iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Attack Resistant of Malicious Nodes for Securing Vehicular Adhoc Networks by an Encryption Alert

Anand N Paatil[1] , Dr Rekha Patil[2]
[1,2,]Computer Science and Engineering Department, PDA College of Engineering, Kalaburagi,INDIA

Abstract: ***Vehicular Ad hoc Network (VANET) is an autonomous wireless network comprising of moving vehicles. A small communication unit is installed in the devices that are capable of transmitting its GPS (Global Positioning System) position and gather important information from other vehicles and road side junctions. As vanet is an open architecture which means the underneath technology being used is essentially either wifi or Bluetooth such networks often referred as public network .one of the most challenging issues of any public network is to ensure privacy and trustworthiness of the data. In vehicular ad hoc network as the vehicle moves with rapid speed the link itself varies with significantly different vehicle will have a enter communicable link which will be keep on changing with the mobility movement of the vehicle .In such a highly dynamic network to determine which packets are malicious or which nodes are malicious is extremely difficult, Therefore the proposed work analysis a novel hybrid technique for trust management and privacy preservation in vanet Our trust management system will enable the nodes to determine the validity of a specific packet, this is known as packet trust or data trust ,validity of the sender also known as node trust ,validity of the type of message is being conveyed also known as functional trust. our entire work demonstrate how to detect and prevent malicious nodes and attacks by analyzing various trust models through the GPS data exchange between the nodes among themselves and the node in the road side unit. The work is simulated using vanetsim which is a java based real time vanet simulator. A result shows that the accuracy of the detection of the attacker and an attack model is extremely efficient in our case.***

Keywords— Vehicular ad hoc network, Road side unit, Trust Management, GPS, Vanet Simulator.

I. INTRODUCTION

A vanet is a mobile network of open radio present in the vehicle where vehicle exchange several information like location data, their sensors data like engine temperature vibration, road condition understand with the other vehicle and the data is aggregated in specific base stations generally known as road side unit. One of the main challenges in the vehicular ad hoc network (VANET) research domain is the realistic simulation of inter vehicle communication (IVC).In general vanet consists of three major components, namely the

Trusted Authority (TA),Road Side Units(RSUs)and Vehicles [1]. Location based service are one kind of promosing and value added applications in vanet, where a service provide can make use of location information to provide various services to vehicle users in a certain area, such as finding the nearest parking lot or establish a location based social network to help vehicle users who have common favorite to share some interesting information in a temporally community on road [2].In vanet a vehicle that is equipped with an on board unit(OBU)communicates with other vehicle via a vehicle to vehicle (V2V) domain and communicates with a road side unit(RSU)via a vehicle to infrastructure(V2I) domain.

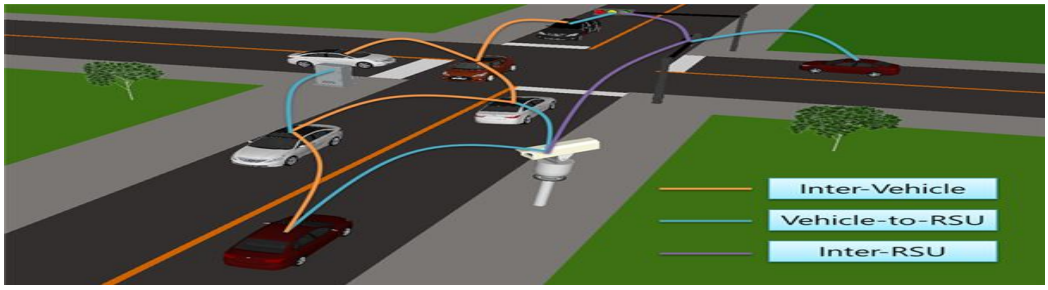


Fig. 1 Example of VANET Network

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V2V and V2I communication domains are mainly for safety vanet application such as road accidents notification and weather warnings [3].Vanet have been envisioned to enhance the passenger safety and comfort in the near future, vehicles will employ an onboard unit to embrace various network services, due to the unique feature of high speed mobility the continuity of communication in vanet is a challenging task [4].Non security applications permit passenger to access many services like interactive communication ,internet access, payment services, online games and information updates whilst vehicles are on move [5].When compare with the traditional networks vanet themselves are more vulnerable to malicious attacks because of their unique features, such as highly dynamic network topology, limited power supply and error-prone transmission media. For instance the wireless communication links among vehicles are prone to both passive eavesdropping and active tampering [6].Traffic congestion have become a major problem faced by big cities. Despite of the great efforts made by government to improve the urban transportation system people still waste a lot of time on the road. Additionally a large number of exhaust emissions from the vehicles in traffic jams cause serious air pollution. The emerging technology of vanet provides a new approach to traffic management [7].

