ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

# Mitigating Black Hole Attack on MANET with AOMDV Protocol

Dr.T.Pandikumar[1], Biruk Zewdie[2], Capt.Zinabu Haile[3]
Associate Professor[1], M.Tech Student[2, 3]
Department of Computer & IT
College of Engineering, Defence University, Debre Zeyit, Ethiopia

**Abstract:**
The rapid usage of wireless devices and spreading of many mobile devices and applications has transformed wireless network security. One of well-known types of network which require high security is the Mobile Ad hoc Network (MANET). The term "Ad hoc" means self-organized nodes that do not have a central object to manage. MANET suffers from several attacks due to lack of centralized governing system. The old-fashioned way of defensive the networks from attacks by only encryption software and firewalls is no longer sufficient. One of the difficult attacks in MANET is the Black Hole Attack against network integrity by absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. Black Hole Attack harm mobile node by falsely replies to the source node that it is having a shortest path to the destination without checking its routing table. Therefore source node sends all of its data to the black hole node and it swallow all the packet sent from source node. In this thesis, a measureable technique applied for mitigating black-hole nodes in the Mobile ad-hoc network. The proposed method applied anomaly based Intrusion Detection System (IDS) which protects the confidentiality, integrity and availability of nodes in MANET. This method is verified by running simulations by NS2 with and without black hole attack on mobile nodes via the AOMDV (Ad hoc on Demand Multipath Distance Vector) routing protocol. The performance metrics shows that IDS able to achieve a remarkable result of packet delivery ratio up to 99.75%.

**Keywords:** MANET, IDS, AOMDV, black hole, NS2

## 1. INTRODUCTION

With the high spread of cheaper, smaller, and more powerful mobile devices, mobile *ad hoc* networks (MANETs) have become one of the fastest growing areas of research. MANETs are independent and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, MP3 player and personal computer that are participating in the network are mobiles. These nodes can act as host/router or both at same time. They can form arbitrary or random topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. (Ullah and Rehman, 2010)(John and Thomas, 2012) The term ad hoc implies that this network is established for a special, often wireless service customized to specific applications. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an infrastructure, it is not adequate or cost effective. The absence of a central coordinator and base stations makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks. (Bansal, 2014) There are many MANET application is on practice on today's world. As the result, MANET can be established anywhere where the nodes have connectivity with other nodes and can join and leave the network at any point of time. The applications of the MANET are *Emergency Service;* in this case it can be used in emergency operations such as, search and recovery from disasters like fire, flood, volcano eruption, earthquake, etc. Information is transmitted from one team member to another over a small portable device. In addition to that it can be used on *Military;* in such application area by using MANET the communication can be established among the soldiers, vehicles, and headquarters of military. *Commercial environment* also MANETs application for business firm so as to share the daily updates of administrative works among departments. (Shaik, 2014),(Journal and Science, 2016; Khasdev, 2016)

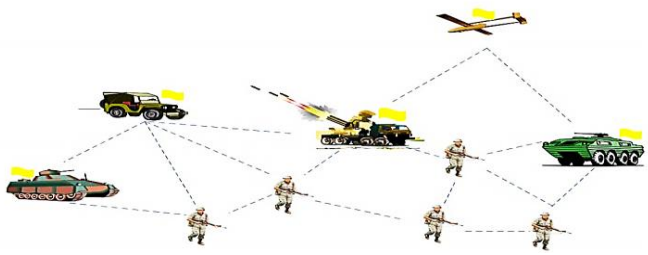

**Figure.1. MANET in the military operations (Lambert, 2013)**

### 1.2 Statement of the Problem

The goal of network is to guarantee effective and secure transmission between the nodes in the network in by creating secure atmosphere. In this work, a black hole attack is elaborated in MANET centered on AOMDV routing protocols and the study also investigate impacts of black hole attack including how this attack damages the communications of nodes on MANET. Previously researches are conducted on Black Hole attack involved in MANET centered on Ad Hoc On Demand Distance Vector (AODV) Protocol.

Therefore, by using AODV routing protocol researches describe how black attacks interrupt the communication of MANET. However slight attention has been given to Black Hole attack in MANET using AOMDV Protocol. There for

this proposed work pinpointed on AOMDV Protocol to mitigate black hole attack.

