Secured Message Transmission between Vehicles for Reducing Delay and Collision in VANET

K. Arthi and Kadivendi Sudha Rani

Abstract: ***With the rapid development of wireless networks, the number of access devices and data volume will continue to grow exponentially due to many new applications beyond personal communications. The routing protocol is a key technology of vehicular ad hoc networks and largely determines the performance of the vehicle in network communication process. The main Aim at the network is congestion problem which exists in commonly used GPSR routing protocols of current vehicular ad hoc networks, in this an existing method improved project of GPSR Geographic Perimeter Stateless Routing (GPSR) routing protocol which controls congestion problem based on the buffering nodes. And Performance simulation for relevant parameters is tested on Ns2 platform. From the results of the analysis, the enhanced GPSR protocol in vehicle's environment has lower packet loss rate and more time delay than the traditional GPSR protocol. In this paper the architecture uses DSDV Destination Sequenced Distance Vector routing protocol,. which has an data packet buffer nodes will sharply increases and also the packet delivery is more, by reducing time delay and collision. Performance parameter improved in larger number of vehicles.***

Keywords: Delay and collision, DSDV protocol, Edge Computing, GPSR routing protocol, RSU, VANET.

I. INTRODUCTION

Vehicular adhoc network is an important role in the industrial field [1]. Actually, VANETs consists of a trusted authority (TRA), and some distributed roadside units (RSUs) and a large number of vehicles. Which has a vehicle with an VANET equipment by using (OBU) on board unit on road. To improve the driving and avoids the accidents, the vehicles will broadcast the traffic signals and jams which are nearby RSU [2]. By using RSU the communications are divided vehicle to vehicle and vehicle to road by controlling DSRC protocol distance short range communication [3]. The TA, which acts as the originally certified equipment which it can checks the vehicles, has original or duplicate equipment. And sends the message to the certified vehicle [4].

RSU: ROAD SIDE UNIT: it maintains the proper infrastructure of RSU unit for sending the route packets to vehicles. It controls traffic signals; RSU is designed to place at road intersections RSU acts as a source of information. Which helps the (OBU) on board unit to get connected to internet.RSU connects with application servers and trust authorities.

Revised Manuscript Received on June 15, 2019

Dr. K. Arthi, Associate professor, Department of Computer Science and Engineering in Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.

Kadivendi Sudha Rani received the B.Tech(computer science and engineering) degree from Jawaharlal Nehru university of india

OBU: ON BOARD UNIT it checks the distance travelled by OBU package. The OBU records which road you drive on verification of exact driven route may take a while when light turns red you have to stop journey. It consists of AU application unit for enhancing safety and to enable the OBU to connect to the network or internet.[fig2]Enhancing security and privacy for identity based and authentication scheme of VANET.

V2V: VEHICLE TO VEHICELE communication provides of potential crash. It checks 360 degree awareness. And the data transmission device equipped in vehicles within 300m range. These V2V warnings are like display, seat vibration, and tone. DSRC is connected to GPS, and then it is V2V it sends the messages common to all the vehicles like vehicle control information, acceleration speed, vehicle speed, Vehicle path history, path prediction.

TRA: TRUSTED AUTHORITY component which enables security in network for two vehicles in VANET to communicate security. It maintains a universally trusted certificate authority.

Functions: Attacks if any happened, Managing list of participating vehicles, Generate keys for encrypting the messages and sending the keys over a secure channel.

V2RSU: vehicle communication with fixed equipments installed along the roadside called RSU to communicate with internet.

OV: Ordinary Vehicle without VANET equipment in vehicle.

