Enhancing Security between V2v, V2i, V2r Using Cryptosystem for Vanet

Dhara M. Patel[1], Kalpesh L. Patel[2]
[1]Student (Master of engineering), [2]Assistant Professor
Computer Engineering Department,
L.C. Institute of Technology, Mehsana, Gujarat, India

Abstract: *Recent advances in wireless communication technologies and auto-mobile industry have triggered a significant research interest in the field of VANETs over the past few years. VANET consists of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications supported by wireless access technologies such as IEEE 802.11p.VANET developed an advanced traffic signaling system for message transmission.so when data transmission from source to destination node various attack and introduces in system and reduce PDR, Information Loss. In these paper we will work on The suggested cryptosystem like MD5 and ECC using proposed scheme increase efficiency, latency, Packet Delivery ratio, Authentication, Scalability and security between communication node.*

Keywords: *VANET, MD5, ECC, Authentication, Scalability, V2V, V2I, V2R, IEEE 802.11p.*

I. INTRODUCTION

Federal Communication Commission (FCC) allocated a frequency spectrum for wireless communication vehicle-vehicle as well as vehicle-roadside. In 2003, Dedicated Short Range Communications (DSRC) Service is established by FCC [16]. DSRC is a communication service that uses the 5.850-5.925 GHz frequency band for the use of public safety as well as private application. Newly developed services and the allocated frequency enable vehicles and roadside units to form Vehicular Ad Hoc Networks (VANETs), in which the nodes can communicate wirelessly with each other without central access point VANETs share some same characteristics with Mobile Ad Hoc Network (MANET). Both VANET and MANET are characterized by the self-organization of the nodes and movement, but they are different in some ways. The unreliable channel conditions and high nodes mobility VANETs to have many challenging research issues, such as data sharing, data dissemination, and security issues[12].

The promises of wireless communications to support vehicular applications supported by wireless communications have led to us several research projects around world. FCC allocated DSRC to “increase traveller safety, reduce fuel consumption and pollution, and continue to advance the nation's economy”. National Highway Traffic Safety Administration (NHTSA) created the Vehicle Safety Communication Consortium (VSCC) to promote V2V networking for safety. There are several projects focusing to develop intelligent vehicles based on DSRC. The Car 2 Car Communications Consortium developed the C2C-CC project in Europe. The Internet ITS (Intelligent Transportation Systems) Consortium in Japan is one of the samples of VANETs projects[11].

II. SECURITY REQUIREMENTS FOR VANET[7]

Authentication: Authentication is the process of determining whether someone or something is, who or what it is declare to be.

Integrity: Integrity means information needs to be change constantly and this can be done by authorized object and through authorized mechanism.

Confidentiality: Confidentiality is the concealment of data or resource. It is the protection of transmitted data from passive attacks.

Non-Repudiation: Non-Repudiation can prevents either sender or receiver from denying a transmitted message. **Pseudonymity**: Pseudonymity is the condition of depicting a hidden personality. A holder that is at least one people are distinguished yet don't unveil their actual names.

Privacy: The assurance of individual information of drivers inside the system from different hubs however removed by experts if there should be an occurrence of mishaps is a noteworthy protection issue which is alluring for VANETs.

Scalability: A capacity of a system to deal with developing measure of work in a proficient way safely is Scalability, which is the principle challenge in VANETs.

Consistency: In authentication, consistency of the information must be required for the most recent information. It ought to happen that the sender is validated yet the information to be sent is false.

Availability of Data: Data from servers should available each and every time of client request. It is necessary to have alternatives of even strong communication channels in case of Denial of Service (Dos) attacks.

Mobility: The hubs imparting in VANETs continually change their areas with various headings and velocities making the system dynamic in nature. In this way, with a specific end goal to make correspondence fruitful, it is trying to set up security conventions.
Key-Management: The key is utilized to encode and unscramble data amid correspondence process. When outlining security conventions for systems like VANET, the issue of key administration must be settled.
Location Verification: This is important to forestall numerous assaults and is useful in information approval process. Along these lines to enhance the Security of VANETs, a strong strategy is required.

III. RELATED WORK

In [6] this paper the authors have proposed an algorithm in which social networks are used to create an active topology from all possible users in sender's profile, who are active at a particular point of time. Message authentication is provided to user with QR (Quick Response) code. The system has an issue of time complexity and the authors concentrated on extracting topology using primary connection.

