Basic Structural Change in Vehicular Adhoc Networks

Shahid H Abbassi[1], I.M. Qureshi[1], Obaidullah Khalid[2], Hameer Abbasi[2]
Department of Electrical Engineering
Air University
Islamabad, Pakistan
[2]Department of Electrical Engineering , MCS
National University of Science & Technology
Rawalpindi, Pakistan
{shahid.abbassi, imqureshi}@mail.au.edu.pk, okhalid@mcs.edu.pk, hameerabbasi@yahoo.com

ABSTRACT: *With the increase in population, vehicle traffic has also increased on roads; which have caused an increase in accidents, due to which many people have lost their lives and millions are injured annually. Hence, a foolproof and secure Vehicular Adhoc Network (VANET) structure is required to reduce the number of accidents considerably. In this paper, a VANET structure has been proposed for highways and urban environments. In the Highway model, separate Road Side Units have been provided for the traffic on each side. In this way group formation for localized traffic will be easy on highways. Simulation results show that by using proposed model, average Throughput and End-to- End delay are improved considerably while packet loss has also been reduced.*

Keywords: MANET, VANET, RSU, Throughput, AODV

Received: 14 May 2013, Revised 19 June 2013, Accepted 21 June 2013

1. Introduction

Vehicular Adhoc Networks (VANETs) are a special form of Mobile Adhoc Networks (MANETs), which deals with the vehicle to vehicle communication and vehicle to infrastructure communication. Main differences between VANETs and MANETs are a high mobility, dynamic topology, and intermittent connectivity. Hence, special kinds of measures are considered while designing the structure and standards for VANETs. VANET hardware has bulk of power available due to frequent charging of batteries in the vehicles as opposed to normal MANETs where the power is limited.

A special frequency band of 5.850-5.925 GHz has been allocated for the purpose of vehicular communication in USA. Similar bands have also been allocated in Japan and Europe. Due to high mobility normal IEEE-802.11 is not suitable for VANET

applications so IEEE is developing a special IEEE-802.11p standard for VANETs [1].

Besides IEEE several consortiums are working on the development of VANETs. These include Car-to-Car consortium and Network on Wheels group (NOW) in Europe; Berkley PATH in USA; and Fleetnet Projects in Germany [1].

VANETs are being designed specially to avoid loss of lives due to road accidents of millions of people around the world. VANETs are also intended to provide toll services, location based services, and infotainment. Main applications of VANETs are:

- Collision Avoidance
- Cooperative Driving
- Traffic Optimization
- Payment Services
- Location Based Services
- Entertainment Applications [2]

Due to a different nature of VANETs as compared to ordinary MANETs; different routing protocols are being considered. These include Reactive protocols like Dynamic Source Routing (DSR), Adhoc on Demand Distance Vector (AODV) and Proactive protocols like Destination Sequenced Distance Vector (DSDV), Wireless Routing Temporally-Ordered Routing Algorithm, and Lightweight Mobile Routing protocols [3].

The nature of traffic is different on highways as compared to urban environments; hence a concrete structure is required to address the issues of both types of road networks. Furthermore there are several issues to be dealt while designing the structure and standards for VANET and categorization of messages is also needed to save the bulk overhead due to security in message size.

This paper highlights the issues arising in VANET to be addressed on top priority and proposes a structure highlighting both highway and urban environments, and categorizes the messages to reduce the size of packets.

2. Issues in VANET's

VANETs face several issues which need to be addressed while designing the standards and a concrete structure for VANETs [4]. These issues are described as follows:

2.1 Vehicle Density

In cities the vehicle density on the road network is quite high, so the vehicles have to move with slower speeds whereas on highways vehicle density is comparatively low, so the vehicles can move with a higher speed. This issue needs to be addressed differently on highways and in cities.

2.2 High Mobility

As compared to normal nodes in MANETs, vehicles move with a higher speed hence the adhoc networks formed by vehicles need to remain intact for smaller duration of time as opposed to adhoc networks formed by normal nodes in MANETs.

2.3 Intermittent Connectivity

Due to high mobility, the probability of connection between any two vehicles moving in opposite directions in an adhoc network is smaller

2.4 Definition of Services

Vehicular infrastructure needs different type of services as compared to MANETs, like toll collection, location based services including locations of fuel stations, restaurants, workshops, and safety messages like safe distance between the vehicles, accident warnings, road closure warnings, and road congestion warnings.

