ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Secured Multi Message Authentication Protocol for Vehicular Communication

C.SelvaLakshmi[1], N.Senthil Madasamy[2], T.Pandiarajan[3]

PG Student, ANNA UNIVERSITY, Nodal Center- Kamaraj College Of Engineering & Technology, Virudhunagar, Tamilnadu, India[1]

Assistant Professor, Depatrment of IT, Kamaraj College of Eng & Technology, Virudhunagar, Tamilnadu, India[2]

Assistant Professor, Depatrment of CSE, P.T.R College of Engineering & Technology, Madurai, Tamilnadu, India[3]

Abstract: VANETs are a subset of mobile ad hoc networks composed of network-equipped vehicles and infrastructure points, which will allow vehicles to communicate with other vehicles and with roadside infrastructure points. The method agreed upon for confidentiality and authenticity by the IEEE 1609 working group is a public key infrastructure (PKI) system. An important part of any PKI system is the revocation of certificates. The revocation process, as well as the time taken for revocation process by Trusted Authority, is an open problem for VANETs. A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. So that communication overheads and consumes delay in message authentication. Hence Secured Multi Message Authentication protocol(SM-MAP) for vehicular communication is proposed. To solve this problem, an efficient way for any On-Board Units (OBUs) to update its certificate from the available infrastructure Road-Side Units (RSUs) in a timely manner. In addition, the SM-MAP introduces batch verification technique for authenticating messages, which significantly decreases the verification overhead. Moreover the scheme achieves excellent security and efficiency for vehicular communications.

Keywords: Vehicular networks, Message Authentication, Certificate Revocation, Security.

I. INTRODUCTION

VEHICULAR Ad Hoc Network (VANET), as a special of mobile ad hoc network, has been subject to extensive research efforts not only from the government, but also from the academia and automobile industry in recent years. Different from the traditional ad hoc networks, VANET contains not only mobile nodes — vehicles, but also stationary Roadside Units (RSUs). According to the Dedicated Short Range Communications (DSRC) [1], in road safety-related applications, each vehicle equipped with On-Board Units (OBUs) will broadcast routine traffic messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. However, before putting this attractive application into practice, security issues in VANET must be resolved [2]–[4]. Without the security guarantees, an adversary in VANET can either forge bogus information to mislead other drivers and even cause deliberate traffic accident, or track the locations of the interested vehicles by collecting their routine traffic messages. 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.

A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. Another significant function of the TA is to publish Certificate Revocation Lists (CRLs).

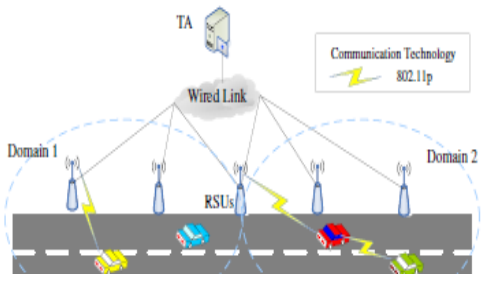

Fig. 1. System model

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

On-Board Units (OBU), The OBU is DRSC transceiver generally installed in or on a vehicle; OBU can communicate either with other OBUs through Vehicle-to-Vehicle (V2V) communications or with the infrastructure RSUs through Vehicle-to-Infrastructure (V2I) communications. Each OBU is equipped with a Global Positioning Service (GPS) receiver which contains the geographical coordinates of the RSUs.

Hardware Security Module (HSM), According to the Wave standard each network is equipped with tamper resistant HSM whose purpose is to to store its security materials, eg., secret keys, certificates, etc. and physically protect sensitive information and provide a secure time base.

Road Side Units (RSU), is a DSRC transceiver fixed units distributed in the network. Moreover, RSUs are responsible for updating the certificates of the OBUs.

In spontaneous vehicular communications, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. Deploying efficient Public Key Infrastructure (PKI) is a well-recognized solution to achieve security for practical vehicular networks [1],[4]. Although VANETs have recently gained extensive attention, very few works have addressed the design of a PKI suitable for the security requirements of VANETs.

