Modeling, Implementation and Performance Analysis of Selfish Behavior in Enhanced Selfish- DSR Routing Protocol of MANET

Rooshabh Kothari
Deptt. Of CSE
Arya Institute of Engg. & Technology
Jaipur, India

Deepak Dembla
Deptt. Of CSE
Arya Institute of Engg. & Technology
Jaipur, India

ABSTRACT

The key confront in Mobile Ad hoc Network (MANET) is its dynamic nature, which itself carries security measures. The Mobile Ad hoc Network is multi-hop in nature where nodes are required to perform communication activity for end to end connectivity which is being used for transferring data packets and thereby spending its resources. A selfish node is one that tries to consume the network resources for its own benefit but is unwilling to spend its own resource for others. If such selfish behavior continues among nodes in network, it may be harmful for network by creating disorder. In this paper, Proposed ES-DSR (Enhanced Selfish DSR) is implemented on NS-2 and results shown significant improvement over original DSR in terms of performance evaluation of network. In proposed protocol, as mobility increases, there is significant decrease in communication overhead that is almost about 50% than DSR protocol which is one of the main beneficial point of our proposed protocol and also as speed increases end to end delay is also decreases almost 35% than DSR, Throughput is also increasing but marginally compared to DSR protocol and packet delivery ratio is also increasing due to less no. of connection breakage between nodes .So by experimental results it is found that in dense mobile ad hoc networks where route breakage is frequent and also communication overhead increases in DSR. But, by selfish behavior of some nodes in proposed protocol communication overhead reduces. Because of high density the negative effect of selfish nodes reduces overheads in ES-DSR and is also indirectly results in saving nodes battery power also. In this paper it has been proved that security attacks are somewhat beneficial to mobile adhoc network.

Keywords

DSR, ES-DSR (Enhanced Selfish DSR), Secured Routing, Selfish nodes, Ad hoc network, security, selfish behavior

1. INTRODUCTION

In this modern era the technology cannot work efficiently in that places where there is no permanent infrastructure. A collection of wireless nodes performing a communication based on self configuring each other is known as a mobile ad hoc network (MANET). Thus it is Easy and fast deployment of wireless networks which will be expected by the future generation wireless systems. This fast network deployment is not possible with the existing structure of present wireless systems. Due to changing Dynamic nature of MANETs requires execution of proper routing protocols, which should be malleable to frequent changes in network topology and the nodes should be able to exchange information regarding topology changes to establish routes. These types of such frequent changes very often bring about the security issues in ad hoc networks [1][2].

Wireless networks can be classified in two types: - infrastructure network and infrastructure less (ad hoc) networks. Infrastructure network consists of a network with fixed and wired gateways. A mobile host interacts with a bridge in the network (called base station) within its communication radius [2]. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it.

Routing protocols are essential for a MANET in order to find out network topology and build routes, MANET routing protocols in spite of frequent topology changes caused by nodes' mobility, they are intended to dynamically maintain routes between any pair of communicating nodes. The main dilemma of all the current ad hoc routing protocols is that they trust all nodes and believe that they behave properly; therefore they are in danger to attacks launched by misbehaving of selfish nodes [7]. According to nodes misbehave because they are malfunctioning, or selfish. Malfunctioning nodes are simply suffering from hardware failure or software errors. Selfish nodes can agree to forward packets on behalf of other nodes but silently drop the packets in attempt to save their resources.

Structure of paper is as follows: section 2 discusses related work; Section 3 is about Problem Statement; Section 4 presents Proposed algorithm ES-DSR and its implementation; Section 5 presents about Experimental setup; Section 6 presents Result Analysis of DSR and ES-DSR; Section 7 Density based Performance Evaluation of DSR and ES-DSR; Section 8 presents Conclusion and Section 9 presents future work.

2. RELATED WORK

Routing is the take steps of moving information from a source to a destination in an internetwork. At least one intermediate node within the internetwork is encountered during the transfer of information. Basically two activities are involved in this concept: determining optimal routing paths and transferring the packets through an internetwork. The transferring of packets through an internetwork is called as packet switching which is straight forward, and the path determination could be very complex.

Routing protocols use several metrics as a standard measurement to calculate the best path for routing the packets to its destination that could be number of hops, which are used by the routing algorithm to determine the optimal path for the packet to its destination. The process of path determination is that, routing algorithms find out and maintain routing tables, which contain the total route information for the packet. The information of route varies from one routing algorithm to another. The routing table's are filled with entries in the routing table are ip-address prefix and the next hop [7].

