www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 8 Aug 2016, Page No. 17482-17488

Prevention of MANET from Co-Operative Black Hole Attacks

M.Dhipa[1], G. Kiruthika[2], K. Gayathiri [3], N. Rajkumar [4]

[1]SNS COLLEGE OF TECHNOLOGY, Assistant Professor Dept. of Electronics and Instrumentation Engineering, Saravanampatti, Coimbatore - 641035, Tamilnadu, India
dhipachandrasekar@gmail.com

[2]SNS COLLEGE OF TECHNOLOGY, UG Graduate Dept. of Electronics and Instrumentation Engineering, Saravanampatti, Coimbatore - 641035, Tamilnadu, India
kiruthika.g1212@gmail.com

[3]SNS COLLEGE OF TECHNOLOGY, UG Graduate Dept. of Electronics and Instrumentation Engineering, Saravanampatti, Coimbatore - 641035, Tamilnadu, India
gayathiri26.eie@gmail.com

[4]SNS COLLEGE OF TECHNOLOGY, UG Graduate Dept. of Electronics and Instrumentation Engineering, Saravanampatti, Coimbatore - 641035, Tamilnadu, India
rajkumar271260@gmail.com

Abstract - ***A mobile ad hoc network (MANET) is an infrastructureless wireless network and consists of mobile nodes. Secure communications among the mobile nodes are achieved by consequential challenges. These challenges are overcome by building the multiple security solutions that protect and enhance the network performance. One of the principal routing protocols used in Ad hoc networks is AODV protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. Black hole attack is one of the severe attacks that come from misbehavior of the node. The misbehaving node acts as selfish or malicious. Malicious node is also called black hole. The black hole intercepts the packet and confidentiality of the message is disclosed. Our approach to combat the Black hole attack is to make use of a 'Fidelity Table'. Fidelity level that acts as a measure of reliability of the node. And by the use of Fidelity Table blackhole was detected and eliminated. The simulation was carried using NS-2 and the performance of the network is analyzed after removal of black hole attack.***

Index terms -Mobile ad hoc network (MANET),Blackhole, Packet dropping, Malicious node, Routing.

INTRODUCTION

An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes.

Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. There are several applications of MANET ranging from a one-off meeting network, emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it. There is lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. We present a technique to identify black attack and a solution to discover a safe route avoiding black hole attack.

Overview of the project

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated.

MANET Challenge

Most of the routing protocols for MANETs are thus vulnerable to various types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very popular routing

algorithm. However, it is vulnerable to the well-known black hole attack.

Blackhole Attack

A black hole attack is used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network. Then, instead of forwarding the packets, the malicious node simply drops it. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed root reply packet to a source node that initiates a route discovery. The source node traffic can be deprived by malicious node. A variant of this black hole is the gray hole attack, which selectively transmits some packets and drops others. Other attacks towards an adhoc network include partitioning and replay attacks.

A blackhole node has two properties.

1. First, the node takes advantage of the ad hoc routing protocol, such as AODV or DSR, to advertise itself as having a valid route to the destination node, even though the route is spurious, with the intention to intercept packets.
2. Second, the node consumes the intercepted packets. This type of attack is dangerous and may cause immense harm to the network.

As an example, consider the following scenario in figure 2.3 Here node S is the source node and D is the destination node. Nodes 1 to 5 act as the intermediate nodes. Nodes 4 (B1) and 5 (B2) act as the cooperative Black holes. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2.3. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the destination or B1 forwards all the data to B2. B2 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

