Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

Enhanced DSR for Detection and Mitigation of Black Hole and Gray Hole Attacks in MANET

Neha Goyal[1], P S Maan[2]

[1]*Department of Computer Science and Engineering, DAVIET, Jalandhar, Punjab*
[2] *Department of Computer Science and Engineering, DAVIET, Jalandhar, Punjab*

Abstract —*Security in case of open medium network of MANET with dynamic environment is a big challenge. In simple DSR [1] based MANET it simply finds the path to destination it has no provision to detect and mitigate black hole or gray hole attack. So under attack DSR gives worst performance. In IDS based methods like in MDSR [2] the operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth-constrained. Even MDSR [2] is not efficient in preventing packet loss as it is seen that in the proposed method black node is detected after occurrence of attack therefore, leading to higher packet loss. Hence, it is very important to have very low computational complexity so that the detection operation is performed in a short time without any loss of packets for real-time applications. Therefore, we have proposed an Enhanced DSR in which packet loss is significantly low and have compared its performance with existing DSR [1] and MDSR [2]*

Keywords- *MANET; DSR [1]; MDSR[2]; IDS; Packet Delivery Ratio, Throughput, packet loss*

I. INTRODUCTION

1.1. Mobile Ad Hoc Network (MANET)

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time; therefore, the limited wireless transmission range of each node gets extended by multi-hop packet forwarding. This kind of network is well suited for the mission critical applications such as- emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources mobile Ad-hoc networks are vulnerable to several different types of passive and active attacks.[3,4]

Attacks in MANETs generally purpose and they are first is not to forward the packet or change the parameters of routing messages and to exhaust the battery of nodes by make them traversing the wrong packet in wrong direction and they also change the parameters of the packets such as sequence numbers and by using mechanism like authentication or cryptography as a preventive approach and can be used against attackers. By means of these mechanisms we can only prevent attacks from outside but not from inside any node inside by using this information can cause hazards in the network. This may lead to false positive detection of a non-malicious node. Another malicious behavior of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism. We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the wireless ad-hoc network. [5]

1.2. BLACK HOLE / GRAY HOLE ATTACK

Gray hole attack is a special kind of black hole attack (selective forwarding attack) in which a malicious node's behavior is exceptionally unpredictable. The gray hole nodes can perform the attack in three different ways: (i) The malicious node may drop packets from certain nodes while forwards all other packets. (ii) A node may behave maliciously for a certain time, dropping packets selectively. (iii) Is the combination of both attacks, i.e. the malicious node may drop packets from specific nodes for certain time only, later it behaves as a normal node. Due to these characteristics, detection of gray hole attacks is very hard. A gray hole attack can disturb route discovery process and degrade network's performance. Both black hole and gray hole attacks can be easily launched on reactive routing protocols like AODV and DSR [1].

1.3. DSR (Dynamic Source Routing) Protocol

DSR is an efficient routing protocol designed for multi-hop wireless ad hoc networks. DSR allows a network to be entirely self-organized and self-configured without need for existing network infrastructure/administration. DSR is a reactive routing protocol using source routing to forward packets. It uses source routing, meaning that source must know complete destination hop sequence. DSR's basic operation consists of two operations: Route Discovery and Route Maintenance. [6]

