RESEARCH ARTICLE OPEN ACCESS

Secure Authentication for Vehicular Ad Hoc Network

Rinsu Aravind [1], Deepa P L [2]
Research Scholar [1], Assistant Professor [2]
Department of Computer Science and Engineering
Cochin Institute of Science and Technology
Muvattupuzha –India

ABSTRACT

Security is an important issue in ad hoc networks, especially for security sensitive applications. This paper mainly focus the authentication based on the group signature for providing the security and privacy in vehicular ad hoc networks (VANET). In VANETs, group signature is widely used for vehicles to achieve unauthenticated vehicles. A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer When receiving a message from an unknown entity, a vehicle has to check the certificate revocation list (CRL) to avoid communicating with revoked vehicles and then verify the sender's group signature to check the validity of the received message. The Public Key Infrastructure ensures user validity. It is based on the concept of asymmetric key cryptography. The security and performance analysis show that our scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.

Keywords:- vehicular ad hoc networks(VANET), certificate revocation list (CRL), Public Key Infrastructure

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 consist of elements including On-Board units (OBUs), Roadside Units (RSUs) and central Trust Authority (TA). On-Board Units (OBU), that are radio devices installed on vehicles, and Road Side Units (RSU) [18], that constitute the network infrastructure. RSUs are placed along the roadside and are controlled by a network operator [2]. VANETs are expected to allow for transmission of information between vehicles or between vehicles and the roadside units (RSUs) [17] and, thus, to enhance the safety of both vehicle drivers and passengers [1].

Securing vehicular communications is an indispensable prerequisite for their deployment. Systems must ensure that the transmission comes from a trusted source and has not been tampered since transmission. Privacy is another major issue. Vehicle safety communication applications broadcast messages about a vehicle's current location, speed and heading several times per second. Ensuring the security and privacy of vehicular wireless communications is still a formidable challenge. Conflicting goals such as security and efficiency as well as privacy and authenticity must be taken into account.

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.

In this paper, group signature based authentication is used. A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of a later dispute, open signatures, i.e., reveal the identity of the signer. Existing schemes based on group signatures suffer from long computation delay in the certificate revocation list (CRL) checking and in the signature verification process, leading to high message loss. As a result, they cannot meet the requirement of verifying hundreds of messages per second in VANETs. The hash message authentication code is used for avoiding the certificate revocation list (CRL) checking problem. Basically the hmac is implemented in MatLab a technical computing tool.

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 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. RELATED WORK

Security and privacy are still open problems in vehicular networks.

A novel RSU-aided message authentication scheme named RAISE has been proposed by Chenxi Zhang [2]. RAISE provides significant improvement in authentication efficiency and scalability for the intervehicle communications (IVC) of VANETs. In this paper, they propose an RSU-aided message authentication scheme named RAISE. With RAISE, RSUs are responsible for verifying the authenticity of messages sent by vehicles and notifying the authentication results back to all the associated vehicles. RAISE also protects the vehicles' privacy by adopting the *k-anonymity* approach. In addition, a cooperative message authentication scheme named COMET has been proposed to work as a supplementary scheme of RAISE in case of the absence of an RSU. But this system does not provide the scalability and also there is a chance for message loss.

Xiaodong Lin proposes a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques [3]. It uses a novel group signature based security scheme which relies on tamper resistance devices (requiring password access) for preventing adversarial attacks on vehicular networks. They demonstrate that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. Communication overhead is the main problem in this paper.

Lin Yao proposed biometrics based anonymous mutual authentication with provable link-layer location privacy preservation [9]. During its authentication phase, two vehicles negotiate their temporary session key and generate two temporary MAC addresses. These two addresses, instead of the real ones, are used in all future communication frames. They further protect the biometric privacy with the help of a biometric encryption technique. During the authentication process, a user's biometric is matched against the biometric template stored in the database through field sampling. This match will prove the user's identity. In order to protect MAC addresses from being eavesdropped, their scheme generates two temporary MAC addresses for the communicating parties. A unique session key is also generated for communication message encryption. Furthermore, biometric encryption is adopted in our scheme in order to protect biometric template from tampering. The communication overhead is the main problem of the paper.