In [4], Hubaux et al. identify the specific issues of security and privacy challenges in VANETs, and claim that a Public Key Infrastructure (PKI) should be well deployed to protect the transited messages and to mutually authenticate among network entities. In [1], Raya et al. use a classical PKI to provide secure communications to VANETs. For this approach, each vehicle needs to pre-load a huge pool of anonymous certificates. The number of the loaded certificates in each vehicle should be large enough to provide security 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. The requirement to load a large number of certificates in each vehicle incurs inefficiency for certificate management as revoking one vehicle implies revoking the huge number of certificates loaded in it.

There is a work addressing the problem of distributing the large-size CRL in VANETs. In [6], Raya et al. introduce Revocation using Compressed Certificate. Revocation Lists (RC2RL), where the traditional CRLs, issued by the TA, are compressed using Bloom filters to reduce its size prior to broadcasting.

In [16] Wasef et al. introduces 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). This work takes much more time in authenticating the messages and for revocation of certificates. All the above process is carried by Trusted Authority (TA) which incurs a long delay.

In the above related works CRL size is reduced but the time by Trusted Authority for checking the revocation status takes a long time. So that communication overheads and causes delay in message authentication. Hence we propose a scalable and efficient message authentication protocol which reduces the delay incurred in verifying the authentication of messages by batch verification and revocation of certificates, which is done by RSU rather than by Trusted Authority in timely and secured manner. Thereby reducing the message loss ratio. Message integrity and confidentiality is achieved to enhance the security with the help of Asymmetric Key Concepts. The main aim is to provide fast and secure communication among vehicles thereby enhancing the safety related communication in road sides.

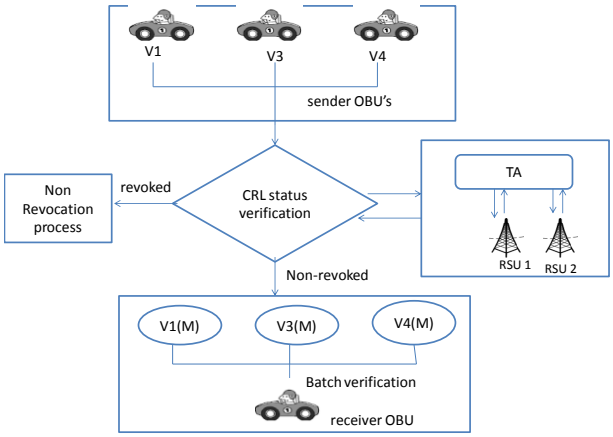

Fig. 2. Overall Design

Vehicular communication is done by registering the vehicles (OBUs) to the Trusted Authority. After registration the TA issues the necessary parameters i.e. Certificates, keys used for sending and receiving the messages which are needed by the OBUs for communication. At first the sender OBU has to share the secret key in the network to which they wish to communicate. The sender OBU now sends the message with MAC prepared by them using their private key. The receiver OBU, before accepting the message does the verification that whether the certificate of the multiple senders' certificate is revoked or not. This revocation process is done by RSU rather than the TA in a timely and secure manner. If non revoked decrypts the message using their own public key. The receiver OBU calculates its own

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

MAC code and compares it with the sent MAC code. If both the MAC code matches, the message integrity is verified and confidentiality is achieved using a pair of private/public keys. Finally the receiver OBU accepts the message. The verification of messages is done on the whole using batch verification method, thereby reducing the delay and message loss ratio.

II PROPOSED WORK

A. Initialization Of vehicles

Vehicles are initialized by creation and registration process. The vehicles are first created in the network and get registered to the TA using the information Vehicle id (Vid) and signature id (Sig id). The signature id is created using the algorithm DSA. After registration; 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.

Finally TA stores the information such as Vehicle id, signature id and Time stamp for each vehicle.

B. Message Authentication

Message Authentication involves two processes such as:-

1. Message Broadcasting
2. Message Verification

OBU which is installed in each vehicle performs all the cryptographic operations such storing the keys, certificates and performing message encryption and decryption. Before starting the process of communication, shared key is exchanged between vehicles for the purpose of secure communication. After sharing the key, the vehicles can disseminate the safety-related message to other vehicles such as vehicle's speed, acceleration, deceleration, velocity and so on.

1. Message Broadcasting:

The source vehicle, OBU_U broadcast its safety related message to the other nearby vehicles along the roadside. Before broadcasting, the OBU_U calculates a REV Check i.e. HMAC using the secret key and the message to be sent. The MAC which is generated ensures message integrity and the authentication services.

