Message Authentication for Secure Data Dissemination in VANET

Pooja Patel[1], Krunal Panchal[2]
[1]Student LJIET, Ahmedabad, India, [2]Assistant Prof. LJIET, Ahmedabad
[1]IT Engineering
[1] LJIET, Ahmedabad, India.

Abstract: *Vehicular Ad-hoc Networks (VANETs) have been explored as to upgrade driver's safety and comfort in revolutionizing the vehicular communication industry. VANETs facilitate vehicles to share safety and non-safety information through messages. Safety information includes road accidents, natural hazards, roadblocks etc. Non-safety information includes falling information, traveller information etc. The primary objective behind sharing this data is to reduce road accidents by alerting the driver about the unexpected hazard. In these paper use advance cryptography mechanism between V2V,V2I,V2R for message authentication using ECC.At long last the relative ease of use of the proposed algorithm in the said application area is worked out and that demonstrates the strength of the scheme over the existingsystems.*

Keywords: VANET, Authentication, Elliptic Curve Cryptographic algorithm

I. INTRODUCTION

Vehicles related with every other through an ad hoc formation form a wireless network called "vehicular Ad hoc Network". "A mobile ad hoc network (MANET) comprises of mobile nodes that associate themselves in as decentralized, self-organizing manner and may likewise build up multi-hop routes. On the off chance that mobile nodes are cars, this is called vehicular ad hoc network" [15]. VANET is subgroup of MANET. Vehicular ad hoc networks (VANETs) are expected in improving road safety and traffic conditions, in which security is essential [7]. Vehicles communicate with each other by means of vehicle-to-vehicle (V2V) communication and with an infrastructure called Road Side Unit (RSU) by means of Vehicle-to-Infrastructure (V2I) communication. Every Vehicle is outfitted with an On Board Unit (OBU) with communication and handling capability. Vehicles communicate with each other and with the infrastructure via Dedicated Short-Range Communication (DSRC) standard [8].

There are three ways for data dissemination in VANET:(1)**Vehicle to Vehicle** is vehicle to vehicle architecture where vehicles act as both consumers and producers as vehicles receive information from other vehicles in the network and distribute that information to other vehicles in the network. So, both collection and distribution of data are done within the network for faster delivery of messages, (2)**Vehicle to Infrastructure** is vehicle to infrastructure wireless architecture in which infrastructure is used to collect information from vehicles and provide that information to other vehicles when necessary, (3) **Hybrid** is the combination of both V2V and V2I. Every node i.e., a vehicle or RSU communicates with other nodes in single hop or multi hop. VANETs are designed with the goals of enhancing driving safety and providing passenger comfort [9].

II. RELATED WORK

ECDH-ECDSA aggregation [1] is a new security schema, by specifying an interaction zone, where a secret shared resulting from ECDH algorithm have been before the authentication step, simulation proves that even if ECDH-ECDSA aggregation schema takes about 40ms more than ECDSA schema and provides higher level ofsecurity but using ECDH-ECDSA aggregation schema average of end to end delay is higher than ECDSA.

QRcode [2] is used in message encryption and decryption increases the performance of the system, since it provides the facility of high speed encoding and decoding process.

Secure data dissemination among vehicles in VANET is difficult for solving that Timestamp defined message authentication code(TDMAC) [3] is used, which performs well in both qualitatively and quantitatively.

Cooperative authentication protocols [4] and group key (GK) [4] distribution protocols were proposed for efficient authentication and revocation. The protocols intake advantage of the fact that each vehicle can cooperate in the message verification processes by selectively verifying its received signatures and by reporting its own verification results to neighbouring vehicles, because vehicles in same area possess nearly the same set of messages.

PBAS [5] propose for reduce the computational overhead of RSUs using the distributing computing. In PBAS proxy vehicles are used to authenticate multiple messages with verification function at the same time [10].

A local identity- based anonymous message authentication protocol (LIAP) [6] for VANETs, in which each vehicle and road side unit (RSU) is assigned a unique long term certification from the certificate authority (CA) in registration phase. RSU is in charge of managing and assigning the local master keys to every vehicle of entering its communication range. When vehicle meets a new RSU, they authenticate each other by their long certificates. The valid vehicle can obtain the local master keys from current RSU to generate the localized anonymous identity. To protect privacy, vehicle randomly chooses the anonymous identity to sign the safety-related message, which can be efficiently verified by the single or batch authentication manner [6].

III. PROPOSED SYSTEM

The broadcast medium is the 5.9-5.95 GHz radio spectrum, and the communication standard are defines in the IEEE 802.11p standards. The information consists of speed and position data is collected from vehicles. Speed data can be gathered from the vehicle speedometers and position data can be gathered using GPS receivers which is fitted to the vehicles.