The fundamental security functions in VC will consist in authenticating the origin of a data packet. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities. Authentication helps also to control the authorization levels of vehicles. Signcryption is a new paradigm in public key cryptography [7]. A remarkable property of a signcryption scheme is that it fulfils both the functions of public key encryption and digital signature, with a cost significantly smaller than that required by signature-then-encryption. The purposes of this paper are to demonstrate how to specify signcryption schemes and to examine the efficiency of such schemes. A signcryption is a primitive that provides private and authenticated delivery of messages between two parties. Proxy signature schemes are variations of ordinary digital signature schemes and have been shown to be useful in many applications.DOS attack con not be solved by the signcryption.

In our proposed system we propose an efficient conditional privacy preserving authentication scheme for VANETs under the semi-trust model of RSU, by jointly using the techniques of distributed management, HMAC, batch group signature verification, and cooperative authentication. We first divide the precinct into several domains so that the system can run in a localized manner. Then, we calculate HMAC with the group key generated by the self-healing group-key generation algorithm [15], which can replace the time-consuming CRL checking and ensure the integrity of messages before batch verification. We also give a practical setting of the Hao *et al.* Cooperative message authentication scheme [14] to improve the efficiency of authentication. The security and performance analysis show that the proposed scheme can achieve more efficient group signature based authentication while keeping conditional privacy for VANETs.

III. SYSTEM MODEL

The system model of VANET in this paper as shown in Fig 1, which consists of a central trust authority (TA), fixed RSU at the road side, and mobile OBUs equipped in vehicles.

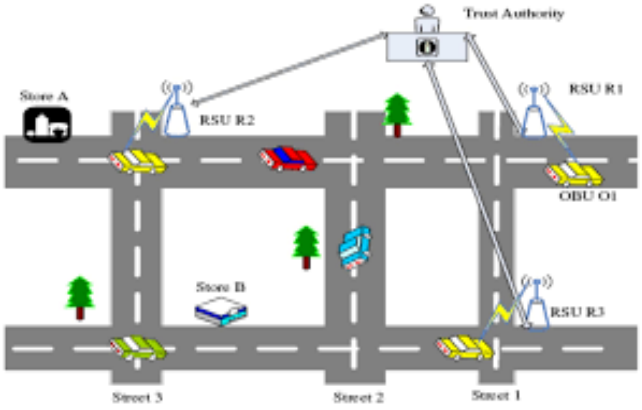

Fig 1 System model

- TA is the trusted management centre for the network. It divides the precinct into several domains. TA is responsible for generate the group key and group signature material for every domain. Then sends these materials to the RSU and also provides registration and certification for RSU and OBU when they join the network
- The RSU is a wave device usually fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11p radio technology, and can also be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network. RSUs are also responsible for issuing the group key materials and group signature related keys to validate OBUs when OBUs join the domain.
- An OBU is a wave device usually mounted on-board a vehicle used for exchanging information with RSUs or with other OBUs. The OBU connects to the RSU or to other OBUs through a wireless link based on the IEEE 802.11p radio frequency channel, and is responsible for the communications with other OBUs or with RSUs; it also provides a communication services to the TA and forwards data on behalf of other OBUs on the network.

IV. PROPOSED SCHEME

The proposed method of this paper used the group signature on privacy-preserving authentication for VANET.

Authentication:- Authentication Protocols are used to convince parties of each other's identity and to exchange session keys. They may be one-way or mutual. Central to the problem of authenticated key exchange are two issues: confidentiality and timeliness. To prevent masquerade and to prevent compromise of session keys, essential identification and session key information must be communicated in encrypted form. This requires the prior existence of secret or public keys that can be used for this purpose. The second issue, timeliness, is important because of the threat of message replays.

Digital Signature Standard:-A digital signature may be formed by encrypting the entire message with the sender's private key, or by encrypting a hash code of the message with the sender's private key. Confidentiality can be provided by further encrypting the entire message plus signature using either public or private key schemes. It is important to perform the signature function first and then an outer confidentiality function, since in case of dispute, some third party must view the message and its signature.

