Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Fast and Secure Message Authentication Protocol Using Hmac for Vanets

Santhosh Kumar B.J

M.Tech, Amrita Vishwa Vidyapeetham, Mysore Campus,
Karnataka, India

Abstract: Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation (withdrawal) 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.

Keywords: HMAC, CRL, EMAP

I. INTRODUCTION

In this system, a fast and secure that is, Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process is proposed. 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).

The application uses:

1) A novel probabilistic key distribution which enables non revoked OBUs to securely share and update a secret key.
2) It can decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL.

Vehicular Adhoc NETworks(VANETs) are a subset of MANETs (Mobile Adhoc NETworks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually
dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications). Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads. VANETs have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles.

VANETs consist of entities including On-Board Units (OBUs) and
infrastructure Road-Side Units (RSUs). Vehicle-to- Vehicle (V2V) and Vehicle-to Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs.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.

In this Application, EMAP (Expedite Message Authentication Protocol) for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC
(Hash Message Authentication Code) function is proposed.

The proposed EMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, EMAP has a modular feature rendering it integrable with any
PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, EMAP can significantly decrease the message loss ratio due to message verification delay
compared to the conventional authentication methods employing CRL checking.

II. SYSTEM ARCHITECTURE

Figure1.1 shows the system architecture of VANET model.

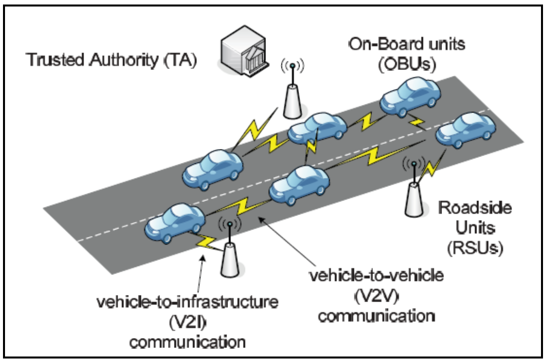

Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Figure 1.1

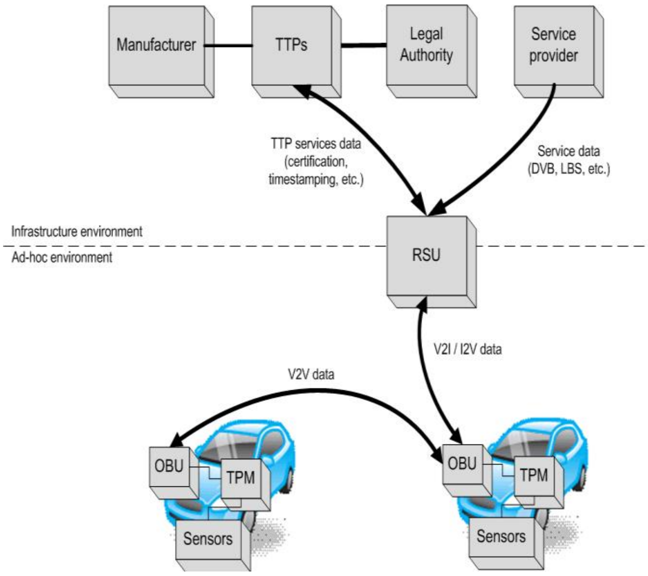


Figure 1.2

Vehicular ad hoc networks (VANETs) are a subgroup of mobile ad hoc networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Nodes are expected to communicate by means of North American DSRC standard that employs the IEEE 802.11p standard for wireless communication. To allow communication with participants out of radio range, messages have to be forwarded by other nodes (multi-hop communication). The primary VANET's goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings or – more generally – telematics information (like current speed, location or ESP activity) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze.

Vehicle registration and offence reporting.

Every vehicle in an administrative region should get registered once manufactured. As a result of this process, the authority issues a licence plate. On the other hand, it also processes traffic reports and fines. Trusted Third Parties (TTP) are also present in this environment. They offer different services like credential management or time stamping. Both manufacturers and the authority are related to TTPs because they eventually need their services (for example, for issuing electronic credentials). Service providers are also considered in VANETs. They offer services that can be accessed through the VANET. Location Based Services (LBS) or Digital Video Broadcasting (DVB) are two examples of such services. They are equipped with a communication unit(OBU, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of sensors to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance). These sensorial data can be shared with other vehicles to increase their awareness and improve road safety. Finally, a Trusted Platform Module (TPM) is often mounted on vehicles. These devices are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable internal clock and are supposed to be tamper-resistant or at least tamper-evident. In this way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored.

This application introduces an expedite message authentication protocol (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

HMAC process used in application.

