International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Parameters Analysis by Implementing Portable Proactive Protocols for Communication of Bandwidth Nodes Using Fuzzy Constraints

Manasvi Mannan[1], Namit Aggarwal[2]

[1]Assistant Professor Punjab College, Lalru (Punjab),

[2]Punjab College of Engineering Technology, Lalru (Punjab)
Electronics & Communication Engineering

Abstract: ***In VANET on-demand/ Proactive protocol had been used for communication that computes the routing path dynamically at the time of transmission. Reactive protocol choose shortest path for communication but the shortest path does not guarantee of delivery of safety message. In the base paper other factor like Delay, probability of collision; Bandwidth had been considered to develop surgery construct rules for communication. This causes problem for communication due to selection of rules. To overcome this fuzzy constant must include number of intermediates nodes & number of hopes used for transmission of safety message.***

Keywords: VANET, Delay, Bandwidth, Intermediates nodes & hopes, AODV, DSR for communication bandwidth nodes

1. Introduction

1.1 VANET

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

1.2 Routing in VANET

1.2.1 Protective routing protocol:

Proactive routing protocols employ standard distance-vector routing strategies (e.g., Destination-Sequenced Distance-Vector (DSDV) routing) or link-state routing strategies (e.g., Optimized Link State Routing protocol (OLSR) and Topology Broadcast-based on Reverse-Path Forwarding (TBRPF)). They maintain and update information on routing to all nodes even then also when the path is not used. Route updates are periodically performed regardless of network load, bandwidth constraints, and network size. The main limitation of such approaches is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently.

1.2.2 Reactive routing protocol

Reactive routing protocols such as Dynamic Source Routing (DSR), and Ad hoc On-demand Distance Vector (AODV) routing implement route determination on a demand or need basis and maintain only the routes that are currently in use, thereby reducing the burden on the network when only a subset of available routes is in use and this limit the bandwidth wastage. Communication among vehicles will only use a very limited number of routes, and therefore reactive routing is particularly suitable for this application scenario.

1.2.3 Position-based routing

Position-based routing protocols require that information about the physical position of the participating nodes be available. This position is made available to the direct neighbors in the form of periodically transmitted beacons. A sender can request the position of a receiver with the help of a location service. The routing decision at each node is then based on the destination's position contained in the packet and the position of the neighbor of the forwarding node. Consequently, position-based routing does not require the establishment or maintenance of routes.

1.2.4 Forwarding

A geographic unicast transports packets between two nodes via multiple wireless hops. When the requesting node wants to send a unicast packet, it finds the position of the destination node by looking at the location table.

1.2.5 Protocols for dedicated short-range communication (DSRC)

Protocols, namely Coordinated External Peer Communication (CEPEC) and Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks .(CARAVAN) use mapping and timeslot allocation to minimize the occurrence of denial of service attacks or attacks that burden the limited bandwidth present in vehicular networks. Communications in a vehicular network are susceptible to denial of service attacks by jamming the communication medium or taxing the limited wireless bandwidth that is available. These attacks are occurs due to the DSRC standard specification that a vehicle only send data when it senses that the channel is ideal, allowing a malicious vehicle to constantly transmit noise to prevent transmission from within sensing range of the attacker vehicles.CARAVAN includes a new link layer protocol called Adaptive Space Division Multiplexing (ASDM) that allocates timeslots to vehicles to maximize anti-jamming protection.

2. Review of Literature

Sharanappa (2014) et al. in the paper "Performance Analysis of CSMA, MACA and MACAW Protocols for VANETs" analyse the Carrier sense multiple access (CSMA), Multiple Access with Collision Avoidance (MACA) and Multiple Access with Collision Avoidance for Wireless (MACAW) for VANET environment. Vehicular Ad Hoc Networks (VANETs) are a special type of Mobile Ad Hoc Networks (MANETs). Recent advances in various wireless communication technologies and the emergence of computationally rich vehicles are pushing VANET research to the forefront in academia and industry. A lot of research results have been published in various areas (such as routing, broadcasting, security and others) of VANET in the last decade covering both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) scenarios. One specific area of VANET that still faces significant challenges is the design of reliable and robust media access control (MAC) protocols for V2V communications. Many algorithms of V2V MAC methods (including various VANET standards) have been proposed for VANETs over the last, few years that also focused on the benefits and limitations of the proposed MAC techniques as well as their ease of implementation in practice and future deployment.[1]

