Throughput Enhancement of the Prioritized Flow in Self Aware MANET Based on Neighborhood Node Distances

Kiran M
Dept. of Information Technology
NITK, Surathkal,
Mangalore, INDIA
kiranmanjappa@gmail.com

G. Ram Mohana Reddy
Head, Dept. of Information Technology
NITK, Surathkal
Mangalore, INDIA
profgrmreddy@gmail.com

Abstract - **Mobility causes frequent link failures in ad hoc network resulting in packet losses. Another cause of packet loss is collision which MANET misinterprets as link failure and triggers route maintenance phase. Triggering of this unnecessary route maintenance phase adds extra overhead to the network resulting in low throughput. In this paper a Quality of Service (QoS) aware cross layer model PrioritizedQoS (PrQoS) is proposed to improve the throughput of the prioritized flow in Self Aware MANET. According to the distance of the receiving node from the transmitting node, which is found using Received Signal Strength, packets are treated differently in lower layers by dynamically adjusting the Request To Send (RTS) retry limit based on the priority of the flow. The simulation is done in ns-2 and the PrQoS is compared with the traditional methods i.e. default behavior of the protocols. The results show that the prioritized flow achieves higher throughput than the unprioritized flow when compared to traditional method. Further the PrQoS also avoids unnecessary route re-discovery attempts by finding the root cause of the packet drop based on the distance between the nodes thereby reducing the network load.**

Key Words - **Cross Layer Design, Received Signal Strength, RTS retry limit, QoS,**

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a group of Mobile Nodes (MN's) with self organizing, self configuring and rapidly deployable capability with no fixed infrastructure. MN's in MANET plays a dual role as a host and as a router at the same time and they communicate with each other on multi hop basis. MANET is rapidly gaining its popularity due to its network architecture which is very useful in the situations where temporary networks are needed like disaster recovery, military applications etc. Mobility of MN's causes frequent link failures in MANET which in turn causes packet losses. Another reason for packet loss is collision which MANET misinterprets as target node is no longer reachable and triggers route maintenance phase. This phenomenon is called as False Route Failure (FRF). The route maintenance phase is a complicated process both in terms of time and network load and eventually reduces the throughput. Finding the exact reason for the packet drop is very difficult. Because of this distinguishing characteristic of MANET, providing Quality of Service (QoS) is difficult and challenging task. Traffic in future MANET is expected to carry a mix of real time multimedia, and non real time file transfer etc with different importance. Also there may be some distinctive services which can be either real time or non real time which should be given priority. For example, user may find file transfer over FTP, which is non real time, is more important than a phone call which is real time. Since the wireless resources are finite, distinguishing and giving priorities for such kind of traffics is difficult.

In [1], Tom Goff et. al. suggested a method which checks the received packet power to see whether path is likely to break or not. If it is close to the minimum detectable power, a warning is sent to the source indicating the likelihood of a disconnection so that source can initiate path re-discovery early potentially avoiding the disconnection. Authors have demonstrated through experiment that the proposed method significantly reduces the number of broken paths with a small increase in protocol overhead. In [2], Fabius Klemm et. al. proposed a signal strength based mechanism to improve the TCP performance and link management in Ad Hoc Networks. If the measured signal strength indicates that a link failure is likely due to a neighbor moving out of the range, higher transmission power is used to temporarily keep the link alive also route re-discovery process is initiated proactively before the link actually fails. Through simulation the authors have shown that TCP session increases as much as 54% when their method is incorporated. In [3], Ning Yang et. al. proposed a cross layer model to improve the performance of the ad hoc networks. Cross layer processing is applied between Physical, MAC and Network Layer where MAC layer adaptively selects a transmission data rate based on the channel signal strength information from physical layer. The authors have used DSR routing protocol for the experiment and they have demonstrated through ns-2 that the proposed method improves the performance. In [4], San-Yung Wang et.al. proposed a signal strength based , on-demand routing protocol which first uses the earliest established path to forward packets, then changes to the strongest signal strength path for long transmissions. Through simulations on ns-2, authors have showed that the proposed method exhibits superior performance.