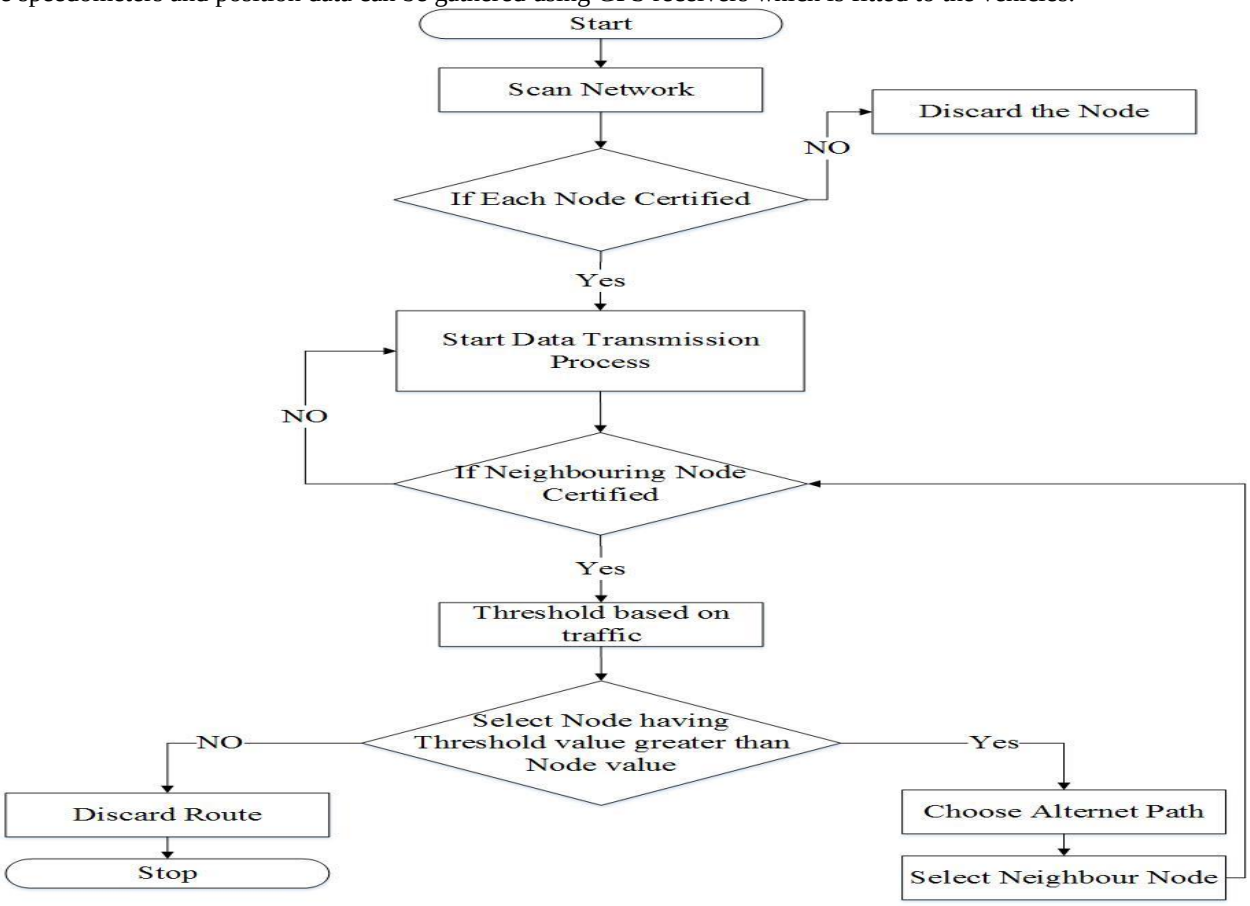

Fig- 1 Proposed Method

Data are gathered and encapsulated in data packets that are broadcast over the wireless medium. This is what calls the data dissemination phase. Data dissemination process done using “Event Driven Safety Message”. Event Driven Safety messages may be generated as a result of a dangerous situation or when abnormal condition is detected such as road accident. This message usually has strong reliability and need to be delivered to each neighbour with almost no delays.

IV. RESULT ANALYSIS

Experiment of proposed method is executed on computer having Intel (R) Core (TM) i5-6200U CPU@2.30GHz with 4GB RAM having Windows 10(64 bit) operating system. Using this proposed methodology end to end will reduce than existing method which is shown in figure-2. The parameters of the chosen scenario are describe in Table-1.