G. Lavanya and A. Ebenezer Jeyakumar shown that DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades routing performance.

Shailendar Gupta, C.K.Nagpal and Charu single proposed that as no. of selfish nodes increases quality of service becomes poorer and poorer and also throughput comes down to nearly 50 % as its peek and also percentage of packet drop gets nearly 60%.

Main Problem in behavior of selfish nodes in mobile adhoc network is that, it drops route request and route reply packets so end to end delay increases and this can lead to more consumption of battery power of nodes, so it is affecting harmfully to performance parameter when selfish behavior goes beyond limit in mobile ad hoc network.

Dynamic Source Routing (DSR)

DSR [6] is an on-demand routing protocol which is based on source route approach. The Dynamic Source Routing (DSR) [10] is a reactive unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt. In this approach, each packet carry in its header the source route which contains the complete, ordered list of nodes through which the packet must pass. The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node ***S*** wishing to send a packet to a destination ***D*** obtains a source route to ***D***. To perform a Route Discovery, the source node ***S*** broadcasts a ROUTE REQUEST (RREQ) packet that is flooded through the network in a controlled manner and is answered by a ROUTE REPLY (RREP) packet from either the destination node or another node that knows a route to the destination. To reduce the cost of Route Discovery, each node maintains a cache of source routes it has learned or overheard. Route Maintenance is the mechanism by which a packet's sender ***S*** detects if the network topology has changed. When Route Maintenance indicates a source route is broken, ***S*** is notified with a ROUTE ERROR (RERR) packet. The sender ***S*** can then attempt to use any other route to ***D*** already in its cache or can invoke Route Discovery again to find a new route.

Route Discovery

In route discovery mechanism the source node broadcast request packet. The route request packet in addition to address of original initiator of request and target of request contain route record, which records sequence of hops taken by route request packet as it is propagated through ad hoc network during route discovery.

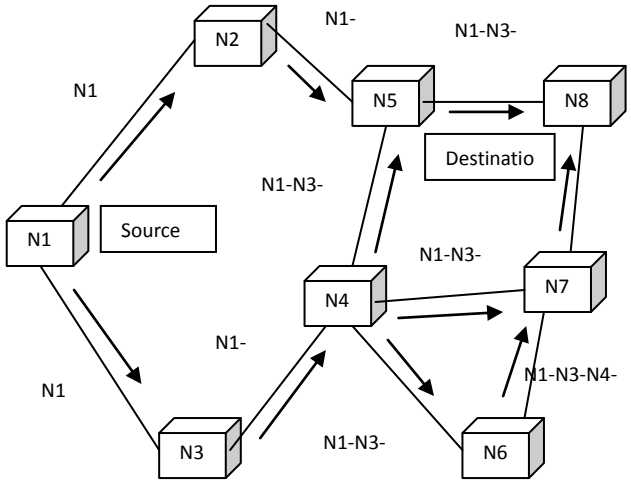

Figure 1. : DSR Route Request

Route Maintenance

Each intermediate node receiving this packet broadcasts it till some node that has route to destination receives it. The node send back route reply packet with route record appended with path to destination from it. Route maintenance monitors correct operation of route in use [6]. When route maintenance detects a problem with route in use. It re-initiates route discovery phase.

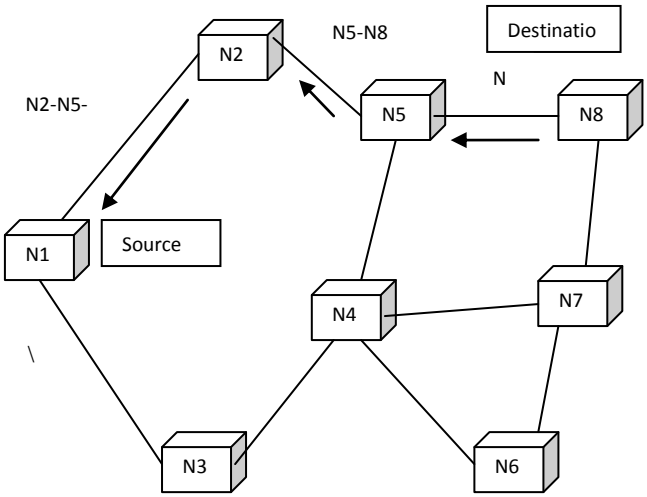

Figure 2. : DSR Route Reply

To limit the communication overhead of route request packets, a node processes route request packets that both it has not seen before and its address is not presented in the route record field. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache [6].