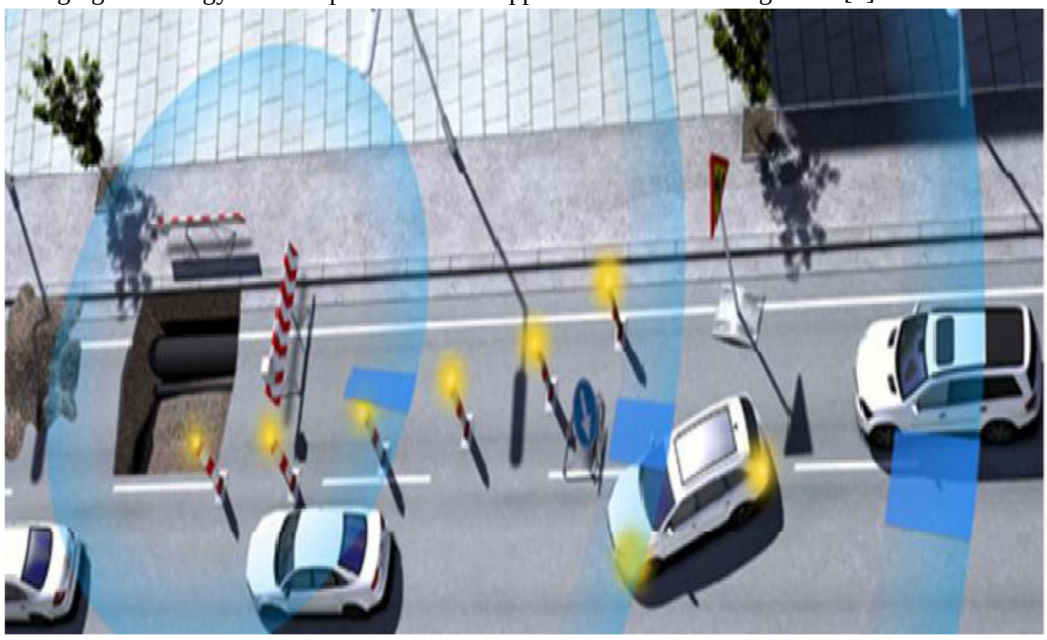


Fig. 2 Example of a VANET application: Warning of Obstacles in the Road

The above figure shows that a men at work signal which may broadcast information about the existence of the road works so that drivers would know their existence in advance. VANET simulation environments only takes into account of network characteristics like node position, mobility and Network traffic conditions.

In vanet vehicle can broadcast a message to neighboring vehicle regarding the vehicle speed,position,and road situations [8]. The basic application of vanet is to allow arbitrary vehicles to broadcast safety messages to other nearby vehicles and RSUs such that the other vehicles may adjust their traveling routes, and RSU may inform that traffic control centre to adjust traffic lights for avoiding possible traffic congestion [9].

Organization of Paper: I. Introduction, II. Related Work, III .Proposed Work, VI. Implementation and Results, V. Conclusion and Future Work.

