International Journal of Research
Available at
https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

# Expedite Message Authentication Protocol For Vanets: A Study

**Divya Boya[1], Sravya Boya[2]**
*[1]Assistant Professor, Arjun College of Technology and Science*
*[2]Assistant Professor, Arjun College of Technology and Science*

**Abstract:Vehicular ad hoc networks (VANETs) undertake the general public Key Infrastructure (PKI) and certificate Revocation Lists(CRLs) for their protection. In thischallenge Expedite Message Authentication Protocol for VANETsis proposed which replaces time consuming CRL checkingmethod by using an efficient revocation checking procedure. Therevocation examine procedure in EMAP uses keyed Hash MessageAuthentication Code where the key utilized in calculating theHMAC is shared best between non revoked OBU. MoreoverEMAP uses a novel probabilistic key distribution which allows fornon revoked OBU to safely share and replace a secret key.EMAP can tremendously cut down the time consumed forchecking list and therefore the EMAP is demonstrated to be secureand efficient.**

**Keywords-**Vanets, security, public key infrastructure,revoke, OBU

## I. INTRODUCTION

VANETs consist of On-Board Units (OBUs) and Road-Side Units (RSUs).Vehicle-to-Vehicle (V2V) and Vehicleto-Infrastructure (V2I) communications are the two communication modes, which, respectively, allow OBUs tocommunicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels,many attacks such as injecting false information, modifying and replaying the disseminated messages can be easilylaunched. A security attack on VANETs can have severe harmful effect to legitimate users. A popular solution to secureVANET is use of Public Key Infrastructure (PKI), and Certificate Revocation Lists (CRLs) for managing the revokedcertificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitallysigned before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revokedcertificates. In a PKI system, the authentication of any message is performed by first checking if the sender's certificateis included in the current CRL, i.e. checking its revocation status then verifying the sender's and finally verifying thesender's signature on the received message. Security in VANET is crucial to take care before it is actually deploying intoreal time.

The paper proposes an EMAP protocol for secure communication in VANETS. EMAP uses a keyed Hash MessageAuthentication Code (HMAC) where the hash key is used in calculating the HMAC to provide security in vehicularcommunication. In a PKI system, the authentication of any message is performed by first checking if the sender'scertificate is included in the current CRL. The first part of authentication, which checks the revocation status of thesender in a CRL may incur long delay depending on CRL size and the employed mechanism for searching the CRL.

Vehicles communicate through wireless channels, a variousattacks such as injecting false information, modifying andreplaying the disseminated messages can easily launched.Incur long delay depending on the List size and employeddevice for searching the List. EMAP which replaces the Listexamining process by an effective revocation examineprocess using a fast and secure HMAC function. EMAP issuitable not only for VANETs but also for any networkemploying a PKI Model. To reduce the authentication delayresulting from checking the List in VANETs.Commercial applicationsneed security to protect the potential loss of revenue.Without security, a Vehicular Ad hoc network can be affectedby many attacks like denial of service, message suppressionand propagation of false message attacks etc. that may causeaccidents. VANETs are current emerging technology inwireless communication.

- Security is an important concern in VANETs,because they communicate a real time messagewhich has to reach destination on time and withouttampered.
- If such messages are altered by opponents, then itmay lead to false interpretation of the message andchances of risking once life is more.
- EMAP resists the opponents' attacks in VANETs andprovides authentication for the message withapproximately expected timing.
- The PKI system and List system are replaced withFast and secure Keyed Hash MessageAuthentication Code which cuts the delay.

## II. RELATED WORK

The Public Key Infrastructure (PKI) is the most viable technique to achieve these security requirements [4],[10] suchas entity authentication, message integrity, non-repudiation, and privacy preservation.In [10], Hubaux et al. identify the security and privacy challenges in VANETs, and indicate that a Public KeyInfrastructure (PKI) should be well deployed to secure the transmitted messages and to authenticate network entities.

