DESIGN AND ANALYSIS OF AN ADAPTIVE SELFISH SCHEDULING ALGORITHM USING AODV PROTOCOL IN MANET

S.Lakshmi
Research Scholar, Department of ECE,
Sathyabama University
Tamilnadu, Chennai
slakmy@yahoo.co.in

Dr. S.Radha
Professor &Head, Department of ECE,
SSN College of Engineering
Tamilnadu, Chennai
radhas@ssn.edu.in.

Abstract:
Due to dynamic nature of mobile ad-hoc network (MANETs) which results in link breaks and repeatedly changing topology the aim of scheduling algorithm becomes more complex. In this paper we present an adaptive selfish aware queue scheduler for a M/M/1 and M/M/n queuing mechanism to schedule the packets for selfish nodes in mobile ad-hoc networks using AODV as the routing protocol. The performance of this scheduler has been studied using ns-2 simulator and performance can be analyzed by using metrics such as packet delivery ratio, end to end delay, throughput, control overhead and total overhead. This scheduler provides overall improvement under different packet sizes.

Keywords: Ad-hoc networks; selfish nodes; ASSQM; AODV; Trust value.

1. INTRODUCTION

Mobile ad-hoc wireless networks is self organizing and adaptive .This means that a formed network can be deformed on the fly without the need for any system administration [1].The term “ad hoc” tends to imply “can take different forms” and “can be mobile, stand alone and networked”. The mobile nodes in the network dynamically establish route among themselves to form their own network by wireless links , the ad-hoc network is also called the infrastructure less network. All nodes of these networks behave not only as hosts but also routers, forwarding packets to other mobile nodes in the network.
In Ad-hoc networks the frequent changing network topology error prone nature of wireless medium pose many changes like repeated route changes and packet losses. Due to this problem decreases packet delay and decreases throughput. The simplest possible scheduling discipline FIFO(first in first out).The main disadvantage in this technique frequent dropping of packet or may not reach the destination quickly. Hence the option of scheduling algorithm to decide which queued packet to process next will have a important effect on overall performance. The effect on scheduling algorithms on two different protocols are studied AODV and DSR.[2],[5] .AODV is an on demand distance vector protocol and DSR is an on demand non geographic routing p rotocol which are based on the supposition that every node forwards every packet. Some nodes use its services and network except they do not assist with other nodes we call these types of nodes as selfish nodes .There are two techniques Trust based technique and Credit based techniques to detect selfish nodes in MANET. But in this paper we discussed about Trust based technique. Generally network nodes cooperatively distinguish and state the misbehavior of a suspicious node. Such a statement is then transmitted through out the network.

2. RELATED WORK

Different routing protocols for ad-hoc network have been planned in the previous few years. No previous attention is given to all the nodes which will not necessarily fully help to route the packets from source to destination in the network.

In Collaborative Reputation Mechanism or CORE [1] consists of limited explanation that are jointly and circulated to work out the standing value for each node. From this work out value ,nodes are accepted to take part in the network or it can be excluded .Researchers in their work indicate in detail how they should react to negative reputation of nodes and they assist to combine local reputation values to a global reputation value.

Many researchers [13] projected that sustaining a MANET is a cost–intensive movement of a mobile node. Identifying routes and forwarding packets consumes memory energy network band width and local CPU time.

The ADHOC on demand distance vector routing protocol (AODV) is an enhancement of the destination sequenced distance vector routing protocol (DSDV) the benefit of AODV is that it tries to reduce the number of required broadcasts. AODV [2] generates the route on, on demand basis as contrast to maintain a complete list of route for each destination. The procedure of the AODV protocol for mobile ad-hoc networking request make available results for large scale scenarios [3].