ECV: EDGE COMPUTING VEHICLE which can be placed at the junction of road map and maintains the messages by using RSU in Fig.[2]

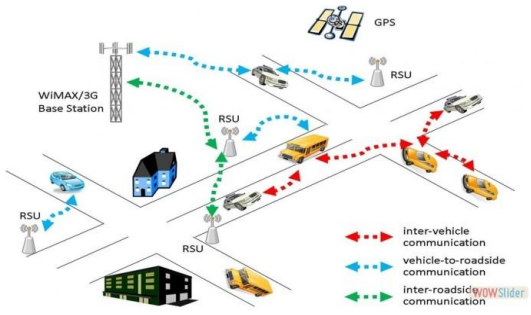

Fig. 1. (a) RSU in junction road

Fig 1 shows the RSU is sending information to vehicles

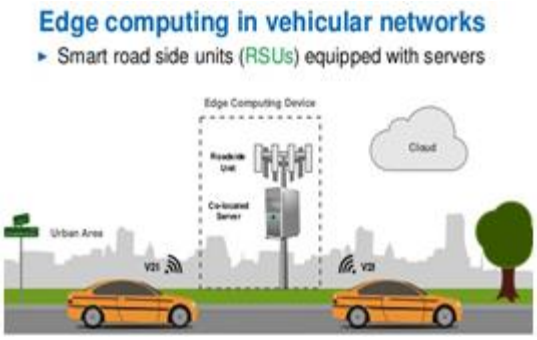

Fig. 1. (b) Edge computing between two vehicles Shows the ECV which describes in above sections

II. RELATED WORK

Fault Tolerance is an important factor in Wireless Sensor Network (WSN) as an emerging research field. Nodes in WSN get easily depleted due to battery limitation in battlefield and unattended environment. Fault causes severe damage in a network, to reduce the effect of this fault, fault tolerance becomes very essential method. To track the network node failure, Negative code Answering (NCA) Algorithm is proposed in wireless sensor network with the assist of Mobile Agent (MA) techniques. MA is lightweight process and this paper used MA as Collecting Agent (CA) and Monitoring Agent (MNA). Agents provide fault tolerance in a network. NCA is used to identify the non-working, malicious, fault node in a network by using Collecting Agent Monitoring Agent. CA can communicate with MNA and made network as fault free. This method increases the performance of the network using Mobile Agent concept in achieving fault tolerance. [5]

Wireless sensor network (WSN) plays an important role in many application areas like in military surveillance, health care etc. A WSN is deployed with a large number of sensor nodes in a wide geographical area. These nodes collect information depending on type of the application and transmit the data towards the sink node. When a large number of sensor nodes are engaged in transmitting data, there is a possibility of congestion in the network. Congestion is one of the critical issues in WSNs because it has direct impact on energy efficiency of sensor nodes, and the application's throughput. Congestion degrades overall channel capacity and increases packet loss rate. In order to handle these problems, an efficient congestion control mechanism required. a number of congestion control mechanism have been proposed in literatures. Any congestion control mechanism consists of congestion detection, congestion notification and rate adjustment mechanisms. Some of the mechanisms reviewed in this paper are CODA, PCCP, FACC, Fusion, and Siphon. The paper has discussed the pros and cons of each of these mechanisms. [6]

Despite the huge number of protocols proposed in the literature, congestion control in WSN remains challenging. A review and taxonomy of the state-of-the-art protocols from the literature up to 2013 is provided in this paper. First, depending on the control policy, the protocols are divided into resource control vs. traffic control. Traffic control protocols are either reactive or preventive (avoiding). Reactive solutions are classified following the reaction scale, while preventive solutions are split up into buffer limitation vs. interference control. Resource control protocols are classified according to the type of resource to be tuned. [7]

Wireless Sensor networks (WSN's) are expected to have wide range of applications and increasing deployment in the near future as it provides a low cost solution with respect to both maintenance and installation WSN's are distributed self governing sensors used to monitor the physical conditions of the environment. They are constructed by "nodes" where each of them is connected to sensors. A sensor node carries all the necessary components for transmission and reception of data packets. When nodes are densely distributed or due to high flow rate, Congestion of data packets are encountered which leads to packet loss, inefficiency and lack of f. [8] In wireless network the congestion problem will not only leads to packet loss but also increases the delay of time in delivery of packets .so by these situation the effective system if packet loss and energy can be increased. In this, we propose a novel decentralized and weighted fairness guaranteed congestion control protocol (WFCC). It introduces the weight of a node and reflected area. Based on these it uses closed loop for metrics i.e., $1 - (10c/9)^2$ where 0 <; c <; 0.2 is a constant. It achieves 95% based congestion control. Moreover, it achieves 50% and 19% network throughput and weighted [9]. It has an average of PCCP congestion control.

