ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

To Avoid Congestion by Using Flooding Approach in Wireless Ad Hoc Networks

V.Elamathi[1], D.Dhivya[2]
[1]Assistant Professor, Department of MCA, Narasu`s Sarathy Institute of Technology, Salem
[2]Assistant Professor, Department of CSE, Narasu`s Sarathy Institute of Technology, Salem

Abstract – Talent of a routing algorithm to converge quickly when network topology changes frequently is a critical requirement for routing in multi-hop wireless networks, Due to its exceptional convergence performance, Link State Routing protocol is the state of art in wireless network routing. The protocol is to operate Link State Packet with flooding at interconnected networks, with each node participating in the routing protocol get a copy of link state information from all other nodes at the same time. Whereas most routing algorithms for ad hoc networks use minimum hop count as their routing metric, our protocol uses link costs that are proportional to the control that the node needs to reach the next hop. In this paper we propose an LSRP protocol which is effectively reduce the degradation of packet loss and faulty nodes. Although this approach produces routes with more hops, it allows to minimize the congestion on the link.

***Key words*-Congestion, LSRP, LSP, RREQ, Flooding.**

I. INTRODUCTION

A mobile ad hoc network usually consists of wireless mobile nodes that communicate with each other, in the absence of a fixed infrastructure. Thus, it is suitable for use in situations where an infrastructure is unavailable or to deploy one is not cost effective [4]. In mobile wireless ad hoc networks the key issue is network congestion and traffic blocking. The congestion occurs in mobile ad hoc networks due to limited availability of resources. In such networks, Transmission errors also cause burden on the network due to retransmissions of Packets in the network. Congestion leads to packet losses and bandwidth degradation, and wastes time and energy on congestion recovery. Although, it is not possible to get rid of congestion problem but it is possible to limit the impact of congestion on network efficiency by using some suitable procedures and rules for traffic flow. To minimize congestion in network routing algorithms are used [5]. Major problem of routing in mobile ad hoc network is path selection. Sometimes the problem of routing may lead to congestion. By avoiding this Routing is important concept in wireless networks. In which routing table only mainly maintains routing information about nodes at the interconnected networks. Where as we can maintain a source address, intermediate and destination address. So that, the packet correctly reaches to end system without any delay.

Long delay: It takes time for a congestion to be detected by the congestion control mechanism. In severe congestion situations, it may be better to use a new route. The problem with an on-demand routing protocol is the delay it takes to search for the new route.

High overhead: In case a new route is needed, it takes processing and communication effort to discover it. If multipath routing is used, though a alternate route is readily found, it takes effort to maintain multiple paths.

***Many packet losses*:** Many packets may have already been lost by the time congestion is detected. A typical congestion control solution will try to reduce the traffic load, either by decreasing the sending rate at the sender or dropping packets at the intermediate nodes or doing both. The consequence is a high packet loss rate or a small throughput at the receiver end. To overcome the limitations of proactive routing protocols [3], reactive routing protocols like dynamic source routing (DSR) and ad hoc on-demand distance vector routing (AODV) protocols have been proposed for MANET. In reactive routing protocol, a route is discovered when it is required. Reactive routing protocol consists of two main mechanisms: (a) route discovery and (b) route maintenance [5].

At present, AODV routing protocol is often used in ad hoc network. But its biggest shortcoming is delay. In routing discovery and maintenance, a large number of data is transmitted through a small number of nodes is bound to lead to network congestion. At the same time, imbalanced data load will be exhaust nodes energy rapidly. With the increase of brownout nodes, network connectivity will be weakened and network overall survival time will be shorten subsequently. Therefore, In order to balance the network load and maintain network continuous, efficient and stable operation, it is necessary to take into account the routing nodes load and congestion in network [8].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

A fault-tolerant multipath routing protocol has been designed to reduce packet loss due to route breakage. In this protocol, nodes determine multiple disjoint routes using AOMDV having more battery power and residual energy, to every active destination. In fault-tolerant mechanism, the received signal strength is measured and based on its value; it can send warning packets to the previous node. When a downstream node encounters a forwarding error, an upstream node with the same data in its buffer and alternative route can retransmit the data. The faults have proactively detected and provided fault-tolerant routing but didn't consider the losses due to congestion. The AOMDV protocol is used as a base for the multipath routing. In existing reactive routing protocols, only the node encountering the error can salvage or retransmit a data packet. (i.e.,) packet salvaging is centralized. This proposed scheme enables more nodes to salvage a dropped packet, (i.e.,) packet salvaging is distributed [4].

The flooding attack is the most common attack found in MANET. The aim of the flooding attack is to exhaust the network resources such as bandwidth and to consume a node's resources or to disrupt the routing operation to degrade the network performance. This leads to a kind of attack, wastage of bandwidth, wastage of node's processing power and exhaustion of node's battery power as well as a degraded performance. Most of the network resources are wasted in trying to generate the routes to the destination that do not exist. In this attack, the malicious node will generate a large number of RREQs, possibly in the region of hundreds or thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets.

