ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Defended Data Communication in VANET Using Dual Authentication

D.Kiruthika[1], S.Dharani[1], S.Abirami[1],.J.Nandhini[2]

[1]UG Scholars, Department of Electronics and Communication Engineering, Jay Shriram Group of Institutions, Tirupur, Tamilnadu, India

[2]Associate Professor, Department of Electronics and Communication Engineering, Jay Shriram Group of Institutions, Tirupur, Tamilnadu, India

ABSTRACT-Dual authentication and special key are becoming a crucial security component in vehicle, where the technology that employs moving vehicles as a nodes in a network and use a wide variety of authentication in vehicles, fixed roadside units (RSUs) and regional trusted authorities (RTAs) as mobile wireless devices and demand for vehicle to vehicle communication (V2V) and vehicle to roadside communication (V2R) increases. Information exchanged between vehicles with help of RSUs and explained about possible attacks and their solutions are discussed. In this paper, we investigate the authentication issues and utilizing the IBS scheme in V2R communication and together with the IBOOS scheme in V2V communication for better performance. In IBOOS for VANETs the offline phase can be executed initially at RSUs or vehicles, while online phase is to be executed in vehicles during the V2V communication. We further introduce a special key distribution individually by approaching NS2 simulator.

KEYWORDS: Authentication, VANET, IBOOS, Roadside units, Regional trusted authority, and identity based signature.

I.INTRODUCTION

VANET is the application of MANET. The vehicular adhoc networks having the functionalities of vehicular safety, traffic monitoring and location based route planning and which is working among moving vehicles and which is enabled by wireless communication and it produce enormous research attention to rising challenges of safe driving. VANET, consisting of a network of vehicles, moving at high speeds that communicate among themselves with different purposes, being the main purposes that of improving security on the road.

In VANETs, the authentication issues of users is a crucial security service to both inter-vehicle and vehicle to roadside communication had to be control and attacks on their privacy and private data will be misuse in case of vehicles have to be protected. VANET project is still research in India, vehicle to vehicle communication is must in the passing traffic congestion. Road side units are used to connect the regional trusted authorities and vehicle for communication to avoid the traffic and accidents. Trusted authority (TA) is used for register the vehicles details such as owner's name, vehicle number, owner's address etc. In VANETs, the importance of privacy raised by security. There is a possibility of misbehavior in a RSUs, the key distribution is secured process with the authentication framework.

For identifying the malicious node packets, the RSUs are mainly involved. A vehicular ad hoc networks [VANET] is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among vehicle nearby fixed road side units [RSUS] and regional trusted authorities [RTAS].A VANET considered as a variant from of a mobile ad hoc network (MANET) However, the mobility of vehicles is constrained by predefined roads ,the road speed limits or the congestion level in VANET.

In VANETs, the user authentication is crucial security service for access control in both inter vehicle and road side communication. In networks, vehicular communication systems in which vehicles and road side units are communicating through the nodes, providing each other with information and warnings for safety and it can be effectively working for avoiding the traffic.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The major contributions of this paper are summarized as follows:

i. In vanet, we introduce a dual authentication technique with the prevention of malicious vehicles.
ii. We propose a special key management technique to transfer the data among vanet vehicles.
iii. VANET, emergency warning messages are simultaneously transmitted via V2V and V2R communication in order to achieve multipath diversity routing.

V2R communication is necessary to provide reliability, safety and comfort. Vehicles appear as a nodesVANET faces the challenges like security, privacy, latency and mobility. These vehicles are registered in regional trusted authority. VANET provide the connection between the vehicles, when they have limited communication infrastructure.

II. PPREVIOUS WORKS

Many techniques are available in the VANET for concerning for improving security and faced the attacks. In this paper, the vehicle secret key (VSK) is the main mechanism of authenticating the vehicles. This technique is mainly responsible for the communication from one vehicle to another vehicle or one vehicle to RSUs while they entering into the VANET environment. By using this to improve the security and safety measures. In order to evaluate this technique can be performed by two times. By the first time, it is performed on vehicle side and on the other hand the authentication is performed in trusted authority side. So the intruder has no possibility to enter into the VANET environment. In trusted authority side, the security performance is enhanced by obtaining by the hash code. These hash code (HC) are generated by the vehicles by using VSK on the other hand, the security performance is obtaining by fingerprint in vehicle. At the time of registration, the fingerprint is verified by the user. The main purpose of the dual authentication technique is that the intruder cannot enter into the VANET communication because they were not register their fingerprint and also they cannot have VSK of particular vehicle.