2.5 Identification of Service Recipients

Since many services involve online payments, the actual service recipient is needed to be identified as the service is provided

to the party who actually has paid for the said service.

2.6 Incremental Deployment of VANET
Lot of research work is being carried out around the globe on VANETs, so new ideas are needed to be implemented in VANET network designs to improve the services hence the deployment of VANETs is incremental. Therefore, the network designs and infrastructure shall be such that new ideas can be incorporated easily.

2.7 Open Approach to VANET Architecture
Till now different approaches have been found on VANET around the globe which may cause disharmony in the networks. Hence a uniform approach is needed for VANET designs.

2.8 Unreliable Components Generate Unreliable Data
Most of the people are sincere and trustworthy, but there are a few people which may not be trusted. These people can generate unreliable data which may harm the network or even may cause serious accidents. So the network design should be rigid and secure to face these challenges.

2.9 Privacy
It is deeply desired that identity and personal information of the person using the VANET network shall not be disclosed to anyone except the controlling authority so that no one may misuse the data or harm the individual by knowing the location of the person.

2.10 Authentication
To use a service or even generating the safety messages, authentication of the person generating the message is needed as false safety messages may cause accidents or congestion.

2.11 Non Repudiation
Someone may deny the sending or receipt of any message, especially the warnings and instruction messages by controlling authorities, for example speed control warnings. This issue needs to be given top priority while designing the standards for VANETs.

2.12 Reliability, Integrity and Scalability
The communication channels need to be reliable and scalable and message integrity is to be given top priority

2.13 Real Time Guarantees
Messages, especially safety messages and road warnings, require the delivery of messages in real-time, so that traffic hazards can be avoided.

3. Message Categorization

Categorization of messages is important in the sense that these may be treated differently by the channel according to their priority, authentication requirement, or privacy requirement. This categorization may save the bulk overhead in the size of messages, improve the speed and decrease the occupancy of channel by one message for long time. These messages are categorized as under: [5]

3.1 Emergency Message
Examples are accident information, congestion information, bridge broken, and train crossing etc. This type of message needs authentication but does not need privacy.

3.2 Safety Message
Examples are inter-vehicle distance, speed, intersection collision avoidance, and location information. This type of message needs authentication but does not need privacy.

3.3 GPS Message
This type of message mostly provides road map with reference to location of the vehicle. This type of message needs

authentication but does not need privacy.

3.4 Probe Message
This is the periodic message for keep-alive between the road side unit and the vehicle. This type of message needs neither authentication nor privacy.

3.5 Traveler Information
Examples are signal status, road signs, school ahead, hospital ahead, and service are ahead etc. This type of message needs authentication but does not need privacy.

3.6 Location Based Service
Examples are toll collection, and online payments etc. This type of message needs both authentication and privacy.

3.7 Informative
These are the messages involving ordinary net-surfing. This type of message needs neither authentication nor privacy.

3.8 E-mails
E-mails usually need both authentication and privacy.

4. Proposed VANET Structure

Earlier research on VANETs has not proposed any structure which may cater to the needs of both urban (city) and Highway/ Motorway environments, or the different problems related to both. We propose a VANET structure as depicted in Figure 3. The proposed structure includes the LCA (Legal Certification Authority) which is overall controlling authority of the country's VANET communication. LCA has sub-offices RCAs (Regional Certification Authorities) for certification in different regions to reduce the burden on one office. These issue certificates to RSUs (Road Side Units), SPs (Service Providers), and the vehicles belonging to individual regions.

The structure also includes the VCA (Verification and Controlling Authority) having sub-offices for different regions. VCAs are responsible for the verification of certificates in the individual regions. In the case certificate is found to be illegal; VCAs have the authority to shut off the communication of the concerned vehicle or service provider and add them in the RL (Revocation List). VCAs can also act in case any certificate holder is violating the rules.

The structure includes the SPs which provide the different services like toll collection, internet services, entertainment services (games, audio, video), and location based services like location of restaurant, fuel station, or workshops. Concrete security measures are required for the services involving online payments.

