PERFORMANCE ANALYSIS OF AN EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VANETS

R. Priya[1], Dr. C. Kumar Charlie Paul[2]
Department of Computer Science, Anna University Chennai.
A.S.L Paul's College of Engineering & Technology, Coimbatore.

Abstract: **Vehicularad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. The VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). The two basic communication modes are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) that allow OBUs to communicate with each other and with the infrastructure RSUs. For Security the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) are adopted by VANETs. The authentication of a received message is performed by checking if the certificate of the sender is included in the current and verification of the authenticity of the certificate and signature of the senderCRL is performed in any PKI system. 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 is proposed in this paper. EMAP employs HMAC in the revocation checking process in which the key used in calculating the HMAC for each message is shared only between unrevoked OBUs. Also, EMAP is free from the falsepositive property which is common for lookup hash tables. EMAP is demonstrated to be secure and efficient by conducting security analysis and performance evaluation.**

I. INTRODUCTION

Vehicular ad hoc networks (VANET) have recently drawn the attention of the research community .They represent arapidlyemerging, particularly challenging class of MANETs. Vehicular applications will provide warnings on traffic and road conditions, environmental hazards, and local information .Vehicular communications (VC) aim to enhance safety and efficiency of transportation systems. Vehicular networks emerge as one of the most convinces and yet most challenging instantiations of the mobile ad hoc networking technology among civilian communication systemsas described in [2].

Privacy is an important issue in VANETs as the wireless communication channel is a shared medium. Exchanging messages without any security shield over the air caneasily leak the information that users may want to keep confidential. Pseudonym based schemes [3]–[5] have been proposed to preserve the locality privacy of vehicles. Nevertheless, those schemes need the vehicles to store a large number of pseudonyms and certification. And also they do not sustain some important secure functionality such as authentication and integrity.

To the best of our knowledge, all of the existing group signature schemes in VANETs [7]–[9] are based oncentralized key management which preloads keys to vehicles off-line. The disadvantages of the centralized key management are that:the system maintenance is not flexibleand that many existing schemes assume a tamper-proof device [1] being installed in each vehicle. This tamper-proof devicenormally costs several thousand dollars as in [9] that uses IBM 4764card. The framework to be developed in this paper does not require the exclusive tamper-proof device.

According to the Dedicated Short Range Communication (DSRC) [10] that is part of the WAVE standard every OBU has to broadcast a message every 300 msec about its information. In this case, each OBU may receive a large number of messages every 300 msec. And also it has to check the currentCRL for all the received certificates that may acquire longauthentication delay depending on the CRL size and the number of received certificates. It is an inevitable challenge for VANETs ability to check a CRLfor a large number of certificates in a timely manner.

Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate.Each OBU should be able to check the revocation status of all the received certificates in a timely manner in order to ensure reliable operation of VANETs and increase theamount of authentic information gained from the received messages.An expedite message authentication protocol 1 (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function is introduced here. EMAP is suitable not only for VANETs but also for any network employing a PKI system. This is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

II. RELATED WORK

The primary security requirements are identified as entity authentication, privacy preservation, message integrity and non-repudiation in VANETs. The PKI is the most viable technique to achieve these security requirements [4],[12]. It employs CRLs to efficiently manage the revoked certificates. The delay of checking the revocation status of a certificate included in a received message is expected to be long because of the CRL size is being very large.

Studer et al. proposed an efficient authentication and revocation scheme called TACK in [13]. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. A group signature where the trusted authority acts as the group manager and the vehicles act as the group members is adopted by the authors. Upon entering a newregion every vehicle must update its certificate from the RAdedicated for that region. A requestsigned by its group key is sent by the vehicle to the RA to update its certificate. This is when the RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL). Next, it issues short- lifetime region-based certificate. The certificate is valid only within the coverage range of the RA. TACK requires the RAs to wait for some time, at least2 seconds, before sending the new certificate to therequesting vehicle. Hence the vehicle will not be able to send messages to neighboring vehicles within this period making TACK not suitable for the safety applications. InVANETs, as the WAVE standard [9] requires each vehicle to transmit beacons about its location, direction, and speed. TACK requires the RAs to completely cover the network or else the TACK technique may not function properly. Although TACK eliminates the CRL at the vehicles level it needs the RAs to verify the revocation status of the vehicles upon requesting new certificates. The RA has to verify that this vehicle is not in the current attached to every certificate request thatreduces the privacy preservation of TACK and rendersthe tracking of a vehicle possible.

