International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

A Secured Dual Authentication Scheme for Data Transmission in VANET

Harshiny J. S, Roshini P, Lakshmi Priya S
Department of Computer Science and Engineering, Prince Dr. K.Vasudevan College of Engineering and technology Chennai, Affilated Anna University, Tamilnadu, India

ABSTRACT

Vehicular ad hoc networks (VANETs) are an important communication paradigm in modern-day mobile computing for exchanging live messages regarding traffic congestion, weather conditions. A trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. TA classifies the users into primary, secondary, and unauthorized users. First, we present a dual authentication scheme to provide a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANET. Second, we propose a dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users' join and leave operations. From this project, we must send the messages or some safety information from the authority to the primary user and the primary user to the secondary user with full of secured process.

Keywords: Authentication, Road Side Unit, On Board Unit, PJW hash algorithm.

I. INTRODUCTION

VEHICULAR Ad-hoc network(VANET) is a distributed self-organizing communication network, which is built among moving vehicles. VANET consists of three components, namely the TrustedAuthority(TA),RoadSide Units(RSU) and vehicles. The Trusted authority provides a variety of online services to the users through RSU. The RSU are fixed at the road sides which are used to connect the vehicles to the Trusted Authority. Each vehicle is installed with an the On Board Unit. Two types of communication are performed in VANETs.The first type is Vehicle To Vehicle (V2V)communication and second type is Vehicle to RSU communication .The V2V and V2R communication are carried out using the Dedicated Short Range Communications (DSRC).These communications are performed through an open wireless channel. Each RSU and OBU uses a DSRC radio, based on IEEE 802.11p radio channel. In this paper, the proposed dual group key management scheme minimizes the computational cost of the TA and group members in the re-keying operation. To achieve this goal, the TA performs only simple addition and subtraction operations to update the group key. Similarly, each vehicle user of the multicast group performs only one modulo division operation for recovering the updated key when the group membership changes. After completing the authentication process, the TA can multicast the information to the authenticated vehicles. The authenticated vehicles can broadcast the information to other vehicles in a secure way. We have proposed a algorithm to generate the secret key using P.J.W.Hash Algorithm . In this technique, the Trusted Authority(TA) generates two different group key for two different groups of users, namely primary user group and secondary user authority to the primary user and the primary user to the secondary user with full of secured process. We propose a dual authentication technique with the capability of preventing malicious vehicles entering into the network and dual key management technique used to transmit the information from trusted authority to group of users in an secure way. In this paper, the main objective of developing a dual authentication scheme is to improve the security in the vehicle side. The dual authentication scheme depends on the Vehicle Secret Key(VSK) which is

given to the user at the time of registration by the Trusted Authority.

II. METHODS AND MATERIAL

1. PREVIOUS WORKS

Existing schemes available in the literature are used to provide authentication only. Among the various existing techniques, proposed an Elliptic Curve Digital Signature Algorithm (ECDSA), which is mathematically derived from the basic digital signature algorithm. ECDSA uses an asymmetric key pair which consists of a public key and a private key. The public key used in this technique is a random multiple of the base point, where the multiples are generated from the private key. Here, both the public and the private keys are used for user authentication. The two attacking techniques that are performed in this method are the attacks on Elliptic Curve Discrete Logarithmic Problem (ECDLP) and the attacks on the hash function.Then they proposed a technique for the management of digital certificates, namely Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV). This method is based on a Public Key Infrastructure (PKI). In this technique, each vehicle has a short lifetime certificate and this certificate can be updated from a RSU. Cooperative Message Authentication Protocol (CMAP) to find out the malicious information broadcasted by the malicious vehicles in the road transport system. The cooperative message authentication is a promising technique to alleviate vehicle's computation overhead for message verification. However, the communication overhead increases when the density of vehicles is higher. The main limitation of this method is that if there is no verifier to verify messages, then the malicious messages may be consumed by vehicle users. The main limitation of these existing works is that the computation complexity involved in recleaning operations leading to the decrease in performance. In addition, the memory requirements are high. The finger print is verified in the vehicles side for authentication of the user for making communication with the VANET. Revocation mechanism allows vehicles to be identified and revoked from the network. Distributed key management is expected to facilitate the revocation of malicious vehicles, maintenance of the system, and heterogeneous security policies, compared with centralized key management. Each road side unit (RSU) act as the key distributed for the group. There is a need to develop security protocols for the scheme which are able to detect compromised RSUs and their colluding malicious vehicles.

