Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Expedite Message Authentication Protocol

Ms. Shraddha Gajare, **Mrs. Nilima Nikam**

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 message authentication 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 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

Keyword: CRL, HMAC, EMAP, PKI

I. INTRODUCTION

VANETs consist of On-Board Units (OBUs) and Road-Side Units (RSUs).Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, many 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 effect to legitimate users. A popular solution to secure VANET is use of Public Key Infrastructure (PKI), and 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 and finally verifying the sender's signature on the received message. Security in VANET is crucial to take care before it is actually deploying into real time.

The paper proposes an EMAP protocol for secure communication in VANETS. EMAP uses a keyed Hash Message Authentication Code (HMAC) where the hash key is used in calculating the HMAC to provide security in vehicular communication. 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. The first part of authentication, which checks the revocation status of the sender in a CRL may incur long delay depending on CRL size and the employed mechanism for searching the CRL.

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. The first part of authentication ,which checks the revocation status of the sender in a CRL may incur long delay depending on CRL size and the employed mechanism for searching the CRL. reason:1) To preserve the privacy of drivers i.e., to decline leakage of real identities and location information of drivers from any attackers, each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to frequently change its anonymous certificate to mislead attackers.2) The scale of VANETS is very large. According to the Dedicated Short Range Communication (DSRC) where, each OBU has to broadcast a message about its location, velocity and other information. In such scenario, each OBU may receive a large number of messages, and it has to check the current CRL for all the received certificates, which may take long authentication delay depending on the CRL size and the number of certificates received.

The remainder of the paper is organized as follows. The related works are discussed in section II. The proposed EMAP is presented in section III. Security analysis and performance evaluation are given in section IV and section V, respectively. Section VI concludes the paper.

II. RELATED WORK

The Public Key Infrastructure (PKI) is the most viable technique to achieve these security requirements [4],[10] such as entity authentication, message integrity, non-repudiation, and privacy preservation.

In [10], Hubaux et al. identify the security and privacy challenges in VANETs, and indicate that a Public Key Infrastructure (PKI) should be well deployed to secure the transmitted messages and to authenticate network entities.

In [11], Studer et al. 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. After entering a new network, 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 be noted 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 is 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. Checking the revocation status of a vehicle may be a time consuming process. The authors suggested using an optimized search method to reduce the computation while RL check. 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.

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 CRL, each OBU uses the secret key of each revoked vehicle to 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.

III. EMAP

The main aim of this project is to develop an architectural framework to authenticate bulk messages in VANETs using EMAP. The proposed system ensures low end-to-end delay, low overhead and thus a better communication channel. The EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution. 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. Extension of EMAP for bulk authentication in VANETs clearly reduces the communication overhead thereby making the communication faster and easier.

As shown in the figure the system model 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.

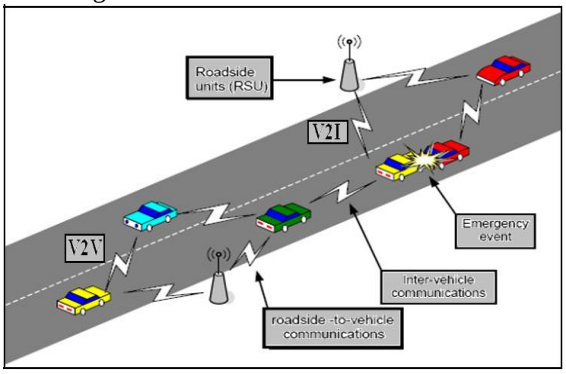

Fig. 1: System Model

A. System Initialization:

TA issues the following parameters to each vehicle.

1. Public Key (PKU) , Private Key (PRu), which is used for both encryption and decryption purposes using RSA algorithm.
2. Secret Key (Kg), which is used for generating MAC code to ensure message integrity and authentication generated using the algorithm MD5.

3. Shared Key, which is used for secure communication between vehicles.
4. Time Stamp, denotes the time when the vehicles are registered to the network.
5. Certificate, owned for each vehicle that binds the public key.

Note that the system model under consideration is mainly a PKI system, where each OBU_u has a set of anonymous certificates ($CERT_u$) used to secure its communications with other entities in the network. In specific, the public key PK_u , included in the certificate $cert_u$, and the secret key SK_u are used for verifying and signing messages, respectively.

