An Effective Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks

[1]Dr. SHAIK ADBUL MUZZER, [2]B RAJITHA

Megha Institute of Engineering & Technology For women's
Edulabad, Ghatkesar mandal, RangaReddy Dist, Telangana, India

***ABSTRACT*: 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 VAN ETs 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 VAN ETs.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.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.**

***IndexTerms*: Vehicular networks, Communication security, Message authentication, Certificate revocation.**

I.INTRODUCTION:

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. 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. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender 's signature on the received message. The first part of the authentication, which checks the revocation status of the sender in a CRL, may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: (1) To preserve the A of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper [1]-[3], each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers [4]. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size; (2) The scale of VANET is very large. According to the United States Bureau of Transit Statistics, there are approximately 251 million OBUs in the Unites States in 2006 [5]. Since the number of the OBUs is huge and each OBU has a set of certificates, the CRL size will increase dramatically if only a small portion of the OBUs is revoked.

II.Existing System

In Existing System, 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 the CRL size in VANETs is expected to be large for the following reasons: To preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper should be preloaded with a set of anonymous digital certificate, where the OBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificate carried by that OBU leading to a large increase in the CRL size.

Disadvantage

• An important feature of the proposed EM AP is that it enables an OBU to update its compromised keys corresponding to previously missed revocation processes provided that it picks one revocation process in the future. To the best of our knowledge, this is the first work to propose a rekeying mechanism capable of updating compromised keys corresponding to previously missed rekeying processes.

• Note that EM AP has a modular feature, which makes it integral with any PKI system. In other words, EM AP does not require any modification to the core of the PKI architecture. It only needs a key distribution module to be added to the TA during the system initialization.

• EM AP is suitable for not only VANETs but also any type of networks employing PKI.

OBU - On-Board Units

In Existing system, vehicles communicate through wireless channels, a variety of attacks such as

- Injecting false information,
- Modifying and replaying the disseminated messages can be easily launched.

III.Proposed System

In Propose System an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network.
The proposed method can reduce the RL checking to two pairing operations. However, this solution is based on fixing some parameters in the group signature attached to every certificate request, which reduces the privacy preservation of TACK and renders the tracking of a vehicle possible.

Advantages

- safety -related VANETs applications

Modules

1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure
2. Expedite M essage Authentication Protocol
3. Security Analysis

a. Hash Chain Values
b. Resistance of forging attacks
c. Forward secrecy
d. Resistance to replay attacks
e. Resistance to colluding attacks

Modules Description

1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure

In this M odule, 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 certificate. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is alist containing all the revoked certificate. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message.

2. Expedite Message Authentication Protocol

In this Module,

Trusted Authority(TA): This is responsible for providing anonymous certificate and Distributing secret keys to all OBUs in the network.

Roadside units (RS Us): 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.

3. Security Analysis

a. Hash Chain Values : The values of the hash chains are continuously used in the revocation processes, and hence, the TA can consume all the hash chain values. As a result, there should be a mechanism to replace the current hash chain with a new one.

b. Resistance of forging attacks : To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgeable.

c. Forward secrecy : 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 received in a previous revocation process to get the current hash chain value, a revoked OBU cannot update its secret key set.

d. Resistance to replay attacks : Each message of an OBU includes the current time stamp in the revocation check value check an attacker cannot record REV check at time T and replay it at a later time process as the receiving OBU compares the current time.

e. Resistance to colluding attacks : A legitimate OBU colludes with a revoked OBU by releasing the current secret key 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.

IV.Algorithm:

Linear Search Algorithm:

In the linear search algorithm, the revocation status of a certificate is checked by comparing the certificat e with each entry in the CRL. If a match occurs, the certificate is revoked and vice versa.

Binary Search Algorithm:

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 identity) database of the revoked certificate 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. In the binary search, the revocation status of a certificate is checked by comparing the identity of the certificate with middle value (which in this case will be the median value) of the sorted database. If the identity of the certificate is greater than the median value, the right half of the database will be considered in the next comparison process and vice versa. This process continues until a match is found, i.e., the certificate is revoked, or the process is finished without finding a match which means that the certificate is unrevoked.

Algorithm 2
Message verification

Require: $(M||T_{stamp}||cert_u(PID_u, PK_u, sig_{TA}(PID_u||PK_u))||sig_u(M||T_{stamp})||REV_{check})$ and K_g

1: Check the validity of Tstamp
2: if invalid then
3: Drop the message
4: else ?
5: Check RE Vcheck = HMAC (Kg , PIDu||Tstamp)
6: if invalid then
7: Drop the message
Fig 2. The system model
8: else
9: Verify the TA signature on cert O BUu
10: if invalid then
11: Drop the message
12: else
13: Verify the signature
sigu (M||Tstamp) using OBUu public key (PK u)
14: 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

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.

