Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.476 – 482

RESEARCH ARTICLE

PRECIPITATE MESSAGE MANIFEST PROTOCOL FOR VEHICULAR AD HOC NETWORKS

[1]Ramya. K, [2]Nithya. N

[1]PG scholar, Department of Computer Science and Engineering, Anna University Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

[1,2]Ranganathan Engineering College, Coimbatore

[1] ramyacse015@gmail.com, [2] Nithya.varsha1@gmail.com

Abstract* - *Vehicular ad hoc networks (VANETs) adopt the Expedite Message Authentication Protocol (EMAP) and Certificate Revocation Lists (CRLs) for their security. In any EMAP 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 a Message Authentication Acceleration (MAAC) protocol for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation check process. The revocation check process 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). The MAAC protocol uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key .By conducting security analysis and performance evaluation, the MAAC protocol is demonstrated to be secured and efficient.

Keywords – Vehicular Networks, Message Authentication, Certificate Revocation, Communication Security, ECDS algorithm

I. INTRODUCTION

The 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. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: 1) 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 [1], [2], [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], [5], [6]. 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 [7]. Since the number of the OBUs is huge and each OBU has a set of certificates, the CRL size will increase dramatically. The Wireless Access in Vehicular Environments (WAVE) standard [9] does not state that either a non-optimized search algorithm, e.g., linear search, or some sort of optimized search algorithm such as binary search, will be used for searching a CRL. To have an idea of how large the CRL size can be, consider the case where only 100 OBUs are revoked, and each OBU has 25,000 certificates [8]. the Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematics information.

II. RELATED WORK

A. Expedite Message Authentication Protocol (EMAP) have some entities

A Trusted Authority (TA): This is responsible for providing anonymous certificate 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.

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

In this Module, 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 a list containing the entire 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.

C. Search algorithms

In existing system have two algorithms one is linear search algorithm which is only comparison of each entry in the CRL checking process and the second one is binary search algorithm which is worked only sorted list. 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.

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.

III. PROPOSED SYSTEM

During the first phase, EMAP and CRL using which is also have some in secured problem. But In this paper the Vehicular ad hoc domain have two basic communication mode one is vehicular to vehicular communication which is communicate through onboard units (OBUs) and another one is vehicular to infrastructure which is communicate through road side units (RSUs).Here both communication have EMAP using keyed HMAC. Where the key is used to calculating the Hash Message Authentication code which is shared only between the non-revoked OBUs. This EMAP have been some problem i.e. it will take more time consuming for that revocation checking process, inefficient communication and authentication delay occurred. So that we want to propose MAAC protocol which is meant by Message Authentication Acceleration Protocol. In this protocol replace the certificate revocation list and key distribute to the intended entities. It can be enabling the non-revoked OBUs and each OBU update its secret key. Finally transmit the message to trusted authority of base station here check the message valid are not by using MAAC protocol.

