IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. V (Nov.-Dec. 2016), PP 87-91
www.iosrjournals.org

Smart Decongestion Model Based Upon QoS and Multicasting Mechanisms for Vehicular Networks

Gurjot Kaur[1], Samanpreet Singh[2] , Bharti Chhabra[3]
[1]*(Chandigarh engineering College Landran, India)*
[2]*(Chandigarh engineering College Landran, India)*
[3]*(Chandigarh engineering College Landran, India)*

Abstract: *The availability deals with network services for all nodes comprises of bandwidth and connectivity. In order to encounter the availability issues, prevention and detection technique using vehicular network traffic decongestion scheme has been introduced. The scheme is focusing on retaining the maximum availability by exchanging the messages smartly and with less effort and minimized volume between vehicles to vehicle and vehicle to RSUs. The major objective of this research work is to maximize the resource availability by smartly analyzing and forwarding the data. The load balancing mechanism has been utilized for the reduction of the scenarios with overloaded data volumes, specifically around the squares. The proposed model has been designed to achieve the goal to maximize the network resource availability and the resource utilization by using the combination of the quality of service for flow prioritization and isolation along with the load balancing mechanism for sharing the data among the multiple paths. The proposed model has shown the results with no data drop between the vehicle and RSU communications during the heavy load scenarios.*

Keywords: *Load balancing, Decongestion, Congestion aware data propagation, Centralized data propagation management.*

I. Introduction

In transportation system, vehicular networks are developed to enhance the efficiency, safety and security, and enable new mobile functions, services and applications for the passengers [2]. For the longer term intelligent road traffic management systems the transport or automobile network is become an important part. A future intelligent road traffic management system has many key merits contrast to the present traffic management systems. The main merits are reform or fix information primarily based real time traffic signal systems, reduced transport emissions and improved security and safety of transport traffic. Researchers in traffic management systems and communication engineering engaged for quite a decade to build appropriate vehicular ad hoc networks (VANETs) for traffic security systems including driver and passenger safety.

The self-organizing autonomous system known as VANETs. During a timely manner the vehicular ad hoc network distribute traffic, emergency data and information to automobile or vehicle [3]. VANETs have many merits over the standard wireless networks like Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) and Wi-MAX networks. Main merits are self-organization, and lower native information dissemination time, lowprice of implementation and low price of maintenance. In this analysis or research, the prankster object propagating wrong information into the VANET cluster which is the main issue because prankster object cause of an accident, traffic congestion and harmful or terrorist activities. Vehicles stop the addressed security threat by act with one another. In this situation or scenario no road side units (RSU) are used during, hence, this methodology will be applicable any place while not regard to the road side unit (RSU) network. Offender or selfish driver launches prankster attack as a result of he needs to create his manner clear to succeed in his destination with none hurdle. Offender or terrorist might use Prankster attack to forma traffic congestion to cause the utmost range of causalities. This is depends on an offender or attacker what he want to do harmful with vehicular network.

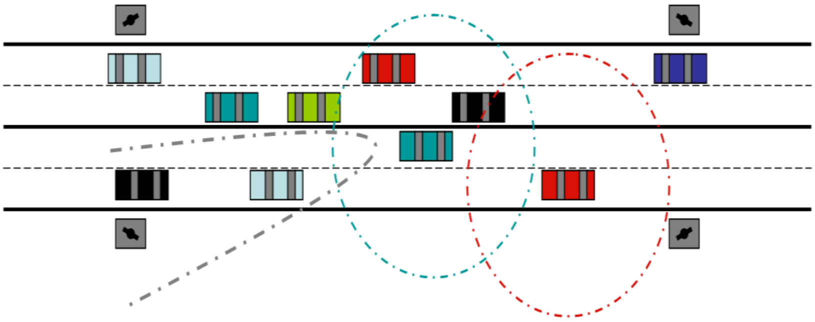

Figure 1.1: A simple VANET in action [4]

