EFFICIENT VANET COMMUNICATION USING EMAP

S.FATHIMABEE[1], J.SUGANYA[2]
PG Scholar[1], Assistant Proferssor[2]
Department of Electronics and Communication,
Mailam Engineering College, Mailam
Villupuram, Tamil Nadu, 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. It is proposed that 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 nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked 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.**

***Index Terms*-Vehicular networks, message authentication, certificate revocation.**

I. INTRODUCTION

A 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. 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. Asecurity attack on VANETs can have severe harmful or fatal consequences to legitimate users.

To ensure the 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. In this paper, we introduce 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 delayresulting from checking the CRL in VANETs. The rest of the paper is structured as follows. In Section 2, an overview of existing VANET communication process and EMAP using VANET communication as described . In Section 3, we introduce EMAP with AODV protocol. In Section 4, we described our study network performance and results and evaluations are also explained in the same section. Finally, Section 5 concludes the paper.

II. VANET COMMUNICATION USING EMAP

A. GENERAL VANET COMMUNICATION PROCESS

In Existing works, we consider both nonoptimized and optimized search algorithms. According to the Dedicated Short Range Communication (DSRC) [10], 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.we have proposed EMAP for VANETs, which expedites message authentication by replacing time consuming CRL(Certificate Revocation Lists) checking process with a fast revocation checking process employing HMAC function. The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

A VANET environment consists of vehicle nodes and Road Side Units (RSUs). It is mainly used to model communication in a Vehicular environment where the vehicles are considered as VANET nodes with wireless links.Communication from the source can either directly reach the destination directly or through an intermediate node which may be a router or a road side unit. All vehicles use a communication device known as On Board Units (OBUs) equipped with GPS (Global Positioning System) which is used to track the vehicles.OBUis used to communicate with the OBU in other vehicles and also with roadside units. The roadside units are connected with backbone network. Thus VANET provides both Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Infrastructure communication (V2I).The moving vehicles have access to internetthrough the backbone network. The vehicles of a VANET are equipped with DSRC (Dedicated Short Range Communication). Vehicles can move along the same road way and transmit information or receive information. The movement of the vehicles is limited by the road condition such as narrow or curved.

III. VANET COMMUNICATION USING EMAP BASED ON AODV PROTOCOL

A. *Motivation*

Vehicular communications using EMAP for VANET which replaces time consuming CRL checking process by an efficient revocation checking process.The proposed EMAP inauthentication reduces the end-to-end delay compared with that using either the linear or the binary CRL checking process.To detectthe passenger safety by using the Random key Exchange between the nodes.

The VANET communication using EMAP is to provide message authentication and to increase communication between the vehicles in timely manner. We propose an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. EMAP is suitable not only for VANETs but also for any network employing a PKI system.A well recognized solution to secureVANET is to deploy Public Key Infrastructure (PKI) and to use Certificate Revocation Lists (CRL) for managing revoked certificates. In PKI, each entity in the network hold 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.In a PKI system, the authentication of message is performed by checking if the sender certificate is included in the current.

In this mechanism VANET communication using five modulessuch as VehicleRoute Construction,Centralized server, Priorities based Vehicle movement, Identify the traffic and accident, Alertnate and Best Path Identification.The proposed EMAP is authenticating entity to communicate securely and quickly.The sender/requester will give the request to the PKI system.If the request is deny access,then go back to the sender otherwise access the process.Then the PKI security system is to check the traffic and accident details also.The EMAP is used to identifying possible routes and allocate the available routes.

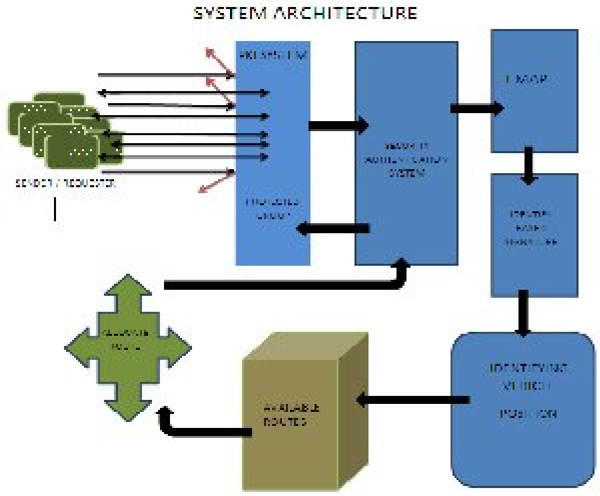


Fig.1.System Architecture

Identifying vehicle position is based on the indicating signal that is vehicle ID which shows the position of vehicle. So that the user can know that the traffic has been occurred in the specific path. In Available routes, the user will take an alternative route to reach their destination. Those intimation will flow the Server maintaining and monitoring for each and every vehicles in the entire network. Allocation of routes are user can give a request to the server regarding the source and destination information that they want to travel. The server will display the best path identification to reach the destination. The user can priory knows about the traffic in the specific location and takes alternate/best route to reach the destination.

