Novel Technique for Multi-cast Routing VANET

Goonjan [1], **Abhinash Singla** [2]
Department of Computer Science Engineering
[1] Student M.Tech Bhai Gurdas Institute of Engineering & Technology, Sangrur, Punjab
[2]HOD Bhai Gurdas Institute of Engineering & Technology, Sangrur, Punjab

Abstract- *The vehicular adhoc network is a dynamic network in which mobile nodes can join or leave the network when they want. Three major issues of VANET are routing, security and quality of service. The routing protocols are used to establish path from source to destination. The routing protocols are broadly classified into reactive, proactive and hybrid. AODV is a reactive routing protocol which broadcast the route request to all neighboring node and then those nodes will forward the request to their neighboring nodes. In my proposed work, AODV multicast the route request to root nodes only and then ant colony optimization technique is applied to optimize the path. It will generate a path with shortest distance and leads to improve throughput, reduce packet delivery ratio and delay when compared with the existing protocol.*

Keywords- Multi-casting, broad-casting, fish-swarm optimization, VANET

I. INTRODUCTION

The boom in technology has increased the use of wireless networks. Wireless networks help in connecting people across world and provide communication link among them. When devices are connected they establish a spontaneous connection resulting in an ad hoc network. In this network, devices directly communicate with each other. They use spontaneous establishment of connection because they often evade access point (like router). Several ad hoc networks are LAN networks where devices (computers, mobile phones) communicate directly without passing through access point they are wired networks. When devices are connected wirelessly, they are termed as wireless ad hoc networks (WANET). WANET is a dynamic and a self-configuring network with freely moving nodes. It establish infrastructure less network, devices can join or leave the network whenever they want. One of the rule zones of research examinations of correspondence among the vehicles and street side units all the more particularly the vehicular especially named system (VANETS). In this system every single one of the vehicles and parts of roadside foundation related with each other without requiring a covered structure, send and get data and give admonishing about current activity condition [1]. In-vehicle correspondence can be utilized to trade the data between various parts like vehicles. This framework generally utilized as a part of current vehicle that are available in today time. For the most part two application territories for in-vehicle correspondence it can be recognized into two sections: in the vehicle system of sensor, actuator and controller and second is high rate multi-media correspondence for comfort applications for instance [2]. In vehicle to street side correspondence is likewise called a vehicle to framework correspondence. In this time vehicles impart from the vehicle to a settled framework. This correspondence in the two structures is unidirectional or bidirectional settled framework. Communicate framework bolster the unidirectional exchange of data from communicate station to the vehicle. In this framework the whole vehicle conveys point to point with the base station or access point. In the security of VANET, authenticity is a major challenge. Before accessing all the available services, it is necessary to authenticate by all the active stations in the network. The process of identification or authentication damages the whole network due to violation or attack within the network. The main objective of authentication is to protect nodes from outside or inside attacks in a vehicular network [3]. The authorization levels of vehicles are controlled by the process of authentication. Sybil attacks are prevented by the authentication in VANETs by specifying identity to each vehicle. Message integrity is very important as it ensures that there is no transformation in message between the moment it was sent and received. Hence, the transferred message should match with the received message. It is easy to identify sender location and its identity which is approved by special authority. With the help of authenticated messages it sends, it is easy to identify vehicle. In order to maintain the privacy in the system, it is necessary to have confidential property. This privacy is enforced by the law enforcement authority only in order to create privacy between the communicating nodes. The development of a dynamic routing protocol is one of the major challenges in the design of vehicular ad-hoc network. This protocol provides the assistance in the dissemination of information from one node to another [4]. There is difference between the traditional MANET and the routing in VANET due to utilized topologies is highly dynamic as compared to former. All the developed protocols for MANET environment was tested on VANET. Hence, it remains as a challenge that how to reduce the associated delays form the passing information from one node to another. These protocols can be implemented in real time applications for VANET environment by overcoming issues related to MANET

protocols. It is also necessary to reduce other control overheads so that routing protocol should be able to survive the unpredicted and dynamic nature of vehicular network topology. The major task in VANET is to find out and maintain the desired path for the communication purpose. The used topology in the network architecture is commonly linked with most of the routing protocols in VANET. VANET suffer from various attacks; which are discussed further. As the name recommends the aggressor sit amidst the two communicating vehicle and dispatch this assault [5]. In this aggressor control all the correspondence between the sender and the beneficiary yet communicating vehicles accept they are specifically speaking with each other. It is the most genuine level assault in vehicular system. In this assault assailant sticks the primary correspondence medium and system is not any more accessible to honest to goodness client. Dark gap assault is the assault in which hubs don't take an interest in the system. The dark opening is framed when a set up hub drops out. All the activity in this is diverted towards the particular hub which really don't present because of which information lost [6]. Assailant makes a false picture because of which wastage of information happens. Sybil Attack is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity. It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route. The principle target of assailant is to include some schedule vacancy in the first message that makes delay in the first message and these messages are gotten after these require a period.

