Dual Authentication and Key Management for Secure Transmission in Vanet

SAYANA S S[1], L M BERNALD[2]

[1]M.Tech Computer Science and Engineering, Rajadhani Institute of engineering and Technology Nagaroor, Attingal, Thiruvanathapuram, Kerala, India
[2]HOD Department of Computer Science and Engineering, Rajadhani Institute of engineering and Technology Nagaroor, Attingal, Thiruvanathapuram, Kerala, India

---***---

Abstract - *VANET is a self-organizing communication network that is constructed among the moving vehicles. VANET have recently become popular for research, with attention to improve the driving experience and road safety. VANET usually encompass Trusted Authority (TA) that is meant to supply online premium service to nodes in network. It is necessary to keep up the authentication and confidentiality of the messages transmitted between the TA and nodes. Trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. Therefore, it is important to maintain the confidentiality, security and authentication of messages exchanged between the TA and the VANET nodes. Dual authentication scheme to produce advanced security level to effectively top the unauthorized vehicle going in VANET environment. Group key management theme with efficiency distributes a group key to different VANET nodes. Vehicular communication networking is a promising approach of facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. However, it is subject to various malicious abuses and security attacks which hinder it from practical implementation. In order to solve these problems and to enhance the driving comfort, appropriate traffic information should be provided to the drivers in a smart and secured way. Security improvement in the vehicle's side to resist malicious users entering into the VANET, After completing the authentication process, the TA can multicast the information to the authenticated vehicles.*

***Key Words*: Authentication, vehicle secret key, Chinese remainder theorem, group key management, VANET.**

1. INTRODUCTION

VEHICULAR Ad-hoc Network (VANET) is a distributed, self-organizing communication network, which is built among moving vehicles. Due to the promising features and their security properties, VANETs have extensive attention in the research community in recent years. In general, a VANET consists of three major components, namely the Trusted Authority (TA), Road Side Units (RSUs) and vehicles. The TA provides a variety of online premium services to the VANET users through RSUs. The RSUs are fixed at the roadsides which are used to connect the vehicles to the TA. Each vehicle is installed with an On Board Unit (OBU) which is used to perform all computation and communication tasks. Various statistical studies reveal that due to road accidents, many people have either died or injured and the traffic jams generate a tremendous waste of time and fuel. In order to solve these problems and to enhance the driving comfort, appropriate traffic information should be provided to the drivers in a smart and secured way. Therefore, VANETs are developed to provide attractive services such as safety services that include curve speed warnings, emergency vehicle warnings, lane changing assistance, pedestrian crossing warnings, traffic-sign violation warnings, road intersection warnings and road-condition warnings. In addition, it can offer the comfort services such as weather information, traffic information, location of petrol stations or restaurants, and interactive service such as Internet access.

In addition, it can offer the comfort services such as weather information, traffic information, location of petrol stations or restaurants, and interactive service such as Internet access. Two types of communications are performed in VANETs. The first type is the Vehicle to Vehicle (V2V) communication in which the moving vehicles can communicate with each other and the second type is the Vehicle to RSU (V2R) communication in which the moving vehicles can communicate with the RSUs which are located aside the roads. The V2V and V2R communications are carried out using the Dedicated Short Range Communications (DSRC) standard [2]through an open wireless channel. Each RSU and OBU uses a DSRC radio, based on IEEE 802.11p radio technology to access the wireless channel along with a directional or a unidirectional antenna. If an RSU wants to transmit a message to a specific location, a unidirectional antenna is used. Authentication is a process of verifying a user identity prior to granting access to the network. It can be considered as the first line of protection against intruders. The authentication process ensures that only valid vehicles can be part of the group in VANET. A new dual authentication scheme is proposed to provide the security improvement in the vehicle's side to resist malicious users entering into the VANET. After completing the authentication process, the TA can multicast the information to the authenticated vehicles. In this technique, the TA generates two different group keys for two different groups of users, namely primary user group and secondary user group. In the generated group keys, one group key is used for multicasting the information from the TA to primary users (PUs) and the other group key is issued for broadcasting the information from primary users to secondary users (SUs).However, the shared cryptographic group keys should be refreshed through a proper racing operation at the time of group membership changes due to new users joining into the network or old users leaving from the network. Therefore, an old group member has no access to present communications (forward secrecy) and a new member has no access to previous communications. 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.

