ISSN:0975-9646

Adaptive Broadcasting in Vehicular Ad-hoc Networks

Priyanka Chourse[#1], Santosh K Mishra[*2]

[#*] *Computer Science & Engineering Department,*
VNS Group of Institutions, RGPV, Bhopal, India.

***Abstract*— Vehicular Ad hoc Network (VANET) is a network of vehicles. VANET is a subclass of mobile ad hoc networks (MANET), and this is a promising and distinguishes approach for the intelligent transportation system (ITS). The design of routing protocols in VANETs is an important issue to support the ITS. The key difference of VANET and MANET is the mobility pattern and rapid changing topology. Due to the different traffic condition in VANET successfully data dissemination without redundancy becomes a key challenge. To overcome these problems a routing protocol is needed with the low communication delay, the maximum throughput. The performance of the proposed protocol has been studied using simulation programs. Proposed adaptive broadcasting approach for messages dissemination in VANET results minimum latency, minimum probability of collision in the different traffic volumes.**

***Keywords*— Adaptive, Broadcast, Beacon, VANET, Delay**.

I. INTRODUCTION

VANET is the technology of building a robust Ad-Hoc network between mobile vehicles and each other, besides, between mobile vehicles and roadside units. As shown in Figure 1, there are two types of nodes in VANETs; mobile nodes as vehicles (On Board Units) and static nodes as Road Side Units (RSUs). A vehicle resembles the mobile network module and a central processing unit for on-board sensors and warning devices. The RSUs can be mounted in centralized locations such as intersections, parking lots or gas stations. They can play a significant role in many applications such as a gate to the Internet [3][5].

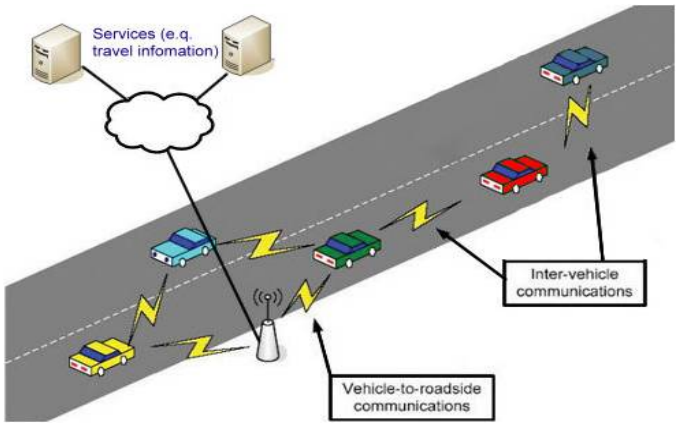

Figure 1: Vehicular Ad hoc Network

A. *Security Requirements for VANET*

1. Authentication: It ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers can be reduced to a greater extent.
2. Message Integrity: This is very much requires as this ensures the message is not changes in transit that the messages the driver receives are not false.
3. Message Non-Repudiation: Sender cannot deny the fact having sent the message
4. Entity authentication: It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period.
5. Access control: It ensures that all nodes function according to the roles and privileges authorized to them in the network.
6. Message confidentiality: It is a system which is required when certain nodes wants to communicate in private.
7. Privacy: It ensures that the information is not leaked to the unauthorized people who are not allowed to view the information.
8. Real time guarantees: Many safety related applications depend on strict time guarantees.

B. *Application of VANET*

1. Collision Avoidance: Vehicle reduces its speed significantly after observing an accident or experiencing an accident, it will broadcast its location to its neighbor vehicles.
2. Cooperative Driving: Violation warning, turn conflict warning, curve warning and lane merging warning these services may greatly reduce the life-endangering accidents.
3. Traffic Optimization: Vehicles could serve as data collectors and transmit the traffic condition information for the vehicular network.
4. Payment Services: This application is very suitable for toll collection without even decelerating the car or waiting in line.
5. Location-based Services: Finding the closest fuel station, restaurant and lodge can be done effectively using location based service. Although,

GPS systems have such kinds of services already present in it but it can also be achieved using VANET.