## 1I. LITEARTURE REVIEW

### 2.1 Literature Review at International Level

A thesis work written by Semih Dokurer which title is "SIMULATION OF BLACK HOLE ATTACK IN WIRELESS AD-HOC NETWORKS" (SEMIH, 2006)describes the Mobile- Adhoc Networks and black hole attack at different views and its impact on the adhoc communication. The writer main focus is to investigate the causes and initial points of the attack and how the attack can create a forged short route that enables the attacker to attract all sending packet and drop the entire packet. This thesis uses Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol 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. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. The proposed solution of the writer is by simulating AODV Protocol by adding a black hole node to the protocol and changes it to "blackholeaodv". The writer also cloned (copies) the "aodv" protocol, changing it to "idsaodv" as it did "blackholeaodv" before. The solution tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start to send the packets. The writer uses UDP protocol for the reason that, if TCP is used the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets. This is the solution to find the black hole attack. A Journal which titled as "SOLUTION TO BLACK HOLE ATTACK IN AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL" (Ibrahim and Zaki, 2015)it is an input which clearly clarifies the black hole attack and its mitigation mechanism. In this paper the writers proposed a mechanism to modify the AODV protocol by adding encryption/decryption features to Overcome Black Hole attack using pre-shared key. For encryption and decryption feature the writers implement CESAR cipher. These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text three positions. Any encryption/decryption algorithm with symmetric key can be implemented here. When using encryption the writers can use any kind of algorithms like SHA-1, MD5, AES, DES and so on. Since the complexity of these algorithms the writers chose a simple polynomial algorithm to implement it. The RREQ message at the source node is encrypted before forwarding to the neighbors, Nodes which know the pre-shared key can decrypt the RREQ correctly and generate the RREP message and send it to the source node, the source node received the trusted RREP starts to establish route to destination.. Consequently the Black Hole node can't decrypt RREQ. The writers implemented the proposed mechanism using the Network Simulation program NS2.(Ibrahim and Zaki, 2015) The succeeding proposed methodology is written by Neetika Bhardwaj and Rajdeep Singh "DETECTION AND AVOIDANCE OF BLACKHOLE ATTACK IN AOMDV PROTOCOL IN MANETS" (Bhardwaj and Singh, 2014) the proposed method by the writers is to detect black hole attack by sending the data packet through all possible routes, after sending a random number of packets. The destination node is modified to receive packets and compare them. If black hole nodes have caused an exposed attack then the destination will come to know about it as the data packet will not be received by it from the active route and it will then send Finish packet through the other route. The sender after receiving FINISH will stop forwarding data through the current route by purging the current entry from the routing table and will send packets through alternate route present in the routing table. This whole procedure will be repeated after sending of data packets which are exponentially more than the previous one until the whole transmission has been done. This is done to ensure that if the other route selected for communication is affected by black hole nodes then it can also be avoided. Also by increasing the counter exponentially, the overhead of sending packets through all routes can be brought down.(Bhardwaj and Singh, 2014)

The writers proposed routing is based on DSR with modification for detection of black hole attack. It is divided into two phases: Detection before route establishment and avoidance of malicious nodes during data forwarding. This algorithm has been designed based on the concept that malicious node may drop the packet or modify the packet. The DSR is modified to contain new header called Trap Header (TH). During detection phase, the nodes first sources the entire two hop neighbor node id's and sends trap packet with TH consisting of invalid data destination to its two hop neighbors. If the receiving node states that it has the route to the invalid destination in its cache, and has forwarded the data packet to next hop then the node is assumed to be a black hole malicious node. This information about the maliciousness is stored in the nodes. During route discovery, the nodes cross check the routes in its cache and if the route consists of a malicious node, the node invalidates that route and starts a fresh route discovery avoiding the malicious node. Thus, the proposed mechanism mitigates the black hole attack by a simple mechanism of trapping the malicious nodes and avoiding it in any of the routes during transmitting data packets. "Dynamic Training Intrusion Detection Scheme for Black-hole Attack in MANETs" (Naveena, 2012) In this paper, the writer propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of the writer scheme compared with conventional scheme. However, in MANET where the network state changes frequently, the pre-defined normal state may not accurately reflect the present network state. In this paper, the writer use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing for analysis of the effect of the black-hole attack when the destination sequence numbers are changed via simulation. Then, a feature is selected in order to define the normal state from the characteristic of black-hole attack. Finally, the writer present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment. "Analysis and Detection of Black Hole Attack in MANET" (Saini and Saroha, May-2013) In this paper a mechanism based on FUZZY LOGIC is proposed to detect the black hole attack in MANET with AODV protocol. An introduction of black hole in MANET with NS2 (2.35) is done, after applying the detection technique result reflects the performance. This paper is intended for audience having prior knowledge about network routing protocols and its related quantitative performance metrics. In this paper an implementation of black hole in wireless network is presented and the analysis is performed using AODV protocol with fuzzy logic detection system. The performance metric is based on different fuzzy parameters