978-1-4577-2059-8/11/$26.00 ©2011 IEEE

In [5] , Wooi King Soo et.al proposed an intelligent link diagnostic controller for IEEE 802.11B wireless networks. The proposed method incorporates fuzzy controller in the MAC layer which based on the distances and relative velocities diagnosis the link before the attempt to reconnect is made and accordingly the retry limit is adjusted. Through simulation the authors have shown that the proposed mechanism improves the TCP performance by 7% on average. In [6], Fuad Alnajjar et. al. proposed cross layer design to achieve a reliable data transmission in MANET. The proposed method allows the Network Layer to adjust its routing protocol dynamically based on SNR and received power along the end-to-end routing path for each transmission link. Through evaluation authors have shown proposed cross layer design improves the performance. In [7], Boumedjout Amel et. al. proposed a cross layer design among Physical and Routing layers using Pr as cross layer parameter. The authors have implemented and tested new routing protocol in ns-2 which guarantees the enhanced connectivity. In [8], Yaser Taj et.al. proposed a new scheme called Signal Strength Based Reliability (SSBR) which uses signal strength as a metric for choosing the path. The new scheme uses the measured signal strength changes of the neighbor nodes, and identifies which nodes have high mobility and may cause link failure and while path selection such nodes are neglected. Through simulation authors have shown that the SSBR gives better performance when compared to traditional ad hoc AODV routing protocol.

Vijay T. Raisinghani and Sridhar Iyer [9] have concluded that the existing layered protocol stack functions inefficiently in mobile wireless environment due to highly variable and the limited nature of the mobile devices. Manjul Walia et al [10] and J. W. Dawei Man et al [11] have shown that the breaking of the layered architecture can significantly improve the performance of the wireless network. Cross Layer Design is receiving tremendous attention among the researchers for increasing the efficiency of mobile wireless networks. In the literature most of the authors have concentrated mainly on entire network throughput and not on the per flow throughput of the network. Our objective in this paper is to add self awareness in MANET in terms of neighborhood node distances and to increase the throughput of the prioritized flow by finding the root cause of the packet drop based on the distance of the receiving node from the transmitting node. While the distance between the nodes is found using Received Signal Strength (Pr) from the Physical Layer.

The rest of the paper is organized as follows. Section II discusses about the packet loss in ad hoc networks. Section III discusses the proposed model. Simulation environment is discussed in section IV followed by results and discussion in section V. The paper is concluded with future work in section VI.

II. PACKET LOSS IN AD HOC NETWORKS

Mobility of MN's and hidden nodes are the two main reasons for the packet losses causing degradation of throughput. Figure 1 describes the hidden node problem. False Route Failure (FRF) occurs when the host node 'A' declares the target node 'B' is no longer reachable since it could not establish RTS-CTS four way handshake with it even though it is within its transmission range. The nodes within the transmission range of node 'A' can receive packets from it and the nodes which are not within the transmission range but are within the interference range like node 'X' can sense a transmission from node 'A' but cannot respond to any transmission requests if node 'A' is in the process of transmitting a packet. During this time if any other node like node 'Y' which is hidden to node 'A' sends RTS control packets to node 'X', it will ignore it till channel becomes free from node 'A'[2]. In the scenario shown in Figure 1, node 'Y' tries for default number of RTS retransmissions and drops the data packet assuming node 'X' is no more reachable and triggers route maintenance phase[1].

