ISSN: 2321-8169
595 - 599

Certificate Based Scheme and Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks

Ms. Rupali H. Kandhari
PG Student, Department of Computer Engineering,
JSPM's RSCOE, Tathawade, Pune.
e-mail: rupali.kandhari@gmail.com

Prof. S. B. Thakare
Associate Professor, Department of Computer Engineering,
JSPM's RSCOE, Tathawade, Pune
e-mail: mail2sbt@gmail.com

Abstract- VANET security is major issue for researcher. Thus Ad-Hoc Networks embrace the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security purpose. EMAP was presented to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. From the experimental analysis it was observed that it is resistant to common attacks while performing the authentication techniques. Therefore, EMAP can significantly decrease the message-loss ratio due to message verification delay as compared to the conventional authentication methods employing CRL checking. Thus to further address these issues along with EMAP protocol, new EMAP method is presented called as CEMAP (certificate based EMAP) which is intended to overcome the authentication delay in message processing by reducing the complexity in Authentication process. CEMAP authentication protocol is constructed based on the combination of the new signature scheme and EMAP. The proposed algorithm reduces the delay by 10% than EMAP.

Keywords*—CEMAP authentication protocol, EMAP authentication, Vehicular networks, Communication security, Message signature authentication.*

*****

I. INTRODUCTION

Vehicular networks area unit terribly doubtless to be deployed within the coming back years and therefore become the foremost relevant variety of mobile unplanned networks. Vehicular Ad-Hoc networks (VANET) have recently drawn consideration of the analysis community. Vehicular Ad-hoc Networks represent a promptly emerging, significantly difficult category of MANETs. Vehicular communications (VC) aim to reinforce safety and efficiency of transportation systems. Transport applications will offer warnings on environmental hazards, traffic and road conditions and native information. In fact, transport networks emerge, among civilian communication systems, mutually of the foremost convincing and however most difficult instantiations of the mobile Ad-hoc networking technology. Unfortunately, VANET is facing numerous security challenges [3], and far attention has been dedicated to its security problems. V2V and V2I communication have totally different security requirements: for V2V communication, authentication, conditional privacy protection, and non-reputation; for V2I communication, message integrity, origin authentication, non-repudiation is required for RSUs, anonymity, conditional privacy preservation, authentication, message integrity, non-repudiation for OBUs. Some attentions are dedicated to the protection of V2I communication. The prevailing solutions for the protection issue of V2I communication primarily target the authentication and message integrity of RSUs. However, very little attention has been paid to namelessness, conditional privacy preservation, non-repudiation for OBUs.

Anonymity, conditional privacy preservation, and non-repudiation area it needs attention for OBUs. However, OBUs might request numerous added services from RSUs, or it's going to send traffic-related data to RSUs. As an example, OBUs might inform RSUs the number of the vehicle concerned in associate accident. But, OBUs don't wish to be derived by a 3rd party. According to the Dedicated Short vary Communication (DSRC) [8], which is an element of the WAVE normal, every OBU has got to broadcast a message each three hundred time unit regarding its location, velocity, and alternative telemetric data. In such situation, every OBU could receive an oversized range of messages each three hundred time unit, and it's to visualize the present CRL for all the received certificates, which can incur long authentication delay counting on the CRL size and therefore the range of received certificates. The flexibility to visualize a CRL for an oversized range of certificates. An exceedingly in a very timely manner leads an inevitable challenge to VANETs. To ensure reliable operation of VANETs and increase the quantity of authentic data gained from the received messages, every OBU ought to be able to check the revocation standing of all the received certificates during a timely manner. Most of the present works unnoticed the authentication delay ensuing from checking the CRL for every received certificate. Thus to beat this problems recently we've studied new protocol referred to as expedite message authentication protocol (EMAP) that replaces the CRL checking method by associate economical revocation checking method employing a quick and secure HMAC perform. EMAP is appropriate not just for VANETs however conjointly for any network using a PKI system. To the most effective of our data, this was the primary resolution to cut back the authentication delay ensuing from checking the CRL in VANETs. But this approach is suffered from limitation just in case of speed in certificate and message signature authentication. Therefore during this project we have a tendency to are presenting ensuing version of EMAP during which we'll beat up acceleration of certificate moreover as message signature authentication. This new protocol is termed as CEMAP (Certificate primarily based EMAP).