Here we are going to propose the method called ECV. Which it can maintains in the junction road with an RSU communication process

SECURITY REQUIREMENTS

Authentication process: Authorizing OBUS and sending of messages.
Message integrity: it secures the data integrity.
Privacy key: which provide the content unlink ability and prevent drivers hacking.
Traceability and revocation: tracing and invalid changing of OBUs by the authority.
Availability: it provides the network availability and traffic jam attacks.
Efficiency: maintains the low computation ratio of the output and input of any system.

III. PROPOSED METHOD

In this method we are using GPSR routing protocol (geographic perimeter stateless routing protocol). By using the TCP and FTP transmission process for congestion control in VANETs. This GPRS protocol maintains slowly processing It consists of More number of Packet losses and more time delay in sending packets and also parameters are low.

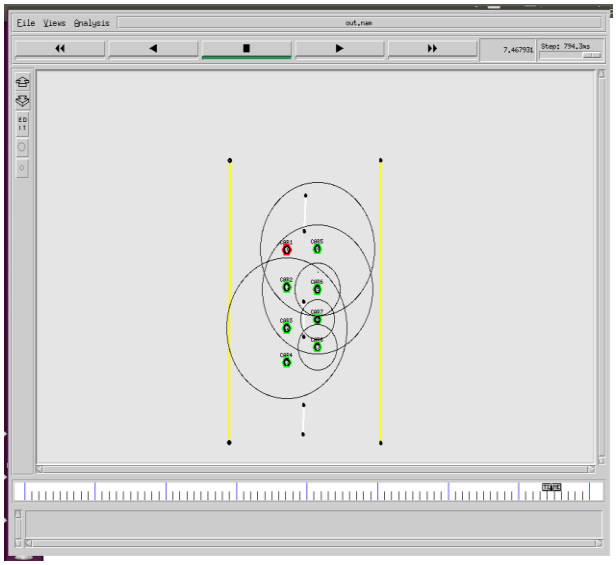

Fig. 2. Moving vehicles in two way shows that the vehicle is sending message about accident

In this paper we are using DSDV Protocol. Destination Sequenced Distance Vector routing (DSDV). It maintains the shortest path of the first node and maintains the short distance of the other node. It is a routing protocol which maintains the low in buffering nodes and maintains time delay [10]. It updates the vehicles and maintains the buffering nodes.

UDP and CBR Transmission protocol is used and maintains fast processing. By number of data packets in nodes Buffer will increase sharply when number of Broadcast nodes transmits data to the same Forwarding node successively. Time delay is low. And Performance parameter Improved in larger number of vehicles.

System Implementation

Module:

1) Node creation
2) Packet transfer
3) Attacker node
4) Receiver.

NS2 is a distinct event simulator focused on networking research. NS2 imparts considerable support for simulating the wired and wireless protocols. Here the user's perspective is NS2 is an OTCL interpreter which takes OTCL as input and gives the trace file as the output. There are two languages in NS2 tool (C++ and OTCL) [10]C++ is used for creating objects and mains speed in giving output. OTcl is used as a front-end to setup the simulator and to configuring the objects. The common procedure for generating a simulation can be classified into various steps.

They are

1) Topology definition
2) Node and link configuration
3) Execution
4) Performance analysis
5) Graphical Visualization (X graphs)

A. Tran receiver

It consists of Transmitter as well as receiver configuration, which act as a VANET node.

B. TCP

Transmission control protocol is the responsibility for communication. It is one of the main network protocol. It placed in initial network which can be implemented by the internet protocol(IP).it can be referred as TCP/IP.