Authors [14] tinted that the monitoring algorithm which can distinguish node misbehavior in the term of selfishness. Since the majority of the other mechanism give the suspicious node i.e., selfish node. Some degree of trust, we totally avoided keep away from any trust for the selfish node by relying only an information from the neighboring nodes of the suspicious node and not all the neighboring nodes. Besides the new mechanism can notice the selfish node in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other. In addition authors[15] the MAC selfish behavior has been highlighted and planned extension for the detection system[16] where the receiver allocate a back off value for the sender through both sender and receiver will swap some additional commitment information to check verify that none of the hosts is misbehaving prior to the task.

3. ADAPTIVE SELFISH SCHEDULER QUEUE MANAGEMENT

The major focus in our work environs on demand routing protocol we are using routing protocol is AODV. In AODV protocol route is exposed only when a node wants to send data to another node.
When there are selfish nodes selfish aware scheduling offer privileged weight to data packets when the packets are transmitted from source to the destination in a AODV protocol. Now we consider that only the nodes which acts as a router nodes can be of selfish manner by dropping the RREQ packets.

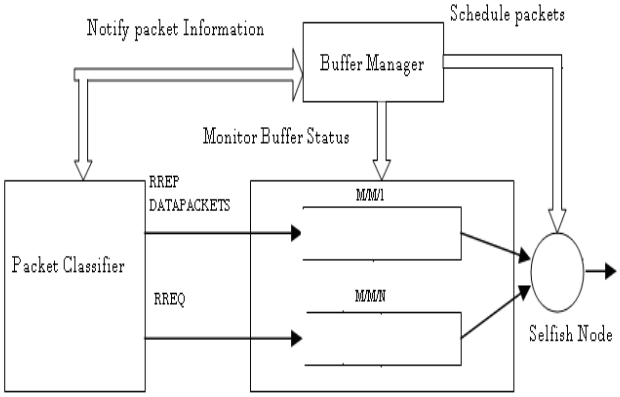

FIGURE 1. ADAPTIVE SELFISH SCHEDULER QUEUE MANAGEMENT SCHEME

In adaptive selfish scheduler queue management scheme as shown in figure 1.we can send the packet either in M/M/1 or M/M/n. In our approach after probing the result of giving main concern to control traffic, we are taking into consideration the effects of setting main concern in data traffic.
In this attitude, we implement two queues M/M/1 and M/M/n queue fashion, if it is RREQ packets are scheduled in M/M/n fashion when the node is detected as a selfish node the scheduler unicasts the data packet. Thus the data packets can be propagated through the selfish node in order to achieve network throughput.
Adaptive selfish scheduler queue management scheme have a scheduler which is enclosed by the packet classifier .The packet classifier differentiates the packet and scheduler monitors the buffer status. Then the scheduler will make decision either to transmit the data packet from M/M/1 or M/M/n. If the average trust value is higher than the trust value then the node is a reliable node otherwise it is a selfish node.

3.1 Algorithm: Detection Of selfish nodes

Notations:
TV1: Trust value calculated for the first past-recent delivery of data packets.
TV2: Trust value calculated for the second past-recent delivery of data packets.
TVC: The current trust value of the node.
ATVC: The average trust value of the node.
SN: Source Node
RN: Intermediate Node
DN: Destination Node
NHN: Next hop Node
1. SN broadcasts RREQ to establish the forward route with DN addresses.
2. SN receives RREP through the reverse route from the DN's
3. If (packets are from DN's or a Reliable Node) {
4. Compute (ATVC = (TV1+TV2)/2)
5. If (ATVC>=TVC) {
6. Route data packet through RN
7. else if (ATVC<TVC){
8. RN is a selfish node
9. Call ASSQM Scheme ( )
10.} do
11. Current RN =NHN
12.}.