Flooding Attack can seriously degrade the performance of reactive routing protocols and affect a node in the following ways. a) Degrade the performance in buffer - The buffer used by the routing protocol may overflow since a reactive protocol has to buffer data packets during the route discovery process. Furthermore, if a large number of data packets originating from the application layer are actually unreachable, genuine data packets in the buffer may be replaced by these unreachable data packets, depending on the buffer management scheme used. b) Degrade the performance in wireless interface - Depending on the design of the wireless interface, the buffer used by the wireless network interface card may overflow due to the large number of RREQs to be sent. Similarly, genuine data packets may be dropped if routing packets have priority over data packets. c) Degrade the performance in RREQ packets - Since RREQ packets are broadcast into the entire network, the increased number of RREQ packets in the network results in more MAC layer collisions and consequently, congestion in the network as well as delays for the data packets. Higher level protocols like TCP which is sensitive to round trip times and congestion in the network will be affected. d) Degrade the performance in duration of MANET - Since MANET nodes are likely to be power and bandwidth constrained, RREQ can reduce the lifetime of the network through useless RREQ transmissions as well as additional overheads of authenticating a large number of RREQs, if used [6].The flooding attack be able to cause node encountering error, dropped packet and degrade the route performance.

II. PROPOSED MODEL

In this study, it is proposed to design an effective congestion control technique which proactively detects node level and link level congestion and perform congestion control using the fault-tolerant multiple paths. More reactive routing protocols, only the node encountering the error can salvage or retransmit a data packet. But this proposed link state routing protocol [Open shortest routing protocols] enables more nodes to salvage a dropped packet at the same time.

A. Congestion Detection Algorithm

The algorithm shown below states the proposed congestion detection and notification strategies. The congestion detection algorithm is buffer and LSP based. On reception of a data packet, each intermediate node monitors its current buffer size and calculates a running average value using exponential weighted moving average formula. If this average value becomes greater than a predefined threshold then the congestion is detected. Here, we represent the weight factor given to the current size of the buffer. Once the congestion is detected, the intermediate node empties its buffer of all pending data packets in order to reduce the amount of backlogged packets. This also boosts up the forwarding of current data packet and it would be routed. For congestion detection, finding the faulty node should be important one, and then only the collision can be identified and rectified. This the function mainly performed by link state routing protocol. The basic idea behind in link state routing protocols is very simple. In which every node knows how to reach directly connected neighbors.

B. Link state routing protocol

The main function of Link State Routing Protocol is flooding. Reliable flooding is the process of making sure that all the nodes participating in the routing protocol get a copy of link state information from all other nodes. As the term suggests, each node that receives this information and forwarding it out on its entire links. This process

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013
continuous until the information has reached all the nodes in the network. By using of this protocol each node creates an update packet, also called a link state packet (LSP), which contains the following information
1. The ID of the node that created the LSP.
2. The cost of the link to each one.
3. A sequence number.
4. A time to live for this packet.
The above following information's are needed to enable route calculation and process of flooding the packet to all nodes reliable.

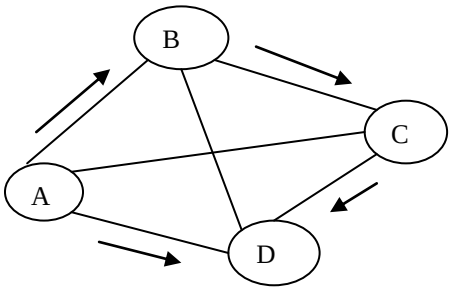

Fig 1. Flooding of Link State Packets

C. Route Calculation Algorithm

Once a given node has a copy of the LSP from every other node, it is able to complete map for topology of the network, and from this map it is able to find the best route to each destination. The algorithm is defined as follows
M={s}
for each node n in N-{s}
C (n) = l(s,n)
While (N = /M)
M =M U {w} such that C(w) is the minimum for all w in (N-M)
for each n in (N-M)
C (n) = MIN(C (n), C(w) + l(w,n)).

