Selfish Aware Context based Reactive Queue Scheduling Mechanism for MANETs

J.Sengathir
Research Scholar
Dept., of CSE
Pondicherry Engineering College,
Pondicherry

R.Manoharan
Associate Professor
Dept., of CSE
Pondicherry Engineering College,
Pondicherry

ABSTRACT

The Selfish Aware Reactive Queue Scheduler Mechanism (SARQSM) requires a high degree of interaction between the packet differentiator, cache manager and the scheduler queue which forms the integral component of all mobile nodes participating in an ad hoc environment. This reactive queue scheduling scheme performs better when deployed in a scenario where non co-operating i.e selfish nodes are present as the intermediate routers of information in the network. However when SARQSM is implemented in the MANET environment, it provides a reactive and lightweight solution with respect to memory and battery life. To the best our knowledge, a mechanism for packet scheduling based on context like SARQSM is not available in the existing literature. The performance of SARQSM is studied using ns-2 simulator by varying the number of selfish nodes and mobile nodes with respect to the evaluation parameters namely Packet Delivery Ratio, Control Overhead, Total Overhead, Throughput and Packet Latency.

General Terms

MANETs, Reactive Solution, Packet Delivery Ratio, Control Overhead, Total Overhead, Throughput and Packet Latency

Keywords

Selfish Behavior, SARQSM, Context awareness, Queue Scheduler

1. INTRODUCTION

Mobile ad hoc networks always suffer from the limitation of possessing scarce amount of resources which has to be shared by all the mobile nodes in the topology. The optimal utilization of the scarce resources is a critical issue that has to be considered. Many effective resource management schemes were proposed for achieving this objective [1]. One of the similar resource management scheme is the packet scheduling mechanism that allocates bandwidth among multiple paths effectively [2].The packet scheduling algorithm mainly aims in eradicating the critical issues that are related with multiple sessions that a single node has to handle while they share a common wireless channel [3]. Other scheduling methodology considers different issues that are distinct for MANETs namely dynamic topology, multi-hop relay and resource sharing with the help of selfish consciousness [4]. A mobile node may misbehave due to the feature of open structure as well as based on available energy [5]. The terminology "Context aware" in our work refers to the knowledge about the kind of behavior that the selfish nodes perform based on dropping either the control packets or the data packets based on residual energy [6]. The term "Selfish" refers to an individual mobile node that may deny cooperating with the other nodes participating in packet relay but tries to benefit from other nodes in terms of resources [7]. Thus the selfish nodes maintain the communication with the nodes to which it wants to send the packets whereas it refuses to cooperate while routing to some other nodes that it has no interest in. Thus they either drop data packets are refuse to transmit routing packets that has no interest in.

The node is said to exhibit a selfish behavior [8], when it does not participate in active communications with the other nodes by turning its power off, when it does not forward the broadcasted RREQ packets during forward routing, when it does not forward the RREP packets during Reverse routing, when it Re-broadcasts RREQ, forward RREP on reverse route but it does not co-operate to relay data packets. When it does not deliver Route Error (RERR) packets when data packets are delivered but there is no route to the destination [9]. When it partially drops data packets. This strategy in particular can be used to detect selfish nodes and mitigate them.

The communication in MANETs depends on the co-operation between nodes [10]. Thus, the nodes have to interact with each other to guarantee the correct routing establishment strategies and routing information [11]. However, this reliability may be misused by the other participating nodes. The Classical approach to establish security in network is based on authentication through cryptography. However, this is not adequate to solve the issues arising from the node misbehaviors in mobile ad hoc networks (MANET). Hence, providing securing MANET against node level misbehavior is one of the major issues for the researchers.

The remaining part of the paper is organized as follows. In section 2, We present some of the existing works available in the literature. The elaborate explanation of the proposed Context Aware Reactive Queue Scheduling and the algorithm of the proposed schema when deployed in the routing of the protocol, AODV is presented in section 3. The experimental analysis and the Simulations results are presented in section 5 and 6. Section 6 concludes the paper.

2. RELATED WORK

From the recent past, various routings protocols for Ad-hoc Networks are proposed. But some of the protocols do not support the Co-operation of nodes while routing the packets from source to destination. As proposed by L. M. Feeney [12] mobile devices work on battery energy. Hence, the energy consumed for each communication incurs a cost and importance. So, assuming all the nodes to perform the operation forwarding data without any own benefits, while

consuming its own battery power is infeasible. Therefore some nodes refuse to relay packets hence the efficiency of the network decreases.