2. LITERATURE SURVEY

2.1 In 2007 Xiaoting Sun et al., [2] propose a novel security protocol based on group signature and identity-based signature scheme to meet the unique requirements of vehicular communication networks. The proposed protocol not only guarantees security and anonymity, but also provides easy traceability property when the identity of the sender of a message has to be revealed by the authority. To further enable Internet access, the network architecture incorporating with the proposed security protocol is introduced. Simulation is conducted to analyze the system performance which proves the feasibility of the proposed scheme. Vehicular communication networking is a promising approach of facilitating road safety, traffic management, infotainment dissemination for drivers and passengers. However, it is subject to various malicious abuses and security attacks which hinder it from practical implementation. This paper tackles the problem of security assurance and conditional privacy protection in VANETs. To the best of our knowledge, this is the first study that deals with the issue of security and conditional anonymity in VANETs through a cryptographic approach, where the techniques of group signature and identity-based signature are adopted. it presents a novel security mechanism for IVC applications based on group signature scheme. With the group signature, security, privacy, and efficient traceability can be achieved without inducing the overhead of managing a huge number of stored certificates.

2.2. In 2005 L. Wischhof, et al., [1] a novel method for scalable information dissemination in highly mobile ad hoc networks is proposed: segment-oriented data abstraction and dissemination (SODAD). With SODAD, information can be distributed in an information range multiple orders of magnitude larger than the transmission range of the air interface, even if only 1%–3% of all vehicles are equipped with an IVC system,e.g., during market introduction. By restricting the method to the dissemination of map/position-based data, scalability is achieved. An example application for the SODAD method is presented: a self-organizing traffic-information system (SOTIS). In SOTIS, a car is equipped with a satellite navigation receiver, an IVC system, and a digital map. Each individual vehicle collects traffic information for its local area. Using the digital map, the traffic information is analyzed based on road segments. The performance of the proposed methods is evaluated using network simulation with vehicular mobility models. Simulation results for typical scenarios are presented. Furthermore, a prototype implementation based on commercially available standard hardware demonstrates the feasibility of the proposed approach. Inter vehicle communication (IVC) is an emerging topic in research and application that is getting increasing attention from all major car manufacturers.

2.3. In 2013 K. Mershad et al., [5] system that takes advantage of the RSUs that are connected to the Internet and provide various types of information to VANET users. it provide a suite of novel security and privacy mechanisms in our proposed system, and evaluate its performance using the ns2 software. it show by comparing its results to those of another system its feasibility and efficiency. Inter-vehicular communications (IVC) lie at the core of a number of industry and academic research initiatives aiming to enhance safety and efficiency of transportation systems. Many forms of attacks against service-oriented VANETs that attempt to threaten their security have emerged. . How to ensure security and privacy in service-oriented VANETs represents a challenging issue. proposed privacy-preserving data-acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption. We are designing an RSU scheduling mechanism in which an RSU builds a schedule that is divided into time-slots (TSs). In each TS, all users that are expected to connect to the RSU are specified.

2.4. In 2011 Jiun-Long Huang, et al., [4] introduce an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. In vehicular ad hoc networks (VANETs), the speed of a vehicle is for efficient authentication is inevitable. Compared with the current key agreement scheme, ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. ABAKA considers not only scalability and security issues but privacy preservation as well. To deal with the invalid request problem, a detection algorithm has also been proposed. In the analytical analysis, we have elaborately evaluated ABAKA with current standard ECDSA schemes and other batch-based schemes in terms of verification delay and transmission overhead, as well as the verification cost forereach verifications. Moreover, the efficiency and practicality to the real-world applications have been verified by the simulation analysis.