II. RELATED WORK

Vehicular ad hoc networks are an important communication paradigm in modern day mobile computing for exchanging live messages regarding traffic congestion, weather conditions, road conditions to improve driving comfort [1].To achieve a vehicle user's privacy they first introduce a privacy preservation authentication technique that not only provides the vehicles user's anonymous authentication but enables double registration detection as well [2].The integration supports communication between road side units(RSUs)and vehicles and provides internet access through public hotspots located inside public transportation system [3].The identity privacy and location privacy cannot be raveled in public [4].An ART scheme is suggested for vanets that is able to cope and detect using malicious attacks and evaluate trustworthiness of both cell nodes and data in vanet [5].The trustworthiness of vanet could be improved by addressing holistically both data trust, which is defined as the assessment of weather are not and to what

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

extent the reported traffic data are trustworthy and node trust which is defined as how trustworthy the nodes in vanet are [6].In urban areas, traffic congestion has become a serious phenomenon resulting in a great waste of time and fuel, how to detect road condition and disseminate traffic information effectively has become a significant challenge [7].The implementation of vanet technology does not only help drivers to avoid fatal road accidents but it can also provide the experience smooth driving and many different types of entertainment [8].Vehicular ad hoc networks is initially designed for enhancing driving safety and convince through intervehicle communication (IVCs) or communication with units in the road side infrastructure [9]. Vanet enables various traffic safety applications such as collision avoidance and lane change assistant [10].

III.PROPOSED WORK

We design a unique system that not only detects attacks but also can asserts the nodes to prevent the occurrence of the attack using a trust management system. Using a Trust management system each of the node present in a routing table , each of the packet coming from the node, each of the event specified by the packet are marked with probability with malicious and non-malicious . High probability is then mitigated by RSU per sec as well as the nodes. This leads to the distributed coordinate processing of the event .