A Routing protocols designed based on Auction [13] for ad hoc network does not consider the presence of selfish nodes in an ad hoc network but assumes that all the nodes in the network will co-operate with each other and does accomplishes the objectives of routing. But, routing a packet that belongs to the neighbor nodes consumes large amount of Router nodes energy. This energy loss is considered to be vital energy. This energy loss is considered to be vital for mobile nodes because MANET's always contain scarce resources, when the mobile nodes in the network belongs to different authorities, there is a lack of common objectives, which may be includes selfishness. For this reason, nodes in a ad hoc networks may behave in a selfish manner to save their resource, which any threaten the proper functioning of networks.

On other hand, the author of [14] proposed that supporting a MANET is a expensive activity for all mobile nodes. Detection activity and forwarding of packet could consume more bandwidth, memory space and power. Hence, there is a strong adherence for a node to deny a packet routing to other while a same instance use the services to forwarding the packet.

The authors of [15] proposed that the monitoring algorithm (PCMA) could detect any node misbehaving with to selfish node i.e., non –co-operating node. Since almost the other mechanism provide the selfish node, a degree of reputation and only the neighboring node can send or receive data from or to the misbehaving node. This every aware approach. Furthermore, this mechanism could detect and selfish node a rapid rate.

Then, the authors of [16] portrayed the selfish node misbehavior at the MAC layer level and the other proposed version of detection mechanism [17] was implemented under the conclusion that at lest one parties involved in routing is trusted. Then strategy assigns a back off value for the sender from the receiver. How ever, both the source and receiver can exchange extra commitments information to ensure randomness and to verify that none of them are misbehaving. The reputation management system keeps track of any defected maliciousness.

Finally, the authors of [18], proposed a selfish aware scheduling that provides a high priority to data packet when compared to control packets, when the packets are forwarded through the selfish nodes. The type of queue used was the fair weighted queue and totally two queues are used one for storing the data packets and the other one storing the control packets.

3. CONTEXT AWARE REACTIVE SELFISH QUEUE

In our proposed work, the main focus is on how the packets are relayed from one node to another node, only when the route is discovered in a reactive Ad hoc On demand distance vector protocol. The routing protocol used in this study is the AODV protocol.

In context aware selfish queue scheduling mechanism, the higher priority is triggered based on the need of the packet to be relayed from the source to the destination. The proposed is based on the assumption that only the forwarding nodes are considered to exhibit selfish behaviour.The characteristic feature of the proposed work is that the packet needs to traverse, with the maximum potential so as to reach its destination quickly and with the least queue cost. The context aware reactive selfish scheduler relays the packets in weighted fair queuing fashion. We have devised a scheduling algorithms by using Energy metrics, considering fairness, and applying the multiple roles of nodes as both routers and data sources.

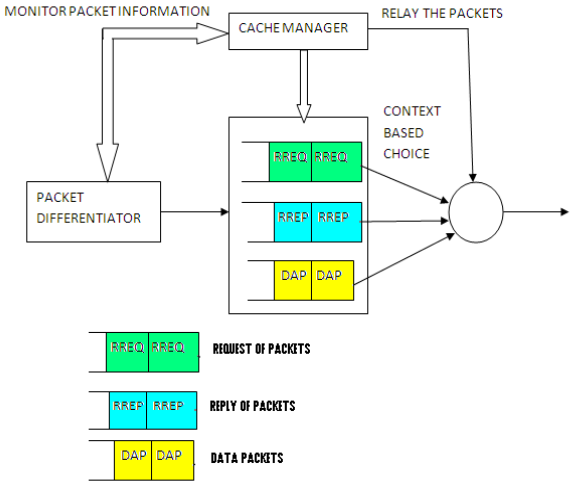

Figure 1. **Context Aware Reactive Selfish Queue Schelduler**

In the proposed mechanism the energy of each node is computed. For each node a threshold value is set then set as $ET_{\text{received channel value.}}$ If $ET_{\text{relayed channel value}}$ when compared with the received channel is found to be less. Then the node is identified a malicious node. Then CARSQR is incorporated, in this technique the node is monitored using context aware technique. In which the node is monitored based on three queue schedulers namely RREQ, RREP and DAT. If the node is found to transmit less than the threshold value set for the above parameters. The parameter which has low threshold value will be given high priority. Thus the normal functioning of the network is recovered to a maximum extend even though the presence of selfish nodes.