1)Packet lost 2)Last packet time 3) Bitrate 4)Packet loss rate5)Packet delay. *Enhance Black-Hole AODV (EBAODV) (*Rachh et al. 2014 letter revised by Noureldien, 2015) proposed an Enhance Black-hole AODV solution (EBAODV). In this solution, what is called leader nodes are created first, these nodes are responsible for detection of malicious nodes. After sending the first Routing Request message (RREQ) a timer is started. If a RREP is received before the timer is expired, then one stale packet will be send to the destination. To ensure that the stale packet is received by the destination, the source node must receive acknowledgement (ACK) from the destination. When the source node receives the acknowledgement it sends the original packet.

## I1I. METHDOLOGY AND IMPLEMENTATION

### 3.2. Wireless networking in NS-2

#### 3.2.1. Mobile Node

The wireless networking in NS-2 essentially consists of the Mobile Node at the core. Mobile Node is the basic ns Node object with added functionalities like ability to move within a given topology, and to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. Moreover, routing in mobile networks especially in Ad-hoc networks is distributed and there is no centralized entity (as router in wired network). Therefore a mobile node acts as a router and as a node at the same time. (Project *et al.*, 2008)

#### 3.2.2. Node movement

The mobile node is designed to move in a three dimensional topology. However the third dimension (Z) is not used. That is, the mobile node is assumed to move always on a flat topography with Z always equal to 0. Thus, the mobile node has X, Y, Z (=0) co-ordinates that is constantly adjusted as the node moves. The mechanism to make the movement in mobile nodes is by starting position of the node and its future destinations must set clearly. The starting position and future destinations for a mobile node may be set by using the following APIs:

```
$node set X_ \<x1\>
$node set Y_ \<y1\>
$node set Z_ \<z1\>
$ns at $time
$node setdest \<x2\> \<y2\> \<speed\>
```

**Figure 2: Node movement in NS-2**

At $time sec, the node would start moving from its initial position of (x1,y1) towards a destination (x2,y2) at the defined speed. In this method the node-movement-updates are triggered whenever the position of the node at a given time is required to be known. This may be triggered by a query from a neighboring.

#### 3.2.3. Network Components in a mobile node

The network stack for a mobile node consists of a link layer (LL), an ARP module connected to LL, an interface priority queue (IFq), a MAC layer (MAC), a network interface (netIF), all connected to the channel. These network components are created and understood together in OTcl.

#### 3.2.4. Routing Protocols or Agents

There different types of Ad-hoc routing agents defined by NS-2. Such as:

- AODV(Ad-hoc On-Demand Distance Vector)
- AOMDV(Ad hoc on Demand Multipath Distance Vector)
- DSDV (Destination Sequenced Distance Vector)
- DSR (Dynamic Source Routing)
- TORA (Temporal Ordered Routing Algorithm)

#### 3.2.6. NS-2 Network Animator (NAM)

Network Animator (NAM) is an animation tool for looking network simulation traces and real world packet traces. It supports topology layout, packet level simulation and various data inspection tools. Before starting to use NAM, a trace file has to be created. This trace file is usually generated by NS-2. It contains topology information for example node and links as well as packet losses. During simulation, the user can produce topology configuration, layout information and packets traces using tracing events in NS-2. Once the trace file is generated, NAM can be used to animate it. Upon starting, NAM will read the trace file, create the topology, pop up a window, do layout if necessary and pause at time 0. Through its user interface, NAM provides control over many aspects of animation .(Project *et al.*, 2008). Here figure describes the NAM window.

