Analysis of AODV Routing Protocol in Vehicular Environment

Bhanupriya[1], Akansha Dhall[2]

M-Tech Student[1,] Assit. Prof. [2] & Department of ECE
Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India

Abstract:
Vehicular Ad hoc Network (VANET) is a new way of communication which includes communication between vehicles moving at high speeds on the roads. Routing protocols plays a significant role for enhancing Quality of Service (QoS) in Mobile Ad hoc Network (MANET). The reactive AODV routing protocol faces some difficulties i.e. time delay, long route, mobility and many others during routing. In this work the quality of AODV routing protocol has been enhanced to improve the routing capability. In this paper, the performance of general AODV routing protocol is enhanced based on Quality of Service (QoS). Here we set the constant TTL Value and variable threshold value for demonstrated the connection in long route and also evaluate the variant queue length technique according to that no packet is loss from queue if the node buffer is full, it means the queue size is changing according to data. The variable TTL value demonstrated the link with long route receiver and the changing queue decreases the packet drop. The routing protocols quality should incorporate QoS metrics in route discovering and holding, to provide support to end-to-end QoS. The performance of enhanced AODV protocol is evaluated based on performance metrics.

Keywords: MANET, QoS, AODV, TTL, Queue length.

I. INTRODUCTION

The Vehicular Ad hoc Network (VANET) is a kind of mobile ad hoc network (MANET) and is a platform to provide car safety and traffic applications VANET is the powerful technology that can provide authentic vehicle to vehicle (V2V) and vehicle to roadside infrastructure (V2I) communication that shown in fig. 1. [1]. In order to make capable data transfer they either communicate by a single hop or by multiple hops with the support of intermediary nodes. Though MANETs permits available service access, anytime, anywhere without any static infrastructure they can be broadly used in crisis management services, military battlefields, conference halls and classrooms etc. MANETs ad-hoc networking developments cause to development of tremendous multimedia applications i.e. video conferencing, video-on-demand etc. In mobile ad hoc networks and some static wireless networks multiple-hop routing is used. Routing protocols for this type of wireless network should be capable to manage and keep the paths to other nodes and

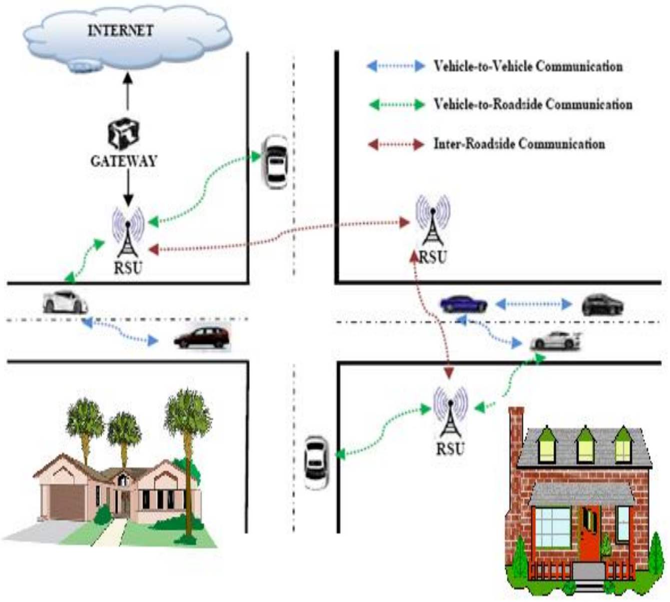
INTERNET
GATEWAY
RSU
RSU
RSU
Vehicle-to-Vehicle Communication
Vehicle-to-Roadside Communication
Inter-Roadside Communication

