Collision Avoidance System for Safety Vehicular Transportation System in VANET

Dr.K.SURESH BABU[1], BOJJA JYOTSNA[2]
[1]*Associate Professor,* [2]*PG Scholor*
[12]*Department of Computer Science & Engineering, JNTUH, SIT, Hyderabad, Telangana, India*

Abstract- **Background/Objectives:** To analyse the performance in VANET and to suggest a framework for collision avoidance in VANET. **Methods/Statistical Analysis:** A Vehicular Ad hoc Network (VANET) has emerged to be one of the novel and powerful technologies providing safety for the persons driving the vehicles and also provides reliable communication between the vehicles. In this VANET technology, each vehicles act as a mobile node that communicates with each other using the Road Side Units (RSU). There are numerous protocols employed in the VANET. The different routing technique such as geographic, hybrid, topology and clustered routing helps in the reliable delivery of the packets from the origin to the target nodes by determining their geographical location. **Findings:** To facilitate efficient transfer of data we need to improve the QOS parameters such as jitter, delay, congestion, energy efficiency and latency. In order to eradicate the frequent occurrence of accident, the implementation of VANET technology is being used in various modes of transportation. Here, we had made an accumulative study of various routing protocols and collision avoidance techniques that are used in the field of navigation and biological collision avoidance.

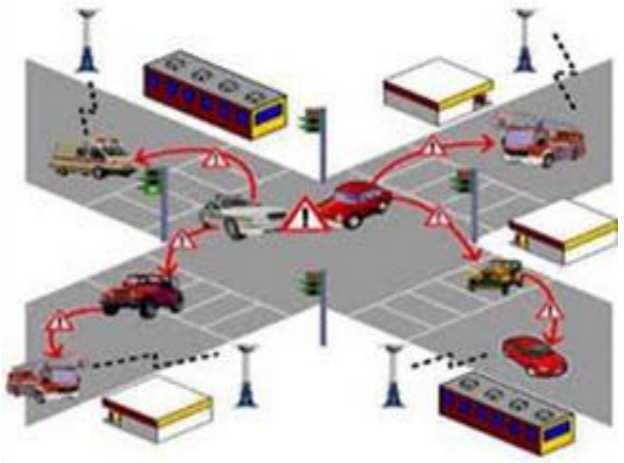
Applications/Improvements- The result observed from this work will motivate to develop a collision avoidance framework in

VANET.Keywords- collision avoidance, vehicular ad hoc networks, early message.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are specialized type of mobile ad hoc networks, in which vehicles are assumed to be mobile nodes. It consists of two different types of entities such as access points and vehicles. The access points are firm and usually connected to the internet and they could perform as a distribution point for vehicles. VANET includes the wireless communication from one vehicle to another (V2V) and from vehicle to infrastructure access point (V2I). Vehicle to vehicle communication is of two types: one hop communication which involves direct vehicle to vehicle communication and multi hop communication which includes vehicle that relies on other vehicles to retransmit. VANET also has unique characteristics that distinguish it from other mobile ad hoc networks. The most important characteristics includes maximum mobility, self-organization, geographically distributed communication, restricted road pattern, and network size without any restrictions, thus all these characteristics made vehicular ad hoc network environment as a challenge to develop routing protocols in an efficient way.

The vehicles provide a great opportunity for the development of new driver assistance systems by exchanging information among them. The systems ofthis type will be able to publish and to gather information about the other vehicles along with the road traffic and environmental conditions in real time. These data will be handled and evaluated to ease the driving by contributing useful information to the user.



The applications of VANETs are mainly categorized into two types: safety and efficiency applications. The VANETs based systems finds many difficulties in terms of system design and implementation. Such difficulties include security, routing, connectivity, quality of services and privacy.

II. MOTIVATION

The hiked mobility of people caused a higher cost for societies as impact of the increasing number of traffic problems like fatalities, congestions and injuries. Vehicular Ad-Hoc Networks determines supporting services for Intelligent Transportation Systems such as monitoring of traffic, vehicle navigation, collision avoidance, control of traffic signals, and congestion management by signalling to drivers. VANETs comprise vehicles and roadside equipment owning wireless interfaces able to communicate among them by wireless and multi-hop communication.