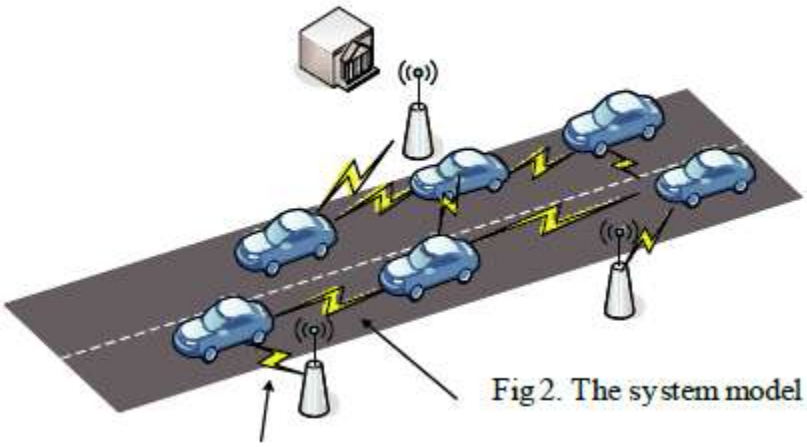

Fig 2. The system model

According to the WAVE standard [7], each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e. g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. We consider that legitimate OBUs cannot collude with the revoked OBUs as it is difficult for legitimate OBUs to extract their security materials from their H SM s. Finally, we consider t hat a compromised OBU is instantly detected by the TA.

V.Related work:

. propose an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. The authors adopted group signature where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA to update its certificate, the RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short- lifetime region-based certificate.

This certificate is valid only within the coverage range of the RA. It should enoted that TACK requires the RAs to wait for some time, e. g., 2 seconds, before sending the new certificate to the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard [7] requires each vehicle to transmit beacons about its location, speed, and direction every 100 ~ 300 msec. Also, TACK requires the RAs to completely cover the network, otherwise, the TACK technique may not function properly. This requirement may not be feasible especially in the early deployment stages of VANETs. Although TACK eliminates the CRL at the vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current Revocation List (RL) by preforming a check against all the entries in the RL. Each check requires three

VI. CONCLUSION:

. The proposed EM AP 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, EM AP 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, EM AP 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.

VII. 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. M atsuura, and K. Sezaki, “CARAVA N: Providing location privacy for VA N ET,” Proc. Embedded Security in Cars (ESCAR), November 2011.

[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, 2012.
[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] "U S 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 1609.2-2013, 2013
[8]"5.9 G Hz D SRC." [Online]. Available:
[9]A. Wasef and X. Shen, "M A AC: M essage authentication acceleration protocol for http://grouper.ieee.org/groups/scc32/dsrc/index.html.vehicular ad hoc networks," Proc. IEEE GLOBECOM'09, 2013.
[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, 2013.
[12] M . Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE Journal on Selected Areas in Communications, vol. 25, pp . 1557–1568, 2011.
[13] P. P. Papadimitratos, G. M ezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communication systems," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp . 86–87, 2012.
[14]K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution For VA N ET," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp . 88–89, 2008.

[15]H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proc. 2013 IEEE Symposium on Security and Privacy, pp . 197–213, 2013.
[16]L. Eschenauer and V. D. Gligor, "A key - management scheme for distributed sensor networks," Proc. ACM conference on Computer and communications security, pp . 41– 47, 2012.
[17] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKM PA N: An efficient group rekeying scheme for secure multicast in ad-hoc networks," Journal of Computer Security, vol. 14, pp . 301–325, 2012.
[18] A. Wasef and X. Shen, "P P GCV: Privacy preserving group communications protocol for vehicular ad hoc networks,"Proc. ICC'08, pp . 1458–1463, 2008. decentralized revocation protocol for vehicular ad hoc networks," IEEE Trans. On Vehicular Technology, vol. 58, no. 9, pp . 5214 – 5224, 2011.
[20] D. Boneh and M . K. Franklin, "Identity -based encryption from the Weil pairing," Proc. 21st Annual International Cryptology Conference on Advances in Cryptology, pp . 213–229, 2011.
[21] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.
[22] M . Scott, "Computing the Tate pairing," Topics [28] "Crypto++ library 5.5.2." [Online]. Available: http://www.cryptopp .com/in Cryptology, Springer, pp . 293–304, 2012.
[23] N. Koblitz, A. M enezes, and S. Vanstone, "The state of elliptic curve cryptography," Designs, Codes and Cryptography, vol. 19, no. 2, pp . 173–193, M ar. 2012.
[24] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp . 770–772, 1981. [25] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to algorithms. M IT Press, 2001.
[26] S. Frankel, R. Glenn, and S. Kelly, "The A ES-CBC cipher algorithm and its use with IPsec," RFC3602, Sept. 2003. [27] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," RFC 3174, Sept. 2001.