Expedite Message Authentication Protocol For VANETS

Meghana D [1], Sowmya C H [2]

[1] *Student, Dept. of E&C, REVA ITM, Karnataka, India.*
[2] *Assistant Professor, Dept. of E & C, REVA ITM, Karnataka, India*

---***---

ABSTRACT*: VANETS uses public key infrastructure and certificate revocation list for their security. The authentication of a received message in any public key infrastructure system is performed by checking the certificate of the sender. In this project Expedite Message Authentication Protocol for VANETs is proposed which replaces time consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses keyed Hash Message Authentication Code where the Key used in calculating the HMAC is shared only between non revoked OBU. In addition EMAP uses a novel probabilistic key distribution which enables non revoked OBU to securely share and update a secret key. EMAP can significantly decrease the time consumed for checking list and hence the EMAP is demonstrated to be secure and efficient.*

KEY WORDS: Vanets, security, public key infrastructure, revoke, OBU.

1 INTRODUCTION:

VANETs are required to support a vast variety of applications, extended from safety-related to notification and other value added services. The inherent human desire for change, progress, mobility, entertainment, safety and security are leading the way to the development of intelligent transportation systems (ITS). The world today is living a combat, and the battle field lies on the roads, the estimated number of deaths is about 1.2 million people yearly worldwide, and injures about forty times of this number, without forgetting that traffic congestion that makes a huge waste of time and fuel The growth of the increased number of vehicles are equipped with wireless transceivers to communicate with other vehicles to form a special class of wireless networks, known as vehicular ad hoc networks or VANETs. However, before putting such applications into practice, other security concerns like as integrity and authenticity should be solved because any malicious behavior of users, such as modification and replay attacks with respect to disseminate traffic-related messages, could be fatal to other users and may risk life of humans. Thus, in VANETs, the information exchanged plays an important role. In particular, for safety-related applications, the information transmitted among vehicles is considered critical. If an attacker manipulates the information could potentially cause harm; therefore, implementing security measures is the utmost important. Hence this motivates to undertake project based on security concerns in VANETs.

As stated implementing security measures is of the utmost important. A well-recognized solution to secure VANETs is to deploy the Public Key Infrastructure (PKI), and to hold Certificate Revocation Lists (List) for being in charge for the revoked certificates. In PKI, every node in the network holds an identity certificate, and each information should be digitally signed before its transmission. A List, usually distributed by a Trusted Authority (TA), is a list containing all the revoked certificates. In the PKI model, the authentication of any information is performed by first analyzing if the sender's certificate is included in the current List, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on receiving messages.

The first part of authentication, which checks the revocation status of the sender in a List, may include long delay rely On the List size and employed mechanism for searching the List. unfortunately, The List size in VANETs is believed to be large for the following reasons: 1) To Keep the privacy of the drivers, i.e., to abstain the leakage of the real identities an location information of the drivers from any external eavesdropper, each OBU must be preloaded with a set of anonymous digital certificates, where the OBU need to periodically alter its anonymous certificate to mislead hackers. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a raise in the List size. 2) The scale Of VANET is very large.

2 MAIN OBJECTIVES

Vehicles communicate through wireless channels, a various attacks such as injecting false information, modifying and replaying the disseminated messages can easily launched. Incur long delay depending on the List size and employed device for searching the List. EMAP which replaces the List examining process by an effective revocation examine process using a fast and secure HMAC function. EMAP is suitable not only for VANETs but also for any network employing a PKI Model. To reduce the authentication delay resulting from checking the List in VANETs.

3 SCOPE OF THE WORK

Vehicular ad hoc networks are mainly designed for safety applications to ensure the safety of driver's and vehicles and also to avoid or minimize the road accidents. VANET is a special type Of Mobile ad hoc networks customized for automobiles with some distinctive features, e.g. predictable mobility patterns, movement of nodes along predefined paths instead of random directions. There are no battery constraints in VANET therefore it is suitable for long range communications through vehicles. In addition to safety applications, various other applications like collision avoidance, traffic management, trip planning and infotainment are also developed for them. Safety applications must be protected from hackers and crafty attacker because a compromised safety application could result in the loss of human life. Commercial applications need security to protect the potential loss of revenue. Without security, a Vehicular Ad hoc network can be affected by many attacks like denial of service, message suppression and propagation of false message attacks etc. that may cause accidents.