III. PROPOSED SYSTEM

An Expedite Message Authentication Protocol (EMAP) for VANETs that replaces the time-consuming CRL checking process by an efficient revocation checking process. Revocation check process in EMAP uses a keyed Hash Message Authentication Code HMAC in which the key used in calculating the HMAC is shared only between non-revoked On-Board Units (OBUs). Also, EMAP uses a novel probabilistic key distribution that enables non revoked OBUs to securely share and update a secret key. With the conventional authentication methods employing CRL. EMAP is demonstrated to be secure and efficient by conducting security analysis and performance evaluation.

The proposed method can reduce the RL checking to two pairing operations. Though, this solution is based on fixing some parameters in the group signature attached to every certificate request that reduces the privacy preservation of TACK and renders the tracking of a vehicle possible.

Design Implementation

A fast HMAC function is used by the proposed EMAP protocol. Also a novelkey sharing scheme employing probabilistic random keydistribution is used here too. The assumptions for the system model design contain A Trusted Authority,Roadside units and OBUs as described below:

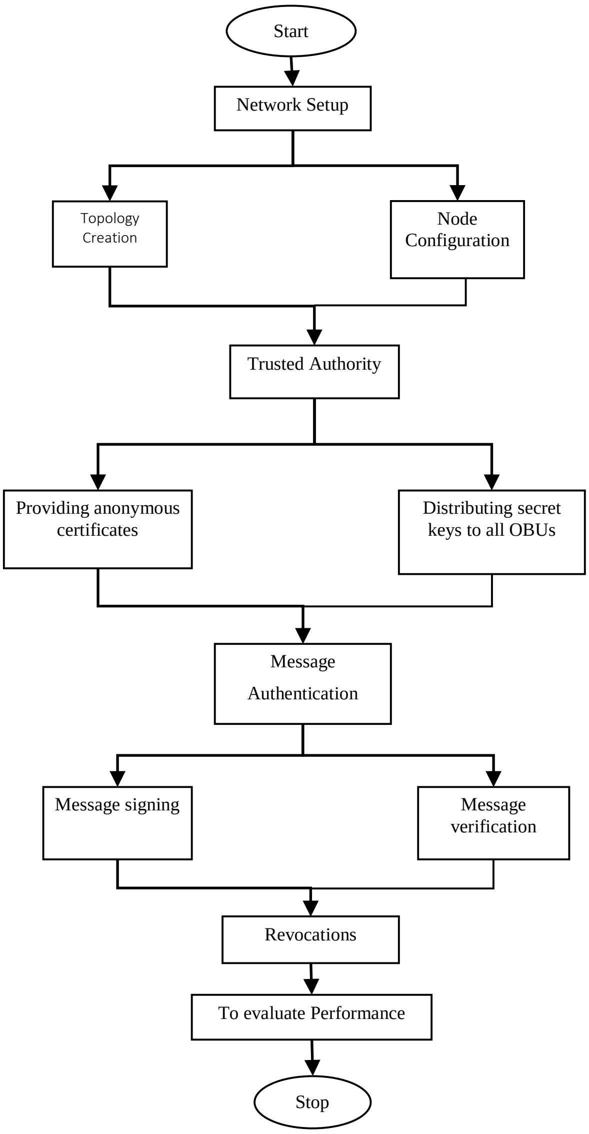


Figure 1. Working Flow

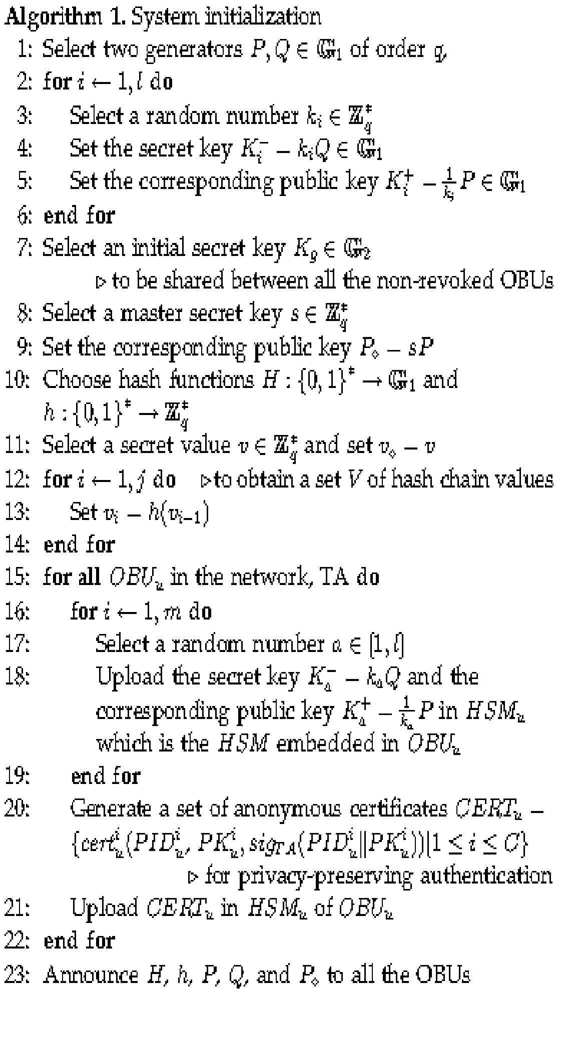
- A Trusted Authority: it is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.
- Roadside units (RSUs): these are fixed units distributed all over the network that can communicate securely with the TA.
- OBUs: these are embedded in vehicles and can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

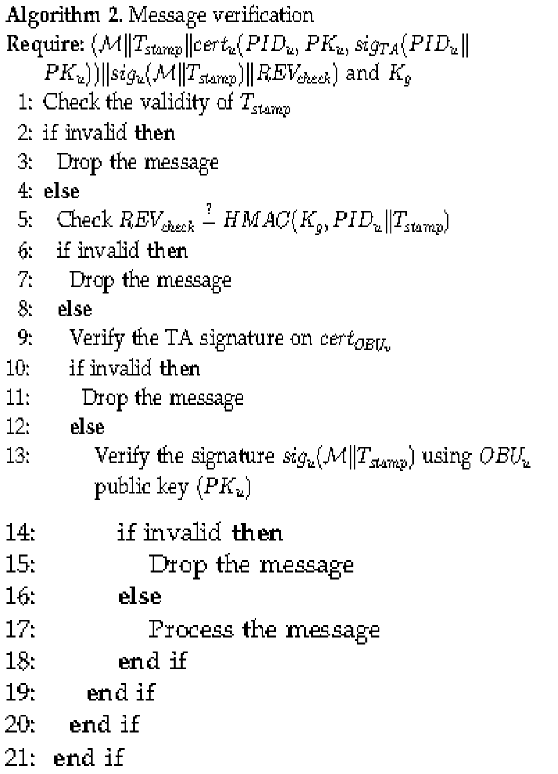
According to the WAVE standard [9] every OBU isequipped with a Hardware Security Module (HSM thatis a tamper-resistant module used to store the securitymaterialsof the OBU.The HSM in each OBU is responsible for performingall the cryptographic operations. We consider thatlegitimate OBUs cannot collude with the revoked OBUs asit is difficult for legitimate OBUs to extract their securitymaterials from their HSMs. Lastly we consider that acompromised OBU is instantly detected by the TA.

