EMAP: EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VANETS

Bhagyashree .R
Asst.Professor, Dept.of CSE
A.P.S.C.E, Bangalore

Abstract -- Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code (HMAC) where the key used in calculating the HMAC is shared only between non-revoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient.

Key words—Vehicular networks, communication security, message authentication, certificate revocation.

1. INTRODUCTION:

1.1. Background

An Ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infrastructure or centralized administration. Vehicular Ad-hoc Networks (VANETs) is a form of ad-hoc network which provides communication among the nearby vehicles. Vehicular ad 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 architecture consists of a backbone network including authorities and management centers, equipment installed beside the roads, namely Road Side Units and the corresponding devices inside the vehicles, namely the On-Board Units. These components are interacting with each other as shown in Figure 1.1

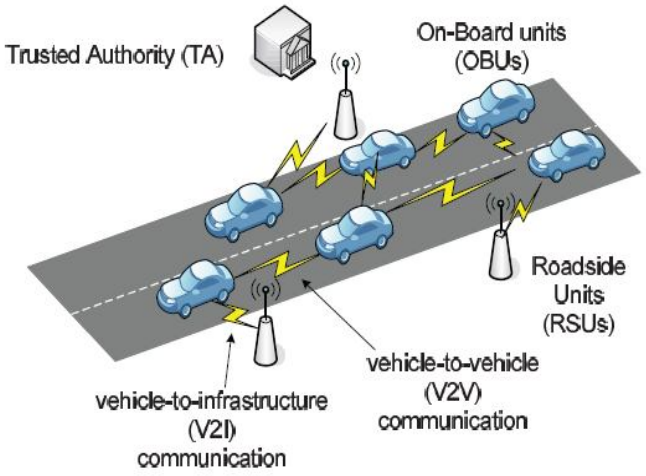

Figure 1.1: VANETs architecture

TRUSTED AUTHORITY (TA)

In VANETs trusted authority is an essential entity which provides identity for vehicles and monitors the entire network and other the major responsibility of the trusted authority is public key management. Public key management includes public key registration, public key publication, and public key revocation processes. It is also responsible for issuing the secret keys to the vehicles.

Road side Units (RSU)

RSUs are stationary devices placed in critical locations of the road (e.g. junctions) capable of communicating with vehicles and the backbone network. RSUs are collaborating in VANETs by distributing/collecting traffic and non-traffic related information to/from vehicles and by providing different features to manage the system. In other words, RSUs works as an interface between the backbone infrastructure and the vehicles. One interesting application of RSUs is to recommend optimized speed to vehicles approaching to junctions equipped with traffic lights. This will let the driver pass the junction without stopping and smoothing the traffic which will increase efficiency (e.g. fuel consumption of heavy vehicles can be dropped drastically)

ON BOARD UNITS (OBU)

In VANET, vehicles are equipped with devices called OBU, capable of communicating with RSUs and other nearby OBUs. OBU frequently broadcasts messages including information about the vehicle position, speed, direction, braking status and other related information associated to the vehicle. OBUs in collaboration with vehicle sensors can compute and generate a variety of messages upon different situations (e.g. emergency braking, traffic jams, accidents and change in weather condition)

Each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e.g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. Figure 2.1 is describing the two main types of communication modes in VANETs: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Roadside Infrastructure (V2I) communication. In V2V communication mode a vehicle communicates with other vehicles present in the network and all the vehicles engaged in the communication are mobile. V2I communication refers to a type of communication that involves Road Side Units (RSUs) communicating with the vehicles

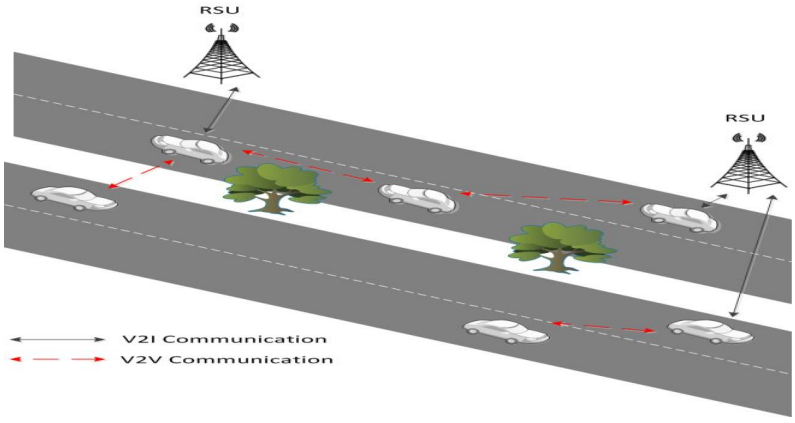

Figure 2.1 Communication modes in VANETs

1.2. Attacks on VANETs

Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Different types of attacks which are most commonly encountered in VANETs are listed below.