According to this technique, the registration process is done in two modes: offline mode and online mode. In online mode, the registration process can be performed in the TA's by register their details such as name of the owner, address, vehicle number, contact number etc,.through the internet connection. In offline mode, the user goes to the TA's office directly and he/she register their details for further clarification. In these existing techniques, the authentication process is only performed in office mode. In order to complete this registration process, the user can get the authentication code (AC) to proceed the VANET communication environment by completing dual authentication process. After providing the authentication code (AC), the TA starts its services to the permitted vehicles. By using this technique, the vehicle can communicate from one node to another node.

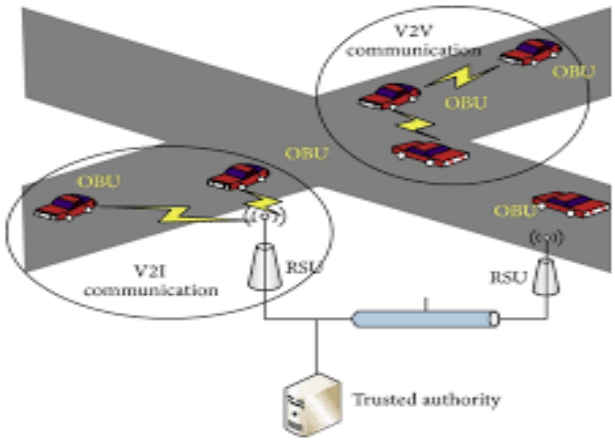


Fig.1 VANET network

In radio frequency identification, the authentication is performed by using hash code. Various protocols are used that make use of hash code method. However, the authors concluded many protocols but these are not specified and also cannot retrieve the problems related to hash code. Therefore, it is difficult to achieve key based approaches with non-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

repudiation. This technique is namely Timed Efficient Stream Loss-tolerant Authentication (TESLA) to provide the key generation.

III. RELATED WORKS

Many proposals are available for privacy preservation of VANET. In preciously, to provide a security for VANET the group key signature is performed. One public key is distributed to all users who all are proceeded in VANET environment. Every user can receive the message which is sent by the group of users. But no user can be identified the sender of any particular messages [7]. The main responsibility for secure group private key distributed is to be provided by the road side units. From the RSU, each vehicle can get the private key for a group of users. For this privacy concern, the RSU misbehave with the vehicle at the time of providing key management [9]. Therefore, many protocols are introduced to enhancing the security for the distributed key management security and also to reduce the collision. Another main critical issue is computation overhead. Vehicles can broadcast the safety messages for every 300 milliseconds while safety driving application.

Since, the computation overhead for every vehicle become intolerable when the density of the vehicle is high and this technique of group key signature is expensive. The technique introduced for the privacy is called Cooperative Message Authentication Protocol (CMAP) and this protocol is mainly responsible for navigation process [6]. In this CMAP, the safety messages are carried the location of the sender. This location information is generated through Global Positioning System (GPS).

IV.PROPOSED SYSTEM

In this section, we propose a private key cryptography (PKC) for security enhancement and privacy preservation. The protocol used in this technique is Identity Based Signature (IBS) and Identity Based Online/Offline Scheme (IBOOS). These schemes are used for authentication process between the vehicles and RSUs. In VANET, the IBOOS scheme is not specifically designed.

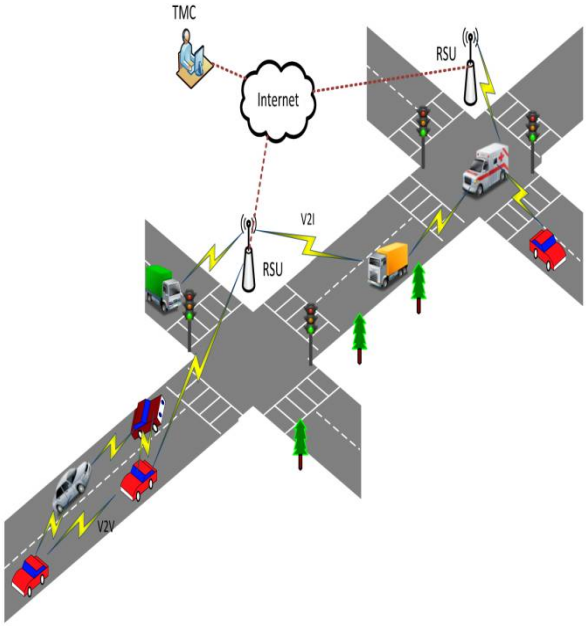


Fig.2 Communication between RSU and Emergency vehicle

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

In PKC various keys are generated and the message will be authenticated by encrypt and decrypt process. This method is used to convert the underline signature into online/offline signature. In offline mode, the messages will be transmitted over a short distance [1]. In online mode, the messages will be transmitted over a wide distance area. In IBOOS scheme, the authentication depends on discrete logarithm problem. In offline signature, more than one message will be reused to sign. IBOOS schemes are consists of following five steps. These five steps are setup, key abstraction, offline signaling, online signaling and verification.