In next section II we are presenting the literature survey over the various methods addressed for Vehicular Ad-hoc Networks. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

II. RELATED WORK

In this section we are addressing the different techniques those are presented to solve the security problems of VANET. In [1], Albert Wasef and Xuemin (Sherman) Shen presented an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL.

In [4], Raya et al. use a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicle needs to pre-load a huge pool. anonymous certificates. The number of the loaded certificate in each vehicle must be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificate from the central authority during the annual inspection of the vehicles. In this approach, revoking one vehicle implies for revoking the huge number of certificates loaded in it. This renders the vehicle not able to send messages to neighboring vehicles

In [11], Studer et al. propose an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted privacy authority and regional authorities (RAs) distributed all over the network. The authors adopted group signatures where the trusted authorities' acts as the group manager and the vehicle act as the group members. Upon entering a new region, each and every vehicle must update its certificates from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA to update its certificate; the RA verifies the group signatures of the vehicles by ensuring that the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short lifetime region-based certificate. This certificate is valid only within the coverage range of the RA. It should be noted that TACK requires the RAs to wait for some time, e.g., 2 seconds, before sending the new

In [12], Raya et al. introduce RC2RL (Revocation using Compressed Certificate Revocation Lists), where the traditional CRLs, issued by the TA, are compressed using Bloom filters to reduce its size prior to broadcasting.

Papadimitratos et al. [13] propose to partition the CRL into small pieces and distribute each piece independently.

Haas et al. [16] develop a mechanism to reduce the length of the broadcast CRL by only sending a secret key per revoked vehicles. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to re-produce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. The probabilistic approach is one of promising technique for the key management in ad hoc networks [15], [16].

Zhu et al. introduce the GKMPAN protocol [17], which adopts a probabilistic key distribution approach based on pre-deployed symmetric keys.

within this period, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard [7] requires each vehicle to transmit beacons about its location, speed, and direction every 100 ~ 300 msec. Also, TACK requires the RAs to completely cover the networks; otherwise, the TACK techniques may not function properly. This requirement may not be feasible especially in the early deployment stages of VANETs. Although TACK will eliminate the CRL at vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current RL that is Revocation List by performing a check against all the entries in the RL. Each check requires three pairing operations.

In [10], Hubaux et al. identify the specific issues of security and privacy challenges in VANETs, and indicate that a Public Key Infrastructure-PKI should be well deployed to protect transited messages and to mutually authenticate entities of network.

Laberteaux et al. [14] use car to car communication to speed-up the CRL broadcastings.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Problem Definition

In the literature study we have presented different methods for efficient and effective authentication protocol for VANETs; however each method is suffered from different kinds of limitations. Recently we have studied the new approach presented for VANET authentication called EMAP. We have studied that the proposed EMAP was presented 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 (HMAC) in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs. In addition, EMAP is free from the false positive property which is common for lookup hash tables as it will be indicated in the next section. From the experimental analysis we observed that it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, EMAP significantly decreases the message loss ratio because message verification delay compared to the conventional privacy authentication methods employing CRL checking.

However this EMAP protocol is suffering from the limitations such as no anonymity, inefficient use of certificate authentication and message authentication mechanism. Thus we need to further address these issues along with EMAP protocol.

B. System Architecture

In this paper new EMAP method is presented called as CEMAP (Certificate based EMAP) which is intended to overcome the issues of certificate and message signature authentication acceleration. Along with EMAP we presenting the efficient method for certificate based Signature Scheme which can accelerate overall processing time of authentication protocol for VANET. In this for certificate based Signature Scheme which can accelerate overall processing time of authentication protocol for VANET. In this work method is presented to tackle the problem of anonymity, conditional privacy preservation, authentication, non-repudiation for OBUs in V2I communication. To the best of our knowledge, it is the first study that deals with these security requirements for OBUs in V2I communication. We introduce a novel anonymous authentication protocol in V2I communication. The protocol is based on a certificate-based signature scheme which combines the advantages of the signature based on traditional public key cryptosystem (no key escrow) and that based on ID-PKC (implicit authentication). A new certificate-based signature scheme and the verification result of the signature is a constant with respect to the signer's unique identifier and public key. Then, new CEMAP authentication protocol is constructed based on the combination of the new signature scheme and EMAP. The proposed protocols will claims anonymity, conditional privacy preservation, non-repudiation, and mutual authentication. A secure session key is established in the protocol which also achieves perfect forward secrecy.

