International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.3, March 2015 DOI:10.15693/ijaist/2015.v4i3.163-166

Performance Enhancement of VANET Using EMAP

First A. Premalatha, Second B. D.S.K.Lena, Third C. Lakshmipriya.S, Fourth D.Lakshmipriya.R

***Abstract*—**In this paper, we present an efficient privacy preserving authentication scheme based on group signature for vehicular ad hoc networks (VANETs). Although group signature is widely used in VANETs to realize anonymous authentication, the existing schemes based on group signatures suffer from long computation delay in the certificate revocation list (CRL) checking and in the signature verification process, leading to high message loss. As a result, they cannot meet the requirement of verifying hundreds of messages per second in VANETs. In our scheme, we first divide the precinct into several domains, in which roadside units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized manner. we use a Expedite message authentication protocol (EMAP) using VANET for message authentication and secure data transfer using hash message authentication code (HMAC) to avoid time consuming CRL checking and to ensure the integrity of messages before batch group authentication. Finally, we also use ALERT protocol to improve security of routing paths in vehicular network .The proposed system simulated using NS2 simulator The security and performance analysis show that our scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.

***Keywords*—**Message authentication, Certificate revocation

I.INTRODUCTION

THE adhoc network (VANET), As a special kind of mobile adhoc network, has been subject to extensive research efforts not only from the government but also from academia and the automobile industry in recent years. Different from the traditional ad hoc networks, the VANET contains not only mobile nodes—vehicles—but stationary roadside units (RSUs) as well. Due to this hybrid architecture, the VANET opens new doors to facilitating road safety and traffic management and providing multimedia services for vehicles on the road. According to the dedicated short-range communications (DSRC) [1] in road safety-related applications, each vehicle equipped with onboard units (OBUs) will broadcast routine traffic messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. With this information, drivers can be better aware of their driving environment and take early action to respond to an abnormal situation, such as a traffic accident. However, before putting this attractive application into practice, security and privacy issues in VANETs must be resolved [2]–[5]. Without security and privacy guarantees, an adversary to a VANET can either forge bogus information to mislead other drivers, and even cause a deliberate traffic accident, or track the locations of the interested vehicles by collecting their routine traffic messages. Therefore, how to achieve anonymous authentication has become a fundamental requirement for securing VANETs. 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. RELATED WORK

In spontaneous vehicular communications, the primary security requirements are identified as entity authentication, message integrity, non repudiation, and privacy preservation. Deploying an efficient PKI is a well-recognized solution for achieving security and privacy for practical vehicular networks [6], [7]. Although VANETs have recently gained extensive attention, very few works have addressed the design of a PKI that is suitable for the security requirements of VANETs. In [6], Hubbub identifies the specific issues of security and privacy challenges in VANETs and claims that a PKI should be well deployed to protect the transited messages and to mutually authenticate among network entities. In [1], Raya and Hubbub use a classical PKI to provide secure and privacy-preserving communications to VANETs. For 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. The requirement to load a large number of certificates in each vehicle incurs inefficiency for certificate management, as revoking one vehicle implies revoking the huge number of certificates loaded in it. Lin *et al.* [7] use the group signature in [11] to secure the communications between vehicles. For

the group signature technique, any group member can sign messages on behalf of the group without revealing its real identity. Signatures can be verified using the group public key, thus providing excellent privacy for the users, as the identities of the users are revealed in neither signing nor verifying a message. However, the delay incurred in this technique to verify a signature is linearly proportional to the number of revoked vehicles

.

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 in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs. In addition, we are going to implement the cluster based method in this process. Due to large vehicles equipped in this field we are going to divide it in cluster format and then include the Expedite Message Authentication protocol. Here Credit algorithm is implemented. The transaction can only occur within the credit nodes. Credit method will focus on the certificate and message signature authentication acceleration

III. EXPEDITE MESSAGE AUTHENTICATION PROTOCOL

The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution. As shown in Fig. 1, the system model under consideration consists of the following:

1. A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.

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

3.OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications

A.System initialisation

The TA initializes the system by executing Algorithm 1. PK $^{i}_{o}$dinates the it public key for OBUu, where the corresponding secret key is SKu. PIDi u denotes the ith pseudoidentity (PID) for OBUu, where the TA is the only entity that can relate PIDi to the real identity of OBUu; sigTA and (PID||PKi) and PK_i is the signature .|| is the concatenation of PIDi and PKiu .C is the number of certificates loaded in each OBU

