A CLUSTER BASED EXPENDITE MESSAGE AUTHENTICATION PROTOCOL FOR VANETS

A.M.Suhavaneswari[1] A.Muthukrishnan[2]

[1] *PG Student, Anna University, Chennai. Regional Centre Madurai, Tamilnadu, (India)*

[2] *Faculty, Anna University, Chennai. Regional Centre Madurai, Tamilnadu, (India)*

ABSTRACT

It is well recognized that security plays a vital for the reliable operation of vehicular ad hoc networks (VANETs). One of the critical security issues is the revocation of misbehaving vehicles, which is essential for the prevention of malevolent vehicles from other vehicles. Vehicular ad hoc networks (VANETs) adopt the Public Key infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the confirmation of a received message is performed by checking if the record of the sender is included in the current CRL, and verifying the validity of the certificate and signature of the sender. The proposed scheme is 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 shared only between non revoked On-Board Units (OBUs). EMAP can 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 by NS2 simulator tool, EMAP is demonstrated to be secure and efficient.

Keywords: Message Authentication, Certificate Revocation

I INTRODUCTION

The ad hoc network (VANET), as a special kind of mobile ad hoc 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 introduces new methods 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 false information to delude other drivers, and even cause a purposeful traffic accident, or track the locations of the interested vehicles by collecting their routine traffic messages. The ad hoc network (VANET), as a special kind of mobile ad hoc 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 be a false 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 unidentified 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 protocol (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], Hubaux 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 Hubaux 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 [10] 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 the reprogramming protocols are discussed and also classify the different reprogramming protocols. SDRP is the distributed protocol which supports multiple users simultaneously and also it is important in large-scale sensor networks used by different users from both public and private sectors. The security to this protocol is provided by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique.

III EXPEDITE MESSAGE AUTHENTICATION PROTOCOL

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

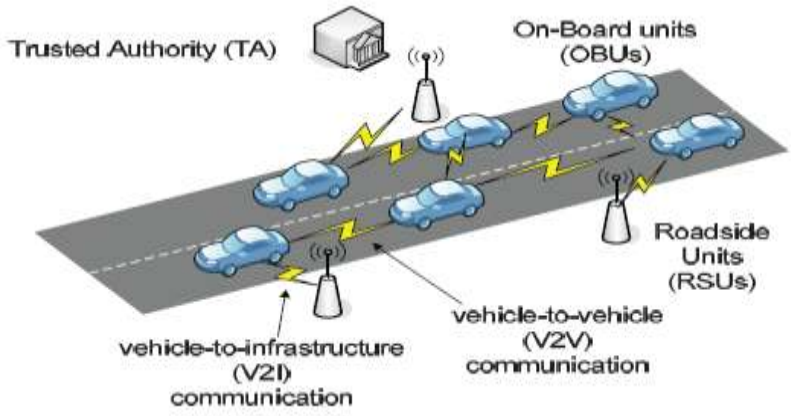

Figure 1. System model

IV SYSTEM MODEL

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

V SYSTEM INITIALIZATION

The TA initializes the system by executing Algorithm 1. PK^{i}_{u} denotes the i^{th} 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

Algorithm 1. System initialization

1: Select two generators P;Q € GG1 of order q,
2: for i ->1,l do
3: Select a random number ki € Zq
4: Set the secret key K=kiQ €GG1
5: Set the corresponding public key K= P/K_I
6: end for
7: Select an initial secret key Kg € GG2 to be shared between all the non-revoked OBUs
8: Select a master secret key s € ZZ
9: Set the corresponding public key P_S=SP
10: Choose hash functions H:{0,1}
11: Select a secret value v € ZZ and $V_{00=V}$
12: for i ←1; j do . to obtain a set V of hash chain values
13: Set V_I=h(v-1)
14: end for
15: for all OBUu in the network, TA do
Announce H, h, P, Q, and P to all the OBUs

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

6.1 Message Signing

Before any OBUu broadcasts a message M, it calculates its revocation check REVcheck as REVcheck = HMAC(Kg; PIDk||Tstamp)[2] where Tstamp is the current time stamp, and = HMAC(Kg; PIDk||Tstamp)[2]is the hash message authentication code on the concatenation of PIDu and Tstamp using the secret key Kg. Then, OBUu broadcasts

$M||T_{stamp}||cert_u(PID_u PK_u sig_{TA}(PID_u||PK_u))||sig_u(M||T_{stamp})||$ REV_{check})

where HMAC(Kg; PIDk||Tstamp)is the signature of OBUu on the concatenation of the message M and Tstamp.

6.2 Message Verification

Any OBUy receiving the message (M||Tstamp||cert(PIDu;PKu;sigTA(PIDu||PKu)Tstamp REVcheck can verify it by executing Algorithm 2.

Algorithm 2. Message verification

1: Check the validity of Tstamp
2: if invalid then
3: Drop the message
4: else
5: Check REVcheck = HMAC(Kg : PIDukTstamp)
6: if invalid then
7: Drop the message
8: else
9: Verify the TA signature on certOBUu
10: if invalid then
11: Drop the message
12: else
13: Verify the signature sig(M||Tstamp) using OBUu
public key PKu
if invalid then
15: Drop the message
16: else
17: Process the message
18: end if
19: end if
20: end if
21: end if

VII PERFORMANCE EVALUATION

Authentication Delay 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 the HMAC functions.

