**Performance Analysis of Vehicular Ad Hoc Network (VANET) Considering Different Scenarios of a City**

Md. Mamunur Rashid  
Assistant Professor,  
American International University-Bangladesh (AIUB)  

Prithwiraj Datta  
American International University-Bangladesh (AIUB)

**ABSTRACT**

Vehicular Ad Hoc Network (VANET) is becoming a popular technology day by day in which moving vehicles are able to exchange various information (traffic engineering, traffic management, provides emergency information to avoid accidents and other user applications) among them. VANETs are similar to Mobile Ad hoc Networks (MANETs) but with different characteristics like, movement at high speeds, mobility, sufficient storage and processing power, unpredictable node density and difficult communication environment with short link lifetime etc. So for testing of any protocol for VANET, realistic environment is needed. In this Paper, we have created a realistic network environment with several vehicles and measured various performances like Delay, Throughput, Packet Loss, Load etc. in case of sending images throughout the network.

**General Terms**  
Wireless Communication, Vehicular Adhoc Network, Speed.

**Keywords**  
VANET, OPNET, MANET, Mobility.

1. **INTRODUCTION**

Vehicular Ad-hoc Network (VANET) is a form of Mobile Ad Hoc Network. It is a combination of vehicle to vehicle and vehicle to infrastructure communications. Communication is done among vehicles themselves and also among vehicles and nearby fixed roadside equipments which are generally called Road Side Unit or simply RSU. RSUs are interconnected to each other by a transmission link. Vehicles can communicate with themselves through RSU. A wireless LAN server is needed to be set up if the applications like email transfer, video conferencing, image browsing etc are to be enjoyed. [1]

A. **Historical Background**

The primary motive of the vehicular communication was to provide safety on the road. Due to brake failure or trap present on the road vehicles crash is very normal. To remove unawareness of the drivers, an application namely cooperative collision warning was introduced for the first time of vehicular communication. Many more safety applications were appeared and the applications for effective transportation were emerged as well. But they were not well enough to perform efficiently using only vehicle to vehicle communication. RSU was needed to solve this problem. Then in addition to road safety, new application proposal is done, such as ETC, car to home communications, travel and tourism information distribution, multimedia, game applications etc. However, these applications require reliable communication equipments having ability to gain high data rates and fixed connectivity between the transmitter and the receiver under high mobility conditions and different situations. [2]

B. **Recent Research**

Many projects have been commenced recent years. Daimler Chrysler AG, BMW AG, Volkswagen AG, Fraunhofer Institute for Open Communication Systems, NEC Deutschland GmbH and Siemens AG founded a German research project named Network On Wheels (NOW) in 2004, maintaining an IEEE 802.11 standard for wireless access. Solutions of communication protocols and data security for car-to-car communications are the primary objectives of the project are the solutions of communication protocols and data security. FleetNet was another program which ran from 2000-2003. MANET protocols standardization efforts dominated the research. [3]. A paper was published on “Security attacks and solutions for vehicular ad hoc networks” by J.T. Isaac, S. Zeadally, and J.S. Camara in 2010. Some of the major security attacks were explained in the paper that have been reported on VANETs before and in 2010. For the prevention of those security attacks and vulnerabilities corresponding security solutions have also been proposed. Anonymity, key management, privacy, reputation, and location are the primary security areas got focused by the authors. [4]

2. **VANET ARCHITECTURE & APPLICATION**

In VANET technology, moving vehicles are used as nodes and the network structure is mobile in nature. Though it is a subclass of mobile ad hoc network (MANET), the characteristics and features of VANET are different. [5]

2.1 **System Architecture**

VANET system can be partitioned into three domains according to the IEEE 1471-2000 [6,7] and ISO/IEC 42010 [8] architecture standard guideline.

- **Mobile Domain**
- **Infrastructure Domain**
- **Generic Domain**
- **Mobile Domain**

Mobile domain is also divided into two parts.

1. Vehicle domain consisting of all kind of vehicles
2. Mobile device consisting of all kind of personal navigation devices.

- **Infrastructure Domain**

The infrastructure domain is also divided into two parts.