REVcheck=MAC (Kg,M)

After calculating the REV Check, OBU_u broadcast the message by encrypting with public key. Finally the message is broadcasted to other nearby vehicles.

2. Message Verification:

The destination vehicle, OBU_Y before receiving the message checks CRL status that the certificate of the intended OBU_U is revoked or not. After verification, if the certificate is non-revoked OBU_Y 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_Y 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.

C. 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_Y. The CRL verification is performed using the concept of hash chain. RSU, 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 ensuring fast revocation verifying process without any delay.

D. Batch Verification

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

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 a mass of messages. 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.

Fig. 3. RSU aided Verification

E. Revocation Process

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.

F. Security Services

In order to better understand the data flows of message exchanges employing a certificate-based PKI scheme in VANETs, two services are used to provide a conceptual view of data flows in the certificate-based PKI scheme. The two services occurring in a VANET includes:

1. Communication that require the provision of data integrity.
2. Communications that require the provision of confidentiality.

Case 1: Communications require the provision of data integrity

Vehicle A broadcasts a safety-related message to the relevant vehicles and Roadside Units in the area. The data flows for a message exchange pattern requiring data integrity in VANETs are illustrated.

Sender's End:

Step 1. Creation of safety-related message:
The sender initiates a safety-related message.
Step 2. Creation of a MAC code for the safety-related message:
The safety-related message and secret key is used to create a MAC code.
Step 3. Message delivery:
The message and the MAC code are ready for message dissemination to the intended recipient.

Receiver's End:

Step 4. Message reception:The intended recipient receives the message (safety-related message and MAC code).

Step 5. Certificate verification:

Notice that there is not a universal sequence in which these processes should be performed.
Step 5.1 To examine the validity time period of the certificate against the current time.
Step 5.2 To check if the certificate is revoked against the CRLs.
Step 6. Client authentication and data integrity verification:
Step 6.1 To authenticate the received message from the sender.
Step 6.2 To verify the MAC code on the received message by using the secret key.
Step 7. Message display:
Upon successful validation, the received message is rendered to the recipient.

Case 2: Communications requiring the provision of confidentiality services

Vehicle A sends a safety-related message to Vehicle B requiring confidentiality. The confidentiality is achieved using the asymmetric key cryptography algorithm RSA. The

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

data flow for a message exchange pattern requiring confidentiality is illustrated.

key exchange:

The public/private keys are issued by the TA as soon as the vehicles get registered in the network. These keys are used for encryption/decryption.

Vehicle A:

Step 1. Creation of safety-related message:
Vehicle A initiates a safety-related message.
Step 2. Message encryption:
Vehicle A uses the public key to encrypt the message.
Step 3. Message delivery:
The encrypted safety-related message is ready for message dissemination to the intended recipient.

Vehicle B:

Step 4. Message reception:
Vehicle B receives the encrypted safety-related message.
Step 5. Message decryption:
Vehicle B uses the private key to decrypt the message.
Step 6. Message display:
Upon successful validation, the received message is rendered to the recipient.

III PERFORMANCE EVALUATION

A. Computation Complexity of Revocation Status Checking

Let Nrev denote the total number of revoked certificates in a CRL. To check the revocation status of an OBU_u using the linear search algorithm, an entity has to compare the certificate identity OBU_u with every certificate of the Nrev certificates in the CRL. Consequently, the computation complexity of employing the linear search algorithm to perform a revocation status checking for an OBU by TA is $O(N_{rev})$.

In (SM-MAP), the revocation checking process by RSU requires only one comparison between the calculated and received values of REV_{check}. As a result, the computation complexity of (SM-MAP) is O(1), which is constant and independent of the number of revoked certificates. In other words, (SM-MAP) has the lowest computation complexity compared with the CRL binary search algorithms.

B. Authentication Delay

For the authentication phase to check the revocation status of the sender, we employ either the CRL or (SM-MAP).

