ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

HMEP: Hasten Message Endorsement Protocol for Vehicular Ad hoc Networks

D.Thriveni[1], G.T.Prasanna Kumari[2]

[1] M.Tech Student, S.V.Engineering College for Women, Tirupati, India

[2] Associate Professor, Dept. of CSE, S.V. Engineering College for Women, Tirupati, India

ABSTRACT: Vehicular Ad hoc Network (VANET) governs a customer to maintain intelligent transportation system to reduce traffic congestion & Accidents. In presence of Honored Authority message encrypted with receiver's public key appending with sender's certificate retraction list and signature. Delay occurs at receiver side due to authenticate the sender's certification from large size of Certificate Retraction List (CRL) & signature. To reduce this delay we present Hash Message Endorsement Code (HMEC) where the key used to calculate the HMEC is shared only between non-revoked On-Board Units (OBUs) to securely share and update the secret keys. With this we can eradicate Message Endorsement loss compare to previous approach.

KEYWORDS: certification revocation list, on-board units, digital signature, public key infrastructure, hash-based message endorsement.

I.INTRODUCTION

Vehicular Ad hoc Network (VANET), a subclass of Mobile Ad hoc Networks (MANETs), is a promising approach for future Intelligent Transportation System (ITS). These networks have no fixed infrastructure and instead rely on the vehicles themselves to provide network functionality. Vehicular ad hoc networks consist of entities including On-Board Units (OBUs) and Infrastructure Road Side Units (IRSUs) are part of vehicular communications network. A honored authority was responsible for all the vehicles registered in that region i.e., national territory, state, cities, towns etc., police cars and any other public vehicles which are appointed for public service may have specific roles and be considered as mobile infrastructure units.

VANET will enable both Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications. The OBUs which are embedded with the vehicles can communicate with each other vehicle and with the Infrastructure Road Side Units (IRSUs). Since Vehicles can communicate through wireless links the broadcast messages can be easily launched and a variety of dangerous attacks such as giving false information are occurred.

Vehicular ad hoc networks (VANETs) are special cases of mobile ad-hoc networks(MANETs), and mainly consist of On-Board Units (OBUs) and Infrastructure Roadside Units (IRSUs) .OBUs are installed on vehicles to provide wireless communication capability, and IRSUs are deployed and managed by the Honored authority (HA). VANETs are expected to improve the safety of roads and optimize traffic management, however, there are also many challenges such as information security and privacy preservation. For example, vehicles need to exchange speed and location information in the driving assistance and accident warning applications. The endorsement for such life-critical information is essential, which can make sure that any received message is indeed sent by a right user and has not been changed or erased.

However, significant challenging factor to be met is a security which is a critical factor. A well known solution for the security issue in VANETs is to distribute the Public Key Infrastructure (PKI) and using Certificate Retraction Lists (CRLs) for managing the retracted certificates. In PKI, each entity in the network is having an reliable certificate, and every

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

message in the Certificate Retraction List should be digitally signed before it is transmitted. A CRL, usually issued by a Honored Authority (HA), is a list containing all the retracted certificates

In PKI system, the Endorsement of any message is performed by first checking if the sender's certificate is included in the current Certificate Retraction List. Endorsement in this may takes long postponement depending on the size of the CRL and the working procedure for searching the current certificate in the CRL. Unluckily, the size of the CRL is awaited to be large in order to store the privacy of the drivers, to avoid the leakage of the real and right identities and location information of the drivers from any external hearer, each OBU should be preloaded with a set of unsigned digital certificates, where the OBU has to periodically change its unsigned certificates to misdirect attackers. Therefore, retraction of an OBU results in retracting all the certificates carried by that OBU leading to large increase in the CRL size.

II. PROTOCOLS IN VEHICULAR AD HOC NETWORKS

PPGCV: Wasef and Shen proposed Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks. The primary goal of PPGCV for vehicular ad hoc networks is to provide provisional full statelessness equity, which make this to be reliable, efficient and scalable. Privacy is the thing which is mainly associated to covering the real identity and secures the area details of the vehicle users. Hiding the user area information which is necessary, but the message delivered by the vehicles contains sufficient details, such as point of the vehicle, speed and direction of the vehicle. So the association broadcasting is one of the auspicious ways to reach the target. But main problem in this group communication is how updating the associative key in a protected and positive way.

GKMPAN: Zhu, Setia, Xu, and Jajodia proposed An Efficient "Group Rekeying Scheme for Secure Multicast in Ad-hoc Networks" for Vanets. The major efficient property in this is the key assistant does not need any information about the topology of the ad hoc network. The most efficient approach for getting secured associated broadcasting is to service a balanced associated key that is mutual by all the points for data encryption. The major target is to form an effective association rekeying plan that build up the adjusted keys effectively once the adjusted nodule are identified. The pattern should enable the non-adjusted nodule to refuse false group keys inserted by adjusted nodules. The pattern should also be booming to rejection-of-assistance attacks in which adjusted nodules avoid other nodules from getting group keys by descending packets going over them.