2. SYSTEM OVERVIEW

The attack model and system assumptions are used in our proposed method

A. SYSTEM MODEL

Trusted Authority (TA):the TA is responsible for the registration of RSU, vehicle OBU and the vehicle users. It is responsible for key generation and distribution to support secure services in the VANET system. When a vehicle moves from one state to another state, the vehicles credentials will be verified using TA. Road Side Unit (RSU): RSUs are deployed at the road side and they are regularly monitored and managed by the TA. On Board Unit (OBU): The OBU which is used to perform all computation and communication tasks. The smart card is used through a smart card device which is controlled by the OBU. The smart card is given by the TA during the time of registration which contains the Vehicle Secret Key (VSK).

3. PROPOSED SYSTEM

The proposed dual group key management scheme minimizes the computational cost of the TA and group members in the rekeying operation. To achieve this goal, the TA performs only simple addition and subtraction operations to update the group key. Similarly, each vehicle user of the multicast group performs only one modulo division operation for recovering the updated key when the group membership changes. There are two types of users i.e. primary and secondary. The service information is shared between the primary and secondary users or between the secondary and secondary users by V2V communications. The service information is shared only by the RSU to primary user which is also called V2R communication.

The major contributions are:

- ✓ We propose a secure dual authentication technique with the capability of preventing malicious vehicles entering into the VANET system.

- ✓ We introduce a dual key management technique into the VANET to disseminate the information from the TA side to the group of vehicle users in an intelligent and secure way.

MODULES

- ✓ Network Formation
- ✓ Vehicle User's Authentication
- ✓ Group Key Allocation
- ✓ V2R & V2V Communication

Network Formation

First, we have to create an authority for monitoring the network. Then we have the RSUs and OBUs for communicating over the vehicles. The OBUs are devices that are embedded inside the vehicles. The services will be transmitted to the OBUs via RSU's. The OBUs which are in the range of RSU will be the vehicles in the range.

Vehicle User's Authentication:

In this module, we have to authenticate the vehicle users with the vehicle's secret key. This operation is used to authenticate the authorized users. In the existing system, unauthorized users are allowed to enter into the network. But in this authority will not give permission to the user to entering. This authentication will be performed using the hashcode.

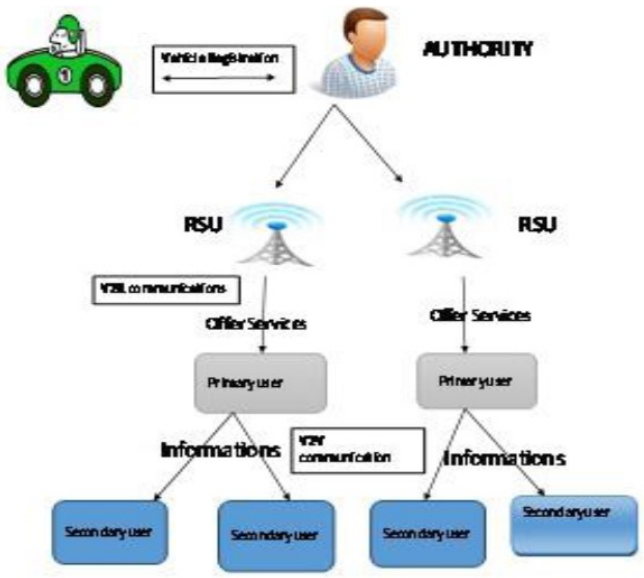
Group Key Management: In this module, we manage two keys for a RSU for authentication process. The two keys namely primary user key and secondary user key. In our project, the primary user only links directly with the authority. The secondary user links with the primary user for temperature conditions, road conditions etc. The services which came from authority will be received only by the primary user.

V2R & V2V Communication

In this, communication process is occurred for transmitting information and services. First, communication between RSU and primary user will happen. Before receiving information by the primary user it has to be checked by the authority whether it is an authorized primary user. Then it will transmit the information to the secondary user. It also has been verified by the primary user by the group key.

