International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference On Emerging Trends in Mechanical and Electrical Engineering (ICETMEE- 13th-14th March 2014)

RESEARCH ARTICLE OPEN

An Effective way for Detection of Single & Colabrative Blackhole Attack in MANETs

Shilpi Agrawal[*],Nidhi Saxena[**],
[*]ECE Department, Institute of Technology and Management Gwalior
[1]sshilpi.agrawal@gmail.com
[**] ECE Department, Institute of Technology and Management Gwalior
[2]nidhi.saxena1803@gmail.com

ABSTRACT
Wireless networks are of two categories i.e. fixed infrastructure and infrastructure less. Mobile Ad hoc Networks (MANET) are among second category i.e. MANET's are such wireless networks in which the nodes can move from one place to another place and thus have no fix infrastructure or topology. This type of networks crate dynamic topology. The nodes of these types of networks find or search the route dynamically in case when a node wants to communicate with other node and thus use adaptive or dynamic routing. For this they mostly prefer the on demand type routing protocols. These network having significant importance into many real life and home applications such as military applications etc. These networks are highly adaptive nature and due to this, these networks can be attacked by a lot of security attacks like Denial of service attack, wormhole attaches, grayhole attack and blackhole attack. it is a dangerous active attack in which a node or couples of nodes give the fake routing information and thus captures all the packets coming through this node. In this paper an effective approach is provided for the detection & correction of the blackhole attack.

Keywords — AODV, DSR, Black hole Attack, DSN, SSN, Selfish Node, On Demand Routing Protocol, Table Driven Routing Protocols.

I. INTRODUCTION

Wireless Networks can be divided into two main categories: Fixed Infrastructure Wireless networks and Infrastructure less Wireless Networks.

A Fixed Infrastructure Wireless network provides communication among wireless nodes through the Access Point (AP), not directly. In these the types of the networks the communication is wireless but the nodes cannot move from their place.

An Infrastructure less Wireless Network is the wireless networks in which the nodes can move from one place to another place and thus has no fix infrastructure or topology. This type of networks crate dynamic topology. The nodes of these type of networks find or search the route dynamically only when a node wants to communicate with other node and thus use adaptive or dynamic routing. For this they mostly prefer the on demand type routing protocols. They networks are showing significant importance into many real life and home applications such as military applications etc. These networks are highly adaptive nature.

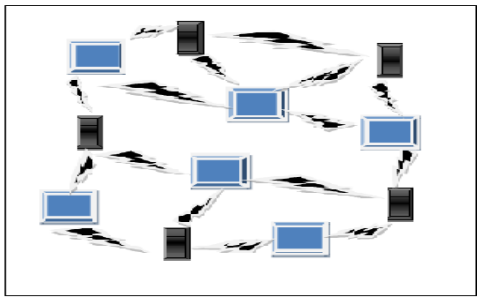


Fig. 1 Mobile Adhoc Networks

II. ROUTING PROTOCOLS FOR MANETS

Mobile ad hoc networks have a lot of routing protocols depends on the type of the service required.

A. Page Layout

On the basis of the routing information updates, there are three types of routing protocols:

(i) Table Driven or Proactive Routing Protocols

(ii) On Demand or Reactive Routing Protocols

(iii) Hybrid Routing Protocols.

1) Table Driven or Proactive Routing Protocols

In this type of protocols each and every mobile node contains a table, called routing table and maintains the routing information in this table. After a particular period, if updates the information in the routing table, if there exist any routing update. DSDV, WRP protocols comes under this category [3].

2) On Demand Routing Protocols

In these types of routing technique, the mobile nodes don't maintain any routing table. The shortest route between source and the destination is finding only when some node want to communicate with other node, the route request is generated dynamically and the route response is also. Instead of maintaining a routing table every node maintains a route cache. DSR, AODV, TORA protocols comes under this category [4].

3) Hybrid Routing Protocols

These types of protocols are simply the combination of the proactive and reactive routing protocols. These types of protocols combine the best features of the both protocols. Zone Routing Protocol (ZRP) is the best example of this category.

III. AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) protocol is a pure on demand routing protocol which enables dynamic, self-starting, multi hop routing among the mobile nodes in the mobile ad hoc networks. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The best thing about the AODV is that AODV provides the loop-free route and also by using the link state routing technique it removes the "counting to infinity" problem and provides quick convergence when the ad hoc network topology changes.

AODV has three types of messages:
Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs).

To find the route to the destination, the source node generates a RREQ and broadcasts it to its neighbors [6]. When the destination get the RREQ packet it prepares a reply packet to the source, called route reply (RREP) packet and unicast it to the source node. All the intermediate nodes which receives the RREQ packet caches a route back to source node. A RERR message is used to notify other nodes When a link break in an active route is detected. The RERR message contains the information about those destinations which are unreachable though any broken link.

IV. THE BLACKHOLE ATTACK

Blackhole attack is a type of DoS attack which a router discards the packets. It is mainly occurs from a router which is compromised from a number of different types of causes. One of them cause mentioned in research is by a denial-of-service attack on the router using a known DoS tool. Because packets are routinely dropped from a lossy and busy network, so that the packet drop attack is very tough to detect and prevent.

However, if the malicious router begins dropping packets on a specific time period or over every *n* packet, it is often harder to detect because some traffic still flows across the network.

As shown in the following figure (fig.2), black hole attack behaves like the black hole available in our galaxy, which absorbs all the things in its own and develop very harmful environment for our universe.

Fig. 2 Blackhole attack in galaxy

Black hole attack is dangerous active attacks on the Mobile Ad hoc Networks. A black hole attack is performed by a single node or combination of nodes as shown in figure 1. This attacker node is also called selfish node. In Black hole attack an attacker node sends a fake Route reply (RREP) message to the source node which initiates the route discovery procedure order to find the route to the destination node. When the source node received multiple RREP, it selects the greatest one as the most recent routing information and selects the route contained in that RREP packet [5]. In case the sequence numbers are equal it selects the route for which the hop count is minimum. Then the attacker drops all data packets rather than forwarding them to the destination node [6].

As shown in Figure 3 below, source node 1 broadcasts an RREQ message to discover a route for sending packets to destination node 3. An RREQ broadcast from node 1 is received by neighboring nodes 2, 4 and 5. However, malicious node 5 sends an RREP message immediately without even having a route to destination node 3. The RREP message sent by the malicious attacker node is the first message reaches to the source node .When the source node

receive the message sent by the malicious attacker node, updates its routing table for the new route for the intended destination node and then also discards any RREP message from other neighboring nodes even from an actual destination node.

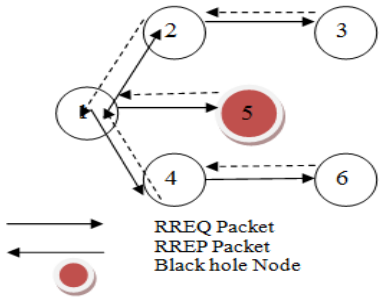


Fig. 3 Blackhole attack in MANETs

Blackhole attacks can be classified into two types:

(i) Single Blackhole Attack

(ii) Co-operative or Collaborative Blackhole Attack

Single blackhole attack, is a type of DoS attack in which a router instead of discards the packets that is supposed to relay all the packets. This is mainly occurs from a router which is compromised from a number of different types of causes.

In collaborative or Co-operative Blackhole attack multiple malicious nodes combined and coordinate malicious activities against some particular node [53]. In this type of attack, the first blackhole node send the packet to another blackhole node and also every blackhole node have the complete information of every other blackhole node.

V. RELATED PREVIOUS WORK

Black hole attack is one of the most dangerous attacks. Many researchers did their work on this attack and try to provide the solution for this attack. The researchers provide a lot of solution based on different technologies, concepts and terms. Some important approaches are described below:

Sowmya K.S. et al. [7] proposed a simple and efficient mechanism for providing the security against the blackhole attack in the mobile ad hoc networks based on the AODV routing protocol. In this algorithm, known as ACO, an optimal path is used which is based on one of the many parameters such as fully distributed approach. In the given approach the operations are performed in each node in a very simple manner. The method is based on the asynchronous and autonomous interaction between agents. The algorithm is robust and fault tolerant so there is no need of defining path recovery algorithms.

