Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET

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

Deepak Dembla
Associate Professor, CSE
Arya Institute of Engg. & Technology,
Jaipur, India

ABSTRACT
A Mobile Ad hoc Network (MANET) is a group of movable hosts with wireless network interfaces that structure a temporary network without the support of any permanent infrastructure or central administration. A MANET is also referred as an infrastructure less network because the mobile nodes in the network dynamically locate paths among themselves to transfer packets provisionally. Due to the dynamic network topology in ad hoc network nodes are exchanging plenty of routing packets for creating communication which intern increase network overhead and also increase collision in network. This brings about the matter of security in an ad hoc network. Security is core concern in routing protocol of MANET and affects the performance. In this paper, a innovative request forwarding mechanism is proposed in which source node generates route request packet and broadcast packet to other neighbor nodes to locate destination by implementing black hole attack. Proposed EM-DSR (Enhanced Malicious DSR) is implemented on NS-2 and results shown significant improvement over original DSR in terms of various performance metrics. it has been found that on dense network certain numbers of malicious nodes are supportive to reducing communication overhead and because of density negative effect of malicious attacks which is proposed EM-DSR that is able to reduce. Hence result shows proposed EM-DSR will be helpful to decrease communication overhead.

Keywords
DSR, EM-DSR (Enhanced Malicious DSR), Secured Routing, Black hole attack, malicious nodes, Selfish nodes, Ad hoc network.

1. INTRODUCTION
By the existence of a permanent supporting coordinate the flexibility of wireless systems is limited. Thus the places where there is no permanent infrastructure the technology cannot work competently. The upcoming invention of wireless systems is expecting easy and fast deployment of wireless networks. This fast network deployment is not possible with the existing structure of present wireless systems [1].

Latest advancements such as Bluetooth introduced a fresh type of wireless systems which is frequently known as mobile ad-hoc networks. Mobile ad-hoc networks manage in the absence of permanent infrastructure. Mobile ad hoc network offers quick and horizontal network deployment in conditions where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad hoc network is an self-governing system of movable nodes coupled by wireless links; each node operates as an end system and a router for all other nodes in the network [1].

A latest growing wireless network allows users to admittance services and information electronically, irrespective of their geographic position. They 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 node interacts with a association in the network (that is known as base station) inside its communication radius. 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.

2. RELATED WORK

Routing is the act of moving information from a source to a destination in an internetwork. During the transfer of information at least one intermediate node within the internetwork is encountered. Mainly two activities are concerned in this concept: transferring the packets through an internetwork and shaping optimal routing paths. The transferring of packets through an internetwork is known as packet switching which is straight forward, and the path determination could be very complex.

Routing protocols use a number of metrics as a standard measurement to analyze 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 [4].

Routing is mainly classified into static routing and dynamic routing. Static routing refers to the routing strategy being stated manually or statically, in the router. Static routing maintains a routing table usually written by a networks administrator. Dynamic routing refers to the routing strategy that is being learnt by an interior or exterior routing protocol. This routing primarily depends on the state of the network i.e. the routing table is affected by the activeness of the destination.

Routing in Mobile Ad hoc Networks

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure

of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks make use of the same random access wireless channel, cooperating in an intimate manner to engage them in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routine procedure. This is always organized to find a path so as to forward the packets suitably between the source and the destination. A base station can arrive at all mobile nodes without routing via broadcast in common wireless networks within a cell. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is random connectivity changes [2].

N.Bhalaji, Dr.A.Shanmugam [6], Proposed Nature of Association between Neighbors in an Ad Hoc Network. It identifies the malicious nodes and isolates them from the active data forwarding and routing. The proposed approach and simulation results shows that The Association based (AB) DSR protocol is tested under different scenarios by varying the number of malicious nodes, throughput of AB-DSR is greater than the standard DSR in the presence of black hole nodes. When no malicious nodes are presented the standard DSR has less dropped data packets percentage than the proposed one. But this changes when the number of malicious nodes increases. It also encourages the nodes to cooperate in the adhoc structure.