1. Roadside infrastructure domain consisting of roadside unit entities like traffic lights.
2. Central infrastructure domain consisting of infrastructure management centers and vehicle management centers. [9]
   • Communication Architecture

Communication architecture is a very important issue in VANETs architecture. This can be categorized into four types. [10]
   1. In vehicle communications
   2. Vehicle to vehicle communications
   3. Vehicle to road infrastructure
   4. Vehicle to broadband cloud

1. In vehicle communications
Using this communication system, vehicle’s performance specially driver’s fatigue and drowsiness can be measured.

2. Vehicle to vehicle communications
Drivers can share information and warning message by using this communication system.

3. Vehicle to road infrastructure
Drivers can get real time traffic update or weather update using this V2I communication system.

4. Vehicle to broadband cloud
Using this communication system vehicle can communicate via wireless broadband. This type of communication can be useful for active assistance and vehicle tracking

Drivers can get real time traffic update or weather update using this V2I communication system.

2.2 VANET Applications
To satisfy the various requirements associated with VANETs and their applications is the most important challenge the researchers are facing now. VANETs are divided into many groups according to many categories and it was discussed above. But based on their applications they can be divided into three major groups: [11]
   • Safety
   • Infotainment & Assistance
   • Efficiency & Management
   • Safety

In this kind of applications VANETs will be used for avoiding collision situation that most frequently occur between vehicles and other objects such as animals, trees and pedestrians. Besides, this uses a V2V scheme relying on real time information. The shared information by vehicles on the road and roadside units is used to predict a dangerous situation. Intersection collision warning, lane change assistance, overtaking vehicle warning etc. are the most popular examples of safety applications. Beacon messages, a single-hop position based or fast-bidirectional communication regime are used in this type of applications, and their latency cannot exceed 100 milliseconds, whereas the packet delivery ratio cannot be lower than 95 %. [11] Besides, they utilize normal messages and bidirectional communication.

   • Efficiency & Management
Traffic management and efficiency are included in this application. Traffic bottlenecks and fuel consumption amongst others including environmental issues are included in this application. Improving the vehicle traffic flow, traffic coordination and traffic assistance are the main focus of this application. Besides, this can provide updated local information, maps and information of relevance bounded in space and time. Like the Infotainment and assistance applications their latency cannot be higher than 400 milliseconds and the packet delivery ratio cannot be lower than 95 % and they also can utilize normal messages and bidirectional communication. [11]

3. ROUTING PROTOCOLS
With the passage of time network structure has changed. Now- a- days for monitoring an environment wireless networks are planned. Most of the research and development focus has been shifted to wireless network. Limitation of wireless network is the identification of nodes because wireless networks are formed by important number of nodes, manual specification of unique identifiers becomes impossible. [12]

3.1 Introduction to MANET
A Mobile Ad hoc Network is a wireless network which is a collection of mobile nodes that are dynamically and arbitrarily arranged in such a way that the inter connection between the nodes is capable of changing on a continual basis. The initial goal of this network is correct and efficient establishment between a pair of nodes so that the message can be delivered in time. Ad Hoc Network is used for ease of deployment, speed of deployment and to decrease dependence on infrastructure. [13]

   • Classification of MANET

3.1.1 Reactive Routing Protocol
These protocols are also called on demand routing protocols because they do not maintain routing activity between the network nodes if there is no communication or connection. If a node wants to send packet to another node, then this protocols create the route and establish the connection for the purpose of transmitting and receiving the packets. Route is maintained until the destination becomes unreachable. [14]

3.1.2 Proactive Routing Protocol
These protocols are known as table driven routing protocols. Each node contains one or more tables which contain routing information to every other node in the network. Tables should be consistent and Up-to-date which reflects the view of the network. Routes information is kept in the routing tables and is periodically changed as the network topology changes. These routing protocols keep different number of tables. The proactive protocols are not useful for larger networks because they need to maintain node entries for each and every node in the routing table of every node which cause more consumption of bandwidth. [14]

3.1.3 Hybrid Routing Protocol
Hybrid protocols are the combination of reactive and
proactive protocols. Hybrid protocols are Zone Routing Protocol and Temporarily Ordered Routing Algorithm. It reduces the control overhead of Proactive routing protocols. Whenever nodes do not find any route to the destination they start to behave like reactive routing protocols and start route discovery. [15]

4. USED NODES
Different types of nodes are used. Descriptions of these nodes are given below.

4.1 Mobile Node
The wlan_wkstn_adv node model represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying Wlan connection at 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps. This workstation requires a fixed amount of time to route each packet, as determined by the "IP Forwarding Rate" attribute of the node. [16]