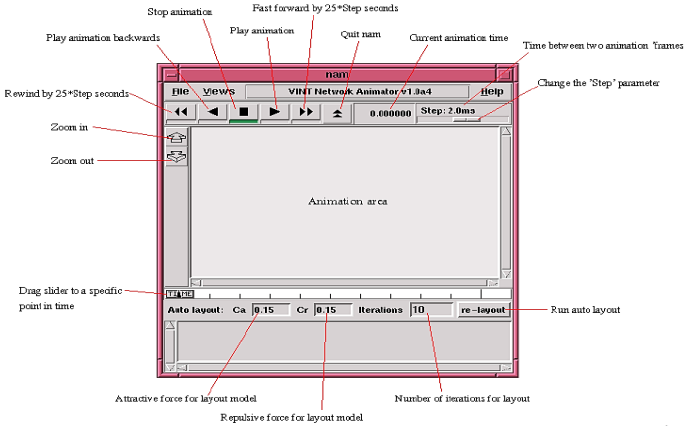


**Figure. 3. NS-2 Network animator window**

### 3.3. Core Problem in MANET

In MANET environment the problem is, nodes are supposed to collaborate among each other dynamically to give routing service and transmit packets. This need represent a security challenge when malicious nodes are exhibit in the network. Certainly, the presence of such nodes may not simply interrupt the normal network operations, but cause serious message security concerns. The security concern is necessary in absence of centralized administration because of no system in network is to monitor the routing information and malicious activities. The routing misbehavior is degrades the network performance by dropping the data packets or capturing the data packets in network.

1. The black-hole node replies false route information.
2. All data is dropped by black-hole node that passes through malicious nodes.
3. The sender has continuously tried to send data even there is failure number of times by black-hole node.

Here the proposed scheme is improves the routing misbehaviour from malicious nodes

### 3.4. Proposed IDS Scheme to secure MANET

IDS (Intrusion Detection System) can be software or hardware design for security purpose to detect any potential malicious that can harm entire network or the selected host or the confidentiality integrity and availability the network. Intrusion Detection Systems is security tools that, like other firewalls

and antivirus software are planned to strengthen the security of information and network systems. Therefore IDS involves taking audit data that can be used to classify and recognize when an intruder is trying to attack a system. IDS can be classified as Host-based based and Network-based, based on the implantation place. Host-based IDS is installed in a host and monitor traffics for particular host only. It does not check traffic that is not directed at the host. Network-based IDS is deployed at strategic places example outside the firewall or various places of network capture traffic going across the wire, and comparing it to a database of known attack signatures.

### 3.4.2. Procedure to create normal AOMDV protocol routing module

To apply normal AOMDV routing protocol, it should be started by copying the whole ns2.35 directory and rename it to normal-ns2.35 or by cloning the Ubuntu platform on VMWARE to have a copy of the platform. On AOMDV directory there are nine C files such as, *aomdv.cc, rqueue.cc, rqueue.h, aomdv packet.h*. There are two ways of using these file. First choice is that to change the name of the directory and later use the new name to declare function, variable and others inside the program or to leave it as it is and work on the modified line of code that makes the normal behaviour normal or a malicious behaviour malicious. For this thesis work we chose to use as it is.

### 3.4.3. The second in presence of black hole attack

The proposed work also tested with presence of black hole attack by AOMDV protocol. The following fields are prone to attack by a black-hole node.