3.1 Algorithm: Detection of selfish nodes in Reactive Queue Scheduler

Notations

CMp: computed maximum energy needed for a mobile node.
ACp: Actual energy present in the node
E_{SCRN} : Energy level of the source node
Enext_hop(i) : Computed next _hop energy level
E-thresh: energy threshold valve for each node
SRCN: Source node
ET_{value} : Threshold value of each node
E_{Pack_Trans} : Energy of packet transmitted
DSTN: Destination node

1. SRCN establishes the forward route to DSTN with help of RREQ packets
2. Initially $E_{SCRN} = E_{Pack\_Trans}$
3. Next compute $E_{next\text{-}hop(i)} = E_{pack\text{-}receive} + E_{control\ packets}$ for all the nodes in the network
4. Set $E_{next\text{-}hop(i)}$ for each node
5. Compute $ET_{value} = E_{next\text{-}hop(i)}$ * no of packets transmitted
6. Set Threshold channel energy value = computed ET_{value}
7. Multiply the number of packets passed with ET_{value} for channel with respect to the forwarding node.
8. Then the ET_{Value} is calculated for each node.
9. $ET_{received\ channel\ value}$ = energy of previous channel * no of packets received
10. $ET_{relayed\ channel\ value}$= energy of current channel * no of packets transmitted
11. If ($ET_{received\ channel\ value} > ET_{relayed\ channel\ value}$)
12. Node is selfish
13. Call Context aware queue scheduler()
14. Else
15. Node is genuine

Context aware reactive Selfish Queue scheduler Management scheme consists of a scheduler which coordinated by the packet Differentiators and the Cache manager. The packet differentiators predict whether the packet to be transmitted is a data packet or a control packet. The scheduler monitors the buffer status so that it can make decisions to forward a data packet first, RREQ or a RREP control packet first. The difference between the residual power of incoming channel of the node and the outgoing channel of a node are computed and the information is passed to the cache manager to detect selfish behavior of the node and to trigger the type of queue to be initiated to relay the packet through the node based on context.

3.2 Algorithm: Context Aware Reactive Selfish Queue Scheduler Mechanism

1. If ($ET_{received\ channel\ value} > ET_{relayed\ channel\ value}$)
2. Node is selfish
3. $\partial = ET_{received\ channel\ value} - ET_{relayed\ channel\ value}$
4. if ($\partial <= 0$)
5. Context aware queue scheduler is enabled
6. Monitor the selfish node
7. If (RREQ < RREQ threshold)
8. RREQ priority is set high
9. RREQ is transmitted to enable transfer of data
10. If (RREP < RREP threshold)
11. RREP priority is set high
12. RREP is transmitted to enable transfer of data
13. If (DATA < DATA threshold)
14. DATA priority is set high
15. DATA is transmitted to enable communication
16. If ($ET_{received\ channel\ value} >= ET_{relayed\ channel\ value}$)
17. Node is genuine

Initially the energy of the received channel is calculated and then followed by the energy of the relayed channel of the node. Then results are compared, when the relayed value is found to be less when compared to that of the received channel. Then the node is found to be malicious and context aware queue scheduler is enabled. The cache manager monitors the node in which part of the route established or data threshold level drops. That scheduler will be enabled and the retransmitted to regain the safer transmission in network.

3.3 Computation of Energy for Transmitting and Receiving a Unit packet

3.3.1 Calculation for Data Packets.

Fixed Packet length = 512 bytes

The Constant bit rate = 250 kbps

The total packet size = Preamble length + PLCP header +MAC header + IP header + Payload = ((144 +48) + (28x8) + (20x8) + (512x8)) bits

The preamble and PLCP header are sent at 1 Mbps where as the remaining pair are sent at 11 Mbps.So we have 144 + 48 bits been sent at 1 Mbps.(The default values of ns version is used)

Hence,

Single Packet transmission time = $144 + 48/ 1x\ 10^6$
$= 192/10^6$
= 0.193 ms

But when 8 x 560 bits of information are sent at 11 Mbps, then,

Single packet transmission time = $8 \times 512/ 11 \times 10^6$
$= 4096/ 11 \times 10^6$
= 0.403 ms.