C. CBR (Constant bit rate)

Constant Bitrate (**CBR**) it is used in telecommunications, which can be related to the quality of service. When comparing with Bitrate, while **constant bit rate** means it maintains the code output.

D. Trust value generation

It gives the data trust, node trust, functional trust and recommendation trust for each communication.

E. Trust based credit value assigner

It receives all trust values and assigns a credit value for a particular node and communication.

F. Data and traffic analyzer

It analyzes the size and content of the data and traffic in the network.

a) In this proposed method they had implemented different types of phases. They are:

1. System Initialization Phase.
2. The Generation Phase of Vehicles' Pseudo Identity and private key
3. The Election Strategy of ECV.
4. The Batch Authentication of ECV.
5. The RSU maintains the result of ECV.
6. The Message scheme of the Ordinary Vehicles.

1. **System Initialization Phase**:

In this phase, TA maintains the necessary system parameters, and reloads the RSU's memory in all vehicles, because TA is connected with RSU through internet.

2. **The generation Phase of Vehicles' Pseudo Identity and public key:**

In this vehicles must pass a private key of message before sending message to ensure authentication. this phase is used to maintain private key, and signature.

3. **The Election Strategy of ECV:**

ECV help the RSU authentication message signatures. In this we choose the trusted vehicles which have an ECV's characters of small distance to RSU and sufficient available computations.

4. **The Batch Authentication of ECV:**

There are some stages in ECV

a)Task determination,
b)Batch authenticity, and
c)Result feedback.

a) Task Determination stage*:*
In this stage, the RSU places pseudo identity list of its received message which is owns to ECV, after receiving the message the RSU sends back the message to ECV.

b&c) Batch Authenticity and Results Feedback Stage:
When the ECV receives the message it checks the message by using public key, if it is trusted it process the steps, otherwise it gets rejected.

5. The RSU verify the Authentication Result of ECV:

The packet loss and delays will always happen in the trusted VANETs. If the RSU doesn't receive the result from ECV, it assigns with another ECV and the RSU checks the whether the message is valid if it is not then it rejects the message.

6. The Message scheme of the Ordinary Vehicles:

In this scheme, the ordinary vehicle has no need to verify the messages independently sent by other vehicles. It has two filters for sending information of nearby vehicles.

PASSIVE MULTI-HOP CLUSTERING ALGORITHM (PMC):

Each VANET vehicle has its own role in cluster process it changes. It modifies its own vehicles there are some states.
1)INITIAL (IN). It is an initial stage which an vehicle is connected to an network.
2) STATE_ELECTION (SE). It is an stage which is connected to network after the initial state has connected.
3) CLUSTER_HEAD (CH). It is an role which can be similar to the clustering heads.
4) CLUSTER_MEMBER (CM). It is an state which can has an distance between cluster head and cluster member which may have multiple hop.

IV. SIMULATION SETUP

In this simulation process the vehicles movement occur in the road map. Here we had done the simulation process by moving the vehicles by using network animator. So we get (.tcl file) and named as (ns2 VANET.tcl) so the program can be rub by ns2 tool. By the below picture we can show the movement of vehicles.

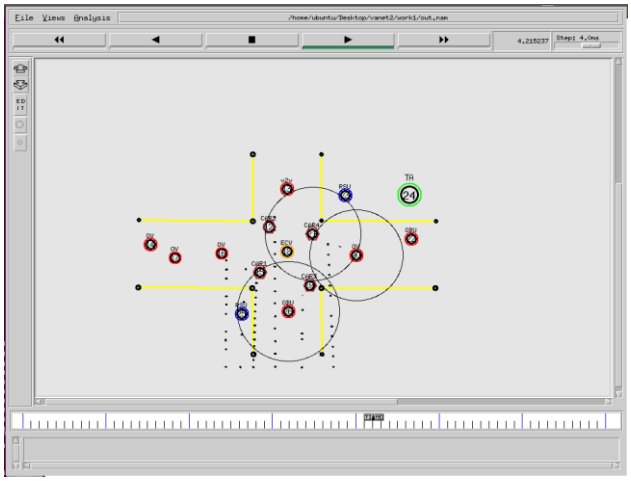

Fig. 4. Vehicles with VANET communication (Shows movement of vehicles with VANET communication)

