Intrusion prevention and Message Authentication Protocol (IMAP) using Region Based Certificate Revocation List Method in Vehicular Ad hoc Networks

G. Anitha [#1], Dr. M. Hemalatha [*2]

[1]Research and Development Centre, Bharathiar University, Coimbatore, India
[1]florenceanitha7@gmail.com
[2]Department of Computer Science, Karpagam University, Coimbatore,India
[2] hema.bioinf@gmail.com

Abstract— Vehicular Ad-hoc network uses some advanced Public Key Infrastructure and digital signature method for security. But, intrusion detection and avoidance is an inevitable challenge in networks. Authentication is performed in any PKI (Public Key Infrastructure) system by checking if the certificate of the sender is included in the CRL (Certificate Revocation List) and verifying the authenticity and checking the sign of the sender. This study focuses on efficient certificate revocation list management by region based certificate revocation list distribution protocol. Instead of storing all invalid vehicle identity in a single CRL, each region maintains a separate CRL which contains the invalid vehicle's identity in the region. This CRL checking process has been done using by Hash function technique, i.e., Bloom Filter which avoids false negative. It replaces the time-consuming CRL Checking process. This protocol can reduce message loss ratio by using fast revocation checking and the CRL updating method as well as it needs very less memory space compared to other methods.

Keyword- VANET, Network Security, Wireless Security, Authentication Protocol, IMAP, Certificate Revocation List.

I. INTRODUCTION

Recently, Vehicular ad-hoc networks is an essential and promising technology for developing a road traffic system and safety applications such as incident warning, collision detection, collision avoidance, etc. It is providing broadband communication services to vehicles. VANET consists of two main entities which are On-Board Units and Road-Side Units. On-board Unit is attached in all the vehicles. The road-side unit is fixed in road side based on the uniform interval distances. There are two types of communications to provide and share information: one is Vehicle to Vehicle (V2V) communications, the other one is Vehicle to Infrastructure (Road Side Unit) communications.

At the time of communication, a variety of security attacks such as network attack (Ex: Sybil attack), application attack (Ex: Message suppress, Message fabricate, Message replay, Message alter) can be easily launched. Security attacks can have stringent harmful for legitimate users. Even though there are a lot of VANET safety applications, it is utterly wasted without VANET security. Ensuring the secured communication in VANET is essential. Regarding the security, a lot of cryptographic mechanisms have been applied. Public Key Infrastructure (PKI) method is a well-recognized and well-defined solution to secure VANET. In PKI, each entity in the network holds an authentic certificate, and every message must be digitally signed prior to its transmission. Trusted authority (TA) distributes valid certificate to all the registered and legitimate users as well as it issues Certificate Revocation List (CRL) to all the vehicles in the network. CRL contains the Id of all certificates issued by the Trusted Authority (TA) that have been revoked and have not yet expired.

In a PKI system, the authentication of the message is done in three phases. First, check the CRL whether the sender's certificate is included in the current CRL or not. By checking in the CRL, the sender's revocation status can be determined. It incurs a long delay depending on the CRL size and the searching mechanism used in CRL. Second, the sender's certificate is verified based on some protocols. Third, sender's signature on the received message is verified. In VANET, CRL size is expected to be large. Because, each OBU is preloaded with multiple anonymous certificates to preserve the privacy of the drivers. OBU can change its certificate in a periodic manner. Using multiple anonymous certificate reduces the leakage of the real identities and location information from the eavesdroppers. As well as, VANET scale is also very large compared to the various other types of networks. Each OBU may receive a large number of messages every 300 msec, and it should check in the current CRL for all the received certificates. Authentication delay may be longer depending on the CRL size and the number of receiving certificates. The ability to check a CRL for huge number of certificates in a timely manner leads an unavoidable challenge to VANETs.

II. RELATED WORK

The four main security requirements in VANET are Privacy (User, Location, etc.,) preservation, Message Authentication, Message Integrity and Nonrepudiation.

Albert Wasef and Xuemin Shen[1] introduced an expedite message authentication protocol (EMAP) which replaces the CRL checking process with an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable for any network (VANET, MANET, etc.,) employing a PKI system. The CRL checking process has been done and compared with various searching algorithms such as linear search, binary search, hashing. As a result, the authentication delay is reduced CRL checking process in VANET by using the hash function method.