Hence, aggregate transmission time for
Unit Packet = 0.193+0.403 = 0.596 ms

3.3.2 Calculation for Control Packets:

Packet size = 14 bytes

Constant source bit rate = 250 Kbps

Total Unit packet size = Preamble length + PLCP header length + Actual packet length
= 144 + 48 +14 x 8
= 0.304 ms.

3.4 Computation of Energy required by each node

The power used for transmission and reception is set as 1.3W and 0.9W respectively as denoted in [19, 20]

Thus, the energy tuples for unit packet are,

$E_{pack\text{-}trans}$ = 0.767 ms

$E_{pack\text{-}receiv}$ = 0.531 ms

$E_{control\ –trans\ =}$ 0.3952 ms

$E_{control\ –receiv\ =}$ 0.274 ms

3.5 Illustration of the Proposed Work

Consider the Group of nodes in a AODV protocol

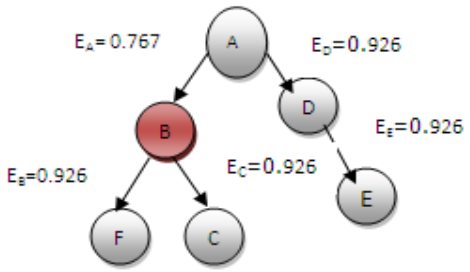

Figure 2. **Computation of Energy for Mobile nodes in AODV**

Initially the energy levels of each node are calculated .The energy level of node A is computed to be E_A= 0.767 and other nodes energy is found to be 0.926. The channel level computation needs to be calculated to find the genuine of the node. It follows the task of the energy of receiving multiplied by the no of packets transmitted and the relayed channel is calculated in the same manner. If the relayed channel value is found to be comparatively lesser than the forwarded channel value. The node is identified as selfish node, the context aware queue scheduler is incorporated and then selfish node is made to retransmit based on the priority level.

4. SIMULATION AND RESULTS

The Network Simulator used for our study is ns-2. The Simulation environment consists of 50mobile nodes, which are placed in a random fashion about a terrain area of 1000m x 1010m. The Simulation time for the study is 50seconds and 2 Mb/s is the wireless channel capacity set. This Selfish based on Reactive queue Scheduler Mechanisms are deployed for varying number of selfish nodes. A Pre-emptive algorithm is compared with SARQSM.

4.1 Performance Metrics

For evaluating the performance of the context aware Reactive selfish queue scheduler Mechanism, the following metrics are considered

4.1.1 Packet Delivery Ratio

Packet delivery Ratio may be considered as the ratio of total number of data packets received by the destination from the source to the actual amount of packets destined from the source towards the destination.

4.1.2 Control Overhead

Control overhead may be expressed as the number of control packets needed for route discovery divided by the number of data packets sent after route discovery.

4.1.3 Total Overhead:

Total overhead may be expressed as the ratio of packets transmitted (i.e.,) comprising of both data packet and control packets to the data packet delivered to the sink.

4.1.4 Throughput

Throughput may be expressed as the aggregate rate of successful packet delivery from the source node to the sink node in a network

4.1.5 Packet Latency

Packet Latency may be expressed as the time required by the packets to reach the destination nodes from the source node.

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 antenna	Antenna/Omni Antenna	Antenna model
Type of protocol	AODV	Ad-hoc on Demand distance vector
Simulation time	50	Maximum simulation time
Packet size	512bytes	Data packet size

5. PERFORMANCE ANALYSIS OF SARQSM

5.1 Performance Evaluation of SARQSM based on selfish nodes

5.1.1 Packet Delivery Ratio

Figure 3 depicts the performance of SARQSM with respect to Packet delivery ratio by varying the number of selfish nodes for three mechanisms namely with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the packet delivery ratio increases when compared to the SSQM Strategy.

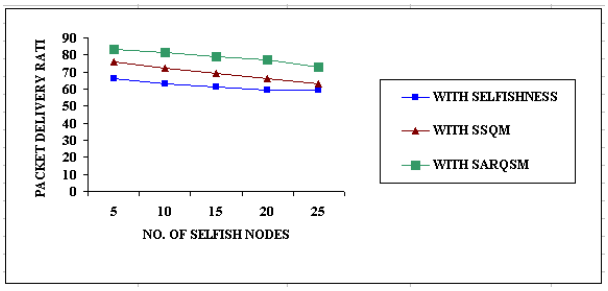

Figure 3 .Evaluation of Packet Delivery Ratio based on selfish nodes

From the graph, it is clear that the proposed scheme shows an increase of 18% when compared to the existing scheme SSQM.The packet delivery ratio determined after the implementation of solution is better when compared with the outcomes of existing literatures.