B.MESSAGE AUTHENTICATION

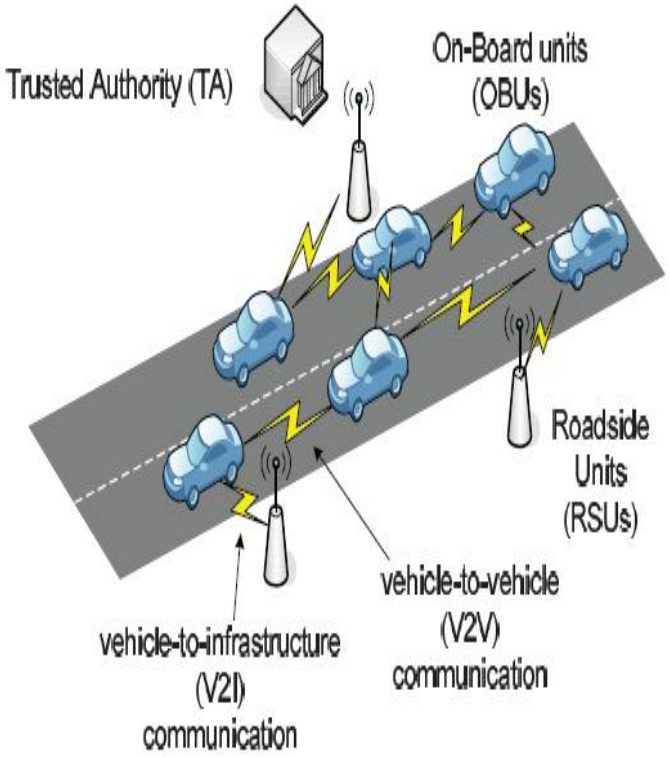

Fig. 1.System model

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. The message signing and verification between different entities in the network are performed as follows.

C. MESSAGE SIGNING

Before any OBUu broadcasts a message M, it calculates its revocation check REVcheck as

$$(M||Tstamp||\mathbf{cert_u}(\mathbf{PID_u},\mathbf{PIC_u},\mathbf{sig_{TA}}(\mathbf{PID_u}||\mathbf{Pic_a}))||\mathbf{sig_h}(\mathbf{m}||\mathbf{S_{tamp}})||\mathbf{Rec_{heck}}),$$

Recheck = HMAC(Kg; Pick||Stamp)^2 where Stamp is the current time stamp, and = HMAC(Kg; Pick||Stamp)^{2}is the hash message authentication code on the concatenation of PIDu and Stamp using the secret key Kg. Then, Oboe

broadcasts where HMAC(Kg; Pick||Stamp)is the signature of Oboe on the concatenation of the message M and Stamp.

D. MESSAGE VERIFICATION

Any Obey receiving the message (M||Stamp||cert(PIDu;PKu;sigTA(PIDu||PKu)) Tstamp ÞkREVcheck can verify it by executing Algorithm

IV.Algorithm

A.System initialization

1: Select two generators P;Q
2: Select a random number ki and set secret key K
3: Set corresponding public key K
4: Select an initial secret key Kg and master secret key s
5: Set corresponding public key P_S
6: Choose hash functions H:{0,1}
7: Select a secret value v and $V_{00=V}$
8:obtain a set V of hash chain values

B. Message verification

1: Check the validity of Tstamp
2: invalid, drop the message
3: valid, Check REVcheck = HMAC
4: else,step 2
5: valid, Verify TA signature on certOBUu
6: else,step 2
7: valid, Verify the signature sig(M||Tstamp) using OBUu public key PK
8:valid, Process the message
9:else,step 2

V. PERFORMANCE EVALUATION

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. For the first authentication phase which checks the revocation status of the sender, we employ either the CRL or EMAP. For EMAP, we adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC) AES and Secure Hash Algorithm 1 SHA-as theHMAC functions.Fig.2 shows a comparison between the authentication delay per message using EMAP, linear CRL checking process, and binary CRL checking process versus the number of the revoked certificates, where the number of the revoked certificates is an indication of the CRL size. It can be seen that the authentication delay using the linear CRL checking process increases with the number of revoked certificates, i.e., with the size of the CRL.Also, the authentication delay using the binary CRL checking process is almost constant.

