Fast and Secure HMAC Function Message Authentication Protocol for Vehicular Ad Hoc Networks

Tushar R Vataliya
Department of Computer Science & Engineering
Narnarayan Shastri Institute of Technology, Jetalpur, Gujarat, India

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.

Keywords: Vehicular ad hoc networks (VANETs), Public Key Infrastructure (PKI), Expedite Message Authentication Protocol (EMAP)

I. INTRODUCTION

Vehicular Ad-hoc Networks are special case of Mobile Ad-hoc Network (MANET). MANET networks are multi hop mobile networks with dynamic topology. VANET is an ad-hoc network which is formed between vehicles as per their need of communication. VANET uses road topology. VANETs have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANET consists of two basic components: vehicle and infrastructures. 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 [8].

Since vehicles communicate through wireless channels, a variety of attacks can be easily launched. A security attack on VANETs can have some harmful effects to legitimate users. So, ensuring secure vehicular communications is to be done before any VANET application can be put into practice. 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. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates.

According to the Dedicated Short Range Communication (DSRC) [1], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telemetic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an inevitable challenge to VANETs.

To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages [8], each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol1 (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.

All rights reserved by *www.ijste.org*

II. RELATED WORK

A. ASIA: Accelerated Secure in Network Aggregation[1]

In order to reduce the computation overhead in the secure vehicular ad-hoc networks this paper introduces an innovative technique called ASIA as an effective and efficient scheme for securing data aggregation in VANETs. This approach can dramatically accelerate message verification because it mainly relies on hash operations which are several orders of magnitude faster than the digital signature scheme. It is able to largely reduce both communication and computational overhead compared to previous strategies. ASIA consists of two basic security mechanisms: Aggregate Consistency Check (ACC) and Generation-Skipping Verification (GSV). Our idea in designing ACC is providing security through introducing redundancy into the aggregation data flow. To this end, we use a directed a cyclic graph (DAG) as the aggregation structure instead of the commonly used tree graph [1]. When performing aggregation in a DAG, one node sends its messages to multiple upstream nodes. Messages with identical content flow through network and will reach eventually a common node which can compare the received messages to detect potential misbehavior during the aggregation process

B. VANET RBC, DSDV, AODV

In this paper performance of three routing protocols namely Ad-hoc On Demand Distance Vector Routing (AODV), Destination Sequence Distance Vector (DSDV) and VANET Radio Broadcasting Protocol (VANETRBC) is compared for various parameters [10]. Here, DSDV protocol is a table driven protocol while AODV is on demand protocol. VANETRBC is a general radio broadcasting protocol taken into consideration. To decide the protocols is a challenge as per author reference. All these three protocols are compared with the help of IEEE 802.11p standard using NS-2.33(Network simulator – 2.33) as per author.

C. Destination Sequenced Distance –Vectors Routing (DSDV)

DSDV[10] is proactive i.e. table driven routing protocol scheme. The contribution of this is to solve routing loop problem as per author. DSDV solves major problems associated with Distance Vector routing of wired networks as per author. Each entry in the routing table contains sequence numbers. Initially every vehicle broadcasts its own routing tables to its adjacent vehicles. The neighbor vehicles updates the routing table with the help of two types of packets namely Full Dump packets and Incremental Normally Full Dump packets which contain information about every participating vehicle in the VANET.

D. AdHoc –On Demand Distance Vector Protocol (AODV):

It is very simple, effective, source initiated and very efficient which do not uses fixed topology as per author [10]. This protocol uses on demand route discovery and route maintenance from DSR and hop by hop routing from DSDV. In this every node in the network maintains a routing table with the routing information entries to its neighboring nodes and two separate counters. A node sequence number and a broadcast id. AODV provides unicast, Broadcast and Multicast communication. All the routes are loop free through use of sequence numbers. On demand route establishment with this protocol is achieved with small delay.

E. TESLA++

TESLA++ is a more efficient and advanced form of Timed Efficient Stream Loss-Tolerant Authentication (TESLA)[11]. TESLA++ is functionally more efficient and more secure than TESLA. TESLA++ has the following advantages over TESLA: (i) TESLA++ prevents occurrence of memory based Denial of Service (DoS) attacks which are prevalent in TESLA. (ii) TESLA++ reduces the memory requirements at receiver's end without affecting the efficiency of its broadcast authentication mechanism. (iii) TESLA++ not only prevents the memory based Denial of Service (DoS) attacks but also the computation-based Denial of Service (DoS) attacks with equal priority. TESLA++ is similar to TESLA in functioning. The mechanism for broadcast authentication in TESLA++, just like in TESLA, uses symmetric cryptography and delayed key disclosure. TESLA++ offers reduced memory requirements at receiver's end as the receiver need not to store all the Message Authentication Codes but only the self generated ones. In TESLA++ Message Authentication Codes are broadcasted earlier than the message and the corresponding keys

F. ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematically derived form of Digital Signature Algorithm (DSA)[11]. It is a mathematical representation for the elliptic curve analogue of the DSA. It has been accepted as a standard worldwide. It is an ANSI standard, as well as IEEE, NIST and ISO standard. The strength per key bit is significantly greater in an algorithm using elliptic curves because elliptic curve discrete logarithm problem has no sub exponential-time algorithm.

All rights reserved by *www.ijste.org*

Being a mathematical entity, the security of elliptic curve can be described in mathematical terms only. The computational intractability and mathematical hardness of the ECDLP contributes towards its security. It is advantageous to use ECDSA to provide secure and faster dissemination of information after authenticating the users in environments where amount of storage offered is less and lesser response time is allocated for user authentication. Asymmetric ECDSA key pair is used in VANET systems to provide User Authentication. ECDSA can also be used to generate and verify signatures. This was the first paper that explained ECDSA to minute details. We have provided an account of important findings of that paper related to User authentication. As per the words of the authors, ECDSA uses an asymmetric key pair of a public key and a private key. The public key is a random multiple of the base point, while the private key is the integer used to generate the multiple. Though ECDSA reduces the scope of attacks from malicious users, but still we need to dedicate a lot of research efforts to further improve the security of the ECDSA system.

III. EXISTING SYSTEM

According to the Dedicated Short Range Communication (DSRC) [6], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an inevitable challenge to VANETs. To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate.

A. Limitations of Existing System

- 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.
- To abstain the leakage of the real identities and location information of the drivers from any external eavesdropper.
- The scale of VANET is very large.

IV. PROPOSED WORK

A. Overview of Proposed Work

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 enables OBUs to securely share and update a secret key[7]. EMAP decrease the message loss ratio due to the message verification delay compared with the CRL. The messages that can be verified using EMAP within 300 msec. EMAP is secure and efficient.
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.
1) System Consists:

1) A Trusted Authority-which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.
2) Roadside units (RSUs)-which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
3) OBUs-which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

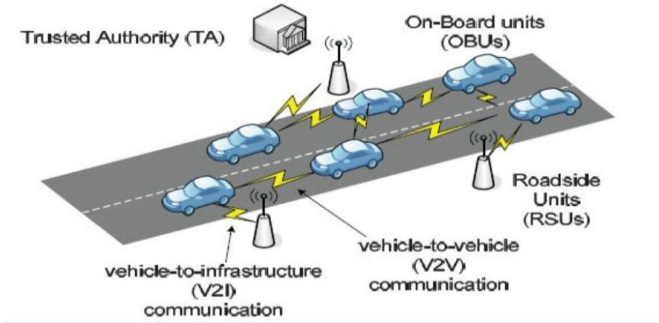

Fig. 1: System Architecture

All rights reserved by *www.ijste.org*

B. Linear Search Algorithm

Linear search algorithm, the revocation status of a certificate is checked by comparing the certificate with each entry in the CRL. If a match occurs, the certificate is revoke otherwise it is unrevoked.

C. Binary Search Algorithm

Binary search algorithm[8] works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted database of the revoked certificates included in previous CRLs and the recently received CRL. The main idea of the binary search Algorithm is to cancel out half of the entries under consideration after each comparison in the search process. In the binary search the revocation status of a certificate is checked by comparing the identity of the certificate with middle value of the sorted database. This Process continues until a match is found, i.e., the certificate is revoked, or the process is finished without finding a match which means that the certificate is unrevoked.