3.2 Algorithm: Adaptive selfish scheduler Queue Management scheme

Notations:
TV1: Trust value calculated for the first past-recent delivery of data packets.
TV2: Trust value calculated for the second past-recent delivery of data packets.
TVC: The current trust value of the node.
ATVC: The average trust value of the node.
SN: Source Node
RN: Intermediate Node
DN: Destination Node
NHN: Next hop Node
1. if (ATVC<TVC){
3. RN is a selfish node.
4. Monitor the buffer status.
5. Notify the packet type to the packet classifier.
6. Call higher priority M/M/1 Queue when packet routed is
a data packet and RREP.
7. ELSE if (ATVC>TVC)
8. Enable Call higher priority M/M/n Queue when packet
routed is a RREQ.
9. Forward the RREQ first to the RN
10. do
11. Current RN =NHN
12.}
13. End.

4. SIMULATION AND RESULT

Network Simulator-2 is used for simulations. 50 mobile nodes are randomly placed in a rectangular area 1000 m×1000 m. The wireless channel capacity is 2 Mb/s. Each simulation can run for 50 seconds. Selfish aware queue management mechanisms are applied for varying number of the selfish nodes. A Simple algorithm is compared with ASSQM under the simulated conditions. A Constant Bit Rate (CBR) source is used as the data source for each node. Each source node transmits packets at a certain rate. Packet size is varied from 256 to 1280. The random waypoint model is used. The maximum allowed speed for a node is 10 meters per second. The following performance metrics are used to compare the two scheduling algorithm are the packet delivery ratio, control overhead and total overhead.

For performance evaluation of secure selfish queue management scheme the following metrics are used:

4.1 PACKET DELIVERY RATIO

Packet delivery ratio can be defined as the ratio of the total number of data packets sent to the receivers to the total number of data packets received by the receivers.

4.2 AVERAGE END TO END DELAY

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.

4.3 THROUGHPUT

This is the average number of packets received by the destination node per second

4.4 CONTROL OVERHEAD

Control overhead can be defined as the total number of the control packets transmitted by the sender to the number of data packets delivered to the receivers.

4.5 TOTAL OVERHEAD

Total overhead can be defined as the total number of data packets and control packets transmitted to the total number of the data packets delivered.

TABLE I Simulation Parameters

Parameter	Value	Description
No. of mobile nodes	50	Simulation nodes
Type of channel	Wireless Channel type	Channel Type
Type of propagation	Two Ray Ground	Radio propagation model
Type of network interface	Phy/WirelessPhy	Network interface type
Type of interface Queue	M/M/n and M/M/1 Queue	Interface queue
Type of antenna	Antenna/Omni Antenna	Antenna model
Type of protocol	AODV	Ad-hoc on Demand distance vector
Simulation time	50	Maximum simulation time
Size of the packet	256,512,768,1024,1280bytes	Packet sizes
Terrain dimensions	1000m 1000m	x-dimension of motion y-dimension of motion

5. PERFORMANCE EVALUATION OF SSQM

5.1. PACKET DELIVERY RATIO

Figure 2 shows the comparison between Packet delivery ratio and packet size for two scenarios namely without ASSQM and with ASSQM. From the figure 2, it is clear that packet delivery ratio decreases when there is a selfish behavior but increases when the SSQM is implemented to the range of packet delivered through the selfish nodes.