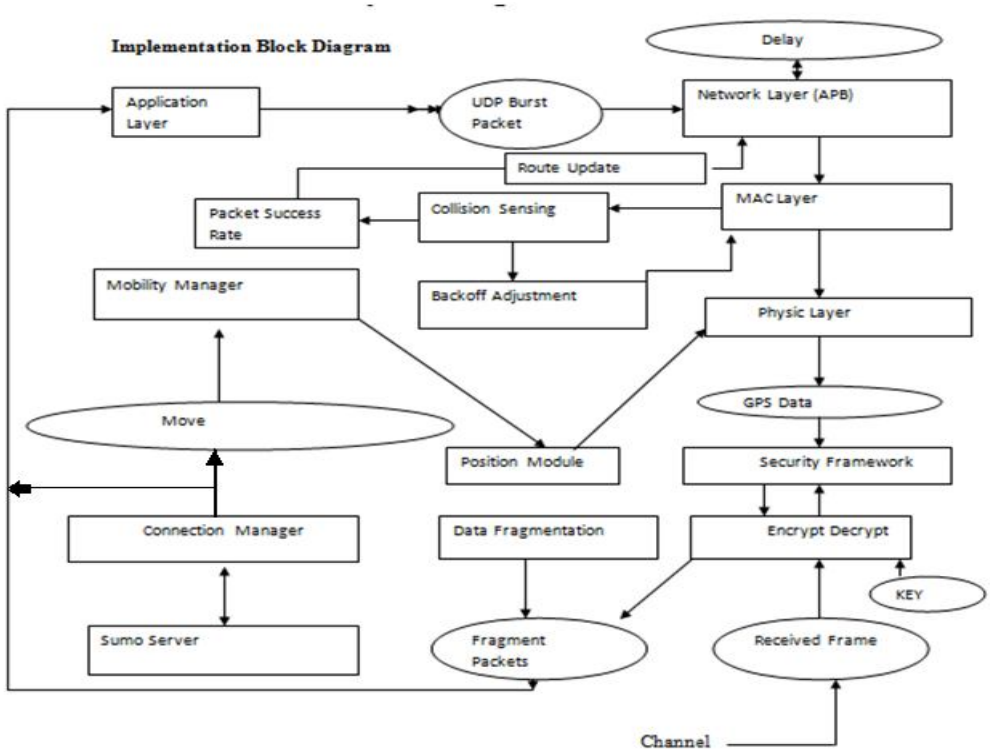


Fig. 3 Block Diagram

First run SUMO server which is responsible for communicating with simulation and for passing it with vehicle position by which it gets connected and it manages the connections sent through the SUMO server. By sending SUMO data then data will be sent to the mobility manager in which it checks for the congestion and position of the vehicle. Application layer determines the network packet performance and data exchanges, type of application such as pothole notification, collision notification and navigational services. By bursting where a node notifies about its position through packet broadcasting that reaches to RSU unit and also reaches to nearest node and moves to the network layer which is associated with the delay factor where delay is associated with congestion of traffic, congestion of network, loss of bandwidth etc. And it updates route which is associated with the link it may be a multicast communication or one to one communication.MAC layer will always have the bakeoff timer bt means it will schedule the next packet how much time it should wait before the next burst packet is going to transmit such adjustment is taken by MAC layer. The physical layer is associated with the navigational data i.e. GPS data. PS data is achieved by the position module which is part of the vehicle i.e. GPS position. Physical layer will give information to the MAC layer which is also give to the network layer for UDP burst packet. It will be having mobility management where it also measures speed, acceleration and change of position module. As GPS is coming the security framework should be integrated because most of the attacks are associated with GPS.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. IIMPLEMENTATION AND RESULTS

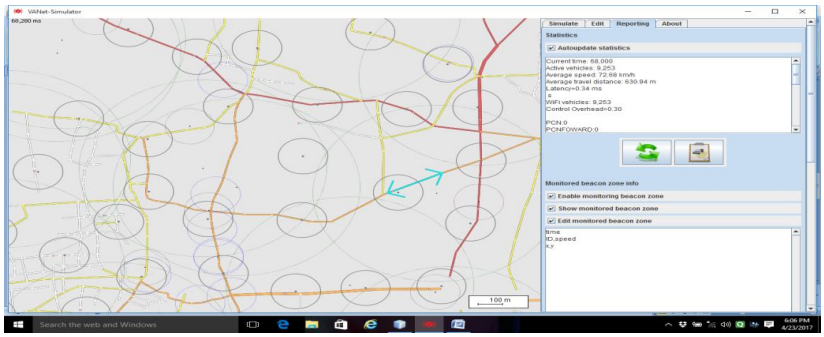


Fig. 4 Mix Security Zone without Encryption

The above figure demonstrates the features of both high security and low security mix zone without encryption and the data will not be secured. So the attacker can easily hack the data.

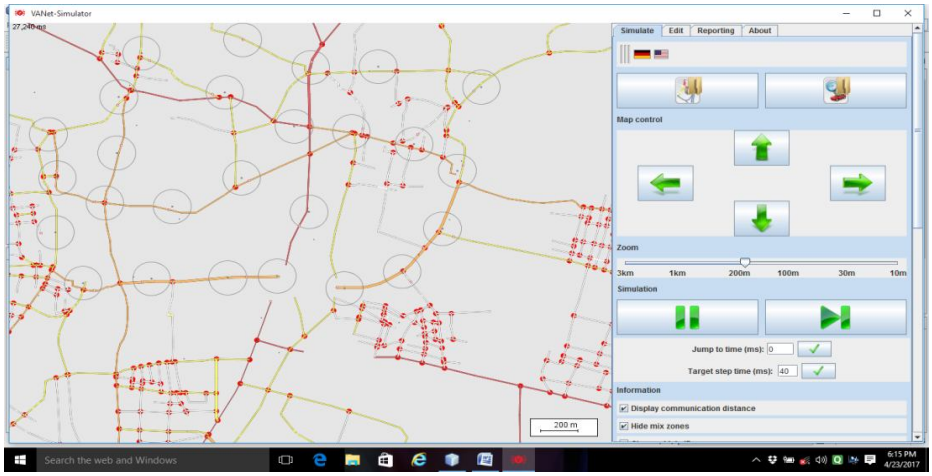


Fig. 5 Mix Security Zone with Encryption

In the figure dotted line represents the features of both high security and low security mix zone with encryption and the data will be secured. So the attacker cannot easily hack the data.