M. Umaparvathy et al. [8] proposed a modified new protocol called as TTSAODV Protocol to identify single as well as collaborative black hole attack in mobile ad hoc networks. This protocol verifies the trueness of the RREP message through the Verification messages sent by neighboring nodes. The basic assumption in this solution is that there is a strong symmetric key distribution system in the MANET. Thus, every pair of nodes in the network has unique common secret key. In the proposed protocol, two levels of security are provided. One level is during the route discovery process and the next is during the data transfer. Even if the detection of Black hole attack fails at the route discovers process, in the next level, it will be identified. So, the proposed protocol has high degree of attack detection and prevention.

Amol Bhosle et al. [9] proposed an efficient solution for the detection of the Blackhole nodes in the Mobile Ad hoc networks based on the AODV routing protocol In this algorithm, known as Modified AODV mechanism a Watchdog mechanism is used. In this mechanism each and every node maintains two extra tables. First one is called the pending packet table and another one is called the node rating table. Pending Packet Table contains Packet ID, Next Hop, Expiry Time and Packet Destination while the Node Rating Table contains Node Address, Packet drops, Packet forwards and Misbehave. For the communication each and every node listens to those packets that are within the communication range of that particular node a threshold value is used for the detection of whether a node is malicious or not and also a node can repair all the nodes locally which contains the malicious node.

Sarita [10] proposed a solution for the detection of the Blackhole and Grayhole attacks in mobile ad hoc networks. The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN. Source node on receiving the RREP takes the following steps

Step 1: If the RREP is received only to the Destination & not to the Restricted IP (RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole detection, by sending a request to enter into promiscuous mode, to the nodes in an alternate path (i.e. neighbors of next hop for RIP).
Step 3: Now, finally the detection of the Blackhole attack the feedback is analyzed which is sent by the alternate paths and then this information is propagated throughout the network leading to the revocation of the Black Holes certificates.
Deng [11] proposed a SIDSR mechanism that detects the BHA attacker when an attacker node sends the RREP packet. In the SIDSR mechanism, when the source node receives a RREP packet from the suspected attacker node , the source node sends a Further Route REQuest (FRREQ) packet to the next hop through a new route to verify that a particular node has a route to the black hole node ,which sent back the RREP packet and announce that it has a route to the destination. As soon as the next hop receives the FRREQ packet, it sends a Further Route Reply (FRREP) packet to the source node. The source node checks the FRREP Packet information and acts according to the following rules:

1. If the next node has routes to the destination node and intermediate node, the source node assumes that node is trusted node and it establishes the route received from that node.
2. If the next hop node has a route to the destination node but does not have a route to the intermediate node, the source node assumes that this node is an attacker node. After that, the source node starts routing through the new route to the next hop and broadcasts an alarm message to isolate the intermediate attacker node.
3. If the next hop does not have routes to the intermediate node and the destination node
   The source node will initiate a new route request.

The SIDSR mechanism is efficient in detecting a Blackhole attacker node, but still this approach has a lot of drawbacks and limitations. Firstly, re-sending a FRREQ packet from the source node towards the next hop and waiting for the FRREP packet from the next hop means increasing routing overhead packets between the source and the next hop node, especially when this mechanism is applied on a large-scale MANET and the distance between the source node and the attacker node is very much. Second, if the source node and the attacker node is so far, then the delay in the discovery period of the route definitely will be high, by which the overall performance of the network get degraded.