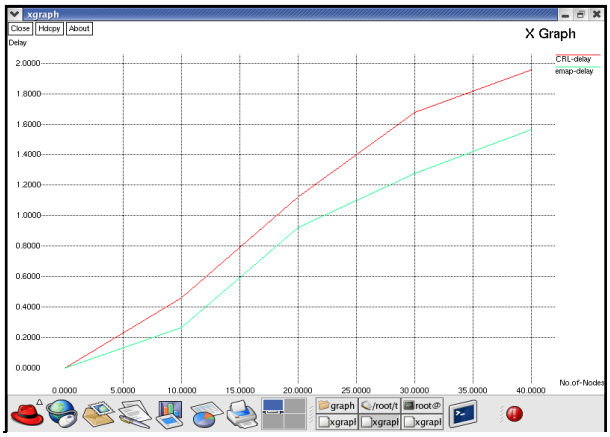

Fig. 2.Delay VS No of nodes

The average message loss ratio is defined as the average ratio between the number of messages dropped every 300 msec, due to the message authenttotal number of messages received every 300 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 communication.

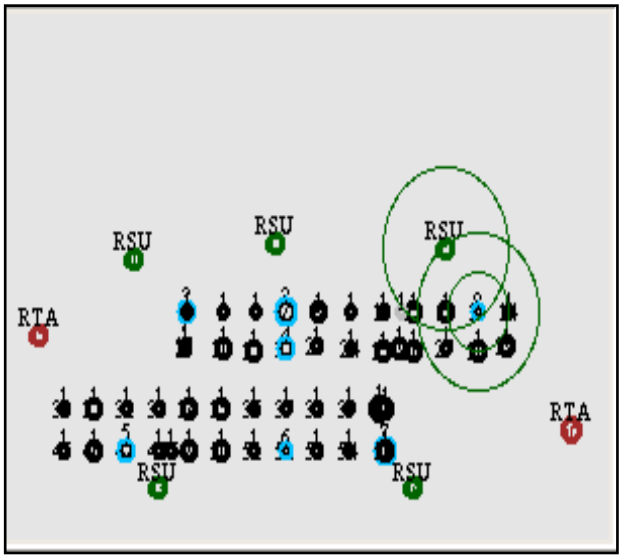

Fig. 3.Verification process

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.Theref e, we chose to measure the message loss ratio every300 msec.

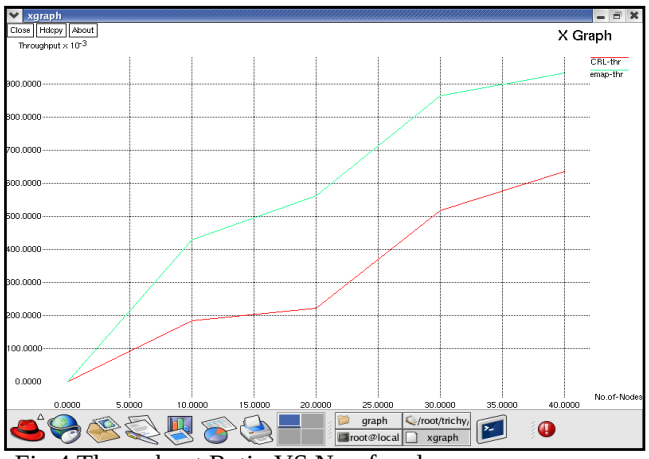

Fig.4.Throughput Ratio VS No of nodes

VI. 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] Dedicated Short Range Communications (DSRC) Home.[Online].Available:http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[2] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc. HotNets-IV, Nov. 2005, pp. 1–6.

[3] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in Proc. INFOCOM, Rio de Janeiro, Brazil, Apr. 2009, pp. 1413–1421.

[4] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in Proc. INFOCOM, San Diego, CA, Mar. 2010, pp. 1–9.

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007

[6] J. P. Hubaux, "The security and privacy of smart vehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[7] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacypreserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007

[8] J.J. Haas, Y. Hu, and K.P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," Proc. Sixth ACM Int'l Workshop VehiculAr InterNETworking, pp. 89-98, 2009.

[9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[10]"5.9GHzDSRC,"http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2012.

[11] A. Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE GlobeCom, 2009.

[12] J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[13] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009.