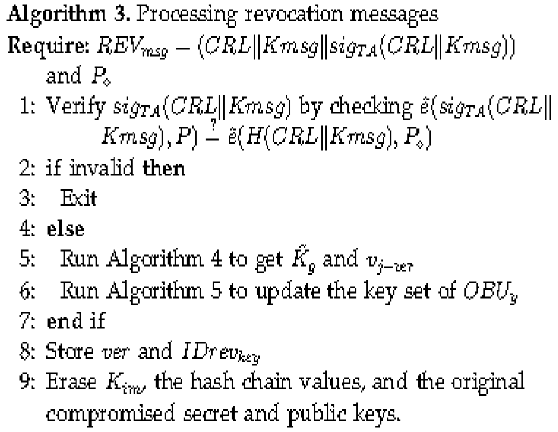
EMAP System Model Creation

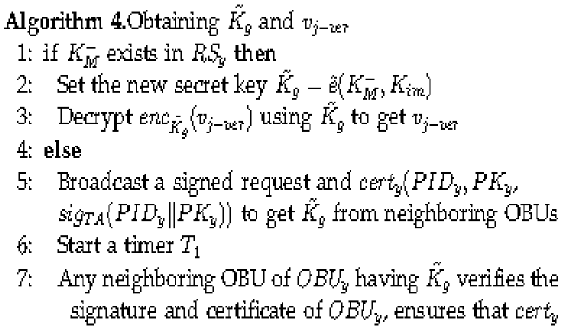
A Trusted Authority responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. The Roadside units (RSUs) that are fixed units are distributed all over the network. RSUs can communicate securely with the TA and OBUs are embedded in vehicles. All the OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

The algorithms that are implemented in the EMAP protocol have been described below.

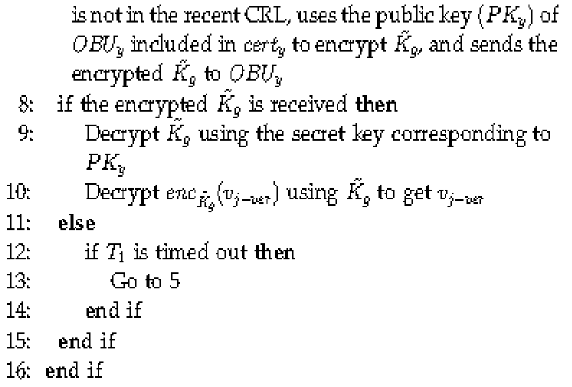

```
Algorithm 1. System initialization
Select two generators $P, Q \in \mathbb{G}_1$ of order $q$,
for $i \leftarrow 1, l$ do
    Select a random number $k_i \in \mathbb{Z}_q^*$
    Set the secret key $K_i^- - k_i Q \in \mathbb{G}_1$
    Set the corresponding public key $K_i^+ - \frac{1}{k_i} P \in \mathbb{G}_1$
end for
Select an initial secret key $K_g \in \mathbb{G}_2$
            ▷ to be shared between all the non-revoked OBUs
Select a master secret key $s \in \mathbb{Z}_q^*$
Set the corresponding public key $P_\diamond - sP$
Choose hash functions $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and
$h : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
Select a secret value $v \in \mathbb{Z}_q^*$ and set $v_\diamond - v$
for $i \leftarrow 1, j$ do    ▷to obtain a set $V$ of hash chain values
    Set $v_i - h(v_{i-1})$
end for
for all $OBU_u$ in the network, TA do
    for $i \leftarrow 1, m$ do
        Select a random number $a \in [1, l]$
        Upload the secret key $K_a^- - k_a Q$ and the
        corresponding public key $K_a^+ - \frac{1}{k_a} P$ in $HSM_u$
        which is the $HSM$ embedded in $OBU_u$
    end for
    Generate a set of anonymous certificates $CERT_u -$
    $\{cert_u^i(PID_u^i, PK_u^i, sig_{TA}(PID_u^i \| PK_u^i)) | 1 \leq i \leq C\}$
                    ▷ for privacy-preserving authentication
    Upload $CERT_u$ in $HSM_u$ of $OBU_u$
end for
Announce $H$, $h$, $P$, $Q$, and $P_\diamond$ to all the OBUs
```


```
Algorithm 2. Message verification
Require: $(\mathcal{M} \| T_{stamp} \| cert_u(PID_u, PK_u, sig_{TA}(PID_u \|$
    $PK_u)) \| sig_u(\mathcal{M} \| T_{stamp}) \| REV_{check})$ and $K_g$
Check the validity of $T_{stamp}$
if invalid then
  Drop the message
else
  Check $REV_{check} \overset{?}{=} HMAC(K_g, PID_u \| T_{stamp})$
  if invalid then
    Drop the message
  else
    Verify the TA signature on $cert_{OBU_v}$
    if invalid then
      Drop the message
    else
      Verify the signature $sig_u(\mathcal{M} \| T_{stamp})$ using $OBU_u$
      public key $(PK_u)$
      if invalid then
        Drop the message
      else
        Process the message
      end if
    end if
  end if
end if
```


```
Algorithm 3. Processing revocation messages
Require: $REV_{msg} - (CRL \| Kmsg \| sig_{TA}(CRL \| Kmsg))$
    and $P_\diamond$
Verify $sig_{TA}(CRL \| Kmsg)$ by checking $\hat{e}(sig_{TA}(CRL \|$
        $Kmsg), P) \overset{?}{=} \hat{e}(H(CRL \| Kmsg), P_\diamond)$
if invalid then
  Exit
else
  Run Algorithm 4 to get $\tilde{K}_g$ and $v_{j-ver}$
  Run Algorithm 5 to update the key set of $OBU_y$
end if
Store $ver$ and $IDrev_{key}$
Erase $K_{im}$, the hash chain values, and the original
compromised secret and public keys.
```


```
Algorithm 4.Obtaining $\tilde{K}_g$ and $v_{j-ver}$
if $K_M^-$ exists in $RS_y$ then
  Set the new secret key $\tilde{K}_g - \hat{e}(K_M^-, K_{im})$
  Decrypt $enc_{\tilde{K}_g}(v_{j-ver})$ using $\tilde{K}_g$ to get $v_{j-ver}$
else
  Broadcast a signed request and $cert_y(PID_y, PK_y,$
  $sig_{TA}(PID_y \| PK_y))$ to get $\tilde{K}_g$ from neighboring OBUs
  Start a timer $T_1$
  Any neighboring OBU of $OBU_y$ having $\tilde{K}_g$ verifies the
    signature and certificate of $OBU_y$, ensures that $cert_y$
```