Khalid (2013) et al. in the paper "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications" An analytical model for the reliability of a dedicated short-range communication (DSRC) control channel (CCH) to handle safety applications in vehicular ad hoc networks (VANETs) is proposed. Specifically, the model enables the determination of the probability of receiving status and safety messages from all vehicles within a transmitter's range and vehicles up to a certain distance, respectively. The proposed model is built based on a new mobility model that takes into account the vehicle's follow-on safety rule to derive accurately the relationship between the average vehicle speed and density. Moreover, the model takes into consideration 1) the impact of mobility on the density of vehicles around the transmitter, 2) the impact of the transmitter's and receiver's speeds on the system reliability, 3) the impact of channel fading by modeling the communication range as a random variable, and 4) the hidden terminal problem and transmission collisions from neighboring vehicles. It is shown that the current specifications of the DSRC may lead to severe performance degradation in dense and high-mobility conditions. Therefore, an adaptive algorithm is introduced to increase system reliability in terms of the probability of successful reception of the packet and the delay of emergency messages in a harsh vehicular environment. The proposed model and the enhancement algorithm are validated by simulation using realistic vehicular traces.[2]

Mahalle (2012) et al. in the Paper "A DSRC Based Smart VANET Architecture" defines the DSRC technology and its defects in order to achieve reliable content distribution. To optimize the performance of the vehicular networks, a novel network architecture using the cross-layer paradigm is presented. The architecture is called Smart Vehicular Ad-hoc Net-work (Smart VANET) architecture. The Smart VANET architecture can support safety, traffic management and commercial applications. The Smart VANET architecture abides by the DSRC channel plan. The architecture divides road into segments and assigns a service channel to each segment. The Smart VANET combines a segment based clustering technique with a hybrid Medium Access Control (MAC) mechanism (known as the Smart MAC protocol). Using cross-layer integration, Smart VANET also provides a solution for broadcast storm problems and offers scalability. The paper presents the Smart VANET architecture and states its advantages.[3]

Chan-Ki (2012) et al. in the paper "Survey of MAC Protocols for Vehicular Ad Hoc Networks" provide a survey of Media Access Control protocols for vehicular ad hoc networks and classify the existing Media Access Control protocols into the three major categories of time-based, dedicated short-range communication-based, and directional antenna-based. Moreover, they discuss the characteristics of these Media Access Control protocols and show their advantages and disadvantages. In addition we define some open issues and future work related to Media Access Control protocols for vehicular ad hoc networks. A vehicular ad hoc network is a special kind of mobile ad hoc network, and can be divided into two further types of networks, a vehicle-to-vehicle network or a vehicle-to-infrastructure network. However, unlike existing mobile ad hoc networks, vehicular ad hoc networks have unique characteristics, including high node mobility and a rapidly-changing topology. Vehicular ad hoc networks should be designed to accommodate these characteristics when we design them. To do this, many researchers have proposed Media Access Control protocols to improve the performance. Most of these studies deal with quick message transmission to support the high mobility of nodes, multiple channels for multiple connections in high-density urban node areas, and channel coordination.[4]

Saurabh (2012) et al. in the paper" DEMO: Simulation of Realistic Mobility Model and Implementation of 802.11p (DSRC) for Vehicular Networks (VANET)" demonstration and description of generating realistic mobility model using various tools such as eWorld, OpenStreetMap, SUMO and TraNS. Generated mobility scenario is added to NS-2.34 (Network Simulator) for analysis of DSR and AODV routing protocol under 802.11p (DSRC/WAVE) and 802.11a. Results after analysis shows 802.11p is more suitable than 802.11a for VANET.[5]