A Vehicular ad hoc network is an exclusive kind of ad hoc networks and it affords basic communication between computers installed vehicle. One of the major goals of VANET is the safety. Therefore, collision avoidance among vehicles is very interesting. For clarification, the term “collisions” here refers to collisions between cars or between cars and pedestrians, not for packet transmission in

MAC.VANETs are subjected to interference and propagation issues, as well as different types of attacks and disturbances which may harm intelligent transportation system services. The high mobility nodes in networks are characterized by, wireless links subject to interference, fading due to multipath propagation and high changes in the network topologies. There was an increase in complexity of security management operations, particularly, access control, node authentication and cryptographic key distribution, allowing the participation of malicious nodes in the network and posing nontrivial challenges to security design due to the absence of central entities. The wireless communication in further is subjected to eavesdropping, jamming and interferences making easy to damage information and service security.

Contributions:

Here, a survey is done based on various routing protocols that have been used in the VANET'S, the different collision avoidance techniques that have been used to avoid collision. Subsequently, for each collision avoidance technique there are some drawbacks. Our preferences were drawn to the techniques that have been published by major journals and conferences.

We did opt for the techniques and protocols that provided that provided major changes and not minor ones. We explained the following i) the general content about VANET's ii) the survey about the different collision avoidance techniques, their issues and their drawbacks if any iii) the different transmission strategies. Some of the vulnerabilities have also been stated and the reason for their occurrence is also stated. Finally a short description of the experimental techniques is stated. Thus the analysis and technical details of some algorithms have not been included and it refers to the reader of the publications to obtain the information about the design and analysis of algorithms.

Organisation:

The flow of work as stated in Section 3 states the mobility in the VANET's. Section 4 provides a literature survey where the different collision techniques are mentioned along with their pros and cons. Section 7 provides the routing techniques and the protocols that are used for routing. Section 8 deals with the detailed description about the quality of service. Section 9 and 10 provides the different threats that occur during the information transfer and the experimental techniques. Section 11 concludes the paper.

VANET Architecture:

The communication between vehicles or between a vehicle and an RSU is achieved through a wireless medium called WAVE. The main system components are the application unit (AU), OBU and RSU. Typically the RSU hosts an application that provides services and the OBU is a peer device that uses the services provided. The application may reside in the RSU or in the OBU; the device that hosts the application is called the provider and the device using the application is described as the user. Each vehicle is equipped with an OBU and a set of sensors to collect and process the information then send it on as a message to other vehicles or RSUs through the wireless medium; it also carries a single or multiple AU that use the applications provided by the provider using OBU connection capabilities. The RSU can also connect to the Internet or to another server which allows AU's from multiple vehicles to connect to the Internet.

On Board Unit (OBU):

An OBU is a wave device usually mounted on-board a vehicle used for exchanging information with RSUs or with other OBUs. It consists of a resource command processor (RCP), and resources include a read/write memory used to store and retrieve information, a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology. . The OBU connects to the RSU or to other OBUs through a wireless link based on the IEEE 802.11p radio frequency channel, and is responsible for the communications with other OBUs or with RSUs; it also provides a communication services to the AU and forwards data on behalf of other OBUs on the network. The main functions of the OBU are wireless radio access, ad hoc and geographical routing, network congestion control, reliable message transfer, data security and IP mobility

Application Unit (AU):

The AU is the device equipped within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, the AU can be connected to the OBU through a wired or wireless connection and may reside with the OBU in a single physical unit; the distinction between the AU and the OBU is logical. The AU communicates with the network solely via the OBU which takes responsibility for all mobility and networking functions.