Golok Panda [12] proposed a new algorithm based on AODV routing protocol. In AODV,
There is a HELLO message is broadcasted to its neighbor for showing the presence in network. There is also a routing table maintain by all nodes for temporary basis those who are in active state. The total bits consume by these routes discovery and route maintenance is 32 bit each. The proposed algorithm is based on the Key Mechanism process. Key Generation process contains 5 steps:
1. Consider the IP address of node
2. Conversion process of IP address into binary form (X).
3. X << 12
4. Z = X AND Y (Y bit stream)
5. Key (K) = 9 bits of Z

The spooler always tries to trace the subnet of IP address. Due avoid this attack we take 12 digit left shift of the binary numbers. Then they take an AND operator for reshuffling or making the number to very complex. After key generation completed, the key will be fitted in the 9 bits reserved sector in packets. The packet has information about originator IP address, Destination IP address, Destination Sequence no., Hope count and Life time. The HELLO message has been broadcasted to its neighbor nodes. When the node got HELLO message then next pseudo code will be applied for confirmation about the node's status. After comparing the both key, the trust value will be decided. The result shows that 1 then the node will be normal or trusty node. If the result shows that 0 then the node will be malicious. The key comparison value will be updated in routing table time to time.
Yibeltal Fantahum Alem [13] proposed an approach for the detection of the black hole attack based on the Intrusion Detection Systems (IDS) .Intrusion detection can be done by two types: network based intrusion detection and host based intrusion detection. Basically network based intrusion detection works on switches, routers etc. In the mobile ad-hoc networks there is no central coordinator that monitors the traffic flow among the mobile nodes. They proposed the technique based on the anomaly detection by using host based Intrusion detection system. In this system every activity of a user is monitored and anomaly activities of an malicious node is identified from normal activities. To detect a black hole this system needs to be provided with a pre-collected set of anomaly activities called audit data. The system compares every activity with audit data. And if it found that any activity of a host is looking like out of the activity provided in the audit data, it isolates that particular node from the network.

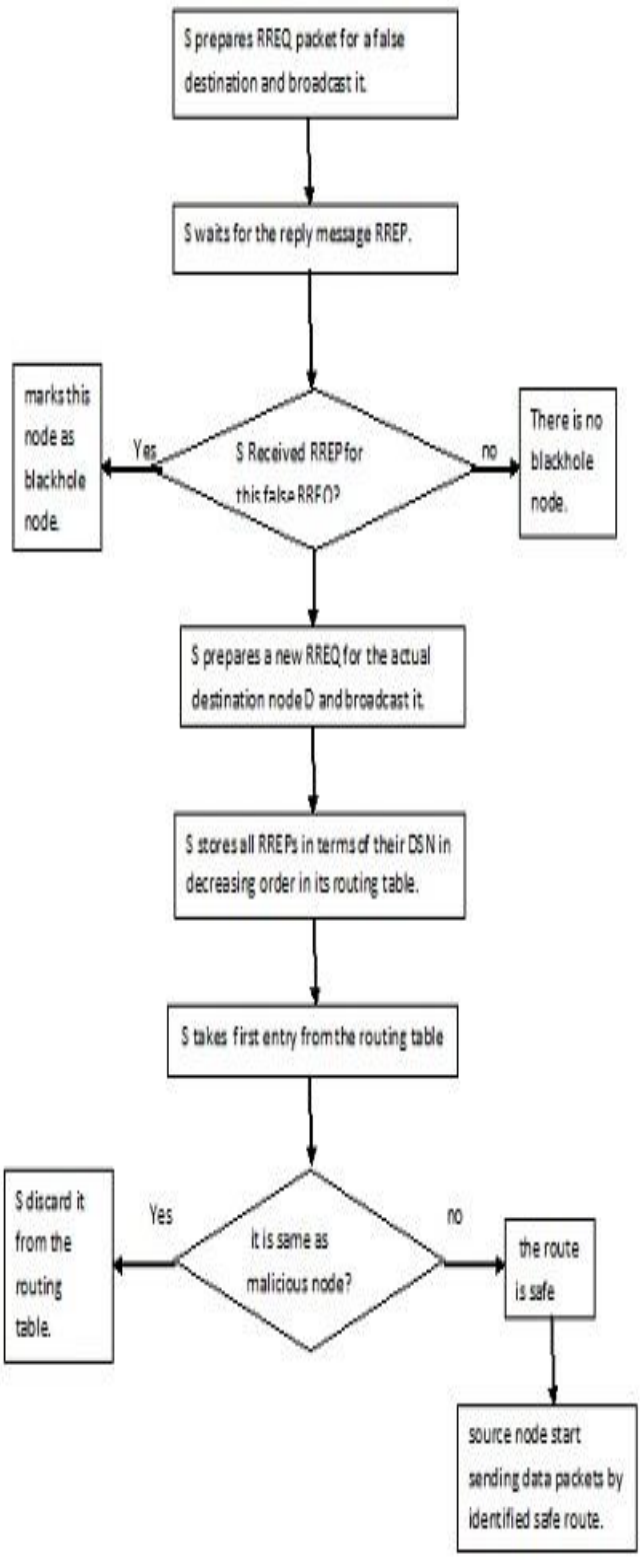
Firoz Ahmed [14] proposed an efficient method for the detection of the Black hole attack in the Mobile Adhoc Networks known as the Encrypted Verification Method (EVM). In this proposed approach when A detection node receives an RREP message from a suspicious node sends an encrypted verification message directly to destination along the path included in the RREP for verification. This approach is very efficient since it not only detects the Black hole nodes but reduces control overhead as well. The verification process is initiated conditionally and it verifies the sequence number that was not faked by any malicious node.