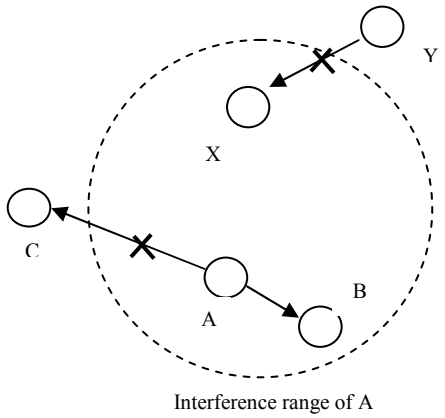

Figure 1. Hidden Node Problem

Another reason for packet drop is mobility due to which the target node may move out of transmission range causing the transmitting node to drop the packet. In Figure 1, node 'A' is trying to establish RTS-CTS handshake with node 'C', which is not in its transmission range. Node 'A' tries for default number of RTS retransmissions and drops the data packet.

III. PrQOS

PrQoS mainly consists of two parts (a) *Cross Layer Model* (b) *Neighborhood Node Distance and Dynamic Retry Limit.*

A. Cross Layer Model

The proposed cross layer model is designed with two cross layer parameters *flow priority* and *Pr*. Since our objective is to give priorities to the flows, the priority information has to be accepted from the user at the

[1]*Default number of RTS retransmission in IEEE 802.11 MAC protocol is 7*

Application Layer (AL) and should be sent to the lower layer for further processing and for finding the distance between the nodes, Pr of the packet from Physical Layer (PL) should be made visible to upper layer. It is hard to achieve these two goals in the legacy protocol stack since it will not allow non adjacent layers to communication with each other. With these two requirements, a cross layer model is designed for PrQoS across the protocol stack as shown in the Figure 2. Through the shared registry AL will inform the other layers about which type of service to be given to which flows and PL shares Pr to upper layers for further processing.

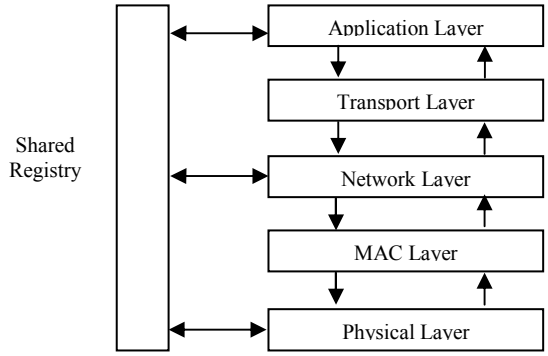

Figure 2. Cross Layer Model

B. Neighbourhood Node Distance and Dynamic Retry Limit

Since we are increasing the RTS retry limit, it is important to identify whether the target node is within the vicinity of the transmitting node. If the target node is not in the transmission range, increasing the retry limit is wasteful in both time and bandwidth. This will in turn cause performance degradation and also there will be a very late response to the actual link failure. Hence retry limit should be increased only when the node is within the transmission range. To find whether the target node is within the transmission range Pr from PL is used since it is inversely proportional to the distance between the nodes [5]. Pr is measured as soon as the packet is received from the neighbor node and the same is used to calculate the distance 'd' to the transmitter of the packet using the free space propagation model which is as follows:

$$d = \sqrt[4]{\frac{Pt \cdot Gt \cdot Gr \cdot ht^2 \cdot}{Pr \cdot L}}$$

where ,
Pt : Default transmission power
Pr: Received signal power
Gt: Antenna gains of the transmitter
Gr: Antenna gains of the receiver
ht and hr: Heights of the antennas
L: System loss (1 by default)

The distance 'd' is maintained in a distance table at every node and it is done only for the neighbor node which participates in the active route and not for all the neighbors there by reducing the distance table entries[5]. Once distance between the nodes is calculated, it is then possible to determine whether the nodes are moving apart or moving closer by calculating the difference between the distances. This information along with the time at which 'd' is calculated are kept in the distance table for further processing. Based on this distance information, for each node a new warning range is created as shown in the Figure 3[1].