4.2 Mobile Server
The wlan_Server model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying IEEE 802.11 connection at 1 Mbps or 2 Mbps. The operational speed is determined by the connected link's data rate. [16]

4.3 Profile Definition
A profile describes user activity over a period of time. A profile consists of many different applications. For example, a "Human Resources" user profile may contain "Email", "Web" and "Database". One can specify various loading characteristics for the different applications on this profile. Each application is described in detail within the application configuration object. [16]

4.3.1 Application Definition
Application Configuration node can be used for the following specifications.

4.3.1.1 ACE Tier Information
Specifies the different tier names used in the network model. This attribute will be automatically populated when the model is created using the "Network->Import Topology->Create from ACE..." option. The tier name and the corresponding ports at which the tier listens to incoming traffic is cross-referenced by different nodes in the network.

4.3.2 Application Specification
Specifies applications using available application types. You can specify a name and the corresponding description in the process of creating new applications. For example, "Web browsing (Heavy HTTP 1.1)" indicates a web application performing heavy browsing using HTTP 1.1. The specified application name will be used while creating user profiles on the "Profile Configuration" object. [16]

5. SIMULATION SCENARIOS & RESULTS
In this section the simulation scenarios and parameters have been discussed. In order to investigate the performances of the networks by creating different traffic scenarios, the OPNET Modeler simulation tool was used [16]. The network consists of a Mobile Server and some Mobile Nodes. In the mobile server, image application was selected so that the Mobile nodes could send images among them. For the comparison of different network parameters, four scenarios (Fig 1-4) were created with different amount of Loads and sources. The common network parameters are shown in the Table 1.

Fig 1: Scenario 1
Fig 2: Scenario 2
Fig 3: Scenario 3
5.1 Simulation Parameters

5.1.1 Traffic Sent & Received
Traffic Sent (packets/sec): Average number of packets per second submitted to the transport layer by the video application in this node.

Traffic Received (packets/sec): Average number of packets per second forwarded to the email application by the transport layer in this node.

5.1.2 Delay
Time required for the messages to be passed among nodes in a network. It actually refers the time taken of a packet of data to go from one node to another. It is generally expressed in seconds. [17] The expected end-to-end packet delay is determined by taking the average of all successfully transmitted data packets. [18]

5.1.3 Load
It signifies the total load submitted to wireless LAN layers by all higher layers in all WLAN nodes. [19]

5.1.4 Throughput
Throughput refers to the average number of successfully delivered data packets on a communication network or network node. Throughput indicates the total number of packet reception at the destination out of total number of packet transmission. It is calculated in bytes/sec or data packets per second.

Throughputs (bytes/sec) = Total number of received packets at destination × packet size /Total simulation time. [20]

5.2 Results
The average traffic sent(packets/sec) for the application of image browsing from a server and the average traffic received (packets/sec) by the vehicular nodes are shown altogether in the Fig. 1. The simulation was done for 600 seconds or 10 minutes. The percentage of data packet loss during the transmission and reception for Scenario1 and Scenario2 has been compared here.

From the graph, it can be seen that up to 100 seconds, no data packet was sent. Because, at first all the nodes of a network got configured and they took a little bit of time to start communicating themselves. In the case of Scenario 1, at 400 seconds approximately 15 packets are sent and approximately 11 packets are received. So, packet loss is approximately \( \frac{4}{15} \times 100 = 26.66\% \). On the other hand, at 400 seconds, about 17 packets are sent and about 12 packets are received in Scenario 2. So, packet loss is \( \frac{5}{17} \times 100 = 29.4\% \). The number of RSU in the 2nd Scenario was reduced to 4 but the number of vehicles remains the same in comparison with Scenario 1. That’s why the loss was increased.

In this case, Scenario 1 and Scenario 3 have been compared. In Scenario 3, the number of vehicles has been increased to 30 but the number of RSU remained fixed compared with Scenario 1. From Fig. 6, it was observed that at 400 seconds, approximately 27 packets are sent and approximately 19 packets are received. So, loss is \( \frac{8}{27} \times 100 = 29.63\% \). So, it is obvious that data loss is increased with the increase of
number of vehicles.

Though the values were different for different cases but still the delay was much low and that signified a satisfactory performance of the network.