VI. PROPOSED WORK

In this paper an efficient and robust approach is described for the detection of the blackhole attack in MANETs. The appeoch is given below:

1. S prepares RREQ packet for a false destination and broadcast it.
2. S waits for the reply message RREP.
3. If S receives RREP for this false RREQ from some node, it immediately stores the address of that replying node and marks this node as the malicious blackhole node.
4. else it marks that there is no malivious node.
5.now, S prepares a new RREQ for the actual destination node D and broadcast it.
6. S stores all the replies RREPs in terms of their DSN in decreasing order in its routing table.
7. S takes the first entry from the routing table(i.e., which has the highest DSN) and chech if it is same as the malicious node.
8. if the address of the top entry in the routing table is same as the identified malkicious node, S discard it from the routing table.
8. else the route is safe.
9. source node start sending the data packets by the identified safe route.

The flow chart is given in the figure below:



VII. SIMULATION RESULTS

A. Simulation Parameters

Simulation parameters are given in the table below

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-2
Version	NS 2.34
Number of Nodes	20
Topography Dimension	1000 m x 1000 m
Traffic Type	CBR
Signal Prop. Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Antenna Type	Omni directional
Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Max pkts in IFqueue	60
Channel	Wireless Channel
Max/Min Movement Speed	60 m/sec.
Min Movement Speed	20 m/sec
Pause Time	15 sec.
Simulation Time	200 sec.

B. Simulation Results

Three parameters End to End Delay, Packet Delivery Ratio and Throughputs show the simulation results. Every graph contains two sub-graphs in which red color sub graph Shows AODV with attackers. And the green color subgraph shows AODV with implemented algorithm.

1) Throughput Graph

This parameter describes the total number of bits send to the physical layer per second (Kbps).

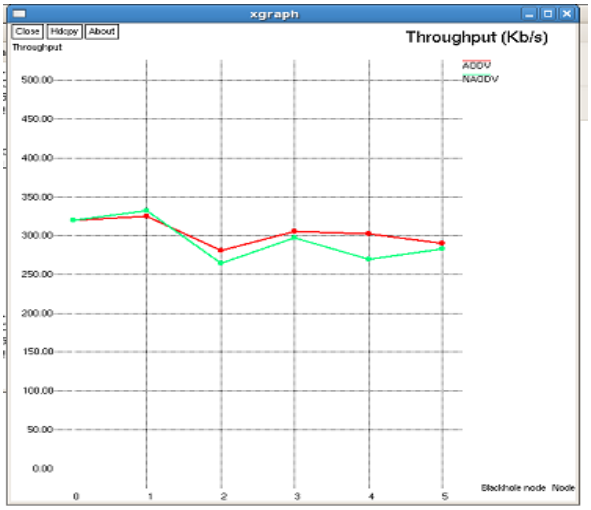


Fig. 4 Throughput Graph for 20 mobile nodes

2) Packet delivery Ratio Graph

This parameter describes the ratio of total incoming packets and actual received packets by the destination.