II. Literature Review

Ghaleb F. et.al. has proposed the security and privacy enhancement in VANETs using mobility pattern. Through this paper the authors have assessed about mobility pattern based misbehavior detection approach in VANETs. The author in this paper starts by classifying the two attackers as outsider and insider An intruder trying to intercept comes under the former type of attack while undesirable or unauthorized actions performed by a trusted node comes under the latter. a) Physical movement and b) information security perspectives are the metrics used by the author to detect misbehavior in VANETs. Anonymous Location-Aided Routing for MANET (ALARM) is implemented in this paper for vehicular network. This paper includes algorithms by which the misbehavior can be detected **Sharma G.** et.al has proposed the mechanism for security analysis of vehicular ad hoc network. The crux of this paper is about problems and challenges faced in VANETs and devising solutions to overcome these. In accordance to this paper each vehicle comprises of an OBU(On Board Unit).which connects vehicles with RSU via DSRC. and the other device is TPD(Tamper Proof Device),which store the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. DOS, Fabrication Attack, Alteration Attack are some of the attacks mentioned with Selfish Driver behind wheels, Pranksters etc. being the possible attackers. **Seuwou. P** et.al. has proposed the effective security as an ill-defined problem in vehicular ad hoc networks. The author defined VANET as a mobile network created with the help of using moving cars as nodes. He emphasized the use of V2V and V2I communications for communications. He classified attacks into a) Physical b) Logical. Tamper proof device being the main cause of the former one and virus being that of the latter one.

III. Experimental Design

The path evaluation and load balancing mechanism with traffic aggregation formula doesn't touch upon position deviation generated by the traffic management and decongestion unit (TMDU). The load balancing mechanism is responsible for the management of the traffic across the vehicular network by analyzing the times with the data congestion and decongesting the data by the means of multiple links sharing for the data transmission across the vehicular networks. The vehicular networks are the networks consisted of the mobile nodes, which requires the continuous routing information updates and regular load balancing across the shuffling path when going peer-to-peer across the network nodes. The following algorithm describes the application of the load balancing mechanism across the vehicular network.

Algorithm 1: Load balancing and decongestion mechanism (LBDM)

```
1. The RSU begins the operations
2. The vehicular nodes begins the operations
3. Establish the inter-connections between the vehicular nodes and the RSU nodes
4. Start the congestion occurrence monitoring mechanism
5. When the RSU receives the data
    i. It shortlist the target nodes for the received data
    ii. Find the best path towards the destinations
    iii. Forward the data towards the target nodes
6. When there is no congestion
    i. Find the best path towards the target node or groups of target nodes
    ii. Propagate the data across the best path
7. When the congestion is detected across the VANET cluster
    i. Find the best path towards the groups of target codes
    ii. Find the best alternative path towards the groups of target codes
    iii. Select both of the paths
    iv. Estimate the bandwidth of the best path (BW1)
    v. Estimate the bandwidth of the best alternative path (BW2)
    vi. Prepare the data ratio
        1. Total Data (T) = estimated total volume of data
        2. Available bandwidth available (A) = BW1 + BW2
        3. Prepare the ratio for first link
            a. R1 = (BW1/A)*100
        4. Prepare the ratio for the second link
            a. R2 = 100-R1
8. Forward the data among the target paths
```

IV. Result Analysis

The network load has been evaluated under this section in the two primary performance evaluation phases. The first performance evaluation is based upon the independent analysis of the vehicular nodes in the given vehicular cluster. The overall load value has been recorded at the network cluster data on the RSU, which is responsible for receiving and propagating the data collected from the various vehicular nodes registered with the RSU.