Katrin (2011) et al. in the paper "How Severe is the Hidden Terminal Problem in VANETs when Using CSMA and STDMA?" propose a definition of the hidden terminal problem suitable for broadcast transmissions and proceed with a case study to find how the packet reception probability is affected by the presence of hidden terminals. Two different medium access control methods; carrier sense multiple access (CSMA) from IEEE 802.11p and self-organizing time division multiple access (STDMA), are subject of investigation through computer simulations of a highway scenario with a Nakagami fading channel model. The results reveal that the presence of hidden terminals does not significantly affect the performance of the two MAC protocols. STDMA shows a higher packet reception probability for all settings due to the synchronized packet transmissions.[6]

3. Problem Formulation

VANET is extension of MANET that deals with vehicles for communication of auto driven system. In this approach the nodes have been approved as vehicles that connected to read side units available in the communication area. RSU available are concerned for transmission of information about traffic density, collision, position & speed of the nodes. The RSU transmit the safety message over the communication range for reliable communication by avoiding collision b/w he nodes. Various protocols had been utilized for reliable communication & transmission of safety message. In VANET on-demand/ Proactive protocol had been used for communication that computes the routing path dynamically at the time of transmission. Reactive protocol choose shortest path for communication but the shortest path does not guarantee of delivery of safety message. In the base paper other factor like Delay, probability of collision; Bandwidth had been considered to develop surgery construct rules for communication. This causes problem for communication due to selection of rules. To overcome this fuzzy constant must include number of intermediates nodes & number of hopes used for transmission of safety message.

4. Results and Discussions

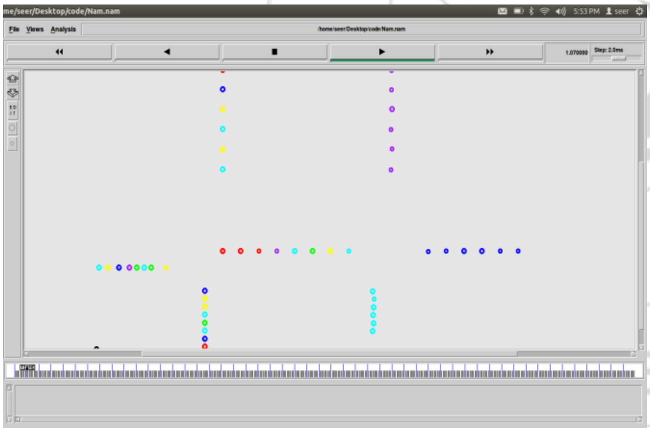


Figure 4.1: Initialization of nodes

This scenario is use to represent the initialization of nodes.

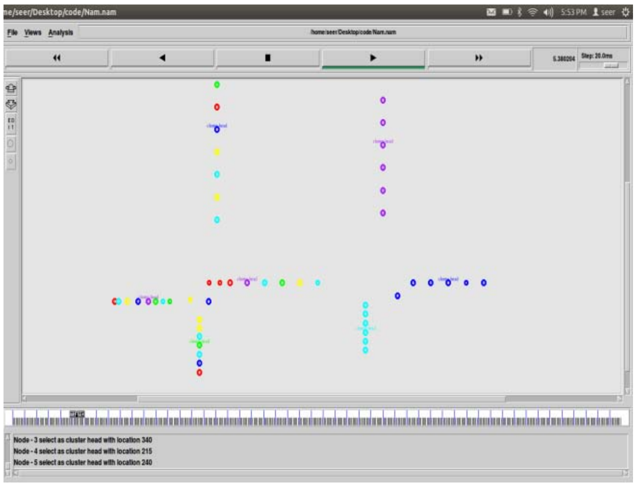
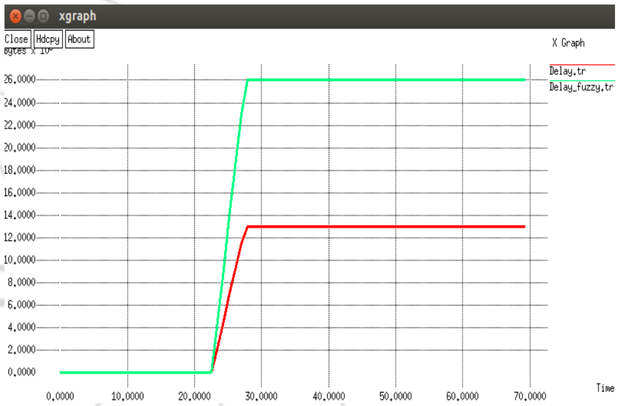