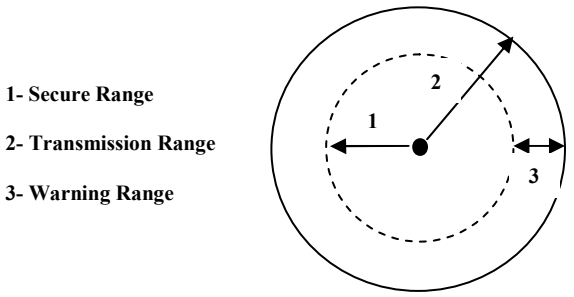

Figure 3. Warning range of the nodes

In the radio propagation models used, it is assumed that each node has a transmission range of 250 meters and an interference range of 550 meters. The warning range is taken between 245 to 250 meters. Whenever a node receives a packet to send, Network Layer (NL) finds the next node i.e, target node, along the path and its distance, time and movement information from the distance table. The relation among these parameters can be approximated in to the following sentences:

Case 1: If the flow is given higher priority among the other flows in the network.

- If the target node is within the secure range then the retry limit is high
- If the target node is in the warning range AND it is coming closer then retry limit is high.
- If the target node is in the warning range AND it is moving away then retry limit is low.
- If the target node is in the warning range AND it is constant then the retry limit is high.
- In any case if the information stored in the distance table is stale then the retry limit is medium.

Case 2: If the flow has a normal priority

- Irrespective of the range where the target node lies, the retry limit is medium.

Based on these approximations NL informs the MAC layer to adjust the retry limit accordingly. A high retry limit is set to double of the default RTS retry limit value , the low retry limit is set to half of the default RTS retry limit value and the medium retry limit is set to the default

RTS retry limit value. If the target node is within the secure range, RTS retry limit is set high as it is obvious that the RTS time out is mainly due to interference and not due to link failure. If the target node is in the warning range and it is moving towards the transmitting node, RTS retry limit is set high as chances of link failure due to target node moving out of the transmission range is almost nil. If the target node is in the warning range and it is moving away from the transmitting node, the retry limit is set to low as the node may go out of the transmission range soon. If the target node is within the warning range and it is constant, the retry limit is set high as the chances of node moving out of the transmission range is less. In any case if the information stored in the distance table is old, then the default behavior will be shown by the protocols.

IV. SIMULATION ENVIRONMENT

Simulation of the PrQoS has been carried out using ns-2 [12] and the results are analyzed. The details of the simulation parameters and performance metrics are given below:

A. Simulation Parameter

In the simulation, AODV is used as routing protocol and IEEE 802.11 DCF is used as the MAC layer protocol. The experiment is conducted using two TCP connections, F1 and F2, with different directions crossing each other. Priority is given to F1 over F2 throughout the experiment. Priority is assigned at the beginning of the data flow and the same priority is kept till the end of the simulation. The 50 MN's move in an area of 300m x 1000m randomly. The data rate of wireless channel is fixed at 2Mbps. The simulation parameters are listed in TABLE 1.

TABLE 1 SIMULATION PARAMTERS

Parameter	Value
Simulation Time	600 sec
Transmission Range	250 m
Interference Range	550 m
Traffic Type	FTP
Payload	1500 bytes
Number of TCP Connections	2
Node Mobility	5-25 m/sec
Pause Time	0
Mobility Model	Random Waypoint
Topology	Nodes are uniformly distributed in the network

B. Performance Metrics

The following metrics are used in various scenarios to evaluate the performance of the PrQoS.

1. *Throughput:* It is defined as the ratio of the number of data packets received by the destination to those sent by the source.
2. *Control Packet Overhead:* It is the total number of control packets (RREQ, RREP and RRER) used during the entire simulation.
3. *Total Route re-discovery attempts:* It is the total number of route re-discovery attempts triggered due to packet drops.

V. RESULTS AND DISCUSSION

I. Throughput

TABLE 2 THROUGHPUT COMPARISION OF ORIGINAL AND PROPOSED MODEL

Node Mobility	Traditional Method		PrQoS	
	F1	F2	F1	F2
5	36	18	61	6
10	26	12	57	14
15	16	21	65	10
20	21	23	62	10
25	22	25	63	8

TABLE 2 shows the per flow throughput of traditional method and PrQoS in Kbps. In the traditional method flows F1 and F2 are given equal priority and for the same reason throughput of F1 and F2 fluctuate, i.e, F1 dominates F2, and F2 dominates F1 in different scenarios. As Priority is given to F1 in PrQoS, throughput of F1 dominates over F2 in all the cases. The main reason for this raise in throughput is increase in RTS retry limit.

