INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2826 - 2833
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018
March 21, 2018

ACCELERATE MESSAGE PROVING PROTOCOLS FOR VANET

Ms.G.Indumathi., M.Sc (Computer science) II[nd] year.
Asst. Prof.E.Bhuvaneshwari.,MCA.,M.Phil.,
Department of Computer Science, Kamban Arts And Science College for Women, Thiruvannamalai.

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 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 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.

1. 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 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 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:

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 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. 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;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. 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 certificates. In this 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 does not state that either a non-optimized search algorithm.

2. STUDY OF 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.

- OBU - On-Board Units

DISADVANTAGE: 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.

3. PROPOSED SYSTEM FOR VANET:

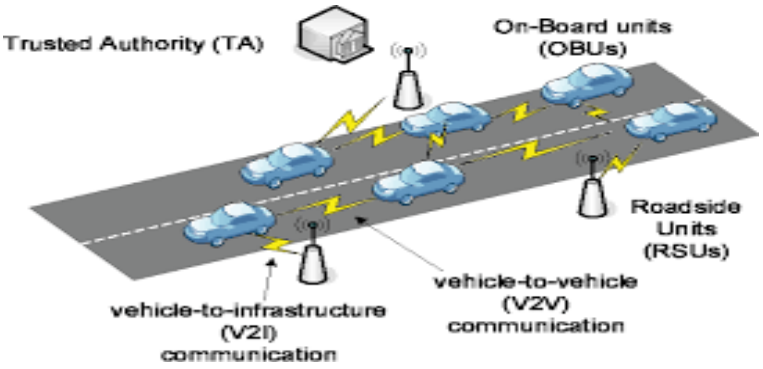
In Propose System an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network.

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 OF VANET: Safety-related VANETs applications.

4. ARCHITECTURE FOR VANET COMMUNICATION:

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2826 - 2833
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018
March 21, 2018



5. IMPLEMENTATION

1. 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 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, **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.

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.

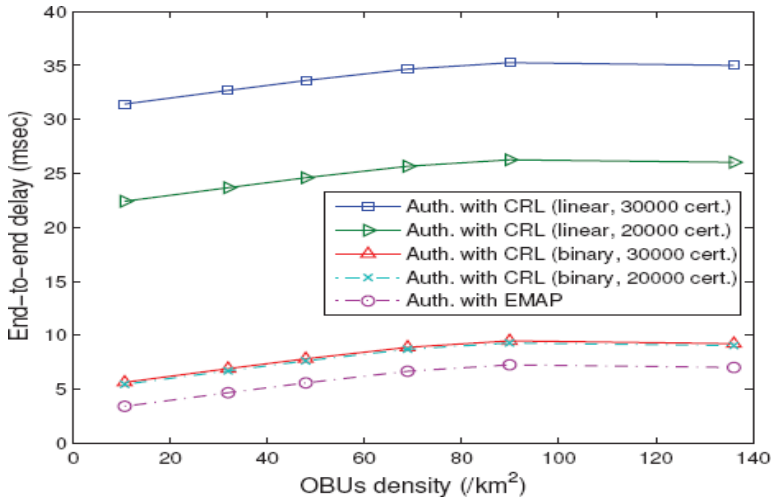
6. PERFORMANCE EVALUATION:

A. Computation Complexity of Revocation Status

Checking: We are interested in the computation complexity of the revocation status checking process which is defined as the number of comparison operations required to check the revocation status of an OBU. Let Nrev denote the total number of revoked certificates in a CRL. To check the revocation status of an OBU using the linear search algorithm, an entity has to compare the certificate identity of OBU with every certificate of the Nrev certificates in the CRL, i.e., the entity performs one-to-one checking process. Consequently, the computation complexity of employing the linear search algorithm to perform a revocation status checking for an OBU is O (Nrev). In the binary search algorithm, the certificate identity of OBUu is compared to the certificate identity in the middle of the sorted CRL.

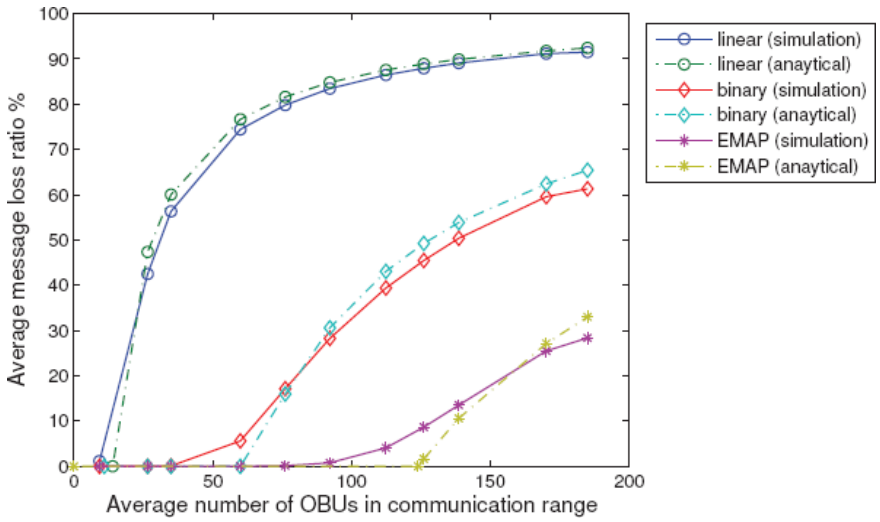
B. End-to-End Delay: To further evaluate EMAP, we have conducted ns-2 simulation for the city street scenario shown in Fig.3. The adopted simulation parameters are given in Table 1. We select the dissemination of the road condition information by an OBU every 300 msec to conform to the DSRC standards. The mobility traces adopted in this simulation are generated using Trans. We are interested in the end-to-end delay, which is defined as the time to transmit a message from the sender to the receiver.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2826 - 2833
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018
March 21, 2018



C. 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. 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 every 300 msec. The below diagram shows the analytical and simulated average message loss ratio vs. the average number of OBUs within the communication range of each OBU for message authentication employing CRL linear checking, CRL binary checking, and EMAP, respectively, for a CRL containing 20, 000 certificates. 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 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.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2826 - 2833
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018
March 21, 2018



D. Communication Overhead: In EMAP, each OBUu broadcasts a signed message on the form (M||Tstamp|| certu(PIDu, PKu, sigTA(PIDu||PKu))||sigu(M||Tstamp)||REVcheck) to its neighboring OBUs. 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 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 [27]. The total overhead incurred in a signed message in the WAVE standard is 181 bytes [7]. Consequently, the total overhead in EMAP (SHA-1), assuming the same message format of the WAVE standard, is 201 bytes. In WAVE [7], 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% for the WAVE standard and EMAP, respectively. EMAP incurs 0.03% increase in the communication overhead compared to the WAVE standard, which is acceptable with respect to the gained benefits from EMAP.

7. EXPERIMENTAL RESULTS:

Our experimental results show that, it overcomes the drawbacks of existing system. the proposed system 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 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.

8. 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.

9. 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. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," *Proc. Embedded Security in Cars (ESCAR)*, November 2005.

[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, 2010.

[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] "US 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 1609.2-2006*, 2006.

[8] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

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

[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, 2009.

[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, 2007.

[13] 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.

[14] 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.

[15] 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.