Behavior of Selfish Nodes

Selfish nodes drops route request so as to attempt to never get onto route so that they will never forward traffic for anyone. They will perform route discovery and route maintenance process but will never forward data packets. The selfish nodes drop the packet because they want to save their battery power. The cheap strategy of these nodes is that it is difficult to detect them by monitoring. Selfish nodes do not cause any damage in network with high node density [2]. But In low node density it can affect end to end delay and lead to congestion in network.

Characteristics of Selfish Nodes:

(i) They do not participate in routing process, it means a selfish nodes drops route request and route reply packets.
(ii) They intentionally delay RREQ packets, by avoiding themselves from routing paths.
(iii) They may participate in routing messages but may not relay data packets [2].

The major reason for such selfish behavior is to save its own battery power. It may therefore be clarified that such selfish node is not malicious and does not involve itself in network but normally restrains itself from activities of other nodes which do not bring any benefit to it.

3. PROBLEM STATEMENT

MANET characteristic acquire many security challenges. There are certain attack from literature and found that selfish nodes have harmful effect on network. Selfish nodes are also working according to their naming characteristics which are harmful to network. Density play important role to reduce effects of security attack. Cooperation based network works with cooperation of participate nodes. As number of nodes is increasing cooperation gets better. Basic characteristic of adhoc network suggest cooperation from participating nodes and DSR works with only cooperation, It has been found that DSR protocol works with source routing mechanism in which source node generates route request packet and broadcast packet to other neighbor nodes to find destination which increases routing overhead and collision in network and indirectly affects throughput of network.

4. PROPOSED ALGORITHM ES-DSR AND IMPLEMENTATION

4.1 Implementation

DSR and Proposed DSR are tested on NS-2 which is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize. Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. Version 2 is the most recent version of ns (ns-2) [18]. The ns-2 simulator has several features that make it suitable for experimental result.

A network environment for ad-hoc networks,
Wireless channel modules (e.g.802.11),
Routing along multiple paths,
Mobile hosts for wireless cellular networks.

Ns-2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns-2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities, which are very important in our project since various information need to be logged for analysis [18].

4.2 Algorithm for Proposed ES-DSR PROTOCOL

Step-1 Read Selfish Nodes information from file.

Step-2 Check whether current node is selfish or not

Step-3 If selfish then drop all route request and route reply packets and also drop data packets

Step-4 else forward route request and route reply as well as data packets.

Step-5 Based on No. of Selfish nodes participating in Enhanced Selfish DSR Protocol its effect being reflected in throughput, routing overhead, End 2 End Delay and packet delivery ratio.