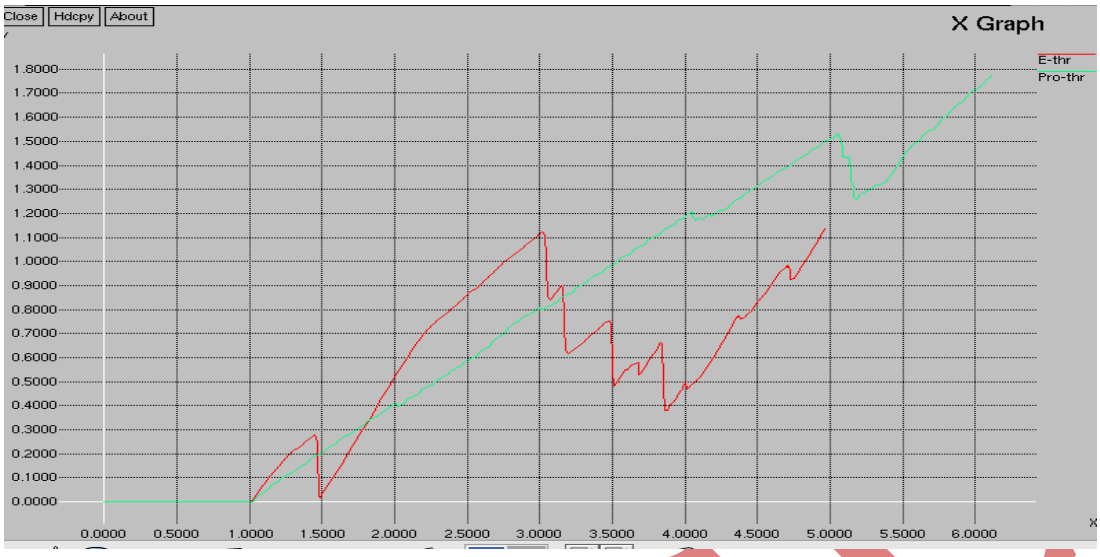

Figure 2.Packet Delivery Ratio

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.

VIII MESSAGE LOSS RATIO

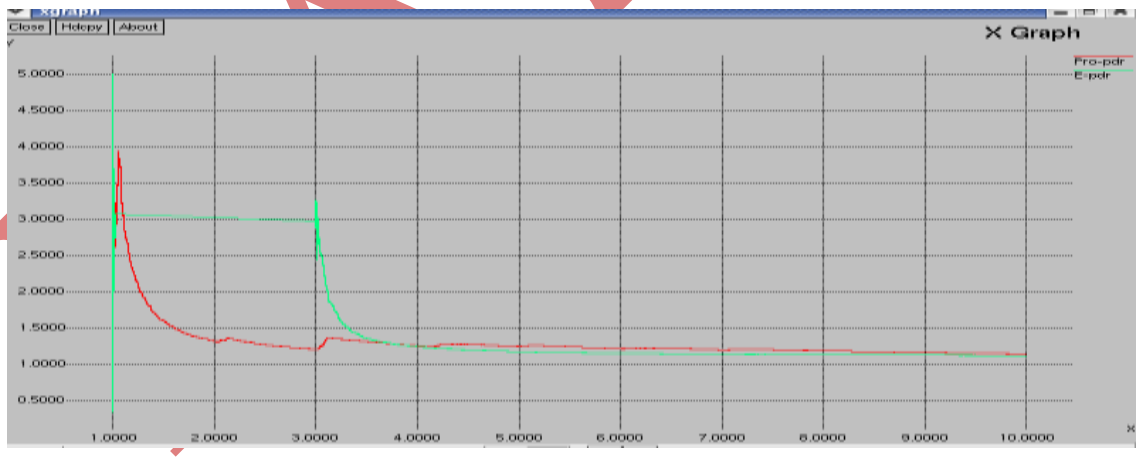

Figure 5 Throughput Ratio

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 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 every300 msec

IX CONCLUSION

In this paper the reprogramming protocols are discussed and also classify the different reprogramming protocols. SDRP is the distributed protocol which supports multiple users simultaneously and also it is important in large-scale sensor networks used by different users from both public and private sectors. The security to this protocol is provided by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique.

REFERENCES

[1]. H. Chan, A. Perrig, and D. Song,(2003) "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp, Security and Privacy, pp. 197-213, 2003.

[2]. L. Eschenauer and V.D. Gligor,(2002) "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

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

[4]. K.P. Laberteaux, J.J. Haas, and Y. Hu,(2008) "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop Vehicular Inter-NETworking, pp. 88-89, 2008.

[5]. R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen,(2012) "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61, no. 1,pp. 86-96, Jan. 2012.

[6]. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su,(2010) "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans.Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[7]. A. Wasef and X. Shen, (2008) "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp.1458-1463, 2008.

[8]. A. Wasef, Y. Jiang, and X. Shen, (2010) "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans.Vehicular Technology, vol. 59, no. 2 pp 533-549, Feb. 2010.

[9]. A. Wasef and X. Shen,(2009) "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 9, pp 5214-5224, Nov. 2009

[10] S. Zhu, S. Setia, S. Xu, and S. Jajodia,(2006) "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks,"J. Computer Security, vol. 14 pp. 301-325, 2006.