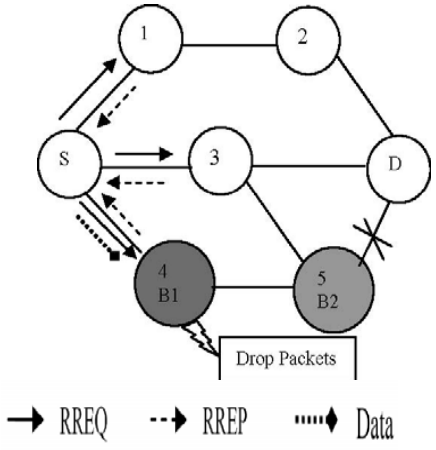


Fig 2.3 Example of blackhole attack

Ad-hoc On-Demand Distance Vector (AODV) Protocol

AODV is categorized as a dynamic reactive routing protocol [5]. In a reactive routing protocol, route will be established based on the demand (upon request by source node). Ad-hoc On-Demand Distance Vector (AODV) [13] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. In AODV route discovery, there are two important control messages namely Route Request (RREQ) and Route Reply (RREP). Both control messages carry an important attribute called destination sequence number and has the incremental value to determine the freshness of a particular route.

Route Discovery Process

In this, the source node will broadcast control packets, RREQ message to its neighbors in order to find the best possible path to the destination node. On receiving the RREQ message from node, the destination node will reply with the RREP message to node by forwarding the message to the node. In turn, node will forward the message to the source node.Once the source node received the RREP message, it will process the message by calling the AODV recvReply() function. This function will update the route entry for destination if either the destination sequence number in the routing table is less than the destination sequence in the RREP message or the destination sequence number in the routing table is equal with the destination sequence number in the RREQ message but the hop count is less than the one in the routing table. In case where source node received multiple RREP messages, this function will select the RREP message with the highest destination sequence number value.

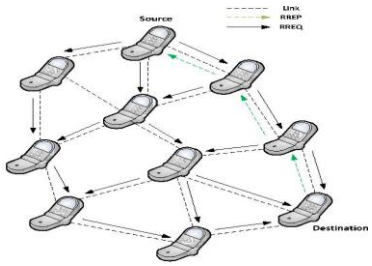


Fig 3 .3.1 AODV Route Discovery

Advanced uses of AODV

1. Because of its reactive nature, AODV can handle highly dynamic behavior of Vehicle Ad-hoc networks.
2. Used for both unicasts and multicasts using the 'J' (Join multicast group) flag in the packets.

RELATED WORK

Proposed Framework for Black Hole Attack Analysis

In this section we have proposed one algorithm, which is an enhanced version of the existing AODV protocol. The algorithm simulates the behavior of black hole attack in MANET using NS-2. In MANET world, when a node uses

AODV protocol it can act as vulnerable by implementing following properties

1. The node can set its hop count field to 1;
2. The node can increase the sequence number by at least one when compared to other nodes in the network;
3. It can set the source IP address to a non existing IP address;
4. It can unicast faked RREP message to the source node;

When a source node receives faked RREP message it updates its routing table towards nonexisting (malicious) node. In our simulation we have considered the property of "send Fake RREP" to the source node at a particular frequency by malicious node .It can be achieved by an increasing destination sequence number and reducing hop count. We have created a simple framework in which the attack can be occurred . Initially we have to check whether the particular packet belongs to AODV protocol. If it is AODV protocol we have to check whether it is RREQ packet. If it is RREQ packet the malicious node updates the sequence number and set its sequence number has the highest; not only that it also set the hop count field in 1 as discussed above. Thus the attack is successfully launched by a black hole node in MANET environment.

Ns-2 Simulation of Black Hole Attack Analysis

Now we discuss NS-2 implementation of this attack in detail.

Pseudo code to simulate the black hole attack

```
1: If (AODV_Packet) {
2: If (RREQ) {
3: If (I am the source or previously seen it) {
4: Drop the Packet
5: } else {
6: If {No Attack} {
7: Resolve the Route;
8: SendRouteReply;
9 :} else if (BlackHoleAttack) {
//The Black hole will send a genuine reply
10: Resolve the Route;
11: SendRouteReply;
12 :}
13: }
14 :} else {
15: Handle it in Normal way
16 :}
17 :}
18: else {
19: If (it is a packet which I am originating) {
20: Handle it in Normal way
21 :} else {
22: //it is the packet I am forwarding
23: If {No Attack} {
24: Handle it in Normal way
25 :} else if (BlakHoleAttack) {
26: //Maliciously dropping the packet
27: Drop the Packet
28 :} else if (BlackHoleAttack) {
29: //Maliciously dropping the packet
30: Drop the Packet
31 :}
32 :}
33 :}
```

PREVENTION OF CO-OPERATIVE BLACK HOLE ATTACK

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node.