II. LITERATURE REVIEW

Navjot Kaur, et.al (2016) presented that Vehicular Adhoc Network is a unique type of the Mobile Adhoc Network which has gotten exceptional consideration with the developing period. There is On Board Units (OBUs) and Road Side Units (RSUs) in the essential model of the VANETs. As every one of these units are convey through an open remote medium, so there will be more risk to the system. Hence, there is a need of security necessities to secure it. The [7] paper portrays different necessities, qualities, testing issues and strategies of security in VANETs. In this paper a hypothetical examination of various security methods of Vehicular Adhoc Networks has been done which think about various plans at various levels like equipment, confirmation, protection and affirmation systems and so on.

Xiao Huang, et.al (2017) proposed a multi-specialist activity flag control framework, which depends on the vehicular impromptu system (VANET), keeping in mind the end goal to enhance the movement limit of the convergence on the genuine street [8]. They likewise build a discrete fluffy controller which is an ideal flag timing system. They did the activity recreation with the improvement of Vissim which depends on Visual Studio and distinctive movement thickness in the street organizes was utilized for the assessment of the flag control impact. According to recreations comes about, it is shown that proposed technique demonstrates viable outcomes when contrasted with others.

Huifang Feng, et.al (2017) displayed in the vehicle specially appointed system (VANET) a fundamental part is played by the key hubs for the spread of data, for which assessment of imperative hubs is important. In this paper, VanetMobiSim was used to examine the time advancement of vital hubs for VANET which depends on the Intelligent Driver Model with Lane Changes (IDMLC). This strategy is actualized by building the fleeting system show at first after which the advancement of critical hubs in VANET was dissected based on four transient measurements [9]. According to got comes about, it is reasoned that the significance of hubs in VANET can't be assessed with the assistance of fleeting closeness centrality. Subsequently, these outcomes help to pick suitable technique for the assessment of the hubs significance in VANET.

Mikhail Buinevich, et.al (2017) displayed issue of determining digital security VANET in this paper which is tackled by changing the estimations of worldwide needs when contrasting elective alternatives for arranging data and specialized communication [10]. Versatile VANET and Internet of Vehicles were used in this paper as an instrument for the investigation of T. Saaty in a mix with an inspecting technique.

Dominik S. Buse, et.al (2018) detested with the improvement and new headways, the cutting edge vehicle frameworks are ending up more unpredictable and cycles are getting to be shorter. Thus, for the cutting edge vehicles, Car-to-X (C2X) correspondence is turning into a more crucial segment [11]. Henceforth, the capacities of framework are investigated by arrange reenactment by utilizing a discrete occasion reproduction approach. In this paper, they additionally proposed an approach for the coordination procedure which is named as Ego-Vehicle Interface (EVI) and the attainability of the proposed approach was gotten from the acquired outcomes.

Jaskaran Singh, et.al (2018) investigated the current vehicular Information Network based on Named Data Networking (NDN) in this paper. The subjective examination showed that normal proposed overhead is 7.36 when contrasted with existing normal overhead which is 9.54 which is fundamental change [12]. Proposed normal conglomeration time is 1.28 over

the current normal collection time are 2.32 and proposed normal time to live is 2.85 over the current normal time to live 3.26. There is no vulnerability is available inside the proposed strategy. Sort 2 fluffy enrollment capacities will likewise be utilized for the further improvement with the goal that more vulnerability can be taken care of in not so distant future.

III. RESEARCH METHODOLOGY

This research work is based on to establish path from source to destination using multicasting approach and also reduce the chances of congestion in the network. In the network, the root nodes are selected in the network for the path establishment from source to destination. The root nodes are selected on the basis of node speed and maximum nodes in the range. The vehicle node which has least speed and maximum number of nodes in the range is selected as the root node. The node which wants to communicate with the destination, firstly source send the route request message to root node and root node check its routing table, if the destination node exists then path will be established to destination otherwise the root node send route request message to another root. This process is repeated until destination node is found in the network. When the destination found in the network, then the root node revert back with the route reply packet and path will be established from source to destination.