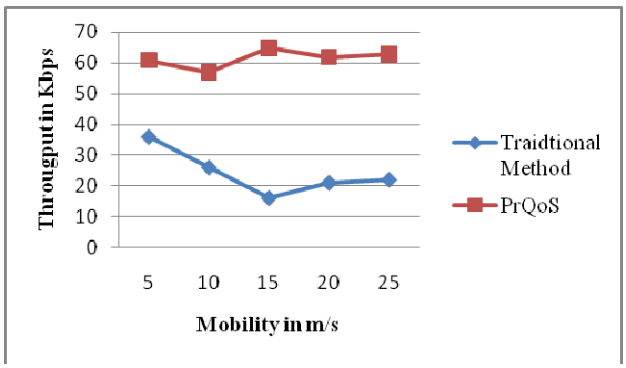

Figure 4. Throughput comparison of F1 with Traditional method and PrQoS

Figure 4 shows the throughput comparison of only F1 between PrQoS and the traditional method. As the mobility increases, throughput of F1 decreases in traditional method. But as PrQoS handles mobility

properly, there is no much fluctuation in throughput curve of F1.

II. Control Packet Overhead

TABLE 3 CONTROL PACKETOVERHEAD COMPARISION

Node Mobility	Traditional Method	PrQoS
5	256372	183748
10	247387	193784
15	263764	183672
20	283784	223784
25	328744	246734

TABLE 3 shows the control packet overhead of both the methods. The results show that the PrQoS reduces the network load since chances of FRF is fewer there by reducing the control packet overhead. It is also one of the reasons for the high throughput in PrQoS. Whereas the traditional method contributes more control packets increasing the network load thereby decreasing the throughput. Figure 5 shows control packet overhead comparison of both the methods. The curve of traditional method raises rapidly because as mobility increases chances of packet drop is more which the node may misinterpret as link breakage and trigger route rediscovery adding extra control packets. Whereas the PrQoS curve rises slowly since it is aware of the reason for the packet drop.

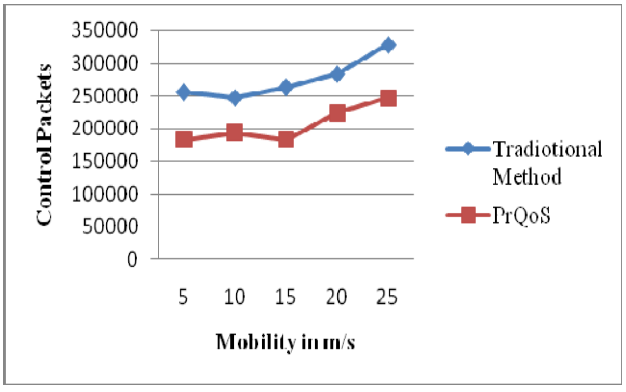

Figure 5 Comparison of Control Packet Overhead

III. Total Route Re-Discovery Attempts

Figure 6 compares the total route rediscovery attempts made by the PrQoS and the traditional method. The graph clearly shows that the PrQoS makes less route re-discovery attempts as chances of FRF is very less. Whereas traditional method makes more attempts because of FRF.