1.2.1. Denial of Service attack

The availability of network is very important in vehicular network environment where all users rely on the network. Denial of Service (DOS) is one of the most serious level attacks in vehicular network. In DOS attack, attacker jams the main communication medium and network is no more available to legitimate users [4]. The main aim of DOS attacker is to prevent the authentic users to access the network services

Figure 3.1 shows the whole scenario when the attacker A launches DOS attack in vehicular network and Jams the whole communication medium between V2V and V2I. As a result, authentic users (B, C, and D) can not communicate with each other as well as with infrastructure [8].

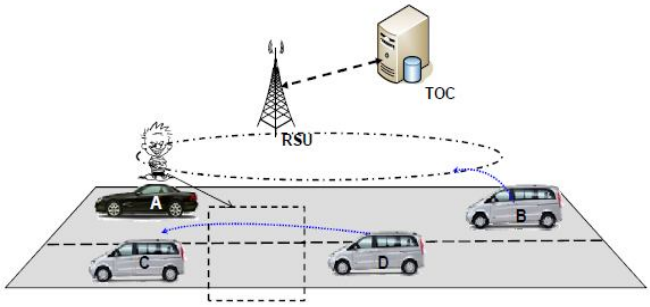

Figure 3.1 DOS attack

1.2.2. Sybil Attack

In Sybil attack,[10] the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID). It provides illusion to other vehicle by sending some wrong messages like traffic jam message [3,4]. Figure 4.1 explains Sybil attack in which the attacker creates multiple vehicles on the road with same identity. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

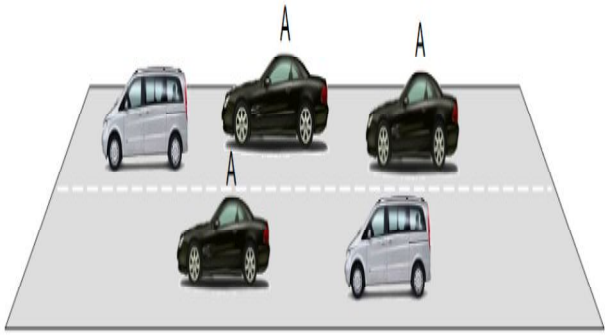

Figure 4.1 Sybil attack

1.2.3. Node Impersonation Attack

Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles [4, 9, and 10]. Fig 5.1 explains this scenario in which vehicle A involves in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.

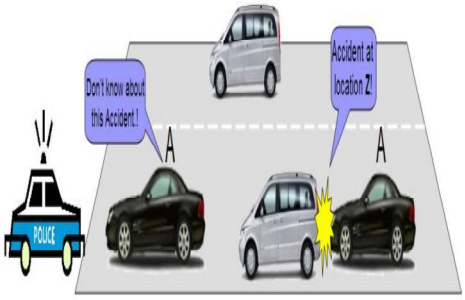

Figure 5.1 Node impersonation attack

1.2.4. Social Attack

It is kind of emotional and social attack. Purpose of these kinds of messages is to indirectly create problem in the network. Legitimate users show angry behavior when they receive such kind of messages. This is actually attacker wants by launching such attack. Figure 6.1 explain this condition, attacker B passes this message **"You are Idiot**" to near by vehicle C. When user receives this message is directly affect his driving behavior by increasing the speed of his/her vehicle. This entire thing is indirectly disturb the other user in the network.

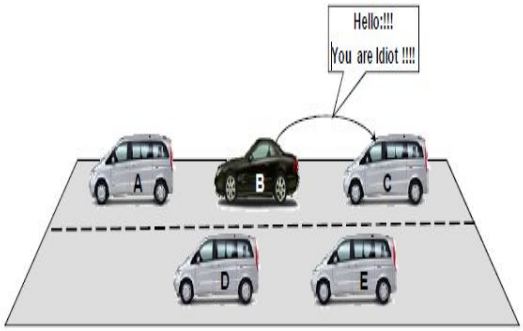

Figure 6.1 Social attack

1.**2.5. Timing Attack**

This is new type of attack in which attacker's main objective is to add some time slot in original message and create delay in original message. Attackers do not disturb the other content of message, only create delay in the message and these messages are received after it requires time. Safety application is a time critical applications, if delay occurred in these applications then main objective of the application are finished.