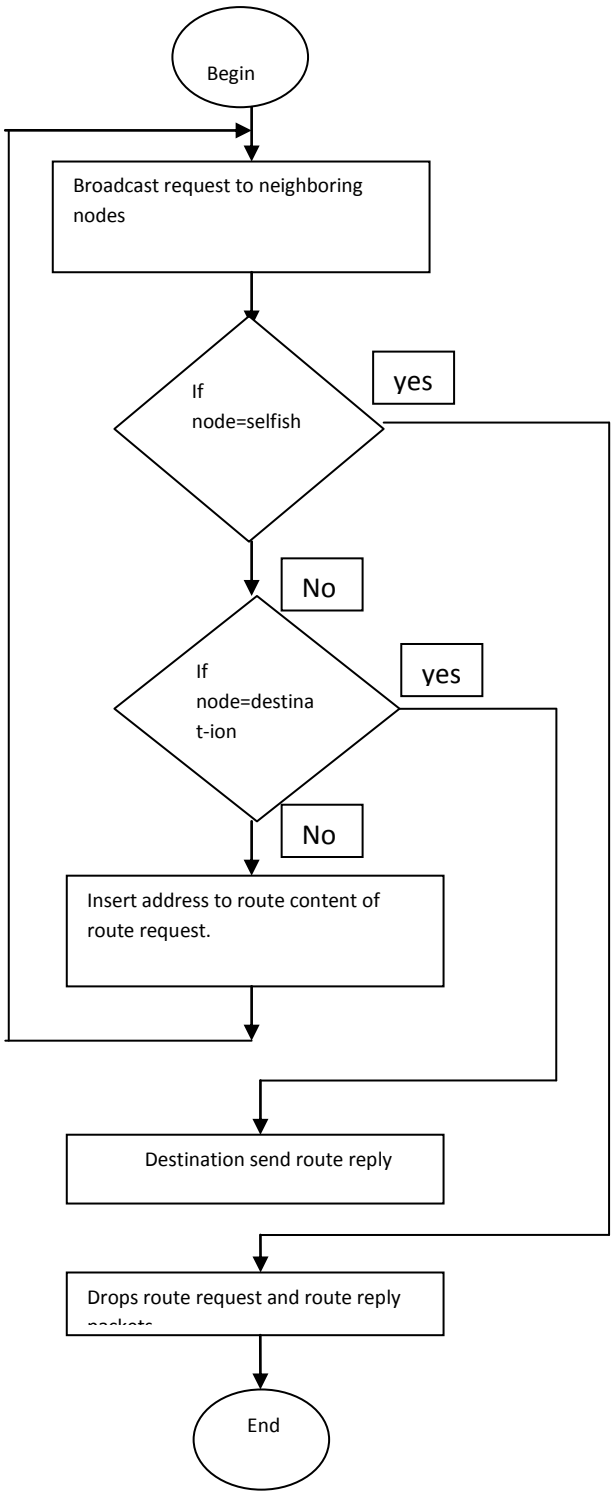

Figure 3 : Flowchart of Selfish Behaviour of node

4.3 Implementation code for Proposed EM-DSR Protocol

The following modification done in original dsr code.for implementing proposed dsr protocol in Route request forwarding

Small modified code is snippet below

Check whether nodes are selfish or not

```
        ifstream myFile("nodes.info");/
 string input;
 isMalicious = false;
 isSelfish = false;
 if (myFile!= NULL) {
 // bypass the [malicious] line
  getline (myFile, input);
  // see if there are a malicious node
   getline(myFile,input);
   if(isMaliciousOrSelfish(input)) {
   isSelfish = true;
     cout << net_id.dump() << " is selfish!" << endl;
}
```

Selfish Operation Performed in Forwarding Function of DSR

```
if(isSelfish && p.src != net_id)

{
    // selfish nodes drop route-request and route-reply packets
// route-request packets are dropped in

handleRouteRequest ()
    //cout << net_id.dump() << "drop route reply " << endl;
     if(srh->route_reply())

{
        drop(p.pkt);
 }
  }
    else {
  // now forward the packet  sendOutPacketWithRoute
(p, false);
  }

if(isSelfish && p.dest != net_id) {
    // selfish nodes drop route-request packets

   drop(p.pkt);
    return;
  }
```

In Proposed ES-DSR, Selfish nodes drops route request packet and route reply packets. If selfish nodes accept route request, they will drop data packets. This type of activity they are doing not to harm the network but just to save their battery power. In other words, such attacker does not allow that all of packets arrive at real destination.

5. EXPERIMENTAL SET-UP

The performance is analyzed against parameters such as mobility, no. of nodes. For the performance analysis of the protocol extensions, a regular well-behaved DSR network is used as a reference. The experimental results are being

studied under NS-2 Simulator. Experiments have been carried out in order to evaluate performance of MANETs under various routing attacks with the effect of density of network. The objective is to reduce no. of routing request packets [5].DSR and Proposed ES-DSR is simulated in same settings of parameters and scenarios. Experiments are run on 4 different mobility and also on different no. of nodes. The mobility model is Random Waypoint model of 1000 * 1000 metres [5]. It has focused on the evaluation of network performance in terms of routing overhead, throughput, and packet delivery ratio and normalized routing load of a mobile adhoc network where a number of nodes and numbers of malicious nodes both are varying.

General Parameter	
Number of Nodes	10,20,30,40,50
Number of traces	10
Topology	Mobile
Mobility model	Dynamic (Random Way Point Model)
Simulation Time	1000 sec
MAC Layer	802.11
Transmission Range	250 meters
Simulation Area	1000 x 1000 meter
Routing Protocol	DSR
Traffic Model Parameter	
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Table 5.1 Simulation setup

6. RESULT ANALYSIS OF MOBILITY BASED DSR AND PROPOSED ES-DSR

In this section the experimental results is shown for mobility based performance of DSR routing protocol and Proposed ES-DSR.