Ghassan Samara et al. [2] proposed an efficient certificate management in VANET which avoids the CRL checking process. Because each vehicle must have a certificate of transmission. Even an adversary vehicle can transmit the message with its certificate. If any vehicle is a legitimate, it has a valid certificate (VC) or else it has an adversary certificate (AC). Each certificate has its own format. While receiving a message, the receiver checks the type of certificate. If it is Valid certificate, the message will be accepted or else it will be discarded.

Julien Freudiger et al. [3] introduce CMIX protocol, which maintains the location privacy in VANET by changing identifiers in the presence of a global passive adversary. This protocol creates cryptographic mix-zones at road intersections. It prevents computationally-bounded eavesdroppers while preserving the functionality of safety messages. Its process is divided into three phases such as Key establishment phase, key forwarding phase and key update phase. In the key establishment phase, all legitimate vehicles within the mix-zone obtain a symmetric key from the roadside unit (RSU) of the mix-zone, and use this key to encrypt all their messages while it resides within the zone. To ensure the functionality of safety messages, the mix-zone key can be received by nodes approaching the mix-zone with the help of a key forwarding mechanism, and the RSU can swap to a new key through a key update mechanism. The location privacy has been achieved by combining mix-zones into mix-networks in VNs.

Jason J. Haas et al. [5] propose an Efficient Certificate Revocation List Organization and distribution which reduced the CRL size. It was an efficient mechanism to check the presence of certificate Id in the CRL. CRL updates have been done by using lightweight mechanism. CRL checking process (checking whether the certificate's identifiers are present in the CRL or not) is done quickly by storing the certificate in a Bloom Filter which is a probabilistic data structure (i.e., searching has a non-zero, but small false positive rate) and has a constant (O(1)) cost in terms of computation for searching and storage.

Ghassan Samara [6] proposed Certificate Revocation Management in VANET which reduces the channel load resulted from frequent warning broadcasting happened in the adversary discovery process. Accusation Report produces a heavy channel load. Because, it receives the adversary report from all the vehicles. It replaces the Certificate Revocation List (CRL) by Local Revocation List (LRL). It reduces searching delay and high load on the channel. As a result, adversary search process is much easier and faster.

In [12], Hubaux identify the specific issues of security and privacy challenges in VANET, and indicate that a PKI should be well deployed to protect the transmitted messages and also authenticate all the network entities.

In [4], Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANET. In this approach, each vehicle needs to preload a large set of anonymous certificates. The loaded certificates in each vehicle should be huge to maintain security and privacy preservation for a long time, e.g., one year. Each vehicle should update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking a single vehicle implies revoking the large number of certificates loaded in it.

Distributing the large-size CRL in VANET is discussed in many works. In [14], Raya et al. introduce Revocation using Compressed Certificate Revocation Lists (RC2RL), where the traditional CRLs issued by the TA, are compressed using the Bloom filter algorithm to reduce its size before broadcasting.

Papadimitratos et al. [15] propose to split the CRL into small size and distribute each portion independently. Laberteaux et al. [16] propose to speed up the CRL broadcasting by vehicle to vehicle (OBU to OBU) communicate. Haas et al., [8] develop a mechanism to reduce the broadcast CRL size by sending a secret key for the revoked vehicle. On receiving the new CRL, each OBU reproduce the certificate identities using the secret key of each revoked vehicle and build the complete CRL. It should be noted that although the size of the broadcast CRL is reduced, the constructed CRL at each OBU. It is used to check the revocation status of other entities. Still, it suffers from the expected huge size exactly as that in the traditional CRLs where all the certificate identities of every revoked OBU are included in the broadcast CRL. He proposed using bloom filter, which is one kind of lookup hash tables, to process CRL checking for the received certificates. To reduce the false-positives in the bloom filter, he proposed that each vehicle should check before sending it certificate whether this certificate will trigger a false positive or not. If so, then it uses another certificate. He proposed to

upload all the vehicle with a set of anonymous certificates to compensate for those which will trigger a false positive. It is used in safety related vehicular applications.