Classification of routing protocols

One of the challenging goals in MANET is the blueprint of routing protocols. The function of routing protocol is to capably find the shortest path between the source and the destination of a flow. Routing protocols may normally be categorized as proactive and reactive (as shown in figure 1. Proactive protocols are also referred to as table-driven while reactive protocols are referred to as on-demand. Proactive protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. On the other hand, reactive protocols initiate route discovery only in the presence of data for transmission at the source. Routing protocols for ad hoc wireless networks can be classified into two types based on the underlying routing information update mechanism employed. An ad hoc routing protocol could be reactive (on demand), proactive (table driven) [6]

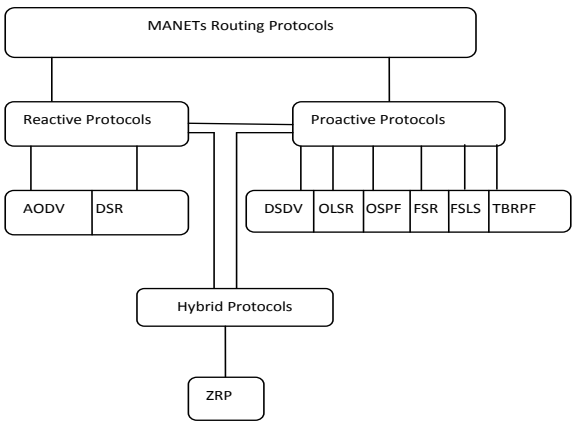

Fig 1: Classification of Routing Protocols

Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) [7] is a reactive unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains whole routing information to reach its destination. To retain route information that it has learnt, in DSR each node uses caching technology additionally.

There are two major phases in DSR, [7] the route discovery phase and the route maintenance phase. When a source node wants to send a packet, it initially consults its route cache. If the required route is existing, the source node includes the routing information within the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting route request packets. A route request packet contains addresses of both the source and the destination and a unique number to identify the request. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors.

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 [5].

After being shaped, either by the destination or an intermediate node, a route reply packet needs a route back to the source. There are three potential to get a backward route. The first one is that the node previously has a route to the source. The second prospect is that the network has symmetric (bi-directional) links. The route reply packet is sent using the collected routing information in the route record field, but in a reverse order as shown in Figure 2 [7]. In the last case, there exists asymmetric (uni-directional) links and a new route discovery procedure is initiated to the source. The discovered route is piggybacked in the route request packet.

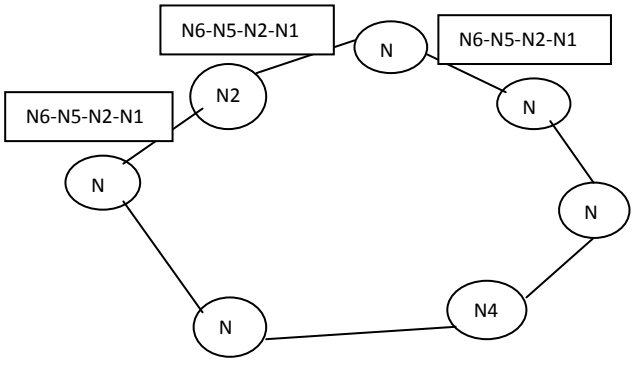

Fig 2: Route reply is piggybacked in RREQ packet

In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source. DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance [7] [9].

Black Hole Attack in DSR

A black hole attack [14] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination.

MANETS are vulnerable to various types of attacks. On the basis of different characteristics the attack on mobile ad hoc network is classified as passive and active attacks. One such active attack is Black hole attack. A black hole is a node that has the characteristics that it always responds with a RREP message to every RREQ, even though it does not really have a legitimate route to the target node. A Black Hole attack [1] [8] is a kind of denial of service where a malicious node can absorb all data packets by fallaciously claiming a new and fresh route to the destination and then drops them without delivering them to the destination. Cooperative Black hole means the malicious nodes act in a group. In black hole attack [6][14], the malicious node waits for the neighbours to initiate a RREQ packet. As the black hole node receives the RREQ packet, it will immediately send a forged RREP packet to the source node advertising itself as having the shortest and optimum route path to the target destination.

On receiving of RREP the source node thinks discovery of route process is over, discards other RREP messages from other nodes and choose the path through the malicious node to route the data packets and starts to transmit the data packets over malicious node as shown in figure 3. When the data packets reach the black hole node that malicious node absorbs the entire packet and dropped them instead of forwarding them to the intended destination which results in denial of communication.