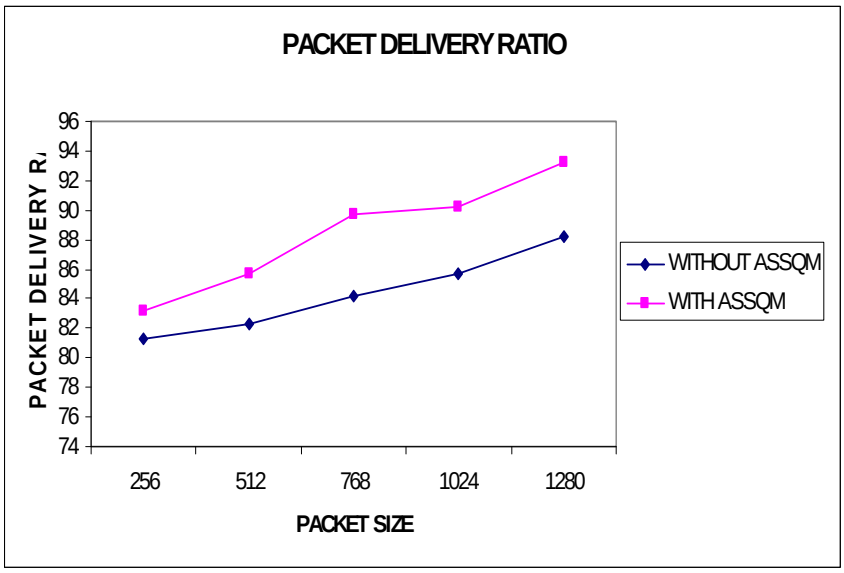

FIGURE 2. PACKET DELIVERY RATIO FOR ASSQM

The chart depicts that the packet delivery ratio decreases during the selfish node behavior can be increased when algorithmic solution is provided . The packet delivery ratio obtained after solution is better compatible with the results of existing literatures.

5.2 END TO END DELAY

Figure 3 shows the comparison between end to end delay and packet size for two scenarios namely without ASSQM and with ASSQM. From the figure, it is clear that end to end increases when there is selfish behavior but decreases when the solution is provided to the range of end to end delay with ASSQM.

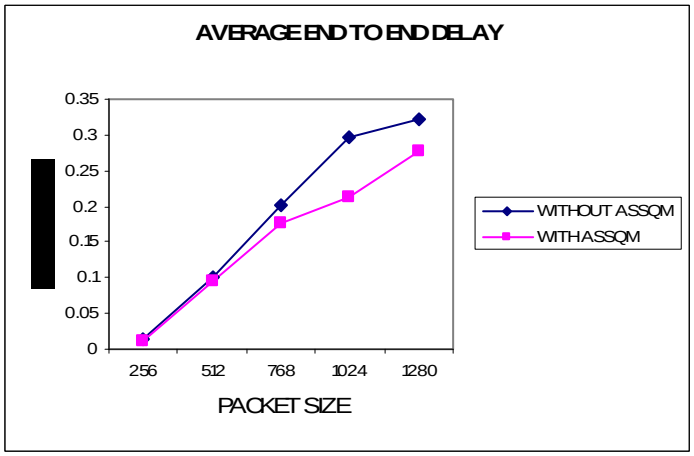

FIGURE 3. END TO END DELAY FOR ASSQM

The chart depicts that the end to end increased during the selfish node behavior can be decreased when algorithmic solution is provided . The end to end delay obtained after solution is better compatible with the results of existing literature.

5.3 THROUGHPUT

Figure 4 shows the comparison between Throughput and packet size for two scenarios namely without ASSQM and with ASSQM. From the figure, it is clear that Throughput decreases when there is attack but increases when the solution is provided with ASSQM.

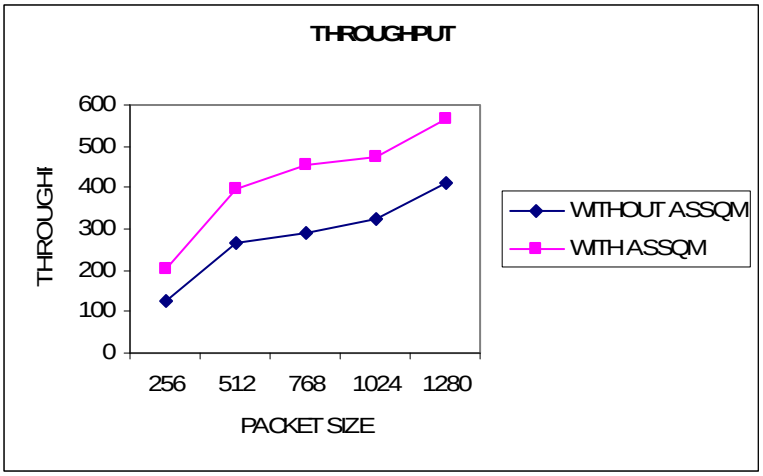

FIGURE 4. THROGHPUT FOR ASSQM

The chart depicts that the end to end increased during the selfish node behavior can be decreased when algorithmic solution is provided to prevent the attack. The end to end delay obtained after solution is better compatible with the results of existing literature.