2.5. In 2011 Y. Hao, et al., [7] . A practical cooperative message authentication protocols thus proposed to alleviate the verification burden, where each vehicle just needs to verify a small amount of messages. Details of possible attacks and the corresponding solutions are discussed. it propose a novel distributed key management scheme based on the short group signature to provision privacy in the VANETs.

3. PROBLEM DEFINITION

Many existing techniques are available in the literature for Providing authentication in the VANET. Among the various existing techniques, Johnson et al. 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. 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 any RSU. This certificate is frequently updated to provide privacy-preserving authentication, which creates an additional overhead. It represented 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 over- head for message verification. However, the communication overhead increases when the density of vehicles is higher.

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. Syamsuddin et al. presented a comparison of various RFID authentication protocols based on the use of the hash chain method. However, among these existing protocols, most of them have addressed a specific issue called authentication. All these schemes fail to propose an integrated approach to provide the authentication as well as confidentiality services in VANET. Perrig represented a Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, which uses symmetric keys instead of using asymmetric keys. Since the symmetric key systems are significantly faster than signatures, the Denial of Service (DoS) attack is averted in this system. In the group signature, one group public key is connected with multiple groups of private keys. In this group signature scheme, an attacker can easily find a message sent by the group, but it is not possible to track the sender of the message. Lin proposed a time-efficient and secure vehicular communications (TSVC) scheme for sequential message authentication. In this scheme, a vehicle first sends a hash chain to its neighbours and then it generates a MAC based on the elements of the hash chain through which the neighbours can authenticate this vehicle's messages. Due to fast MAC verification, this scheme considerably reduces the message loss ratio. However, in large scale networks, a vehicle is needed to broadcast its hash chain much more frequently to neighbours and hence the message loss ratio could increase.

Many existing schemes available in the literature are used to provide authentication only. Therefore, we have discussed some of the existing group key management methods used in the wired and wireless networks. Among these schemes, Wong presented a novel solution to the scalability problem of group or multicast key management. They introduced the concept of key graphs for specifying secure groups. In addition, they presented three strategies for securely distributing rekeying messages after a join and leave operation in the secure group. In the rekeying strategies, join and leave protocols have been implemented in a prototype key server that they have built. The main limitation of this approach is the increased computational complexity. The main advantage of their approach is that the number of broadcast messages to distribute the group key to user side is minimized. Moreover, the user side key computation is also minimized. However, the main limitation of their approach is that computation complexity of the key server is very high. Proposed a CRT based static key structure for distributing the group key to the members of the group when group membership changes. The main contribution of this work is that it minimizes broadcast messages and also minimizes user side key computation. In addition, the memory requirements are high in most existing schemes. Comparing with most of the existing authentication and group key management schemes existing in the literature, the authentication scheme proposed in this paper is a dual authentication scheme with intelligent decision making for vehicle movement.

4. METHODOLOGY

Trusted Authority (TA): The TA is responsible for the registration of RSUs, vehicle OBUs and the vehicle users and it is also responsible for key generation and distribution to support secure premium services in the VANET system. In our scheme, every state in the country has a TA. When a vehicle moves from one state to another state, the vehicle's credentials will be verified using the TA of the registered state, which is initiated by the TA of the state where the vehicle is roaming currently .we have illustrated a single TA for our convenience. In addition to this, each TA authenticates the identity vehicle OBU's or the identity of users to avoid malicious vehicles entering into the VANET system.

Road Side Unit *(*RSU): RSUs are deployed at the roadsides and they are regularly monitored and managed by the TA].These units act like bridges between the TA and the vehicles. The RSUs connect with the TA by a secure wired network and OBUs by an open wireless channel.