V. RESULTS AND ANALYSIS

In these performance metrics, there are different simulations and average value in each plotting graphs. In these result the first graph shows the lost packets. we see that the data packets that were losing at time delay and delivers at the time of delay of packets .This shows the lost packets and the time laps between source and destination during the transmission.

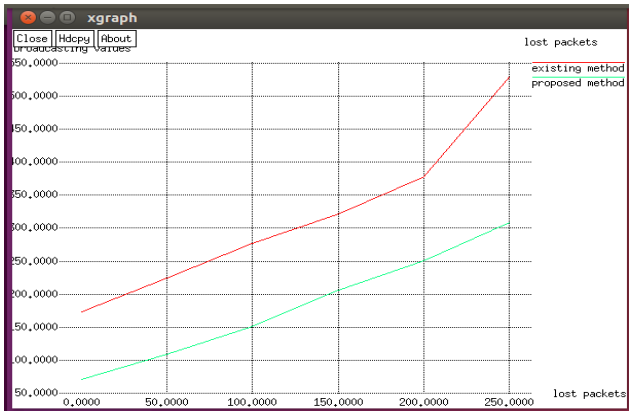

Fig. 5. (how much the input has lost by vehicles)

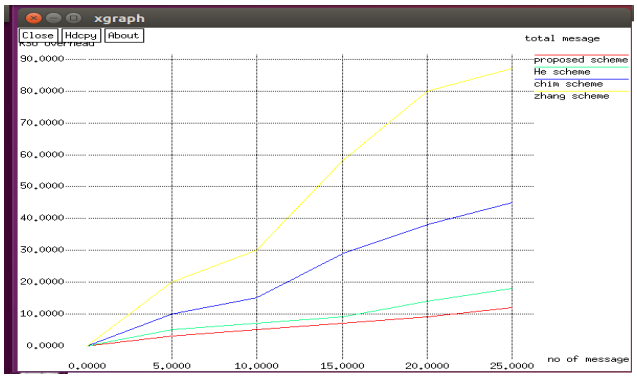

Fig 5.1(The schemes which an authors had proposed in step by step process in RSU overhead)

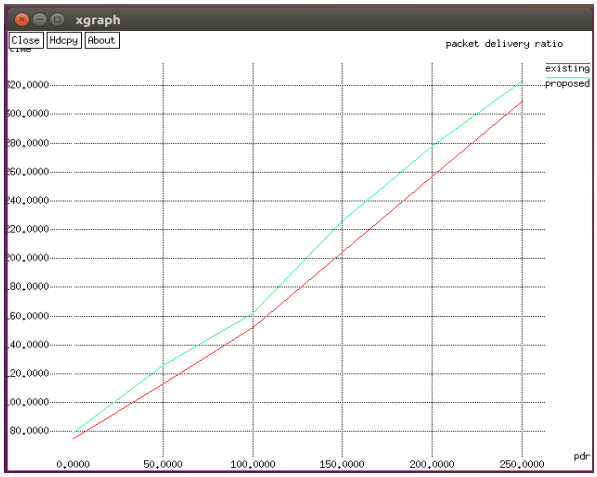

Fig 5.2 The traffic bandwidth for the expected approach has been enhanced than the existing method. Traffic bandwidth in kbps = (Received size / (Stop Time – Start Time)*1/60