**Table.1. vulnerable fields in AOMDV routing protocol**

| Message Field | Alterations |
|---|---|
| Type | Modification of the message type |
| Hop Count | Altering Minimum/Maximum hop-count |
| Sequence number of source and Destination | Increase or decrease sequence number of the node to be chosen by sender node to drop packets. |
| Destination IP Address | Substitute with another IP address |
| Source IP Address | Substitute with another IP address to change the reverse route. |

### 3.5. Intrusion Detection Systems

IDS (Intrusion Detection System) can be software or hardware design for security purpose to detect any potential malicious that can harm entire network or the selected host or the confidentiality integrity and availability the network. Intrusion Detection Systems is security tools that, like other firewalls and antivirus software are planned to strengthen the security of information and network systems. Therefore IDS involves taking audit data that can be used to classify and recognize when an intruder is trying to attack a system. IDS can be classified as Host-based based and Network-based, based on the implantation place. Host-based IDS is installed in a host and monitor traffics for particular host only. It does not check traffic that is not directed at the host. Network-based IDS is deployed at strategic places example outside the firewall or various places of network capture traffic going across the wire, and comparing it to a database of known attack signatures.

Based on solution technique IDS can further categorize to Anomaly based IDS and signature based IDS. Signature based IDS uses technique firs by record any known attack signature, then it compares a patterns with known attacks in network traffic. Signature database must be constantly updated to filter the new born attack. This IDS can't detect any unknown attack that is not registered on the database. In short it act like antivirus system. **A**nomaly based ID**S** first create behavioral profile from deferent program, traffic flow, users activities and other resource of the system; then it detect any user and application activities if it different from the profiles. The profile must updated dynamically by looking at users and system behavior. On this work Host-based IDS is used because a Network-based IDS cannot be employed to mobile ad-hoc networks where there is no central device that monitors traffic flow. According to our methodology black-hole attack is studied under the AOMDV, then later we have introduced anomaly based IDS modified protocol used to mitigate the black-hole nodes and improve the performance of the network to the better level.

### 3.6. Proposed Methodology to mitigate black hole attack:

Type of attacker = Black hole attack
Routing Protocol = AOMDV
Security Provider = IDS (Intrusion Detection System)
Number of nodes = varies from 5 to 20
First sender node broadcast RREQ to all Intermediate node. When intermediate node accept RREQ and if the receiver is a destination node then it quickly reply to the sender node with reverse address, else the intermediate node rebroadcast to its neighbor node. When the intermediate RREQ reach to a black-hole node, the node replies RREP with the highest sequence number which is $2^{32}$. Here whatever the RREP comes to sender node the sender node first check the condition of sequence number of RREP in routable is less than to the new coming sequence number sends by the black-hole node. The result is always false because the sequence number in route table always less than to $2^{32}$ which is sent from the black-hole node. At that moment the sender node reject the new RREP and use other route that comes from other intermediate node. If the RREP sequence number is less than maximum sequence number, first it checks the route table. If the route table is NULL it update the table with the fresh route with the following condition. If the fresh RREP sequence number is greater than maximum sequence number in the route OR fresh RREP sequence number is equal to maximum sequence number in the route table AND fresh RREP hop count less than minimum hop count in the route table, then update the route table with fresh RREP else discard fresh RREP.

### 3.6.1 Steps to mitigate black hole attack by IDS

**1st** Sender node broadcast RREQ to all neighbor node.
**2nd** If the receiver is a destination node then it quickly reply to the sender node with reverse address, else the intermediate node rebroadcast to its neighbor node
**3rd** When the RREQ reach to a black-hole node, the node replies RREP with the highest sequence number which is $2^{32}$.
**4th** If the fresh RREP is not less than the max-sequence number, then sender(S) node reject the new RREP.
**5th** If the RREP sequence number is less than maximum sequence number, first it checks the route table.
**6th** If the route table is NULL it update the table with the fresh route.
**7th** If the fresh RREP sequence number is greater than maximum sequence number in the route OR fresh RREP sequence number is equal to maximum sequence number in the

route table AND fresh RREP hop count less than minimum hop count in the route table, then update the route table otherwise discard fresh RREP.
**8th** End

## IV. RESULTS AND DISCUSSION

In this chapter, we measure the effect of black-hole attack and a mitigation of the attack by anomaly IDS to secure AOMDV routing protocols in MANET. To evaluate these simulations, packet delivery ratio, throughput and packet lost is used. This work also make available a comprehensive examination that obtained from the simulation results.