Figure: 1 Vehicular Ad-hoc Networks

The Transmission control protocol (TCP) is one of the popularly used transport layer protocol on the internet in present time. TCP assure reliable data transfer over unreliable networks. This protocol performs three important tasks a) Connection Establishment b) Data Transfer c) Connection Termination. Significant problems of TCP degradation in mobile networks are high bit error rate, mobility, exposed and hidden node problem and Scalability etc. Presently, conventional wired network are being substituted by wireless networks. The main causes may be the decreasing cost of wireless devices and the enormous technical enhancement in the wireless communication area. Still, there remains a substantial challenge to give QoS solutions and preserve end-to-end Quality of Service with user mobility. Mostly established routing protocols are planned either to decrease the network data traffic or to decrease the mean hops for supplying a packet. [1]. Some protocols i.e. Ad-hoc On demand Distance Vector (AODV), On-demand Multicast Routing Protocol (ODMRP) and Dynamic Source Routing (DSR) are developed without considering QoS explicitly. When QoS is taken in account, some protocols may be impractical or unsatisfactory because of the deficiency of resources and the unlimited calculation overhead. QoS routing generally includes two tasks:

gathering and holding up-to-date status information about the network and discovering viable routes for a connection depending on its QoS needs. [5] To provide support to QoS, a service can be described by a collection of measurable pre defined service needs i.e. minimum delay, maximum bandwidth, maximum delay variance and maximum packet drop rate.

II. AODV ROUTING PROTOCOL

AODV [2] is an on-demand routing protocol that constructs routes only when needed. It uses sequence numbers to assure the originality of routes. To discover a route to a destination, a source node using AODV disseminates a route request (RREQ) packet based on constant Time to Live (TTL) value. The RREQ packets consists the current sequence number, node's IP address, broadcast ID and recent sequence number for the destination node which is known to the source node. The destination node on reception of RREQ, sends a unique route reply (RREP) packet with the reverse route constructed at the mediator nodes on the route discovery process. In situation of link breakage or invalid TTL value a route error packet (RERR) is delivered to the destination and source nodes. Because of use of sequence numbers, the source nodes are all time able to discover new valid routes.

III. LITERATURE SURVEY

In [6], the authors suggested an enhanced AODV to provide support to QoS, presuming the existence of some fixed connections in the network. The authors presented the concept of node consistency, founded on a node's history, which contained both a node's packet processing ratio and its mobility. Only consistent nodes were counted for routing. Still, the authors did not count the affect that indeterminable link failures would have on re-routing. In [7] authors have introduced a consistent, on-demand, weight-based routing protocol. The "weight" contained in the protocol messages used to choose stable routes which depends on three factors: Route Expiration Time (RET), which is the determined time of link failure among two nodes because of mobility, Error Count (EC), which catches the number of link breakage because of mobility, and Hop Count (HC). The authors have accepted that all nodes are moving in the same way and at the same time through a Global Positioning System (GPS), so that two neighboring nodes may determine the RET. Though the suggested scheme may fight against link failures because of mobility, link failures because of the less node energy is a component that also must be considered for when calculating weights for consistent routing. From the suggestions examined till now [8] it is clear that there is a requirement for a routing protocol that can give stability to the routes chosen for routing QoS capabled applications, and also has process for fast re-routing to tackle indeterminable link failures. Moreover, the stability should come at minimum or no overhead for the system to be scalable. In what follows, we suggest enhancements to the AODV protocol that, give routes that are consistent for a session duration, with high probability, and that also contain a fast make-before- break process.

In [10] QoS routing has recently got attention for giving QoS to wireless ad hoc networks and some work has been done to deal with this vital issue. Here, we give a short review of available work addressing the QoS routing effects in wireless ad hoc networks. Generally, QoS routing can be categorised into two basic types: hop-by-hop QoS routing and source QoS. In future, the term routing will relate to QoS routing if not specified. In source routing, the source node of a communication request locally calculates the whole constrained path to the aimed destination with the global state data that it locally holds. Collecting and holding global state information can insert unrestrained protocol overhead in dynamic networks and therefore have the scalability problem. Furthermore, the computation of constraint based routes would be computationally intensive for the computing nodes. The predictive location- based QoS routing protocol is mainly used to provide relief from the scalability problem in carrying out source routing with respect to communication overhead. Rather than broadcasting the status of every link network wide, every node broadcasts its node state (involving its velocity, current position, available resources and moving direction on each of its outgoing links) throughout the network at regular intervals of time or upon a substantial change. With this information, at any moment, each node can locally describe an instant perspective of the whole network. To hold a QoS request, the source node locally calculates a QoS fulfilled route (if available) and propagate data packets through the computed path. Furthermore, the source can determine route failure and predicatively calculate a new path before the old route failures by using the global state it holds. This routing protocol is appropriate or suitable for supplying soft QoS in small or medium-sized networks wherein mobile hosts are fitted with Global Positioning System (GPS) receivers and their moving behavior is determinable. The MANETs routing protocols may be generally categorised as on-demand driven protocols and table driven protocols. Table driven protocols require to hold the global routing information related to the network in each mobile node for all the possible source-destination link and take to interchange routing information at the regular interval. This type of protocol has the characteristics of higher overload and lower latency.