Each of these algorithms is performed one after another as the order is described doing specific functions at every stage. The entire EMAP working can be divided in to three main processes.



```
       is not in the recent CRL, uses the public key ($PK_y$) of
       $OBU_y$ included in $cert_y$ to encrypt $\tilde{K}_g$, and sends the
       encrypted $\tilde{K}_g$ to $OBU_y$
 8:  if the encrypted $\tilde{K}_g$ is received then
 9:     Decrypt $\tilde{K}_g$ using the secret key corresponding to
        $PK_y$
10:     Decrypt $enc_{\tilde{K}_g}(v_{j-ver})$ using $\tilde{K}_g$ to get $v_{j-ver}$
11:  else
12:     if $T_1$ is timed out then
13:        Go to 5
14:     end if
15:  end if
16: end if
```

- System Initialization
- Message Authentication
- Revocation

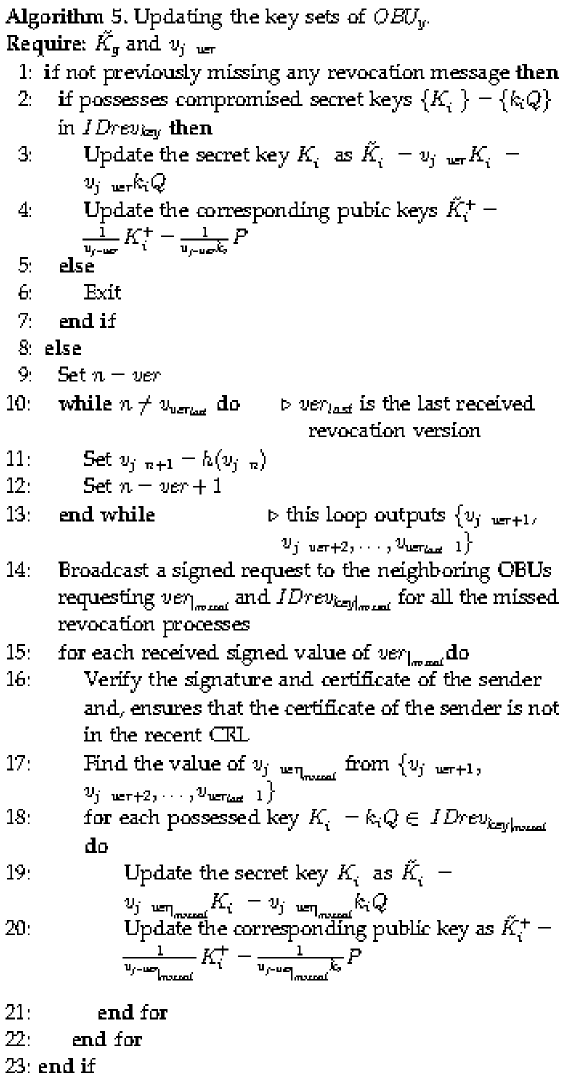
System Initialization
The system model under consideration ismainly a PKI system in which each OBUu has a set ofanonymous certificates (CERTu) used to secure its communicationswith other entities in the network. In specificPKu, included in the certificate certu and thesecret key SKu are used for verifying and signing messages. Each OBUu is preloaded with a set ofasymmetric keys (secret keys in RSu and thecorresponding public keys in RPu). The keys arenecessary for generating and maintaining a shared secretkey Kg between unrevoked OBUs. Here Algorithm 1 is used for system initialization.