Some of important Performance Parameters are analyzed for DSR and ES-DSR [3][7]:

(i) Throughput
(ii) End to End Delay
(iii) Routing Overhead
(iv) Packet Delivery Ratio

(i) Throughput:

Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

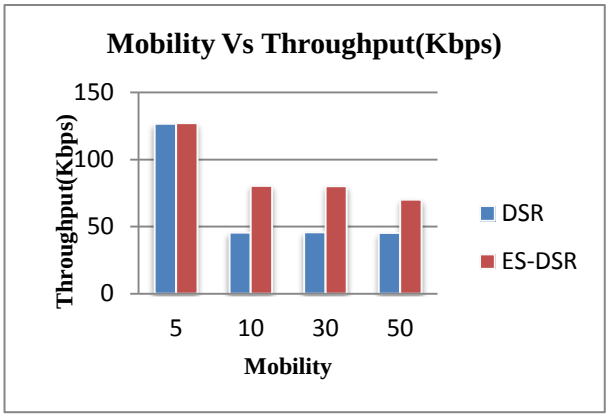

Figure 4 : Mobility Vs Throughput

Figure 4 shows Mobility Vs Throughput in DSR and ES-DSR. From figure 4 it is analyzed that as speed increases in network throughput is decreasing due to breaking of connection between nodes and packets are being discarded in DSR and in ES-DSR throughput is increasing but marginally compared to DSR as no. of nodes is more and also due to increasing speed, generally route request and route reply packets are being dropped by selfish nodes.

Routing Overhead

Nodes often change their location within network. So, some musty routes are generated in the routing table which leads to unnecessary routing overhead.

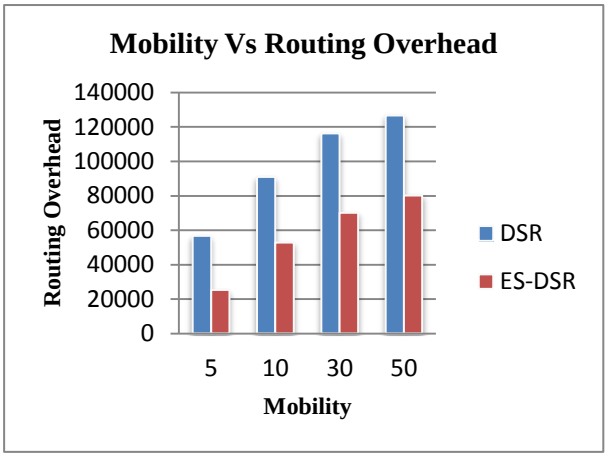

Figure 5 : Mobility Vs Routing Overhead

Figure 5 shows Mobility Vs Routing Overhead in DSR and ES-DSR. The experimental results of dynamic topology where nodes tend to move from one place to another place at different time frame. So links may break and re-route discovery required. It is required to establish lots of connection because of this movement. Line Graph clearly suggests that as mobility increasing in network overall routing overhead will increase in DSR but in proposed ES-DSR Routing overhead is comparatively 50% reducing due to dropping of route request packets by selfish nodes which also reduces collision in network.

(ii) Average end-to-end delay of data packets

There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gave the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance.

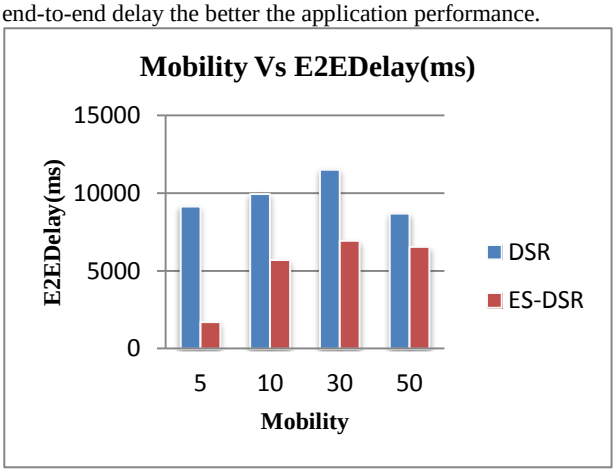

Figure 6: Mobility Vs E2EDelay

Figure 6 shows Mobility Vs E2EDelay in DSR and ES-DSR. From figure 6 it is analyzed that as mobility increases in network the delay time between deliveries of packets between nodes is also increasing due to more breaking of connection between nodes but as mobility increases highly the delay decreases thus ES-DSR is also acting beneficially as mobility increases to some extent.

Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different mobility.