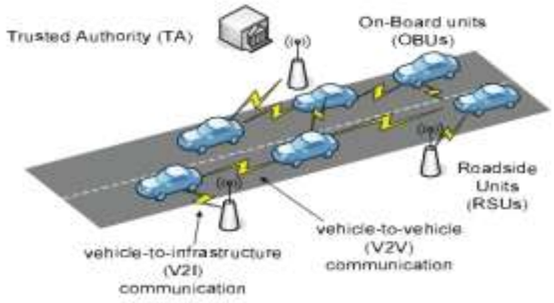
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Figure 1: VANET Architecture

In this project we are presenting efficient certificate based scheme as well as EMAP. Apart from this below are the main objectives of this project:

- To present literature review over the different methods of certificate based schemes as well as authentication protocol for VANETs.
- To present the design of new proposed method called CEMAP.
- To present the practical simulation of proposed algorithms and evaluate its performances.

To present the comparative analysis of existing and proposed algorithms in order to claim the efficiency of proposed method.

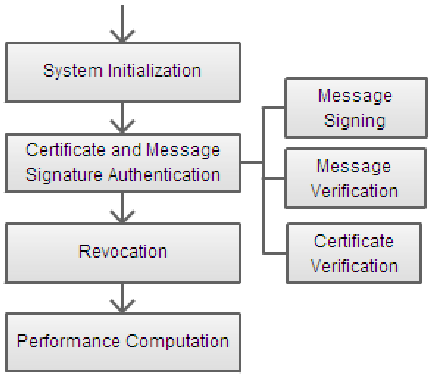

Figure 2: Proposed System Architecture

C. Mathematical Equations

I. Certificate Creation

Let ‘y’ be a random number of order Zq.
Where Zq is set of large random numbers.
We compute Secret Key and Public Key pair as follows:

1. Road Side Unit (RSU Key and Public Key computation

$SK_{RSU} = y$
$PK_{RSU} = y.P$
Where P is key sent by Ticket Authority (TA).

2. On Board Unit (OBU) Secret Key and Public Key computation

$SK = y$
$PK = y.P$

Then certificate creation using a Cryptographic Hash Function $H_1 :\{ 0, 1\}^* \rightarrow Zq^*$

RSU’s Certificate based on H1 is
$C_{RSU} = sH1 (ID_{RSU}, PK_{RSU)}$

OBU’s Certificate based on H1 is
$C_{OBU} = sH1 (ID_{OBU}, PK_{OBU})$

II. Authentication

The mutual authentication process of OBU and RSU is initiated by request from OBU.

i) OBU and RSU authenticate each other. When RSU receives service request message it firstly checks the validity of timestamp *T*. RSU rejects the request if *T* is invalid.

ii) OBU computes following things to Authenticate:

OBU randomly selects r1 є Zq and computes R = r1 P, $R` = r1PK_{RSU}$, and $M=H3 (ID_{OBU}) PK_{RSU}$

iii) OBU picks current time stamp T of login device and computes $h=H2 (T, ID_{OBU}, ID_{RSU}, R)$ and $\sigma= (SK_{OBU} + h)^{-1}$

iv) Otherwise, RSU computes Session Key, MAC (Message Authentication Code and sends it to OBU on OBU's request.)

v) On receiving the reply from RSU, OBU checks the integrity of MAC using agreed Session Key. If negative Terminates otherwise authenticates RSU for further communication.

Process:

A Trusted Authority (TA), which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. TA is responsible for initialise system.

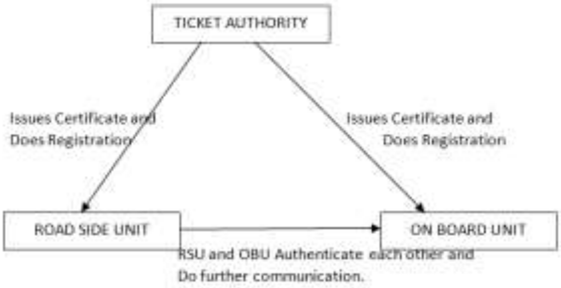
TICKET AUTHORITY
Issues Certificate and Does Registration
Issues Certificate and Does Registration
ROAD SIDE UNIT
ON BOARD UNIT
RSU and OBU Authenticate each other and Do further communication.

Figure3: Flow between Units

Algorithm:

1. Initialization

TA initializes Public and Private Keys for each OBU and RSU & generates MAC (Message Authentication Code)

2. Registration Process

RSU and OBU request registration and certificates from TA. Their public key, private key and certificates are generated. Creation of RSU's certificate happens only once.
Creation of OBU's certificate is frequent and based upon location of On Board Unit.