- VANETs are current emerging technology in wireless communication.
- Security is an important concern in VANETs, because they communicate a real time message which has to reach destination on time and without tampered.
- If such messages are altered by opponents, then it may lead to false interpretation of the message and chances of risking once life is more.
- EMAP resists the opponents' attacks in VANETs and provides authentication for the message with approximately expected timing.
- The PKI system and List system are replaced with Fast and secure Keyed Hash Message Authentication Code which cuts the delay.

4 METHODOLOGY

The proposed system ensures low end-to-end delay, low Overhead and thus a better communication channel. The EMAP apply a fast H-MAC function and novel key sharing technique employing probabilistic random key distribution. Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay involved in examining the revocation status of a certificate using a List. EMAP employs keyed Hash Message Authentication Code [H-MAC] in the revocation checking process, where the key used in calculating the H-MAC for every message is shared only within unrevoked OBUs. In addition, EMAP is free from the false positive property which is common for lookup hash tables. Extension of EMAP for bulk authentication in VANETs clearly reduces the communication overhead thereby making the communication faster and easier

4.1 System Design

A Trusted Authority responsible for providing anonymous certificates and sharing secret keys to all lists in the network. The Roadside units (RSUs) are fixed and it is distributed all over the network. RSUs will communicate securely with the Authority and OBUs are equipped in vehicles. All the OBUs can communicate either with Other OBUs through V2V communications or with RSUs through V2I communication. The system model under consideration is mainly a PKI system in which each vehicle has a set of anonymous certificates used to secure its communications with other parties in the network. In specific public key (PK), included in the certificate and the secret key (SK) are used for checking 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 getting and maintaining a exchanged secret key K_w between unrevoked node.

4.2 Message Authentication:

The details of the Authority signature on a certificate and an OBU signature on a message are not discussed in this work, for the sake of generality, we brought up PKI system. We only focus in how to accelerate the revocation examining process that is conventionally performed by checking the List for every certificate received. After that sender initiate with message signing and verification between different parties in the network are performed.
Authentication is performed by the following steps:

- Message signing
- Verification
  1-RSU - Aided Verification
  2-Batch Verification
- Revocation

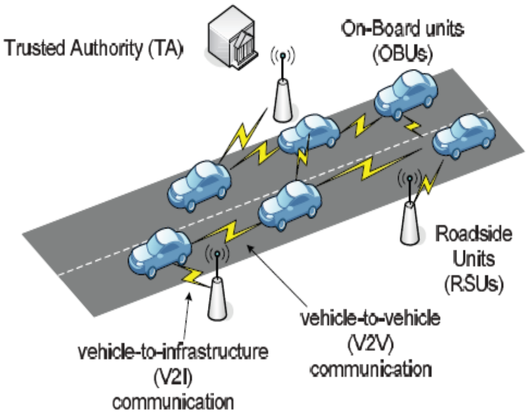

Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-infrastructure (V2I) communication
vehicle-to-vehicle (V2V) communication

Fig-1 System Initialization

4.2.1 Message Signing

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

4.2.2 Message Verification

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

4.2.3 Rsu - Aided Verification

The List consists of set of revoked certificates. The certificate which belongs to the identity of each vehicle is revoked due to the reasons like certificate expiration or any other validation problems. The certificates can be accepted only when they are in state of non-revoked else it is considered as revoked and the privacy-related message that is broadcasted is no more accepted by the destination vehicle. The List verification is performed using the concept of hash chain. RSU is a fixed Structure on the roadside; Each node belongs to their corresponding RSUs depending upon their timestamp value, the time when they get fixed to the network. The certificate upgrade is performed through a Trusted Authority (TA), which forwards the new certificate to the requesting OBU through the available RSUs on the Roads. RSU does this verification rather than by Authority in a timely manner since RSU can securely communicate with Authority. Due to this communication Overhead is reduced. Thus, the SM-MAP scheme Offers a distributed certification services. Finally, when a certificate is found to be revoked it must progress the non-revocation process. Thereby it make sure fast revocation verifying process without any delay.