In [11], Studer et al. propose an efficient authentication and revocation scheme called TACK. TACK adopts ahierarchy system architecture consisting of a central trusted authority and Regional Authorities (RAs) distributed all overthe network. After entering a new network, 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 signatureof the vehicle and ensures that the vehicle is not in the current Revocation List (RL). After the RA authenticates thevehicle, 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 certificateto the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period,which makesACK is not suitable for the safety applications in VANETs as the WAVE standard [7] requires each vehicle totransmit beacons about its location, speed, and direction every 100 ~ 300 msec. Also, TACK requires the RAs tocompletely cover the network; otherwise, the TACK technique may not function properly. This requirement may not befeasible especially in the early deployment stages of VANETs. Although TACK eliminates the CRL at the vehicles level,it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check therevocation status of a vehicle, the RA has to verify that this vehicle is not in the current Revocation List (RL) bypreforming a check against all the entries in the RL. Checking the revocation status of a vehicle may be a timeconsuming process. The authors suggested using an optimized search method to reduce the computation while RL check.There are some works addressing the problem of distributing the large-size CRL in VANETs.

## III. PROPOSED WORK

The proposed system ensures low end-to-end delay, lowOverhead and thus a better communication channel. TheEMAP apply a fas H-MAC function and novel key sharingtechnique employing probabilistic random key distribution.Expedite Message Authentication Protocol (EMAP) toovercome the problem of the long delay involved inexamining the revocation status of a certificate using a List.EMAP employs keyed Hash Message Authentication Code [HMAC] in the revocation checking process, where the key usedin calculating the H-MAC for every message is shared onlywithin unrevoked OBUs. In addition, EMAP is free from the
false positive property which is common for lookup hashtables. Extension of EMAP for bulk authentication in VANETsclearly reduces the communication overhead therebymaking the communication faster and easier

**System Design**

A Trusted Authority responsible for providing anonymouscertificates and sharing secret keys to all lists in the network.The Roadside units (RSUs) are fixed and it is distributed allover the network. RSUs will communicate securely with theAuthority and OBUs are equipped in vehicles. All the OBUscan communicate either with Other OBUs through V2Vcommunications or with RSUs through V2I communication.The system model under consideration is mainly a PKIsystem in which each vehicle has a set of anonymouscertificates used to secure its communications with otherparties in the network. In specific public key (PK), includedin the certificate and the secret key (SK) are used forchecking and signing messages. Each OBUs is preloaded witha set of asymmetric keys (secret keys in RSU and thecorresponding public keys in RSU). The keys are necessaryfor getting and maintaining a exchanged secret key $K_w$between unrevoked node.

**Message Authentication**:

The details of the Authority signature on a certificate and anOBU signature on a message are not discussed in this work,for the sake of generality, we brought up PKI system. Weonly focus in how to accelerate the revocation examiningprocess that is conventionally performed by checking theList for every certificate received. After that sender initiatewith message signing and verification between differentparties in the network are performed.

Authentication is performed by the following steps:

Message signing

**Verification**

1-RSU - Aided Verification

2-Batch Verification

**Revocation**

**Message Sign:**

A Trusted Authority responsible for providing anonymouscertificates and sharing secret keys to all lists in the network.The Roadside units (RSUs) are fixed and it is distributed allover the network. RSUs will communicate securely with theAuthority and OBUs are equipped in vehicles. All the OBUscan communicate either with Other OBUs through V2Vcommunications or with RSUs through V2I communication.The system model under consideration is mainly a PKIsystem in which each vehicle has a set of anonymouscertificates used to secure its communications with otherparties in the network. In specific public key (PK), includedin the certificate and the secret key (SK) are used forchecking and signing messages. Each OBUs is preloaded witha set of asymmetric keys (secret keys in RSU and thecorresponding public keys in RSU). The keys are necessaryfor getting and maintaining a exchanged secret key $K_w$between unrevoked node.

**Message Authentication:**

The details of the Authority signature on a certificate and anOBU signature on a message are not discussed in this work,for the sake of generality, we brought up PKI system. Weonly focus in how to accelerate the revocation examiningprocess that is conventionally performed by checking theList for every certificate received. After that sender initiatewith message signing and verification between differentparties in the network are performed.