Roadside Unit (RSU):

The RSU is a wave device usually fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11p radio technology, and can also be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network. According to C.C. Communication Consortium, the main functions and procedures associated with the RSU are extending the communication range of the ad hoc network by re-distributing the information to other OBUs and by sending the information to other RSUs in order to forward it to other OBUs

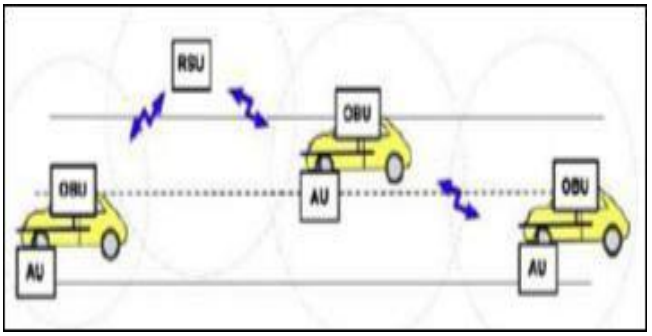


Fig.1: RSU extend the range of the ad hoc network by forward the data of OBUs (C.C. Communication Consortium,)

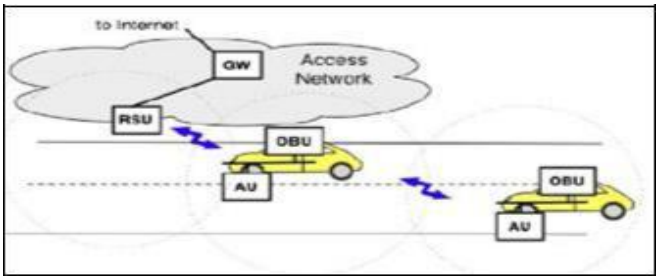


Fig. 2: RSU work as information source (C.C. Communication Consortium)

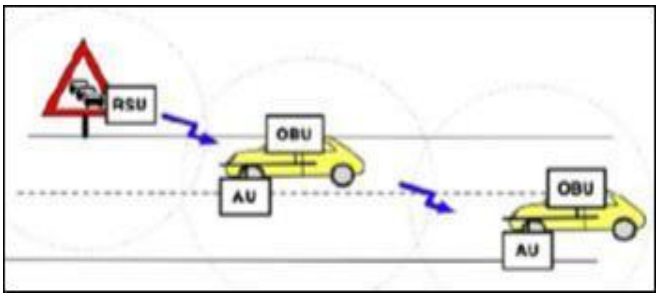


Fig. 3: RSU provides internet connectivity to the OBUs (C.C. Communication Consortium,)

INTELLIGENT TRANSPORTATION SYSTEM:

Vehicular ad-hoc network or VANET is also known as intelligent transportation system (ITS). Intelligent transportation system (ITS) has two types. In first one the vehicles communicate with each other called vehicle to vehicle communication (V2V) or inter vehicular communication and in second one vehicles communicate with the road side equipment's called as vehicle to road communication (V2R). In intelligent transportation systems, each vehicle that lies in active network act as sender, receiver, and router to broadcast information to the vehicular network or transportation agency plays an important role in the network session to secure, safe the data that travels from one node to another node and free flow of traffic.

Vehicle to vehicle communication (V2V):

Vehicle to vehicle (V2V) communication perform the operation (sender, receiver and broadcasting) between vehicles.

In vehicle to vehicle or inter vehicular communication has two types of message forwarding. First one is Naïve broadcasting and another one is intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. In this method broadcast message generated by the in front vehicle and the receiving vehicle sends its own broadcast message to other vehicles behind it. The prime disadvantage of this method is that the large number of collision occurs due to the broadcasting message by this the whole process and the delivery of message becomes slow. In intelligent broadcasting, if the vehicle detecting that they receives the same message from behind, it assumes that at least one vehicle in the back has received it and stop broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles.

Vehicle-to-Roadside Communication:

The vehicle-to-roadside communication configuration is responsible for a single hop broadcast where all equipped vehicles receive a broadcast message from the roadside equipment in the surrounding area. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside equipment for the reliable traffic flow. The distance between the two roadside units may be up to one kilometeror less, In heavy traffic the road side unit provides the high data rates to be maintained. For instance, when broad casting dynamic speed limits, according to its internal timetable and traffic rules the roadside equipment will determine the appropriate speed limits. The roadside unit send the broadcast message periodically when it detect the speed limit and will compare any geographic location or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the surrounded area. If a vehicle violates the speed limit that given in timeline database then the road side unit deliver the message in the form of auditory or visual warning to request the driver, they should reduce their speed.