Setup

The first step of the IBOOS scheme is setup. The RTA provides a key and a public parameter for the privacy preservation.

Extraction

In the process of extraction the private key is generated with the ID.

Offline signaling

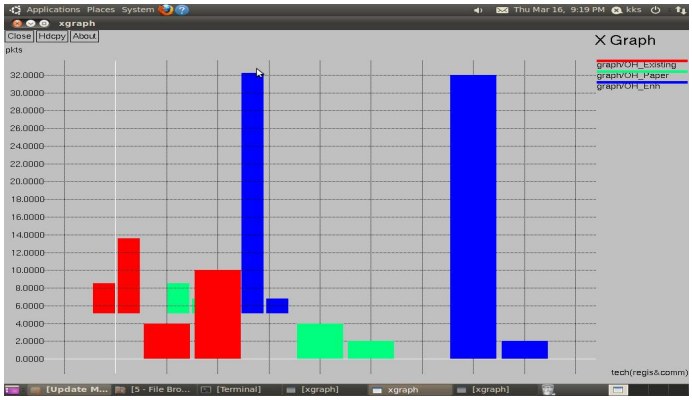
RTA/RSU generates an offline signature based on the private key and public parameter for every vehicle.

Online signaling

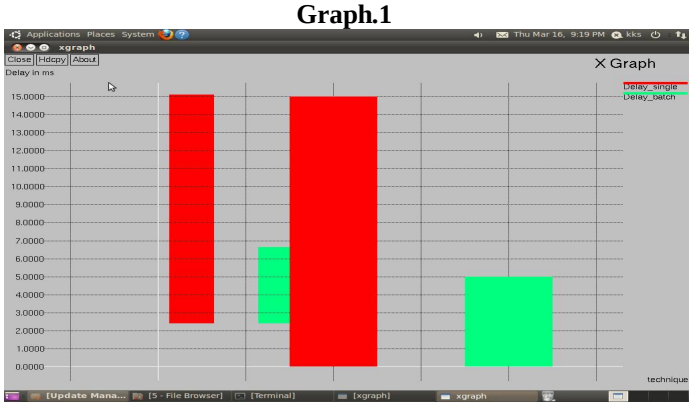
The online signature is generated is generated by the sending vehicle based on the message and offline signature.

Verification

Every vehicle should be verified by the RSU. After verification, the RSU communicate with the vehicle which is covered by the coverage area.



Graph.1



Graph.2

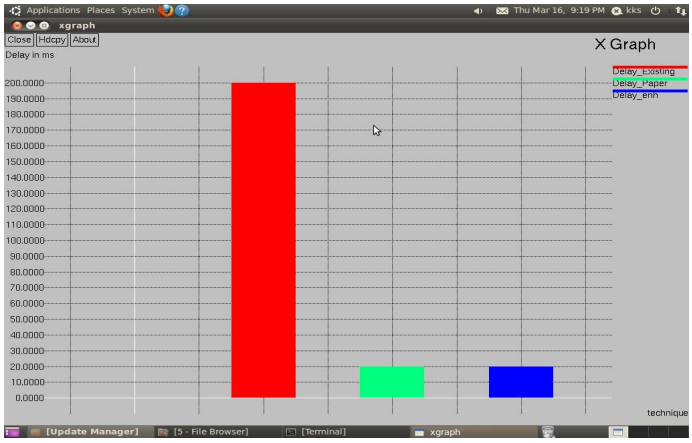
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



Graph.3

A. Network Design

In VANET communication, there are three types of networks such as RSU, RTA and vehicles. This communication of VANET is mainly considered with the vehicles travelling on road. The vehicle should not stop anywhere on the road frequently used for particular period. The RSU depends upon the vehicle's behavior along with the RTA. The attacker doesn't interfere into the VANET communication because everyone having unique ID and this ID cannot hack by the intruder.[2]

VANETs can be classified mainly into the following three types, the vehicle-to-roadside communication, and the roadside to- vehicle communication, and the vehicle-to-vehicle communication. Other communications are through secure wired channels, such as inter-RSU communication and RSU-to-RTA communication [3]. The transmission range of an RSU is assumed to be much longer than that of vehicles. All vehicles use symmetric radio channels.

An RTA generates cryptographic domain parameters for the RSUs and vehicles in its region, and delivers these keys to them over secure channels. It manages a list of vehicles of which the participations have been revoked, updates the list periodically, and advertises the list to the network to isolate the compromised vehicles [8][6]. If a vehicle transmits false messages for malicious purposes on the road, the RTA is responsible for tracing and identifying the source of the messages to resolve any dispute.