D. Work Flow of Proposed Work

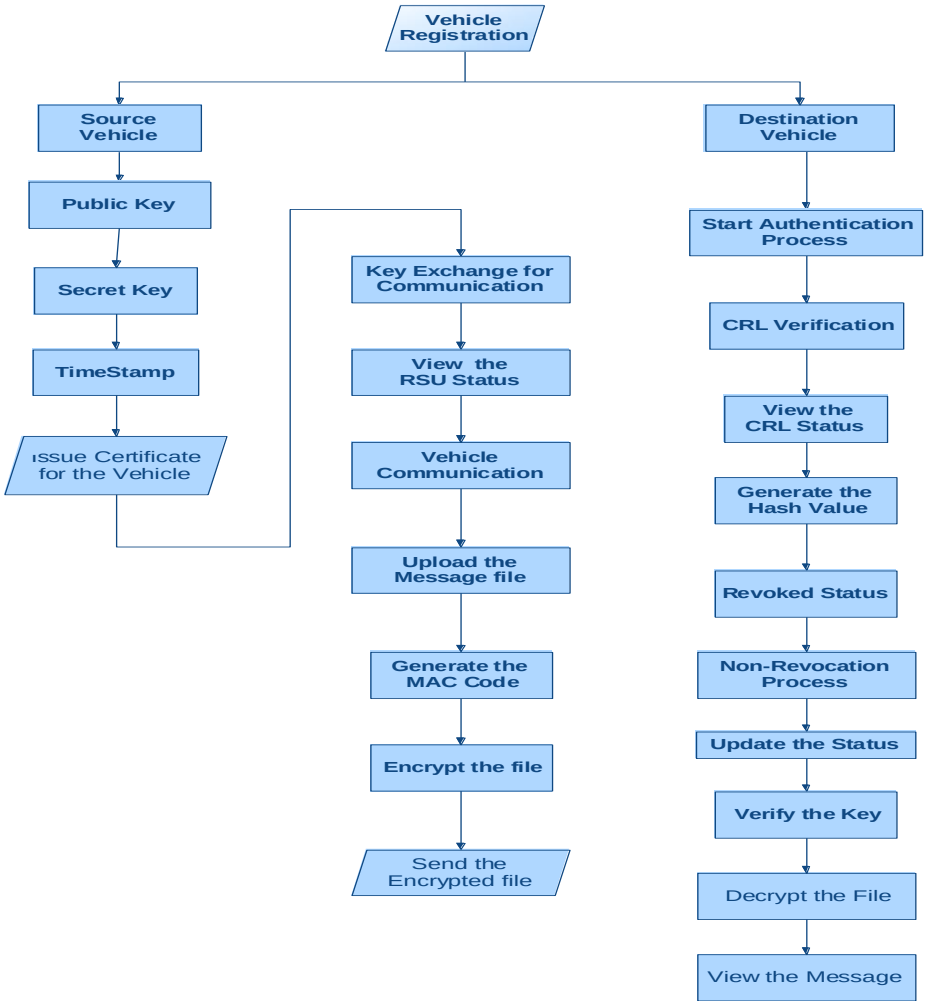

Fig. 2: System Flow

V. PERFORMANCE EVALUATION

The computation complexity of the revocation status checking process is defined as the number of operations required to check the revocation status of an OBU. Nrev used to denote number of revoked certificates in a CRL. To check the revocation status of an OBU using the linear search algorithm, an entity compare the certificate identity of OBU with every certificate of the Nrev certificates in the CRL. The entity performs one-to-one checking process. The linear search algorithm performs revocation checking for OBU. In the binary search algorithm, the certificate identity of OBU is compared to the certificate identity in the middle of the sorted CRL. The certificate identity of OBU is greater than that of the entry in the middle, and then half of the CRL with identities lower than that of OBU are discarded from the comparisons. Certificate identity of OBU is lower than that of the

All rights reserved by *www.ijste.org*

entry in the middle, then half of the CRL with identities higher than that of OBU are discarded. The checking process is repeated until a match is found or the CRL is finished.

A. End To End Delay

To further evaluate EMAP, we have conducted ns-2 simulation for the city street scenario. We select the dissemination of the road condition information by an OBU every 300 msec to conform with the DSRC standards. The mobility traces adopted in this simulation are generated using NS 2. We are interested in the end-to-end delay, which is defined as the time to transmit a message from the sender to the receiver. Figure shows the end-to-end delay in msec versus the OBUs density, by employing authentication using the proposed EMAP (HMAC), the linear CRL checking, and binary CRL checking, respectively. In the simulation, we consider CRLs containing 20,000 and 30,000 revoked certificates, respectively, and the OBUs density as the number of OBUs per km. It can be seen that the end-to-end delay increases with the OBUs density because the number of the received packets increases with the OBUs density resulting in longer waiting time for the packets to be processed by the application layer in each OBU. In addition, the end-toend delay tends to be constant for high OBUs densities as the number of received packets reaches the maximum number of packets an OBU can verify within a specific duration. The end-to-end delay also increases with the number of revoked certificates included in the CRL for the linear CRL checking process. However, the end-to-end delay is almost constant with the CRL size using the binary checking process as the number of comparison operations needed to check CRLs with 20,000 and 30,000 certificates is almost the same. From figure, employing the proposed EMAP in authentication reduces the end-to-end delay compared with that using either the linear or the binary CRL checking process.

