PMAP: Precipitate Message Authentication Protocol for Vehicular Ad Hoc Networks

J.Sahana, PG Scholar
Department of Computer Science and Engineering
Sree Sowdambika College of Engineering
Aruppukottai, India
j.sahana3@gmail.com

S.Ganeshkumar Asst. Prof
Department of Information Technology
Sree Sowdambika College of Engineering
Aruppukottai, India
yrsk_ganeshkumar@yahoo.com

***Abstract*—. Vehicular Ad Hoc Networks (VANETs) admit the Public Key Infrastructure (PKI) and Certificate Revocation List (CRL) for their security. To check trusty action of VANETs and increase the amount of authentic information gained from the acknowledged messages. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. Precipitate Message Authentication Protocol for VANET (PMAP) employs a novel probabilistic key distribution, which authorizes non-revoked OBUs to definitely share and update a secret key. It can extensively drop off the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL.**

***Index Terms*- Vehicular systems, Communication defense, Message confirmation**

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have involved extensive attentions recently as a hopeful technology for uprising the transportation systems and providing broadband communication services to vehicles. VANET consists of entities with 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 permit OBUs to communicate with each other and with the infrastructure RSUs.

Vehicles communicate through wireless channels, a variety of harass such as inserting false information, altering and repeating the disseminated messages can be easily commenced. A security attack on VANETs can have rigorous harmful to valid users. 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 keeps a valid certificate, and every message should be digitally signed before its transmission. A CRL, typically issued by a Trusted Authority (TA), is a list containing all the revoked certificates.. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: 1) To protect the privacy of the drivers, i.e., to withhold 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 sometimes change its anonymous certificate to misinform invaders [4], [5], [6]. 2) The range of VANET is very huge. While the number of the OBUs is enormous and each OBU has a set of certificates, the CRL size will raise significantly if only a small part of the OBUs is revoked. According to the utilization of the mechanism for exploring a CRL, the Wireless Access in Vehicular Environments (WAVE) standard [9] does not state that either a non-optimized search algorithm, e.g., linear search, or some type of optimized search algorithm such as binary search, will be used for exploring a CRL. In this paper, we consider both non-optimized and optimized search algorithms. In proportion to the Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, each OBU has to transmit a message every 300 msec about its position, speed, and other telematic data.

II. RELATED WORKS

In [12], Hubaux recognize the specific issues of security and privacy challenges in VANETs, and designate that a PKI should be well arranged to defend the transited messages and to mutually authenticate network units. In [4], Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicles need 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 [13], Studer et al. propose a proficient 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. Upon incoming a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle drives a request signed by its group key to the RA to renew its certificates; the RA verifies the group signature of the vehicle and guarantees that the vehicle is not

DOI : 01.IJNC.2014.1.16

in the recent Revocation List (RL). After the RA authenticates the vehicle, it issues short-lifetime region-based certificate. This certificate is applicable 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 certificate to the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard [9] requires each vehicle to transmit beacons about its location, speed, and direction every 100-300 msec. Although TACK eliminates the CRL at the 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 by performing a check against all the entries in the RL. Each check requires three paring operations. Consequently, checking the revocation status of a vehicle may be a time-consuming process. The authors suggested using an optimized search method to remedy the computationally expensive RL check. The proposed method can reduce the RL checking to two paring operations.

In [14], 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. Papadimitratos et al. [15] propose to partition the CRL into small pieces and distribute each piece independently. Laberteaux et al. [16] use car to car communication to speed up the CRL Broadcasting. Haas et al. [8] develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to reproduce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which is used to check the revocation status of other entities, still suffers from the expected large size exactly as that in the traditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL. Also, the authors propose using bloom filter, which is some kind of lookup hash tables, to perform CRL checking for the received certificates. To minimize the false-positives in the bloom filter, the authors proposed that each vehicle has to check before sending its certificate whether this certificate will trigger a false positive or no. If yes, then it uses another certificate. The authors proposed to upload each vehicle with additional certificates to compensate for those ones which will trigger a false positive. Although this solution can minimize the false positives, it cannot to completely prevent them, which limits their advantages, especially, in safety-related VANETs applications.

III. Precipitate Message Authentication Protocol

The proposed PMAP employs a fast HMAC function and novel key sharing scheme utilizing probabilistic random key distribution.

A. *System Model*

The system model consists of,

i. A Trusted Authority, which is dependable for given that unsigned certificates and allocating furtive keys to all OBUs in the network.

ii. Roadside units (RSUs), which are fastened units distributed all over the network. The RSUs can converse safely with the TA.

iii. OBUs, which are entrenched in vehicles. OBUs can converse either with other OBUs through V2V communications or with RSUs through V2I communications.