In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated. The source node transmits the RREQ to all its neighbors. Then the source
waits for 'TIMER' seconds to collect the replies, RREP. A reply is chosen based on the following criteria, In each of the received RREP, the fidelity level of the responding node, and each of its next hop's level are checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the highest level.

The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented.

Working principle of PCBHA

Collecting response

The incoming responses are collected in a table, namely, the Response table. The entries will have fields like, source address, destination address, hop count, next hop, lifetime, destination sequence number, source and destination's header address. The responses will be collected till a timer expiry event. This is illustrated in figure 4.4.1.1.

DOI: 10.18535/ijecs/v5i8.09

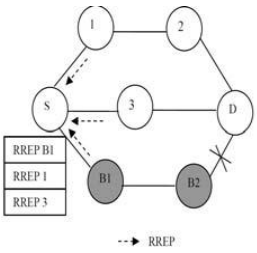


Fig 4.4.1.1 Collecting responses

4.4.1.2 Choosing a response

A valid route is selected from among the received responses based on the following methodology. A fidelity table' is maintained that will hold the fidelity levels of the participating nodes. The basic idea is to select the node with a high fidelity level. Initially the fidelity levels of the responded node and its next hop are looked for.

If the average of their levels is found to be above the specified threshold, then the node is considered to be reliable.

On the receipt of multiple responses, the one with the highest fidelity level is chosen. In case, two or more nodes seemed to have the same fidelity levels, then the one with the minimum hop count is chosen. As shown in Figure 4.4.1.2, the source S chooses the response RREP-3, as highlighted, after checking the fidelity levels. It then transmits the data packets.

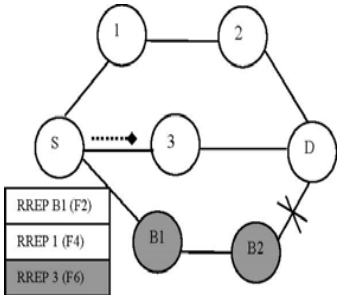


Fig 4.4.1.2 Choosing a response To forward data

Updating the fidelity level

Every destination node sends back an acknowledgement to the source node, upon the reception of the data packets. The receipt of the acknowledgement enables the source node to increment the fidelity level of the intermediate node, for it has proved reliable and safe. In case, the source node doesn't receive the acknowledgement within a timer event, the source node will decrement the fidelity level of the intermediate node which replied and also the level of the node which was given as the next hop of the intermediate node to identify the co-operative attack. This eliminates possible positive next hop information by a cooperative black hole. Periodically the fidelity tables are exchanged among the participating nodes. On receiving the acknowledgement,as seen in Figure 4.4.1.3, the fidelity levels of the respective nodes are incremented, and the fidelity packets are exchanged.

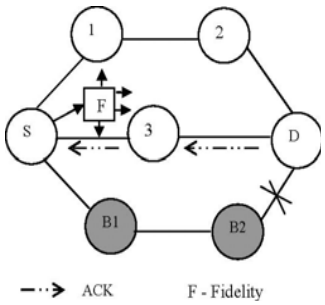


Fig 4.4.1.3 Receiving acknowledgement and broadcasting fidelity packets

Eliminating the Black holes

When the fidelity level of a node drops to 0, it implies it has not forwarded the data packets faithfully and hence a Black hole. The detection of a Black hole has to be intimated to the other participating nodes in the network. This is accomplished by sending alarm packets. When a node receives an alarm packet, it will identify the Black hole and so can eliminate the use of that node from then on. The final scenario where the Black holes have been detected and hence eliminated is shown in Figure 4.4.1.4.