III. LITERATURE REVIEW

Razzaque Mohammad Abdur et al.(2014)[2] have proposed the Mobility Pattern Based Misbehaviour Detection to Avoid Collision in Vehicular Adhoc Networks. This paper presents a misbehaviour detection scheme (MDS) and corresponding framework based on the mobility patterns analysis of the vehicles in the vicinity of concerned vehicles. Initial simulation results demonstrate the potential of the proposed MDS and framework in message's correctness detection, hence its corresponding applications in collision avoidance.

Zhang Linjuan et al. (2013)[3] has proposed a multilevel information fusion approach for road congestion detection in VANETs. In this paper, the authors have proposed a multilevel information fusion approach by combining the fuzzy clustering based feature level information fusion (FCMA) and the modified Dempster–Shafer evidence reasoning-based decision level information fusion (D-SEMA). The FCMA can extract the key features from atomic messages, thereby greatly reducing the network traffic load. Furthermore, the D-SEMA mechanism is used to judge whether the road congestion event occurs.

Ghaleb F. et al.(2013)[4] proposed a mobility pattern based misbehaviour detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions

(Misbehaviour), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse or denial of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives :(i) physical movement and (ii) information security perspectives. This paper includes algorithms by which the misbehaviour can be detected.

Samara G. et al. (2010) [5] proposed various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, and Pranksters.

Seuwou.P et al. (2012) [6] proposed VANET as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst them (V2V communications) and with road -side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in VANET, according to him the attacks are classified into two broad categories physical attack and logical attack.

Qian.yi et al.(2008)[7] proposed an overview on a priority based secure MAC Protocol for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper he proposed that the MAC Protocol is having massages with different priority for different application to access DSRC (Dedicated short range communication channel) Chanel.

Javed.M.A. et al. (2010)[8] proposed "A Geo casting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management". In this paper he proposed the geo casting packet transmission technique to transfer safety message in a vehicular network. He uses OPNET based simulation model to analyses the performance of proposed protocol .According to him the VANET can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. The proposed protocol select the furthest vehicle for the rebroadcast with the help of new back off window design which reduces the number of packet transmission thus lowring the contention levels.

Hung c.c. et al. (2008)[9] proposed traditional ad hoc routing protocols are not well suited for this high dynamic network. In this paper they propose a new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN. According to paper HVN integrates Wireless Metropolitan Area Network (WMAN) with VANET technology and reserves advantages of better coverage in WMAN and high data rate in VANET. Vehicles in HVN can communicate with each other and access Internet ubiquitously. They mainly focus on the routing issue for HVN, because the routing protocol for HVN is different from those used in MANET or VANET.

Dias .A.J. et al. (2011)[10]proposed a tested performance evaluation of DTN-based routing protocols applied to VDTNs(vehicular delay tolerant networks). The objective is to evaluate and understand how popular routing strategies perform in sparse or partitioned opportunistic vehicular network scenarios. This paper based on Spray and Wait protocol. The idea behind using this protocol is to exploit the physical motion of vehicles and opportunistic contacts to transport data between disconnected parts of the network.

Sumra A.I. et al.(2011)[11] proposed a key component of security in vehicular application if any component behave unexpectedly then it would be harmful for other users of the network. In this paper, they are proposed three different trust levels in peer to peer vehicular network. Purpose of proposed trust levels to discuss in detail is the functionality of different component of network which circumvents the attacker and emphasizes the role of trusted users in peer to peer vehicular communication. According to this paper Trust is combination of expectancy, belief in expectancy and willingness to be vulnerable for that belief. This paper divide trust in three levels which are: zero trust level, weak trust level, strong trust level.