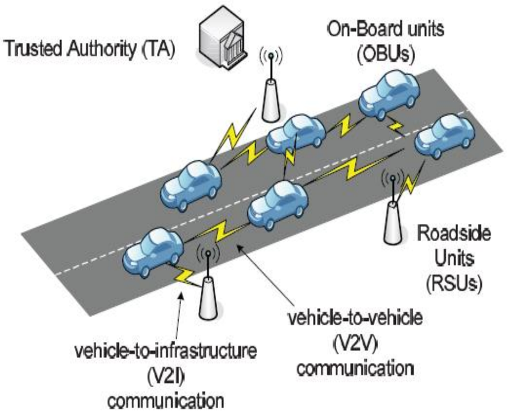
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Fig. The System Model

According to the WAVE standard [9], each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to accumulate the safety materials, e.g., secret keys, certificates, etc., of the OBU.

a. *System Initialization*

The TA initializes the system by executing Algorithm PK_{iu} denotes the ith public key for OBUu, where the corresponding secret key is SK_{iu}; PID_{iu} denotes the ith pseudoidentity (PID) for OBUu, where the TA is the only entity that can relate PIDiu to the real identity of OBUu; sigTA(PID_{iu} || PKiu) denotes the TA signature on the concatenation (||) of PID_{iu} and PK_{iu}; and C is the number of certificates loaded in each OBU.

DOI : 01.IJNC.2014.1.16

System Initialization

```
    Select two generators $P,Q Є G_1$ of order q,
    for i←1, l do
        Select a random number $k_i Є Z^*_q$
        Set the secret key $K_i^- = k_iQ Є G_1$
        Set the corresponding public key $K_i^+ = P Є G_1$ end for
    Select an initial secret key $K_g Є G_2$
      ▷ to be shared between all the non-revoked OBUs
    Select an master secret key $s Є Z^*_q$
    Set the corresponding public key $P_o = {}_sP$
    Choose hash functions
            $H : \{0,1\}^* \rightarrow G_1$ and $h: \{0,1\}^* \rightarrow Z^*_q$
    Select a secret value $υ Є Z^*_q$ and set $υ_o = υ$
    for i←1, j do
         ▷ to obtain a set V of hash chain values
        Set $υ_i = h(υ_{i-1})$
end for
for all $OBU_u$ in the network, TA do
    for i←1, m do
        Select a random number a Є [1,l]
        Upload the secret key $K_a^- = k_aQ$ and the Corresponding public key $K_a^+ = P$ in $HSM_u$
    end for
    Generate a set o unidentified certificates
    $CERT_u = \{cert^i_u (PID^i_u, PK^i_u, sigTA (PID^i_u || PK^i_u)) | 1 \le i \le C\}$
      ▷ for privacy-preserving authentication
    Upload $CERT_u$ in $HSM_u$ of $OBU_u$
end for
Announce H, h, P, Q, and $P_o$ to all the OBUs
```

b. Message authentication

If an OBU want to communicate with other OBU means it sends an encrypted message with a HMAC code using HMAC algorithm. It generates by using the sender id and common secret key which knows all the unrevoked OBUs. The receiver OBU also generates the HMAC code by using common secret key. The message signing and verification between different entities in the network are executed as follows:

1. Message Signing

Before any OBUu transmits a message M, it analyzes its revocation check REV_{check} as REV_{check} as $REV_{check} = HMAC(K_g,PID_U \| T_{stamp})^2$, where T_{stamp} is the present time stamp, and $HMAC(K_g,PID_U \| T_{stamp})$ is the hash message verification code on the concatenation of PID_u and T_{stamp} using the secret key K_g. Then, OBU_u transmits,

$$(M \| T_{stamp} \| cert_u(PID_u,PK_u,sigr_A(PID_u \| PK_u)) \| sig_u(M \| T_{stamp}) \| REV_{check})$$

Where, $sig_u(M \| T_{stamp})$ is the signature of OBU_u on the concatenation of the message M and T_{stamp}.

2. Message Verification

Any OBU_y receiving the $(M \| T_{stamp} \| cert_u(PID_u,PK_u,sigr_A(PID_u \| PK_u)) \| sig_u(M \| T_{stamp}) \| REV_{check})$ can verify it.

