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 6, June 2017

Vehicular Protected Data Transmission over Dual Authentication Algorithm

Uzma Farheen[1], Dr.Ruksar Fatima[2]

P G Student, Department of Computer Science and Engg, Khaja Banda Nawaz College of Engineering, Kalaburagi, India[1]

Vice Principal, Department of Computer Science and Engg, Khaja Banda Nawaz College of Engineering, Kalaburagi, India[2]

ABSTRACT: VANET 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 protection. 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. Hence we address the security issues and challenges where TA classifies the VANET nodes into primary, secondary and unauthorized users. So therefore, in this project we have proposed a dual authentication scheme to produce advanced security level to effectively that stops the unauthorized vehicle entering into VANET environment using smart card. Second, we tend to propose a group key management theme with efficiency distributing a group key to different VANET nodes. From this project, we must send the messages or some safety information from the Trusted authority to the primary user and then primary user to the secondary user with full of secured process.

KEYWORDS: VANET,Dual Authentication;Chinese remainder theorem; key management.

I. INTRODUCTION

For communication between the moving vehicles, a distributed and self-organized network has been built, which is called as VANET that stands for vehicular ad hoc network. Many people have lost their lives because of the road accidents. This may be because of lack of information about the road conditions to the drivers. The safety messages about lane changing assistance, curve speed warnings, road intersection warnings, emergency vehicle warnings, pedestrian crossing warnings, road condition warnings and traffic sign violation warnings. These messages being communicated between the vehicles have to be protected and verified. None of the unauthorized vehicle user should be able to access these safety messages. For increasing the quality of service, intelligent transport systems (ITS) also have been included in the VANETs.

For that purpose, numerous security measures have been implemented such as each vehicular network will be employed with a trust authority (TA); this is called as the authenticated center which validates the authenticity of the vehicles arriving the VANET. The other entities are included in this scheme are Road Side Units (RSU), which are the stationary units, located at the road sides therefore the name given to them. RSU (road side units) are said to be the link between the TA and the third entity called vehicles. TA and vehicles do not communicate directly with each other; hence they pass their messages to RSUs first. RSUs are meant for reducing the broadcast overhead of the TA. As it receives the data sent from TA, it broadcasts it to the vehicles authorized to the VANET. Each vehicle in the VANET will be incorporated with the on board units (OBUs) which are used for performing the tasks related to communication and computation. In addition to the above said safety messages, the other interactive messages about the VANET will be broadcasted by the TA such as weather information, location of the hospitals, restaurants and petrol banks etc., present in that VANET. These messages help in increasing the driving comfort and makes easier for the driver to get the location needed within no time.

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 6, June 2017

II. LITERATURE SURVEY

- **W. Shen, L. Liu and X. Cao** published a paper on **"Cooperative message authentication in vehicular cyber-physical systems" [10].** In this scheme, CMAP which stands for cooperative message authentication protocol is used. It is for finding out the malicious data being broadcasted in the road transport system by the unauthorized vehicles. This favorable technique called cooperative message authentication is used to reduce the computational overhead required for verification of the messages. As the number of vehicle increases in the road transport system, the communication overhead also increases. The main disadvantage of this scheme is that there is no verifier in the system to verify the messages, so the unwanted messages will be communicated between the vehicles.

- **Perring et.al's** publication is **"The TESLA broadcast authentication protocol" [9].** This scheme introduced a protocol with the name timed efficient stream loss-tolerant authentication (TESLA) protocol. This protocol uses symmetric keys for encrypting and decrypting the messages instead of using the asymmetric keys. Symmetric key system uses same key at both the sender and receiver side. Denial of service attacks will be prevented in this scheme as the symmetric keys are being used which are proved to be faster than the signatures. But the limitation of this scheme is that non-repudiation cannot be achieved using symmetric keys.

- **"A group signature based secure and privacy preserving vehicular communication framework"** published by J. **Gua, J. P. Baugh and S. Wang [11].** In this scheme, group signature technique is used to provide the security to the messages being communicated between the vehicles in the VANET. Here, public key of one group will be connected with the private keys of the multiple groups. In this particular group signature method, it is easy for an attacker to find out the group from which the message is sent but the sender of the message cannot be tracked.

- **C. Wong, M. Gouda and S. Lam** published a paper with the title **"Secure group communications using key graphs" [12].** A novel solution for the scalability problem is presented in this scheme of work. As the scalability to the different groups is the biggest problem seen in the network, a concept called key graph is introduced here for the groups. Secure distribution of the rekeying messages is also included in this strategy which will be conducted as a join and leave operation takes place in the system. These join and leave protocols of the rekeying process is implemented in a prototype key server built by them. The main disadvantage of this scheme is that it has high computational complexity.