C. Problems in VANET Security

1. Trade-off between authentication and privacy: For authentication of all message transmission, it is required to track the vehicles for the identification of vehicles from the message they send which most consumers will not like others to know about their personal identification therefore this has to come in equilibrium.
2. High Mobility: Due to high mobility the protocol cannot be handshake based and most of the communications are between nodes that have never interacted before therefore learning based scheme should be introduced so that they learn to know about each other's behaviors.
3. Real-time guarantees: As the major VANET applications are used for collision avoidance, hazard warning and accident warning information, so applications require strict deadlines for message delivery.
4. Location Awareness: Certain location based service is essential for most VANET applications to be truly effective, so that reliance of the VANET system on GPS or other specific location based instruments can be increased as any error in these is likely to effect in the VANET applications.

D. Types of attacks on VANET

1. Bogus Information: In this case, attackers are insiders, rational, and active. They can send wrong information in the network so that it can affect the behavior of other drivers.
2. Cheating with Sensor Information: This attack is launched by an attacker who is insider, rational, and active. He uses this attack to alter the perceived position, speed, and direction of other nodes in order to escape liability in case of any mishap.
3. ID Disclosure: An attacker is insider, passive, and malicious. It can monitor trajectories of a target vehicle and can use this information for determining the ID of a vehicle. Denial of Service (DOS): Attacker may want to bring down the network by sending unnecessary messages on the channel.
4. Replaying and Dropping Packets: An attacker may drop legitimate packets to proceed toward the accident location. Similarly, an attacker can replay the packets after that event has been occurred to create the illusion of accident.
5. Hidden Vehicle: It pretends to be in good position to forward the warning message. This can be fatal for the system.
6. Wormhole Attack: A malicious node can record packets at one location in the network and tunnel them to other location through a private network shared with malicious nodes.
7. Sybil Attack: In this attack, a vehicle forges the identities of multiple vehicles. These identities can be used to play any type of attack in the system.

E. VANET Routing Protocols

1. Topology Based Routing

This routing protocol uses link information that exists in the network to perform packet forwarding. They are further divided into Proactive and Reactive routing protocols.

2. Proactive routing protocols

Proactive routing means that the routing information, like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of proactive routing protocol is that there is no route discovery since the destination route is stored in the background. The disadvantage encountered with this protocol is that it provides low latency for real time application. The various types of proactive routing protocols are: FSR, DSDV, OLSR, CGSR, WRP, and TBRPF.

3. Reactive/On-demand routing Protocols

Reactive routing opens the route only when it is necessary for a node to communicate with each other. Reactive routing consists of route discovery phase in which the query packets are flooded into the network for the path search and this phase completes when route is found. The various types of reactive routing protocols are AODV, PGB, DSR, TORA, and JARR.

4. Position Based Routing/Geographic routing

Geographic routing is a routing technique in which each node knows its own & neighbour node geographic position by position determining services like GPS. It doesn't maintain any routing table or exchange any link state information with neighbour nodes. Information from GPS device is used for routing decision. Geographic routing is broadly divided in two types: Position based greedy V2V protocols and Delay Tolerant Protocols.

5. Cluster-Based Routing

In cluster-based routing a virtual grouping is formed among the vehicles called clusters. Each cluster has a cluster head which is responsible for intra and inter cluster communication. Nodes in a cluster communicate via direct links. The different types of cluster based routing protocols are COIN, LORA-CBF, TIBCRPH, and CBDRP.

6. Geo-cast Routing

Geo-cast routing is a location-based multicast routing. The objective of a Geo-cast routing is to deliver the packet from a source node to all other nodes within a specified geographical area. The different Geo-cast based routing protocols are IVG, DG-CASTOR and DRG.