Message Authentication:
The details of the TA signature on a certificate and an OBU signature on a message are not discussed in this paper for the sake of generality since we adopt a generic PKI system. We only focus in how to accelerate the revocation checking process that is conventionally performed by checking the CRL for every received certificate. Then the message signing and verification between different entities in the network are performed.

Authentication is performed by the two following steps:

- Message signing
- Message Verification

Revocation
An important feature of the proposed EMAP is that it enables an OBU to update its compromised keys corresponding to previously missed revocation processes provided that it picks one revocation process in the future. A rekeying mechanism capable of updating compromised keys corresponding to rekeying processes previously missed is introduced. Revocation process consists of 3 algorithms implemented in EMAP system model after authentication is achieved.



```
Algorithm 5. Updating the key sets of $OBU_y$.
Require: $\tilde{K}_g$ and $v_{j\ ver}$
 1: if not previously missing any revocation message then
 2:    if possesses compromised secret keys $\{K_i\} - \{k_iQ\}$
       in $IDrev_{key}$ then
 3:       Update the secret key $K_i$ as $\tilde{K}_i - v_{j\ ver}K_i -$
          $v_{j\ ver}k_iQ$
 4:       Update the corresponding pubic keys $\tilde{K}_i^+ -$
          $\frac{1}{v_{j-ver}}K_i^+ - \frac{1}{v_{j-ver}k_i}P$
 5:    else
 6:       Exit
 7:    end if
 8: else
 9:    Set $n - ver$
10:    while $n \neq v_{ver_{last}}$ do      ▷ $ver_{last}$ is the last received
                                           revocation version
11:       Set $v_{j\ n+1} - h(v_{j\ n})$
12:       Set $n - ver + 1$
13:    end while                    ▷ this loop outputs $\{v_{j\ ver+1},$
                                    $v_{j\ ver+2}, \dots, v_{ver_{last}\ 1}\}$
14:    Broadcast a signed request to the neighboring OBUs
       requesting $ver|_{missed}$ and $IDrev_{key|missed}$ for all the missed
       revocation processes
15:    for each received signed value of $ver|_{missed}$do
16:       Verify the signature and certificate of the sender
          and, ensures that the certificate of the sender is not
          in the recent CRL
17:       Find the value of $v_{j\ ver|_{missed}}$ from $\{v_{j\ ver+1},$
          $v_{j\ ver+2}, \dots, v_{ver_{last}\ 1}\}$
18:       for each possessed key $K_i - k_iQ \in IDrev_{key|missed}$
          do
19:          Update the secret key $K_i$ as $\tilde{K}_i -$
             $v_{j\ ver|_{missed}}K_i - v_{j\ ver|_{missed}}k_iQ$
20:          Update the corresponding public key as $\tilde{K}_i^+ -$
             $\frac{1}{v_{j-ver|_{missed}}}K_i^+ - \frac{1}{v_{j-ver|_{missed}}k_i}P$
21:       end for
22:    end for
23: end if
```

IV. SIMULATION AND ANALYSIS

The Network Simulator ns-2.28 is used to analyse the system. The NS2 is a discrete event time driven simulator which is used to analyse the performance of a network. The following parameters give the efficiency of the proposed system.

Packet Receive Ratio
The packet receive ratio is one of the Quality of Service (QoS) metric to evaluate the performance of network.

Low packet receive ratio depletes the network performance.Figure.2 shows that the proposed system has a good packet receive ratio.

Packet Loss Ratio
The Packet Loss ratio is the maximum number of packets possible to be dropped by a node. Figure 3 shows that the packet loss is minimized for the proposed scheme.

