ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

AN EFFICIENT GROUP SIGNATURE USED ON PRIVACY PRESERVING AUTHENTICATION FOR VANET

Mr. M.Merlin moses
Assistant Professor, Dept. of ECE,
Einstein College of engineering,
Tirunelveli, India

S.Sonia
PG Scholar, Dept. of ECE,
Einstein College of engineering,
Tirunelveli, India

***Abstract*-- An efficient privacy preserving authentication scheme based on group signature is proposed for Vehicular Ad hoc Networks (VANETs). This scheme first divide the precinct into several domains, in which Road Side Units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized manner. Hash Message Authentication Code (HMAC) is used to avoid time consuming Certificate Revocation List (CRL) checking and to ensure the integrity of messages. Cooperative message authentication is adopted among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.**

Index items — Privacy-preserving authentication, Hash Message Authentication Code (HMAC), Batch group signature, cooperative authentication Vehicular ad hoc networks (VANETs)

I.INTRODUCTION

VEHICULAR ad hoc networks (VANETs) are an instance of mobile ad hoc networks that design to enhance the safety and the efficiency of road traffic. VANETs are consists of elements including On-Board Units (OBUs), Roadside Units (RSUs) and central Trust Authority (TA). It is anticipated that vehicles equipped with wireless communication devices are communicate each other and with roadside units (RSUs) located at critical points such as intersections or gas stations. Compared with wired or wireless networks, VANETs are very dynamic, and their communications are volatile. A self-organized network can be formed with the OBUs and the RSUs, which is called a vehicular *ad hoc* network (VANET). In addition, the RSUs could be connected to the Internet backbone is to support diversified services, such as transmission control protocol and real-time multimedia streaming applications. The creation of a VANET is more significant to traffic management and roadside safety. Unfortunately, a VANET also comes with its own set of challenges, mainly security and privacy.

Short digital signatures are needed in the environments where a human is asked to manually key in the signature. For example, product registration systems ask users to key in a signature provided on a CD label. Generally, short signatures are needed in low-bandwidth communication environments. Hence, to satisfy the security and privacy requirements, it is a prerequisite to design a suite of protocols to achieve security and privacy for practical vehicular networks. In VANETs, each vehicle can communicate with other nearby vehicles or with fixed roadside infrastructure, to perform some useful applications such as safety-related warning functions, traffic management, infotainment, payment services, etc. VANETs allow for vehicles to communicate with one another and with the RSUs. The RSUs are fixed elements and the vehicles are the moving elements.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

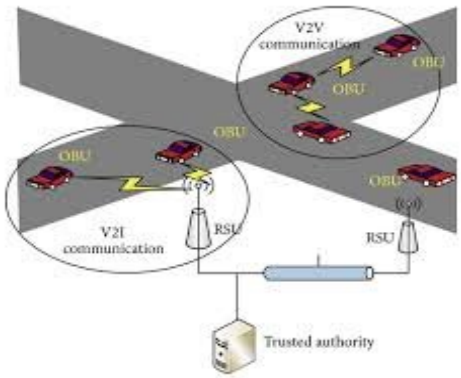

Fig.1 VANET environment

The simplest and the most efficient method is declare to assign to each vehicle a set of public/private key pairs that will allow the vehicle to digitally sign messages and thus authenticate itself to receivers. A group signature scheme is to allow members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key by verifier, but they do not reveal the identity of the signer.

Group signatures are address the privacy issue by providing anonymity within a specific set of users, namely, a group. It calculates HMAC values with the group key generated by the self-healing group-key generation algorithm, which can replace the time-consuming CRL checking and provide the integrity of messages before batch verification. The cooperative message authentication scheme is to increase the efficiency of authentication.

II.REVIEW OF LITERATURE

An Efficient Conditional Privacy-Preserving Authentication scheme for Vehicular Sensor Networks proposed [8] the technique of pseudo-identity based signatures (IBS) for secure vehicle-to-infrastructure communications in VANET. The aim is to design this scheme satisfies the security needs: 1) Authentication and message integrity, 2) Identity privacy preserving, 3) Traceability. Identity-based (ID) signature scheme KIBS to ensure both source authentication and message integrity, when before message is sent one appealing solution is to sign each message with a digital signature. The time can be reduced by up to 18% for verifying 800 signatures in this scheme. It must be verify multiple received signatures.