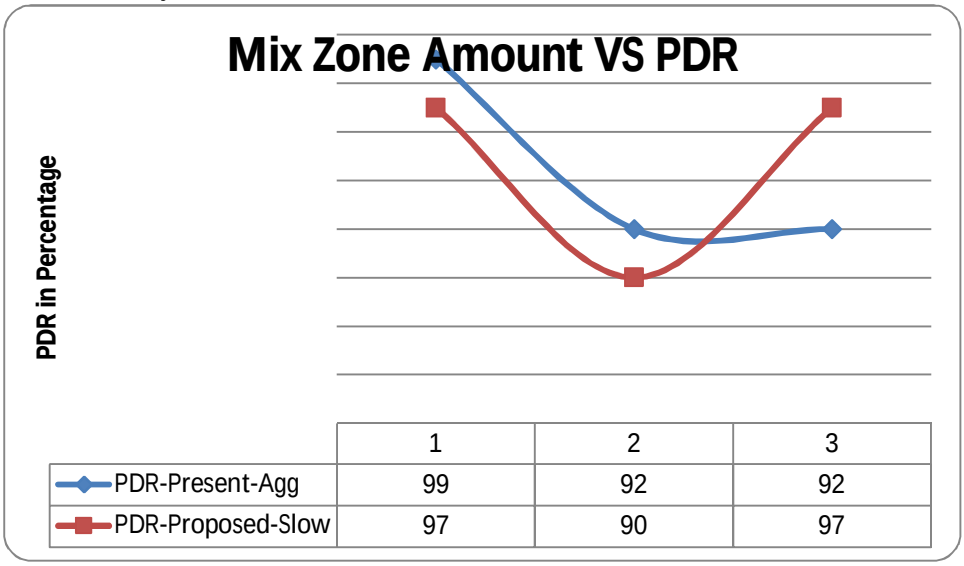
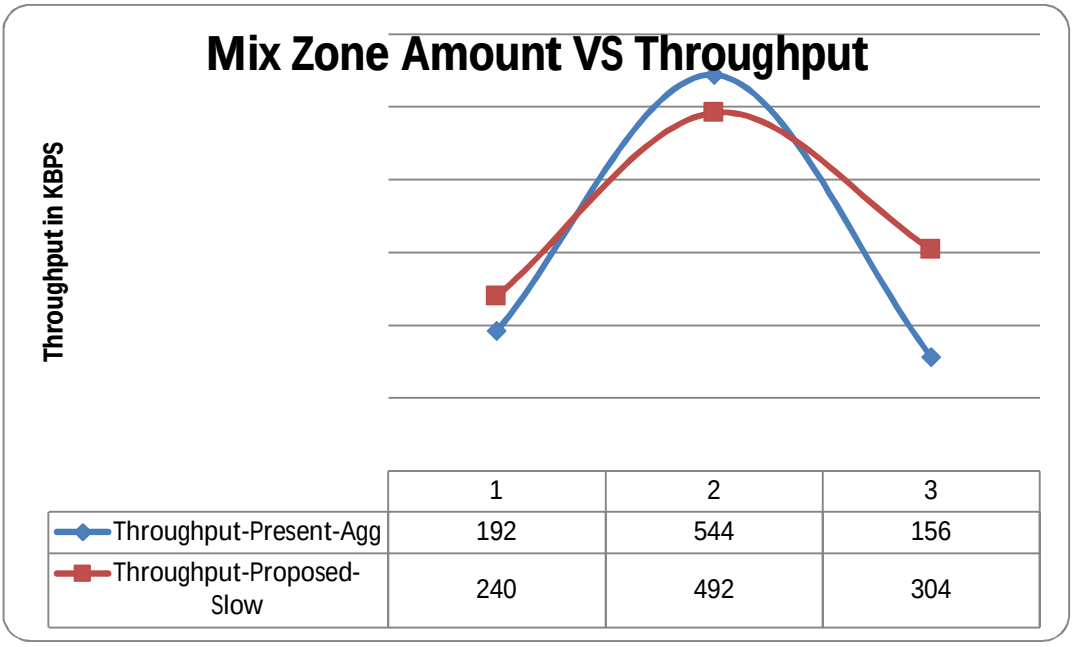