OBU_y calculates HMAC $(K_g,PID_u \| T_{stamp})$ using its K_g on the concatenation $PID_u \| T_{stamp}$, and compares the calculated HMAC $(K_g,PID_u \| T_{stamp})$ with the received REV_{check}.

a) Revocation

The revocation is triggered by the TA when there is an OBU_u to be revoked. The certificates of OBU_u must be revoked. In addition, the secret key set RS_u of OBUu and the current secret key Kg are considered revoked. Hence, a new secret key $K^{\sim}_g$ should be securely distributed to all the nonrevoked OBUs. Also, each nonrevoked OBU should securely update the compromised keys in its key sets RS and RP [19].

Processing revocation messages

Require: $Rev_{msg} = (CRL \| K_{msg} \| sig_{TA}(CRL \| K_{msg}))$ and P_o

- Verify the signature.
- If it is valid,run the next algorithm.

Obtaining new secret key and $υ_{j\text{-}ver}$

```
if $K^-_M$ exists in $RS_y$ then
    Set the new secret key $\tilde{Kg} = ê(K^-_M,K_{im})$
    Decrypt $enc_{K\sim g}(υ_{j-ver})$ using $K^{\sim}_g$ to get $υ_{j-ver}$
    else
    Broadcast a signed request and $cert_y(PID_y,PK_y, sigTA(PID_y \| PK_y))$ to get $K^{\sim}_g$ from neighboring OBUs
    Start a timer $T_1$
    Any neighboring OBU of $OBU_y$ having $K^{\sim}_g$ verifies the signature
        And certificate of $OBU_y$, ensures that $cert_y$ is not in the recent CRL, Uses the public key $(PK_y)$ of $OBU_y$ included in $cert_y$ to encrypt $K^{\sim}_g$, and sends the encrypted $K^{\sim}_g$ to $OBU_y$
    If the encrypted $K^{\sim}_g$ is received then
        Decrypt $K^{\sim}_g$ using the secret key corresponding to $PK_y$
```

DOI : 01.IJNC.2014.1.16

```
        Decrypt enc $_{K\sim g}(\upsilon_{j\text{-}ver})$ using $K^{\sim}_{g}$ to get $\upsilon_{j\text{-}ver}$
        else
                if $T_1$ is timed out then
                Go to 5
                end if
        end if
    end if
```

Updating the key sets of OBU$_y$

```
Require: $K^{\sim}_{g}$ and $\upsilon_{j\text{-}ver}$
If not previously missing any revocation message then
If possesses compromised secret keys $\{K^{-}_{i}\} = \{K_iQ\}$ in $ID_{revkey}$ then
Update the secret key $K^{-}_{i}$ as $\tilde{K}_i^{-} = \upsilon_{j\text{-}ver} K^{-}_{i} = \upsilon_{j\text{-}ver}k_iQ$
Update the corresponding public keys $\tilde{K}_i^{+} = \frac{1}{\upsilon j-ver}$   $\tilde{K}_i^{+} = \frac{1}{\upsilon j-verki} P$
else
Exit
end if
else
Set n= ver
while n ≠ $\upsilon_{verlast}$ do
Set $\upsilon_{j\text{-}n+1} = h(\upsilon_{j\text{-}n})$
Set n = ver + 1
end while
Broadcast a signed request to the neighboring OBUs
Requesting ver$|_{missed}$ and IDrev$_{key}|_{missed}$ for all the missed Revocation processes
for each received signed value of ver$|_{missed}$ do
Verify the signature and certificate of the sender and, ensures that the certificate of the sender is not in the recent CRL
Find the value of $\upsilon_{j\text{-}ver}|_{missed}$ from $\{\upsilon_{j\text{-}ver+1}, \upsilon_{j\text{-}ver+2},.., \upsilon_{j\text{-}verlast+1}\}$
for each possessed key $K^{-}_{i} = k_iQ$ Є IDrev$_{key}|_{missed}$
do
Update the secret key $K^{-}_{i}$ as $\tilde{K}_i^{-} = \upsilon_{j\text{-}ver|missed}\ k_iQ$
end for
end for
end if
```

IV. PERFORMANCE EVALUATION

A. Computation difficulty of Revocation type Checking

The computation difficulty of the revocation type checking method which is classified as the number of contrast operations required to confirm the revocation type of an OBU. Let N_{rev} denote the total number of revoked certificates in a CRL. To confirm the revocation type of an OBU$_u$ using the linear search algorithm, the unit has to evaluate the certificate identity of OBU$_u$ with each certificate of the N_{rev} certificates in the CRL. So, the computation complexity of PMAP is O(1), which is stable and independent of the number of revoked certificates. Other words, PMAP has the lowest computation complexity compared with the CRL checking processes utilizing linear and binary search algorithms.