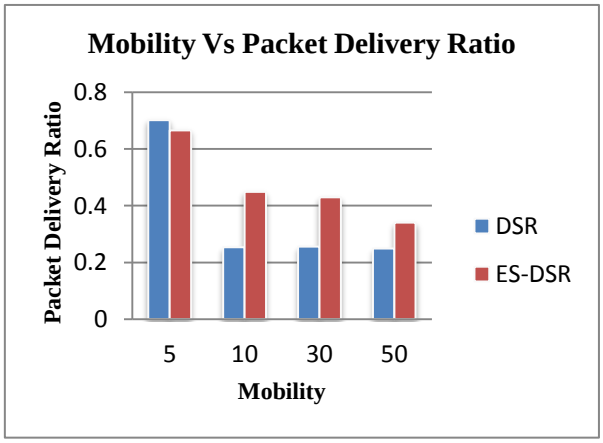

Figure 7: Mobility Vs Packet Delivery Ratio

Figure 7 shows Mobility Vs Packet Delivery Ratio in DSR and ES-DSR. It shows the impact of changing the speed, with which nodes move in an ad hoc network, on the packet delivery ratio. In general, packet delivery ratio decreases with increase in average node speed. ES-DSR also shows that packet delivery ratio marginally decreases compared to DSR because communication overhead is reduces almost 50% than DSR so more no. of packets will making successful connection and packets reaching proper destination.

7. DENSITY BASED PERFORMANCE EVALUATION OF DSR & PROPOSED ES-DSR

(i) Throughput

In this Performance Evaluation of DSR and ES-DSR, On X-Axis, no. of nodes are increased like 10, 20, 30 40 and 50, and on Y-Axis, Throughput is being measured in Kbps.

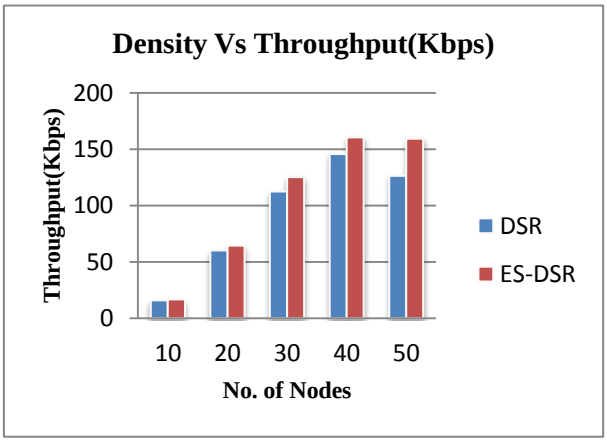

Figure 8: Density Vs Throughput

Performance of DSR and Selfish Behavior in DSR (ES- DSR) is analyzed through various experiments conducted on NS-2. As shown in a Figure 7, as density increasing in DSR throughput tends to get better but as no. of nodes increasing much more chances of breaking of connection is also more so throughput is also decreasing after specific density, whereas in proposed ES-DSR throughput is increasing as no. of selfish is nodes is less but throughput increases marginally as no. of selfish nodes increasing because communication overhead reduces which is beneficial for network and affect marginally on throughput.

(ii) Routing Overhead

In this Performance Evaluation of DSR and ES-DSR, On X-Axis, no. of nodes are increased like 10, 20, 30 40 and 50, and on Y-Axis, Routing Overhead is being measured.

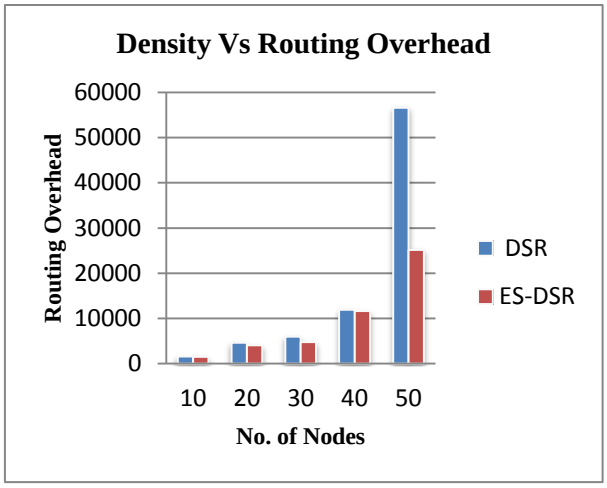

Figure 9: Density Vs Routing Overhead

Routing Packets are having significant influence on network performance. As no. of routing packets increase in a network nodes will waste significant energy, generate more collision, reduces throughput. As shown in figure 8 that as no. of selfish nodes increases in a network more routing packets will drop, which intern reduces collision and routing packets in a network which improves energy saving and throughput. so selfish behavior which is proposed ES-DSR reduces communication overhead almost 50% then DSR which in turn increases throughput.

(iii) E2EDelay

In this Performance Evaluation of DSR and ES-DSR, On X-Axis, no. of nodes are increased like 10, 20, 30 40 and 50 , and on Y-Axis, E2EDelay is being measured in ms.