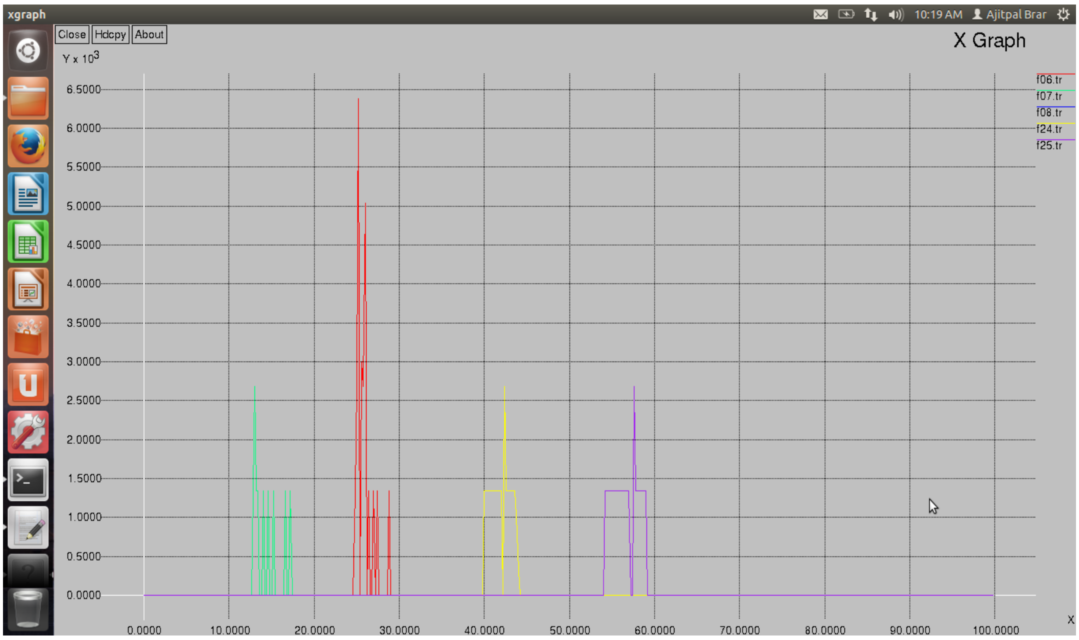

Figure 5.3.1: The load based evaluation from the individual nodes over the first RSU

The figure 5.3.1 shows the load value in the five colors and where each of the color depicts the data sent an individual node. All of the nodes have been programmed to pass the target hurdles over the different times under this scenario, hence this scenario does not show the overlapping data for any of the given node in the scenario. The vehicular nodes are transmitted to propagate the higher volumes of data, when they are either in the critical, moderate or normal phases of the hurdle or hazard update to the other vehicle. The vehicle travelling at the higher speed is intended to pass the hurdle faster, whereas the slower one will remain for the longer in the hurdle zone. The yellow color is shown for the node, which has spent the least time in the RSU reach, whereas the node with the red colored signal has spent the longest time in the RSU reach.

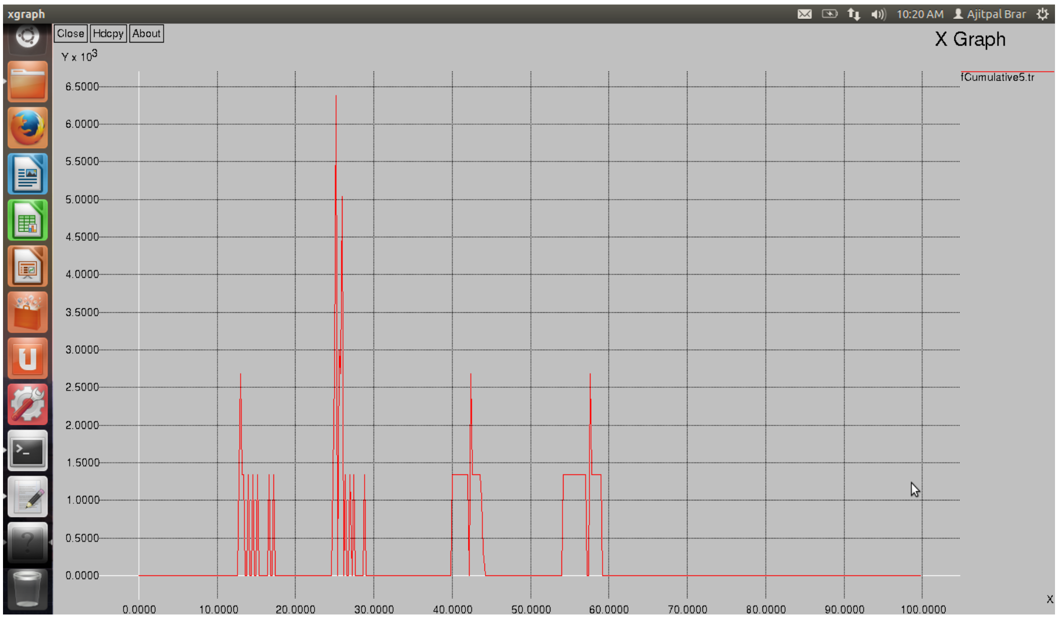

Figure 5.3.2: The load based evaluation in the aggregated mode over first RSU

The figure 5.3.2 shows the cumulative results obtained from all of the nodes over the RSU. The impact of the data over the RSU is clearly similar to the independent analysis. The load ratio rises with the number of the nodes. The node is critical phase propagates the higher volumes of the data, whereas it decreases the data volume significantly in the moderate or normal modes. The data volume has been remained significantly optimized and reduced during this update mechanism. The smarter selection of the data volume according to the target nodes is signified by the traffic flow isolation and load balancing mechanism in the proposed model. The proposed model can be declared as the good performed from this analysis as there is no data drop reported from the communication between the node and the RSU as per shown by the above graphs.