Fig. 6 Mix Zone Amount Vs PDR

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

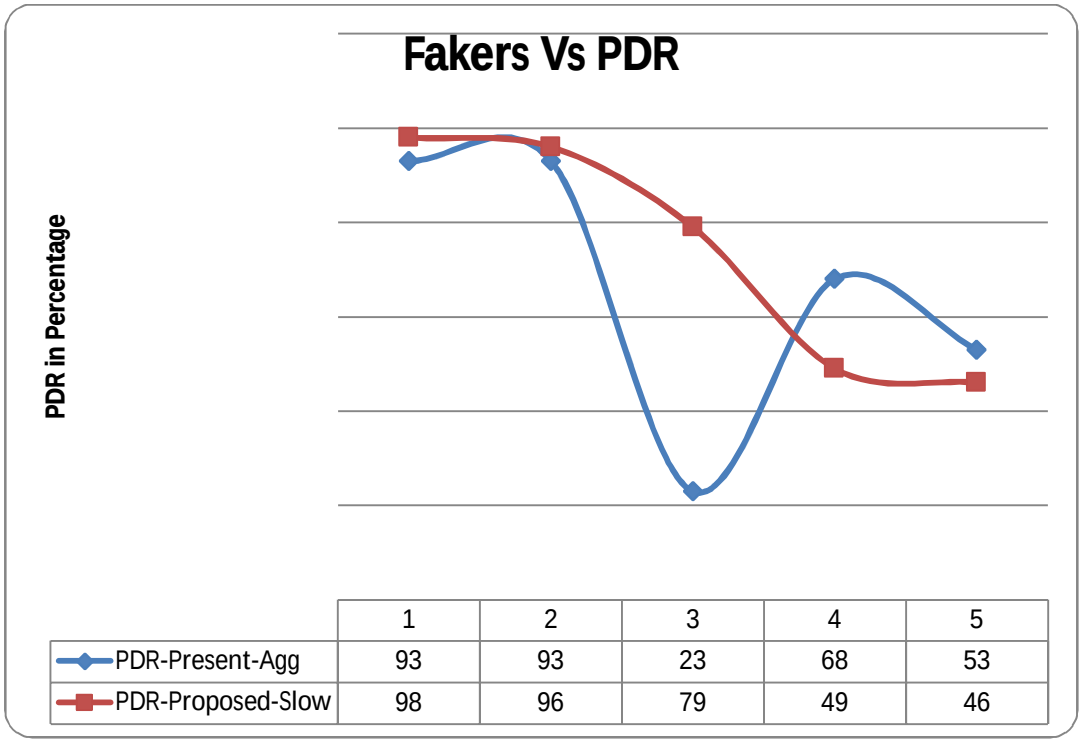
Fig 6 reveals that there is an increase in the percentage of PDR in the proposed system than the present system for an increase in mixzone amount from 2 and above.



	1	2	3
Throughput-Present-Agg	192	544	156
Throughput-Proposed-Slow	240	492	304

Fig. 7 Mix Zone Amount Vs Throughput

Fig 7 reveals that there is an increase in the throughput value for a mixzone amount of below and above 2,than that of present system



	1	2	3	4	5
PDR-Present-Agg	93	93	23	68	53
PDR-Proposed-Slow	98	96	79	49	46

Fig. 8 Fakers Vs PDR

Fig 8 reveals that there is an increase in the percentage of PDR in the proposed system than the present system with an increase in fakers upto 3.5.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