The structure also includes highways/motorways as well as urban (city) environments. On highways, instead of RSUs DRSUs (Directional Road Side Units) have been provided. This helps in group formation on highways. A group of vehicles moving in one direction is easier to manage on highways as the vehicles moving in one direction stay in the group for a longer period of time whereas vehicles moving in opposite direction stay in communication with each other for a shorter duration of time. So the group formation for the vehicles moving in different directions is difficult.

In the urban environment vehicles do not stay longer near to each other so the group formation on the basis of direction is not possible. Instead groups are formed on the basis of categorization of vehicles into buses, taxies, official vehicles, private vehicles registered by one regional office. Hence in cities simple RSUs have been provided. It is also proposed to have RCUs (Road Central Units) instead of RSUs on junctions with more resources than RSUs to cater for the communication needs of vehicles moving on different roads joining the junction. This may help to reduce the infrastructure and installation costs.

5. Simulations and Results

Simulation is performed to check the result of deploying DSRUs. We are working on separate paper to simulate the categorized messages and overall model proposed. The simulation was built using NS2 for highway scenarios. The highway patch is 2 km long, and the traffic is moving in both directions. CASE-1 is the simulation in which RSUs are forwarding the traffic of both

directions whereas CASE-2 is the simulation in which we have to provide DSRUs. To implement DSRUs in NS2 we have provided separate RSUs for each direction. IEEE 802.11 has been used as the MAC layer protocol whereas AODV has been used as the routing protocol. In both cases, the simulation has been performed for 20 mobile nodes (10 in each direction) and 50 nodes (25 in each direction). Average throughput, average end to end delay and packet delivery ratio have been calculated for all cases.

Average Throughput for 20 mobile nodes increased from CASE-1 to CASE-2 by 3.72% while for 50 mobile nodes it.

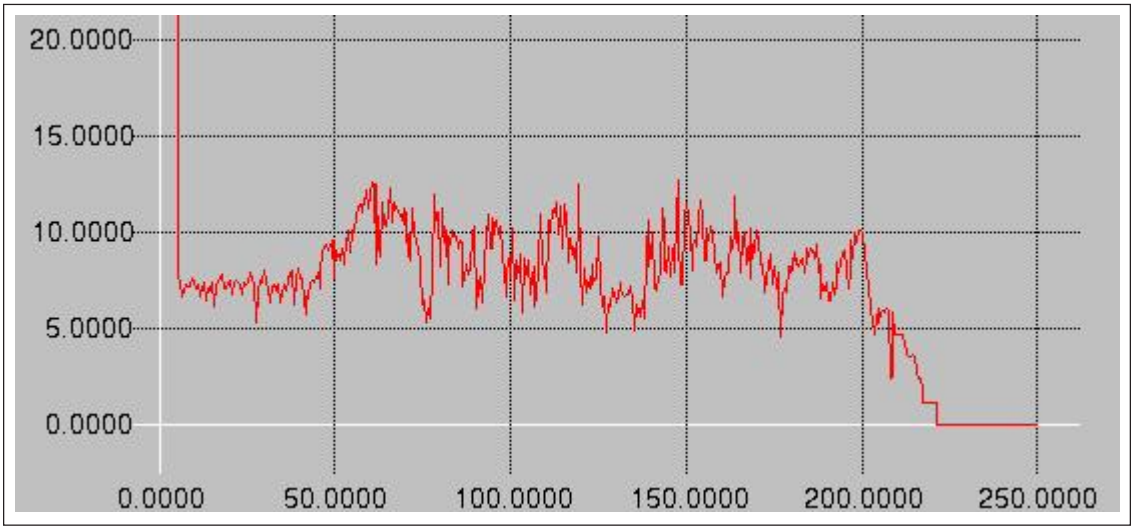

Figure 1. Throughput (RSUs catering both sides' traffic)

Graph for the case that different RSUs dealing with different sides of traffic consisting of 25 mobile nodes on each side is given in figure 2.