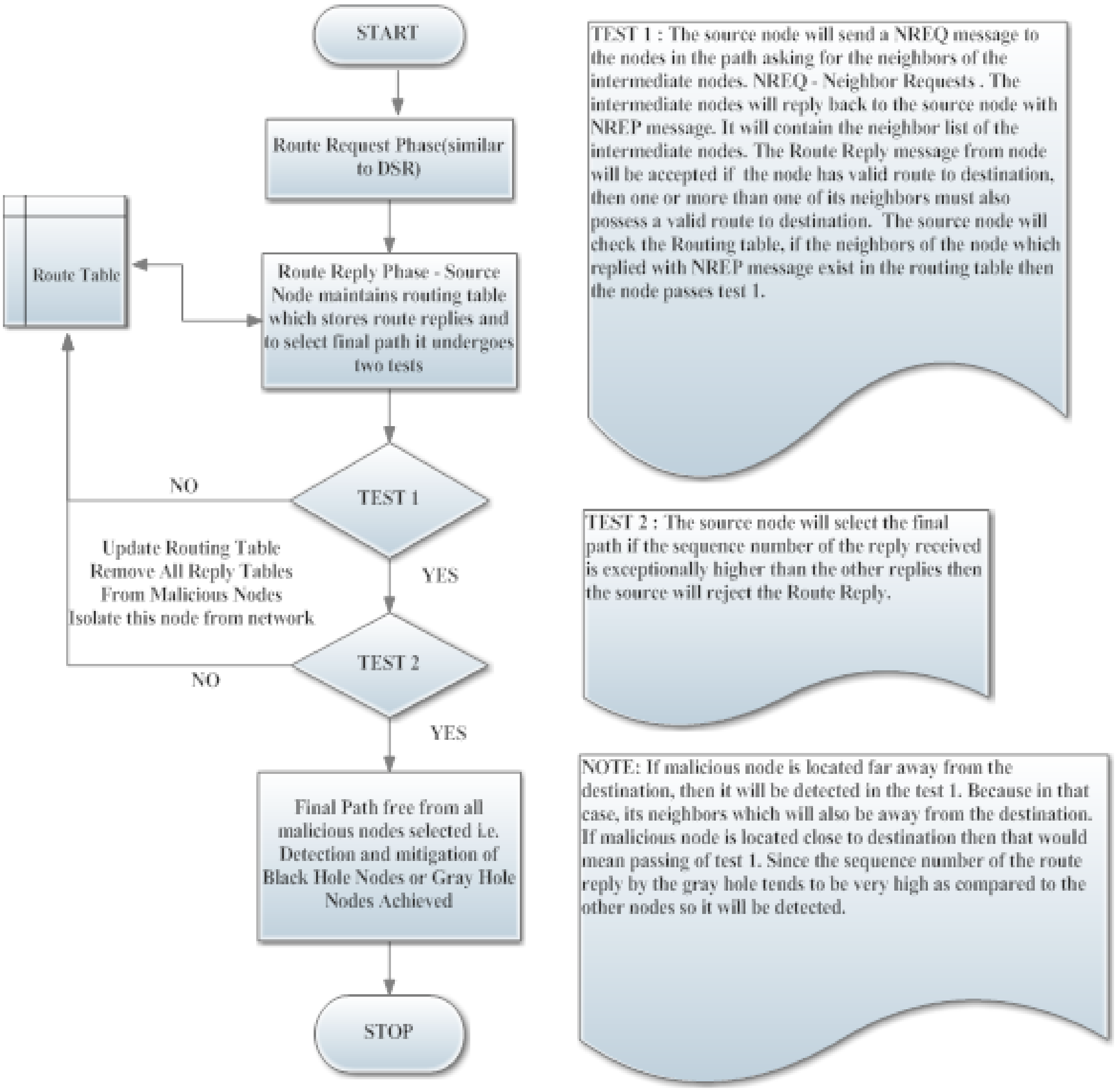
DSR uses Route Error packet and Acknowledgements for route maintenance. When a node has a fatal transmission problem at data link layer, it generates a Route Error packet. On receipt of route error packet, the node removes the hop in error from its route cache. Acknowledgment packets verify correct route links operation. This includes passive acknowledgments where a node hears a next hop forwarding a packet along a route. [7, 8]

1.4 MDSR [2]

They proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network.