### 4..1 Network Modelling

The proposed method is simulated using NS-2.35. The size of the network is stated by selecting the X and Y distance, as a result that, 800 x 800 meters is selected as network size. After selecting the network size, mobile nodes are correctly configured manually based on; node size, color, mobility, label and dimension.

### 4.2 Simulation Parameters

In this simulation UDP connection is used as a replacement for of using a TCP connection. The reason is that in TCP the protocol will terminate the connection if it doesn't get a reply acknowledgement (ACK) from the receiving node for the packets send. Hence when black-hole attack applied at that moment the TCP will terminate the connection when the node drops the packet. Therefore UDP protocol is selected in the simulation. Moreover it is possible to count the total number of packets sent and received in the simulation if UDP protocol is used. However, once TCP protocol is used the sending node will close the connection because it will not receive ACK packet any more.

**Table .2. Parameters for simulation**

| NUMBER | PARAMETER | VALUE |
|---|---|---|
| **1** | Simulator | NS- 2.35 |
| **2** | Number of node | 20 |
| **3** | Routing protocol | AOMDV |
| **4** | Connection type | UDP |
| **5** | Node speed (M/sec) | 1,5,10,15,20 |
| **6** | Network area | 800 x 800 (m) |
| **7** | Number of black-hole attack | 1 |
| **8** | Traffic type | Constant bit rate (CBR) |
| **9** | Node placement | Random |
| **10** | Performance Metrics | Throughput, Packet Delivery Ratio and packet loss |
| **11** | Graphing Utility | Gnuplot 5.0 |
| **12** | Platform | UBUNTU 12.04 |

For this work CBR (Constant Bit Rate) application is used that produces constant packets through the UDP connection. CBR packet size is chosen to be 512 bytes long and the packets are generated at an interval of .05s. The nodes moves to the randomly based on mobility values stated on the tcl script. All mobile nodes are labelled with numbers except sending, receiving and black-hole node. A brief summary of the simulation parameters are listed in the following table.

### 4.3 Normal AOMDV routing module

In the first module there is no black-hole attack at all. The number of node is 20 and AOMDV protocol is used.

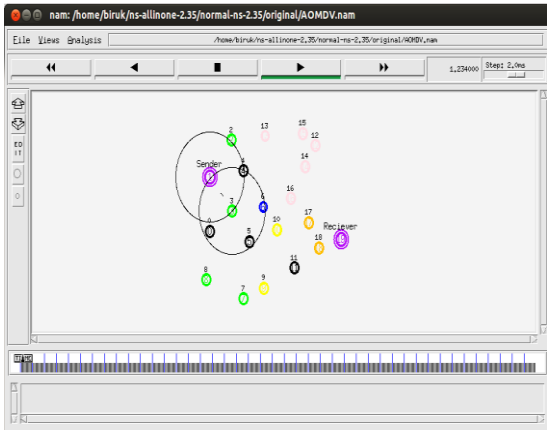


**Figure .4. Normal AOMDV routing module**

### 4.3.1. Presence of black hole attack

In the second simulation module, we add the black-hole attacker Node 11. The attacker node drop/swallow every node that comes through it.

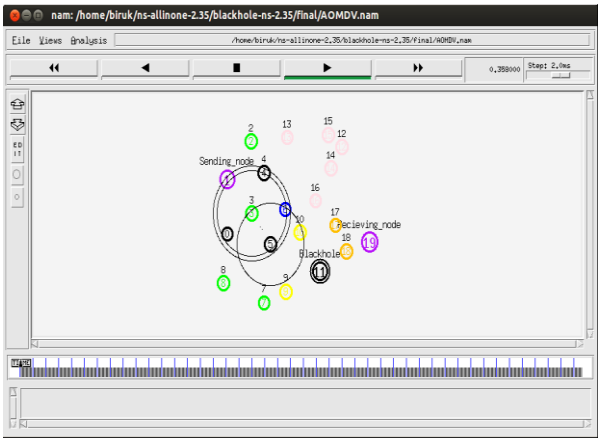


**Figure .5. Presence of black hole attack**

### *4.3.2* Proposed IDS module

In the last simulation, anomaly IDS is used to mitigate black-hole attack from the MANET.