III.PRELIMINARIES

A. Bloom Filter

A Bloom filter is a space-efficient probabilistic data structure. It is used to test whether an item is present in the set. False positive matches are possible, but there is no chance of false negatives, i.e. a query returns either "possibly in set" or "definitely an item is not present in the set". Items can be added to the set, but not removed. The more items that are added to the set, the larger the possibility of false positives. While storing and Checking the Vehicle's ID, It uses the hash function. As a result, the CRL checking process is faster.

It is done by using 3 phases.

1. Creation of empty bloom filter, i.e.| creation of empty CRL. It is created with two parameters falsePositiveProbability and expectedNumberOfElements.

   Here expectedNumberOfElements denotes how many Vehicles ID's are to be stored in CRL.

$$BloomFilter < String > bloomFilter = new\ BloomFilter < String > (falsePositiveProbability, expectedNumberOfElements)$$

2. Insertion of Invalid into CRL has been done by using the following statement.

$$bloomFilter.add(\text{“}CCNo1\text{”})$$

3. To check whether received certificate Id is present in the CRL or not is done by using contains()-method.

$$bloomFilter.contains(\text{“}CCNo1\text{”})$$

B. *Hash Function*

A hash function is an algorithm that maps data of arbitrary length to data of a fixed length. The hash code or hash values are returned by the hash function. Hash functions are mainly used in hash tables, Hash table is a data structure used to create and implement an associative array. It can map keys to values. A hash table computes an index into an array of items using a hash function, from which the correct value can be found. The hash function is used to map the search key to an index; the index gives the place in the hash table where the corresponding record should be stored.

C. Digital Signature

It is an electronic document which achieves non-repudiation. Digitally signing the document means that the person who signs the document assures that he is the author of the document or the message that was signed.

D. Linear Search Algorithm

In the linear search algorithm, the revocation status of a certificate is checked by comparing the certificate with each entry in the CRL from top to bottom sequentially. If a match occurs, the certificate is revoked and vice versa.

E. Binary Search Algorithm

The binary search algorithm works only on sorting lists. As soon as receiving a new CRL, each OBU has to sort the certificate's identity. The main benefit of using the binary search algorithm is to cancel out half of the entries after each comparison in the search process. The revocation status of a certificate is checked by comparing the identity of the certificate with the middle value of the sorted list. If the identity of the certificate is greater than the middle value, the right half of the list will be considered in the next comparison process and vice versa. This process continues until a match is found in the CRL, i.e., If the identity of the certificate is matched with any item in the CRL, it is revoked, or the process is terminated without finding a match which means that the certificate is not yet revoked.

III. SYSTEM ARCHITECTURE

The system model has the following entities. It is shown in Fig 1.

1. *Trusted Authority (TA)*: It distributes anonymous certificates for all the on-board units which are attached in Vehicles and the secret key for all VCRSUs in VANET.
2. *Road Side Unit (RSU)*: It is fixed and distributed all over the network. It is communicated with Trusted Authority and the vehicles. It can store Certificate Revocation List (CRL).
3. *On Board Units (OBU)*: It is embedded in vehicles. It can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