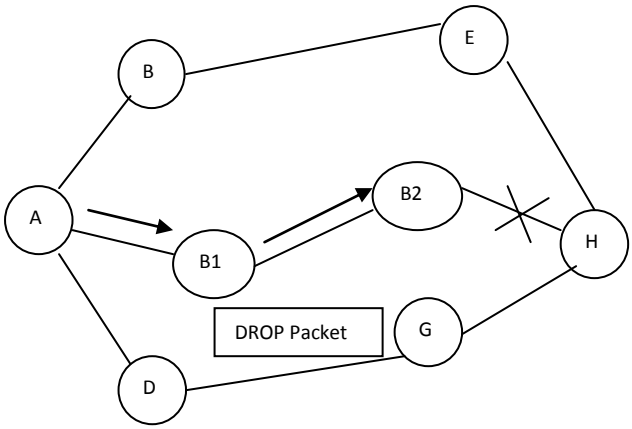

Fig 3: Black Hole Attack

3. PROBLEM STATEMENT

MANET characteristic possess many security challenges. There are certain attack from literature and found that malicious nodes have harmful effect on 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.

4. IMPLEMENTATION OF PROPOSED ALGORITHM EM-DSR

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) [17]. 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 research since various information need to be logged for analysis [17].

4.2 Algorithm for Proposed EM-DSR PROTOCOL

Step-1 Read Malicious Nodes information from file.

Step-2 Check whether current node is malicious or not

Step-3 If Malicious then forward all route request and route reply packets and drop data packets

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

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

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 malicious 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)) {
        isMalicious = true;
        cout << net_id.dump() << " is malicious!"
<< endl;
}
```

Malicious Operation Performed in Forwarding Function of DSR

```
if (isMalicious)