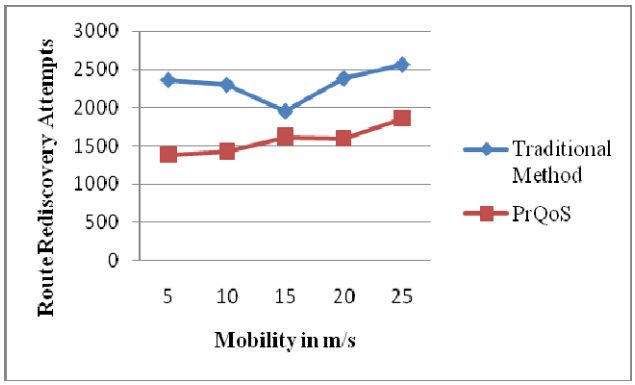

Figure 6 Comparison of Total Route Re-Discovery attempts

VI. Conclusion and Future Work

In this paper MANET is made self aware using a QoS aware cross layer model with *priority of the flow* and *Pr* as the cross layer parameter. The proposed method, PrQoS, improves the throughput of the prioritized flow by increasing the RTS retry limit based on the distance between the target node from the transmitting node where priority is accepted from the user. Through simulation it has been shown that the PrQoS improves the throughput of the prioritized flow, reduces the route re-discovery attempts while decreasing the overall network load in terms of control packets when compared to traditional methods. Since retry limit is increased packet will spend more time in the MAC layer queue which increases the end to end delay. Thus PrQoS is applicable to the applications which are less delay sensitive or non real time applications and require more throughput like file transfer over FTP. Further, we would like to develop a mathematical model to support the proposed framework in near future.

References

[1] Tom Goff, Nael B. Abu-Ghazaleh, Dhananjay S. Phatak, Ridvan Kahvecioglu , " Preemptive Routing in Ad-hoc Networks ", ACM SIGMOBILE , ROME Italy , 2001

[2] Fabius Klemm, Zhenbian Ye, Srikanth Krishnamurthy, Satish K. Tripathu , " Improving TCP performance in Ad Hoc Networks using signal strength based link management ", IFIP persomal and Wireless Communications (PWC), Venice, Italy 2003.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Ning Yang, Ravi Shankar, Jungsik Lee, " Improving Ad Hoc Network Performance Using Cross Layer Information Processing", IEEE International Conference on Communications (ICC),Vol. 4, Pp. 2764-2768,2005.

[4] San-Yung Wang, Jia-Yu Liu,Chun-Chien Huang, Mao-Yuan Kao and Yi-Ho Li, " Signal Strength –Based Routing for Mobile Ad-Hoc Networks ", 19th International Conference on Advanced Information Networking and Applications (AINA'05), IEEE, 2005.

[5] Wooi King Soo, Keat Keong Phang, Teek Chaw Ling, Tan Fong Ang , " Intelligent IEEE 802.11B Wireless Networks MAC layer Diagnostic Controller in Mobile Ad Hoc Networks ", Malaysian Journal of Comupter Science, Vol. 20(2) , 2007.

[6] Faud Alnajjar, Yahao Chen, “SNR/RP Aware Routing Algorithm: Cross-Layer Design for MANETs”, International Journal of Wireless & Mobile Networks (IJWMN), Vol. 1, No 2, November 2009.

[7] Boumedjout Amel, Mekkakia Maaza Zoulikha “Routing Technique with Cross –Layer Approach in AD-Hoc Networks”, Second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT’09),IEEE, PP 313-318, 2009.

[8] Yaser Taj, Karim Faez, “Signal Strength Based Reliability: A Novel Routing Metric in MANET’s “, Second International Conference on Networks Security, Wireless Communications and Trusted Computing.

[9] Vijay T. Raisinghani, Sridhar Iyer “Cross-layer design optimization in wireless protocol stacks“, Elsevier, 2004.

[10] Manjul Walia , Rama Krishna Challa, “ Performance Analysis of Cross-Layer MAC and Routing Protocol in MANETS”, Second International Conference on Computer and Networking Technology, IEEE computer Society , 2010.

[11] J.W.Dawei Man, Lijun Wu, Yu Song “Study of QoS in Cross Layer based Ad-hoc Networks”, International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008), pp. 1- 4,IEEE, 2008.

[12] “The Network Simulator- NS-2”, http://www.isi.edu/nsname/ns/