5.1.2 Control Overhead

Figure 4 depicts the performance of SARQSM with respect to Control Overhead by varying the number of selfish nodes for nodes for three mechanisms namely with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the Control Overhead decreases when compared to the SSQM Strategy.

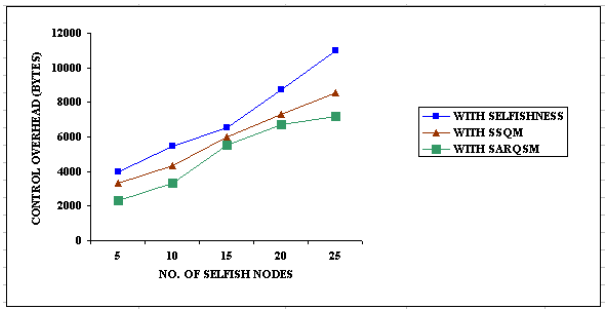

Figure 4. Evaluation of Control Overhead based on selfish nodes

From the graph, it is clear that the proposed scheme shows a decrease of 24% in Control Overhead when compared to the existing scheme SSQM.The decrease in Control Overhead determined after the implementation of solution is better when compared with the outcomes of existing literatures.

5.1.3 Total Overhead

Figure 5 depicts the performance comparison between the number of Selfish nodes and Total Overhead for three mechanisms namely with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the total Overhead decreases when compared to the SSQM Strategy.

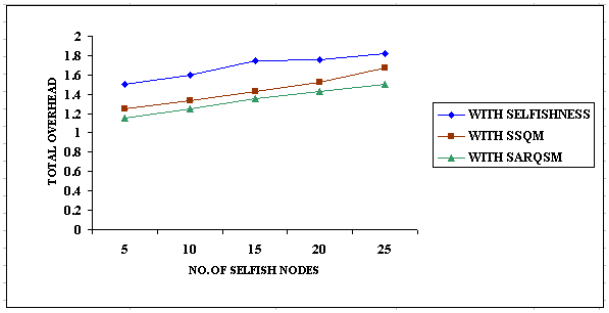

Figure5. Evaluation of Total Overhead based on selfish nodes

From the graph, it is clear that the proposed scheme shows a decrease of 21% in total overhead when compared to the existing scheme SSQM. The decrease in Total Overhead determined after the implementation of solution is better when compared with the outcomes of existing literatures.

5.1.4 Throughput

Figure 6 depicts the performance of SARQSM with respect to throughput by varying the number of selfish nodes for three mechanisms namely with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the throughput increases when compared to the SSQM Strategy.

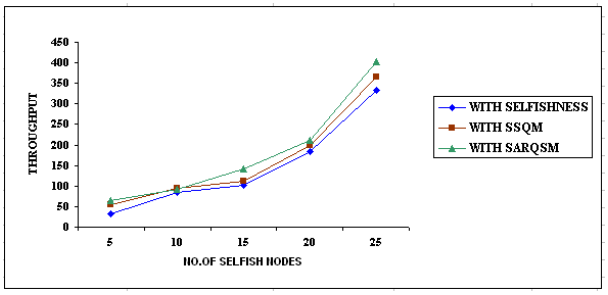

Figure6. Evaluation of Total Overhead based on selfish nodes

From the graph, it is clear that the proposed scheme shows an increase of 16% in throughput when compared to the existing scheme SSQM.The throughput determined after the implementation of solution is better when compared with the outcomes of existing literatures

5.1.5 Packet Latency

Figure 7 depicts the performance comparison between the number of selfish nodes and packet latency for three mechanisms namely with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the packet latency decreases when compared to the SSQM Strategy.

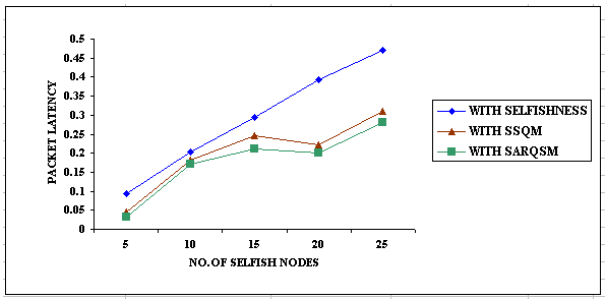

Figure7. Evaluation of Total Overhead based on selfish nodes

From the graph, it is clear that the proposed scheme shows a decrease of 31% in packet latency when compared to the existing scheme SSQM. The decrease in packet latency determined after the implementation of solution is better when compared with the outcomes of existing literatures.