Figure 4.2: Initialization of cluster head & sub cluster head

This scenario is use to represent the cluster head & sub cluster head.

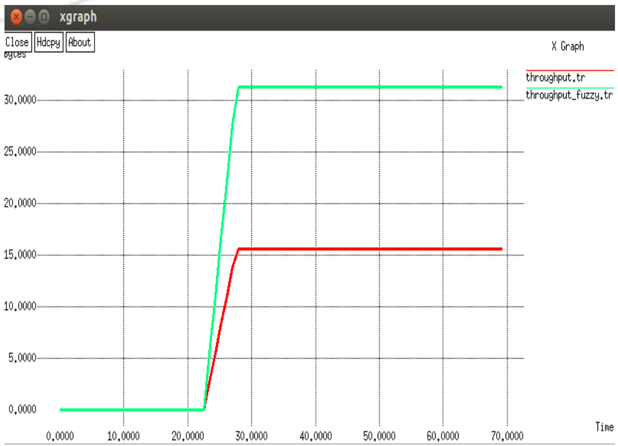


Graph 4.1: Delay

This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D = (T_r - T_s)$$

Where, T_r is receive time and T_s is sent time of the packet. In this figure green line is use to represents the delay with fuzzy. Red line is use to represents end to end delay.

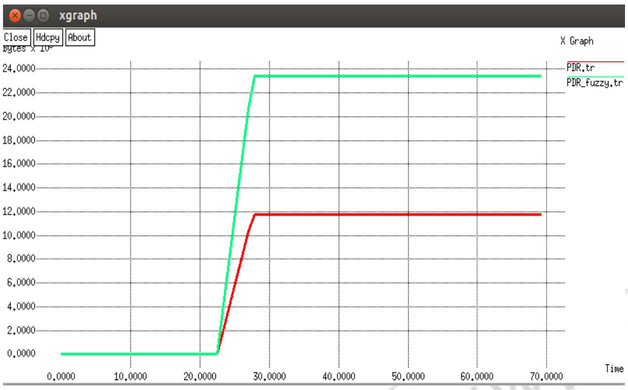


Graph 4.2: Throughput

It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation.

In this figure green line is use to represents the throughput with fuzzy. Red line is use to represents Throughput.

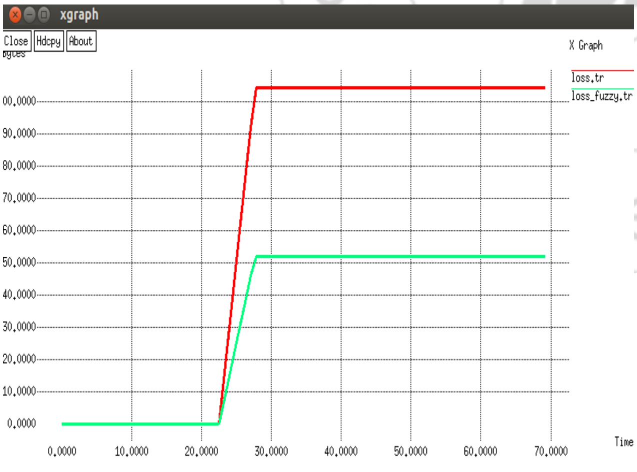


Graph 4.3: PDR

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

$$PDR = (P_r / P_s) * 100$$

Where, P_r is total packet received and P_s is total packet sent. In this figure green line is use to represents the PDR with fuzzy. Red line is use to represents PDR.



