ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

AMAP: Accelerated Message Authentication Protocol for Vehicular ADHOC Networks

R. Rajkumar, S.Shahul Hammed

Dept. of Computer Science And Engineering, Karpagam University, Coimbatore, India

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 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 an Accelerated Message Authentication Protocol (AMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in AMAP uses a Hashed Message Authentication Code HMAC using RSA algorithm where the key used in calculating the HMAC is shared only between non revoked On-Board Units (OBUs). AMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing . CRL.AMAP is secure and efficient.

I . INTRODUCTION

VEHICULAR ad-hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. 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 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 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 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. 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 if only a small portion of the OBUs is revoked. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

certificates [8]. In tis case, the CRL contains 2.5 million revoked certificates. According to the employed mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard [9] does not state that

either a no 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. In this paper, we consider both non optimized and optimized search algorithms.

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 delay resulting from checking the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol1 (AMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC-RSA function. AMAP 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 VANETs,the primary security requirement are identified as entity authentication,message integrity, non repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [4],[12]. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long. In [12], Hubaux identify the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In [4], Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANETs. In 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. In this approach,revoking one vehicle implies revoking the huge number of certificates loaded in it.

2.1 Accelerated Message authentication protocol

The proposed AMAP uses a fast HMAC Using RSA algorithm function and novel key sharing scheme employing probabilistic random key distribution compared to EMAP.

III . SYSTEM MODEL

As shown in Fig. , the system model under consideration consists of the following: A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. ÿ Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA. ÿ OBUs,which are embedded in vehicles. OBUs can communicate either with other OBUs.

According to the WAVE standard [9], 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 HSMs. Finally, we consider that a compromised OBU is instantly detected by the TA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

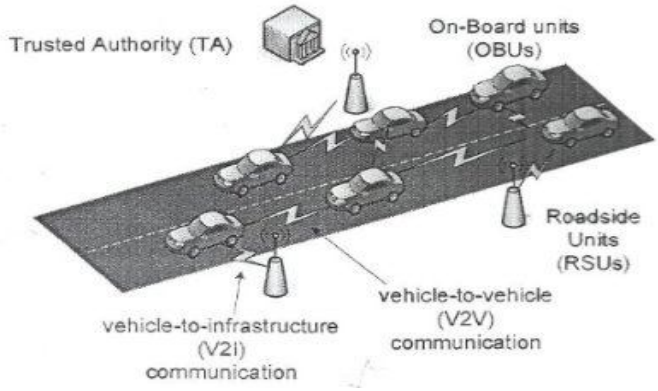
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



3.1 Security Analysis

In this section, we analyze the security of the proposed protocol against some common attacks. 5 Resistance to Forging Attacks To forge the revocation check REVcheck ¼ HMACðKg; PIDukTstampÞ of any OBUu, an attacker has to find the current Kg, which is equivalent to finding t in the following ECDLP problem: given Kim ¼ tKÞM ¼ t kM P and KÞM ¼1 kMP, find t such that Kim ¼ tKÞM . Similar analogy applies to finding the TA secret key s from the TA message signature sgnKmsg ¼ sHðKmsgÞ. Since ECDLP is a hard computational problem [25], i.e., it cannot be solved in a subexponential time, the revocation check and the TA message signature sgnKmsg are unforgivable. Similarly, finding the TA secret value s from P_ ¼ sP is ECDLP problem, which makes it unforgeable. From the aforementioned discussion, it is concluded that EMAP is resistant to forging attacks.

3.2 Authentication Delay

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) [28] and Secure Hash Algorithm 1 SHA-1 [29] as theHMAC functions. We consider the PID of OBU and the time stamp ðTstampÞ having equal lengths of 8 bytes. We adopt the Crypto++ library [30] for calculating the delay of the HMAC functions, where it is compiled on Intel Core2Duo 2 GHz machine. The delay incurred by using CBC-HMAC AES and SHA-1 to calculate the revocation check ðREVcheck ¼ HMACðKg; PIDukTstampÞÞ is 0.23 and 0:42 _sec, respectively. Also, we have simulated the linear and binary CRL checking process using C++ programs compiled on the same machine. The linear CRL checking program performs progressive search on a text file containing the unsorted identities of the revoked certificates, while the binary CRL checking program performs a binary search on a text file containing the sorted identities of the revoked certificates. For the second and third authentication phases, we employ Elliptic Curve Digital Signature Algorithm (ECDSA) [31] 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, a signature verification takes 2Tmul, where Tmul denotes the time required to perform a point multiplication on an elliptic curve. Consequently, the verification of a certificate and message signature takes 4Tmul. In [32], Tmulis found for a supersingular curve with embedding degree k ¼ 6 to be equal to 0.6 msec.Incurred Delay to Obtain the New Secret Key ðK~gÞ. We are interested in the average delay for an OBU without K_ M to get the new secret key K~g from its neighboring OBUs after the revocation message REVmsg is delivered to all the OBUs in the simulated area. We conducted ns-2 simulation for the low and high OBUs densities scenarios considered in the previous section. Initially, the percentage of OBUs having the key K_ M , and capable of independently calculating K~g,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

is 1.97 and 1.56 percent for the low and high OBUs densities scenarios, respectively. Fig. 8 shows the average delay in msec, incurred by an OBU from the moment the revocation message REVmsg is received by all the OBUs in the simulated area until it gets the new secret key K~g, versus the number of simultaneously revoked OBUs. It can be seen that the incurred delay to get K~g is confined to a small range in each scenario. Also, the delay of obtaining K~g in the high OBU density scenario is higher than that in the low OBU density scenario as the value of T1 in the high OBU density scenario is higher than that in the low OBU density scenario. However, for both low and high OBU densities, the delay of getting K~g is less than 1 sec, which indicates that EMAP is feasible and reliable.

IV . CONCLUSION

EMAP for VANETs, which expedites message authentication by replacing the time- consuming CRL checking process with a revocation checking process employing HMAC function. The proposed AMAP 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, AMAP 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, AMAP 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]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]A.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]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.
[6]US Bureau of Transit Statistics, Passenger_vehicles_in_the United_States,2012.
[7]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 Inter NETworking, pp. 89-98,2009.
[8]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