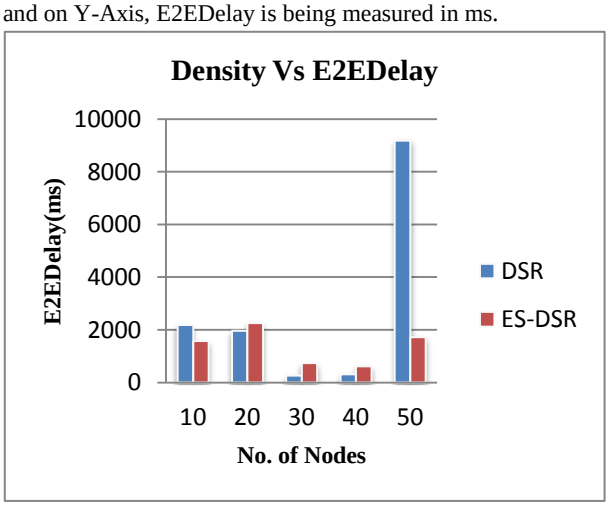

Figure 10: Density Vs E2EDelay

Figure 10 shows experimental results of DSR as well as Selfish behavior in DSR (ES- DSR).As density increasing in DSR end 2 end delay decreasing to some extent of increasing no. of nodes but after that delay is increasing because collision increases between no. of nodes and those results in dropping of packets. But as in ES-DSR it is shown that as no. of selfish nodes increasing in network end to end delay is increasing because of route request and route reply packets are dropped. but as selfish activity increases beyond the network can bear end to end delay increases so this is according to over observation that selfish activity can be helpful in network to some extent compared to DSR.

(iv) Packet Delivery Ratio

In this Performance Evaluation of DSR and ES-DSR, On X-Axis, no. of nodes are increased like 10, 20, 30 40 and 50, and on Y-Axis, Packet Delivery Ratio is being measured.

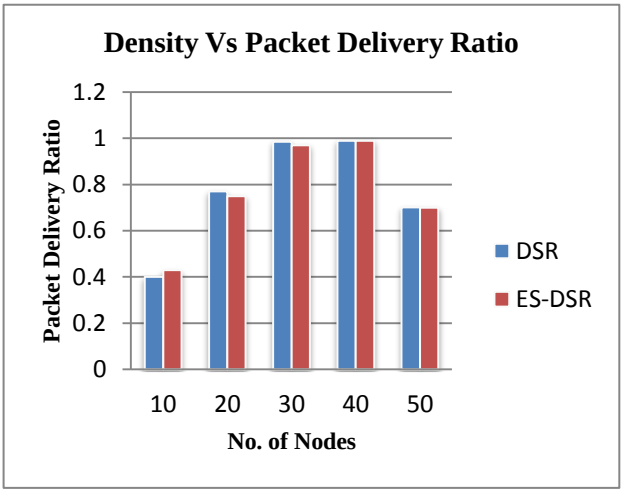

Figure 11: Density Vs Packet Delivery Ratio

Figure 11 show experimental results analysis of DSR as well as Selfish behavior in DSR (Proposed ES- DSR).As it has been analyzed from graphical results that as no. of nodes increases in DSR the packet delivery ratio is increases due to more no. of establishment of routes and connection between nodes which can also be helpful to increases throughput but after increasing nodes much more in network traffic and routing overhead is increasing which creates collision between nodes thus packet delivery ratio is also decreasing which affects the network. In Proposed ES-DSR, as density increase, and no. of selfish nodes increases it helps to give good results by acting in positive way in network as selfish activity increases in network, by reducing communication overhead and also packet delivery ratio is marginally affected by selfish behavior which is very beneficial for network and also throughput is also being very much less affected.

8. CONCLUSION

In this paper, the simulation of DSR and proposed ES-DSR protocols has been carried out using NS-2.34 simulator. Simulation has been done for 10, 20, 30, 40 and 50 nodes in ad hoc network and also as mobility increases from 5, 10, 30 and 50 m/sec various performance parameters are affected. On an average of 10 experimental results are taken to make result more appropriate. it has been analyzed both protocols in terms of throughput, routing overhead and end to end delay and Packet Delivery Ratio. The performance of routing protocols in MANET depends heavily on different kind of attacks. So if we include concept of selfish behavior node in DSR protocol then in enhanced version of protocol, the results of simulation show that this has high effect on DSR protocol. From the simulation results and as shown in graphs that if we include selfish behavior node in DSR protocol then there is significant 50% decrement in communication overhead which reduces connection breakage among nodes which is proved beneficial to reduce almost 70% end to end delay among no. of nodes and so throughput is increasing about 20% and packet delivery ratio is showing marginal effect than DSR protocol.