EMFNVM: Raya, Papadimitratos, Aad, Jungels, and Hubaux proposed "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks" Promptly access to retraction information is a especially hard complication in Vehicular Networks. Eviction of Deviating and inaccurate nodules in Vehicular Networks is mainly identify internal attackers in vehicular networks. In order to avoid this it introduce the aggregation of (i) framework-based retraction rules, the Retraction using Compressed Certificate Retraction List(RC2 RL), (ii) a Misbehavior Detection System(MDS) getting the acquaintances of a deviating or false node to find its misbehaving from common behavior, and commences (iii) a Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol in order to secure the system activity, until the attacker is retracted by the Certificate Authority(CA), to a certain extent or completely based on the conformation LEAVE provides. To eradication the suspect ability window, due to the latency for the authority to identify misbehaving nodules and circulate retraction information, it will introduce the scheme that can robustly and effectively receive their confinement, as well as committed to their conditional retraction. This is done with the help of deviation detection module and a distributed eviction hierarchy.

In this paper, we introduce an Hasten Message Endorsement Protocol (HMEP) to overthrown the problem of the long waiting occurred in checking the retraction status of a certificate using a CRL. HMEP operates keyed Hash Message Endorsement Code (HMEC) in the retraction checking process, where the Hash key used in calculating the HMEC for each message is shared only between unrestricted OBUs. In addition, HMEP is handout from the false positive substance which is frequent for lookup hash tables.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

III. BACK GROUND

The two reasons for long waiting in certificate retraction list, the first part is the Endorsement, which checks the retraction status of the sender in a CRL, May takes long waiting time depending on the CRL size and the working system for searching the CRL. Second thing is the scale of the VANET is expected to be very large.

SYSTEM MODEL:-VANET consists of an Honored Authority, which is responsible for providing unsigned certificates and distributing secret keys to all OBUs in the network. Infrastructure Roadside units (IRSUs), which are fixed units distributed all over the network. The IRSUs can communicate securely with the HA. OBUs which are installed in vehicles. The broadcasting of OBUs can be done either with other OBUs through V2V communications or with IRSUs through V2I communications.

As shown in Fig.1, the following are the system model under consideration.

- A Honored Authority (HA), which is responsible for providing unsigned certificates and circulate the secret keys to all OBUs in the Vehicular Ad Hoc Network.
- Infrastructure Roadside units (IRSUs), which are permanent units, circulate all over the network. The IRSUs can broadcast securely with the HA;
- On-Board Units (OBUs), which are installed in vehicles. OBUs can broadcast either with other OBUs through V2V communications or with IRSUs through V2I communication.

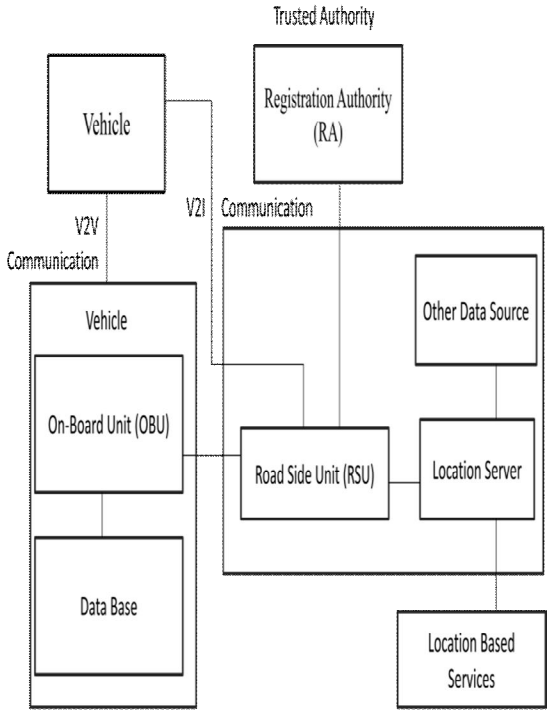

Fig.1.The system model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

According to the Wireless Access in Vehicular Environments (WAVE) standard, each OBU is installed with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e.g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. We consider that reliable OBUs cannot plot with the retracted OBUs as it is difficult for reliable OBUs to abstract their security materials from their HSMs. Finally, we consider that a adjusted OBU is instantly recognized by the Honored Authority (HA).

SYSTEM INTRODUCTION:- The fundamental security need is observed as entity Endorsement, integrity of messages, no cancellation, and privacy conservation.

MESSAGE ENDORSEMENT:- Here it proposes an efficient Endorsement and retraction scheme called Temporary Anonymous Certified Keys (TACK). TACK maintains a grouping system model consisting of a central Honored Authority(HA) and Regional Authorities (RAs) dispersed all over the network .When any vehicle entering a new region, each vehicle must update its certificate from the RA which is dedicated for that region.

RETRACTION:- Message Endorsement involves a generic PKI (Public Key Infrastructure) system, the details of the HA signature on a certificate and an OBU signature on a message are not explained in this paper for the welfare of generalization. It shows that how to expedite the retraction checking process, which is consistently performed by checking the CRL for every acquired certificate.