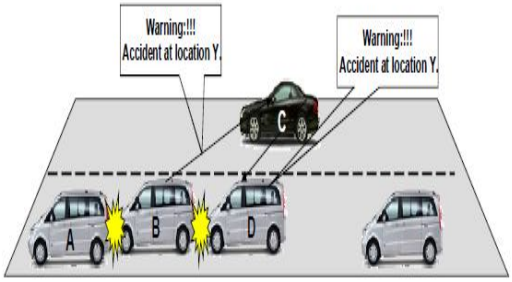

Figure 7.1 Timing attack

Figure 7.1 shows the complete scenario of the timing attack, in which attacker C receive warning message (**Warning! Accident at location Y**) from other vehicle B and then pass this message to other vehicle D by adds some time. Whenever other vehicle D of the network receive this message when accident actually occurred.

1.3. How to Secure VANETS

A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI) and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate and every message should be digitally signed before its transmission.

1.3.1. Public key infrastructure

A public-key infrastructure (PKI) is a set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates.

1.3.1.1. Certificate revocation list (CRL)

The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue and the entities that issued them are also included.

1.3.2. Security features supported by PKI system

PKI is an infrastructure used to support digital signing and encryption mechanisms.PKI scheme is generally used to provide some security services, such as confidentiality,integrity, authentication and non-repudiation which are the primary security requirements need to satisfied by all the VANETs applications.

- **Confidentiality** It is the assurance of data privacy, which means that no one access the data except authorized entity. This service is achieved by cryptographic mechanisms such as public key cryptography and symmetric key cryptography.
- **Integrity** assures that data is not altered by unauthorized entity. This can be achieved by employing digital signature mechanisms.
- **Authentication** within the PKI system is one which verifies the identity of data origin. This is achieved by digital signature mechanism.

- **Non-repudiation** It is to ensure that originator cannot falsely deny the origin of the message by applying digital certificate mechanism**.**

1.3.2.1. Functions of PKI system

- **Registration** is the process whereby a user first makes itself known to a TA , prior to that TA (trusted authority) issuing a certificate or certificates for that user.
- **Initialization:** Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure.
- **Certification:** This is the process in which a TA issues a certificate for a user's public key and returns that certificate to the user's client system and/or posts that certificate in a repository.
- **Key pair recovery:** Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both.
- **Key pair update:** All key pairs need to be updated regularly (i.e., replaced with a new key pair) and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation
- **Revocation request:** An authorized person advises a TA of an abnormal situation requiring certificate revocation. Reasons for revocation include private key compromise, change in affiliation, and name change.
- **Cross certification:** Two TAs exchange information used in establishing across-certificate. A cross-certificate is a certificate issued by one TA to another TA that contains a TA signature key used for issuing certificates.

2. Literature Survey

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [11], [12]. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

In [13], the technique was used to identify the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In this approach, each vehicle needs 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 this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it.

In [12], an efficient authentication and revocation scheme called TACK is proposed. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. Here group signature concept is adopted, where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate 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 signature of the vehicle and ensures 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 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.

A different way of reducing the size of the CRL involves using types of compression techniques. One method for compressing the CRL information using Bloom filters was introduced by in [14] . In this method, each certificate that is revoked is hashed to a fixed number of bits several times. The resulting hash value for each revoked certificate forms a type of signature. The signatures of several revoked certificates can be combined into a single bit sequence that serves as the Bloom filter. Each time a certificate is received, the same hashes are performed and the resulting value is checked against the Bloom filter. If the signature matches a pattern in the Bloom filter, that means the certificate has been revoked with high probability. Storing CRL information in this manner compresses the size of the CRL considerably since a fixed-length Bloom filter is distributed instead of distributing 8 to 14 bytes for every certificate that is revoked.

There is a small probability of a false positive occurring when using this method due to hash collisions, which increases as more certificates are added to the Bloom filter. [15] suggests testing a new pseudonym against the currently-possessed Bloom filter to see if the new pseudonym tests positive (revoked) using the Bloom filter. If the pseudonym does test positive, the user should discard the pseudonym and try a different one.

