EFFICIENT SECRECY MAINTAINING CERTIFICATION SCHEME FOR VANET

P.ANAND SATEESH KUMAR

PG scholar, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India.
anandaug92@gmail.com

Mr.B.DHIYANESH, M.Tech, (Ph.D).,

Associate Professor, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India.
dhiyanu87@gmail.com

Dr.S.SAKTHIVEL.,

Professor, Department of Computer Science and Engineering
Sona College of Technology, Salem, Tamilnadu, India.
sakvel75@gmail.com

Abstract

VANET are one of the new promising techniques used to enable communication on roads. Here for VANETs an efficient secrecy maintaining authentication scheme is done .To detect anonymous authentication group signature is used widely used but in previous scheme it suffers from long computation delay in CRL (certificate revocation list) checking. It leads to a high message loss.so they cannot achieve the target of receiving 100 of messages per second.so HMAC is used here to avoid time consuming CRL checking and to ensure the integrity of messages before batch group authentication. To reduce authentication burden each vehicle needs to verify a small number of messages using cooperative message authentication among entities. Hence security and performance analysis shows that our scheme is more efficient in terms of authentication speed by keeping conditional privacy in VANETs. Thus the proposed scheme is analyzed through simulations in NS2 and proved to out performs the existing available techniques**.**

Keywords- Vehicular Ad Hoc Network (VANET), CRL(Certificate Revocation List)HMAC(Hash Message Authentication Code),Cooperative Message Authentication.

1. Introduction

In the advanced development of wireless communication technologies, car manufactures and telecom industries help to equip each vehicle with wireless devices. It allows vehicles to communicate with each other as well as with other vehicles network communication devices like road side units (RSU) and Trustedauthority (TA)etc. Generally a VANET consists of three components they are onboard units, Road side units and a central trusted authority. In VANET when vehicles communicate with each other and also with RSU and TA in which the attackers can easily get users private information such as identity, tracing etc. The reason is that they are not properly protected so we should design an efficiency secrecy maintaining authentication scheme for VANET.

In previous scheme group signature is used for detecting unknown authentication so for which any group member allows to sign behalf of the group without reveling its real identity. So when a vehicle receives a message from unknown entity, a vehicle has to check the (certificate revocation list) CRL to avoid communicate with revoked vehicles. Also To verify the sender's group signature to check the validity of the received message. The problem here occurs is the time consuming for CRL checking because it takes 11ms to verify a message with a group signature and 9ms to check one identity in CRL. If n revoked number in CRL th number of messages verified in one second is 1000/9n+1 it is very smaller than the target of verifying 600.so we should try to overcome the delay caused by CRL checking and group signature verification to achieve rapid authentication.

Thus an efficient privacy authentication scheme for VANET has been done through RSU by jointly using the techniques of distributed management, HMAC, group signature verification and cooperative authentication. First dividing the precinct into several domains so the system can run in a localized manner. Then HMAC is calculated with group key generated by the self-healing group-key generation algorithm which reduces time consuming CRL checking and ensure the integrity of messages before batch verification. Then cooperative message authentication is used to improve the message authentication scheme .By using these

security and performance analysis shows that our scheme is more efficient in terms of authentication speed by keeping conditional privacy in VANETs.

2. VARIOUS SECURITY AND VERIFICATION METHODS

Title	Algorithm used	Process	Merits	Demerits	Performance evaluation
An efficient identity-based batch verification scheme for vehicular sensor networks	Identity based batch verification scheme	For conditional privacy preserving in which multiple Message receives at sametime.	System performance is improved. Time reduction occurs because of verifying multiple messages at same time	Security is less	Transmission overhead isreduced. Transmission rate is 25.1 percent better than ECDSA
An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications	Pass scheme algorithm is used	Strong Privacy Preservation in which vehicular common takes place	Reduces revocation cost, Uncompromised vehicles cannot trace the other vehicles	Does not considers about energy	Signature verification dominates the message Authentication efficiency so PASS can perform the best.
A scalable ro-bust authentication protocol for secure vehicular communications,	Robust and scalable protocol	Faces challenges in de-centralized group authentication and also managing and distributing data's to vehicles.	False message can be easily traced.	More time Taken for sending data's	Better than ECPP protocol.
A group signature based secure and privacy-preserving vehicular communication framework	Scalable role based, Probabilistic signature verification scheme	Secure Oriented framework	Achieves authenticity Data integrity, Anonymity. Tampered messages can be easily detected from unauthorized node.	Not the best method for key Distribution	Authorized user can only access shows Good privacy for large vehicles
An efficient message authentication scheme for vehicular communications	RSU-Aided Message and Cooperative message authentication scheme	Adopts K-anonymity property for user privacy	Reduces message loss ratio and lower computation	More time taken for message authenticatio n	Compare to PKI and group signature based scheme message loss ratio will be low.
Secure incentives for commercial ad dissemination in vehicular networks,	Signature seeking Drive,Hash chain based n-level advertising,on ion voucher based n-level adverting	Car to car communication for advertisement purposes for business companies	Advertisement company pays for charge for network resources	Uncooperati ve model, malicious node can easily attack the weak area and disrupt the system	storage requirement,co mmunication cost ,computation problemswill be less

An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks	Pseudo-identity based authentication scheme.	RSU is used for verification of vehicles	Verification time will be reduced.	Problems may occurs due to network infrastructure .	Transmission overhead is reduced,
Akaba: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks	Batch authentication and ABAKA scheme is used	Processing different session keys for different vehicles at same time and also to authenticate multiple requests from different vehicles	Message loss ratio and Message delay ratio will be less	Energy taken will be very much high. Security will also not si much compared to other models	Compared to ECDSA scheme message transmission rate will be better.

CONCLUSION

In this paper an efficient privacy-preserving group signature based authentication scheme for VANETs is done by jointly using the techniques of distributed management, HMAC, batch group signature verification, and cooperative authentication to achieve the design goal. First, divide the whole network into several domains, which allows localized management. H MAC is used in our scheme to replace the time-consuming CRL checking and to ensure the integrity of messages before batch verification, reducing the number of invalid messages in the batch. Thus also use cooperative authentication to further improve the efficiency of our scheme. In further process we concentrate on data's security which has been send to the vehicles.

REFERENCE

[1] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme For Vehicular Sensor Networks," in Proc. IEEE INFOCOM, Phoenix, AZ, USA, Apr. 2008, pp. 246–250.

[2] 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. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[3] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol For Secure Vehicular Communications,"IEEE Veh.Technol.,vil.59,no.4,pp.1606-1617, May 2010.

[4] J. Guo, J. P. Baugh, and S. Wang, "A Group Signature based Secure and Privacy-preserving Vehicular Communication Framework," in Proc. Mobile Netw. Veh.Environ., Anchorage, AK, USA, May 2007, pp. 103–108.

[5] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An Efficient Message Authentication Scheme For Vehicular Communications,"IEEE Trans.Veh.Technol.,vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[6] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure Incentives For Commercial Ad Dissemination in Vehicular Networks," in Proc.8th ACM Int.Symp.MobiHoc, Montreal, QC, Canada, Sep. 2007, pp. 150–159.

[7] K. A. Shim, "An Efficient Conditional Privacy-preserving Authentication Scheme For Vehicular Sensor Networks,"IEEE Trans.Veh.Technol.,vol. 61, no. 4, pp. 1874–1883, May 2012.

[8] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "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, Jan. 2011.