Open Challenges:

From the literature overview it clearly emerges that there are several works related to the routing of information between vehicular nodes have been proposed to its inherent potentialities. Regardless of the modifications and enhancements proposed in the VANET's to exceed challenges and constraints of vehicular ad hoc networks, research in the field can be developed with some hints for future deployment can be provided as follows.

Many issues related to the security methods are completely open. Most of the vehicular nodes are resource constrained devices and signature and authentication operations can be expensive in terms of time and energy resources consumption. This complicates the management of the security framework in the transfer of the information. Therefore the use of the general cryptographic methods may help in providing the security necessary for the secure transfer of the information through the network in the encrypted format to the destined nodes where the information can be retrieved with the help of the keys. Thus a secured communication between the nodes in the vehicular network can be provided.

The other major challenge is the congestion and collision control in the VANET. Usually in crammed networks, more number of vehicles transmits information at multiple points and the channel gets congested easily. Such situations will decrease the throughput and the delay will increase. Such issues can be dealt with the event driven detection technique which checks the safety message and starts the congestion control algorithm each time when the safety message is

generated or detected. The low priority messages will be paused as soon as the congestion control is launched and allows the high priority messages to the transferred quickly without any further delay. The measurement-based detection is also used which monitor the packets queue when congestion is sensed then it discards the low priority messages and allows the quick transfer of the prioritized messages. Thus the congestion in the communication network can be managed.

Other such challenge is the bandwidth and packet rate problems. The issue with wireless networks in the transfer of information is there is only a limited amount of bandwidth available in the transfer channels. Such conditions can be managed by the types of safety message in ad hoc networks. Initially, the messages alert other vehicles which are located in that area of vehicle state. Next, in the state of unsafe driving the necessary warnings are generated. When periodic are large because of the high density the warning messages will take a lot of time to be received. In an emergency situation, the flow of periodic messages should be bounded. The possibility that a message will arrive depends on the distance between the sender and the receiver, the rate at which the message will be received is based on the type of message and the models used for simulation. Thus by the use of packet priority the messages can be delivered and the packet transfer rate can be managed.

Identified Challenges:

In this section, we discuss the challenges and future trends derived from our analysis.

Trends and Challenges:

VANET security is one of the trending topics in the field of network security. The traffic problem is one of the annoying things that any driver would dream to avoiding. There are number of vehicles which might cause problems which should be reported to other vehicles state to avoid traffic. Sometimes, irrelevant or incorrect information is transmitted by the vehicles which make the situation worse. Thus the initiatives are taken by car manufacturers and governments to improve the safety in the transport system.

Recent improvements in the Transportation Systems imply that the vehicles will be provided with wireless components that will help in communication between the vehicles and form a wireless vehicular state. The general purpose is to enable safe and secure transportation of the vehicles in the networks. This can be obtained with the help of the sensors and other routing protocols which are used for the transfer of the messages. The car manufacturers are integrating the on board units like radar sensors, GPS and others effective sensors for obtaining and to transfer the routing information between the vehicles VANETs involve the routing and addressing concepts. The focus is on the combination of geo networking with mobility and IPV6 that supports the routing of vehicles. Some technologies like ambient traffic sensor application can also be used where the vehicles are provided with sensors that encounter road faults, accidents and congestion. On the encounter of the event, the vehicles will try to notify the centre which monitors the traffic, by sending the message to one of the roadside units in the city. Thus the information can be accessed by all mobile nodes and the congestion and traffic can be controlled by efficient routing of the mobile nodes. Lack of support for these capabilities in the vehicles lead to the insufficient traffic management and also leads to many traffic control and routing issues. Thus we consider that this is an important area for research for the future.