SECURITY REASONING:- A plotting attack, an appropriate OBU plot with a retracted OBU by releasing the ongoing secret key K~g such that the retracted vehicle can use this secret key to pass the retraction check process by evaluating the appropriate HMEC values for the translated messages. All the security components of an OBU are reserved in its tamper proof Hardware Security Module (HSM). In addition to that , all the keys update actions in Algorithms 3-5 are evaluated in the Hardware Security Module (HSM), which means that the recent secret key K~g is reserved in the tamper proof HSM, and it cannot be translated in clear under any situations.

VALIDATION SUSPENSION:- The performed forward-looking search on a text file, which is containing the primitive existence of the retracted certificates, while the binary CRL checking program executes a binary search on a text file containing the sorted identities of the retracted certificates. For the second and above Endorsement phases, we apply Elliptic Curve Digital Signature Algorithm (ECDSA) in order to check the reliability of the certificate and the trademark of the sender.

END-TO-END SUSPENSION:- Here it selects the circulation of the road situation details by an OBU of every 300 m sec to coordinate to the DSRC measures. The portability traces adopted in this duplication are achieved using TraNS. The end-to-end suspension is defined as the time to translate a message from the sender to the receiver.

MESSAGE FAILURE RATIO:-The average message Failure ratio is defined as the average ratio between the numbers of messages discarded every 300 m sec, due to the message endorsement suspension, and the total number of messages collected every 300 m sec by an OBU of a vehicle. It should be noted that we are only interested in the message failure obtained by OBUs due to V2V communication.

IV PROPOSED SYSTEM

Our advanced work will focus on the certificate and message signature endorsement acceleration. In addition to Honored Authority HA, key server is implemented with Honored Authority. The main focus of key server is to handle the key management process for data encryption and decryption. The IRSU sends encrypted information to Honored Authority HA checks its authority and transfer the information to OBU. The OBU unit requests a private key from key server to decrypt the information. The key server gets a report from IRSU; if it gives a confirmation report the key server provides a private

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

key to OBU to decrypt the data. By this process the message authentication and certificate verification or revocation is done in a secure manner. The proposed technique ensures a trusted message authentication in vehicular networks

V. CONCLUSION AND FUTURE WORK

Hasten Message Endorsement Protocol (HMEP) proposed here for VANETs, which fastens message endorsement by replacing the time-exhausting CRL analyzing process with a quick retraction analyzing process operating HMEC function. It uses a novel key distribution structure which allows an OBU to revise its adjusted keys even if it formerly missed some retraction messages which allow an OBU to update its compromised keys. In addition, HMEP has a standard element translating it integrates with any PKI system. Therefore, Hasten can extremely decreases the message failure ratio due to message authentication delay message signature compared to the traditional endorsement methods monitoring CRL checking. The next generation IoV is an emerging field that crosses multiple disciplines including automotive, intelligent transportation, information technology, communications, energy, etc. In the recent years, there are more and more system technologies and system intelligence being used to make transportation more clean, efficient, connected and safe. Our future work will focus on the certificate endorsement acceleration of VANETS for fast and secure transportation.

REFERENCES

[1] Chan. H, Perrig. A and Song. D (2003), "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp .Security and Privacy, pp. 197-213
[2] Haas. J. J, Hu. Y and Laberteaux. K. P (2009), "Design and Analysis of a Lightweight Certificate Retraction Mechanism for VANET," Proc. Sixth ACM Int'l Workshop Vehicular InterNETworking, pp. 89-98.
[3] Hubaux. J. P (2004), "The Security and Privacy of Smart Vehicles,"IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55.
[4] Laberteaux. K. P, Haas. J. J and Hu. Y (2008), "Security Certificate Retraction List Distribution for VANET," Proc. Fifth ACM int'l Workshop Vehicular Inter-NETworking, pp. 88-89.
[5] Raya. M and Hubaux. J.P (2007), "Securing Vehicular Ad Hoc Networks,"J. Computer Security, vol. 15, no. 1, pp. 39-68.
[6] Studer. A, Shi. E, Bai. F and Perrig. A (2009), "TACKing Together Efficient Endorsement, Retraction, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Command Networks (SECON '09), pp. 1-9.
[7] Sun. Y, Lu. R, Lin. X, Shen. X and Su. J (2010), "An Efficient
Pseudonymous Endorsement Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603.
[8] Wasef. A and Shen. X (2008), "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC'08), pp. 1458-1466.
[9] hmac — Keyed-Hashing for Message Authentication, Python Software Foundation, retrieved 7 May 2014.

BIOGRAPHY

Mrs D. Thriveni is a student in the M.Tech (Computer Science Women, Tirupathi. She was completed her Master of Computer Applications (MCA) in Sri Venkateswara College of Computer Sciences, Chittoor

Mrs G.T. Prasanna Kumari is an Associate Professor in the Department of Computer Science and Engineering, Gokula Krishna College of Engineering, Sullurpet. She is Ph.D,in Computer Science in thearea of Distributed Data Mining Systems. She is in teaching since 1999. She presented papers at National and International Conferences and published articles in National and Internationaljournals