3. Authentication for establishing communication

3a) The On Board Unit sends a request for authentication with its certificate, timestamp.

3b) RSU checks certificate and timestamp if valid then create Session Key for that session.

3c) Communication between RSU and OBU is established.

Since we have a tendency to adopt a generic PKI system, the main points of the TA signature on a certificate associated an OBU signature on a message isn't mentioned during this paper for the sake of generality. We only focus in a way to accelerate the revocation checking method that is conventionally performed by checking the CRL for each received certificate. The message sign language and verification between different entities within the network.

IV. EXPERIMENTAL RESULT

Advantages of System

1. OBU Anonymity

OBU Anonymity means that except for the requesting OBU and the requested RSU, any outsider is unable to relate a particular protocol session with a particular OBU and relate two different sessions to the same OBU.

2. Conditional Privacy Preservation

As OBU Anonymity is satisfied, OBU's privacy can be protected in the protocol. And, if there is any dispute, RSU can trace OBU's identity by proving that OBU has sent the message which is signed by OBU's private key and certificate.

3. Mutual Authentication

RSU and OBU authenticate each other mutually and no other can interrupt as they check the timestamp and if invalid the session ends.

4. Secure Session Key Establishment

As the Session key is shared between RSU and OBU only it is difficult for attacker as only possible way is offline guessing of MAC and checking with that of RSU and it would take years to guess it.

Result of Work Done:

In the experimental, we have focused on authentication delay in milliseconds and numbers of messages send to RSU. The graph shows the time delay required for EMAP and CEMAP to pass the messages.

The following parameters are taken to carried out the experiment.

We have considered area of 10 Km by 10 km and the maximum OBU speed is 60 Km per hour, the OBU transmission range is 300m, protocol is MAC Protocol 802.11a, and the Wireless Channel Capacity is 2 Mbps.

This graph shows the Authentication delay in milliseconds for passing messages. Here we consider the number of messages coming to the RSU simultaneously from the OBU's and the authentication delay is considered. We consider messages starting from 10 and gradually increasing in the order of 10 and Authentication Delay in milliseconds in interval of 50 ms. It has been experimentally found that using CEMAP the delay has reduced by 10% than EMAP.

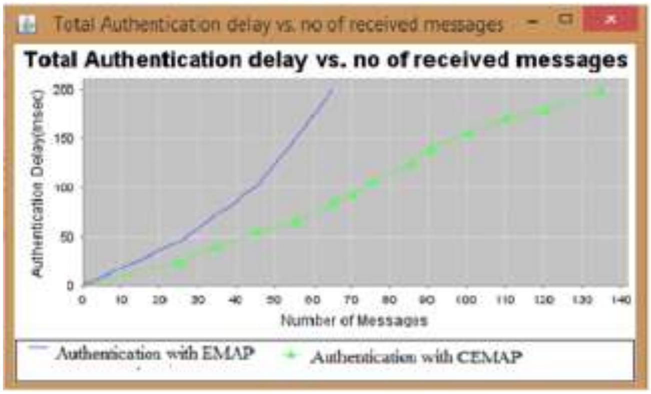

Figure 4. Graph for Authentication Delay

V. CONCLUSION AND FUTURE WORK

In this paper we have presented improved method to solve the problem of network security in VANETs. The new scheme is called as CEMAP which is inspired and based on existing EMAP scheme. The experimental results show that by implementing CEMAP the authentication delay has been reduced 10% by EMAP. Proposed system gives better results than EMAP. Future work can be to focus on reducing Authentication Delay in Vehicle to Vehicle Communication.

REFERENCES

[1] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks",IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.1 YEAR 2013.

[2] 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

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

[4] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, 2006.

[5] 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.

[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] J. P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, pp. 49–55, 2004.

[8] 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.

[9] L.Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. ACM conference on Computer and communications security*, pp. 41–47, 2002.

[10] M. Raya, and J.P. Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, no. 1, pp. 39-68, 2007. Back to cited text no.

[11] 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.

[12] [12] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 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] X. Lin, X. Sun, Pin-Han Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 56, no. 6, pp. 3442-56, 2007. Back to cited text no.

[15] "US bureau of transit statistics." [Online]. Available: http://en.wikipedia.org/wiki/Passenger vehicles in the United States.