Vehicles: Each vehicle is embedded with an OBU in the VANET system. The vehicles can communicate with other vehicles and RSUs through this OBUs. The vehicles can communicate with the TA through the RSUs. The OBU consists of six major components, namely an encryption/decryption agent, data collection agent, spatial-temporal reasoning agent, Fuzzy inference engine, rule base and decision making agent.

Secret Key: In contrast to public key cryptosystems, symmetric key cryptosystems offers the advantage of low communication overhead as well as relatively low computational complexity. symmetric key cryptosystems require transmitting and receiving communication vehicles to agree on a secret key prior to communication.

VANET: It is a self-organizing communication network that is created among the moving vehicles. VANET have recently become popular for research, with attention to advance the driving experience and road. VANET usually incorporate Trusted Authority (TA) that is meant to source online premium service to nodes in network. It is required to keep up the authentication and confidentiality of the messages transmitted between the TA and nodes. protection. VANET usually incorporate Trusted Authority (TA) that is meant to source online premium service to nodes in network.

Chinese remainder theorem Key: computational overhead is also reduced. Overhead on the trusted authority is also decreased here as the communication of the messages happens in the steps like from TA to RSUs, and then RSUs to the primary vehicles and primary vehicles to the secondary vehicles respectively.

4.1 Dual key Management for Communication

Dual Key Management is a group key management scheme in which the TA computes two different group keys intended for two different groups in VANETs. The group is a very important concept in our scheme. Based on the money paid to the TA, a very simple Service Level Agreement (SLA) is considered between the TA and the vehicle users, which categorize the vehicle users into three groups, namely Primary Users (PUs),Secondary Users (SUs) and (UUs) in a predefined manner. The PUs are eligible to get attractive services such as safety, comfort services and interactive services from the TA. The PUs are authorized VANET users who receive these services from the TA side periodically. The SUs are also authorized VANET users who receive the attractive service such as safety services from the PUs without making any requests to them, but they cannot receive the information directly from the TA.

4.2 Proposed Dual Authentication Technique

This VSK is used for authenticating the vehicles when they enter into the VANET to start communicating with other vehicles and RSUs. In order to improve the authentication process, we use a dual authentication technique in this paper where the authentication process is performed two times. For the first time, authentication is done on the vehicle side and the second time, authentication is done in the TA side and hence the intruder has no possibility to enter into the VANETs. In the TA, the authentication is performed by verifying the Hash Code (HC) generated by the vehicle using their VSK. The authentication was performed on the vehicle side by verifying the fingerprint given by the user at the time of registration.

5. CONCLUSION

In this paper, we proposed a new dual authentication scheme for improving the security of vehicles that are communicating with the VANET environment. For providing such authentication in dual mode, we used two components such as hash code and fingerprint of each communicating vehicle user. Therefore, the fingerprint authentication technique is integrated into a hash code creation method in this paper to avoid malicious users to use the secret key of any VANET users in order to participate in the VANET communication. Moreover, to avoid malicious users from spoofing the authentication code issued for any VANET users and sending erroneous messages to other vehicles we have introduced a new dual key management scheme in this research paper. The dual key management scheme implemented in this paper is computationally efficient that supports secure data transmission from TA to PUs and SUs based on two different group keys, one for PUs and another one for SUs for further improving the security among different classes of vehicles. Moreover, our proposed algorithm also takes single broadcast messages from TA to inform the group members in order to recover the updated group key. The future development of this work is to devise new methods in order to preserve the vehicle's location privacy from the intruders.

REFERENCES

[1] L.Wischhof, A. Ebner, and H. Rohling,"Information dissemination inself-organizing inter vehicle networks," IEEE Trans. Intell. Transp. Syst., vol. 6, no. 1, pp. 90–101, Mar. 2005.

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

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

[4] 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.

[5] 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.

[6] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput.Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[7] 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.