IV. PROBLEM STATEMENT

MANET is a distributed network on infrastructure less environment that support less quality of data and unreliable service so our objective is to give more reliable service in comparison of existing routing protocol services using transport layer scheme and improvement of routing protocol and enhance quality of service (QoS) of communication.

.

V. PROPOSED SCHEME:

Here we suggested AODV modified scheme for minimization of routing over head as well as queue variant scheme for minimization of data drop and fetch improvement result of modified routing scheme. At the beginning, in this algorithm we adjust time to live (TTL value) as 7 millisecond, threshold time to live as dynamic and one fixed value and according to that value we propagate route request packet and determine literal receiver and dynamic threshold scheme which is useful for longer route request reaction time case, after this scheme we employ queue variant base technique for minimization of data drop. In this scheme we examine queue limit and we cannot drop data if the limit value is full instead of increasing queue limit by one for saving data into queue. This algorithm provides better quality of service (QoS) as well as highest performance in comparison of existing AODV routing scheme.

VI. SIMULATION RESULTS

This section presents the results that has been produced after employing the suggested scheme and compare the performance with usual ad-hoc distance vector (AODV) protocol.

A. PDR Analysis

Packet delivery ratio is the estimation of total percentage of successfully delivered and received packets in network. This graph presents Packet Delivery Ratio Analysis in case of general AODV protocol and suggested improved Quality of Service (QoS) based routing protocol. Here the performance of suggested QoS based AODV protocol is better in comparison of general AODV. After 30 second the performance of suggested improve AODV protocol is keeping the enhancement up to last of simulation. The percentage of packet in case of general AODV routing is nearly 92% but in case of QoS based AODV routing is approximately 98%, it means the idea of dynamic changing TTL value is definitely enhancing the efficiency of routing and also improved the routing protocol performance.

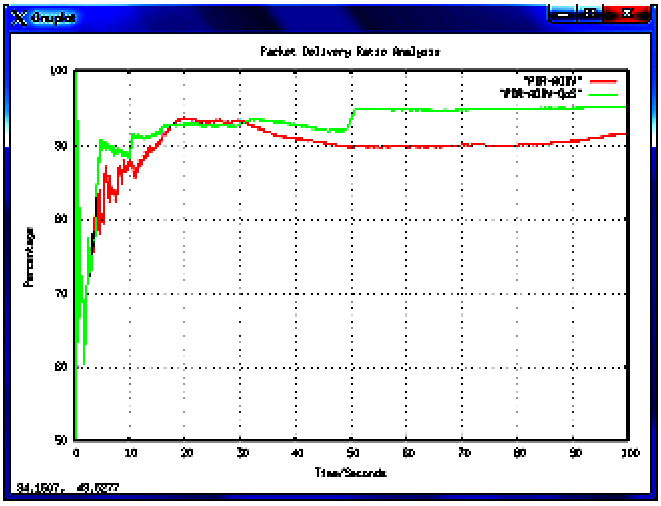

Fig. 2 PDR Analysis

B. Routing Load Analysis

Routing overhead is one of the significant element to evaluate the routing protocol performance in ad hoc network. The connection forming packets or routing packets are needed to hold the connection between receiver and sender after that the data transmission is beginning. Because of the dynamic nature the challenging task in ad hoc network is routing overhead minimization. In this graph, in case of suggested improved QoS based AODV protocol the routing overhead is very effective in comparison of general AODV routing protocol. The lesser value of routing overhead indicates the better performance. In suggested scheme only approx. 50670 routing packets are delivered in network while in case of general AODV routing more than 8900 routing packets are delivered in network. It shows that the performance of suggested protocol is very much better as compared to general AODV protocol and more number of data packets are delivered in network in case of improved QoS AODV.