4.2.4 Batch Verification

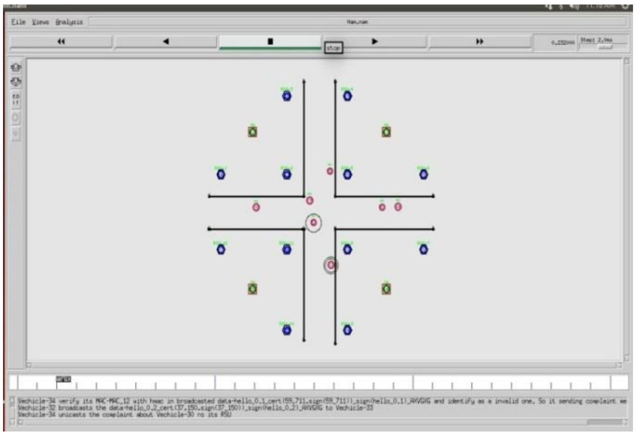
Considering the necessity for each vehicle to verify a large number of messages in a timely manner, SM-MAP introduces batch verification method, which enables any vehicle to simultaneously check number of messages in bulk. The verification is done with help Of Secure Hash.

4.3 Revocation

An important feature of the proposed EMAP will enable a vehicle to upgrade its compromised keys corresponding to previously missed revocation processes provided that it picks one revocation process in the further. A rekeying method id capable of updating compromised keys corresponding to rekeying processes previously missed is introduced.

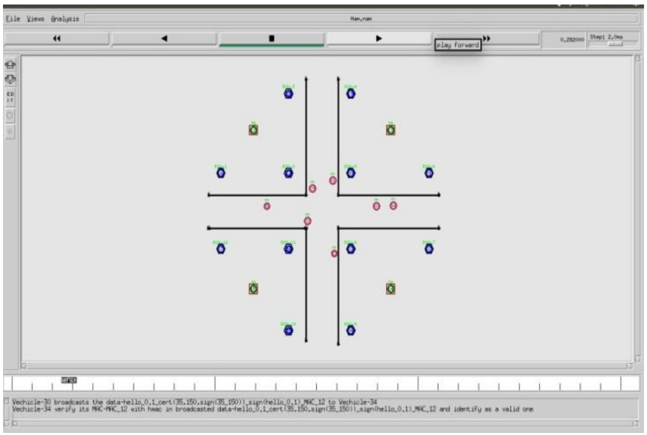
5 SIMULATION AND RESULTS

Fig 2 shows Broadcasting Messages Vehicle to Vehicle Communication. Here vehicle 30 is sending hello message to vehicle 34. Vehicle 30 sends message in format of (Data $||T_{stamp}$ || $cert_u$ (ID_u, XK_u, sig_{TA} (IDu || XK_u))|| sig_u(Data $||T_{stamp}$) || REV_{check}),Then vehicle 34 checks verification, and detects whether the sender is valid or not. Fig 3 shows whether vehicle is valid or not. Vehicle 34 checks whether vehicle 30 is valid or not if valid then it process the message else it complains to the Trusted Authority (TA). Then Revocation Process takes place. Fig 4 shows Revocation Process. If Vehicle is revoked then it has to be involve in CRL list then it takes revocation process, generates new key list. Fig 5 shows Vehicle 34 Complains to TA that vehicle 30 is illegal user and notes that vehicle number in CRL list and updates to all other nodes in the network.