B. Authentication delay

To evaluate the message authentication delay employing the CRL with that utilizing PMAP to verify the revocation type of an OBU. As earlier, the authentication of any message is executed by three consecutive phases: verifying the sender's revocation type, checking the sender's certificate, and checking the sender's signature.

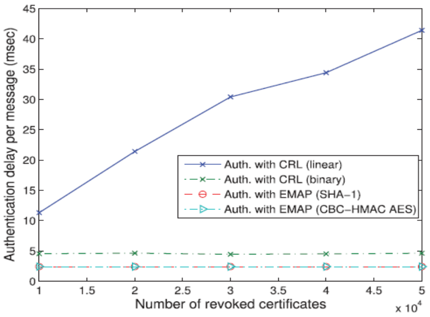

Fig.2. Authentication delay

Fig.2. shows that a comparison between the authentication delay per message using PMAP, linear CRL verifying process, and binary CRL verifying process versus the number of the revoked certificates, where the number of the invalidated certificates is a sign of the CRL size. It can be seen that the authentication delay using the linear CRL verifying process raises with the number of revoked certificates. The range of the number of the comparison operations is very small; the authentication delay is almost stable. The authentication delay using PMAP is stable and independent of the number of revoked certificates.

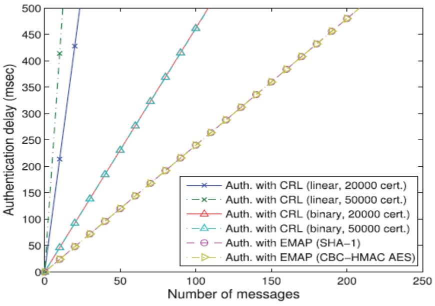

Fig.3. Total no of authentication delay vs. the no of received messages

DOI : 01.IJNC.2014.1.16

C. End-to-End Delay

To further assess PMAP, Fig. 4 shows the end-to-end delay in msec versus the OBUs density, by utilizing authentication using the advised PMAP (SHA-1), the linear CRL checking, and binary CRL checking. The end-to-end delay leans to be stable for high OBUs densities as the number of accepted packets reaches the maximum number of packets an OBU can confirm within a specific period. The end-to-end delay also raises with the number of revoked certificates embraced in the CRL for the linear CRL checking process.It is almost constant with the CRL size using the binary searching process as the number of comparison operations needed to check CRLs.

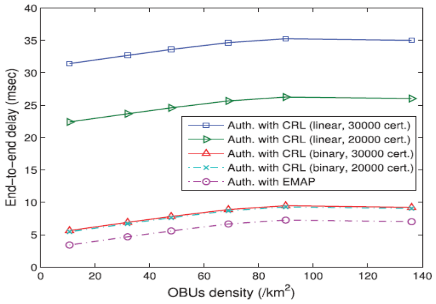

Fig.4. End-to-end delay versus OBUs density.

D. Communication Cost of Updating the Secret Key (K_g)

The communication cost of updating the secret key (K_g), which is the average number of messages an OBU has to transmit and receive after triggering the revocation process to get the new secret key ($\tilde{K}g$) and distribute $\tilde{K}g$ to its unrevoked neighboring OBUs. PMAP incurs 0.03 percent increase in the communication overhead compared to the WAVE standard, which is acceptable with respect to the gained benefits from PMAP.

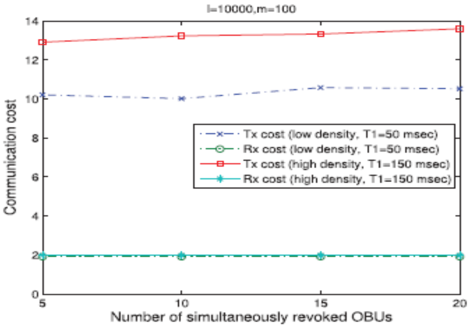

Fig.6. Communication cost of updating Kg in PMAP

V. Conclusion

The principle of VANETs is to make sure the road safety and applications to give comfort for vehicle drivers. The vehicles act as communication nodes to exchange data between OBUs. In this paper, we proposed the TA which gives anonymous certificates and distributing secret keys to all OBUs in the network. PMAP largely can reduce the message loss ratio due to message verification delay. My future work will focus on the revocation process 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] 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 of Transit Statistics, 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 Int’l Workshop VehiculAr Inter NETworking, 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.

[10] “5.9 GHz DSRC,” http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2012.

[11] A. Wasef and X. Shen, “MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE GlobeCom, 2009.

[12] J.P. Hubaux, “The Security and Privacy of Smart Vehicles,” IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

DOI : 01.IJNC.2014.1.16