D. Congestion Control Algorithm

Whenever the source node receives the congestion control Packet sent by the congested node, it executes the congestion control algorithm. At first, the source node stops the forwarding of packets over the active paths. The source node sets a timer for the duration at which this new rate will be activated. If the source node does not receive any congested packet during this period, If the link qualities of any of the active paths deteriorate, eventually the source node starts to load at the lowest possible rate over that path. In this case, the source attempts to switch the congested path with the backup path if possible. Consider residual energy and battery power in paths selection and the energy balance in data transmission to maximize the lifetime of networks. The congestion algorithm is defined as follows
1. Compute the average energy of the nodes.
2. Calculate the energy level of the node.
3. If source requires for route packets to destination, then
3.1. Check the routing table
3.2. If the path is valid, then S performs to send packets(with network wide flood of LSP)
End if.
End if.
4. If the node receives LSP then it routes into destination, then
4.1. Stores the LSP in buffer.
4.2. When TTL reaches 0, the node refloods the LSP.
End if.
5. If the time expires.
5.1. Node drops all packets with LSP.
End if.
6. If the congestion is detected,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

6.1. LSP will inform to source then it stops to send packets through active path.
7. If the traffic is cleared, go for possible backup path.
7.1. Node salvages all packets that are still in its data cache through the established alternate path.
End if.
End if.

III. RESULTS AND DISCUSSION

In experimental process variation in one of the parameter including number of node pause time was done each time and their effect on performance of different protocols was determined. Effect of simulation studies on performance of LSRP and AOMDV protocols under experimental conditions mentioned below are represented graphically as follows. In this simulation, 50 mobile nodes move in a 1400m rectangular region for 50 sec simulation time. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 350 m. In our simulation, the speed is set as 6 m sec. The simulated traffic is Constant Bit Rate (CBR). The pause time of the mobile node is varied as 0-5.

Performance metrics **-** The LSRP protocol is compared with the AOMDV. The performance is mainly evaluated according to the following metrics.

Average end-to-end delay- The end-to-end-delay is averaged over all surviving data packets from the source to the destinations.

Average packet delivery ratio **-** It is the ratio of the number of packets received successfully and the total number of packets sent.

Throughput **-** It is the number of packets received successfully.

Drop **-** It is the number of packets dropped.

TABLE SIMULATION SETTINGS

No. of Node	50
Area Size	1400 X 200
Mac	802.11
Radio Range	350m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	412
Mobility Model	Random Way Point
Speed	6 m/s
Pause time	0,1,2,3,4 and 5

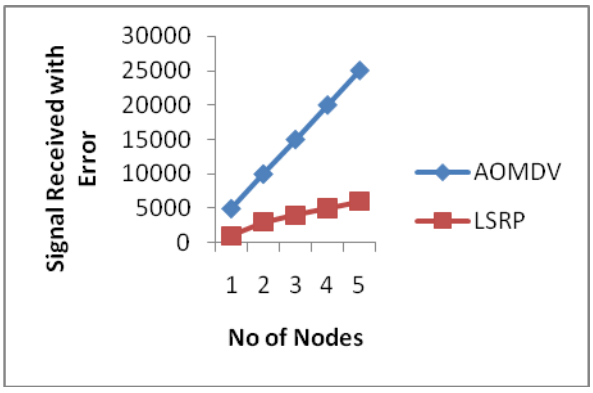

Fig 2. No of nodes Vs Signal

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Figure 2 presents the error ratio of both protocols. Since the packet drop is less and the throughput is more, LSRP achieves good delivery ratio, compared to AOMDV.

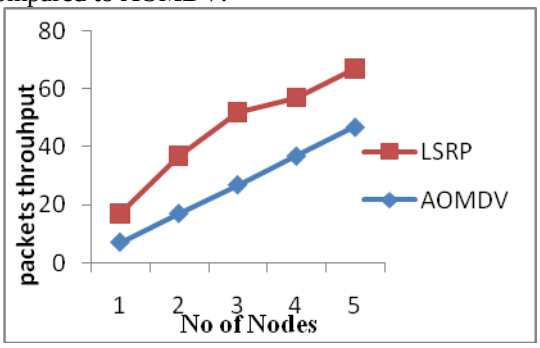

Fig 3. No of nodes Vs Throughput

Figure 3 presents the packet delivery ratio of both the protocols. Since the packet drop is less and the throughput is more, LSRP achieves good delivery ratio, compared to AOMDV.

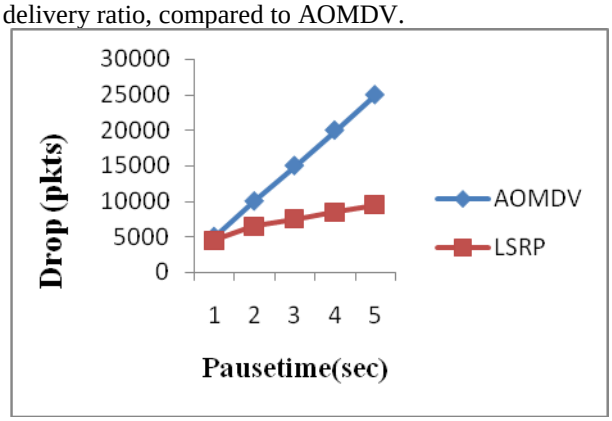

Fig 4. Flow Vs Throughput

Figure 4 gives the throughput of both the protocols when the pause time is increased. As it is seen from the figure, the dropped packets are too low in the case of LSRP, than AOMDV.