{
  // malicious nodes forward route-reply and route-request packets
  if (srh->route_reply() || srh->route_request()) {
    sendOutPacketWithRoute(p, false);
  }
  // but drop all other packets -> DoS attack
  else {
    drop(p.pkt);
  }
 }
   if(srh->route_reply()) {
       drop(p.pkt);
  }
 }
  else {
 // now forward the packet...
 sendOutPacketWithRoute(p, false);
 }
```

In Proposed EM-DSR, Malicious nodes in black hole attack introduce themselves as co-operative node, by correctly participating in route discovery phase. It makes sure that it will be available on the path. After route discovery mechanism, when source node transmit data at that time malicious nodes just drop the entire data packet. 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. Scenarios are tested in NAM also for better understanding of the nodes movement and behavior.

The objective is to reduce no. of routing request packets [3].DSR and Proposed EM-DSR are 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 [3]. It has focused more attention 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. Following parameters are set for experiments on network simulator ns2.

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
MAC Layer	802.11
Range	250 meters
Simulation Area	1000 x 1000 meter2
Routing Protocol	DSR , AODV
Traffic Model Parameter	
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Table 5.1 Simulation Scenario Setup

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

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

Some of important Performance Parameters are analyzed for DSR and EM-DSR [13]:

(i) Throughput
(ii) Routing Overhead
(iii) Average End to End Delay
(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.

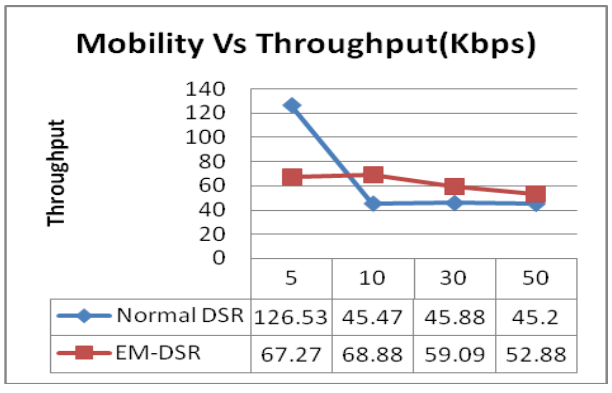

Fig 4: Mobility Vs Throughput

Figure 4 shows Mobility Vs Throughput in DSR and EM-DSR. From figure 6.1 it is analyzed that as mobility increases in network throughput is decreasing as speed increases due to breaking of connection between nodes and packets are being discarded in DSR but in EM-DSR throughput is increasing for some specific mobility after that it is also decreasing as breaking of routes and connection between nodes.

ii). 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.

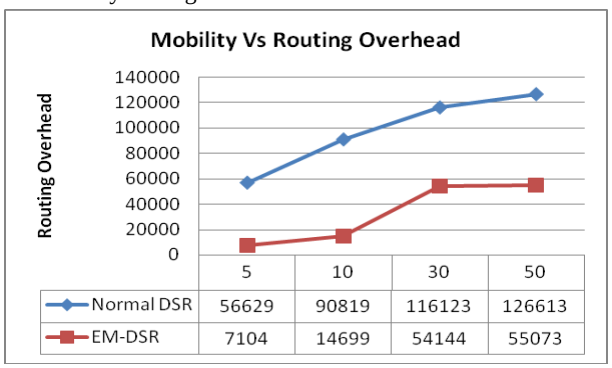

Fig 5: Mobility Vs Routing Overhead

Figure 5 shows Mobility Vs Routing Overhead in DSR and EM-DSR. The experimental results of dynamic topology where nodes tend to move from one place to another place at different timeframe. 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.

iii). 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.

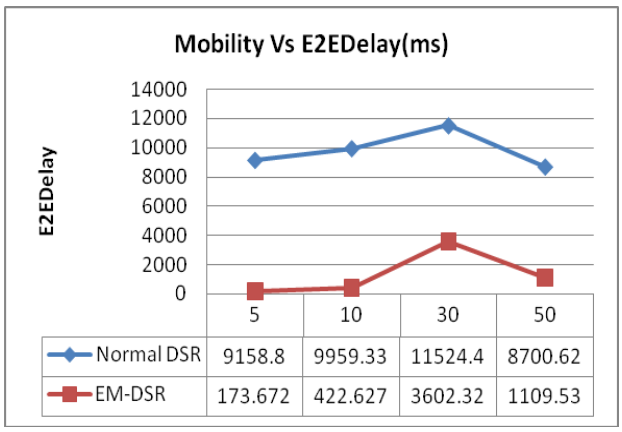

Fig 6: Mobility Vs E2E Delay

Figure 6 shows Mobility Vs E2EDelay in DSR and EM-DSR. From this, 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 EM-DSR is also acting beneficially as mobility increases to some extent.

iv). 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.

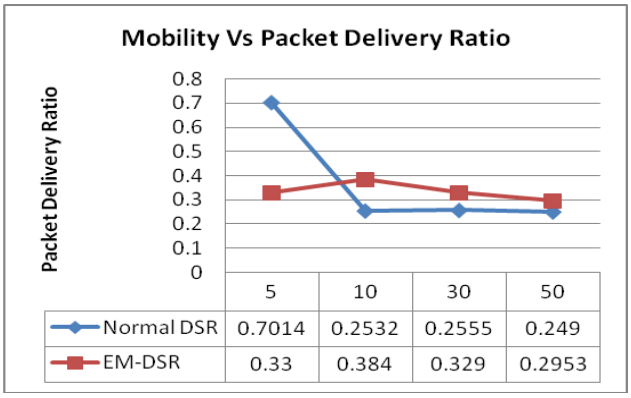

Fig 7: Mobility Vs Packet Delivery Ratio

Figure 7 shows Mobility Vs Packet Delivery Ratio in DSR and EM-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. EM-DSR also shows that packet delivery ratio increases as speed increases s from 5 to 10 but then it continually decreases as mobility increases.

Experimental Results (EM-DSR)

Black hole attack has been simulated by varying number of malicious nodes as well as by varying node density also. In these experimental results various performance parameters are considered:

