Expedite Message Authentication Protocol For Vehicular Ad-Hoc Network

Arun.J[1], Manoj.R[2], Manopriya.G[3], Narmadha.V[4], Mrs.Suganyamahalakshmi A[5], Mr.Dr.Arulprakash.P[6]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[5]Assistant Professor, Dept of Computer Science and Engineering
[6]Associate Professor & Head, Dept of Computer Science and Engineering
[1, 2, 3, 4, 5, 6] Rathinam Technical Campus, 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 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 nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked 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.*

I. INTRODUCTION

Implementing Expedite Message Authentication Protocol(EMAP) for Vehicular ad-hoc network(VANET) that uses a fast Hash Message Authentication Code(HMAC) function which expedites message authentication by replacing the time-consuming Certificate Revocation Lists(CRL) checking process with a fast revocation checking process and novel key sharing scheme employing probabilistic random key distribution which allows on On Board Unit(OBU) to update its compromised keys even if it previously missed some revocation messages.

Expedite Message Authentication Protocol 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 in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs.

II. EXISTING SYSTEM

In this paper, we consider both nonoptimized and optimized search algorithms. According to the Dedicated Short Range Communication (DSRC), which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an inevitable challenge to VANETs. 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 authentication delay resulting from checking the CRL for each received certificate.

III. DISADVANTAGES OF EXISTING SYSTEM

- 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.
- To abstain the leakage of the real identities and location information of the drivers from any external eavesdropper.
- The scale of VANET is very large.

IV. PROPOSED SYSTEM

In this paper, we introduce an expedite message authentication protocol (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 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.

V. ADVANTAGES OF PROPOSED SYSTEM

- EMAP has the lowest computation complexity compared with the CRL checking processes employing linear and binary search algorithms.
- The number of messages that can be verified using EMAP within 300 msec is greater than that using linear and binary CRL checking by 88.7 and 48.38 percent, respectively.
- The proposed EMAP in authentication reduces the end-to-end delay compared with that using either the linear or the binary CRL checking process.

VI. MODULES

1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure
2. Expedite Message 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:

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.

Expedite Message Authentication Protocol:

1. **Trusted Authority (TA):** This is responsible for providing anonymous certificate and Distributing secret keys to all OBUs in the network.
2. **Roadside units (RSUs):** which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
3. **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.

VII. SECURITY ANALYSIS

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.

SYSTEM REQUIREMENTS:

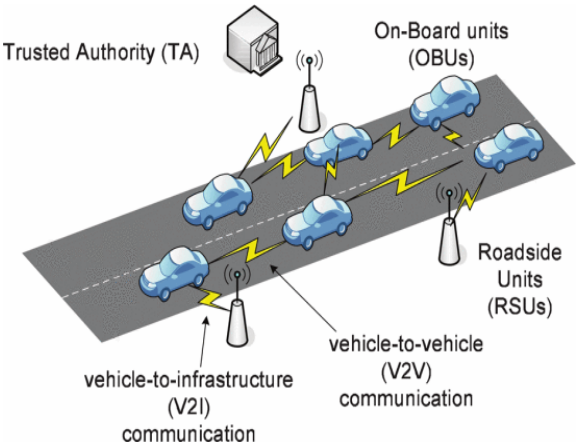
HARDWARE REQUIREMENTS:

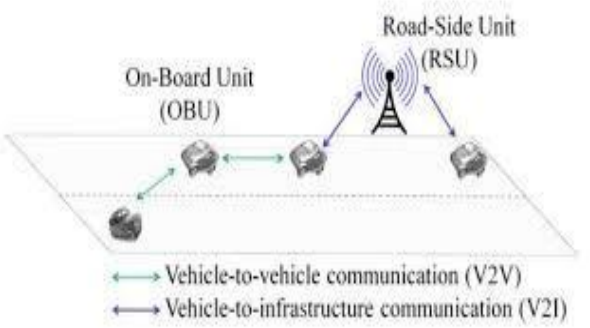
- System : Intel core i3(Min)
- Hard Disk : 40 GB(Min)
- Ram : 1 GB(Min)

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7
- Coding Language : C#, .NET
- Data Base : MS SQL SERVER 2005

SYSTEM MODELS:





VIII. CONCLUSION

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 integral 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] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, Privac 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 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 Net-works, 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 Transit Sttistics, 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 Intl Workshop VehiculArInterNET working, 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.