Graph 4.4: Loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The Transmission Control Protocol (TCP) detects packet loss and performs retransmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and reduces throughput of the connection. In this graphical representation of packet loss different parameters have been computed at different time intervals. In this figure green line is use to represents the loss with fuzzy. Red line is use to represents Loss.

5. Conclusion

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. VANET is extension of MANET that deals with vehicles for communication of auto driven system. RSU available are concerned for transmission of information about traffic density, collision, position & speed of the nodes. The RSU transmit the safety message over the communication range for reliable communication by avoiding collision b/w he nodes. Various protocols had been utilized for reliable communication & transmission of safety message.

In VANET on-demand/ Proactive protocol had been used for communication that computes the routing path dynamically at the time of transmission. Reactive protocol choose shortest path for communication but the shortest path does not guarantee of delivery of safety message. In the base paper other factor like Delay, probability of collision; Bandwidth had been considered to develop surgery construct rules for communication. This causes problem for communication due to selection of rules. To overcome this fuzzy constant must include number of intermediates nodes & number of hopes used for transmission of safety message. At last we got various types of parameters like Delay, Bandwidth, Intermediates nodes & hopes. On the basis of these parameters we conclude that our system gives us better results.

References

[1] Sharanappa P. H. and Mahabaleshwar S. K., "Performance Analysis of CSMA, MACA and MACAW Protocols for VANETs" International Journal of Future Computer and Communication, Vol. 3, No. 2, April 2014.
[2] Khalid Abdel Hafeez, Lian Zhao, Bobby Ma, Jon W. Mark, "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications" IEEE Transactions On Vehicular Technology, Vol. 62, No. 7, September 2013.
[3] Mahalle N.S., Deshmukh G.D., Raut A.S. and Totawar A.L. "A Dsrc Based Smartvanet Architecture", International Journal of Wireless Communication, Volume 2, Issue 2, 2012, pp.-35-37.
[4] Chan-Ki Park1, Min-Woo Ryu2, and Kuk-Hyun Cho, "Survey of MAC Protocols for Vehicular Ad Hoc Networks" Smart Computing Review, vol. 2, no. 4, August 2012.
[5] Saurabh D. Patil, D.V. Thombare, Vaishali D. Khairnar, "DEMO: Simulation of Realistic Mobility Model and Implementation of 802.11p (DSRC) for Vehicular Networks (VANET)" International Journal of Computer Applications, Volume 43–No.21, April 2012.
[6] Katrin Sjöberg, Elisabeth Uhlemann, and Erik G. Ström, "How Severe is the Hidden Terminal Problem in VANETs when Using CSMA and STDMA?" IEEE

Vehicular Technology Conference (VTC Fall), pp. 1-5, 5-8 Sept. 2011.

[7] John B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", Proceedings of the IEEE (Volume:99 , Issue: 7), pp. 1162 – 1182, July 2011.

[8] Yousefi Saleh, Fathy Mahmood, Benslimane Abderrahim, "Performance of beacon safety message dissemination in Vehicular Ad hoc Networks (VANETs)*" Journal of Zhejiang University SCIENCE A, 2007.

[9] Mohammad Nekoui and Hossein Pishro-Nik, "Reliable Inter-Vehicle Communications for Vehicular Ad Hoc Networks" *www.ecs.umass.edu/~nekoui/VINT-Nekoui-final.pdf*

[10] Prabhakar Ranjan, Kamal Kant Ahirwar, "Comparative Study of VANET and MANETRouting Protocols"*rgconferences.com/proceed/acct11/pdf/053.pdf*.

[11] Der-Jiunn Deng, Hsin-Chin Chen, Han-Chieh Chao, Yueh-Min Huang, "A Collision Alleviation Scheme for IEEE 802.11p VANETs" Wireless Pers Commun.

[12] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (2007) 39–68 39, IOS Press

[13] IEEE Draft Standard for Information Technology Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments, IEEE Std. 802.11, 2012.

[14] IEEE Standard for Information Technology—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Std. 802.11e-2005, Amendment to IEEE Std. 802.11.