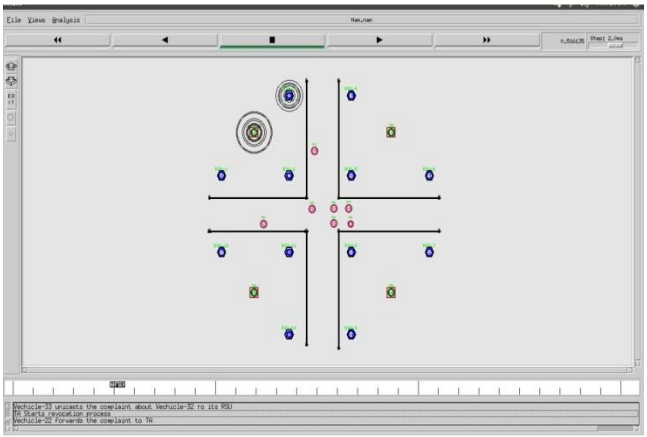
```
Vechicle-34 verify its MAC-MAC_12 with hmac in broadcasted data-hello_0.1_cert(59,711.sign(59_711))_sign(hello_0.1)_AKVGKG and identify as a invalid one. So it sending complaint me
Vechicle-32 broadcasts the data-hello_0.2_cert(37,150.sign(37_150))_sign(hello_0.2)_AKVGKG to Vechicle-33
Vechicle-34 unicasts the complaint about Vechicle-30 ro its RSU
```

Fig 2 Vehicle 30 broadcast the message to vehicle 34



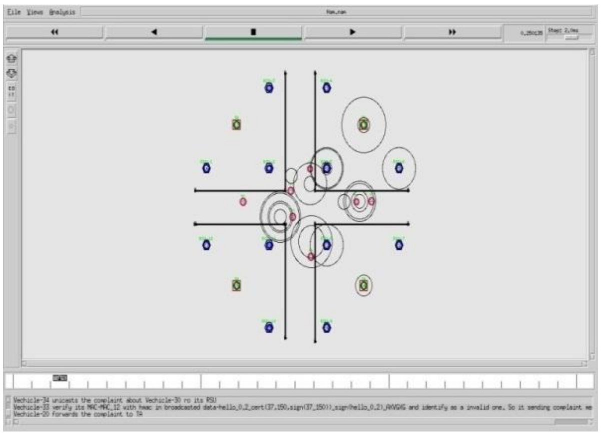
```
Vechicle-30 broadcasts the data-hello_0.1_cert(35,150.sign(35_150))_sign(hello_0.1)_MAC_12 to Vechicle-34
Vechicle-34 verify its MAC-MAC_12 with hmac in broadcasted data-hello_0.1_cert(35,150.sign(35_150))_sign(hello_0.1)_MAC_12 and identify as a valid one
```

Fig 3 Valid vehicle & then it process the message.



```
Vechicle-33 unicasts the complaint about Vechicle-32 ro its RSU
TA Starts revocation process
Vechicle-22 forwards the complaint to TA
```

Fig 4 Revocation process



```
Vechicle-34 unicasts the complaint about Vechicle-30 ro its RSU
Vechicle-33 verify its MAC-MAC_12 with hmac in broadcasted data-hello_0.2_cert(37,150,sign(37_150))_sign(hello_0.2)_AKVGKG and identify as a invalid one. So it sending complaint me
Vechicle-20 forwards the complaint to TA
```

Fig 5 Complain to TA and generates new key

6 CONCLUSION

As security plays important role in VANETs. Proposed EMAP for VANETs, which expedites message authentication by replacing the time-consuming List analyzing process with fast revocation verifying process employing HMAC function. EMAP works on novel key sharing technique which allows an vehicle to set its compromised keys even if it previously missed some revocation process. In addition, EMAP has a modular feature rendering it inferable with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional List. Therefore, EMAP can significantly lower the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

7 REFERENCES

[l] P. Papadimitratos, Kung A, F. Kargl and J.P. Hubaux, “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, K. Matsuura, M. Li, R.. Poovendran and K. Sezaki, L Huang “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.
[3] A. Wasef, X. Shen, “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, J.Hubaux, “Securing Vehicular Ad-Hoc Networks,” Journal Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[5] Y. Sun, , X. Lin, X. Shen, R. Lu, and J. Su, “An Efficient Pseudonymous Authentication Method with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.
[6] R. Lu, H. Luan, X. Shen, and X. Liang, “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.
[8] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.