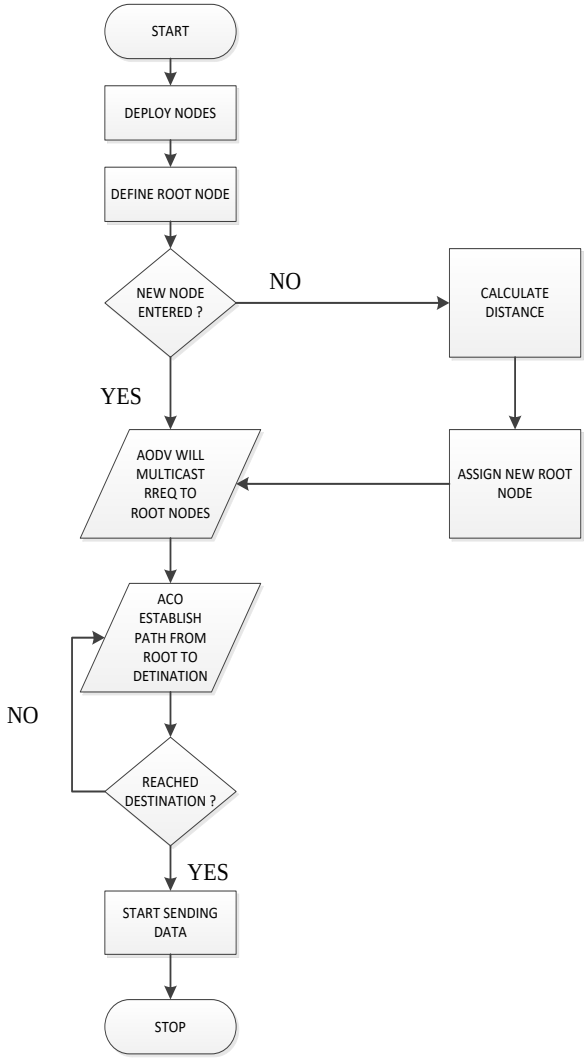

Fig 1: Proposed Flowchart

IV EXPERIMENTAL RESULTS

The proposed work has been implemented in NS2 and the results are analyzed in terms of throughput, packet loss and delay.

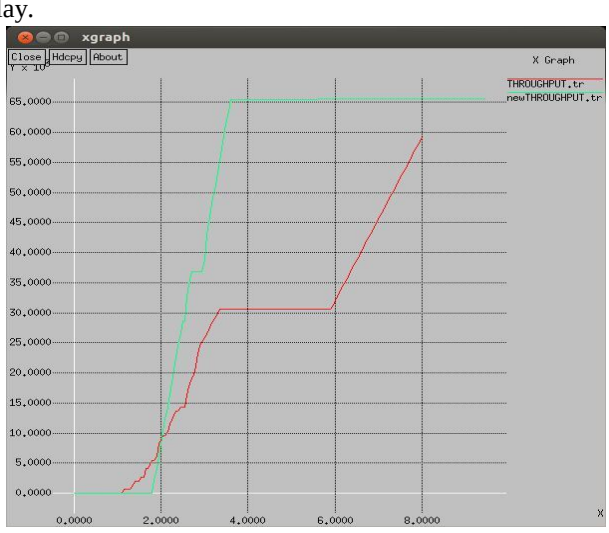

Fig 2: Throughput Comparison

As shown in figure 2, the comparison between the throughput of proposed and existing technique has been shown in graph. From where it is concluded that throughput of proposed technique is high as compared to existing technique.

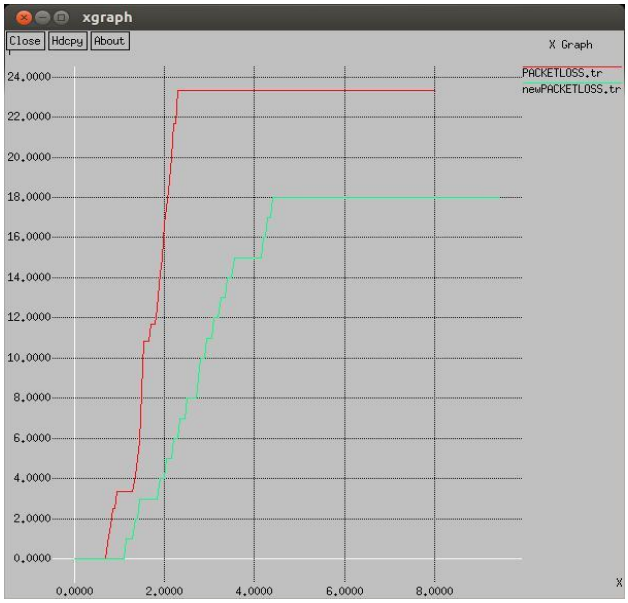

Fig 3: Packet loss Comparison

As shown in figure 3, on the basis of comparison between the proposed and existing method, it is concluded that the occurring of packet loss is less in the proposed protocol as compared to existing protocol.