7. Broadcast Routing

In broadcast routing, flooding mechanism is used where each node rebroadcasts messages to all of its neighbors

except the one it got this message from. Flooding mechanism guarantees that the message will reach to each node in the network. Flooding is easily implemented mechanism for small number of nodes. But for a large number of nodes this mechanism is somewhat time consuming thereby reducing performance of the network. The various Broadcast routing protocols are BROADCOMM, UMB, V-TRADE, DV-CAST, EAEP, SRB, PBSM, PGB, DECA and POCA.

II. Literature Review

In the area of inter-vehicular communication (IVC) including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [1][2] functions and services, the most important projects and protocols that are involved in IVC systems as well as the different issues and challenges that exist at each layer of the networking model. IVC systems are expected to play a powerful role in providing safer and more convenient driving as well as greatly contribute to reaching the goal of ”computing anytime anywhere” of today’s society [8].

A path diversity mechanism is used for delay sensitive VANET safety applications. Sender-oriented multi-hop broadcast protocol introduces auxiliary nodes to reinforce the packet reception at the relay nodes and uses relay nodes to broadcast a packet to a multi-hop distance. With a low overhead, the proposed mechanism can provide a short delay and a high reliability. The performance of the proposed mechanism is affected by the selection of auxiliary nodes. [4][7].

Vehicular Multi-hop Broadcast protocol, called Highway Multi-hop Broadcast (HMB) that addresses the broadcast storm, hidden node, and reliability solution of multi-hop broadcast in VANET. HMB selects the farthest vehicle, with the least speed deviation with respect to the source, to forward and acknowledge broadcast frames.HMB has a very high success rate in delivering safety messages, and efficient channel utilization when compared with existing broadcast based protocols[9][10].

Enhanced intersection mode data dissemination (EIDD) mechanism, which is fully ad hoc in its operations and highly robust. The idea has to keep the emergency message in the intersection long enough to ensure that the message is forwarded to all the intersecting road segments. EIDD performs better than AMB in terms of reliability and robustness as the vehicle density decreases [6].

III. Proposed Work

Proposed adaptive broadcasting algorithm endows with reliable delivery of message and reduces all losses. We consider all network scenarios with respect to traffic i.e. low density and high density traffic situation. Proposed algorithm is getting information of one-hop nodes by its position using beacon message. Using this method every node will come to know about its neighbor positions. According to neighbor’s position prepared a list of nodes which is in promising position to forward message further. After forwarding a message according to the responses coming from receivers, again prepared lists. List1 who received message and list 2 who do not received. Again retransmit the message until list 2 becomes empty. Update both the list after each retransmission.