A Scalable Robust Authentication Protocol for Secure Vehicular Communications [18] proposed a decentralized group-authentication protocol in the sense that group is maintained by each roadside unit. Vehicles are entering the group can broadcast vehicle-to-vehicle (V2V) messages anonymously, that can be instantly verified by the vehicles in the same group. The number of active vehicles within a range of a single RSU is much smaller, compared with the millions of vehicles in a VANET. Hence, the system will not affect from computation and communication bottlenecks.

An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks [1] proposed the DCS scheme introduces an aggregate batch verification technique for authenticating certificate-based signatures, which decreases the verification overhead simultaneously. The proposed DCS batch verification provides the lowest message loss ratio, and the message loss ratio increases as the number of OBUs within communication range increases. The reason for the superiority of the DCS scheme is that it can aggregately verify a number of signatures higher than that of ECPP, ECDSA, BLS, or CAS. An efficient distributed-certificate-service (DCS) scheme for vehicular communications, which features properties are scalability and efficiency.

Anonymous Batch Authentication and Key Agreement (ABAKA) method is to design a secure environment for value-added services in VANETs. To avoid bottleneck problems, ABAKA [5] is simultaneously inspired by the concept of batch verification to authenticate multiple requests sent from different vehicles using Elliptic Curve Cryptography (ECC), which is adopted by the IEEE Trial-Use standard. Meanwhile, multiple session keys can also be negotiated at the same time for different vehicles. This is the first study that provides batch authenticated and key agreements for value added applications in VANETs. ABAKA provides the following unparalleled features like multiple vehicles can be authenticated at the same time rather than one after the other. It is an appealing solution to solve the possible bottleneck problems elaborately. Batch authentication not only can be achieved but batch key agreement can also be accomplished. Depending on different key agreement parameters

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

sent from the requesting vehicles, ABAKA could negotiate a distinct session key with each vehicle to provide the confidentiality of subsequent messages. By creating distinct pseudo identities and the corresponding private keys, the privacy regarding the real identity of a vehicle and private information are guaranteed. Due to the Service Provider (SP), the real identities of the vehicles can be revealed under specific conditions. The efforts on the storage cost and the transmission overhead can be significantly alleviated by the advantage of tamperproof devices in vehicles.

An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks [7] propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, The proposed system is employ an identity-based cryptosystem where certificates are not needed for authentication.

A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks [9] proposed technique data acquisition and delivery systems. In this paper, a service-oriented vehicular security system is design that allows VANET users to exploit RSUs in obtaining various types of data. This scheme designed an efficient routing protocol that transfers messages between a vehicle and an RSU through other vehicles reliably. The routing protocol is called ROAMER, outperformed many routing protocols in terms of delivery ratio, delay and bandwidth consumption. An algorithm designs for securing data messages based on using a symmetric scheme for cryptographic operations. The algorithm to used by the source to generate a sequence of keys from a secret input string (*S*) and uses these keys to encrypt the next packet. The input string (*S*) is notified as part of the data in the current packet.

A Secure and Privacy-Preserving Protocol for Vehicular Communications [13] proposed a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. A signature scheme using ID-based cryptography (IBC) is adopted in the RSUs to digitally sign each message launched by the RSUs to ensure its authenticity, where the signature overhead can greatly be reduced.

III. PROPOSED WORK

The proposed method of this paper used the group signature on privacy-preserving authentication for VANET. The block diagram consists set the VANET environment, generates the private key and public key, Issuing certificate for RSU and vehicles, group key distribution, registration of vehicles using RSU, batch authentication, cooperative authentication. First, initiates the number of nodes, queuing protocols, energy for creating the VANET environment. TA generates the private key and public key by using signature algorithm, issues the certificate for RSU and vehicles. Then TA sends the public system parameters and the group key to all RSUs in domain for secure group key distribution, the vehicles and the RSU can realize mutual authentication by using these pre-stored materials.

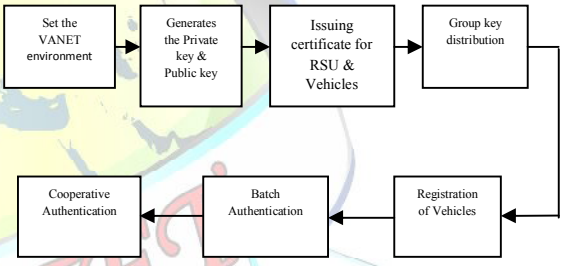

Fig.2 Block diagram of proposed system

When a vehicle joins a new domain, a mutual authentication process between the vehicle and the RSU it first meets should start, if an RSU is compromised, TA will revoke it by broadcasting the information of the domain it belongs to and its identity, i.e., every vehicle can get information of revoked RSUs. During this registration process can prevent illegal vehicles from joining the domain.