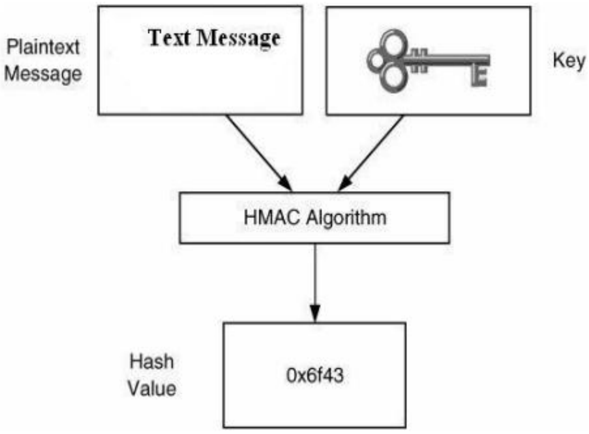


Figure 1.3

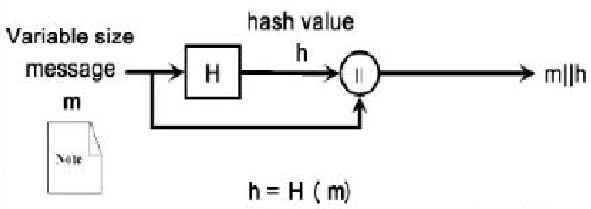


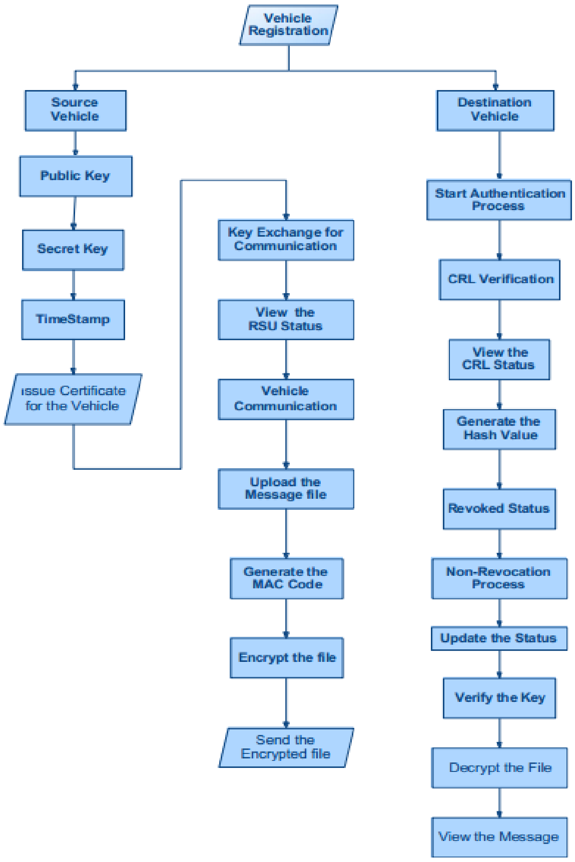
Figure 1.4

III. SYSTEM DESIGN

A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI).Use Certificate Revocation Lists (CRLs) for managing the revoked certificate.

In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificate. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message.

Verifiability.Data owner has to audit data integrity of the received data form the server.



Data flow Diagram
Vehicle-to-Vehicle (V2V) communication and
Vehicle-to-Infrastructure (V2I) communication
Expedite Message Authentication Protocol

Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication. In this Module, the two basic communication modes, which respectively allow

OBUs to communicate with each other and with the infrastructure RSUs. 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 well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificate. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificate. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate

is included in the current CRL, i.e., checking its revocation status, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message. MAP module contains the following important components.

I.Trusted Authority (TA): This is responsible for providing anonymous certificate and Distributing secret keys to all OBUs in the network.

II.Roadside units (RSUs): which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.

III.On-Board Units (OBUs): which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

Each OBU is equipped with a Hardware Security Module (HSM), which a tamper-resistant module is used to store the security materials, e.g., secret keys, certificates, etc.

System initialization
After system initialization
The TA has the following:

- A secret/private key pool
- The corresponding public key
- A master secret/private key and the corresponding public key.
- The secret key
- A set of hash chain values

Each OBU will have the following:

- A set of anonymous certificates used to achieve privacy-preserving authentication.
- A set of secret keys The set of the public keys corresponding to the Secret/private keys.
- The secret key which is shared between all the legitimate OBUs.

Since the system model under consideration is mainly a PKI system, where each OBU has a set of anonymous certificates used to secure its communications with other entities in the network. In specific, the public key included in the certificate, and the secret/private keys are used for verifying and signing messages respectively. Also, each OBU is preloaded with a set of asymmetric keys (secret/private and the corresponding public keys). Those keys are necessary for generating and maintaining a shared secret key between unrevoked OBUs.