A. Flowchart

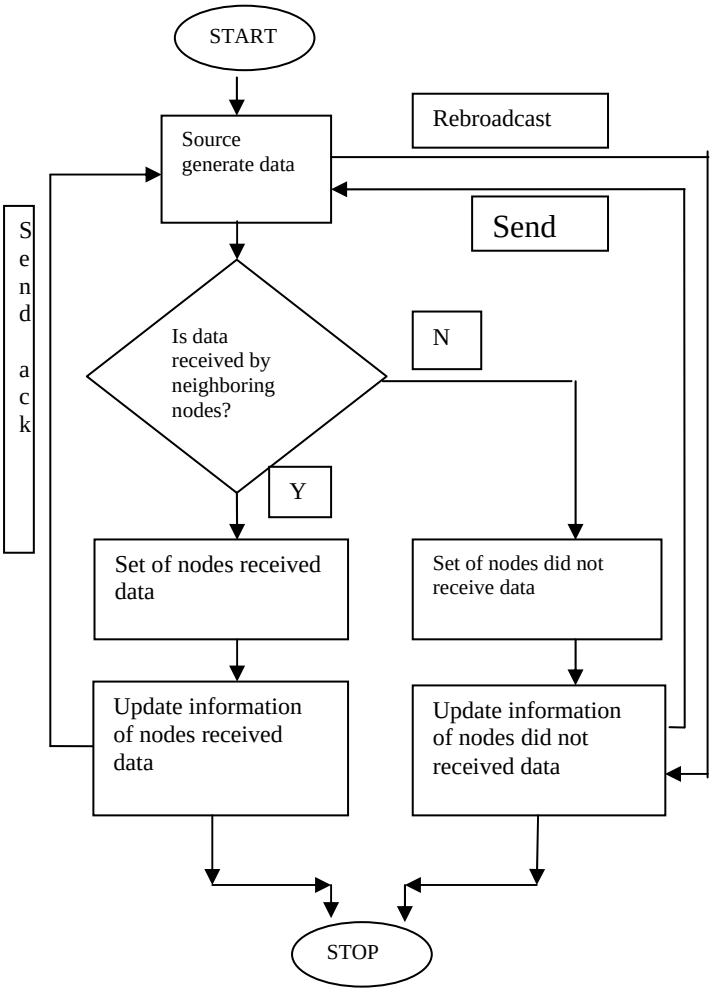

Figure 2: Flowchart of proposed algorithm

B. Algorithm

Step1: There is a network of nodes (vehicles), where source nodes want to transmit data to other.

Step2: After transmission of data, through acknowledgement nodes can be divided into two sets.

Step3: First set: Those nodes, who received data, second set: those nodes who did not received data.

Step 4: Source retransmit data to second set of nodes who did not receive data. Therefore, each and every node having data and retransmission is done only for second set of nodes.

Step 5: This process is repeated until second set gets empty.

IV. Implementation Detail and Result Analysis

Simulation work has been done in Network Simulator ns-2, version 2.34 with the simulation parameters as given in Table 1.

Table 1: Simulation parameter and its value

Simulation Parameter	Values
Simulator	NS2
Network Area	1100*1100
Channel type	Wireless Channel
Radio-propagation model	Two Ray Ground
Antenna type	Omni Antenna
Layer type	Link layer
Interface queue type (ifq)	Queue/DropTail/PriQueue
Max packet in ifq (ifqlen)	200
Network interface type (netif)	Phy/WirelessPhy
MAC type	802.11
Number of mobile nodes (nn)	100
EnergyModel	EnergyModel

Generate the simulation results and run simulation to evaluate the performance of two different protocol routing protocols for VANET in terms of different performance parameters that are Throughput and Delay.

A. Simulation through VANETMobiSim

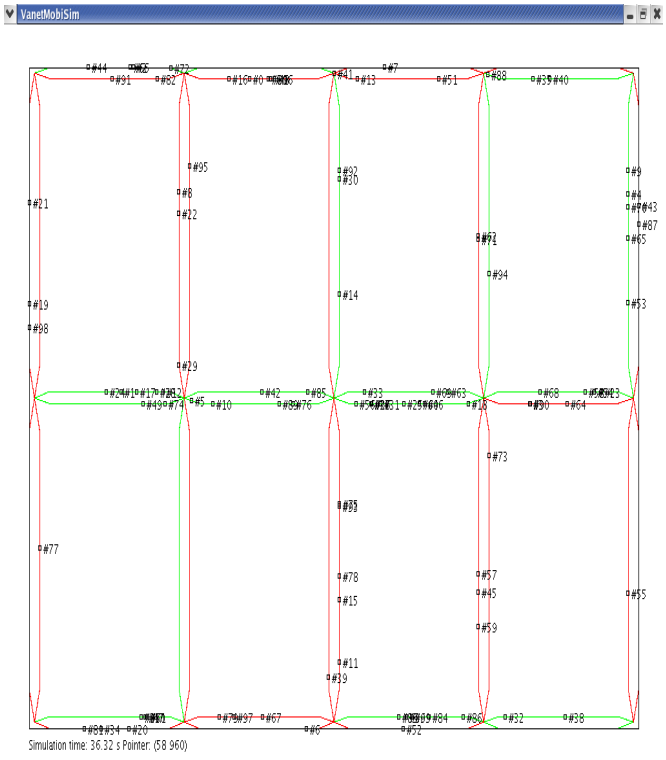

Figure 3: Network Design in VANETMobiSim

V. Result and Analysis

This section represents simulation results and it's analysis. Simulation was run and the results were generated for each performance parameter. After running simulation the results of each scenario were saved. Through simulation checked the performance of two different routing protocols of VANET. Evaluated performance of PBSM and Adaptive broadcasting protocols in VANET in terms of different performance metrics i.e. throughput and delay.