In mutual authentication first every RSU broadcasts its certificates (message format $PK_{Rx,}$ $D_{A,}$ $Cert_{TA,Rx,}$ $GPK_{DA,}$ $Sig_{SKRx}(GPK_{Da})$) in the domain. After that when the vehicle gets this message, it checks the domain, vehicle sends the message about their public key, certificate of TA & signature of private key. The public key and certificate of vehicle are encrypted by the public key of RSU, only RSU can get the plaintext. Next RSU sends the message attached with HMAC value to vehicle, when vehicle receives this message decrypts by its private key SKv, and verifies the signature. If the signature is valid, vehicle sends message with time stamp to RSU.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

RSU sends message to calculating group keys for HMAC computation to vehicle.

The current group key GK_j is computed as,

$$GK_j = H(K_j^F + K^B_{m-j+1}) \quad (1)$$

Where, K_j^F is the forward key chain, and K^B_{m-j+1} is the backward key chain Finally, RSU (Rx) and vehicle (Vi) also stores the information.

HMAC is a main technique which is used for authentication. A one-way hash function h(·) is said to be secure if the following properties are satisfied.

1) h(·) can take a message of arbitrary length as input and produce a message digest of a fixed-length output.

2) Given x, it is easy to compute h(x) = y. However, it is hard to compute $h^{-1}(y) = x$ given y.

3) Given x, it is computationally infeasible to find x□≠ x such that h(x□) = h(x).

HMAC is used to authenticate the source of a message and its integrity by attaching a Message Authentication Code (MAC) to the message, which is accomplished by a cryptographic keyed hash function. In this method, HMAC is used for two purposes: 1) ensuring the validity of sender's identities, since only valid users can generate correct HMACs and 2) checking the integrity of messages before batch verification, thus achieving the efficiency of batch verification.

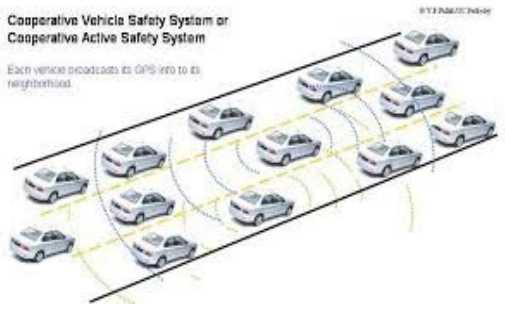

Fig.3 Cooperative authentication

Cooperative authentication can ensure that a vehicle knows the authenticity of all received messages without verifying all the message signatures by making the neighboring vehicles work cooperatively. In this scheme verifier can measures the distance between message sender and receiver that each security related message carries the location information of the sender vehicle. Verifier should be in front of or behind the vehicle, away from each other and neither too small nor too large to computes the direction and location.

In this proposed work HMAC technique used to avoid time consuming CRL checking because it provides two purposes. The validity of sender's identity is to ensure for HMAC generation and integrity of messages checks before batch verification that are overcome the CRL checking problems. This scheme should reduce the delay caused by CRL checking and group signature verification to achieve the rapid authentication. The signature verification time is to reduce by these schemes employ batch group signature verification, in which a large number of messages can be authenticated in a timely manner.

VI. RESULTS AND ANALYSIS

This paper provides two parameters analysis for privacy-preserving authentication. They are delay and packetloss performance.

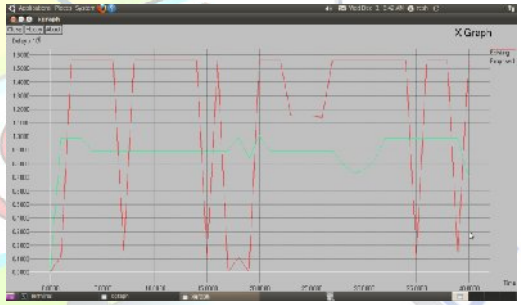

Fig.4 Delay performance

In Fig.4.the delay performance is reduced by using batch verification technique in the timely manner. The batch verification mechanism is an efficient way of ensuring the trust of multiple messages received in a unit time. The CRL checking introduces too much computation delay, greatly degrading the system performance. To improve the efficiency of authenticating the message source, the HMAC checking is employ to replace the time consuming CRL checking.