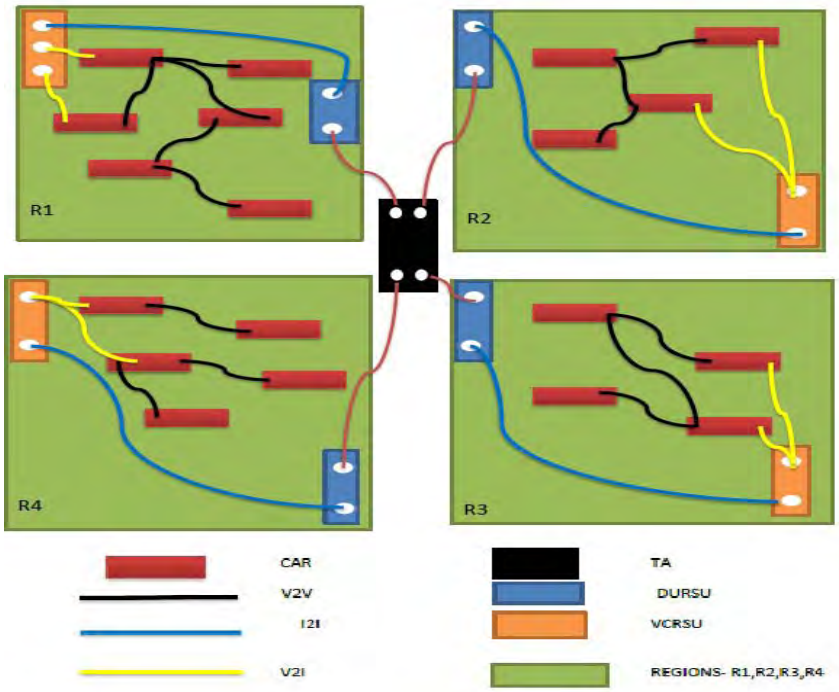


Fig 1. VANET Architecture

Trusted Authority creates a set of anonymous certificates for all OBUs in the network and also it distributes a private and public keys of OBUs to the corresponding region VCRSU in the network.

1. The total network areas are classified into regions, i.e. Mix zones. Each region has two types of RSUs.
   - *Vehicle communication RSU (VCRSU)*: This type of RSU is involved in communication with vehicles in its region.
   - *Data Updating RSU (DURSU)*: It monitors the incoming and outgoing vehicles in the region and updates the CRL data and send the same to VCRSU which is in its region.

A System Initialization

A set of anonymous certificates is created by TA for all the OBUs in the network. Each certificate has its certificate identity (cert_Id). Certificate Identity consists of two things such as private_key and public key. It also provides secret key for all the VCRSU.

Each VCRSU contains the list of Certificate Identity for all the OBUs in their region. Only the public key of this list is passed to all the OBU's in the region.

During the vehicle's mobility time, Each DURSU monitors the incoming and outgoing vehicle and update in VCRSU.

Algorithm for System Initialization:

1. Select two generators $P, Q \in G_1$ $order$ q
2. For $i \leftarrow 1, l$ do
3. Select a random number $K_i \in Z_q^*$
4. Set the secret key $K_i = K_i Q \in G_1$
5. Set the corresponding public key $K_i = \frac{1}{k_i} P \in G_1$
6. End for
7. Select an initial secret key $K_g \in G_2$
8. To be shared between all non-revoked OBUs
9. Select a master secret key $s \in Z_q^*$
10. Set the corresponding public key $P_0 = sP$
11. Choose hash functions $H: \{0,1\}^* \rightarrow G_1$ and $h: \{0,1\}^* \rightarrow Z_q^*$
12. Select a secret value $v \in Z_q^*$ and $v_0 = v$
13. For $i \leftarrow 1, l$ do ∇ to obtain a set V of hash chain values
14. Set $v_i = h(v_{i-1})$
15. End for

16. For all OBU_U in the network, TA do
17. For $i \leftarrow 1, m$ do
18. Select a random number $a \in [1, l]$
19. Upload the secret key $K_a = K_a Q$ and the
20. Corresponding public key $K_a = \frac{1}{K_a} P \ in \ HSM_u$
21. Which is the HSM embedded in OBU_u
22. End for
23. Generate a set of anonymous certificates
24. $CERT_U = \{cert_u^i \ (PID_u^i, \ PK_u^i, sig_{TA}(PID_u^i \mid PK_u^i)) \mid 1 \leq i \leq C\}$
25. Upload $CERT_U \ in \ HSM_u \ of \ OBU_u$
26. End for
27. *Announce H, h, P, Q and Po to all the* OBU_s.

B Message Sending

If an OBU needs to send any message, it should receive the region's secret key from the RSU (VCRSU) using its private key. VCRSU maintains CVL (Certificate of valid vehicles list in the region) and CRL.

Accessing Secret Key:

Step 1: The OBU sends the request to its region VCRSU for secret key.

Step 2: VCRSU checks the private key of the OBU which is present in the CVL or not.

Step 3: It it so, it will send the secret key, else it will not send it.

Step 4: After receiving the secret key of the region, each OBU sends the message with the followings.

1. Certificate Identity – It contains only the public key of OBU.
2. Digital Signature – Electronic signature of the OBU.
3. Time Stamp – It denotes at which time the message has been sent.

OBU sends the message in the following format.