5.4 CONTROL OVERHEAD

Figure 5 shows the comparison between control overhead and packet size for two scenarios namely without ASSQM and with ASSQM .From the figure, it is clear that control overhead increases when there is selfish behaviour but decreases when the solution is provided with ASSQM.

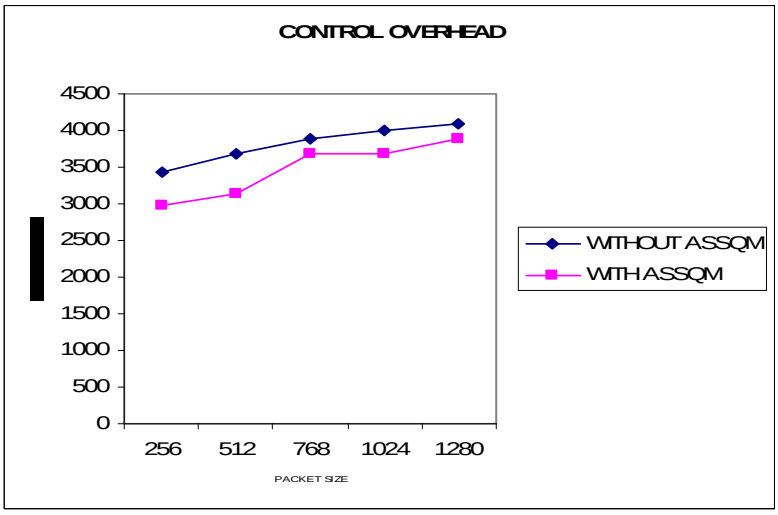

FIGURE 5. CONTROLOVERHEAD FOR ASSQM

The chart depicts that the end to end increased during the selfish node behavior can be decreased when algorithmic solution is provided . The control overhead obtained after solution is better compatible with the results of existing literature.

5.5 TOTAL OVERHEAD

Figure 6 shows the comparison between Total overhead and packet size for two scenarios namely without ASSQM and with ASSQM .From the figure, it is clear that Total overhead increases when there is selfish behavior but decreases when the solution is provided with ASSQM.

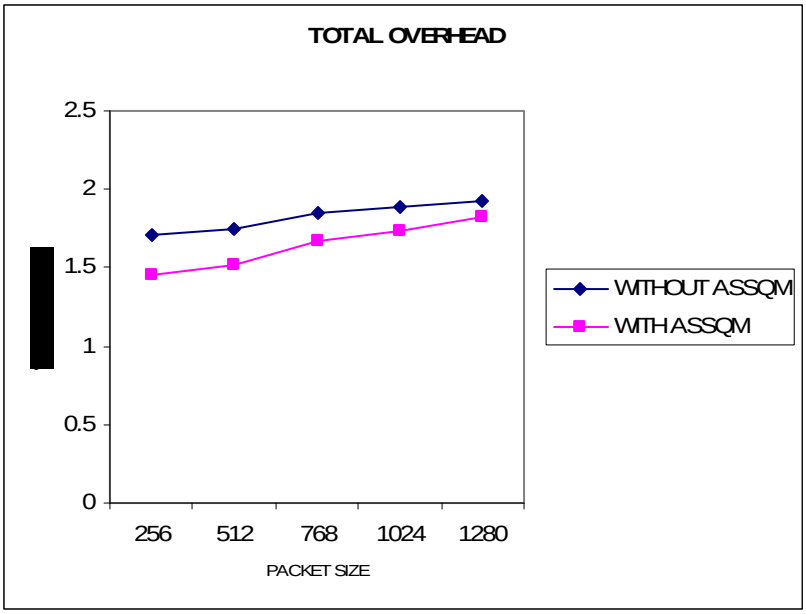

FIGURE 6. TOTALOVERHEAD FOR ASSQM

The chart depicts that the total overhead increased during the selfish node behavior can be decreased when algorithmic solution is provided . The total overhead obtained after solution is better compatible with the results of existing literature.