In [11] this paper a light weight security solution for secure data dissemination among vehicles in VANET known as timestamp defined MAC(TDMAC) . The performance results of TDMAC are qualitatively and quantitatively efficient than existing MACs.

In [3] this paper authors have proposed a security schema and all the security tools like authentication, integrity, anonymity, Non-repudiation are satisfied by using the AES and ECDSA algorithm. The performance results of this algorithm are satisfied most of the security requirements but by using this the time is more required and all the process can be depends on group leader. Here GL is selected by the trusted authority.

In [10] this paper proxy based authentication scheme (PBAS) to reduce the computational overhead of road side units (RSUs) using distributed computing. Proxy vehicles are used to authenticate multiple messages with a verification function at the same time. RSU is able to verify the outputs from the verification functions of the proxy vehicles.

In [1] this paper authors have proposed a security schema to firstly ensure identification for RSU by an Elliptic Curve Diffie-Hellman (ECDH) algorithm where the vehicle confirms that the two neighbours RSU have the same shared secret, then secondly the vehicle authenticates the message beforehand signing, using Elliptic Curve Digital Signature Algorithm (ECDSA).

IV. PROPOSED WORK

We would like create a sumo scenario. Data are collected from vehicles. Location of vehicle and speed of vehicle are collected by use of sumo simulator.
Then data are encapsulated in data packets that are broadcast over the wireless medium. Data dissemination process done using "Event Driven System"with platoon. Safety messages might be produced because of a risky circumstance or when anomalous condition is recognized, for example, street mischance. This message more often than not has solid unwavering quality and should be conveyed to each neighbour with no postponements. Nodes are divided into same size and small chunks known as platoon.
Data packets being transferred are encrypted using MD5 and ECC algorithms and sent to the respective receiving nodes. Using private key the destination node will decrypt the encrypted data packet. The message transmission is based on congestion.

V. PROPOSED FLOWCHART

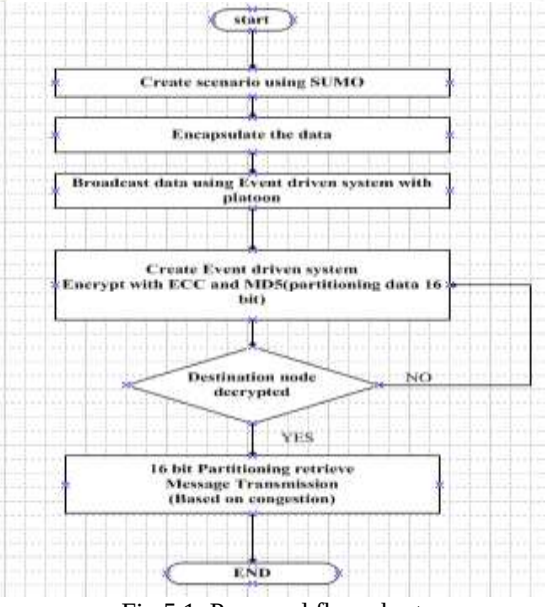

Fig 5.1: Proposed flow chart

Step 1: Create traffic scenario using SUMO tool.
Step 2: Put this scenario into NS2.
Step 3: Encapsulate the data
Step 4: Broadcast the data in wireless medium using event driven system and a message is divided into chunks.
Step 5: Encrypt data with ECC and MD5 (Partitioning of data in 16 bit)
Step 6: Destination node decrypted
If get
Go to Step 7
Else
Go to Step 5
Step 7: Receiver receive message
Step 8: Calculate PDR, energy, delay, throughput
Step 9: OUTPUT
Step 10: END

VI. EXPERIMENTAL EVALUATION

Experimental of proposed system is done in sumo simulation and ns2 network simulator. After performing the proposed algorithm on ns2 we find the result shown as below fig. 6.1, fig 6.2, fig 6.3 with respect PDR, Delay time and throughput. We find the stable result compare to existing result. Authentication and Scalability can achieve in proposed system.