The Fig 2 shows system architecture of the proposed scheme.

A. System Setup

For the considered system, there are three types of network entities: the TA, the RSU, and the mobile OBUs equipped on the moving vehicles. When the vehicles are entered into the domain , they regularly broadcast routine traffic related messages such as position, current time, direction, speed, brake status, steering angle, acceleration/deceleration, traffic conditions, and traffic events, etc., to help drivers getting a better awareness of what's going on in their driving environment and taking early actions to respond to an abnormal situation.

Our system aims at providing the anonymous authentication between two vehicles. We model our system into two logical layers, the security layer and the network layer as shown in Fig 2. Network layer can provide routing services for the security layer and is transparent to the security layer. Therefore, in our scheme, we only focus on the security layer. The security layer can achieve anonymous authentication based on the pseudonym scheme. The working process of the system is summarized as follows:

- System initialization: Before a communication begins, every entity must go to register as a legal entity.
- Anonymous mutual authentication: Two vehicles can achieve anonymous authentication with the help of TA.
- Pseudonym generation: After mutual authentication, a session key will be established and a pseudonym for every user will also be negotiated

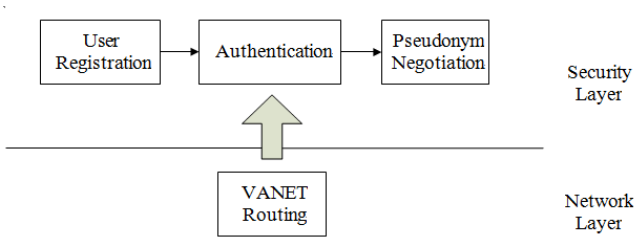

Fig 2 Logical Layer

B. Group Key Distribution

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.

C. Registration of vehicles

When a vehicle joins a new domain, a mutual authentication process between the vehicle and the RSU it first meets should start. Notice that, in our protocol, 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.

D. Batch Authentication

In mutual authentication first every RSU broadcasts its certificates 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 and verifies the signature. If the signature is valid, vehicle sends message with time stamp to RSU. RSU sends message to calculating group keys for HMAC computation to vehicle. Batch verification scheme remarkably increases the number of signatures that can be simultaneously verified. Hence, OBUs can meet the real life verification requirements of VANETs.

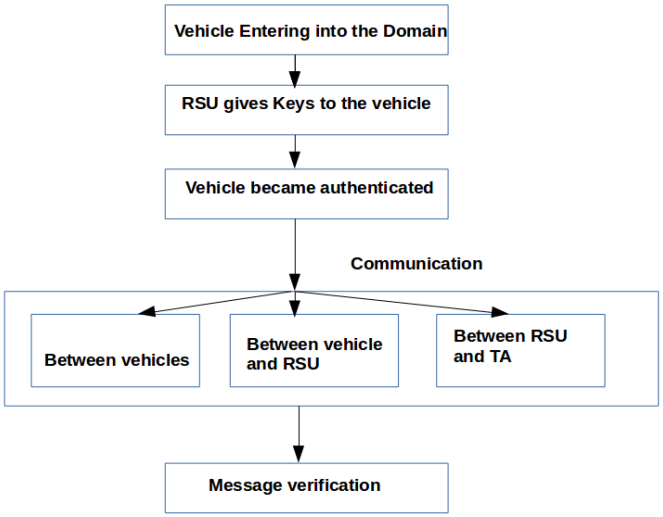

Fig 3 System architecture

E. 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.

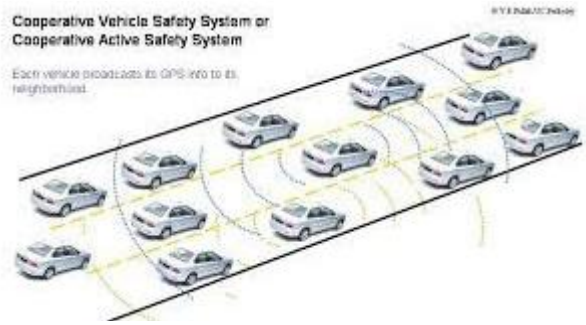

Fig 4 Cooperative authentication

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.