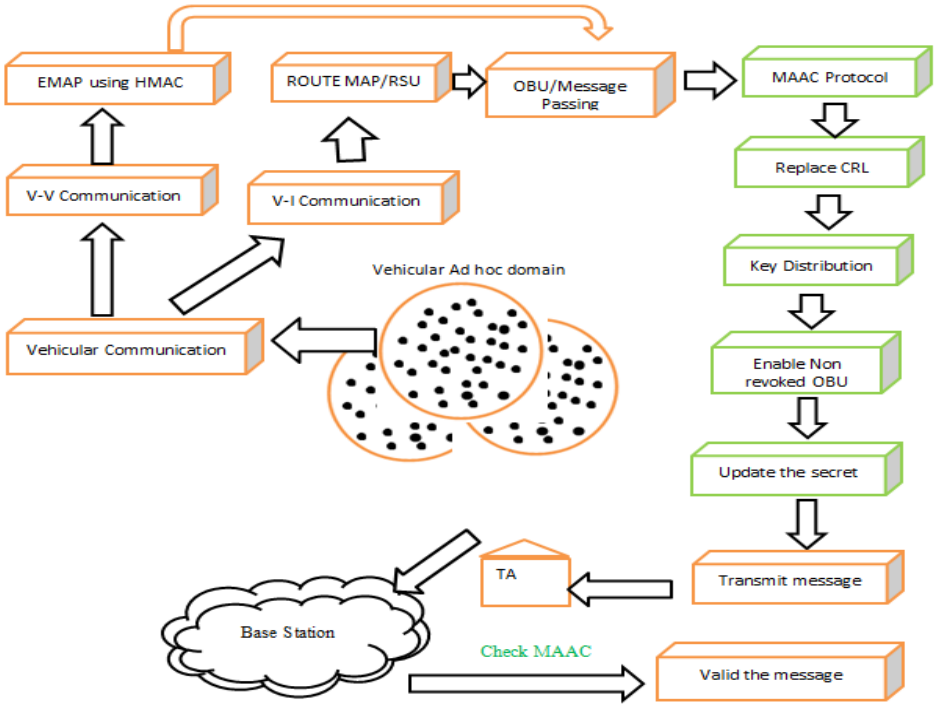
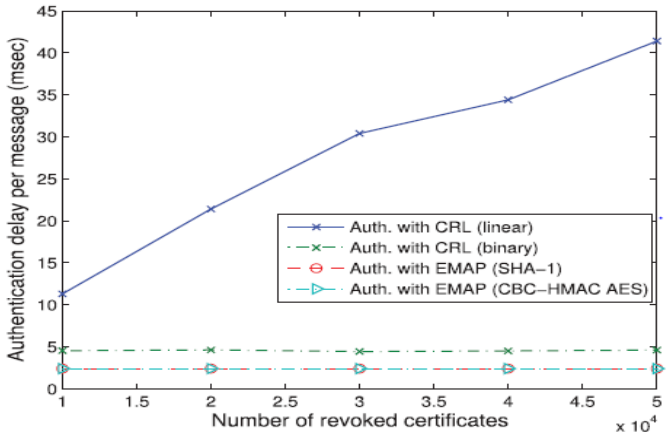


Fig.1 System Architecture diagram.

IV. PERFORMANCE EVALUATION

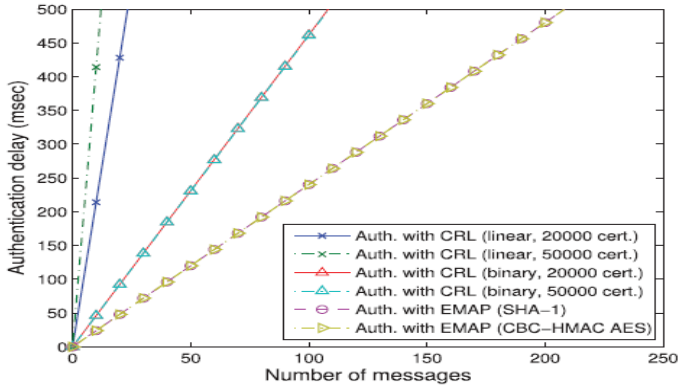
A. Authentication delay

Compare the message authentication delay employing the CRL with that employing MAAC to check the revocation status of an OBU. To employ either the CRL or EMAP. For MAAC, To adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES) Also, It have simulated the linear and binary CRL checking process using C++ programs compiled on the same machine. 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. In ECDSA, signature verification takes 2Tmult, where Tmult denotes the time required to perform a point multiplication on an elliptic curve. Consequently, the verification of a certificate and message signature takes 4Tmul, Tmul is found for a super singular curve with embedding degree k ¼ 6 to be equal to 0.6 msec.



(a) Authentication delay per message

Fig.2 Authentication delay per message



(b) Total authentication delay vs. the number of the received messages

Fig.3 Authentication delay of received messages

B. Message loss ratio

It can be seen that the simulated average message loss ratio closely follows the analytical message loss ratio which is calculated based on the maximum number of messages that can be authenticated within 300 msec. The difference between the analytical and simulations results stems from observing that some zones in the simulated area become more congested than other zones, thus, some OBUs experience higher message loss than other OBUs, which leads to that difference between the analytical and simulations results. It can also be seen that the message loss ratio increases with the number of OBUs within communication range for all the protocols under considerations. In addition, the message authentication employing MAAC 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.