In [17] a mechanism is introduced 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 still suffers from the expected large size exactly as that in the traditional CRLs .
The other revocation method discussed in [23] is Revocation using Compressed Certificate Revocation Lists (RC2RL). This method sends out certificate revocation lists that are compressed using Bloom filters to make the lists smaller. This method reduces the size of the CRL by using about half the number of bytes to specify the certificate ID for revocation. This shortens the already hashed value so that the number of false positives increases.

3. 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 possible2

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.

System Initialization

The system model under consideration is mainly a PKI system in which each OBUs has a set of anonymous certificates used to secure its communications with other entities in the network. In specific public key(PK),included in the certificate and the secret key (SK) are used for verifying and signing messages. Each OBUs is preloaded with a set of asymmetric keys (secret keys in RSU and the corresponding public keys in RSU). The keys are necessary for generating and maintaining a shared secret key Kg between unrevoked OBUs.

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

Message signing

OBU (on board units broadcast the message by concatenating the time stamp , pid (process id) and hash code. Message is authenticated by attaching the trusted authority's and sender's signature.

Message verification

Receiving OBU verifies the time stamp,sender signature ,trusted authority signature. It calculates its own hash code and verify it with the sender's OBU to ensure message authentication

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.

4. SIMULATION AND ANALYSIS

The Network Simulator ns-2.35 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 8.1 shows that the

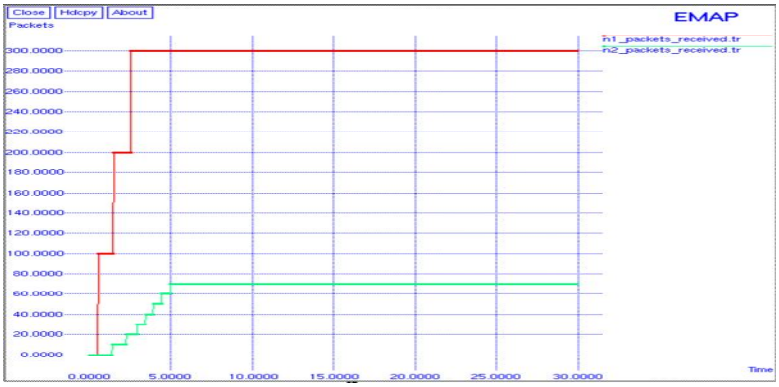

Figure 81 . Packet Receive Ratio

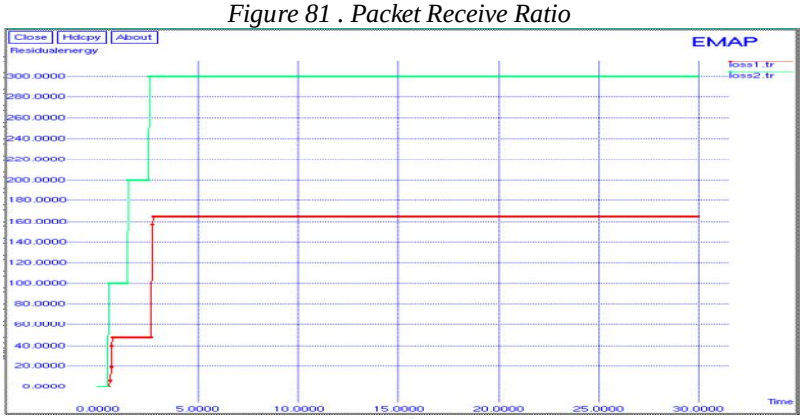

Figure 9.1. Packet Loss Ratio

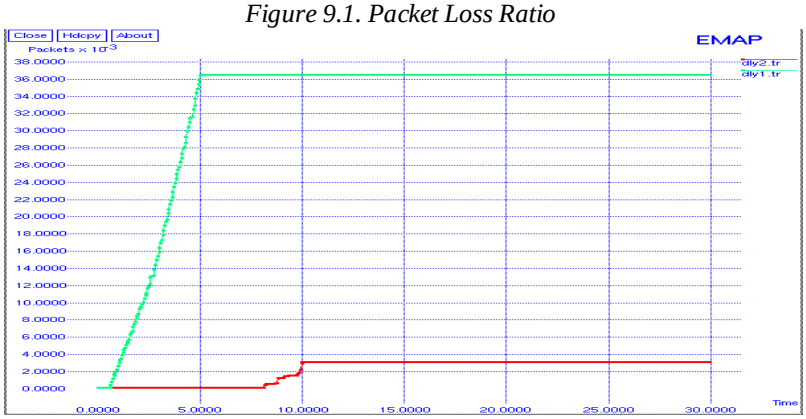

Figure 10.1. Packet Delay

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

Authentication Delay

We compare the message authentication delay employing the CRL with that employing EMAP to check the revocation status of an OBU. As stated earlier, the authentication of any message is performed by three consecutive phases: checking the sender's revocation status, verifying the sender's certificate, and verifying the sender's signature.