B. Message Authentication

i. Message Signing

Before any OBU_u broadcasts a message M, it calculates its revocation check REV_{check} using HMAC function with parameters Secret Key (Kg),pseudo identity and current time stamp. HMAC function will generate a HMAC code by concatenating pseudo identity number with current time stamp using secret key. Then OBU broadcasts message with current stamp and certificate, signature of trusted authority and signature of an OBU.

ii. Message Verification

On receiving broadcasted message receiver OBU calculates HMAC code and compares it with REV_{check} . The destination vehicle, OBU before receiving the message checks CRL status that the certificate of the intended OBU is revoked or not. After verification, if the certificate is non- revoked
OBU receives the message and decrypt it using the
Public key since asymmetric key cryptosystem is used. Else progress the revocation process. After decrypting, the OBU generates a REV Check by itself using the secret key and the message. It then verifies the generated REV check and the received REV Check matches or not. If match occurs, the message integrity is verified. Else it specifies that false information or replay attacks has been involved and indicates that integrity is lost. Once the integrity is verified, the safety-related message is accepted and displayed. Otherwise the message is ignored.

iii. *RSU - Aided Verification*

The CRL consists of list of revoked certificates. The certificate which belongs to the identity of each vehicle is revoked due to the reasons like certificate expiration or any other validation problems. The certificates can be accepted only when they are in state of non-revoked else it is considered as revoked and the safety-related message that is broadcasted is no more accepted by the destination vehicle OBU. The CRL verification is performed using the concept of hash chain. RSU is a fixed infrastructure unit on the roadside.

Each OBU belongs to their corresponding RSUs depending upon their timestamp value, the time when they get registered to the network. The certificate update is performed through a Trusted Authority (TA), which sends the updated certificate to the requesting OBU through the available RSUs on the Roads. RSU does this verification rather than by TA in a timely manner since RSU can securely communicate with TA. Due to this communication overhead is reduced. Thus, the SM-MAP scheme offers a distributed certification services. Finally, when a certificate is found to be revoked it must progress the non-revocation process. Thereby it ensures fast revocation verifying process without any delay.

iv. Batch Verification

Considering the requirement for each vehicle to
verify a large number of messages in a timely manner, SM-MAP introduces an efficient batch verification technique, which enables any vehicle to simultaneously verify number of messages in bulk. The verification is done by using Secure Hash
Algorithm (SHA-1). Therefore, the SM-MAP can meet the security and efficiency requirements for certificate service in vehicular communications.

C. Revocation

The revocation is triggered by the TA when the certificates of OBU is to be revoked. In addition, the secret key set RS_u of OBU_u and the current secret Key K_g are considered revoked. Hence, a new secret key $\widetilde{K_g}$ 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 [17]. The revocation process is carried out by altering the revoked certificate into a non-revoked. Once the certificate has been non-revoked it can used further by the OBUs for disseminating the safety-related message without ignorance.

The process can be performed by gathering the revoked OBU's secret key which is used for secure communication and the hash value from the hash chain. Update both the secret key and the hash value and finally redistributed. The updated CRL is now distributed by the RSU to the all other OBUs.

IV. SECURITY ANALYSIS

1. Resistance of forging Attack

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 unforgivable.

2. 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. 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.

3. Resistance to Replay Attack

Since in each message an OBU includes the current time stamp in the revocation check value, an attacker cannot record REVcheck at time T and replay it at a later time T+1 to pass the revocation checking process as the receiving OBU compares the current time T+1 with that included in the revocation check. Consequently, EMAP is secure against replay attacks.

4. 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

V. PERFORMANCE EVALUATION

1. Computation Complexity of Revocation Status Checking

In EMAP, the revocation checking process requires only one comparison between the calculated and received values of REVcheck. As a result, the computation complexity of EMAP is O(1), which is constant and independent of the number of revoked certificates. In other words, EMAP has the lowest computation complexity compared with the CRL checking processes employing linear and binary search algorithms.