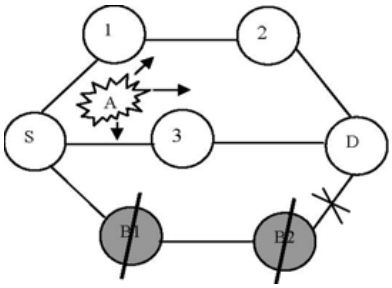


Fig 4.4.1.4 Black hole nodes elimination

Our proposed algorithm to detect black hole attack as follows

Notations:
RREQ : Route Request
RREP_COLLECT_TIME: Time for which responses(route replies) are collected
RSPT : Response Collection Table
IN : Intermediate Node
ACK_TIMEOUT: Time for which a node waits for ACK
ALGORITHM:

```
source broadcasts RREQ
while(simclock=current_time+RREP_COLLECT_TIME)
{
store in RSPT
}
if(size of RSPT = 0)
{
retransmit RREQ
}
else
{
find AVG_FIDELITY_LEVEL =FIDELITYIN +
```

```
FIDELITYnext hop
select route with highest AVG_FIDELITY_LEVEL
if FIDELITYIN > THRESHOLD and FIDELITYnext hop > THRESHOLD
{
send data
}
else
{
repeat until a maximum TTL value.
if not {
declare no valid route is found
}
}
}
while (simclock = current_time + ACK_TIMEOUT)
{
if RACK is received
{
increment the fidelity level of the IN
broadcast the fidelity packets
}
}
if (no RACK is received)
{
decrement the fidelity level of the IN and next hop
broadcast the fidelity packets
}
if (FIDELITY of a node = 0)
{
remove the node from neighbour table and fidelity table
broadcast alarm packets
}
```

Detection of Black Hole Attack using DBA-AODV

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated.

The source node transmits the RREQ to all its neighbours. Then the source waits for 'TIMER' seconds to collect the replies, RREP. A reply is chosen based on the following criteria, In each of the received RREP, the fidelity level of the responding node, and each of its next hop's level are checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the highest level.

The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented.

The algorithm for the proposed solution is as follows:

Notations:

RREQ : Route Request

RREP_COLLECT_TIME: Time for which responses(route replies) are collected

RSPT : Response Collection Table

IN : Intermediate Node

ACK_TIMEOUT: Time for which a node waits for ACK

```
source broadcasts RREQ
while(simclock=current_time+RREP_COLLECT_TIME)
{
store in RSPT
}
if(size of RSPT = 0)
{
retransmit RREQ
}
else
{
find AVG_FIDELITY_LEVEL =FIDELITYIN + FIDELITYnext hop
select route with highest AVG_FIDELITY_LEVEL
if FIDELITYIN > THRESHOLD and FIDELITYnext hop > THRESHOLD
{
send data
}
else
{
repeat until a maximum TTL value.
if not {
declare no valid route is found
}
}
}
while (simclock = current_time + ACK_TIMEOUT)
{
if RACK is received
{
increment the fidelity level of the IN
broadcast the fidelity packets
}
}
if (no RACK is received)
{
decrement the fidelity level of the IN and next hop
broadcast the fidelity packets
}
if (FIDELITY of a node = 0)
{
remove the node from neighbour table and fidelity table
broadcast alarm packets
}
```

DOI: 10.18535/ijecs/v5i8.09

Parameters	Values
Network size	1000m * 1000m
Number of nodes	25
Max speed/mobility	50 m/s
Wait/Pause time	10 s
Traffic model	CBR
Routing protocol	AODV
Packet size	512 Bytes
Number of attackers	25%
Simulation time	1000s
Number of sources	5
Transmission range	250m

Minimum threshold value used for the simulation is taken as 2 units as a test case. To find a valid route the proposed solution tries up to a maximum of RREQ_RETRIES TIMES at the maximum TTL value. Otherwise declare no valid route is found.