V. SECURITY ANALYSIS

We discuss security issues of the proposed scheme according to the security objectives

A. Against RSUs' Compromission

Considering the problem of RSUs' compromission, in the communication process of mutual authentication and group key generation, can get services without revealing its real identity to RSUs. Therefore, if there exist some RSUs compromised, our protocol can still preserve the privacy of vehicles' identities.

In our protocol, each message sent by signed by its private key, and the group private key and private key are bound together. We also store the information about the mutual authentication,

B. Nonrepudiation of Giving the Group Private Key to a Vehicle

Public parameters of the group signature are generated by TA, it can compute the group private key. If private key is correct, TA verifies the signature to ensure *the* authenticity.

C. Preventing Colluding With Vehicles:

A compromised RSU may collude with a malicious vehicle and then send other legal vehicles' group private key to its accomplice. Then, the malicious vehicle can broadcast messages on behalf of other vehicles.

To prevent this kind of attack, by computing the group private key and verifying the signature, TA can affirm to which vehicle belongs.

VI. RESULTS AND ANALYSIS

This paper provides two parameters analysis for privacy preserving authentication. They are throughput and packet delivery ratio.

A. Throughput

Throughput is the ratio of number of packets which are forwarded and received. Fig 4 shows the graph of throughput.So that input parameters are packets and number of nodes. From the numerical analysis, we can see that initially throughput increases faster as number of nodes increases and get maximum throughput for the maximum number of nodes for a fixed transmission range.

B. Packet Delivery Ratio (PDR)

Packet delivery ratio is the ratio of the number of packet received by the destination to the number of packet sent by the sender. It is most significant metric that we should consider in packet forwarding. It may affect by different crucial factor such as packet size, group size, action range and mobility of nodes .Fig 6 shows the PDR of our proposed system.

The basic idea for PDR is that choose reliable routes. Reliable route need longer predictable lifetime and less number of hops. If the sender have prior information about routes should be chosen instead of the shortest paths which may probably break soon and introduce high maintenance overhead.