Their IDS model was based on the following assumptions. (a) All the nodes are identical in their physical characteristics. If node A is within the transmission range of node B, then node B is also within the transmission range of A. (b) Also their solution assumes that all the nodes are authenticated and can participate in communication, i.e., all nodes are authorized nodes.(c) The source node, destination node and IDS nodes are taken as trusted nodes by default. (d) All the IDS nodes were set in promiscuous mode only when needed, and an IDS node will always be neighbor to some other IDS node. (e) Since there are multiple routes from a source to destination, the source node has to cache the other routes to mitigate the overhead incurred during new route discovery process. [2]

II. METHODOLOGY OF PROPOSED WORK


START
Route Request Phase(similar to DSR)
Route Table
Route Reply Phase - Source Node maintains routing table which stores route replies and to select final path it undergoes two tests
NO
TEST 1
YES
Update Routing Table
Remove All Reply Tables
From Malicious Nodes
Isolate this node from network
TEST 2
NO
YES
Final Path free from all malicious nodes selected i.e. Detection and mitigation of Black Hole Nodes or Gray Hole Nodes Achieved
STOP

TEST 1 : The source node will send a NREQ message to the nodes in the path asking for the neighbors of the intermediate nodes. NREQ - Neighbor Requests . The intermediate nodes will reply back to the source node with NREP message. It will contain the neighbor list of the intermediate nodes. The Route Reply message from node will be accepted if the node has valid route to destination, then one or more than one of its neighbors must also possess a valid route to destination. The source node will check the Routing table, if the neighbors of the node which replied with NREP message exist in the routing table then the node passes test 1.

TEST 2 : The source node will select the final path if the sequence number of the reply received is exceptionally higher than the other replies then the source will reject the Route Reply.

NOTE: If malicious node is located far away from the destination, then it will be detected in the test 1. Because in that case, its neighbors which will also be away from the destination. If malicious node is located close to destination then that would mean passing of test 1. Since the sequence number of the route reply by the gray hole tends to be very high as compared to the other nodes so it will be detected.

Fig 1: Image showing Flowchart of proposed enhanced algorithm

In the Flowchart given above we can see that first a route request phase is similar to simple DSR then comes the Route Reply Phase which is modified from original DSR. Upon finding a route its replies are stored and to find the shortest path free from black hole nodes among all the routes it undergo two tests stated above. If nodes fails Test 1 it is confirmed as Black Hole node and routing table is updated accordingly and if it passes Test 1 it undergo Test 2. Then if Test 2 is failed it is confirmed as black hole node and is removed from path, routing table is updated. Text Boxes given in the right of flowchart describes the two Tests in detail.

2.1 ROUTE REQUEST PHASE: BASIC OPERATION

Each node in the network maintains a route cache in which it caches the routes it has learned. To send data to another node, if a route is found in its route cache, the sender puts this route (a list of all intermediate nodes) in the packet header and transmits it to the next hop in the path. Each intermediate node examines the header and retransmits it to the node indicated after its id in the packet route. If no route is found, the sender buffers the packet and obtains a route using the route discovery process described below [1].

2.2 ROUTE DISCOVERY AND MAINTENANCE IN DSR

To find a route to its destination, a source broadcasts a route request packet to all nodes within its radio transmission range. In addition to the addresses of the 2 source and the destination nodes, a route request packet contains a route record, which is an accumulated record of nodes visited by the route request packet. When a node receives a route request, it does the following:

2.2.1 If the destination address of the request matches its own address, then it is the destination. The route record in the packet contains the route by which the request reached this node from the source. This route is sent back to the source in a route reply packet by following the same route in reverse order. (We assume bidirectional links. The alternative reply mechanism for unidirectional links is not considered here.)

2.2.2 Otherwise, it is an intermediate node. If the node has not seen this request before and has a route to the destination in its cache table, it creates a route reply packet with the route from its cache, and sends it back to the source. Such replies are called Intermediate-Node replies; if it does not have a route, it appends its own address to the route record, and increments hop count by one, and rebroadcasts the request. When the source receives a route reply, it adds this route to its cache and sends any pending data packets. If any link on a source route is broken (detected by the MAC layer of the transmitting node), a route error packet is generated. The route error is unicasted back to the source using the part of the route traversed so far, erasing all entries that contain the broken link in the route caches along the way [1].