The working of DBA-AODV includes four steps. They are as follows,

1. Collecting response
2. Choosing a response
3. Updating the fidelity level
4. Eliminating the Black holes

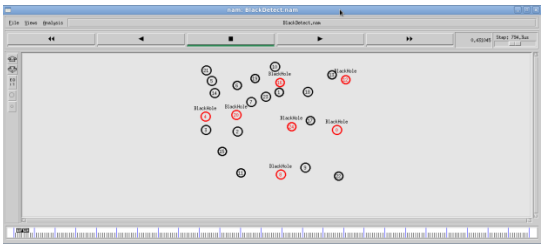
The percentage of packets received through our system is better than that in AODV in presence of cooperative black hole attack. The solution is simulated using the Network Simulator and is found to achieve the required security with minimal delay & overhead.

SIMULATION AND RESULTS

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2. The numbers of nodes we have considered for simulation are 25 mobile nodes in the terrain area of 1000m * 1000m. Around 25% of them to be attackers are assumed, which are performing Black hole attack. We have also used some CBR (Constant Bit Rate) connections with packet length of 512 bytes to emulate traffic over the network. Each node independently repeats this behaviour and mobility is varied by making each node stationary for a period of pause time.

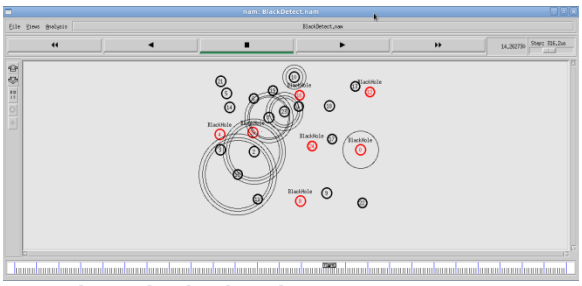
Table 1: Simulation Parameters

Network Setup:



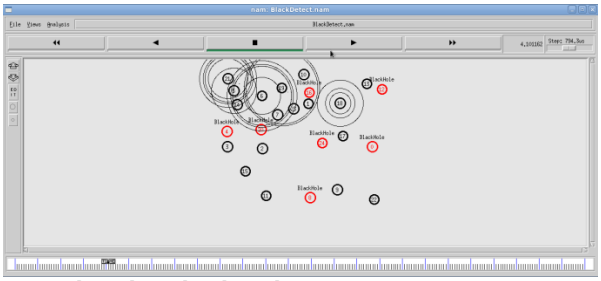
Black-Normal Nodes , Red-Malicious Nodes(Blackhole Nodes)

Case I: Data Packet Transmission with Elimination of Black hole Nodes.



S: 10→ 23→7→2→15→11:D,Here Nodes 16 and 20 are eliminated.

Case II: Data Packet Transmission with Elimination of Black hole Nodes.



S: 21→ 6→19→1→18→13: D, Here Nodes 16 and 4 are eliminated

Performance Evaluation

The metrics used in evaluating the performance are:

Packet Delivery Ratio:

It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes. It is clear from fig.4.7.1 that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV is immune to it. It is represented by P and calculated as:

$$P = \frac{number\ of\ data\ packets\ received}{number of\ data\ packets\ sent} * 100$$

The PDR decreases when there is malicious node (black hole) in AODV because some packets are dropped due to attack. This means the number of correctly received packet is very less than the number of transmitted packets.

This figure 4.7.1 confirms that while proposed AODV is secure against black holes, AODV is not. This is mainly due to the fact that our protocol detects the attacker and allows the source nodes to avoid it.