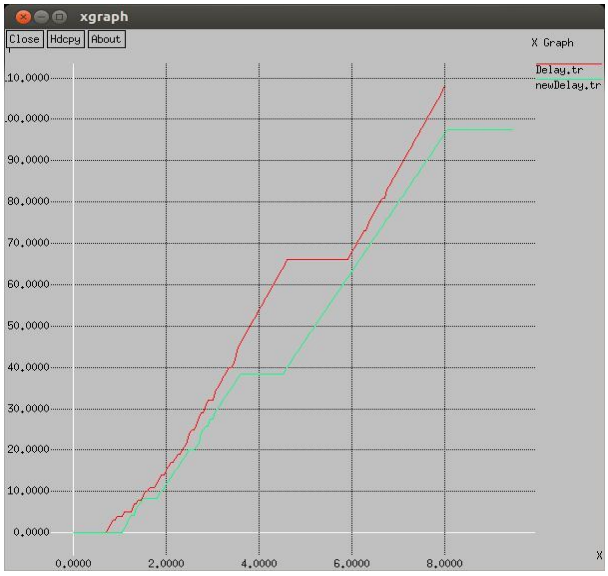

Fig 4: Delay Comparison

As shown in figure 4, the delay comparison between the proposed protocol and existing protocol was done which analyzed that delay is less in proposed protocol as compared to existing protocol.

V. CONCLUSION

In this work, it has been concluded that vehicle adhoc network is self configuring type of network in which network topology change at very steady rate. The secure and shortest path will be established from source to destination using prediction based analysis technique. In the prediction based technique, source node flood route request packets in the network and adjacent nodes of the destination will respond back with the route reply packets. The source select best path on the basis of hop count and sequence number. Due to higher node mobility in the network, the time required for path establishment. In this work, improvement will be proposed in LAR algorithm for predicting locations of the nodes which can make path to destination. This research leads to improve network throughput and reduce network delay.

REFERENCES

[1] Kim JH, Lee S. Reliable routing protocol for vehicular ad hoc networks. AEU-International Journal of Electronics and Communications. 2011 Mar 31;65(3):268-71.

[2] Venkata, M. D., MM Manohara Pai, Radhika M. Pai, and Joseph Mouzna. "Traffic monitoring and routing in VANETs—A cluster based approach." In ITS Telecommunications (ITST), 2011 11th International Conference on, pp. 27-32. IEEE, 2011.

[3] Kanwalpreet kaur and sandeep kad “A Study of Vehicular Information Network Architecture based Named Data Networking (NDN)” International Journal of Computer Applications(IJCA) , Volume 140 –No.6, April 2016.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “Openflow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.

[5] S. I. Fadilah and A. R. M. Shariff, “A time gap interval for safe following distance (tgfd) in avoiding car collision in wireless vehicular networks (vanet) environment,” in 2014 5th International Conference on Intelligent Systems, Modelling and Simulation, Jan 2014, pp. 683–689.

[6] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, “An intrusion detection system against malicious attacks on the communication network of driverless cars,” in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Jan 2015, pp. 916–921.

[7] Navjot Kaur, Savdeep Kad,” A review on security related aspects in vehicular ADhoc networks, 2016, ELSEVIER

[8] Xiao Huang, Qi Zhang , Yu Wang, “Research on Multi - Agent Traffic Signal Control System Based on VANET Information”, 2017 IEEE 20th International Conference on

Intelligent Transportation Systems (ITSC), Vol.3, issue 8, pp. 9-16, 2017.

[9] Huifang Feng, Junxia Wang, Junpeng Zhang, Youji Xu, "Time Evolution of the Importance of Nodes in VANET Based on Temporal Networks", 2017 3rd IEEE International Conference on Computer and Communications.

[10] Mikhail Buinevich, Konstantin Izrailov, Ekaterina Stolyarova, Andrei Vladyko, "Combine Method of Forecasting VANET Cybersecurity for Application of High Priority Way", International Conference on Advanced Communications Technology(ICACT), 2017.

[11] Dominik S. Buse, Max Schettler, Nils Kothe, Peter Reinold, Christoph Sommer and Falko Dressler, "Bridging Worlds: Integrating Hardware-in-the-Loop Testing with Large-Scale VANET Simulation", 2018

[12] Jaskaran Singh, Dr.Karanjit Singh, "Advanced VANET Information Dissemination Scheme Using Fuzzy Logic", IEEE, 2018