Table-1 Simulation parameters

Parameter	***Value***
Number of vehicle	*15-40*
Vehicles's speed	*20-60km/h*
Wireless protocol	*IEEE 802.11p*
Channel bitrate	*11Mbps*
Carrier frequency	*2.47 X 10^9 Hz*
Message sending time in the interaction zone	*2s*
Distance between RSU	*100-300m*
Interaction zone	*10m*
Bandwidth	*11 X 106 Hz*

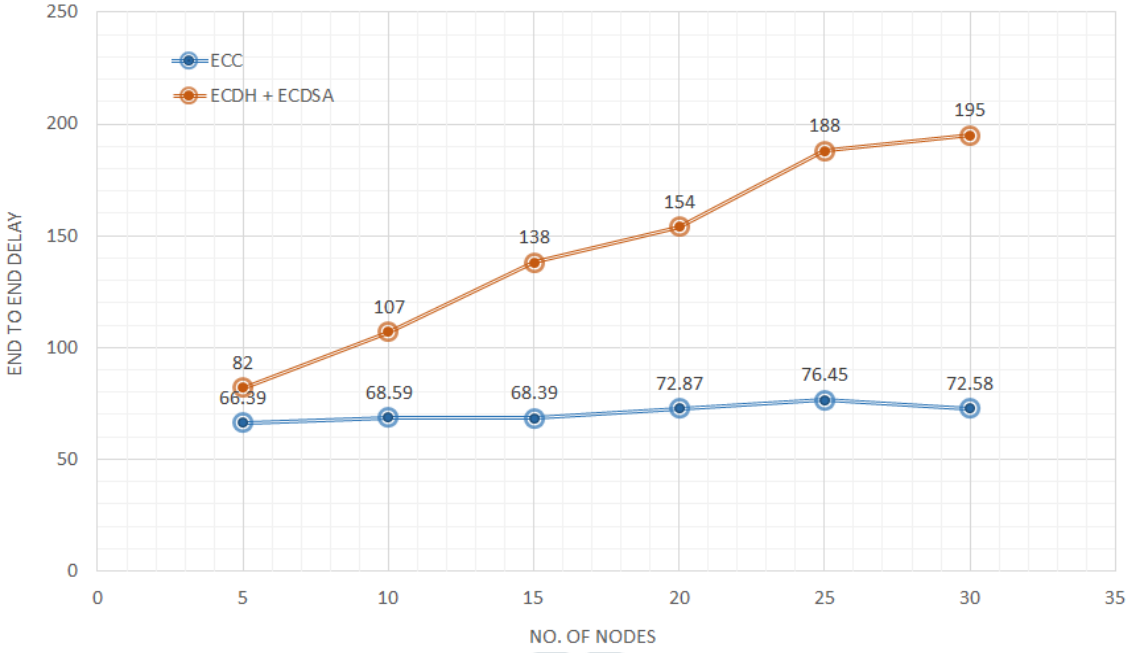

Fig- 2 End to End delay

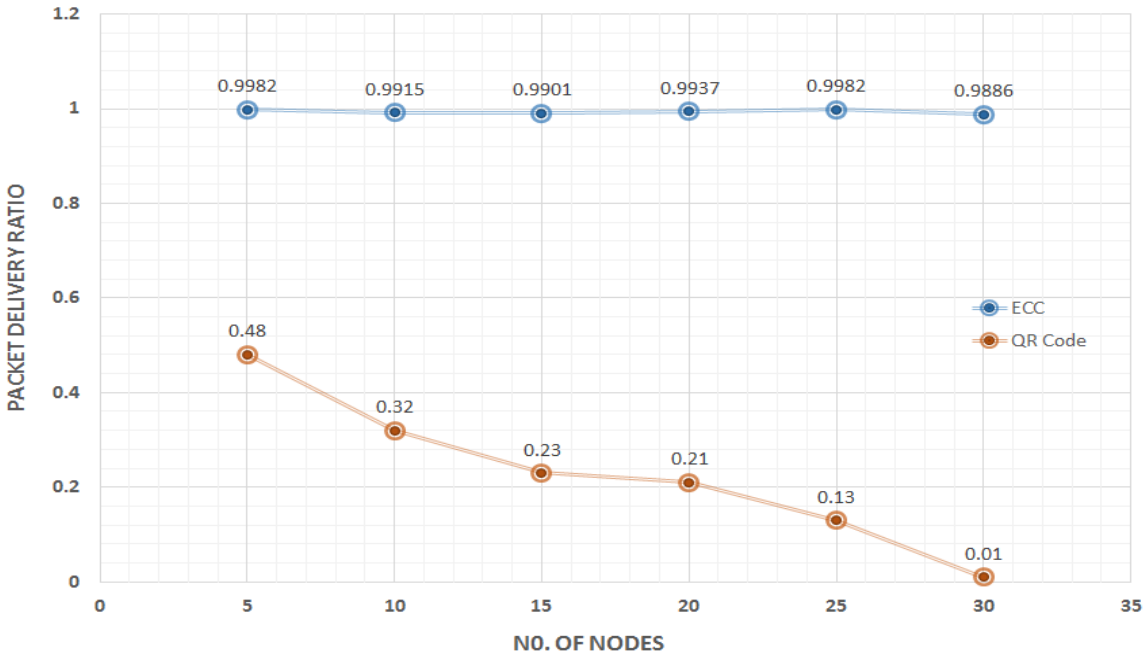

Fig- 2 Packet Delivery Ratio

V. CONCLUSION

In ebb and flow time of innovation Vehicular Ad hoc Networks(VANETs) have been researched with regard to enhance driver'ssafety and comfort. So according to literature analysis we find out certain restriction in existing system related to node authentication and message security so utilizing proposed architecture design robust system for communication between V2V,V2I,V2R using ns-2.35 and furthermore analyzed performance of proposed system.

VI. REFERENCES

[1] Amina Bendouma, Boucif Amar Bensaber." RSU authentication by aggregation in VANET using an interaction zone"978-1-4673-8999-0/17/$31.00 ©2017 IEEE.

[2] Anirudh Paranjothi, Mohammad.S.Khan,Mais Nijim,Rajab Challoo." MAvanet- Message Authentication in VANET using Social Networks" 978-1-5090-1496-5/16/$31.00 © 2016 IEEE. pp. 1-8.

[3] Atanu Mondal , Sulata Mitra." TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET" pp. 1-6,IEEE-2016.

[4] Hyo Jin Jo, In Seok Kim, and Dong Hoon Lee." Reliable Cooperative Authentication for Vehicular Networks1524-9050 © 2017 IEEE. pp. 1-15.

[5] Yiliang Liu, Liangmin Wang, Member, IEEE, and Hsiao-Hwa Chen." Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Network" vol. 64, IEEE Transactions on Vehicular Technology, pp. 3697-3710,IEEE-2015.

[6] Shibin Wang [a,b] , Nianmin Yao [a,*] ," LIAP: A local identity-based anonymous message authentication protocol in VANETs" vol.112, pp. 154-164,ELSEVIER-2017.