In Fig.5 the packetloss performance ensured when the RSU checks vehicle whether valid or invalid to authenticate with Trusted Authority, if the vehicle is invalid, the checked

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

information is dropped. If it is valid vehicle, then authentication process is continued. The packetloss parameter is to better than existing method in this paper to reduce the packet dropping due to proposed scheme.

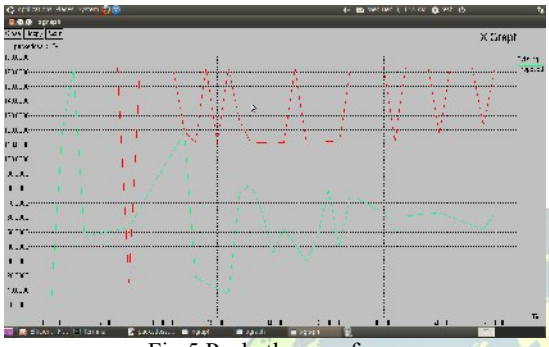

Fig.5 Packetloss performance

V. CONCLUSION

This paper is reduced time-consuming CRL checking, to ensure the integrity of messages before batch verification and reducing the number of invalid messages in the batch by using HMAC in Privacy-Preserving Authentication scheme. The design goal is verified jointly using the techniques of distributed management, HMAC, batch group signature verification and cooperative authentication. The cooperative authentication is also used to further improve the efficiency of authentication scheme. By employing the given methods, this scheme can meet the requirement of verifying 600 messages per second. The security and performance analysis show that this scheme can achieve efficient group signature based authentication while keeping conditional privacy for VANETs. In this project, the range of packetloss is reduced, compared than the existing method.

REFERENCES

[1] Albert Wasef, *Member,* Yixin Jiang, and Xuemin Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks"
[2] Bellur B, (2008) "Certificate assignment strategies for a PKI-based security architecture in a vehicular network," in Proc. IEEE GLOBECOM, New Orleans, LA, pp. 1–6.
[3] Camenisch J and Groth J (2005), "Group signatures: Better efficiency and new theoretical aspects," In Security in Communication Networks 2004, volume 3352 of LNCS, Springer Verlag.
[4] Cheon J H and Yi J H, (2007) "Fast Batch Verification of Multiple Signatures," in Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography - PKC 2007, Beijing, China, pp. 442–457.
[5] Huang J L, Yeh L Y, and Chien H Y, (2011) "AKABA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262.
[6] Jianping Wang "Ns-2 Tutorial (1)," Multimedia Networking Group, The Department of Computer Science, UVA
[7] Jinhua Guo, John Baugh P, and Shengquan Wang Department of Computer and Information Science, University of Michigan-Dearborn,"A Group Signature Based Secure and Privacy-Preseving Authentication for Vehicular Communication Framework".
[8] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks"
[9] Ke Liu (2004) "Network Simulator 2: Introduction," Department Of Computer Science, SUNY Binghamton.
[10] Kyung-Ah Shim K A, (2012) "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883.
[11] Mershad K and Artail H, (2013) "A framework for secure and efficient data acquisition in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 62, no. 2, pp. 536–551.
[12] Raya M and Hubaux J P (2007), "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68
[13] Rongxing Lu, Xiaodong Lin, Tom Luan H, Xiaohui Liang and Xuemin (Sherman) Shen, (2012), "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1
[14] Vishal Kumar1, Shailendra Mishra1, Narottam Chand2 (2013),"Applications of VANET: Present & Future," Communications and Network, 2013, 5, 12-15 doi:10.4236/cn.2013.51B004 Published Online.
[15] XiaodongLin, Xiaoting Sun, pin-Han Ho and xuemin shen, (2007), "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communication," IEEE Trans. Veh. Technol.,vol. 56, no.6
[16] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li (2014) "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks," IEEE Trans. Veh. Technol., vol. 63, no. 2,
[17] Xun Yi, Member, IEEE (2003), "An Identity-Based Signature Scheme from the Weil Pairing," IEEE Communication and networks, vol. 7, no.2
[18] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen and Jinshu Su, (2010), "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Veh. Technol., vol. 59, no.7
[19] Zhang C, Lin X, Lu R, Ho P H, and Shen X, (2008) "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368.
[20] Zhang L, Wu Q, Solanas A, and Domingo-Ferrer J, (2010) "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617.