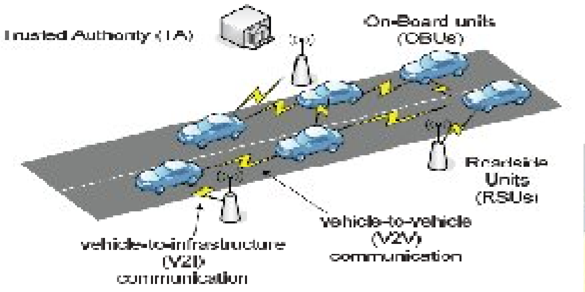

Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Fig. 2.System model

As shown in Fig 2, the system model under consideration consists of the following:

A Trusted Authority (TA), which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA. It is a router between vehicle on the road and connected to other devices.On Board Unit(OBUs), which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications orWith RSUs through V2Icommunications.Vehicle to Vehicle communication: Applications transmit messages from one vehicle to another.Vehicle to/from Infrastructure communication: Applications in which messages are sent either from vehicle to a Road Side Unit (RSU) or vice versa.

B. AODV Protocol

AODV is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicastrouting.

In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a linkfails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network.

As shown in Fig.3.Node A wants to initiate traffic to node J for which it has no route. A transmit of a RREQ has been done, which is flooded to all nodes in the network. When this request is forwarded to J from H, J generates a RREP.This RREP is then unicasted back to A using the cached entries in nodes H, G and D. AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables.

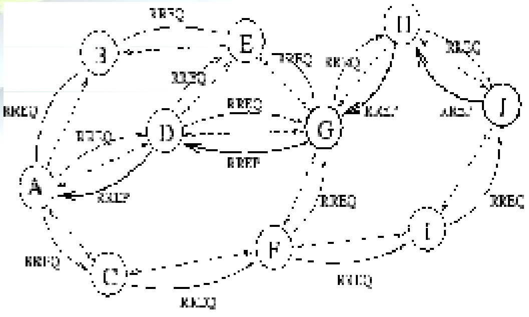


Fig. 3.AODV route lookup session

A node getting the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicast a RREP back to the source . Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination .Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables.If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destinations. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery. Multicast routes are set up in a similar manner. The counting to infinity problem is avoided by AODV from the classical distance vector algorithm by using sequence numbers for every route.

IV. PERFORMANCE EVALUTION

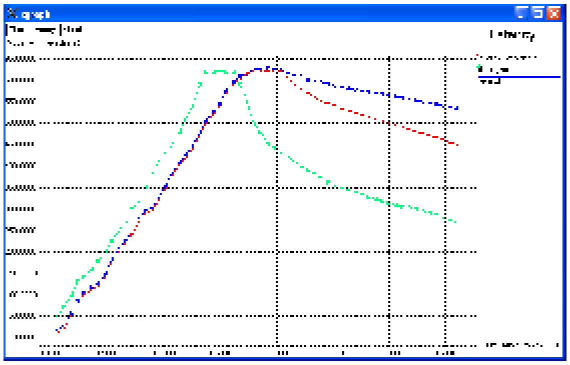
A. *Performance metrics*

The performance metrics which is defined to considered for the simulationexperiments are as follows

1) *Throughput:* It represents the average rate of successful message delivery over a communication channel. It is usually measured in bits per second (bits or bps), and sometimes in data packets per second or data packets per time slot.

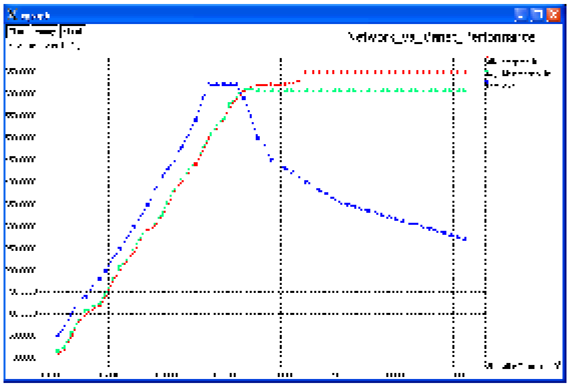
2) *Average end-to-end (E2E) delay:*It represents the timeto transmit a message from sender to the receiver.