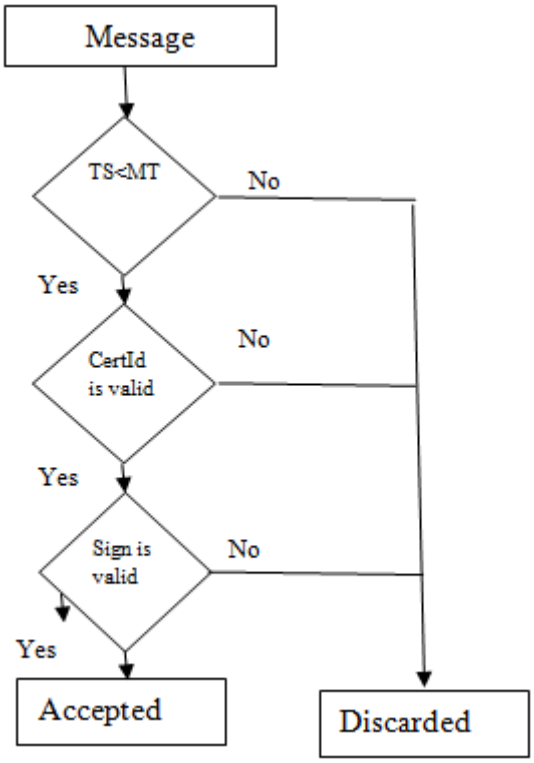
$$\left(M \mid T_{stamp} \mid cert_u \ \ (PID_u, PK_u, sig_{TA}(PID_u \mid PK_u)) \mid sig_u(M \mid T_{stamp}) \mid REV_{check}\right)$$

C. Message Verification

After receiving the message, each receiver checks the following in a sequential way.

- Timestamp of the message.
- Checking on the Certificate Revocation List.
- Digital Signature.

First, it checks the timestamp of the message. If it exceeds the maximum time which has been set for the region, it is discarded or else if the Id matches with any item in a CRL, the message is discarded or else it will check the final condition i.e.| Digital signature verification. If it is valid, the message will be accepted. It is shown in Fig.2.



Algorithm

1. Check the validity of Tstamp
2. If invalid then
3. Drop the message
4. Else
5. Check $REV_{check} = HMAC\left(k_g,\ PID_u \mid T_{stamp}\right)$
6. If invalid then
7. Drop the message
8. Else
9. Verify the TA signature on $cert_{OBU_u}$
10. If invalid then
11. Drop the message
12. Else
13. Verify the signature $sig_u\left(M \mid T_{stamp}\right)$ using OBU_u public key (PK_u)
14. If invalid then
15. Drop the message
16. Else
17. Process the message
18. End if
19. End if
20. End if
21. End if

```
PublicKey pubKeyRSA = certRSA.getPublicKey();
Signature sig = Signature.getInstance("SHA1withRSA", "FlexiCore");
sig.initVerify(pubKeyRSA);
sig.update(message);
boolean isValid = sig.verify(sigBytes);
System.out.println("The signature of the email verifies: " + isValid);
```

D. Revocation

If the message sent by any OBU is not coinciding with any messages of any other OBUs. It will be considered as Adversary OBU. Its certificate identity will be added in CRL and its anonymous Id and private keys are removed from other OBU, RSU and TA. Therefore, sending messages to this OBU can also be avoided.

E. Keys updating in DURSU

If any OBU gets inside the region, it changes its public key. This public key can be inserted in the new region VCRSU and the previous public key can be removed from the previous region VCRSU. The current VCRSU gets the remaining information such as private key of the newly added OBU using its public key from the Trusted Authority (TA).

IV. SECURITY ANALYSIS

A. *Eavesdropping*

If any adversary OBU knows any other public key and secret key of the region, it cannot eavesdrop the message. Because Each OBU has anonymous keys, it will change it often.

B. *Forging attacks*

Even any adversary finds the public key of other OBU, it cannot send and receive the message. If any OBU want to transmit and receive the message, it needs to get a secret key from its region's RSU. So forging attack is not possible with this protocol.

C. *Colluded attacks*

If any legitimate OBU colluded with any other adversary OBU, It can receive the secret key of the region. The private key the OBU is not in the RSU's Certificate of valid list (CVL) , its message will not be accepted by any other OBUs.