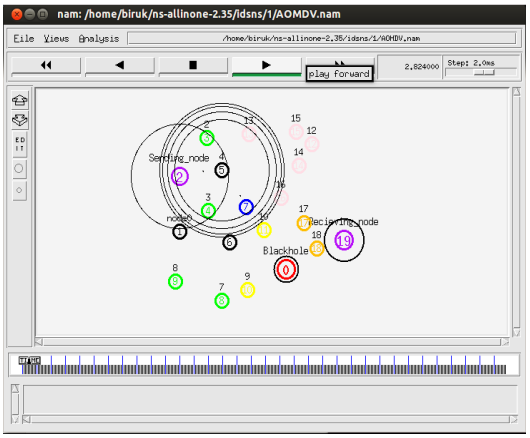


**Figure. 6. Proposed IDS module**

### 4.5 NS-2 Trace File

tr. means a trace file which has output trace file of the Tcl scripts by .tr extension. Trace files has all events in the simulation including sent, received, dropped, forward etc. In the simulations trace file format is analyse/identify the result off simulation.(Project *et al.*, 2008)

#### 4.5.1. Event type

In the traces file, the first column describes the type of event going on at the node and can be one of the four types.

**Table .3. Event type in the trace file**

| | |
|---|---|
| S | Send |
| R | Receive |
| D | Drop |
| F | Forward |

#### 4.5.2. General tag

The second column starting with "-t" may stand for time setting. -t Time

#### 4.5.3. Node property tags

This column indicates the node properties like node-id, the level at which tracing is being done like agent, router or MAC. The tags start with a leading "-N" and are listed as below.

**Table .4. Node Properties tag**

| | |
|---|---|
| -Ni | Node id |
| -Nx | Node's x-coordinate |
| -Ny | Node's y-coordinate |
| -Nz | Node's z-coordinate |
| -Ne | Node's energy level |
| -Nl | Trace level, such as AGT,RTR,MAC |
| -Nw | Reason for event |

## V. CONCLUSION

Due to MANET characters, such as, self-organizing, open node to node connections and dynamic topology the following key security points are vulnerable to threats or attacks. One of the threat that has highest vulnerability to the network is black-hole attack. In this thesis the properties of MANET and black-hole attack is briefly describes in first four chapter. A black-hole attack degrade the network performance in packet delivery ration throughput and packet loss. This attack simply drop/swallow all the packet by falsifying the sender node with highest sequence number.

For thesis work anomaly based IDS is implemented to mitigate black-hole attack in vulnerable environment. From the simulation it's easy to understand the mitigation mechanism minimize the impact of a black-hole attack from the network by using anomaly IDS. IDS is implemented by modifying the AOMDV protocol. When the simulation is executed under IDSAOMDV the packet lost radically improves almost as the same as to normal routing behavior, perhaps, when the attack executed the packet lost is highly increased. This result describes packet lost on normal is 0.00% and packet lost at IDSAOMDV is 0.00, when the number of mobile node is 20 in number. The packet delivery ratio under different mobility on normal module/scenario is 100%, when it is under black-hoe attack it is 0.25% and when it is on IDSAOMDV the result is 99.75%. Throughput result also shows the performance of IDSAOMDV with different mobility. Once the simulation is under normal module the result of throughput is 3.07%, when the network is under black-hole attack the result is 0.15% and when IDSAOMDV is applied it become 3.03%. The result describes the IDSAOMDV still has highest performance by improving the average throughput value.

### 5.1. Future Work

This thesis work achieve the mitigation of black-hole attack on MANET with AOMDV protocol and carried out comparative analysis of with 3 module/scenario which shows that black hole attack consequence on the performance of the MANET. The proposed IDS performs better in terms of throughput, packet loss and packet delivery ratio. Future work has to be done for more performance metrics evaluation and improvement in terms of energy consumption, Jitter and end to end delay and eradication of black-hole attack in MANET. In addition to that external black-hole and multiple black-hole attack can be done with different routing protocol.

## VI. REFERENCES


[1]. Anuradha, T. and Shedbalkar, P. S. (2014) 'Detection and Prevention of Cooperative Wormhole Attack in a MANET', 3(12), pp. 2302–2305
.