Route Discovery Algorithm of DSR

```
When Route-Request_Packets received by Destination {
    //Updating Cache Info
        If Route_Record has useful info then update cache info
    //Processing of duplicate packets are avoided
        If
            SrcReqId == Already_Taken_Route_Discovery_Packet_List[]
                Then Packet is discarded
            // For loop free algorithm
            Else if DestinationId == Route_Record[]
                Then Packet is discarded
            Elseif (DestinationId == Me)
                //if Destination has path to sender and Source is present in cache
                If (Source == Cache[]      )
                Then
                    Copy mimimum cost
                    Copy most reliable path to Route_Reply Packet
                // Source is not present in cache
                Elseif (Source not equal to Cache[])
                Then
                    Create Route_Request_packets to find sender
                End
            End
            End
        Else
            Append address in RouteRecord[]
            Except the ones which was recorded earlier
        End
        End
```

2.3. PROCEDURE 1

Upon finding a route, the nodes send route reply messages back to source node.
The source node maintains the a routing table, which will store the route replies received by it from the nodes which claim they have route to destination node.

Suppose Ri= set of nodes that reply to source node claiming path to destination

```
for i = 1 Ri
    Node(s) – Rep(i)  //Source sends NREQ message to node
    Check Neighbor
    Rep(i) – Node(s)  //Node replies with neighbor list
End
```

The source node will select the path is the nodes consisting of those paths pass the following 2 tests:

2.4. TEST 1

The source node will send a NREQ message to the nodes in the path asking for the neighbors of the intermediate nodes. NREQ **-** Neighbor Request messages. The intermediate nodes will reply back to the source node with NREP message. It will contain the neighbor list of the intermediate nodes.
The Route Reply message from node will be accepted if it passes following condition:
If the node has valid route to destination, then one or more than one of its neighbors must also possess a valid route to destination. The source node will check the Routing table, if the neighbors of the node which replied with NREP message exists in the routing table then the node passes Test 1.
Suppose Nei = Neighbor list of ith Node

```
for x = 1 : Ri
    for y = 1 : Nei
        if Nei(y) == Rep(x)
            Test 1 is passed
        else
            Put node in suspected list
            And Node is confirmed as malicious
        End
    End
End
```

2.5. TEST 2

If the node failed test 1 then the source node will update the Routing table by removing all the reply tables from these nodes.
For the nodes which passed the test 1, the source node will select the final path if the nodes passes the following condition:
If the sequence number of the reply received is exceptionally higher than the other replies then the source will reject the Route Reply.
Suppose Pass = set of nodes that passed Test 1

```
for i = 1 : Pass
    If SequenceNo(i) is very high
    Node is confirmed as Blackhole
    End
End
```

Note: If the grey hole node will be located far away from the destination, then it will be detected in the test 1. Because in that case, its neighbors which will also be away from the destination, will not reply to source claiming the shortest path to it. Since the malicious node has replied but its neighbors has not, so it will be detected.
If the grey hole node will be located close to destination, then its neighbors will also be located close to the destination and they would have replied to the source node. That would mean passing of test 1. Since the sequence number of the route reply by the grey hole tends to be very high as compared to the other nodes so it will be detected.

III. RESULT ANALYSIS

Comparing the performance of the proposed enhanced technique with existing MDSR [10] and DSR [13] based on following performance metric:

3.1. PDR (Packet Delivery Ratio)

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender

$$\sum \text{Number of packet receive} / \sum \text{Number of packet send}$$

Here is a graph to compare the PDR of the proposed enhanced technique with existing MDSR [10] and DSR [13].