No. of Nodes	Packet Delivery Fraction	
	Normal AODV	DBA-AODV
20	580	805
40	610	830
60	700	840
80	735	868
100	765	873

DOI: 10.18535/ijecs/v5i8.09

Table 2: PDR vs. number of nodes

Network throughput

A network throughput is the average rate at which message is successfully delivered between a receiver (destination node) and its sender (source node). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are mentioned in: these are unreliable communication, changes in topology, limited energy and bandwidth.

Fig 4.7.3 shows the impact of the Black hole attack to the networks throughput. The throughput of the network also decreases due to black hole effect as compared to that without the effect of Black hole attack. We vary the speed of the node and take the result to the different node speed.

No. of Nodes	Throughput	
	Normal AODV	DBA-AODV
20	115	250
40	125	215
60	100	185
80	60	140
100	80	110

Table 3: Throughput vs. number of nodes

Performance Evaluation:

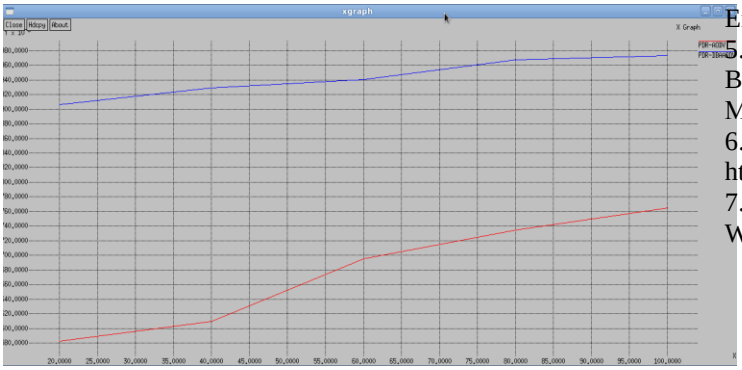


Fig 4.7.1 PDR vs. number of nodes

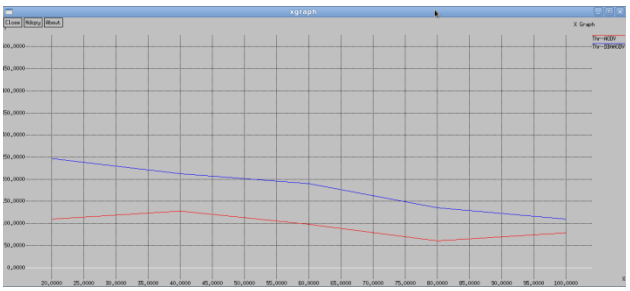


Fig 4.7.2 Throughput vs. number of nodes

CONCLUSION

In this project we have presented a feasible solution to detect the malicious nodes(Black Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the malicious nodes.

FUTURE WORK

As future work we intend to -

1. Develop simulations to analyze the performance of the proposed solution.
2. Future works will includes some authentication mechanism to make sure that the ACK packets are genuine and also includes mechanism to punish misbehaving nodes.

REFERENCES

1. Isaac Woungang, Mohammad S. Obaidat, Rajender Dheeraj Peddi, Sanjay Kumar Dhurandher, (2012)'Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks', IEEE.

2.Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee,(JANUARY 2012.) 'Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks', IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 1.

3.Ziming Zhao, Gail-Joon Ahn, (MARCH/APRIL 2012) 'Risk-Aware Mitigation for MANET Routing Attacks' IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2.

4.Sandeep Lalasaheb Dhende, Prof. Mrs. D. M.Bhalerao,(August 2012) 'Detection/Removal of Black Hole Attack in Mobile Ad-Hoc Networks',International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 6.

5.Akanksha Saini, Harish Kumar,(December 2010) 'Effect Of Black Hole Attack On AODV Routing Protocol In MANET',IJCST Vol. 1, Issue 2.

6.IETF MANET work group. http://www.ietf.org/dyn/wg/charter/manet- charter.html

7.C.Siva Ram Murthy and B.S.Manoj, A text book on Ad Hoc Wireless Networks.