D. *Replay attack*

Each message is sent with the Timestamp information. So it cannot be used later by any other adversary vehicle.

E. *Forward Secret key*

Even though any adversary OBU gets the secret key of the RSU, they cannot send and receive information without their private and public keys which are presented in the CVL.

V. PERFORMANCE EVALUATION

A. *Computation Complexity*

The computation complexity of revocation status checking process is defined as the number of comparison operation required to check the revocation status of an OBU. In the linear search method, the CRL checking process started from the first item in the list sequentially. In Binary search method, the certificate identities in the list are sorted. Then searching id is compared with the middle id in the list. If it is less than the middle one, right side id will be considered for checking. Only left side of the middle one will be the portion for searching. Until it finds the id, the same process is to be followed. This binary searching is better than linear searching method. Hash method is searching in the CRL using the Hash Function. In this study, one kind of hash method, Bloom Filter is used for checking the revocation status in CRL. As well as compared to EMAP protocol, the road or network is classified into regions. Each region has its own CRL which consist of the revoked certificate id in the region. Computation complexity is very much lesser than the other protocols.

B. *Space Complexity*

Space complexity defines how much spaces needed to store CRL. Instead of storing all the revoked certificated in a single CRL, a separate CRL is maintained in each region. Each OBU has limited memory space. Storing limited data in this memory is most preferable. Compared to EMAP protocol, it takes very less space to store CRL.

C. *Authentication Delay*

We compare the message authentication delay employing the CRL with that employing this IMAP protocol to check the revocation status of an OBU. The authentication of any message is performed by three consecutive phases: the sender's revocation status checking, the sender's certificate verification, and the sender's signature verification. In the first authentication phase, we can apply any searching method for checking the revocation status of the sender. In IMAP, bloom filter technique has been used to check the revocation status. Compare to linear, binary searching method, it takes very less authentication delay. It is shown in Fig 3.

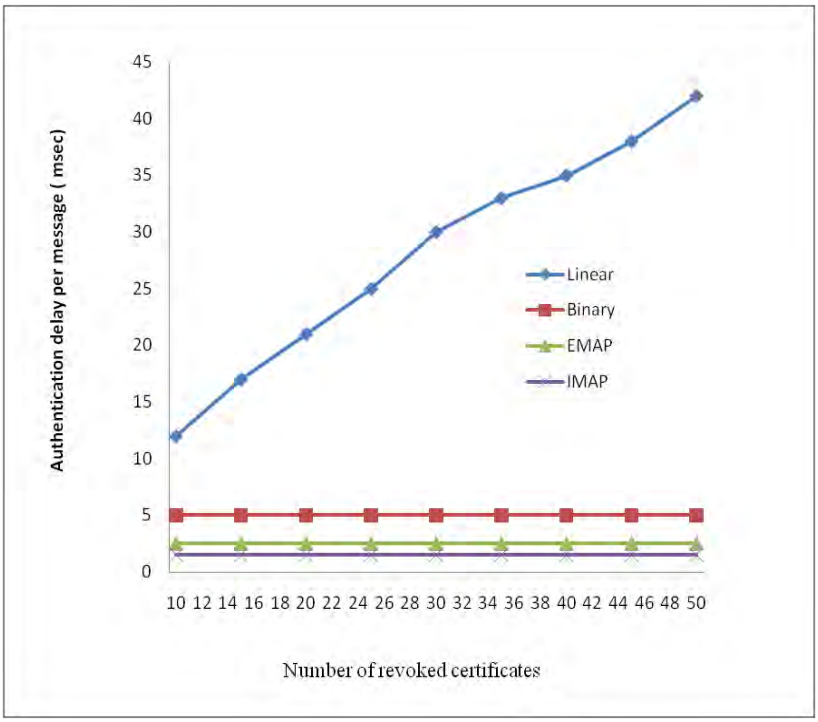


Fig 3: Authentication Delay

D. *End-to-End Delay*

It is the time to transmit the data from the sender to the receiver. It depends on the number of revoked certificates included in the CRL and also it depends on the CRL checking process. In the linear search method, it will search sequentially from the first item in the list. Already it was explained in computation complexity measurement. The proposed system consists of region-wise CRL which consists of revoked certificates in its region. The time taken for sending the data from sender to the receiver is less when compared to linear, binary, EMAP method. It is shown in Fig 4.