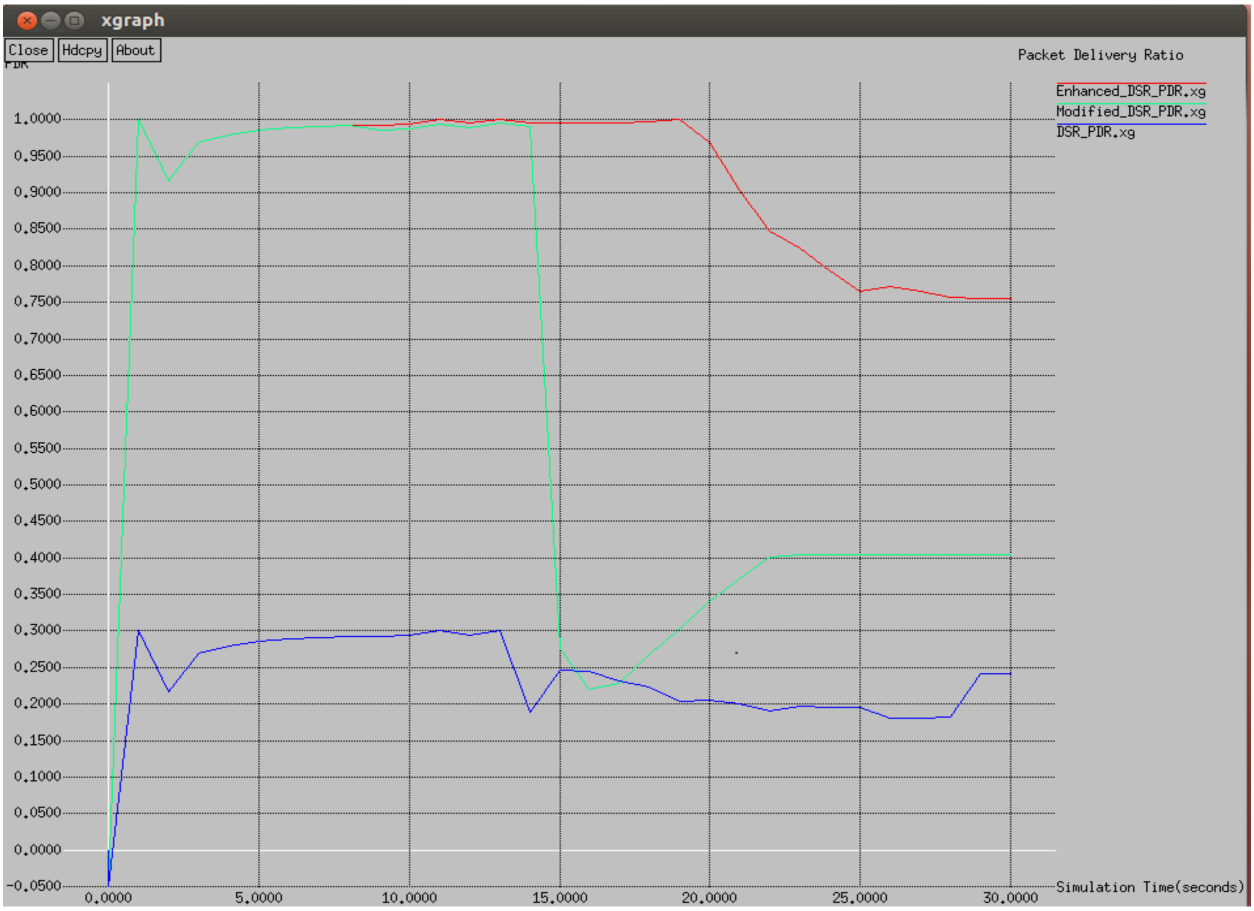


Fig 2. Graph Plotted for PDR against simulation time (seconds)

Above graph is plotted for PDR ratio against simulation time in seconds.