- **X. L. Zheng, C. T. Huang, and M. Matthews** published a paper on **"Chinese remainder theorem based group key management" [13].** In this scheme, a two centralized group key management protocols is proposed based on the Chinese remainder theorem (CRT). Here the number of the messages broadcasted for distributing the group keys to the vehicle users is minimized. Key computation time is reduced. Key computation overhead of the vehicle users is also minimized. The main drawback of this system is it introduces high computational complexity on the server during key generation process.

III. EXISTING METHODOLOGY

In the existing pattern of work, verification of the vehicles was performed by utilizing the asymmetric key idea, which is public key and private key idea. The verification center used to generate both the keys. Private Key was for the verification center itself and the related public keys will be circulated among the vehicles. It was the responsibility of the verification center to broadcast the public keys to the vehicles and to the road side units. Here the notion of gathering the fingerprint from the vehicle users was excluded. The public keys were produced in a sequence in which the attacker was able to guess the keys easily. Verification center broadcasts the message by encoding it utilizing its private key and vehicles decode of by utilizing their public keys. As the idea of smart cards is not utilized here that is, no fingerprints will be gathered from the vehicle users so any of the unapproved vehicle user who gets the broadcasted public key message will be capable to access the facilities given by the VANET

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 6, June 2017

IV. PROPOSED WORK

The proposed project is distributed between three components such as trusted authority, roadside units and the vehicles. Trusted authority is the verification center where the vehicles are required to get register in order to benefit the facilities. Registration of the vehicle will be done offline because as soon as the vehicle come into the VANET and requests to acquire the services, then the vehicle user must first go to the verification center for getting registered. Amid the registration process, the the TA gathers the fingerprint of the vehicle user and issues a smart card to the user of the vehicle which is having a vehicle secret key (VSK) which is assembled in that. VSK and the relating vehicle user's fingerprint must match then no one but user can benefit the facilities being given by the VANET. Roadside units are said to be the links associating the verification center and the vehicles as there is no immediate communication likely possible between the vehicles and the TA. And the TA encodes the message utilizing its private key and it includes the ID of the vehicle to which the message is expected and directs it to the RSU, and after that the RSU forward the message to the corresponding vehicle. RSUs are the static units and they have reduced considerable part of the work load of the TA as far as broadcasting the messages to the vehicles. Vehicles subsequently receiving the safety message from the TA by means of RSU, decodes it utilizing the public key of the TA. At that point the primary users (PUs), broadcasts the message to the secondary users (SUs).

System Architecture

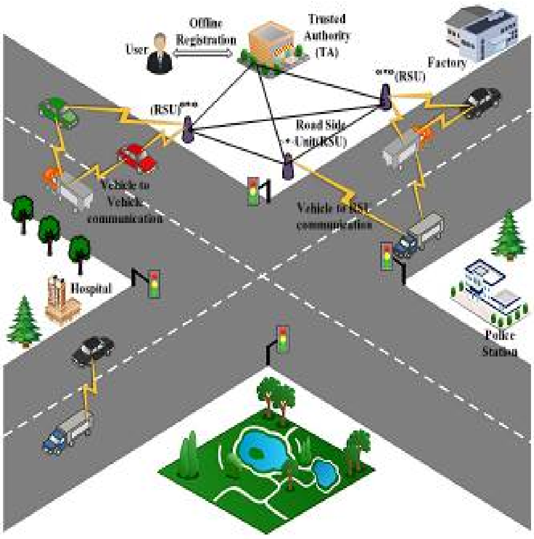

Fig 1: System architecture of the VANET

Fig 1 system architecture includes design of VANET consist of a trusted authority (TA) which is additionally known as the verification center. TA is utilized for vehicle registration, key generation and key distribution and so on. At that point, roadside units (RSUs) are the communication links between the TA and other vehicles

V.SIMULATION AND RESULTS

Simulation studies involves that there is increase in performance ratio and packet delivery rate in the proposed system as depicted in Fig 2 by and there is zero packet loss ratio as depicted in Fig 3 thus decreasing the overhead of the TA in the VANET. The dual key management technique implemented in this paper is computationally efficient that supports secure data transmission from TA to PUs and PUs to 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