The performance of routing protocols in MANET depends heavily on much kind of attacks. One of these attacks is Black hole attack. The results show that this attack has high effect on DSR protocol. In this case, based on the number of attacker, the throughput is high or low. If the number of them increases, the throughput is low, because of Black hole attack. It drops data packet so throughput will decrease. End to End Delay showing decrement of connection time. This happens because of malicious nodes. As the numbers of malicious nodes are increasing, more number of nodes is removed from path which interns help to reduce end to end delay.

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

(i) Throughput

In this Performance Evaluation of DSR and EM-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.

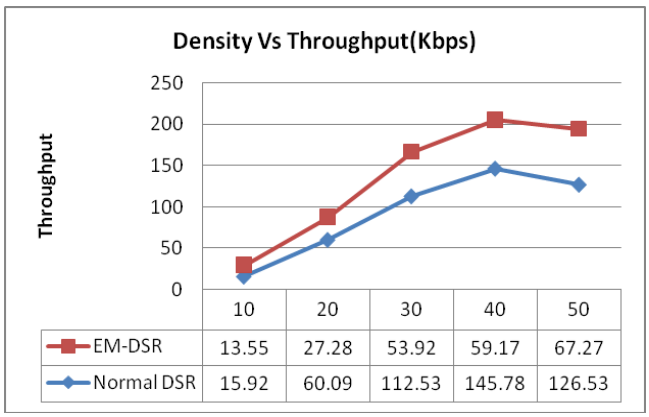

Fig 8: Density Vs Throughput

Performance of DSR and Black Hole Attack in DSR (EM-DSR) is analyzed through various experiments conducted on NS-2. As shown in a Figure 8, as density increasing in DSR throughput tends to get better, whereas similar behavior can be observed when experimenting black hole attack in a network. The Reason behind this kind of result is malicious node which drops routing packets which intern reduces communication overhead and help to reduce collision, which intern increase the throughput.

(ii) Routing Overhead

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

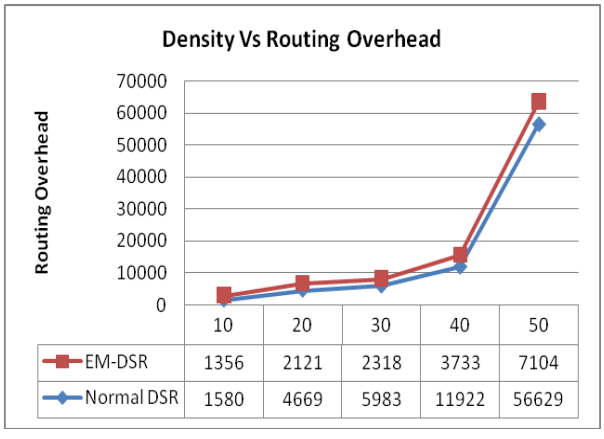

Fig 9: Density Vs Routing Overhead

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 9 that as no.

of malicious nodes increase in a network more routing packets will drop, which intern reduces collision and routing packets in a network which improves energy saving and throughput.

(iii) E2E Delay (End to End delay)

In this Performance Evaluation of DSR and EM-DSR is analyzed, 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.

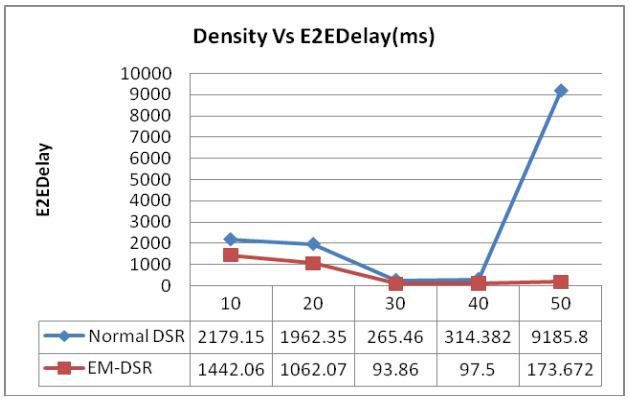

Fig 10: Density Vs E2E Delay

Figure 10 shows experimental results of DSR as well as Black Hole Attack in DSR (EM- 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 EM-DSR it is shown that as no. of malicious nodes increasing in network end to end delay is decreasing that is because collision reduces due to dropping of packets and that results in getting timely delivery of packets but as malicious activity increases beyond the network can bear end to end delay increases so this is according to over observation that malicious activity can be helpful in network to some extent.

(iv) Packet Delivery Ratio

In this Performance Evaluation of DSR and EM-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.

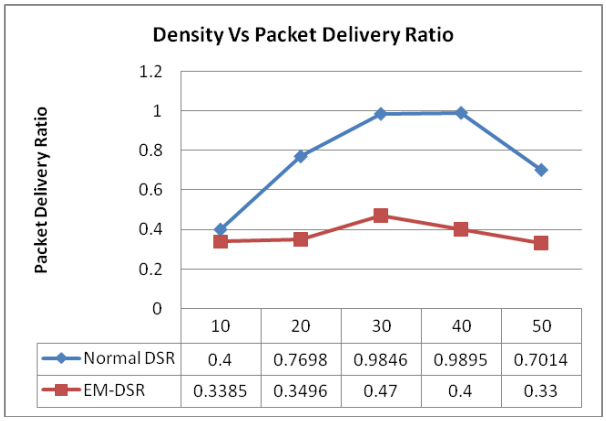

Figure 11: Density Vs Packet Delivery Ratio

Figure 11 shows experimental results analysis of DSR as well as Black Hole Attack in DSR (Proposed EM- 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 EM-DSR, as density increase, and no. of malicious nodes increases it helps to give good results by acting in positive way in network as malicious activity increases in network, it helps in increasing packet delivery ratio and thus indirectly helps in throughput and end to end delay but as malicious activity increases beyond network can tolerate packet delivery ratio decreases, because traffic increases which create collision and thus dropping packets.

8. CONCLUSION