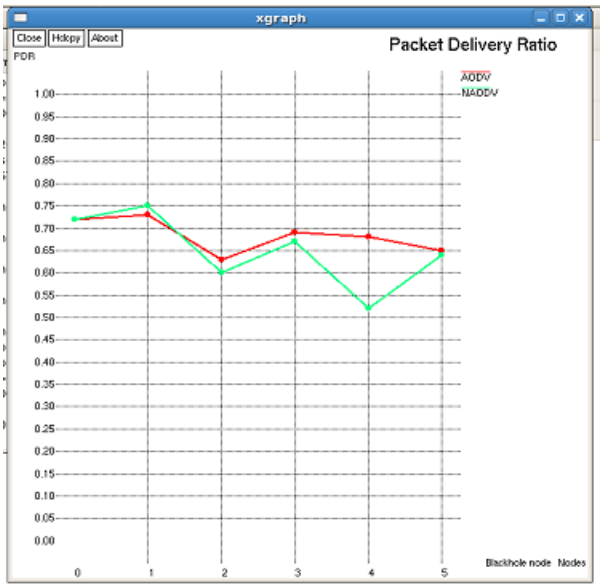


Fig. 5 PDR Graph for 20 mobile nodes

3) Average End to End Delay Graph

This parameter describes the average time to send a packet from source to the destination.

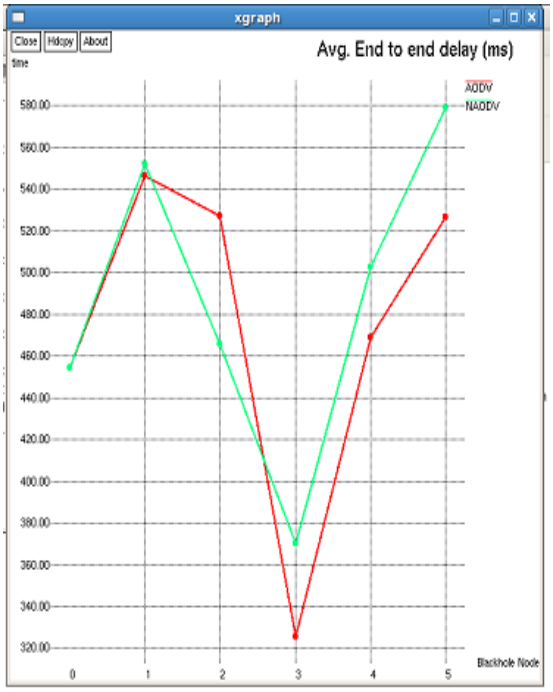


Fig. 6 End to end delay Graph for 20 mobile nodes

Figure 7 below showing the initial simulation of 30 mobile nodes in NAM.

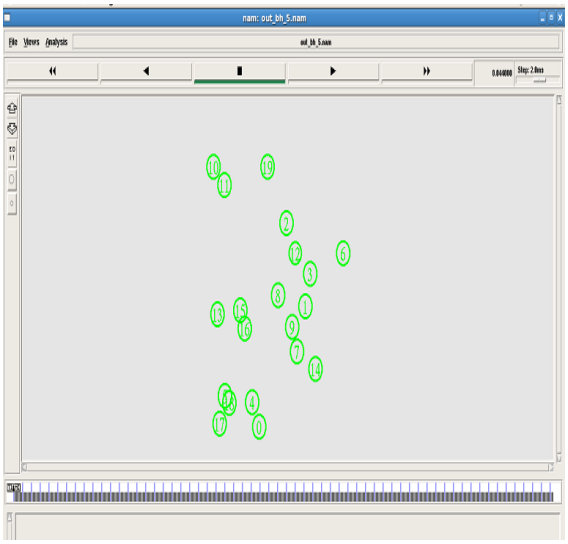


Fig. 7 Initial Simulation of 20 mobile nodes in NAM

Figure 8 below showing the simulation of 30 mobile nodes with five attacker node in NAM.