From paper it has been proved that the effect of density in network is observed during experiment of selfish behavior on DSR. During this attack selfish node tends to drop route request packets which intern improve network performance, reduces collision and saving resources for whole network. In a way density always reduce the effect of attack because more no. of good nodes will do more work to solve problem.

9. FUTURE SCOPE

In this paper it has been proved that security attacks are somewhat beneficial to mobile adhoc network. It has been simulated using selfish behavior by using Proposed Enhanced Selfish DSR protocol on Network simulator using different number of nodes. It has been proved that selfish nodes are also encouraging the different parameters of mobile adhoc network. In this paper selfish nodes drop route request and route reply packets and isolates them from the active data forwarding and routing and hence saves their battery power. The paper represents the analysis of the selfish behavior over the proposed scheme to analyze its performance. In future we will analyze the protocol over Grey hole and other types of Attacks and we will implement it by combining different scenarios and further we will include different other routing protocols.

10. REFERENCES

[1] Rooshabh Kothari and Deepak Dembla ,"Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET", International Journal of Computer Application(IJCA),Vol.64, No.18, pp 1-8, February 2013

[2] Shailender Gupta, C. K. Nagpal and Charu Singla," Impact of Selfish node concentration in MANETs" ,International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2 pp 29-37 , April 2011

[3] Shin Yokoyama, Yoshikazu Nakane, Osamu Takahashi and Eiichi Miyamoto,"Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods," Proceedings of the 7th International Conference on Mobile Data Management (MDM'06) pp 95, IEEE 2006

[4] Mahesh Kumar Yadav, Ram Kishan Khola and Deepak Dembla, " Modeling, Analysis & Implementation of Improved AODV Routing Protocol in MANETs, International Journal of Computer Applications(0975-8887) Volume 41-No.21 pp 37-42 ,September-2012

[5] Deepak Dembla, Dr.Yogesh Chaba, "Modeling and Analysis of an intelligent AODV Routing Protocol based on Route Request Retransmission Strategy in MANETs", International Journal of Computer Applications (0975-8887) Volume 30-No.11 pp 6-13, September-2011

[6] G.Lavanya, A. Ebenezer Jeyakumar," An Enhanced Secured Dynamic Source Routing Protocol for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume X, Issue-4 pp 135-140, September 2011

[7] Hemang Kothari and Manish Chaturvedi, "Effect of Selfish behavior on power consumption in mobile Adhoc Network", Proceedings of the Asia-Pacific Advanced Network 2011 v. 32, pp . 91-100, APAN-2011

[8] RajenderNath, Pankaj Kumar Sehgal, Atul Kumar Sethi, "Effect of Routing Misbehavior in Mobile Ad Hoc Network" ISBN 978-1-4244-4791-6/10, IEEE 2010.

[9] Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah," A Simulation Analysis of Routing Misbehaviour in Mobile Ad hoc Networks", "NGMAST/Workshop on Mobile Security, Europe (2008)"

[10] N.Bhalaji, Dr.A.Shanmugam,"Association between nodes to combat black hole attack in DSR based MANET", 978-1-4244-3474-9/09/ pp 403-407, IEEE 2009

[11] Dinesh Mishra1, Yogendra Kumar Jain, Sudhir Agrawal," Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", 978-0-7695-3915-7/ pp 621-623 , IEEE 2009

[12] Abdul-Aziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah,"A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks",pp 592-597, IEEE 2008,

[13] L. Abusalah, A. Khokhar, M. Guizani, "A survey of secure mobile Ad Hoc routing protocols," IEEE Communications Surveys & Tutorials,vol. 10, no. 4, pp. 78-93, IEEE 2008

[14] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[15] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks in Wireless/Mobile Network Security", Springer 2008.

[16] Mon Bo Su, Xiao Hannan, A. Adereti, J. A. Malcolm, B. Christianson, "A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack", Proc. of Third International Symposium on Information Assurance and Security, 'IAS 2007', pp. 50-55, Aug. 2007.

[17] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", March 2007

[18] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Mobile Network Security pp 1-38, Springer 2006.

[19] D B. Johnson, D A. Maltz, and Y. Hu. "The dynamic source routing protocol for mobile ad hoc network," IETF, pp 43-53, April 2003.

[20] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540- 7993/04/,2004 IEEE pp 28-39 , May/June 2004

[21] S. Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. of MobiCom 2000 pp 255-165, Boston, August 2000.