[2]. Arfaat, P. G. (2011) 'The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks', 8491, pp. 421–425.

[3] Badiwal, S. (2013) 'Survey of IDS in MANET against Black Hole', 2(5), pp. 401–406.

[4] Bansal, P. (2014) 'Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol', 3(4), pp. 90–99.

[5]. Bhardwaj, N. and Singh, R. (2014) 'Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs', 3(5), pp. 376–383.

[6]. By, P. and Awad, B. M. (no date) 'Wormhole Attack Detection and Prevention Model in MANET Based on Hop-Count and Localization'.

[7]. Chandure, O. V (2012) 'Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol', 41(5), pp. 27–32.

[8]. Gopichand, G., Saravanaguru, R. K. and Babu, K. R. (2016) 'Available Online through USAGE OF AODV AND AOMDV PROTOCOLS IN PERCEIVING BLACK HOLE ATTACKS IN A MANET ISSN : 0975-766X CODEN : IJPTFI Research Article', 8(4), pp. 22305–22313.

[9]. Goyal, S. and Rohil, H. (2013) 'Securing MANET against Wormhole Attack using Neighbor Node Analysis', 81(18), pp. 44–48.

[10]. Gupta, S., Volume, I., July, I. and No, P. (2015) 'Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques', 4(7), pp. 13268–13272.

[11]. Ibrahim, A. and Zaki, N. E. (2015) 'Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol', 3(4), pp. 90–93. doi: 10.12691/jcsa-3-4-1.

[12] Jathe, S. R. and Dakhane, D. M. (2012) 'Indicators for Detecting Sinkhole Attack in MANET', 2(1), pp. 2–5.

[13]. John, N. P. and Thomas, A. (2012) 'Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review', 2(9), pp. 1–6.

[14]. John, S. L. (2015) 'ENSC 427 Communication Networks Black-hole Attack in Mobile Ad- Hoc Network by using NS-2'.

[15]. Joshi, A., Srivastava, P. and Singh, P. (2010) 'Security Threats in Mobile Ad Hoc Network', 1(2), pp. 125–129.

[16]. Journal, I. and Science, C. (2016) 'Routing and Reducing Perturbation in Mobile ad Hoc Networks ( Manets ) for Efficient Communication', (February).

[17]. Kashyap, R. (2015) 'Prevention of Black Hole Attack in MANET', International Journal of Computer Engineering in Research Trends, 351(5), pp. 2349–7084. Available at: http://www.ijcert.org.

[18]. Kaur, R. (2013) 'Towards Security against Malicious Node Attack in Mobile Ad Hoc Network', 3(7), pp. 273–281.

[19]. Kaushal, S. and Aggarwal, R. (2015) 'A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack', 4(2), pp. 301–305.

[20]. Khasdev, S. (2016) 'Attacks and Security Issues over Mobile Adhoc Network', 2(2), pp. 89–92.

[21]. Koo, V. (2012) 'Preventing Collaborative Wormhole Attacks In AODV-based Mobile Ad-Hoc Networks'.

[22]. Kumar, M. (2014) 'Network Layer Attacks and Their Countermeasures in Manet : A Review', 16(2), pp. 113–116.

[23]. Lambert, É. D. J. (2013) 'Harris SIMAREMARE A DEVELOPMENT OF SECURE AND OPTIMIZED AODV ROUTING PROTOCOL USING ANT ALGORITHM'.

[24]. Mahamuni, K. and Chandrasekar, C. (2013) 'Mitigate Black Hole Attack In Dynamic Source Routing ( DSR ) Protocol By Trapping', 10(4), pp. 49–54.

[25]. Manikandan, T., Shitharth, S., Senthilkumar, C., Sebastinalbina, C. and Kamaraj, N. (2014) 'Removal of Selective Black Hole Attack in MANET by AODV Protocol', 3(3), pp. 2372–2377.

[26]. Mr. Sagar (2012) '"A system for manet to detect selfish node in ns2"', (December 2012).

[27]. Muhammad, S. and Gillani, R. (no date) 'Analysis of Security and Reliability of Routing Protocols in MANETs By Table of Contents'.