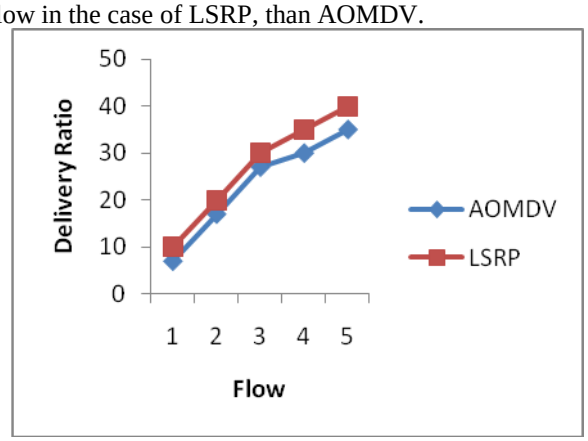

Fig 5. Flow Vs Throughput

Figure 5 presents the packet delivery ratio of both the protocols. Since the packet drop is less and the throughput is more, LSRP achieves good delivery ratio, compared to AOMDV.

IV CONCLUSION

In this study most traditional routing protocols do not well adopt to mobile ad hoc networks. So there is a need for a congestion aware routing metric which incorporates transmission capability, reliability, and congestion around a link. So we have developed a link state routing protocol to reduce the congestion losses. In this protocol, a congestion control technique is followed which proactively detects node level and link level congestion and performs congestion control using link state packet updates. The congestion detection algorithm is LSP based.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Whenever the source node receives link state packet sent by the congested node, it executes the congestion control algorithm. We have proved that our proposed routing protocol attains high throughput and packet delivery ratio, by reducing the packet drop and delay.

REFERENCES

[1] Boris Mitelman, Arkady Zaslavsky, Workshop on CSIT'99, Moscow, Russia, 1999. Link State Routing Protocol with Cluster Based Flooding for Mobile Ad-hoc Computer Networks.

[2] Prof. S.A. Jain, Mr. Abhishek Bande, Mr. Gaurav Deshmukh, Mr. Yogesh Rade, Mr. Mahesh Sandhanshiv, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 509-514, ISSN: 2248-9622. An Improvement In Congestion Control Using Multipath Routing In Manet.

[3] Laxmi Shrivastava, G.S.Tomar and Sarita S. Bhadauria, International Journal of Compute Theory and Engineering, Vol. 3, No. 2, April 2011, ISSN: 1793-8201.A Survey on Congestion Adaptive Routing Protocols for Mobile Ad-Hoc Networks

[4] Rajkumar. G and K. Duraiswamy, Journal of Computer Science 8 (5): 673-680, 2012 ISSN 1549-3636 © 2012 Science Publications. A Fault Tolerant Congestion Aware Routing Protocol for Mobile Ad hoc Networks.

[5] Santhosh baboo.S and Narasimhan.B, International Journal of Computer Science and Information Security,Vol. 3, No. 1, 2009. A Hop-by-Hop Congestion-Aware Routing Protocol for Heterogeneous Mobile Ad-hoc Networks.

[6] Ujwala D. Khartad & R. K. Krishna, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Volume 1, Issue 4, 2012, ISSN No. 2248- 9738. Route Request Flooding Attack Using Trust based Security Scheme in Manet.

[7] G.Vijaya Lakshmi and Dr. C.Shoba Bindhu, IJCTA, July-August 2011, Vol 2 (4), 750-760, ISSN: 2229-6093.Congestion Control Avoidance in Ad hoc Network using Queuing Model.

[8] Vishnu Kumar Sharma and Dr. Sarita Singh Bhadauria, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.2, April 2012. Performance Analysis on Mobile Agent Based Congestion Control Using AODV Routing Protocol Technique with Hop by Hop Algorithm for Mobile Ad-hoc Network.

AUTHOR BIOGRAPHY

Ms.V.Elamathi is currently working as a Assistant Professor in the Department of Computer Applications in Narasu`s Sarathy Institute of Technology, Salem. She received her MCA degree in Computer Applicatios under Anna University, Coimbatore in May 2011. She received her B.Sc degree in Microbiology, under Periyar University, Salem in May 2008. Her research interest is in Wireless Networks, Bioinformatics and Neural Networks.

Ms.D.Dhivya is currently working as a Assistant Professor in the Department of Computer Science and Engineering in Narasu`s Sarathy Institute of Technology, Salem. She received her M.E degree in Computer Science and Engineering under Anna University of Technology, Coimbatore in May 2011. She received her B.E degree in Computer Science and Engineering, under Anna University Chennai in May 2009. Her research interest is in Data Mining, Neural Networks and Bioinformatics.