Simulation And Analysis Of A Common Security Threat (Black Hole) In Wireless Ad Hoc Networks

Omeed kamal khorsheed , Waseem Ahmed Hussein

Abstract— AD-HOC is a temporary wireless network between mobile Nodes like laptop computers and smart phone or any device with wireless adapter, so we can call it mobile ad-hoc network (MANET), MANT is none infrastructure network based on several routing protocols, the most important protocol is AODV. AODV (Ad-hoc On-Demand Distance Vector) is an important Reactive routing protocol for mobile ad-hoc networks, Since AODV is none infrastructure network, it will be unprotected and there is no any prerequisite security against a attacks and malicious Nodes, Black Hole and Wormhole attacks are the main critical attacks against ad-hoc Nodes. In ad-hoc wireless network the expression (Black hole) refer to malicious nodes that conform the request data packet instead of destination node to routing reply message which involve the fresh routing sequence number. Immediately after the Sender Node receive the reply message from the Black hole node it will start sending data packet ,All data packet will be lost and will not reach the real destination node. The black hole nodes decrease the network performance and exhaust its neighbor's nodes resource. In this Paper, we will try to simulate data transmission over ad-hoc wireless network and the AODV Routing Table , In the same simulation we will imitate the black hole attackI

Keywords; MANET, AD-HOC, Wireless Network, Black Hole, Broadcasting, Malicious Node, Mobility, Simulation, Security, ADOV, Routing Table ,LAN ,WAN ,MAN ,PAN WLAN WIMAX.

1 Introduction

In general there is tow type of network, infrastructure network and ad-hoc wireless network , ad-hoc as expression is an old Latin word which means (For This Purpose) , in communication word the ad-hoc network is a kind of mobile wireless network without any infrastructure or any prepared configuration or administration , ad-hoc is a temporary wireless network that we can use for temporary purpose like communicate in disaster area such as earthquake, flood and of course in military communications.

Ad-hoc consisting of connected portable devices or mobile nodes, so we call it Mobile Ad-hoc wireless network (MANET), those mobile device communicate in limited geographic area via shared wireless medium without any need for access points. Each ad-hoc node has its own network configuring and in this case communicate nodes will not need a dedicated router or centralized administration, each node will represent a network router and dependence on the transmission range between sender node and destination node ad-hoc network may have multi routers node (multi-hop).

MANET nodes are mobility nodes and the neighbor nodes can communicate directly if the sender node and the destination node in the transmission range, if the destination node out off transmission range and there is another intermediate node in the transmission range then this node will act like network router. So the topology of the MANET network will be change dynamically, This incessant change brings different challenges in network performance and security issue. Hackers and attackers can have an immense advantage to find out a gap or a hole to attack an ad-hoc network nodes. The (Black hole) is the most known attack in ad-hoc networks, Black hole attacker aim to counterfeit the ad-hoc network routing protocol, The counterfeited routing data will disturb and exhaust the network resource and case serious damage to the network topology ,and of course losing the transmission data. We can classify the routing protocols into three categories based on the routing information update mechanism:

- **Proactive Protocols (Table-Driven Protocols).**
- **Reactive Protocols (On-Demand Protocols).**
- **Hybrid Routing Protocols.**

In ad-hoc net work Data transmission operation start be sending a broadcast message to all other nodes in the ad-hoc network, Broadcasting message is a routing request which is used to discover the routing node or nodes (Path). Since the mobility of ad-hoc nodes and disconnect of some nodes, Broadcasting will be done frequently to ensure and maintain the routing discovery operation. But sometimes broadcasting operation is unreliable since the destination node is out off the transmission range for all ad-hoc nodes, Or if there is a black hole node in the middle of ad-hoc network which will interrupt the broadcast discovery message by fake routing reply message which contains a fresh routing sequence number.

2. Types of Networks

In general there are different types of computer network, we can categorize those types depending on the network scope or scale (net work range).

2.1. Local Area Network LAN and WLAN

LAN network is a computers device connecting over a comparatively short scope in local area such as school, hospital, house, company building, and sometimes we can have more than one LAN in the same building, and LAN could be available on a group of buildings in the same geographic area, LAN often has a single TCP/IP subnet which is managed by a single administrator. In LAN each workstation or personal computer has its own resources like CPU and Memory, however LAN nodes has the ability to access data and sharing devices or applications on the LAN. Besides sharing the expensive devices such as laser printers, LAN nodes can also communicate with each other at very fast rates[1][2].

2.1.1 Main Local Area Network Technologies

- **Ethernet**

The most widely installed LAN technology is Ethernet which specified in (IEEE 802.3) stander, Ethernet technology was developed by Xerox, DEC, and Intel. LAN which uses Ethernet technology connects (cabling) via coaxial cable or twisted pair wires. Ethernet system started with tradition LAN transmission speeds up to 10 Mbps for that it called 10BASE-T .After that Ethernet has evolved to 100 Mbps (fast Ethernet) ,and then to Gigabit Ethernet (1 to 10 Gbps). Ethernet is CSMA/CD system using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol, when LAN node start transmissions first it listen to the LAN medium to see if another transmission is in progress (Carrier Sense) ,if the LAN medium is idle then node can transmit data, but if we have synchronize transmission and more than one node try to transmit in the same time then it will be a collision and the transmission will not succeed ,for that collision node normally wait 96 bit periods before starting data transmission [1][2].