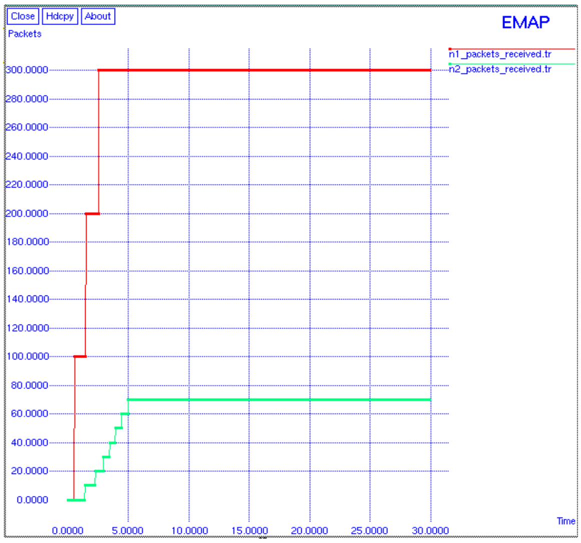


Figure 2. Packet Receive Ratio

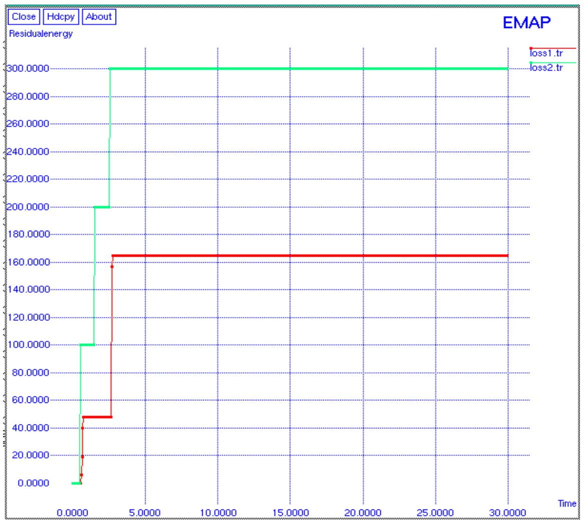


Figure 3. Packet Loss Ratio

Packet Delay:

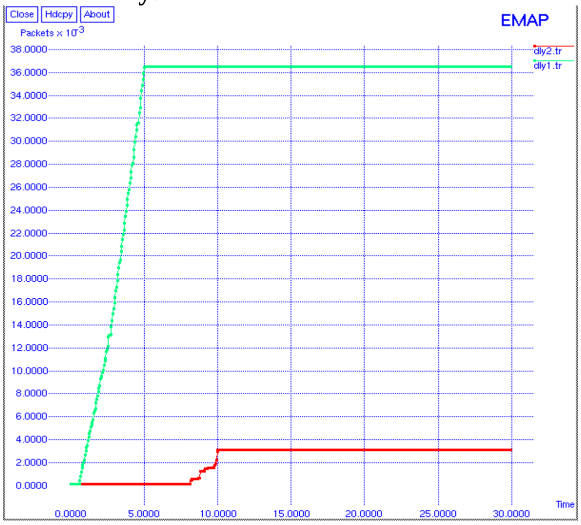


Figure 4. Packet Delay

Packet Delay is the delay occurred during data transmission and it is given in figure 4.

Performance evaluation

During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like packet received, Packets lost, and delay etc. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms. All the graphs obtained can be used to conclude that EMAP is efficient for the VANET operations.

- Packet Receive Ratio is high
- Packet loss is low
- Delay is minimal

V. CONCLUSION

We have analysed EMAP for VANETs that expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. A novel key sharing mechanism allows an OBU to update its compromised keys even if it previously missed some revocation message s. Also EMAP has a modular feature rendering it integral with any PKI system. Moreover, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. This means that EMAP can appreciably decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

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 PrivacyPreservation 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 Internetworking, 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] A. Wasef and X. Shen, “MAAC: Message Authentication AccelerationProtocol for Vehicular Ad Hoc Networks,” Proc. IEEEGlobeCom, 2009.

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

[12] A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing TogetherEfficient Authentication, Revocation, and Privacy in VANETs,”Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. AndNetworks (SECON ’09), pp. 1-9, 2009.