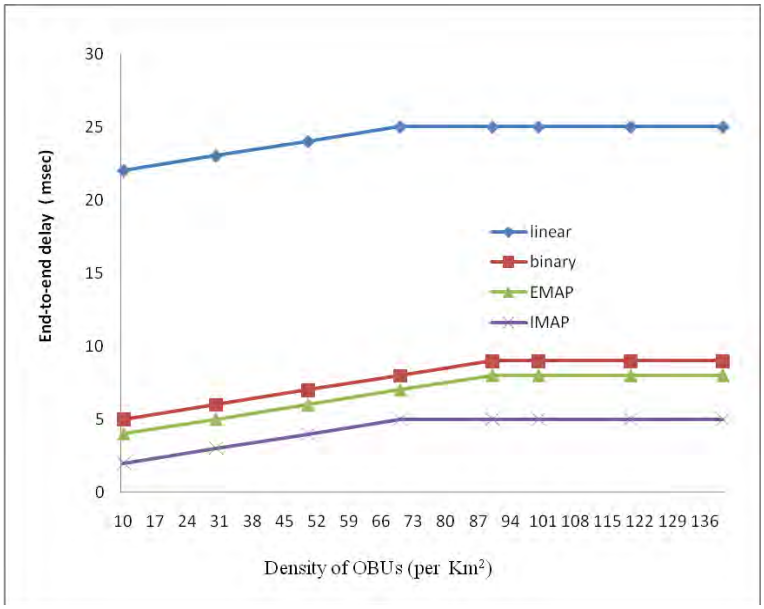


Fig 4: End-to-end delay

E. *Message Loss Ratio*

The average message loss ratio is defined as the average ratio between the number of dropped messages every 300 milliseconds, due to the message authentication delay, and the total number of received messages every 300 milliseconds by an OBU. It increases with the number of OBUs within the communication range. In IMAP, only limited OBUs may be involved in communication within the region and also it incurs the minimum revocation status checking. As a result, IMAP decreases the message loss ratio compared to that employing either the linear or binary or EMAP. It is shown in Fig 5.

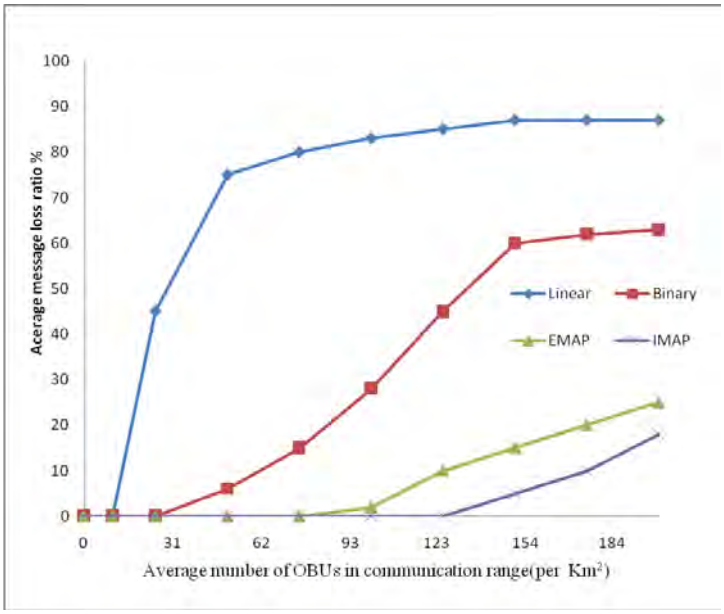


Fig 5: Message Loss ratio

F. *Communication Overhead*

In IMAP and EMAP, each OBUu broadcast the message in the form $(M \mid T_{stamp} \mid cert_u \ (PID_u, PK_u, sig_{TA}(PID_u \mid PK_u)) \mid sig_u(M \mid T_{stamp}) \mid REV_{check})$. In the WAVE standard, a signed message has the certificate and signature of the sender with a time stamp on the transmitted message. The additional communication overhead incurred in IMAP and EMAP compared to that in the WAVE standard is mainly due to REVcheck.