The greater value of packet delivery ratio means the better performance of the protocol.

As we can see PDR value for simple DSR [1] under attack its range lies between 0.2 – 0.3.
While in case of MDSR [2] it lies between 0.4 -1. It rises to 1 initially but after 15000 seconds it falls to 0.4
In Enhanced Proposed DSR value of PDR lies between 0.75 -1. It rises to max level initially and after 20000 seconds it comes at 0.75.
We can see that simple DSR [13] under attack gives lowest value for PDR among all described techniques. Though MDSR [10] is better than simple DSR [13] but after sometime it fails to perform better. Therefore, it's proved that Enhanced Proposed DSR has highest value so it is better than both MDSR [10] and simple DSR [13].

DSR [13] z	**range lies between 0.2 – 0.3**
MDSR [10]	range lies between 0.4 – 1
Enhanced_DSR	range lies between 0.75 - 1

Table 1: Comparing PDR values of existing DSR [1] and MDSR [2] with Enhanced DSR

3.2. THROUGHPUT

Throughput is the average 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.

Throughput is the number of successfully received packets in a unit time.

Here is a graph to compare the Throughput of the proposed enhanced technique with existing MDSR [2] and DSR [1].

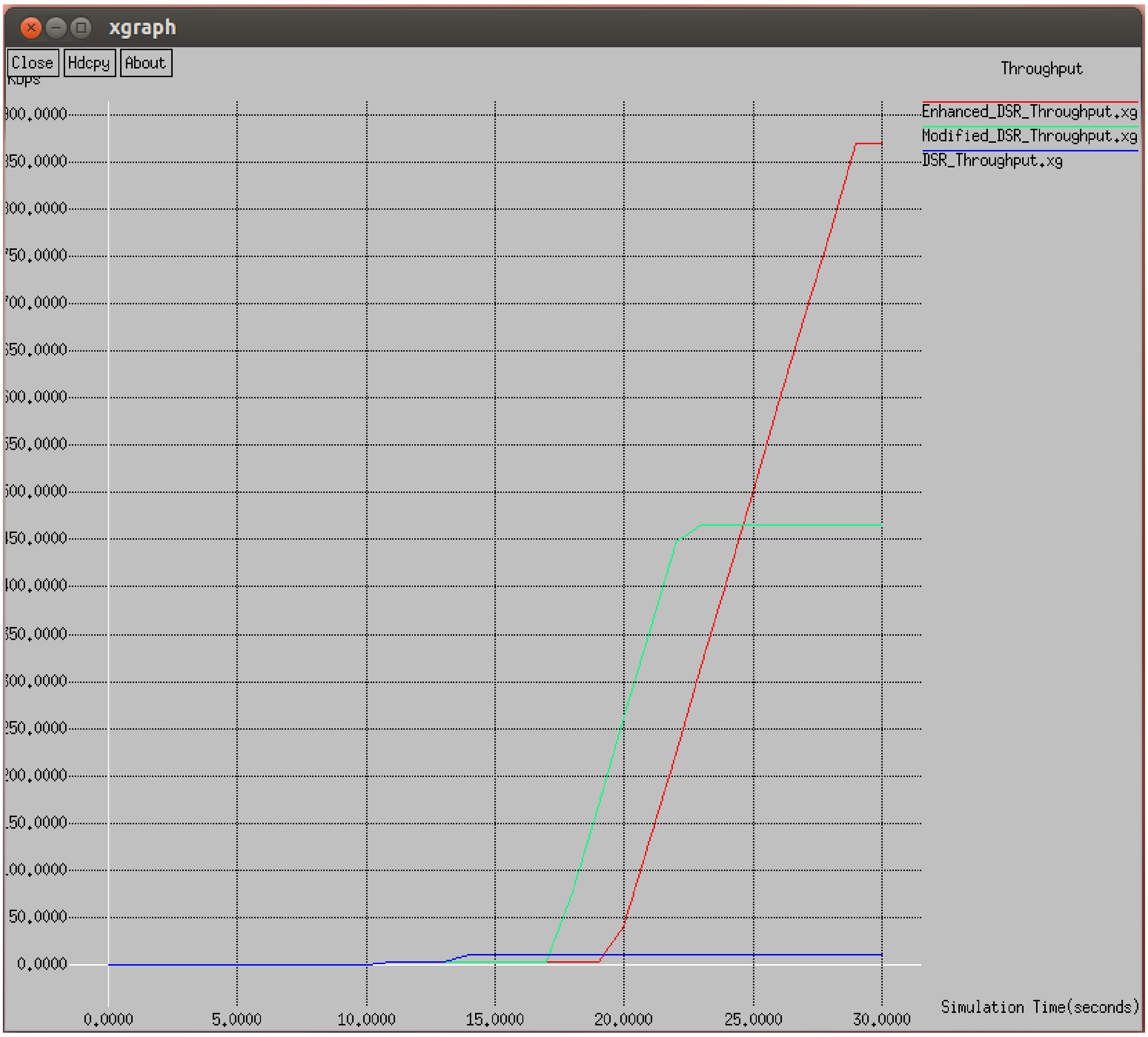


Fig 3. Graph Plotted for Throughput (kbps) against simulation time (seconds)

As we can see in graph Throughput value for simple DSR [1] under attack lies below 50 kbps.
While in case of MDSR [2] its value lies between 450 kbps – 500 kbps
In case Enhanced Proposed DSR value of Throughput lies between 850 kbps – 900 kbps.
We can see that simple DSR [1] under attack gives lowest Throughput value among all described techniques. Though MDSR [2] is better than simple DSR [1] but fails to achieve desired Throughput value. Therefore, it's proved that Enhanced Proposed DSR has highest value for Throughput i.e. in this case maximum no. of Packets are delivered successfully per unit time. So it is better than both MDSR [2] and simple DSR [1].