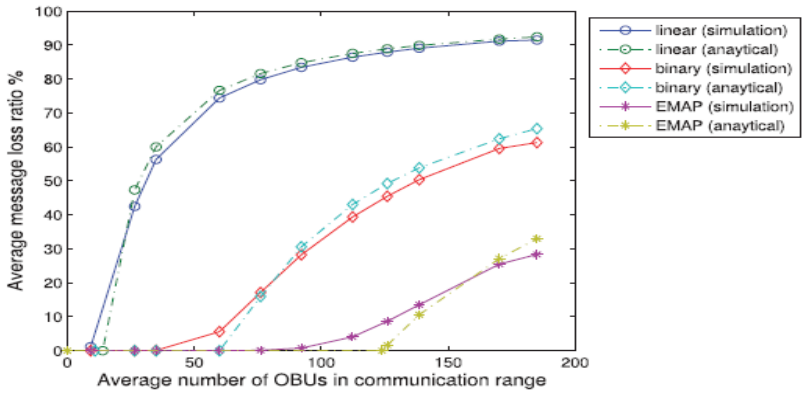


Fig.4 Comparison between message loss ratio for different schemes

C. Communication overhead

A signed message in the WAVE standard should include the certificate of the sender, a time stamp, and the signature of the sender on the transmitted message. Consequently, the additional communication overhead incurred in EMAP and MAAC compared to that in the WAVE standard is mainly due to REVcheck. The length of REVcheck depends on the employed hash function. For example, when SHA-1 is employed in EMAP for calculating REVcheck, this is corresponding to an additional overhead of 20 bytes. The total overhead incurred in a signed message in the WAVE standard is 181 bytes. Consequently, the total overhead in EMAP (SHA-1), assuming the same message format of the WAVE standard, is 201 bytes. In WAVE, the maximum payload data size in a signed message is 65.6 Kbytes. Accordingly, the ratio of the communication overhead in a signed message to the payload data size is 0.28 and 0.31 percent for the WAVE standard and MAAC, respectively. EMAP incurs 0.03 percent increase in the communication overhead compared to the WAVE standard, which is acceptable with respect to the gained benefits from EMAP.

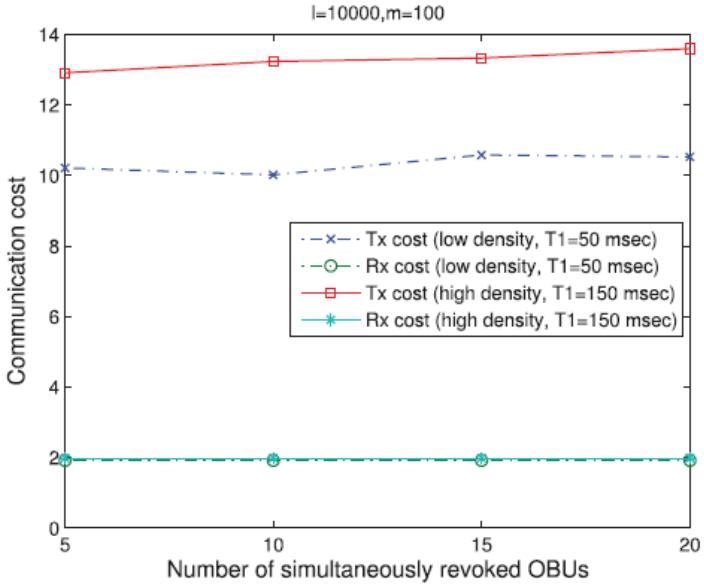


Fig.5 Communication cost of updating Kg in MAAC.

V. CONCLUSION

This approach ensures that MAAC for VANETs, which is Message Authentication Acceleration by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed MAAC uses a novel key sharing mechanism and ECDS algorithm which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, MAAC 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, MAAC can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

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 Standards for Privacy in User-Centric Identity Management, July 2006.

[2] 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) Conf., Nov.2005.

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

[4] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "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.

[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "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.

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

[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] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012. [1] P.Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems:A Position Paper," Proc. Workshop Standards for Privacy in User-Centric Identity Management, July 2006.

Authors Profile

Ramya. K – Currently pursuing her M.E in Computer Science and Engineering from Ranganathan Engineering College, Coimbatore. Her areas of interest are Mobile computing and network security

Nithya. N –She is working as an Assistant Professor in Department of Computer Science and Engineering in Ranganathan Engineering College, Coimbatore, India. His areas of interest are Mobile computing, and Data Mining.