IV. OBJECTIVES

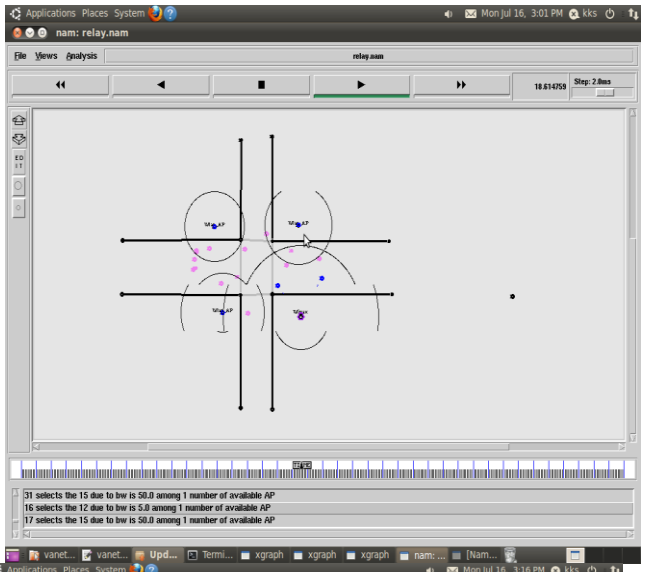
a. To study the literature of various collision detection and avoidance techniques in the VANETs.
b. To study the shortcomings and advantages of the existing solutions.
c. To design the mechanism for detection of point of collision.
d. To design the mechanism for the collision prediction using the movement analysis of vehicle node.
e. To design the mechanism to avoid the prediction collision by altering the movement vehicular.
f. To implement the new security mechanism in Network Simulator 2 (NS2).
g. To obtain and analyze the results.

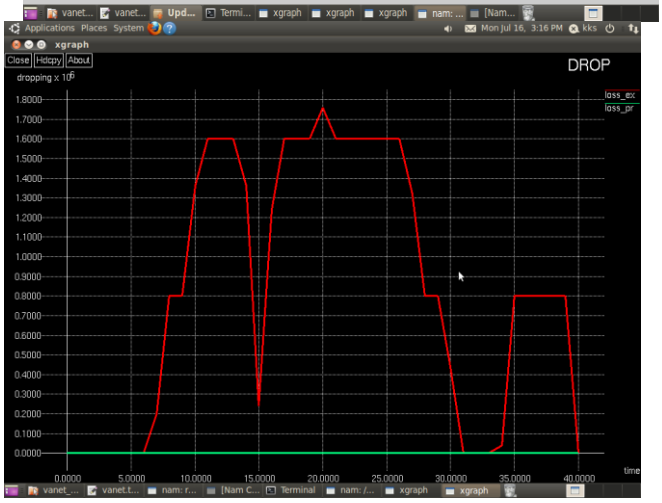
V. METHODOLOGY

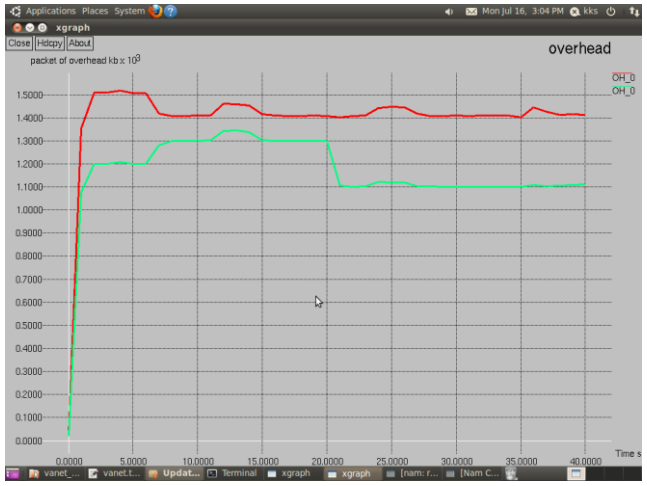
- We will start our research project by conducting a detailed literature review on the prankster attack in case of selfish driver in VANETs to know the problem in detail.
- A detailed security mechanism would be designed to prevent the prankster attack in VANETs.
- The simulation would be implemented using Network Simulator (NS2).
- The obtained results would be examined and compared with the existing security mechanism to address the similar issues.Waterfall methodology comprises the following steps: working out system requirements, drawing up and approving the specification; design and prototyping; development; delivery; analysis and finalization.