An RTA serves in one region, e.g., a city, a province or a country. An ID pool of RSUs in a region is preloaded in each vehicle, in which the number of RSUs is usually fixed that does not change frequently [4] [5].

B. RTA Registration

Road side units need registration for vehicles in OBUs with response of TA and also users responded the key generation and distribution services in VANET. In each country, every state need trusted authority purposing of registration in TA, which helps to identified or verified the moving vehicle credentials from one state to another state[10]. And it helps to identify the current roaming of vehicle, mainly TA where used to avoid the malicious or unauthorized vehicle in VANET system. The cryptographic technique is used in the system where the private keys are generated and distributed to the RSU for the secure data transmission. Each vehicle have a separate key to avoid the malicious node enter into the VANET environment. The vehicle registration is required before a vehicle starts off to hit the road in a region. If the vehicle is newly manufactured, it can be registered to the RTA at the car dealer via a secure network infrastructure [8]. If a vehicle is driven into a new region, it can be registered to the RTA at the entry-exit administration or the border immigration office via the secure network infrastructure. Through the vehicle registration of each vehicle, the RTA registers the vehicle ID and profile [5].

C. RSU registration

RSU act like a bridge between the vehicle and trusted authority, and it collects the information about the location of the vehicle from the trusted authority. The trusted authority connects with the RSU used for the purpose of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

secure wired network [7]. The vehicle, RSU and RTA are made as node here. In simulation the initial process is to create node and it transfers the information to the vehicle about the traffic, any emergency event etc.,

The summery of RSU base registration is given below:

- Vehicle has to generate the Pseudonym by using *Time, Home region, Current RSU, Modified vehicle id*.
- RSU has to broadcast the own information's periodically, which contains the *Time, own public key, RSU id, Digital Sign*
- Vehicle joins into the RSU with newly generated Pseudonym
- RSU verifies the Pseudonym from the vehicles if it correct then RSU will reports to RTA
- RSU will broadcast verified Pseudonym as modified Pseudonym (offline sign).

V. CONCLUSION

In this paper, we proposed the scheme for improving security of vehicles with the help of new dual authentication and single key management. Authentication in dual mode such as username and password with special key. These methods are advanced due to the device method to avoid malicious vehicle users and also avoid unauthorized persons. The computational efficiency of the paper that supports the transmission of the data from TA to public users and public user to separate users based upon the private key. The messages carried and broadcasted from the TA to all vehicles and every vehicle should update the private key for a particular interval. If there is any misuses of the key the users inform to the trusted authority immediately and renew their key for a security concern. The future development of this work is to modify and develop new methods and protocols in order to improve the security.

REFERENCES

[1] L.Wischhof, A. Ebner, and H.Rohling, "Information dissemination in self-organising inter-vehicle networks," IEEE Trans. Intell. Transp. Syst., vol.6, no.1,pp.90-101, March.2005.
[2] Y.Hao, Y.Cheng, C.Zhou, and W.Song, " A distributed key management framework with cooperative message authentication in VANET," IEEE J.Sel.Areas Communi.,vol.29,no.3,pp.616-629, Mar. 2011.
[3] 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.
[4] P.Vijaykumar, S.Bose, and A.Kannan,"Centralised key distribution protocol using the greatest common divisor method," Comput.Math. Appl., vol.65, no,9,pp.1360-1368,May.2013.
[5] N.V.Vighnesh, N.Kavita, R.Shalini, and S.Sampalli, "A Novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in Proc. IEEE ICC, Beijing, China, May 19-23,2008,pp.1451-1457.
[6] X.Cheng, L.Yang, and X.Shen, " D2D for intelligent transportation system: A feasibility study," IEEE Trans.Intell. Transp. Syst. Vol.16, no.4,pp. 1784-1793,Aug, 2015.
[7] X.Cheng Et Al., "Electrified vehicle and the smart grid: The ITS perspective, " IEEE Trans. Intell. Transp. Syst. Vol.16,no.1, pp. 411-416, Feb. 2015.
[8] R.Zhang, X.Cheng, L.Yang, X.Shen, and B.Jiao, " A novel centralized TDMA – based scheduling protocol for vehicular networks," IEEE Transp. Syst., vol.15,no.5, pp.411-416, Oct. 2014.
[9] X.Lin Et Al., "TSVC: Timed Efficient and Secure vehicle communication eith privacy preserving," IEEE Trans. Wireless Commun., vol.7, no.12,pp.4987-4998, Dec.2008.
[10] Pandivijayakumar, Maria Azees, Arputharajkannan, and Lazarus Jegatha Deborah, " Dual authentication and key management for secure data transmission in VANET," IEEE Trans.Intell. Transp.Syst. vol.16 no.6,pp. 1524-9050 Mar.2015