G. *Communication Cost of Updating list and key*

The communication cost of updating the CRL and OBU's keys is much lesser than the EMAP. Instead of updating in a large CRL, In IMAP, it is done in region-wise CRL. It is very easy as well as it incurs minimum cost when compare to EMAP, Linear and Binary method. It is shown in Fig 6.

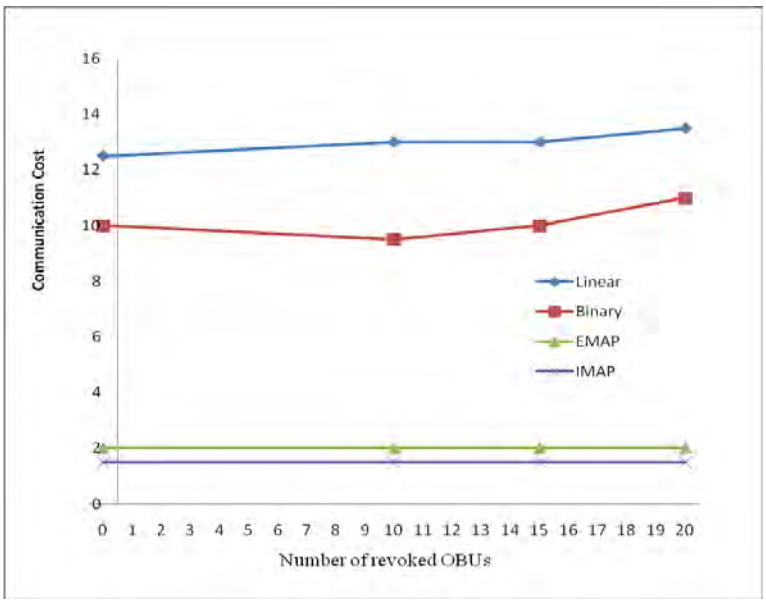


Fig 6: Communication Cost

VII. CONCLUSION

In this paper, we have proposed IMAP for VANET which provides message authentication and efficient certificate revocation list management by replacing the time-consuming CRL checking process with a fast revocation checking process with Bloom filter. It reduces message loss ratio and space complexity in RSU and OBU by introducing region-based revocation checking process and also it maintains privacy by using anonymous keys for OBUs. Authentication is done by Digital signature method. In the future, Instead of sending the CRL to all the OBUs in the region at a time, it will be sent only to the needy OBU based on some criteria as well as anonymous certificates can be generated automatically in OBUs.

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, JANUARY 2013.

[2] Ghassan Samara, Wafaa A.H. Al-Salihy, R.Sures, "Efficient Certificate Management in VANET", IEEE, 2010.

[3] Julien Freudiger, Maxim Raya, Mark Felegyhazi, Panos Papadimitratos and Jean-Pierre Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks", WiN-ITS 2007 Vancouver, British Columbia, Canada

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

[5] Haas, J.J., Yih-Chun Hu , Laberteaux, K.P , Efficient Certificate Revocation List Organization and Distribution, vol. 29, 2011.

[6] Samara, G, Al-Salihy, W.A.H, Sures, R, Efficient certificate management in VANET, Future Computer and Communication (ICFCC), V3-750 - V3-754, IEEE, 2010

[7] 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.

[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] 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.

[10] 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.

[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.

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

[14] 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.

[15] 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.

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

G. Anitha works as a lecturer in the department of computer applications, Karpagam University, Coimbatore. Her area of interest is VANET or Wireless network Security. She is pursuing her Ph.D degree in Bharathiar university, Coimbatore. She has more than 7 years of teaching experience in colleges and universities.

Dr. M. Hemalatha completed M.Sc., M.C.A., M. Phil., Ph.D (Ph.D, Mother Terasa women's University, Kodaikanal). She is Assistant Professor and guiding Ph.D Scholars in Department of Computer Science at Karpagam University, Coimbatore. Twelve years of experience in teaching and published more than hundred and fifty research papers in International Journals and also presented more than eighty papers in various national and international conferences. Area of research is Data Mining, Software Engineering, Bioinformatics, and Neural Network. She is a Reviewer in several National and International Journals.