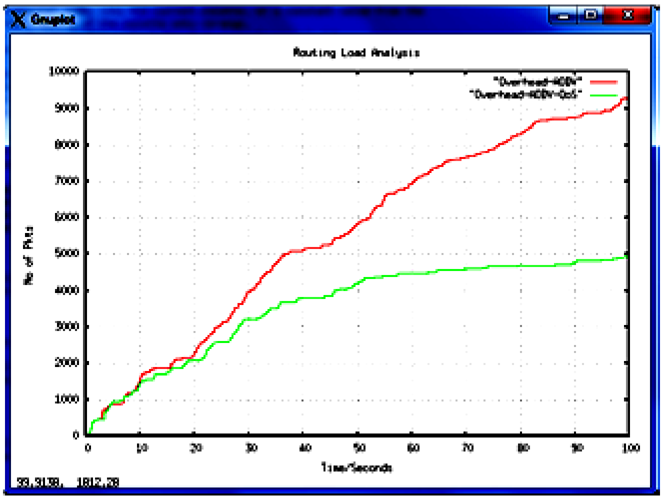

Fig. 3 Routing Load Analysis

C. Throughput Analysis

Throughput means number of packets receive or send per unit of time in network. Throughput shows the successful receiving or delivery according to time.

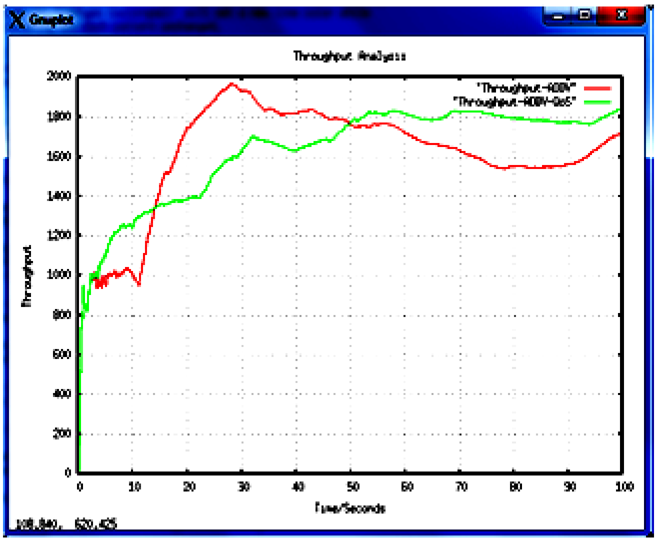

Fig. 4 Throughput Analysis

In this graph, the throughput performance of general AODV routing protocol and suggested enhanced QoS based AODV routing protocol is evaluated, here we notice that at the beginning, at time from initiating to 15 seconds the performance of suggested protocol is better but after that AODV is better up to 50 seconds and then again the performance of suggested protocol is better after 50 seconds. It shows the idea of dynamic TTL value is surely enhances the routing protocol performance. Due to the higher routing overhead as depicted in fig. 3 the network performance of general AODV routing protocol decreases. If the high numbers of routing packets are delivered in network it means that data packets are looking for connection establishment then packets routing ability influenced and network performance decreases.

D. UDP packet Analysis

Here, the performance of User Datagram Protocol (UDP) is evaluated because of their unreliable nature it means that due to their connection less property, no connection is established here, data delivery is initiated directly in network. Because of connection less property the probability of packet drop is high it means that this protocol performance depends on network conditions. The performance of suggested and general AODV routing protocol is approx. equal from beginning to 50 second in this graph. But after that in case of suggested improved QoS based UDP packet obtaining capability increases continuously till the end of simulation in comparison of general AODV. In suggested case about greater than 300 packets are obtained in network but in case of general AODV only approx. 220 packets are received in network. It means that the suggested protocol is more reliable as compared to previous one.