5.2 Performance Evaluation of SARQSM by varying the number of Mobile Nodes.

5.2.1 Packet Delivery Ratio

Figure 8 depicts the performance of SARQSM with respect to Packet delivery ratio by varying the number of mobile nodes for four mechanisms namely without selfishness in AODV protocol with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the packet delivery ratio increases when compared to the SSQM Strategy.

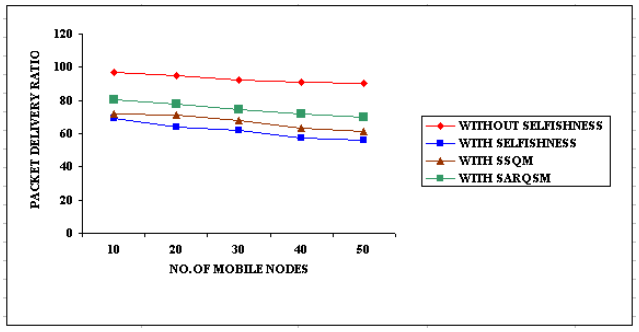

Figure.8. Evaluation of Packet Delivery Ratio based on Mobiity

From the graph, it is clear that the proposed scheme shows an increase of 21% when compared to the existing scheme SSQM.The packet delivery ratio determined after the implementation of solution is better when compared with the outcomes of existing literatures.

5.2.2 Control Overhead

Figure 9 depicts the performance of SARQSM with respect to Control Overhead by varying the number of mobile nodes for four mechanisms namely without selfishness in AODV protocol with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the Control Overhead decreases when compared to the SSQM Strategy.

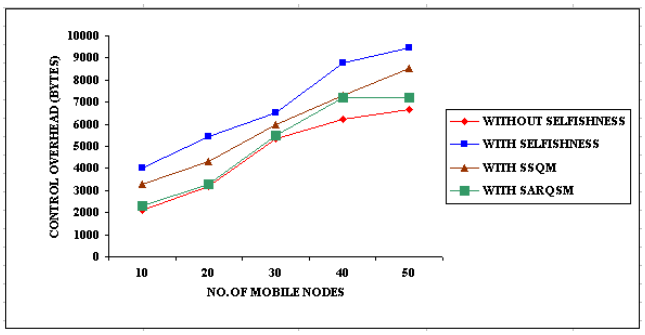

Figure.9. Evaluation of Control Overhead based on Mobile nodes

From the graph, it is clear that the proposed scheme shows a decrease of 19% when compared to the existing scheme SSQM.The Control overhead is marginally reduced after the implementation of solution when compared with the outcomes of the solutions present in the existing literatures.

5.2.3 Total Overhead

Figure 10 depicts the performance of SARQSM with respect to Total Overhead by varying the number of mobile nodes for four mechanisms namely without selfishness in AODV protocol with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the Total Overhead decreases when compared to the SSQM Strategy.

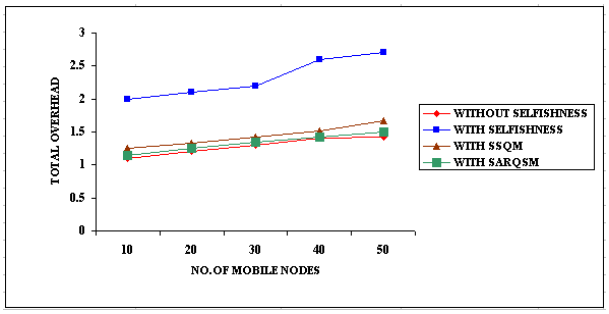

Figure.10. Evaluation of Control Overhead based on Mobile nodes

From the graph, it is clear that the proposed scheme shows a decrease of 23 % when compared to the existing scheme SSQM.The Total overhead determined is marginally reduced after the implementation of the solution when compared with the outcomes of the solutions present in the existing literatures.

5.2.4 Throughput

Figure 11 depicts the performance of SARQSM with respect to throughput by varying the number of mobile nodes for four mechanisms namely without selfishness in AODV protocol with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the throughput increases when compared to the SSQM Strategy.