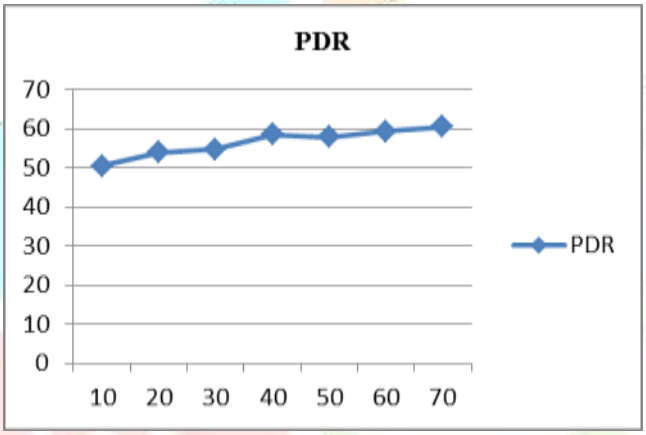

Fig 6.1 Packet Delivery Ratio

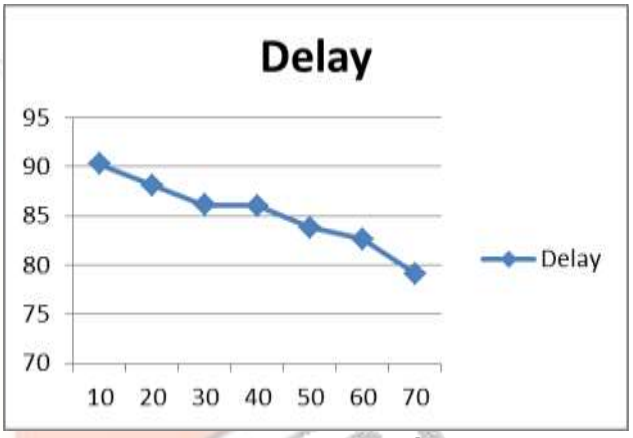

Fig 6.2 Delay time

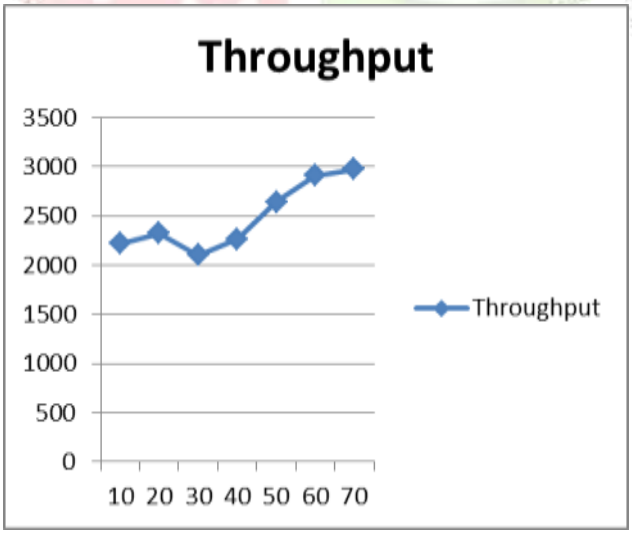

Fig 6.3 Throughput

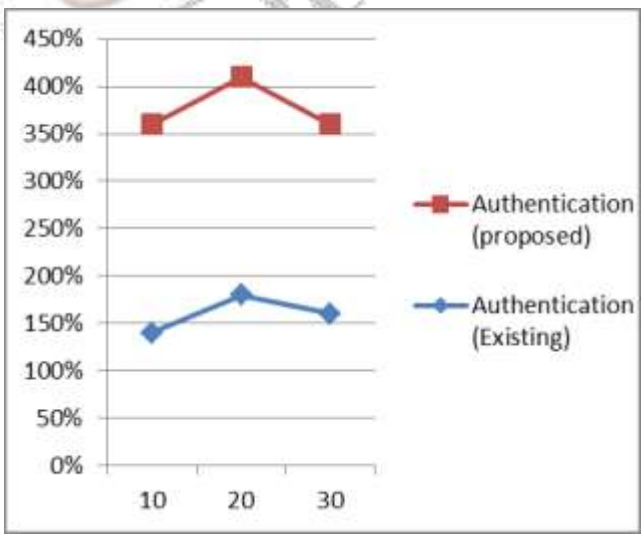

Fig. 6.4 Authentication

VII. CONCLUSION

VANET is one of the most upcoming technology in nearest generation. Using proposed algorithm we work an efficient data transmission between V2V, V2I, V2R with high accuracy and high PDR, throughput and delay with scalability and authentication. So we achieve high performance rate using proposed system for nodes 10 to 70 and enhance the security in VANETs.