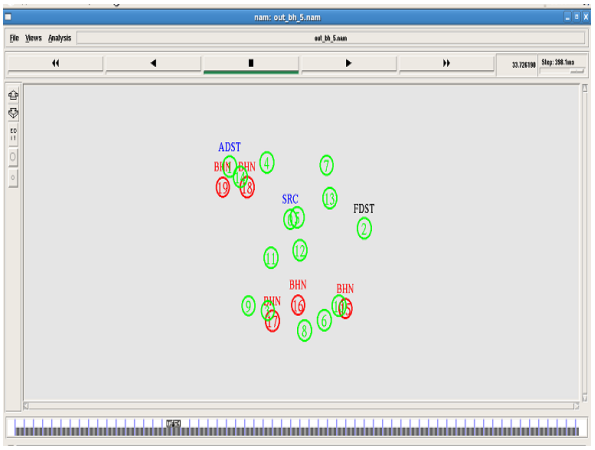


Fig. 8 Simulation of 20 mobile nodes with 5 attacker nodes in NAM

VIII. CONCLUSION AND FUTURE SCOPE

MANETs crate dynamic topology. The nodes of these type of networks find or search the route dynamically only when a node wants to communicate with other node and thus use adaptive or dynamic routing. For this they mostly prefer the on demand type routing protocols. They networks are showing significant importance into many real life and home applications such as military applications etc.

In this research paper an effective approach is provided for the detection of the blackhole attack in AODV based MANETs. The proposed approach is used to detect the cooperative blackhole attack.

As the future work, we want to develop an efficient approach for the detection and identification of the Blackhole attack for the very large network (near about 1000 or more mobile nodes) with the requirement of very less hardware.

REFERENCES

[1] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248.

[2] "Ad Hoc Wireless networks" By Shivarammurthy, Pearson Education

[3] T. Lin, S. Midkiff, and J. Park,"A framework for wireless ad hoc routing protocols", in WCNC: Wireless Communications and Networking. IEEE Computer Society, 2003, pp. 1162.1167.

[4] Arun Kumar, lokantha Reddy and Prakash Hiremath, "Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[5] K. Lakshmi, S.Manju Priya, A. Jeevarathinam K.Rama, K.Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology.

[6] Hongmei Deng, Wei Li, Dharma, P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[7] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of Blackhole Attack in MANET Using ACO", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012 21

[8] M. Umaparvathi, Dharmishtan K. Varughese, "Two Tier Secure AODV against Black Hole Attack in MANETs", European Journal of Scientific Research ISSN 1450-216X Vol.72 No.3 (2012), pp. 369-382

[9] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre,"Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012 DOI: 10.5121/ijcsea.2012.210545.

[10] Sarita Choudhary, Kriti Sachdeva,"Discovering a Secure Path in MANET by Avoiding Black Holes", International Journal of Recent Technology and Engineering (IJRTE) SSN: 2277-3878, Volume-1, Issue-3, August 2012.

[11] Deng, H., W. Li and D. Agrawal, 2002. Routing security in wireless ad hoc networks". IEEE communications magazine, 40(10): 70-75.

[12] Firoz Ahmed, Seok Hoon Yoon and Hoon Oh," An Efficient Black Hole Detection Method using an Encrypted Verification Message in Mobile Ad Hoc Networks**",** International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012 .

[13] Lalit Himral, Vishal Vig, Nagesh Chand," Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST).

[14] Yibeltal Fantahum Alem & Zhao Hheng Xaun, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection ", from Tainjin 300222, China 2010, IEEE Vol.2 (6), 2010.