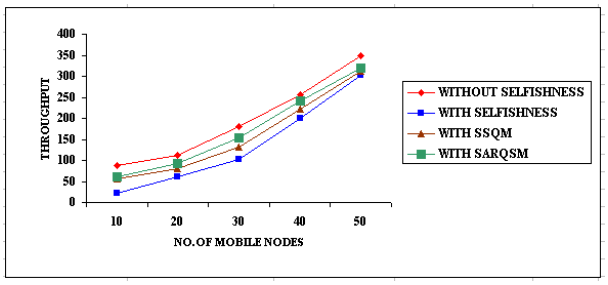

Figure.11. Evaluation of Throughput based on Mobile nodes

From the graph, it is clear that the proposed scheme shows an increase of 26% in throughput when compared to the existing scheme SSQM.The throughput determined after the implementation of solution is better when compared with the outcomes of existing literatures

5.2.5 Packet Latency

Figure 12 depicts the performance comparison between the number of mobile nodes and packet latency for four mechanisms namely without selfishness in AODV protocol with Selfishness in AODV protocol, With SSQM and with SARQSM. From the figure, it is obvious that when SARQSM is deployed the packet latency decreases when compared to the SSQM Strategy.

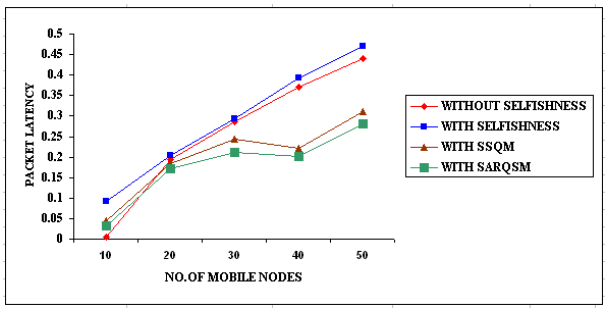

Figure.12. Evaluation of Packet Latency based on Mobile nodes

From the graph, it is clear that the proposed scheme shows a decrease of 22% in packet latency when compared to the existing scheme SSQM. The decrease in packet latency determined after the implementation of solution is better when compared with the outcomes of the existing literature.

6. CONCLUSION

In this paper, a Context aware reactive scheduling methodology is presented which is analyzed based on the number of nodes and the number of selfish nodes present in the scenario with respect to performance metrics like packet delivery ratio, control overhead ,total overhead, throughput and packet latency. This proposed scheme takes into account of the behavior of nodes during packet scheduling. Through simulation, the performance of this strategy is compared with that of existing SSQM algorithm. A simulation result predicts that this algorithm performs better. The proposed scheduling mechanism mainly focuses on the traffic, but has least importance to QoS. Since QoS is one of the major key parameter in the implementation of MANET. In the near future, this strategy can be made to support QoS.

7. REFERENCES

[1] 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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Yih-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] 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.

[9] 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.

[10] 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*.

[11] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *Proc. of CNDS*, 2002.

[12] L. M. Feeney, "*Energy Efficient Communication in Ad Hoc Wireless Networks*,"Computer and Network Architectures Laboratory, Swedish Institute of Computer Science, 2003.

[13] 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 June 2007.

[14] TaragFahad &Robert Askwith *"A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks"* ,PGNet 2006.

[15] P. Kyasanur and N. Vaidya. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing.*, April 2004.

[16] M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva and Mohamed Eltoweissy. "*A Reputation-based Mechanism forIsolating Selfish Nodes in Ad Hoc Networks*", In Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems:Networking and Services 2005.

[17] A. C´ardenas, S. Radosavac, and J. S. Baras. Detection and prevention of MAC layer misbehavior for ad hoc networks. In *Proc. of SASN*, October 2004.

[18] Lakshmi.S,Radha.S,"Selfish aware queue scheduler for packet scheduling in MANET",In Proceedings of Recent trends in Information technology(ICRTIT),2012

[19] L. M. Feeney, M. Nilsson, "*Investigating the energy consumption of a wireless net-work interface in an ad hoc networking environment*," in Proceedings of IEEE In-focom, April 2001.

[20] L. M. Feeney, M. Nilsson, "*Investigating the energy consumption of a wireless net-work interface in an ad hoc networking environment*," in Proceedings of IEEE Infocom, April 2001.