6. CONCLUSION

In our planned work, an adaptive selfish scheduling algorithm is presented. This paper takes variation of packet size into account when scheduling. By means of simulation studies, the performance of this algorithm is compared with that of simple priority algorithm. Simulation results show that adaptive selfish scheduling algorithm performs better. The scheduling scheme of this paper mainly deals with best-effort traffic, but the quality of service provision is becoming more and more important to the deployment of MANET. In the future, this scheme will be used to support QoS.

References

[1]. Pietro Michiardi and Refik Molva. A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. In Proceedings of the 6th IFIP Communication and Multimedia.Security Conference, Portorosz, Slovenia, September 2002.

[2]. Charles E. Perkins, Elizabeth M. Royer, and Samir Das. Ad Hoc On Demand Distance Vector (AODV) Routing. IETF Internet draft, Mobile Ad-hoc Network Working Group, IETF, January 2002.

[3]. Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In Proceedings of the Tenth Euromicro Workshop onParallel, Distributed and Networkbased Processing, pages 403–410, Canary Islands, Spain, January 2002.

[4]. J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols.In Proceedings of ACM/IEEE MOBICOM, Dallas, TX, October 1998.

[5]. Samir R. Das, Charles E. Perkins, and Elizabeth. Royer. Performance comparison of two on demand routing protocols for ad hoc networks. In Proceedings of the IEEE INFOCOM, Tel-Aviv, Israel, March 2000.

[6]. wih-Chun Hu, Adrian Perrig, and David B. Johnson.riadne: A secure On-Demand Routing Protocol for Ad hoc Networks. In Proceedings of MobiCom 2002,Atlanta, Georgia, USA, September 2002.

[7]. Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad hoc Networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.

[8]. V. R. Ghorpade, Y. V. Joshi and R. R. Manthalkar,"Fuzzy Logic based Trust Management Framework for MANET," DSP Journal, Volume 8, Issue 1,December, 2008.

[9]. S.Anuradha , G.Raghuram, K.E.Sreenivasa murthy,B.Gurunath Reddy, "New Routing Technique to improve Transmission Speed of Data Packets in Point to Point Networks", ICGST-CNIR Journal,Volume 8, Issue 2, January 2009.

[10]. Kai Chen and Klara Nahrstedt, iPass: An Incentive compatible Auction Scheme to Enable Packet Forwarding Service in MANET, In Proceedings of 24th International Conference on Distributed Computing (ICDCS'04), Tokyo, japan, Mar 2004.

[11]. Pandey, A. K. and Fujinoki, H., 2005. Study of MANET Routing Protocols by GloMoSim simulator.International Journal of Network Management; 15(6):pp. 393–410.

[12]. Hu, Y. C., Perrig, A., and Johnson, D. B., 2004. Secure Routing in Ad hoc Networks: Securing Quality-of- Service Route Discovery in On-demand Routing for Ad hoc networks. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04.
[13]. P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In Proc. of CNDS, 2002.
[14]. Demir, C and Comaniciu C, "An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Nodes". Communications, 2007. ICC '07. IEEE International Conference in June 2007.
[15]. TaragFahad &Robert Askwith "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks" ,PGNet 2006.
[16]. [P. Kyasanur and N. Vaidya. Selfish MAC layer misbehavior in wireless networks. IEEE Transactions on Mobile Computing., April 2004.