It is being simulated on Dynamic Source Routing (DSR) and balckhole attacks on DSR protocol (EM- DSR). The simulation of these protocols has been carried out using NS-2.34. Simulation has been done for 10, 20, 30, 40 and 50 nodes ad hoc network and also increase mobility 5, 10, 30 and 50. As a traffic parameter Constant Bit Rate is used. As far as mobility concern Random Way Point Model is used. 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. The results of simulation show that this attack has high effect on DSR protocol. In malicious attack case, based on the number of attacker, the throughput is high or low. If the number of them increases, the throughput is low, because actually data packets are dropped rather than routing packets.

When number of nodes increasing in network, End to End delay tends to decrease because it is having better chance to find shortest path. So from experimental results it is analyzed that , as far as throughput concern in simple DSR as the number of nodes increase it gets better but when black hole attacks is implemented it is decreasing as the number of malicious node increase.

The effect of density in network is observed during experiment of black hole attack on DSR. During this attack malicious node tends to drop routing 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 black hole attack by using Proposed Enhanced Malicious DSR protocol on Network simulator using different number of nodes. It has been proved that malicious nodes are also encouraging the different parameters of mobile adhoc network. In this paper, Black hole attack identifies the malicious nodes and isolates them from the active data forwarding and routing. The paper represents the analysis of the black hole attack over the proposed scheme to analyze its performance. Future work will consist of analyzing the protocol over Grey hole and other types of Attacks and selfish behavior of nodes will be studied and implemented in different scenarios and further will include different other routing protocols.

10. REFERENCES

[1] Ashish T. Bhole, Prachee N. Patil," Study Of Black hole Attack in MANET" , International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4 pp 99-102, October 2012

[2] 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

[3] 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

[4] 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.

[5] Elizabeth M. Royer, C-K Toh. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", 168-175, 2004, ISSN 1682-6027 pp 46-55, IEEE 2009.

[6] 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

[7] 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

[8] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004, ISSN 1682-6027 2004 Asian Network for Scientific Information, pp 169-175.

[9] Latha Tamilselvan, Dr. V Sankaranarayanan," Prevention of Black hole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0-7695-2842-2/07 ,pp 6-11.

[10] 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.

[11] 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.

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

[13] 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.

[14] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF," A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks". IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan pp 72-77, 28-30 March 2005.

[15] 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.

[16] Ioannis Chatzigiannakis, Elena Kaltsat and Sotiris Nikoletseas, "on the effect of user mobility and density on the performance of ad-hoc mobile networks", 12th IEEE International Conference on Networks, 2004, pp 336-341. (ICON 2004) Proceedings.

[17] Xiao Yang Zhang, Yuji Sekiya and Yasushi Wakahara, "Proposal of a Method to Detect Black Hole Attack in MANET ", Autonomous Decentralized System 2009 pp 1-6 ,ISADS'09

[18] Mohammad AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004)

[19] 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.