III. RESULTS AND DISCUSSION

ARCHITECTURE



All vehicles must be registered to the authority. The registration can be done both online and offline. In offline mode the VANET users first approaches the TA office directly to make offline registration and provide the essential information like name, address, phone number, e-mail id, etc. to the TA. After completing the registration process the TA provides the VSK to the registered user, which is unique for every vehicle. The TA also maintains the list of all vehicles and their respective VSKs in its storage area. RSU will contain the primary user and the secondary user. The TA is directly connected to the RSU. The RSU share the information with the primary user only. This communication is called V2R communication. The primary user can share the information services between the secondary users. This communication is called V2V communication.

ALGORITHM

RSA and PJW hash algorithms are used in our concept.RSA algorithms are used for encryption and decryption process. The algorithm used for generating public and private key used to encrpt and decrypt messages.PJW hash algorithm are used for efficiently generating the secret key to a group of users.

IV.CONCLUSION

In this paper, we proposed a dual authentication scheme to authenticate both the OBU and authority for an authorized the users entering into the network. We manage key techniques for secure data transmission smart card device in vehicular ad hoc networks. The dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users join and leave operations. The primary user will directly link with the authority and secondary users receive the information from the primary user. It also has been verified by the primary user by the group key. The future development of this project provides a numbers for authentication but in future strings will be used for authentication purpose and transmit text messages to the users, in future system will transmit images and videos too to the users.

V. REFERENCES

[1]. X. Sun, et al., "Secure vehicular communications based on group signature and ID-based signature scheme," in Proc. IEEEICC, 2007, pp. 1539–1545.

[2]. A. Dhamgaye and N. Chavhan, "Survey on security challenges inVANET," Int. J. Comput. Sci., vol. 2, no. 1, pp. 88–96, 2013.

[3]. J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: 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.

[4]. K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular Ad Hoc networks," IEEE Trans. Veh. Technol., vol. 62, no. 2, pp. 536–551, Feb. 2013.

[5]. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[6]. W. Shen, L. Liu, and X. Cao, "Cooperative message authentication in vehicular cyber-physical systems," IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 84–97, Jun. 2013.

[7]. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLAbroadcast authentication protocol," RSA Crypto., vol. 5, no. 2, pp. 2–13, Aug. 2002.

[8]. J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy preserving vehicular communication framework," in Proc. IEEE INFOCOM, Anchorage, AK, USA, May 2007, pp. 103–108.

[9]. C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16– 30, Feb. 2000.

[10]. X. L. Zheng, C. T. Huang, and M.Matthews, "Chinese remainder theorem based group key management," in Proc. 45th ACMSE, Winston-Salem,NC, USA, 2007, pp. 266–271.

[11]. P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method," Comput. Math.Appl., vol. 65, no. 9, pp. 1360–1368, May 2013.

[12]. N. V. Vighnesh, N. Kavita, R. Shalini, and S. Sampalli,"Anovel sender authentication scheme based on hash chain for vehicular ad-hoc networks,"in Proc. IEEE Symp. ISWTA, Langkawi, Malaysia, 2011, pp. 96–101.

[13]. P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communicationsassumptions, requirements, and principles," in Proc. 4th Workshop ESCAR, Lausanne, Switzerland, 2006, pp. 5–14.

[14]. C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,"in Proc. IEEE ICC, Beijing, China, May 19–23, 2008, pp. 1451– 1457.

[15]. L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch based group key management protocol applied to the Internet of things," Ad Hoc Netw., vol. 11, no. 8, pp. 2724– 2737, Nov. 2013.

[16]. S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in Proc. IEEE Int. Conf. ITST, St. Petersburg, Russia, 2011, pp. 613–618.

[17]. X. Lv, H. Li, and B. Wang, "Group key agreement for secure group communication in dynamic peer systems," J. Parallel Distrib.

Comput.,vol. 72, no. 10, pp. 1195–1200, Oct. 2012.
[18]. P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralized group key management for secure multicast communication,"IET Inf. Security, vol. 8, no. 3, pp. 179–187, May 2014.
[19]. X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in Proc. IEEE ICC,Jun. 2007, pp. 1539–1545.
[20]. K. Matusiewicz, J. Pieprzyk, N.Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of simplified variants of SHA-256," in Proc. WEWoRC, Louvain, Belgium, Jul. 2005, pp. 112.