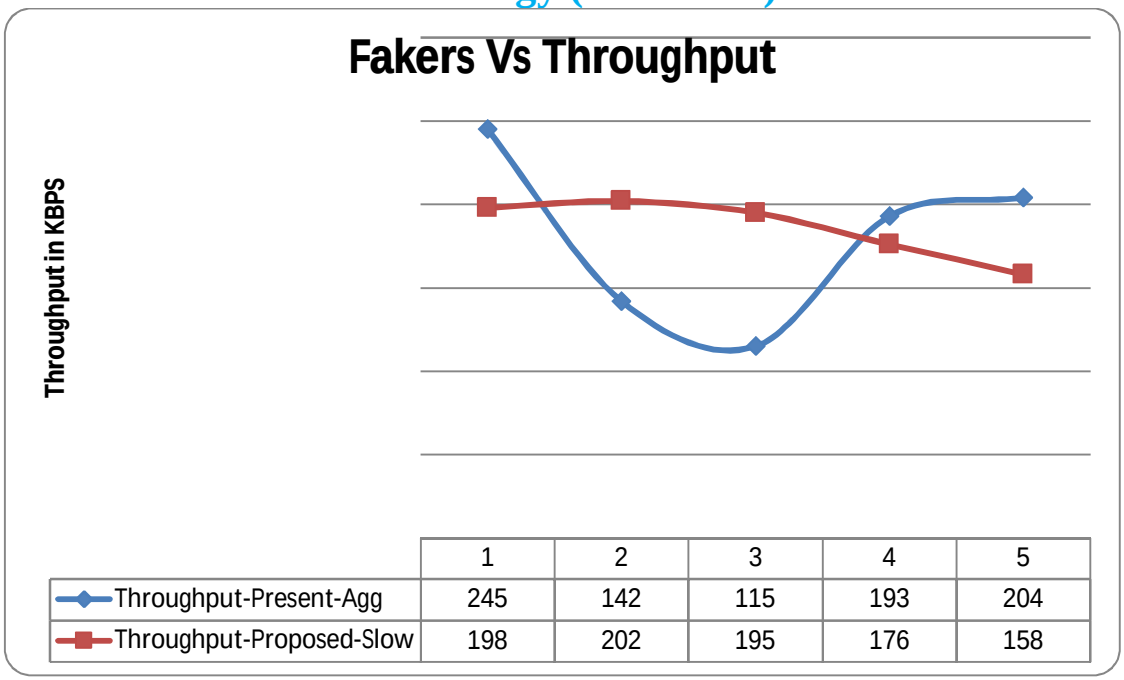


Fig. 9 Fakers Vs Throughput

Fig 9 reveals that, an overall increase in the throughput of the proposed system than the present system for the fakers up to 4.