Delay:

Delay is the time taken by a packet to route through the network from a source to its destination.

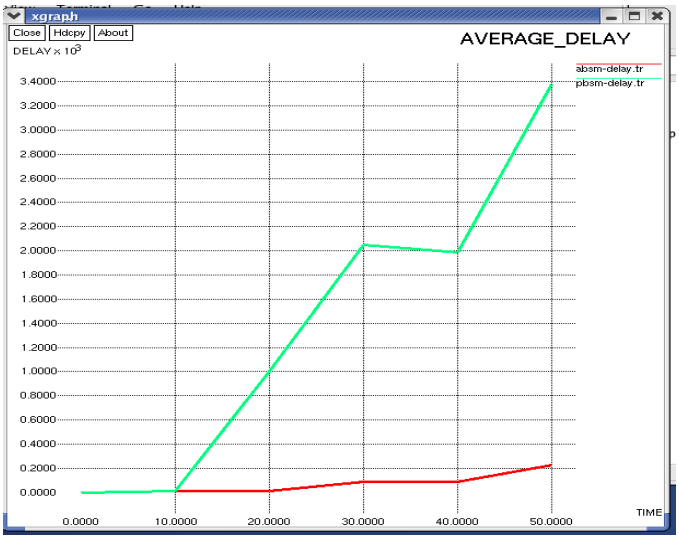

Figure4: Average delay of PBSM and Adaptive broadcasting protocol

Due to adaptive nature of protocol packets reached to the destination without any delay. Therefore this factor shows less delay by Adaptive broadcasting protocol as compared to PBSM delay.

Throughput:

Throughput is total number of received packets at destination out of total transmitted packets from source. Throughput is calculated in bytes/sec.

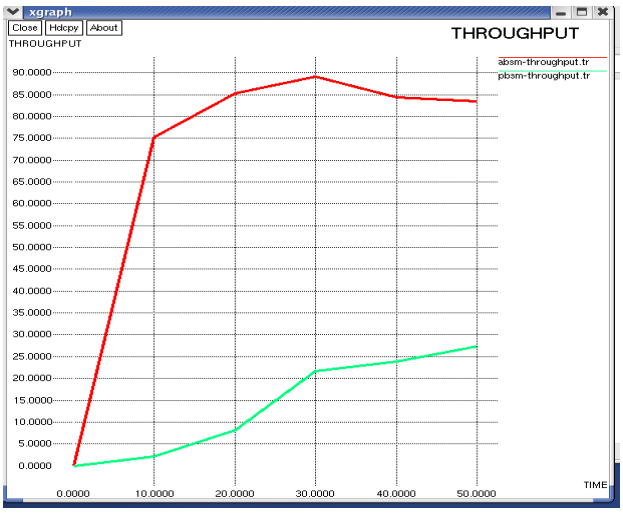

Figure 5: Throughput of PBSM and Adaptive broadcasting protocol

Packet receive success rate of Adaptive broadcasting protocol is high as compared to PBSM. Therefore this shows higher throughput.

Compare generated simulation result figure 4 with the existing result figure 5; it shows amount of delay is decreased in Adaptive broadcasting protocol as compared to existing PBSM and RBDP.