VI. RESULT

No of Nodes	No of RSU's	No of LAN's	No of Wi Max
32	4	3	1







Packet Delivery ratio

Fig shows the Xgraph for existed and proposed with a pause time set to 25ms. The X-axis of the graph indicates the No.of Nodes and the Y-axis shows the 92 Packet Delivery Ratio. This graph shows at node 50 the PDR ratio of proposed is 96.59 % and PDR Ratio of existed is 84.62 %. In this figure when the transmission goes from 25th node to 100th node. Here the PDR of proposed will increases but the PDR of existed will decreases .In fig PDR of existed method decreases when the mobility of the vehicles increases whereas PDR of EMMDV increases when mobility of vehicles increases because it has less packet loss. Existed scheme provides 80.87% PDR but proposed scheme provides 97.02% PDR in network size with 100 vehicles and four access points.

Packet Loss

It is the number of data packets that are not successfully sent to the vehicles. The figurative transmission is shown in figure. In this figure, the existed method losses 14% of packets at node/time 25. At the same time proposed method no loss is occurred. In terms of dropped packets, proposed method performance is better than existed. In existed method when the mobility of vehicles increases, the number of packets dropped also increases which means that number of packets not successfully reaching the vehicles is high. The proposed method the number of packets dropped is negligible which means that almost all packets reach the destination successfully.

VII. CONCLUSION

The proposed model has been designed to offer the collision free movement in the VANET cluster. The proposed model has been designed to work in the three layered model whichcomprised of point of collision detection, probability of collision calculation and collision avoidance methods. The proposed model is intended to solve the maximum problems arising in the VANETs in the case of collisions. The expected outcome must be obtained in the form of collision rate, probability of detection, probability of false alarm, etc. The experimental results are expected to solve the problems of collision and to overcome the problems in the existing model.

VIII. References

[1]. Pant V, Higgins CM. Tracking improves performance of biological collision avoidance models. Journal of Biological cybernetics. 2012; 106(4):307–22.

[2]. Liu Y, Yang C, Yang Y, Lin F, Du X. A CBR-based Approach for Ship Collision Avoidance. Proceedings of the 21st International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems: New Frontiers in Applied Artificial Intelligence. 2008. p. 1–12.

[3]. Amudhavel J, et al. An robust recursive ant colony optimization strategy in VANET for accident avoidance (RACO-VANET). International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–6.

[4]. Valdes-Vela M, Toledo-Moreo R, Terroso-Saenz F, Zamora-Izquierdo MA. An Application of a fuzzy classifier extracted from data for collision avoidance support in road vehicles. Journal of Engineering Applications of Artificial Intelligence. 2013; 26(1):173–83.

[5]. Milanes V, Perez J, Godoy J, Onieva E. A fuzzy aid rear-end collision warning/avoidance system. Journal of Expert Systems with Applications. 2012; 39(10):9097–107.

[6]. Amudhavel J, et al. A krill herd optimization based fault tolerance strategy in MANETs for dynamic mobility. International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–7.

[7]. Wang L, Schmidt B, Nee AYC. Vision-guided active collision avoidance for human-robot collaborations. Journal of Manufacturing Letters. 2013; 1(1):5–8.
[8]. Khan AM. Bayesian-Monte Carlo Model for Collision Avoidance System Design of Cognitive Connected Vehicle. International of Intelligent Transportation Systems Research. 2013; 11(1):23–33.
[9]. Amudhavel J, Prabu U, Dhavachelvan P, Moganarangan N, Ravishankar V, Baskaran R. Non-homogeneous hidden Markov model approach for load balancing in web server farms (NH2M2-WSF). Global Conference on Communication Technologies; Thuckalay. 2015. p. 843–5.
[10]. Toledo-Moreo R, Zamora-Izquierdo MA. Collision avoidance support in roads with lateral and longitudinal maneuver prediction by fusing GPS/IMU and digital maps. Journal of Transportation Research Part C: Emerging Technologies. 2010; 18(4):611–25.