DSR [13]	**below 50 kbps**
MDSR [10]	**Lies between 450 kbps – 500 kbps**
Enhanced_DSR	**Lies between 850 kbps – 900 kbps**

Table 2: Comparing Throughput values of existing DSR [1] and MDSR [2] with Enhanced DSR

IV. CONCLUSION

Hence, based on the above analysis we can conclude that our proposed technique is better than both existing simple DSR [1] and MDSR [2]. With our technique packet loss is comparatively low. It is even less complex and easy to implement in real time applications.

REFERENCES

[1] Rajendra V. Boppana and Anket Mathur, “Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks” Workshop on Next Generation Wireless Networks, December 2005

[2] M. Mohanapriya and Ilango Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET” Computers and Electrical Engineering, Vol. 40, pp. 530–538, 2014

[3] Wenjia Li and Anupam Joshi, “Security Issues in Mobile Ad Hoc Networks- A Survey”, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2008.

[4] Tiranuch Anantvalee and Jie Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks” Springer Wireless/Mobile Network Security, pp. 170 - 196, 2006

[5] Arvind Dhaka, Amita Nandal and Raghuveer S. Dhaka, “Gray and Black Hole Attack Identification using Control Packets in MANETs” Elsevier Eleventh International Multi-Conference on Information Processing, 2015

[6] K. Mahamuni, Dr. C. Chandrasekar, “Trust based Dynamic Source Routing protocol for MANET against Routing Attacks” Journal of Theoretical and Applied Information Technology , Vol. 77(1), pp. 1992-8645, 2015

[7] Rath B, “Implementing and comparing DSR and DSDV routing protocols for Mobile Ad Hoc Networking”, Doctoral dissertation, National Institute of Technology Rourkela, 2009

[8] Rao D. J., Sreenu k., and Kalpana P., “A study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks”, International Journal of Advance Research in Computer and communication Engineering, I (8), pp, 2319-5940, 2012