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 6, June 2017

Fig 2: Packet Delivery Rate

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 6, June 2017

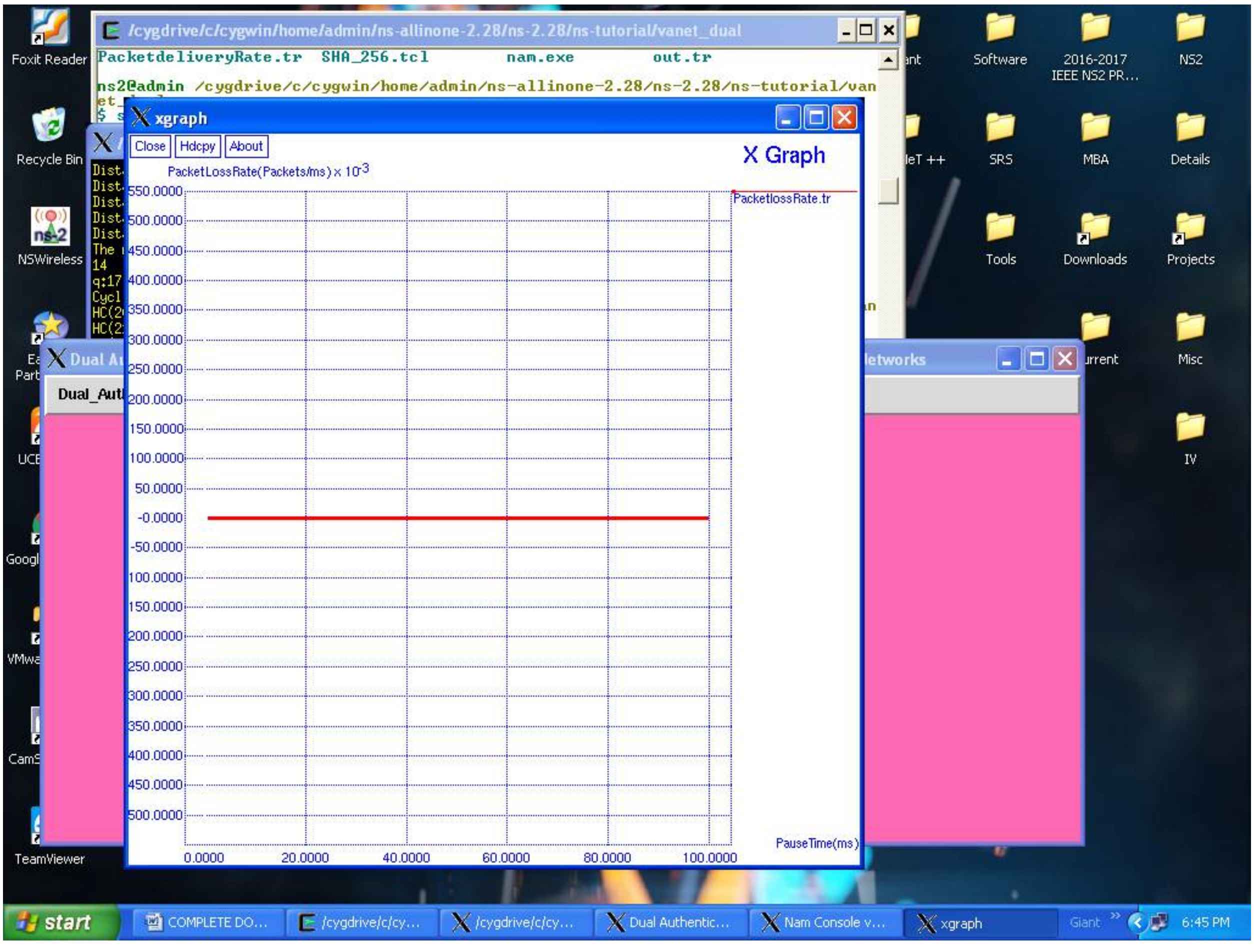

Fig 3: Packet loss ratio graph

VI. CONCLUSION AND FUTURE WORK

In this proposed project, for growing the security of the messages that are being communicated in the VANET, a new dual authentication technique is presented. The hash code function is used along with the fingerprints of the registered vehicles to avoid the unauthorized user. Because of the use of 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. TA updates the keys very easily with a single message. The future development of this work is to create new approaches to save the vehicle's area security from the intruders

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 in VANET," Int. J. Comput. Sci., vol. 2, no. 1, pp. 88–96, 2013*

[3] 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.*

[4] 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.*

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 6, June 2017

[5] D. Johnson, A. Menezes, and S. Vanstone, *"The elliptic curve digital signature algorithm (ECDSA)," Int. J. Inf. Security, vol. 1, no. 1, pp. 36–63, Aug. 2001.*

[6] A. Wasef, Y. Jiang, and X. Shen, *"ECMV: Efficient certificate management scheme for vehicular networks," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, 2008, pp. 1–5.*

[7] 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.*

[8] I. Syamsuddin, T. Dillon, E. Chang, and S. Han, *"A survey of RFID authentication protocols based on hash chain method," in Proc. 3rd ICCIT, 2008, vol. 2, pp. 559–564.*

[9] 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.*

[10] 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.

[11] 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.

[12] 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.*

[13] 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.*