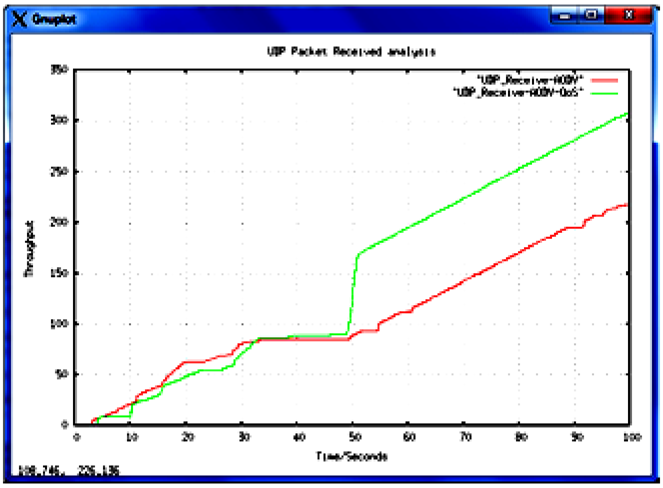

Fig. 5 UDP packet analysis

VII. CONCLUSION

The new developments of the protocols are prompted by special objectives and needs on the basis of various assumptions about the application area or network properties. Thus, it is very crucial that these networks must be capable to provide effective quality of service (QoS) that can fulfill the vendor needs. To provide effective QoS (Quality of Service) in mobile ad-hoc networks, there is a strong requirement to build new technique for routine network controls. Maintaining the QoS has been a significant and suitable element of MANETs. Although it is complicated but quite challenging and interesting to build and develop QoS provisioning techniques in MANET for routing. This research gives a quality enhancement in AODV routing technique to improve the performance. The suggested routing schemes are developed on the basis of deviating queue size at nodes of the network. Nodes with static queue length might lead to the probability of higher packet losing by that we chose the suggested method to overcome the problem of lack of long route establishment and manage the load with deviating queue length. The suggested scheme surely enhances the network performance and this protocol enhancements are evaluated by performance metrics and results proves that the performance of suggested AODV QoS protocol is much better in comparison of general AODV routing. In future, only data rate metric is taken into consideration in terms of metrics in QoS aware routing protocols in the simulations. The additional metric can be End to End delay metric in the path determination and maintenance in the routing protocol. Therefore, end to end delay can be summed to the AODV routing protocol.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, “Defending AODV Routing Protocol Against the Black Hole Attack”, International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,”DPRAODV: A dynamic learning system against black hole attack in AODV based Manet”, International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, ”Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, “Study of Different Attacks on Multicast Mobile Ad hoc Network”, Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks”, 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, “New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks”, 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, “A Simple and Efficient Detection of Wormhole Attacks”, New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis of Wormhole Intrusion Attacks in MANETs”, Military Communications Conference, November 2008, pp.1-7

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, ”Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing

Analysis”, Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, “Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks”, Second International Conference on Computer and Network Technology, 2010, pp. 102-104

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, “Defending against Wormhol Attacks in Mobile Ad Hoc Networks”, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[16] L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,” IEEE Wireless Commuunication. and Networking Conference, 2005.

[17] I. Khalil, S. Bagchi, N. B. Shroff,” A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks, 2005

[18] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach”, IEEE Communication Society, WCNC 2005.

[19] L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, 11th Network and Distributed System Security Symposium, pp.131-141, 2003

[20] L.Lazos, R. Poovendran, “Serloc: Secure Range-Independent Localization for Wireless Sensor Networks”,ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[21] W. Wang, B. Bhargava, “Visualization of Wormholes in sensor networks”, ACM workshop on Wireless Security, pp. 51-60, 2004.

[22] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE, April 2004, pp.96- 97.

[23] Anu Bala, Munish Bansal and Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, First International Conference on Networks & Communications, 2009, pp. 141-145.

[24] Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[25] Geng Peng and Zou Chuanyun,”Routing Attacks and Solutions in Mobile Ad hoc Networks”, International Conference on Communication Technology, November 2006, pp. 1-4

[26] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks”, International Conference on Parallel Processing Wowrkshops, August 2002.