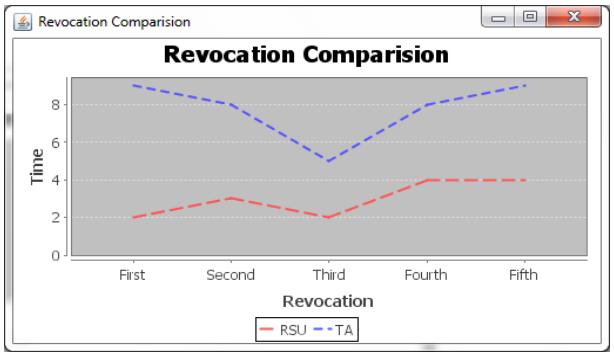

Fig. 4. Performance Evaluations for Revocation

We compare both the message authentication. Employing the linear method to check the revocation status of an OBU takes long time. For (SM-MAP), we adopt the Batch Verification using Secure Hash Algorithm 1 SHA-1 as the HMAC functions.

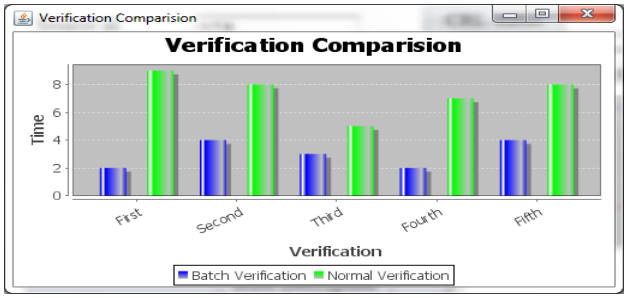

Fig. 5. Performance Evaluations for Message Verification

Fig. 4 shows a comparison between the authentication delays per message using (SM-MAP), linear CRL checking process, versus the number of the revoked certificates, where the number of the revoked certificates is an indication of the CRL size. It can be seen that the authentication delay using the linear CRL checking process increases with the number of revoked certificates, i.e., with the size of the CRL.

IV CONCLUSION

This paper, addresses a major issue to ensure secure communications for vehicular ad hoc networks, namely, certificate revocation of revoked OBU. Secured Multi Message Authentication Protocol, proposed an efficient distributed certificate service for any OBUs to update or revoke its certificate from the available RSUs in a timely manner. In addition with the batch verification, the vehicle (OBU) can rapidly verify a mass of messages and certificates simultaneously. Therefore, the scheme significantly decrease the message loss ratio and message verification delay compared to the conventional authentication methods. The extensive results have demonstrated that, in comparison with the existing methods,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

the proposed SM-MAP can significantly reduce the complexity of certificate management, and achieve excellent efficiency and scalability, reducing revocation time as well as the message verification time, and improving the accuracy and reliability of certificate revocation. Also message integrity and confidentiality is ensured thereby enhancing the security efficiently.

REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacyand Identity Management for Vehicular Communication Systems:A Position Paper," Proc., July 2006.

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

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

[4] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An EfficientPseudonymous Authentication Scheme with Strong PrivacyPreservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, Sept. 2010.

[5] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," 2009.

[6] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[7] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," Proc. Fifth ACM Int'l Workshop VehiculAr Inter-NETworking, pp. 86-87, 2008

[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.

[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification xScheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM, pp. 246-250, 2008.

[10] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.

[11] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

[12] 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.

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

[14] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'lWorkshop VehiculAr Inter-NETworking, pp. 88-89, 2008.

[15] C.Zhang, X.Lin, R.Lu, P.H. Ho, RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks in: Proceedings of the IEEE ICC'08, May 2008, pp.1451-1457.

[16] Albert Wasef , Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" IEEE Transactions on Mobile Computing, vol. 12, no. 1, January 2013

BIOGRAPHIES

C.SelvaLakshmi- Received the Bachelor of Engineering in Computer Science from Anna University of India in 2009 .Currently she is pursuing Master of Engineering in Computer Science at Anna University of India. Her research interest includes Network Security and Database Management Systems.

N.Senthil Madasamy- Received the Bachelor of Engineering in Computer Science from Madurai Kamaraj University of India in 1998 and the Master of Engineering in Computer Science from Anna University in 2007. Currently he is doing Ph.D in Peer to Peer Networks at Anna University of India. He is working as an Assistant Professor in Kamaraj College of Engineering and Technology, Tamilnadu, India. His research interests include Networking, Parallel Computing and Image Computing Processing.

T.Pandiarajan- Received the Bachelor of Engineering in Computer Science from Anna University of India in 2007 and the Master of Engineering in Computer Science from Thiagarajar College of Engineering in 2010. Currently he is working as an Assistant Professor in P.T.R College of Engineering an Technology, Tamilnadu, India. His research interests include Data Mining and Networks.