![Fig 7: Traffic Sent & Received (Scenario 1 & Scenario 4)](image)

Scenario 1 and Scenario 4 have been compared here. The number of vehicles was reduced to 8 in the Scenario 4 but the number of RSU remained the same. It was seen from Fig. 7 that at 400 seconds, the average number of packets sent by the wireless LAN server is 9 and the average number of data packets received by the vehicular nodes is 7. So, the loss is \( \frac{8}{27} \times 100 = 22.22\% \). Loss has been decreased with the decrease number of vehicles.

So, from the above discussion of these three graphs we can see that the packet loss ranges from 20 to 30 percent. The quality of application such as image or video streaming depends on user’s demand. If a user is satisfied with low quality image, then large amount of data loss would not be a big problem but if a user requires a high-quality image then data loss must be very low. So, it is difficult to comment about the acceptable range of data loss. However, as the data loss is not so much in our designed network, the application for sending images would be easily implemented.

![Fig 8: Wireless LAN Delay](image)

Delay represents the time required for data transmission from one node to another. In the above graph, average delay for data transmission is measured in seconds. At the earlier stage, delay is very low. There was no transmission of data at that time. A network can’t start working immediately. It requires a little bit of time to be active. That’s why it is very natural for delay to be very low initially.

Vehicle number affects delay. From Fig. 8, it can be clearly seen that delay was more in Scenario 3 and less in Scenario 4. Vehicle was more and less in Scenario 3 and Scenario 4 respectively. Delay was same for Scenario 1 & Scenario 2.

![Fig 9: Throughput](image)

Throughput refers to the average number of successful delivery of data to the destination. It is an estimation of total number of packet reception at the destination out of total number of packet transmission from the source. As usual, at the beginning, the throughput was the least and after certain time it started to increase. From Fig. 9, throughput was almost same for Scenario 2 and Scenario 4 and it was the least for both scenarios compared with the Scenario 1 and Scenario 3. In Scenario 2, there were only 4 RSUs and in Scenario 4 there are only 8 vehicles. As the RSU number and vehicle number were less in Scenario 2 and Scenario 4 respectively, the throughput was less but that did not mean the network performance to be bad for both scenarios. The two curves never went down and it justified that the network performance was good. In the 1st scenario, the vehicle number is 17 and RSU number is 16. As vehicle & RSU number was greater than Scenario 2 and Scenario 4 respectively, the value of throughput was increased. Scenario 3 had 30 vehicles and 16 RSUs. That’s why the value was maximum. Scenario 3 shows the best performance in terms of throughput as the slope of the curve was greater than others.

![Fig 10: Wireless LAN Load](image)

Load denotes the total load applied to WLAN layers by all higher layers in all WLAN nodes. In the above figure, average load is shown. Initially, as the network was busy to be configured, the load was less. After certain time, the load increased gradually as the pressure on the network increases. As the load depends on the number of vehicles, the expected result was found. Actually, load showed the same behavior as...
delay. Load is maximum for Scenario 3 as there were 30 vehicles and minimum for Scenario 4 as there were only 8 vehicles. The load remained the same for Scenario 2 & Scenario 4 because the number of vehicles was equal in both scenarios.

6. CONCLUSION

In our thesis, we wanted to design and evaluate the performance of a network which could provide a safety application on the road. Some parameters were taken for the analysis. The results were evaluated for the overall performance of the network to fulfill our goal without having any problem. Though it is difficult to say whether the design would be the best or when it would not perform the task just evaluating the network performance for a single model, it can be predicted or commented about a network’s performance to be in a good range having some basic idea about networking. The model designed is only a demo considering a very small area of 3 x 3 kilometers and it gives just a basic idea about the design, operation and the performance for the application wanted. The default design elements used i.e., RSUs, WLAN server in the simulator have some predefined characteristics like speed, bandwidth etc. So, it would be unrealistic to assume the designed model in OPNET could be implemented exactly in real life scenario. In order to implement the design in practical scenario, many things need to be considered. First the decision would need to take about the area and the approximate availability of the number of vehicles in that area. For that scenario, the number of RSUs, the capability of server etc. would need to be considered then. There are many effective routing protocols and algorithms such as CMV (cognitive MAC for VANET) and GyTAR (greedy traffic-aware routing) [21] which can be used in these scenarios for better performance.

7. REFERENCES