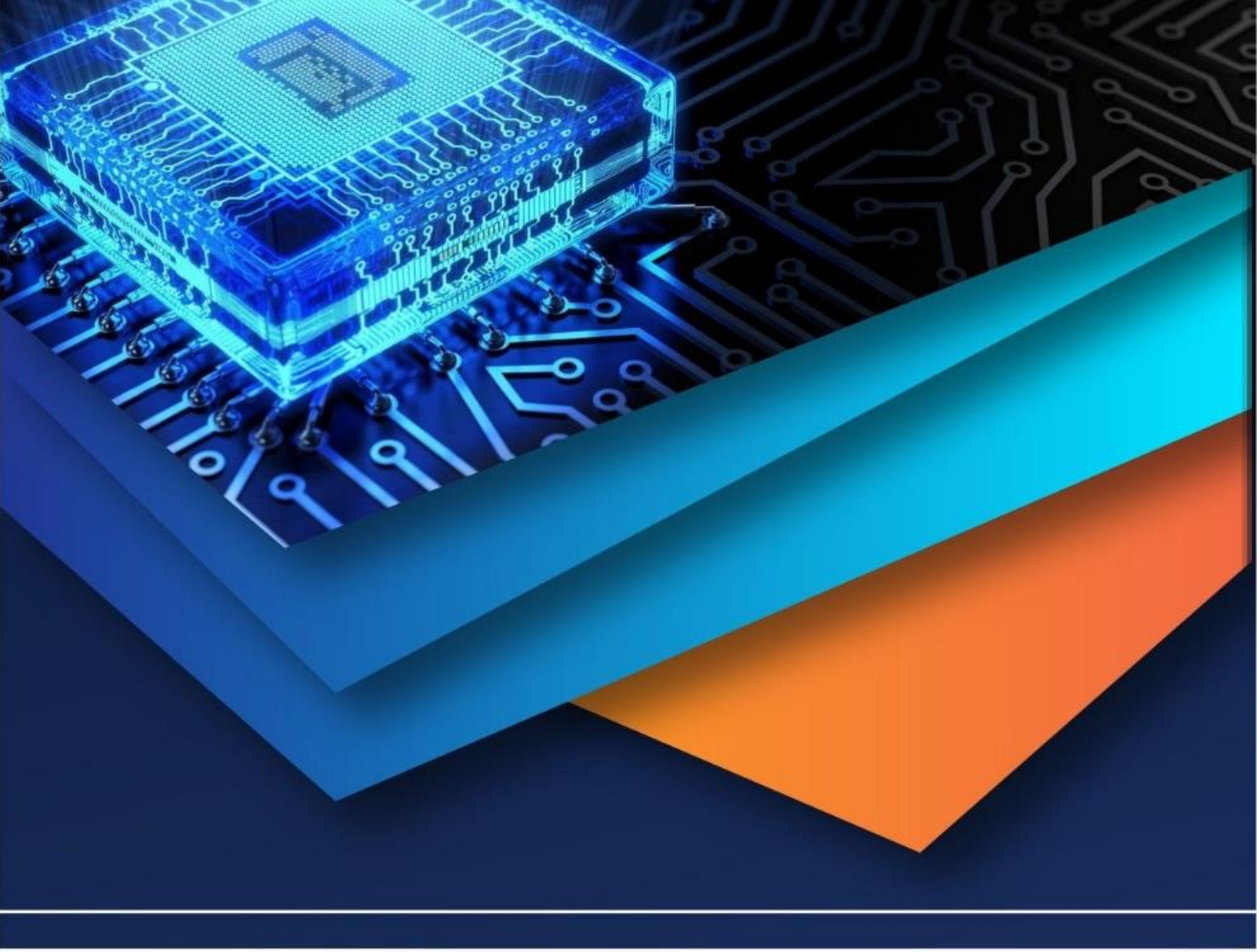
V. CONCLUSION AND FUTURE WORK

An attack resistant of malicious node is proposed to evaluate the trustworthiness of both traffic data and vehicle nodes. Several data security models have been offered in the past through encryption and efficient exchange in the fast moving traffic scenario such encryption and decryption leads to extreme amount of packet congestion due to frequent key exchange and frequent link changes. In order to overcome the computational and temporal complicity associated in ensuring privacy and security we offer a fuzzy based model for detecting and avoiding the attackers in the vanet. Our system is based on creating a model based on ideal time observation of the vehicular data. Results show that the accuracy of our system is independent of type of vehicle in the case of moderate and high traffic where as it suffers from some misdetection when the traffic is significantly low. Therefore, it can be further extended that the system can be improved by incorporating historical decision making system with the current fuzzy based system through more advanced machine learning techniques like deep learning as by incorporating centralized decision making system through cloud based decision making system. The accuracy of the detection can be improved further.

REFERENCES

[1] Pandi Vijayakumar, Maria Azees, and Lazarus Jegatha Deborah" "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks" , IEEE Transactions On Intelligent Transportation Systems, VOL.17, NO.4, APRIL 2016
[2] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen," A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs" IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, march 2012
[3] Sanaa Taha, and Xuemin (Sherman) Shen, Fellow,"A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs" IEEE Transactions on Intelligent Transportation Systems" VOL. 14, NO. 4, DECEMBER 2013
[4] -Yao Yeh and Yu-Cheng Lin" A Proxy-Based Authentication and Billing Scheme With Incentive-Aware Multihop Forwarding for Vehicular Networks" IEEE Transactions On Intelligent Transportation Systems, vol. 15, no. 4, august 2014
[5] Sudha Dwivedi, Rajni Dubey, Nirupma Tiwari" Trust Based Scenario using AES Encryption in VANET" Volume 6, Issue 8, August 2016
[6] Wenjia Li,and houbing Song ART: An Attack Resistant Trust Management Scheme For Securing Vehicular Ad Hoc Networks IEEE Transactions On Intelligent Transportation Systems, vol. 17, no. 4, april 2016
[7] Yuwei Xu, Jian Wang, Tingting Liu, Wenping Yu, Jingdong Xu"Detecting Urban Road Condition and Disseminating Traffic Information by VANETs" IEEE 2015 UIC-ATC-ScalCom-CBDCom-IoP 2015
[8] Asif Ali Wagan and Low Tang Jung Security Framework For Low Latency Vanet Applications IEEE 2014
[9] T.W.Chin.S.M.Lucas C.K.Huli OPQ:OT-Based Private Querying In Vanets IEEE Transactions On Intelligent Transportation Systems, vol 12,No 4\
[10] Zhengming Li,Congyi Liu, and Chunxiao Chigan On secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control IEEE Transactions On Intelligent Transportation Systems, vol 14,no 1.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)