Message Authentication and Message Signing process.

Step1:
Before any OBU_u broadcasts a message M, it calculates its revocation check Rev_{check}
$Rev_{check= HMAC(Kg,PIDu||}T_{stamp)}$
where
PID_u is the vehicle ID
T_{stamp} is the current time stamp, and
$Rev_{check= HMAC(Kg,PIDu||}T_{stamp)}$ is the hash message authentication code on the concatenation of PIDu and Tstamp using the secret key k_g

Step2: **Message Verification**
Any OBU_u receiving the message
$M \| T_{stamp|| cert(PID,PKu,}Sig_{TA,(PID|| PKu))||}\ Sigu(M\| T_{stamp)||}\ Rev_{check\ amd\ Kg}$
Can do the Message verification as follows:

```
1: check the validity of $T_{stamp}$
2: if invalid then
3:    Drop the message
4: else
5:   check $Rev_{check= HMAC(Kg,PIDu||}T_{stamp)}$
```

```
6: if invalid then
7:     Drop the message
8: else
9: verify the TA signature on $CERT_{OBUu}$
10: if invalid then
11:     Drop the message
12: else
13: verify the signature $sig_u$ (M|| $T_{stamp)}$ using
        OBUu,public key PKu
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
```

In step (5), OBUu calculates HMAC(Kg,PIDu ∥ Tst$\boldsymbol{amp}$) using its $\boldsymbol{K}$g on the concatenation PIDu ∥ Tst$\boldsymbol{amp}$, and compares the calculated H$\boldsymbol{M}$AC(Kg,,PIDu ∥Tst$\boldsymbol{amp}$) with the received $\boldsymbol{Re}$v$_{\boldsymbol{c}heck}$

Source vehicle

Form 1: Register

1. Registration of vehicle by entering vehicular ID and signature ID is done.
2. Generating key for communication by Trusted Authority(TA).
3. Trusted Authority issues a certificate to registered vehicle.
4. TA maintains a list of registered vehicles.

Form 2:

1. Key exchange for secure communication between source and destination vehicles.
2. Verifying the RSU status(RSU1 or RSU2) of communicating vehicles

Form 3:

1. Uploading a notepad file to be transferred from source to destination.
2. Encrypting the uploaded file and sent over the channel.

Destination vehicle

Form 4:

1. Message authentication process is started.

Form 5:

1. CRL status verification is done.

Form 6:

1. Updating Hash chain and Non Revocation process
2. Updating Secret key.

Form 4:

1. Verifying whether the vehicle is authentic.
2. Decrypting the received file.
3. Verifying the integrity of received file.
4. Receiving the decrypted file.
5. Viewing the contents of received file.

IV. CONCLUSION

The values of the hash chains are continuously used in the revocation processes, and hence, the TA can consume all the hash chain values. As a result, a mechanism to replace the current hash chain with a new one is used. After using the last value in the current hash chain, the TA generates a new hash chain. To forge the revocation check of any on board unit which uses HMAC function, an attacker has to find the current problem, the TA secret key and signature.

Since HMAC is irreversible, the revocation check, TA message and signature are unforgeable.

Each message of an OBU includes the current time stamp in the revocation check value; an attacker cannot record revocation check at time T and replay it at a later time to pass the revocation checking process as the receiving OBU compares the current time with that included in the revocation check. Hence EMAP is secure against replay attacks.

A legitimate OBU colludes with a revoked OBU by releasing the current secret key such that the revoked vehicle can use this key to pass the revocation check process by calculating the correct HMAC values for the transmitted messages. All the security materials of an OBU are stored in its tamper-resistant Hardware Security Module (HSM). Also all the key update processes are executed in HSM and only encrypted keys are transmitted and can be decrypted only by the OBU not in the CRL.

Since it is infeasible to extract the security materials from the tamper-resistant HSM,an unrevoked OBU cannot collude with a revoked OBU by releasing the current secret key to the revoked OBU. Hence EMAP is secure against colluding attacks.

V. FUTURE ENHANCEMENT

To provide Usage of High security cryptographic Using Blowfish algorithm, which is 448 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security. Data Integrity checking. It helps to ensure the data owner’s data being stored in the cloud is valid or not. Data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many researches are yet to be identified in future.

REFERENCES

[1] Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow, “EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 1, JANUARY 2013

[2] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.

[3] 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.

[4] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

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

[6] 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.

[7] “Network security essentials-Applications and standards”-, Prentice hall, 2007 edition, by William Stallings.
“Cryptography and Network security –Principles and practices”-, Prentice hall, 4th edition, 2006 ,by William Stallings.