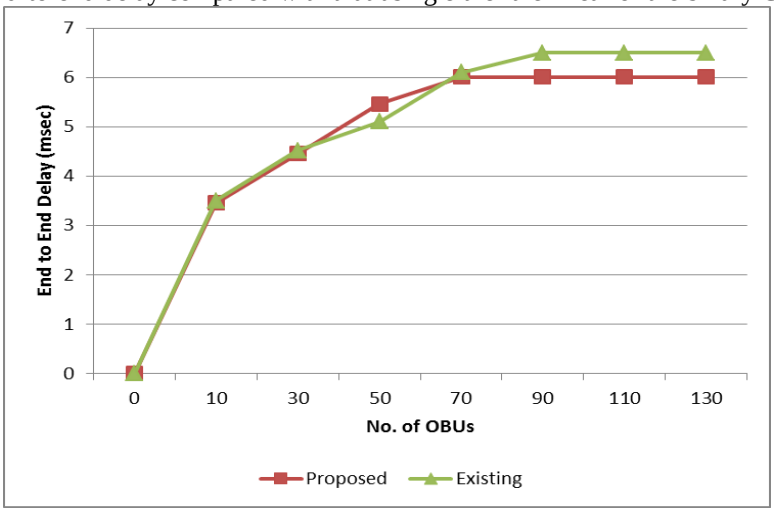

Fig. 3: End to End delay

VI. CONCLUSION

We have proposed EMAP for VANETs, which expedites message authentication by replacing the time consuming CRL checking process with a fast revocation checking process employing HMAC function. 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. Our future work will focus on the certificate and message signature authentication acceleration.

REFERENCES

[1] The Security in the Vehicular Ad Hoc Network (VANET). Alisherov, Farkhod. 2, s.l. : Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, 2011, Vol. 1. 99-106.
[2] Security Enhancement based on (HMAC) Hash Message Authentication Coding for Vehicular Adhoc Networks. Nagarjuna Narsimha Chary, K.Gnana Mayuri. 7, s.l. : International Journal of Technology and Engineering Science [IJTES], 2014, Vol. 2. 2068-2073.
[3] Secured Multi Message Authentication Protocol for Vehicular Communication. C.SelvaLakshmi, N.Senthil Madasamy, T.Pandiarajan. 12, s.l. : International Journal of Advanced Research in Computer and Communication Engineering, 2013, Vol. 2. 2278-1021.
[4] Secure Network Discovery Using Expedite Message Authentication in VANET. Ashwini N H, Anand S Uppar. 5, Karnataka : IJCAT International Journal of Computing and Technology, 2014, Vol. 1. 2348 - 6090.
[5] PERFORMANCE EVALUATION OF RADIO PROPAGATION MODEL FOR VEHICULAR AD HOC NETWORKS USING VANETMOBISIM AND NS-2. Ramesh C. Poonia and Vikram Singh. 4, s.l. : International Journal of Distributed and Parallel Systems (IJDPS) , 2012, Vol. 3.

All rights reserved by *www.ijste.org*

[6] Infrastructure based Authentication in VANETs. Brijesh Kumar Chaurasia and Shekhar Verma. Allahabad : International Journal of Multimedia and Ubiquitous Engineering, 2011, Vol. 6.
[7] EMAP: EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS. Aspari Nagaraju, Om Prakash, K. Prasanth Kumar. 10, 2014, Vol. 4. 2277-2685.
[8] EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. Albert Wasef and Xuemin (Sherman) Shen. 1, s.l. : IEEE TRANSACTIONS ON MOBILE COMPUTING, 2013, Vol. 12.
[9] DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks. Albert Wasef, Yixin Jiang, and Xuemin Shen. 2, s.l. : IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2010, Vol. 59.
[10] Comparative Analysis of VANET Routing Protocols Using VANET RBC and IEEE 802.11p. A. N. Mahajan, Dr. Reena Dadhich. 4, s.l. : International Journal of Engineering Research & Applications(IJERA), 2013, Vol. 3. 2248-9622.
[11] A survey on securing user authentication in vehicular ad hoc networks. Mrs. Arzoo Dahiya, Mr. Vaibhav Sharma. 5, Gurgaon : IJSRD, 2013, Vol. 11.
[12] Comparative Study of Simulators for Vehicular Ad-hoc Networks. Narendra Mohan Mittal, Savita Choudhary. 4, Haryana : International Journal of Emerging Technology and Advanced Engineering, 2014, Vol. 4. 2250-245

All rights reserved by *www.ijste.org*