[7] Han Yiliang[1,2], Lin Xi[2], Jiang Di[2], Fang Dingyi[1]." Attribute-based Authenticated Protocol for Secure Communication of VANET" 978-1-5090-4657-7/17/$31.00_c 2017 IEEE. pp. 4078-4081.

[8] Ubaidullah Rajput[1], (Student Member, IEEE), Fizza Abbas[2], (Member, IEEE), Hasoo Eun[1] (Student Member, IEEE), and Heekuck Oh[1], (Member, IEEE)." A Hybrid Approach for Efficient Privacy Preserving Authentication in VANET" DOI 10.1109/ACCESS.2017.2717999, IEEE Access,vol. 5, pp.12014-12030, 2016.

[9] Er. Gaganpreet Kaur, Dr. Sandeep Singh Kang."Technique to control Data Dissemination and to support data accessibility in Meagerly Connected Vehicles in Vehicular Ad-Hoc Networks (VANETS)" 978-93-85670-72-5 © 2016 RTCSIT. pp. 58-64.

[10] Jay Rupareliya[a]*, Sunil Vithlani[b] , Chirag Gohel[c] "Securing VANET by preventing attacker node using Watchdog and Bayesian Network Theory" vol.79, 7th International Conference on Communication,Computing and Virtualization, pp. 649-656, ELSEVIER-2016.

[11] Greeshma S Chirayil[a] , Ashly Thomas[*] "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement" vol. 25, pp. 356-363, ELSEVIER-2016.

[12] Prof. Gayatri A. Jagnade, Prof. Saleha I. Saudagar, Prof. Sonika A. Chorey "Secure VANET from vampire attack using LEACH protocol", Intenational conference on Signal Processing, Communication, Power and Embedded System, pp. 2001-2005, IEEE-2016.

[13] Sujata V. Mallapur, Siddarama . R. Patil,"Survey on Simulation Tools for Mobile Ad-HocNetworks", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501vol.2, No.2, April 2012.

[14] B.Ayyappan[1], Dr.P.Mohan kumar[2]." Vehicular Ad Hoc Networks (VANET): Architectures, Methodologies And DesignIssues" 978-1-5090-1706-5/16/$31.00 ©2016 IEEE. pp. 177-180.

[15] https://www.google.co.in/url?sa=t&source=web&rct=j&url=http://shodhganga.inflibnet.ac.in/bitstream/10603/68269/7/07_chapter%25201.pdf&ved=0ahUKEwjUmNO18_XAhWKOY8KHQLzC3sQFghDMAI&usg=AOvVaw0wuV-rfUX-VAkeJdS3tZ69accessed on 14th November 2017.