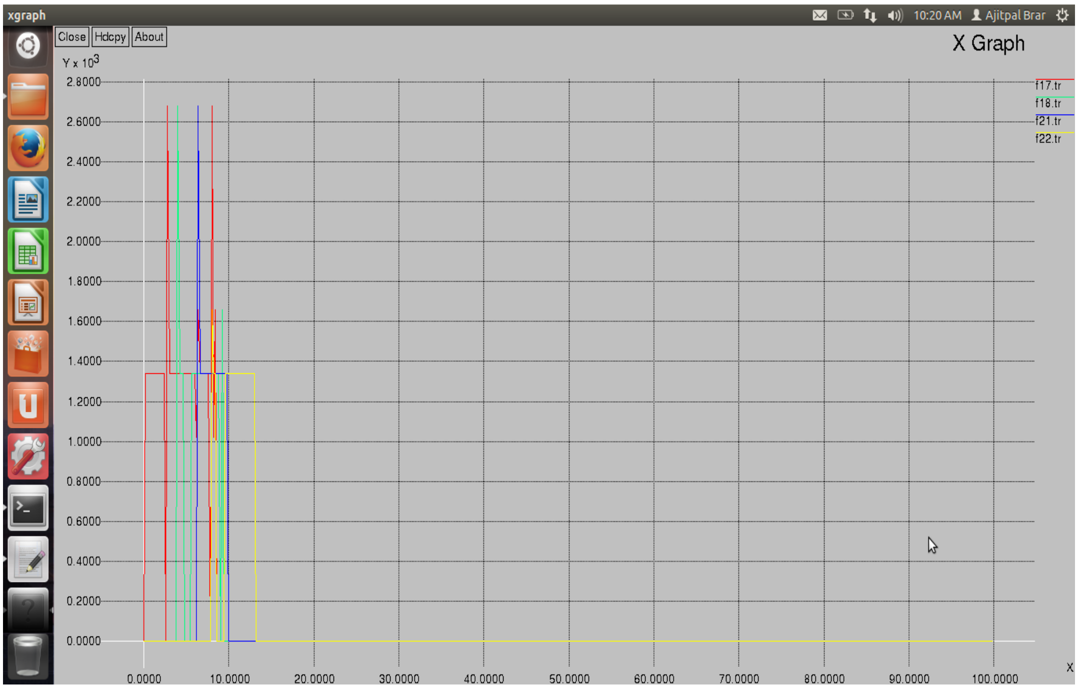

Figure 5.3.3: The load based evaluation from the individual nodes over the second RSU

Another group of the nodes has been evaluated in the given VANET cluster for the performance evaluation of the load balancing method under the situation, when the nodes are transmitting the data together at one point of time. The proposed model has been tested with the four nodes in this scenario. All of the nodes are transmitting the data over the approximately same time. The peaks of the different colors have been recorded within very low distance, which is also shown the collective figure (Figure 5.3.4).

