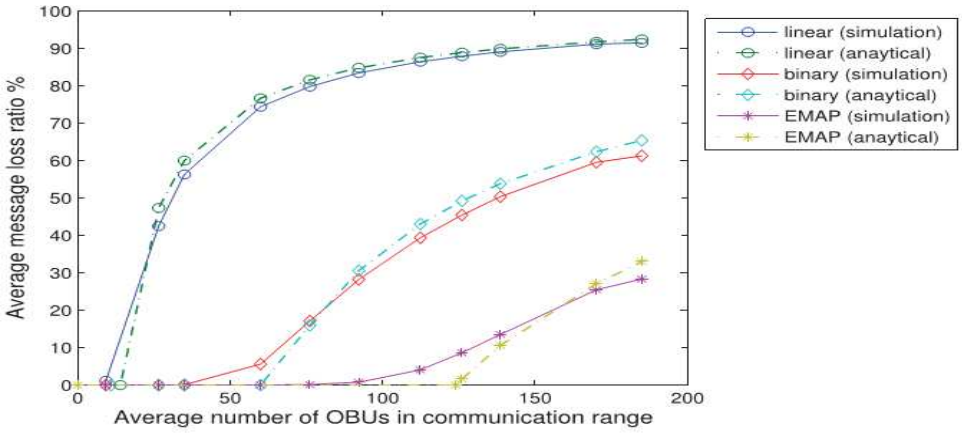


Fig 3: Comparison between message loss ratio for different schemes

CONCLUSION

We have proposed EMAP for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. 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. Therefore, EMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. Our future work will focus on the certificate and message signature authentication acceleration.

REFERENCES

[1] Papadimitratos P, Kung A, Hubaux JP, Kargl F. Privacy and Identity Management for Vehicular Communication Systems:A Position Paper. Proc. Workshop Standards for Privacy in User Centric Identity Management, July 2006.

[2] Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K. CARAVAN: Providing Location Privacy for VANET. Proc. Embedded Security in Cars (ESCAR) Conf, Nov. 2005.

[3] Wasef A, Jiang Y, Shen X. DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks. IEEE Trans. Vehicular Technology 2010; 59(2): 533-549.

[4] Raya M, Hubaux JP. Securing Vehicular Ad Hoc Networks. J. Computer Security 2007; 15(1): 39-68.

[5] Sun Y, Lu R, Lin X, Shen X, Su J. An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications. IEEE Trans. Vehicular Technology 2010; 59(7): 3589-3603.

[6] Lu R, Lin X, Luan H, Liang X, Shen X. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets. IEEE Trans. Vehicular Technology 2012; 61(1): 86-96.

[7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/ Passenger_vehicles_in_the_United_States, 2012.

[8] Haas JJ, Hu Y, Laberteaux KP. Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET. Proc. Sixth ACM Int'l Workshop Vehicular Internet working, 2009; 89-98.