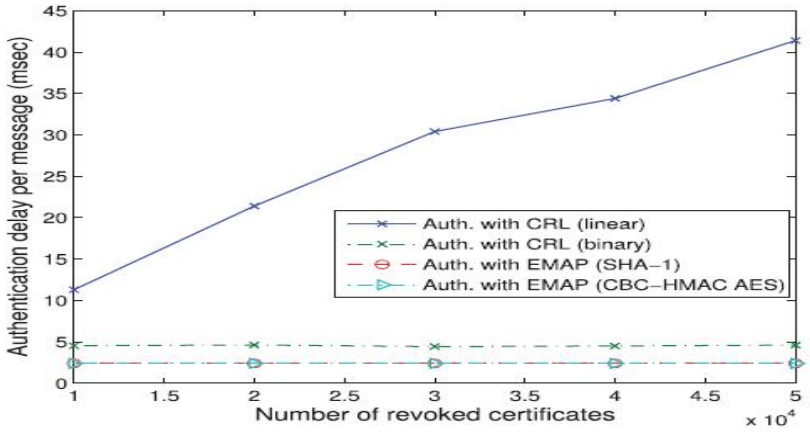

Figure 11.1 authentication delay

Fig. 11.1 shows a comparison between the authentication delay per message using EMAP, linear CRL checking process, and binary CRL checking process versus the number of the revoked certificates, where the number of the revoked certificates is an indication of the CRL size. It can be seen that the authentication delay using the linear CRL checking process increases with the number of revoked certificates, i.e., with the size of the CRL. Also, the authentication delay using the binary CRL checking process is almost constant. The authentication delay using EMAP is constant and independent of the number of revoked certificates. Moreover, the authentication delay using the EMAP outperforms that using the linear and binary CRL

5. 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] H. Hartenstein and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164--171, June 2008.
[2] "Vehicle Safety Communications Project - FINAL REPORT - CAMP IVI Light Vehicle Enabling Research Program, DOT HS 810 591," U.S. National Highway Traffic Safety Administration, 2006.
[3] N. H. T. S. Administration, "Traffic Safety Facts, DOT HS 811 172 ", 2009.
[4] "Traffic Safety Facts, DOT HS 811 291," U.S. National Highway Traffic Safety Administration, 2010.
[5] "The Economic Impact of Motor Vehicle Crashes, 2000," U.S. National Highway Traffic Safety Administration, 2002.
[6] A. A. Carter and J. Chang, "Using Dedicated Short Range Communications for Vehicle Safety Applications – the Next Generation of Collision Avoidance," 2009.
[7] H. Hartenstein and K. P. Laberteaux, "VANET: Vehicular Applications and Inter-Networking Technologies," John Wiley & Sons, Ltd, 2010.
[8] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks Alexandria, VA, USA, 2005.
[9] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, IEEE Standard 1609.2-2006, 2006.
[10] "FCC Report and Order 99-305," 1999.
[11].P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems,” Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.
[12].A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,” Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON ’09), pp. 1-9, 2009.
[13].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.
[14]. J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc.Sixth ACM International Workshop Vehicular Inter NETworking, pp. 89-98, 2009.
[15]. S. Zhu, S. Setia, S. Xu, and S. Jajodia, “GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks,”2006.

[16]. A. Wasef and X. Shen, “MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE GlobeCom, 2009.
[17]. J.P. Hubaux, “The Security and Privacy of Smart Vehicles,” IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.
[19]Albert wasef, xumen shen EMAP :expedite message authentication protocol for vehicular adhoc networks”,2013
[20] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks Montreal, Quebec, Canada, 2007.
[21] P. Kamat, A. Baliga, and W. Trappe, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks," Security and Communication Networks, vol. 1, pp. 233--244, 2008.
[22].M. Nowatkowski, J. Wolfgang, C. McManus, and H. Owen III, "The Effects of Limited Lifetime Pseudonyms on Certificate Revocation List Size in VANETs," in IEEE SoutheastCon Charlotte, North Carolina 2010.