Authentication is performed by the following steps:

- Message signing
- Verification

1-RSU - Aided Verification

2-Batch Verification

Revocation

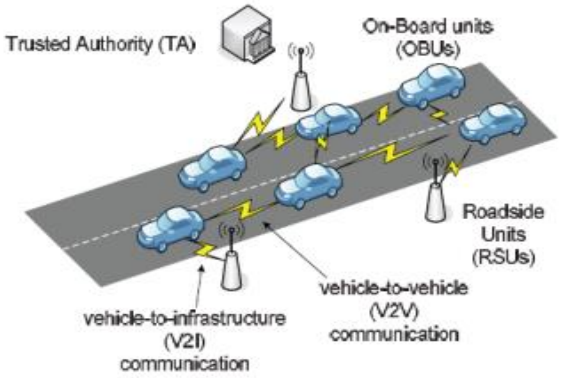
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Fig-1 System Initialization

**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'sand sender's signature.

**Message Verification:**
Receiving OBU checks the time stamp, sender signature,trusted authority signature. It calculates its own hash codeand check it with the sender's OBU to ensure messageauthentication.

**Rsu - Aided Verification:**
The List consists of set of revoked certificates. The certificatewhich belongs to the identity of each vehicle is revoked dueto the reasons like certificate expiration or any othervalidation problems. The certificates can be accepted onlywhen they are in state of non-revoked else it is considered asrevoked and the privacy-related message that is broadcastedis 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 belongsto their corresponding RSUs depending upon theirtimestamp value, the time when they get fixed to thenetwork. The certificate upgrade is performed through aTrusted Authority (TA), which forwards the new certificateto the requesting OBU through the available RSUs on theRoads. RSU does this verification rather than by Authority ina timely manner since RSU can securely communicate withAuthority. Due to this communication Overhead is reduced.Thus, the SM-MAP scheme Offers a distributed certificationservices. Finally, when a certificate is found to be revoked itmust progress the non-revocation process. Thereby it makesure fast revocation verifying process without any delay.

**Batch Verification:**
Considering the necessity for each vehicle to verify a largenumber of messages in a timely manner, SM-MAP introducesbatch verification method, which enables any vehicle tosimultaneously check number of messages in bulk. Theverification is done with help Of Secure Hash.

**Revocation:**

An important feature of the proposed EMAP will enable avehicle to upgrade its compromised keys corresponding topreviously missed revocation processes provided that itpicks one revocation process in the further. A rekeyingmethod id capable of updating compromised keyscorresponding to rekeying processes previously missed isintroduced.

## IV. CONCLUSION

EMAP has amodular feature rendering it inferable with any PKI system.Furthermore, it is resistant to common attacks whileoutperforming the authentication techniques retaining theconventional List. Consequently, EMAP can significantly lowerthe message loss ratio due to message verification delaycompared to the conventional authentication methodsemploying CRL checking

## REFERENCES

[l] P. Papadimitratos, Kung A, F. Kargl and J.P. Hubaux,"Privacy and identity Management for VehicularCommunication Systems: A Position Paper," Proc. WorkshopStandards for Privacy in User- Centric identity Management,July 2006.

[2] K. Sampigethaya, K. Matsuura, M. Li, R.. Poovendran andK. Sezaki, L Huang "CARAVAN: Providing Location Privacyfor VANET," Proc. Embedded Security in Cars (ESCAR) Conf.,Nov. 2005.

[3] A. Wasef, X. Shen, "An Efficient Distributed CertificateService 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-HocNetworks," Journal Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Y. Sun, , X. Lin, X. Shen, R. Lu, and J. Su, "An EfficientPseudonymous Authentication Method with Strong PrivacyPreservation 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, "PseudonymChanging at Social Spots: An Effective Strategy for LocationPrivacy in Vanets" IEEE Trans. Vehicular Technology, vol. 61no. 1, pp. 86-96, Jan. 2012.

[7] IEEE Std 1609.2-2006, IEEE Trial-Use Standard forWireless Access in Vehicular Environments – SecurityServices for Applications and Management Messages, IEEE,2OO6.

[8] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications andmanagement messages," IEEE Std 1609.2-2006, 2006.

[9] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[10] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks,"Proc. IEEE GLOBECOM'09, 2009.

[11] J. P. Hubaux, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 2, pp. 49–55, 2004.

[12] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy inVANETs," Proc. 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 invehicular networks," IEEE Journal on Selected Areas in Communications, vol. 25, pp. 1557–1568, 2007.

[14] P. P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicularcommunication systems," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 86–87,2008.

[15] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," Proc. 5thACM international workshop on VehiculAr Inter-NETworking, pp. 88–89, 2008.

Authors:

Divya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.

Sravya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.