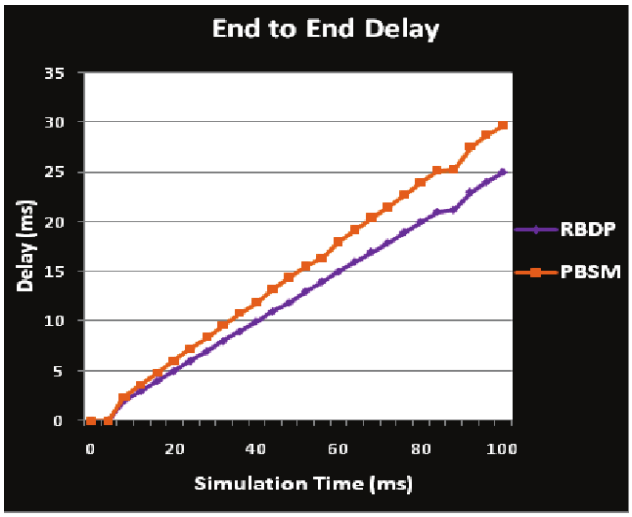

Figure5: Average delay of PBSM and Adaptive broadcasting protocol[11].

VI. Conclusions

The performance of proposed approach is compared with that of the traditional flooding method in broadcasting. It is found that the number of retransmissions has reduced to a greater extent. We have implemented a localized broadcast protocol for vehicular ad hoc networks. It uses location information and acknowledgements of messages so far received to enhance the protocol's reliability and efficiency. We have studied the scalability as the number of data sources increases. The proposed protocol turned out to be robust and reliable and significantly reduces the number of transmissions required to complete a single broadcast.

References

[1] Masanori Taketsugu, Yoshinori Nagata, "A new highly efficient multicast protocol on adhoc network under slow fading environment", IEEE, 1999, pp 1982-1986.

[2] Ivan Stojmenovic, Mahatab Sedddigh and Jovisa Zunic, "Dominating Sets and Neighbor Elimination-Based Broadcasting Algorithms in Wireless Networks", IEEE Transaction on Parallel and Distributed Systems, vol. 13, No. 1, January 2002, pp. 14-25.

[3] OzanTonguz, NawapornWisitpongphan, Fan Bai, Priyantha Mudalige, and Varsha Sadekar, Broadcasting in VANET, IEEE INFOCOM 2008 proceedings, pp 1-6.

[4] JosianeNzouonta, NeerajRajgure, Guiling Wang, and CristianBorcea, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information", IEEE Transaction on Vehicular Technology, Vol. 58, No. 7, September 2009, pp 3609-3626.

[5] Kaveh Shafiee, Victor C. M. Leung A Reliable Robust Fully Ad Hoc Data Dissemination Mechanism for Vehicular Networks, International Journal of Advanced Science and Technology, Vol. 2, January, 2009, pp 53-62.

[6] Francisco J. Ros, Pedro M. Ruiz, Ivan Stojmenovic,"Reliable and Efficient Broadcasting in Vehicular Ad Hoc Networks", IEEE, 2009.

[7] Celimuge Wu, Satoshi Ohzahata, and Toshihiko Kato," A Broadcast Path Diversity Mechanism for Delay Sensitive VANET Safety Applications, IEEE Vehicular Networking Conference (VNC), 2011, pp. 171-176.

[8] Imad Jawhar, Nader Mohamed, and Liren Zhang, "Inter-Vehicular Communication Systems, Protocols and Middleware", IEEE, 2010.

[9] Ai Hua Ho, Yao H. Ho, Kien A. Hua, Roy Villafane, and Han-Chieh Chao, "An Efficient Broadcast Technique for Vehicular Networks", Journal of Information Processing Systems, Vol.7, No.2, June 2011, pp. 221-240.

[10] MohssinBarradi, Abdelhakim S. Hafid, Sultan Aljahdali, "Highway Multihop Broadcast Protocols for Vehicular Networks", Wireless Networks Symposium, IEEE ICC 2012, pp 5296-5300.

[11] J. Lenin, "Providing Security For Privacy Information By Using Anonymous Technique In Pervasive Network", tesis submitted in the department of computer science and engineering, Manonmaniam sundaranar university Tirunelveli,August-2014