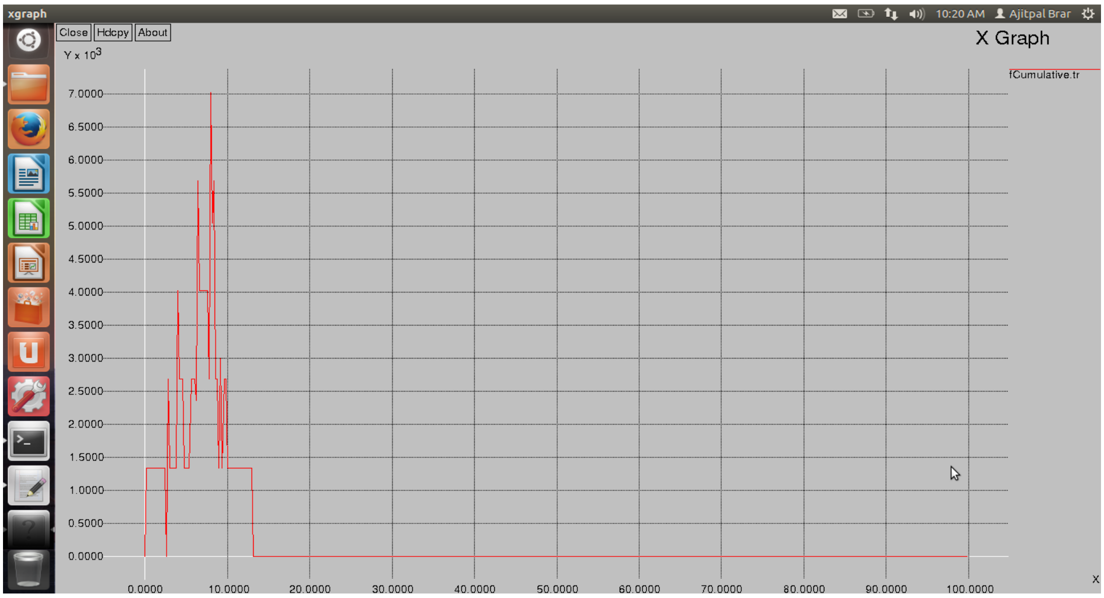

Figure 5.3.4: The load based evaluation in the aggregated mode over first RSU

The above figure (Figure 5.3.4) shows the collective data received over the target RSU from the four vehicles as per defined in the figure 5.3.3. The rising graph shows the aggregated requests received by the RSU from the multiple vehicles over the same time. The rising trend is clearly visible and shows the higher data received ratio than the individual nodes. Even after the recording of the rising trends, the proposed model hasn't dropped any of the data during the update transmission, which has been achieved due to the incorporation of the flow prioritization and the load balancing model.

V. Conclusion

The proposed model has been empowered for the high availability based connectivity with the area of RSU nodes by enabling the node-to-node and node-to-RSU model. The vehicular node connects itself with the neighboring node while the RSU is not in range with the assurance of the vehicular node it is being connected with some of the RSU. The proposed model has been evaluated on the basis of various performance parameters. The proposed model has performed better than the existing models. The experimental results have proved its efficiency which is obtained by load balancing mechanism called LBDM.

References

[1]. Chen, Lu, Hongbo Tang, and Junfei Wang. "Analysis of VANET security based on routing protocol information." In *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, pp. 134-138. IEEE, 2013.

[2]. Dias, João A., João N. Isento, Vasco NGJ Soares, Farid Farahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 51-55. IEEE, 2011.

[3]. Ghaleb, Fuad A., M. A. Razzaque, and Ismail Fauzi Isnin. "Security and privacy enhancement in vanets using mobility pattern." In *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, pp. 184-189. IEEE, 2013.

[4]. Hung, Chia-Chen, Hope Chan, and EH-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks." In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 2200-2205. IEEE, 2008.

[5]. Javed, Muhammad A., and Jamil Y. Khan. "A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." In*Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1-6. IEEE, 2011.

[6]. Khabazian, Mehdi, and M. K. Mehmet Ali. "A performance modeling of vehicular ad hoc networks (VANETs)." In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 4177-4182. IEEE, 2007.

[7]. Moser, Steffen, Simon Eckert, and Frank Slomka. "An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 36-41. IEEE, 2012.

[8]. Qian, Yi, Kejie Lu, and Nader Moayeri. "Performance evaluation of a secure MAC protocol for vehicular networks." In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-6. IEEE, 2008.

[9]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pp. 393-398. IEEE, 2010.

[10]. Sepulcre, Miguel, Javier Gozalvez, Onur Altintas, and Haris Kremo. "Integration of congestion and awareness control in vehicular networks." *Ad Hoc Networks* 37 (2016): 29-43.

[11]. Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." In *Road Transport Information and Control (RTIC 2012), IET and ITS Conference on*, pp. 1-6. IET, 2012.

[12]. Sumra, Irshad Ahmed, Halabi Hasbullah, and J-L. A. Manan. "VANET security research and development ecosystem." In *National Postgraduate Conference (NPC), 2011*, pp. 1-4. IEEE, 2011.

[13]. Sumra, Irshad Ahmed, Halabi Hasbullah, J. A. Manan, Mohsan Iftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pp. 708-714. IEEE, 2011.