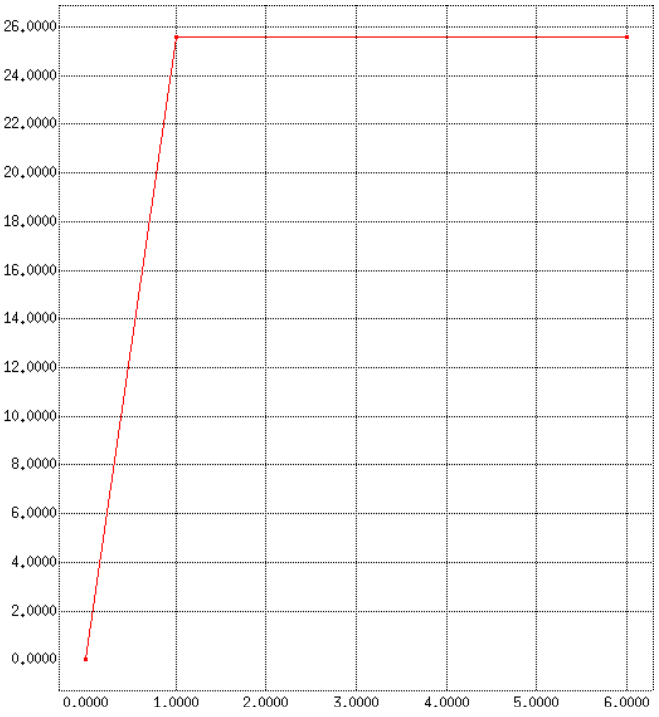

Fig 5 Throughput

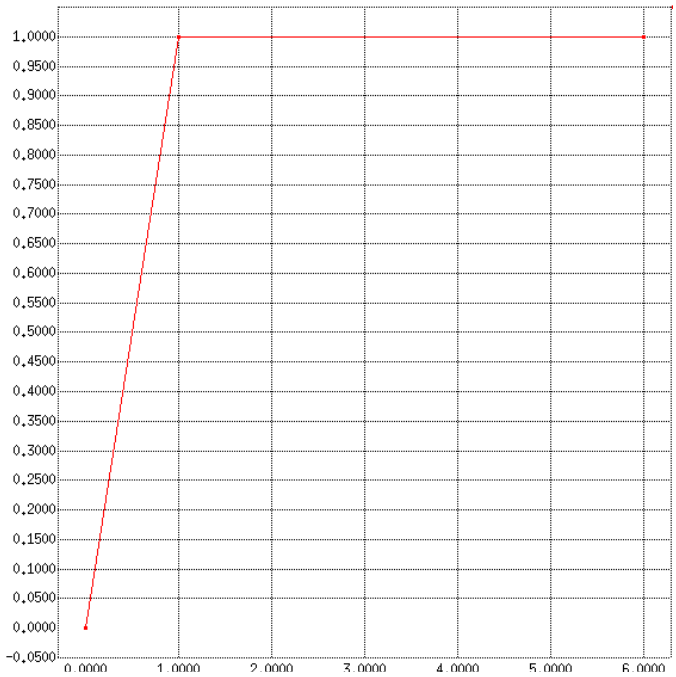

Fig 6 Packet Delivery Ratio

VII. CONCLUSIONS

The deployment of vehicular communication networks is rapidly approaching. There is an urgent need to develop techniques that ensure both security and privacy in vehicular network. We have proposed an authentication based group signature for protecting the security and privacy in vehicular ad hoc network (VANET). The main techniques used here are group signature, hmac, batch authentication and cooperative authentication for achieve the design goal. The group signature mainly provides the authentication with TA. The encrypted and decrypted keys are help full for that. Hmac avoids the delay of CRL checking.

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] Mrs. Arzoo Dahiya, Mr. Vaibhav Sharma, "A survey on securing user authentication in vehicular ad hoc networks" Proc. of the 12th International Conference on ITS Telecommunications (ITST 2011), St. Petersburg, Russia, Aug. 2012.

[2] 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.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. Adv. Cryptol._CRYPTO, vol. 2139, Lecture Notes in Computer Science, 2001, no. 2001, pp. 213–229.

[4] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEETrans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[5] Y. Hao, Y. Chen, C. Zhou, and S. Wei, "A distributed key management framework with cooperative message authentication in VANETs," IEEEJ. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[6] A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in Proc. Top. Cryptol.—CT-RSA, vol. 5473, Lecture Notes in Computer Science, 2009, no. 2009,pp. 309–324.

[7] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacypreserving authentication based on group signature for VANETs," presentedat the IEEE Global Telecommunications Conf., Atlanta, GA, USA, Dec. 2013, Paper WN-23.

[8] 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.

[9] L. Yao, X. Kong, and Q. Fan, "A privacy-preserving authentication scheme using biometrics for pervasive computing environments," Journalof Electronics, vol. 27, pp. 68–78, 2010.

[10] G. Samara, W. A. Al-Salihy, and R. Sures, "Security analysis of vehicular ad hoc networks (vanet)," 2010 Second International Conference on Network Applications, Protocols and Services, pp. 55–60, 2010.

[11] B. Bellur, "Certificate assignment strategies for a pki-based security architecture in a vehicular network," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE, 2008, pp. 1–6.

[12] Lei Zhang, Qianhong Wu, Agusti Solanas and Josep Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications", Vehicular Technology, IEEE Transactions Volume: 59, Issue: 4, May 2010, ISSN: 0018-9545, INSPEC Accession Number: 11285973, doi: 10.1109/TVT.2009.2038222

[13] Brijesh Kumar Chaurasia and Shekhar Verma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, April, 2011

[14] Mrs.Kadam Megha V, "Security Analysis in VANETs: A Survey", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012, ISSN: 2278-0181.

[15] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: Keyed-hashing for
message authentication," RFC 2104, Feb. 1997.