A. VANET Vs THROUGHPUT



In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. VANET communication using EMAP to overcome the process of authentication end to end delay, time consuming CRL checking process and also increase the throughput than conventional method

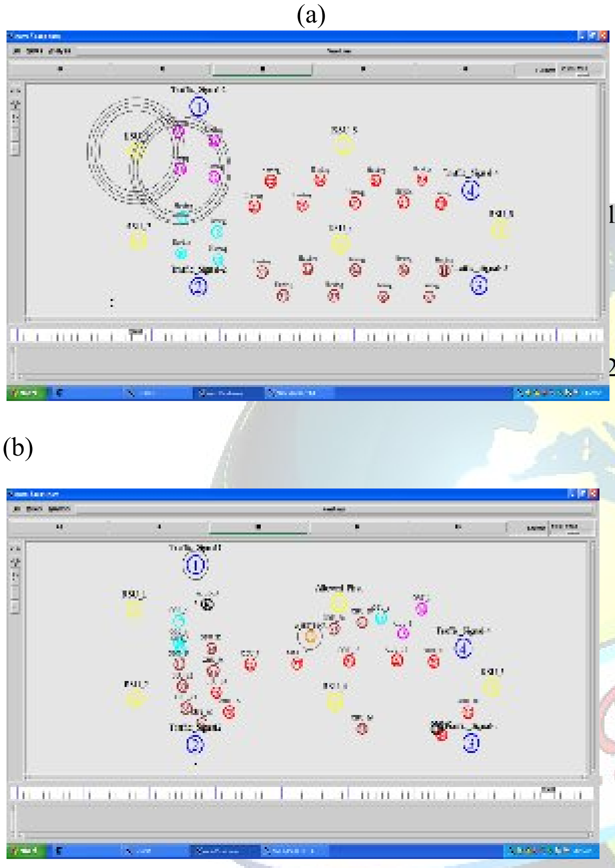
B. NETWORK Vs VANET PERFORMANCE



The System performance is improved by using based on the EMAP protocol, and also VANET transmission increases with reducingauthentication end to end delay.

B. *Simulation results*

The proposed model is simulated in Network Simulator (NS) version 2.29. NS is a discrete event simulator targeted at networking research. NS provides substantial support for simulation of TCP (Transmission Control Protocol), routing, and multicast protocols over wired and wireless (local and satellite) networks. For this project, Network Simulator runs on Windows XP using Cygwin. The simulation setup consists of a number of movable nodes. Two ray ground propagation models are employed. The MAC type used is 802.11 and logical link layer type is utilized. The antenna model is Omni-directional. Routing protocols include Ad hoc Ondemand Distance Vector protocol (AODV).



(a)

(b)

Fig. 4.(a) Consists of vehicle construction,Packet transmission in VANET (NAM-Network Animator Window) (b)In VANET Communication, Movement of Priority Vehicle.

V. Conclusion

The 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.

References

1] 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.

2]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.

[3]A. Wasef and X. Shen, “EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad HocNetworks,” IEEE Trans. VehicularTechnology, vol. 58, no. 9, pp. 5214-5224, Nov. 2009.

[4]A. Wasef and X. Shen, “MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE GlobeCom, 2009.

[5]D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” Int’l J. Information Security, vol. 1, no. 1, pp. 36-63, 2001.

[6]J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,”Proc. Sixth ACM Int’l Workshop Vehicular InterNET working, pp.89-98, 2009.

[7] K.P. Laberteaux, J.J. Haas, and Y. Hu, “Security Certificate Revocation List Distribution for VANET,” Proc. Fifth ACM int’l Workshop Vehicular Inter-NETworking, pp. 88-89, 2008.

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

[9] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of Misbehaving and Faulty Nodes in Vehicular Net- works,” IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557- 1568, Oct. 2007.

[10]P.P. Papadimitratos, G. Mezzour, and J. Hubaux, “Certificate Revocation List Distribution in Vehicular Communication Sys- tems,” Proc.Fifth ACM Int’l WorkshopVehicular Inter-NETworking,pp.86-87, 2008.

[11]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 IdentityManagement, July2006.

[12]R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “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.

[13]“The Network Simulator - ns-2,” http://nsnam.isi.edu/nsnam/index.php/UserInformation, 2012.

[14] “Traffic and Network Simulation Environment - TraNS,” http:// trans.epfl.ch, 2012.