REFERENCES

[1] A.Bendouma and B.A. Bensaber, " RSU authentication by aggregation in VANET using an interaction zone" *2017 IEEE International Conference on Communications (ICC)*, Paris, 2017,pp.1-6.doi: 10.1109/ICC.2017.7997017

[2] Prof. G.A.Jagnade and Prof. S.I.Saudagar Prof. S.A.Chorey, " Secure VANET from vampire attack using LEACH protocol " 2016 IEEE International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[3] R. Waghmode, R. Gonsalves and D. Ambawade, "Security enhancement in group based authentication for VANET," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2016, pp. 1436-1441. doi: 10.1109/RTEICT.2016.7808069

[4] P.A.Sumayya and P.S.Shefeena, " VANET Based Vehicle Tracking Module for Safe and Efficient Road Transportation System " 2014 sciencedirect International Conference on Information and Communication Technologies(ICICT 2014)

[5] Nicholas S. Samaras, " Using Basic MANET Routing Algorithms for Data Dissemination in Vehicular Ad Hoc Networks (VANETs) " 2016 IEEE Telecommunications forum (TELEFOR 2016)

[6] Anirudh Paranjothi, M.S.Khan, Mais Nijim, Rajab Challoo "Mavanet: Message Authentication in VANET using Social Networks " 2016 IEEE

[7] Vijay Kumar Tripathi and Dr. S.Venkaeswari "Secure Communication with Privacy Preservation in VANET-Using Multilingual Translation " 2015 IEEE Global Conference on Communication Technologies(GCCT 2015)

[8] Mrs. S.A.Abbad and Mr. S.P. Godse " Priority based emergency message forwarding scheme for time critical maodels in VANET " 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)

[9] Tanjida Kabir , Novia Nurain and Md. Humayun Kabir " Pro-AODV(Proactive AODV): Simple Modifications to AODV for Proactively Minimizing Congestion in VANETs" 2015 IEEE

[10] Yiliang Liu,Liangmin Wang "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks" 2014 IEEE

[11] Atanu Mondal and Sulata Mitra " TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET " 2016 IEEE Advanced Networks and Telecommunications System (ANTS 2016)

[12] Yue Liu, J. Bi and Ju Yang, "Research on Vehicular Ad Hoc Networks," 2009 Chinese Control and Decision Conference, Guilin, 2009, pp. 4430-4435. doi: 10.1109/CCDC.2009.5192343

[13] Anand bihade, roshani talmale," Detection and Avoidance of road traffic congestion using VANET", Proceedings of IRAJ International Conference, 21st July 2013, Pune, India, ISBN.

[14] W. Liu, X. Wang, W. Zhang, L. Yang and C. Peng, "Coordinative simulation with SUMO and NS3 for Vehicular Ad Hoc Networks," 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, 2016, pp. 337-341. doi: 10.1109/APCC.2016.7581471

[15] Martins, David, And Herve Guyennet. "Wireless Sensor Network Attacks And SecurityMechanisms: A Short Survey", 2010 13th International Conference On Network-Based Information Systems, 2010.

[16] Hoang Lan Nguyen, Uyen Trang Nguyen," A Study Of Different Types Of Attacks In Mobile Ad Hoc Networks", Department Of Computer Science And Engineering, 2012, IEEE.

[17] http://learning.maxtech4u.com/vehicular-ad-hoc-network-vanet/

[18] http://ijarcsse.com/Before_August_2017/docs/papers/Volume_7/7_July2017/V7I7-0159.pdf

[19] https://www.researchgate.net/figure/280958696_fig1_Figure-1-VANET-Architecture

[20] https://www.cse.wustl.edu/~jain/cse571-14/ftp/vanet_security/index.html

[21] https://www.urbanafrica.net/news/huge-express-highway-planned-connect-nigerian-cities/

[22] http://shodhganga.inflibnet.ac.in/bitstream/10603/68269/7/07_chapter%201.pdf

[23] http://www.ijcte.org/papers/590-K172.pdf