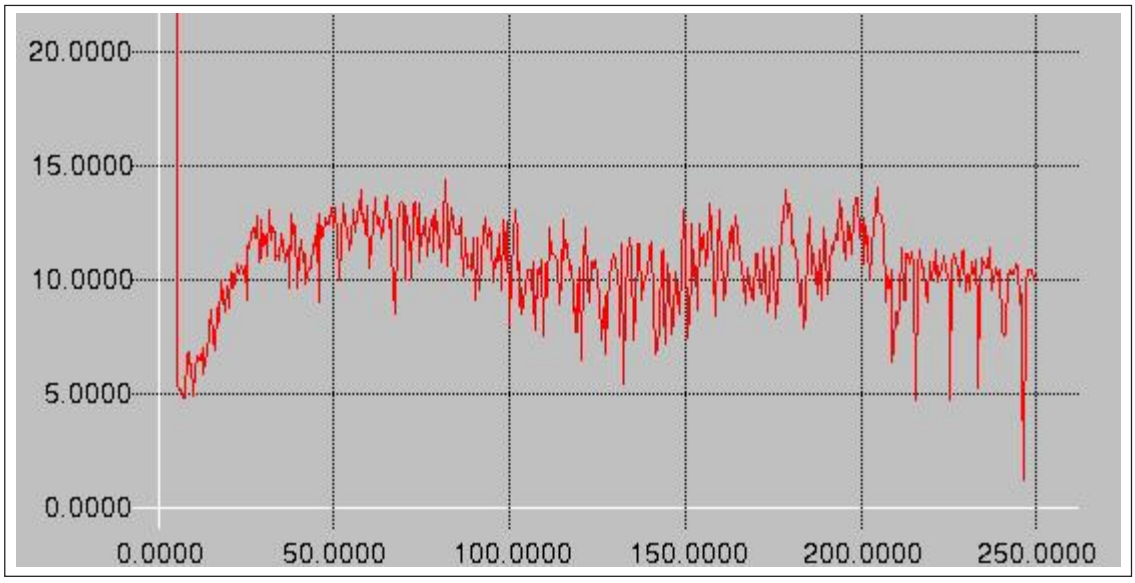

Figure 2. Throughput by using DRSUs

Average End to end delay for 20 mobile nodes decreased by 7.26% whereas for 50 mobile nodes it decreased by 23.8%.

Packet delivery ratio for 20 mobile nodes increased by 2.93% whereas for 50 mobile nodes it increased by 5.37%. Results in tabular form which shows the percent change in Average Throughput, End-to-End Delay and Packet Delivery Ratio are given in Table 1 below.

No. of Nodes	*Throughput Increase*	*End-to Delay Decrease*	*Packet Delivery Ratio Increase*
20	3.72%	7.26%	2.93%
50	47.44%	23.8%	5.37%

Table 1. Comparision

6. Conclusion and Future Work

In VANETs vehicles move with high speed and switch from one RSU to other very quickly. Hence it will be difficult for Road Side Units to bear the load of the traffic of nodes on both sides. With the introduction of directional Road Side Units and from simulation results it is observed that average throughput is increased considerably when the traffic on the road increases. Also the End to end delay is reduced by a better margin with the increase in traffic. Packet delivery ratio is also increased.

In future it is proposed that opposite side RSUs may be integrated into one RSU to reduce the cost of the hardware to be installed. Further work may also be carried out to check formation of groups for localized traffic and security issues.

7. Acknowledgment

I hereby acknowledge the services of Brig. Umar, Dr. Faisal and Mr. Bahman Ramzan to help me in minimizing the errors in the simulations.

References

[1] Al-Sakib Khan Pathan. (2011). Security of Self-Organizing Networks, CRC Press, *Taylor and Francis Group*.

[2] Rizwanul Karim Sakib, Bisway Reza. (2010). Security Issues in VANET, BRAC University, Dhaka, Bangladesh.

[3] Irshad ullah, Shoaib ur Rehman. (2010). Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols, *School of Computing, Blekinge Institute of Technology*, Sweden.

[4] Jagadeesh Kakarla, Siva Sathya, S., Govinda Laxmi, B., Ramesh Babu, B. (2011). A Survey on Routing Protocols and its Issues in VANET, *International Journal of Computer Applications* (0975 – 8887), 28 (4) 38, August.

[5] SAE J2735: Dedicated Short Range Communications (DSRC) message set dictionary.

[6] Intelligent Transport Systems (ITS). Vehicular Communications; Basic Set of Applications, ETSI TS 102 637-2 V1.2.1 (2011-03).

[7] De Fuentes, J. M., Gonzalez-Tablas, A. I., Ribagorda, A. (2010). Overview of security issues in Vehicular ad-hoc networks, *Handbook of Reseach on Mobility and Computing, IGI Global*.