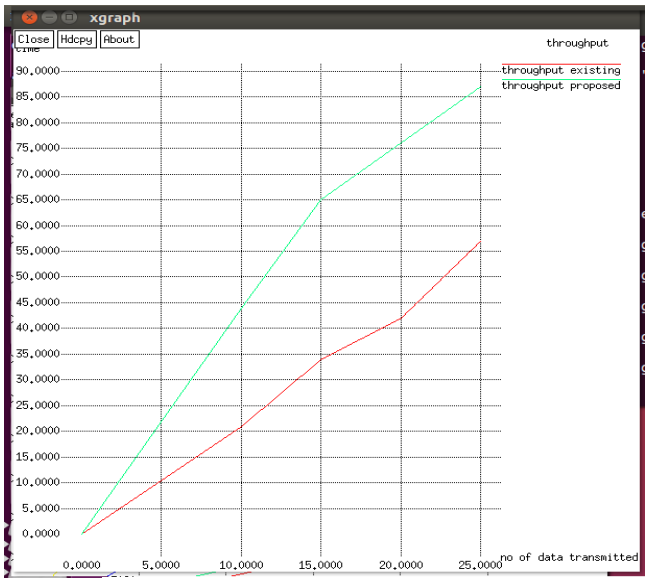

Fig 5.3.Throughput is defined as number of packets transmitted from source to destination in a particular time (megabit/sec). Alsothe existing techniques of throughput analysis have been improved for the forecast technique.

VI. CONCLUSION

This paper mainly focuses on analyzing the topology based routing protocols in VANET. Here we used the GPRS routing protocol for buffer nodes but here the GPRS protocol has some delay in packets. So the proposed system uses NS2 tool to simulate DSDV routing protocols with realistic mobility model. without buffering the nodes and time delay is low in sending packets. In future, it can be simulated with more number of nodes in vehicles.

REFERNCES

1. Y. Toor, P. Muhlethaler, and A. Laouiti, “Vehicle ad hoc networks: Applications
2. And related technical issues,” IEEE communications surveys &tutorials, vol. 10, no. 3, 2008.
3. F. Qu, Z.Wu, F.-Y. Wang, and W. Cho, “A security and privacy review ofVANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 16,no. 6, pp. 2985–2996, 2015.
4. J. B. Kenney, “Dedicated short-range communications (dsrc) standards inthe united states,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182,2011.
5. S.Zeadally,R.Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehiculared hoc networks (VANETs): Status, results, and challenges,” TelecommunSyst., vol. 50, no. 4, pp. 217–241, 2012.
6. J.Yick, B.Mukherjee and D.Ghosal, “Wireless sensor network survey”, Computer Networks, Vol.52, No.12, pp.2292–2330, 2008.
7. S. Borasia and V. Raisinghani, “A review of congestion control mechanisms for wireless sensor networks”,Springer BerlinHeidelberg Technology Systems and Management, pp.201–206,2011.
8. A. Rezaei and M.K. Rafsanjani, “Congestion control protocolsin wireless sensor networks: A survey”, Journal of AmericanScience, Vol.8, No.12, pp.772–777, 2012.
9. C. Luo and W.X. Xie, “Fuzzy AQM for congestion avoidanceand control in sensor networks”,Chinese Journal of Electronics,Vol.42, No.4, pp.679–684, 2014.
10. G. Li, J. Li and B. Yu, “Lower bound of weighted fairness guaranteedcongestion control protocol for WSNs”, Proceedings ofIEEE INFOCOM, pp.3046–3050, 2012.
11. Dharmendr Sutariya, Shrikant Pradhan, “Evaluation of Routing Protocols for VANET in City Scenarios” 978-1-4577 IEEE, 2011

AUTHORS PROFILE

Dr. K. Arthi is an Associate professor in the Department of Computer Science and Engineering in Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India. She received her Ph. D and M.E. degrees in Computer Science from the Anna University, Chennai, in 2015 and 2005, respectively. She has 10 research publications in reputed journals. Her research interests include wireless networking, wireless sensor networks, network protocol, Biometrics and algorithm design and resource management in computer networks.

Kadivendi Sudha Rani received the B.Tech(computer science and engineering) degree from Jawaharlal Nehru university of india in 2015 & currently pursuing M.Tech(CSE) in Vel Tech University.