2. Authentication Delay

The message authentication delays are employed in checking the revocation status of the OBU units. The authentication messages are performed by three processes: checks the sender revocation status, verify the sender certificate and also check the sender signature. For VANET the CRL adopt secure hash algorithm by encrypting the message. For the second and third authentication phases, we employ Elliptic Curve Digital Signature Algorithm (ECDSA) to check the authenticity of the certificate and the signature of the sender. ECDSA is the digital signature method chosen by the WAVE standard.

3. End -to- end delay

The end-to-end delay is defined as the time to transmit a message from the sender to the receiver.

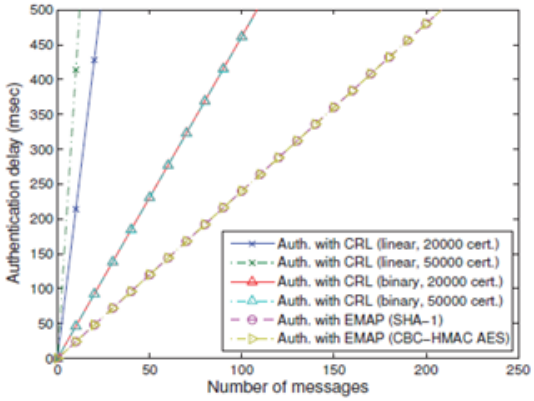

Fig: 2 Authentication Delay per message

It can be seen that the end-to-end delay increases with the OBUs density because the number of the received packets increases with the OBUs density resulting in longer waiting time for the packets to be processed by the application layer in each OBU.

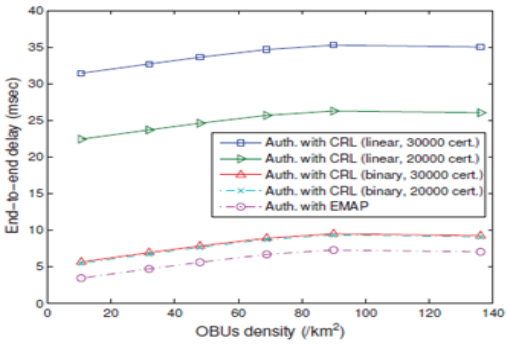

Fig. 3 End to end delay vs OBU Density

4. 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 the message authentication employing EMAP significantly decreases the message loss ratio compared to that employing either the linear or binary CRL revocation status checking. The reason of the superiority of EMAP is that it incurs the minimum revocation status checking delay compared to the linear and binary CRL revocation checking processes.

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] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.1 YEAR 2013.

[2] 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. 29

[3] 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.

[4] 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.

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

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

[7] 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.

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

[9] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

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

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

[12] 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.

[13] 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, 2007.

[14] P. P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communication systems," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 86–87, 2008.

[15] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 88–89, 2008.

[16] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proc. 2003 IEEE Symposium on Security and Privacy, pp. 197–213, 2003.

[17] 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, 2002.

[18] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," Journal of Computer Security, vol. 14, pp. 301–325, 2006.

[19] A. Wasef and X. Shen, "PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks," Proc. ICC'08, pp. 1458–1463, 2008.

[20] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," IEEE Trans. On Vehicular Technology, vol. 58, no. 9, pp. 5214 – 5224, 2009.

[21] 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, 2001.

[22] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[23] M. Scott, "Computing the Tate pairing," Topics in Cryptology, Springer, pp. 293–304, 2005.
[24] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," Designs, Codes and Cryptography, vol. 19, no. 2, pp. 173–193, Mar. 2000. 30
[25] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.
[26] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to algorithms. MIT Press, 2001.
[27] S. Frankel, R. Glenn, and S. Kelly, "The AES-CBC cipher algorithm and its use with IPsec," RFC3602, Sept. 2003.
[28] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," RFC 3174, Sept. 2001.
[29] "Crypto++ library 5.5.2." [Online]. Available: http://www.cryptopp.com/
[30] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.
[31] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," Proc. IEEE INFOCOM 2008, pp. 246–250, 2008.
[32] "The network simulator - ns-2." [Online]. Available:http://nsnam.isi.edu/nsnam/index.php/User Information.
[33] "Traffic and network simulation environment - TraNS." [Online]. Available: http://trans.epfl.ch/