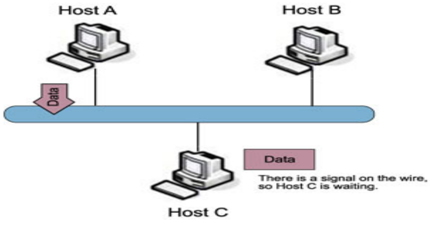


Figure 1: Ethernet collision

- **A Token Ring**

A Token Ring protocol is specified as IEEE 802.5 standard, A Token Ring network is a local area network that all computers are connected in a ring or star topology and a bit- or token-passing method is used in order to prevent the collision of data between two nodes that want to transmit data at the same time. In this net work all nodes take turns in transmit data and each node is allowed to transmit only during its turn, so there will be a rotation which called token passing, The Token is a placeholder frame which shift from node to another around the ring, when the node has the token placeholder it can transmit data and after node end the transmission the token passed node to another until it come across a new sender node[1][2].

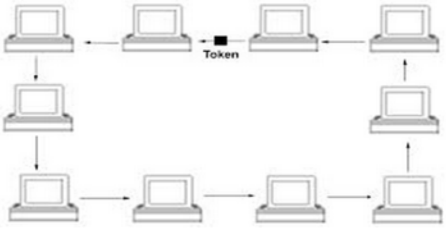


Figure 2: Token Ring protocol

- **Fiber Distributed Data Interface (**FDDI)

FDDI protocol is based on the token ring protocol and we can use it in the simple LAN or even in extended LAN up to 200 km , FDDI is the pivot in the wide area network communication . FDDI protocol is a set of ANSI and ISO standards for data transmission on fiber optic lines. An FDDI network has two token rings primary and secondary, the secondary token is spare or backup token in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps[2].

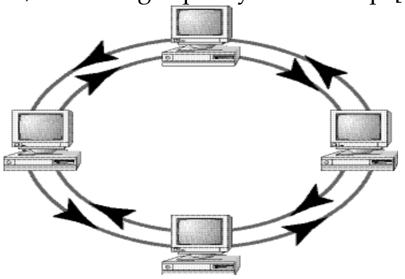


Figure 3: Fiber Distributed Data Interface

- **Wireless Local Area Network (WLAN)**

Wireless local area network (LAN) is the most recent communication system to built local area network in small area same as traditional wires LAN ,WLAN provides high data transmission to mobile nodes over electromagnetic air waves radio frequency or infrared waves. WLAN is less expensive and more fast without any complicated installation step and it is simple to re-configuration, WLAN is flexible environment with free mobility so all user can access the network any place in the frequency range without any wires , WLAN can configure in different topologies to meet net work requirements but it could not perform the wire LAN bandwidth or to ensure security considerations in network[1][6].

2.2. Personal Area Network (PAN)

A personal area network (PAN) is a computerizes network organized around one user in a single building such as a small office or house. PAN could include one or more computers, smart phones, printer , TV screen and other personal entertainment devices. If PAN has more than one user we can call it home network (HAN),in PAN or HAN we get the Internet connection via a single wired connected to a modem, after that the modem distributes the conduction for wired and wireless devices[3].

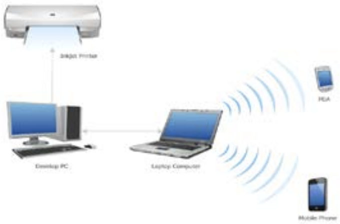


Figure 4: A personal area network

2.3. Metropolitan Area Network (MAN)

A metropolitan area network(MAN) is a computerizes network across a city or college campus or small region. MAN network is larger than LAN or WAN network. MAN network can cover several miles area and MAN often contain several LANs connecting together[1][3].

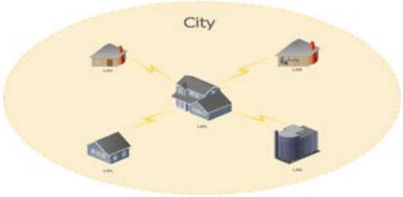


Figure 5: A metropolitan area network

2,4. WIMAX Network

WIMAX network is wireless MAN network with microwave access , WIMAX was described as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". The range of WIMAX network extending from 4 to 30 miles depending on tree cover and building height in the network area[1][2][4] .

2.5. Wide Area Network (WAN)

Wide Area Network (WAN) is a large geographic area network, such as country or territory. WAN often contains connect multiple smaller networks, such as LANs or MANs. Internet is The Largest WAN in the world it contains connected WANs[1][4].

3. AD-HOC Networks

After we categorized the networks depending on the network scope, now we will categorize the networks depending on the network infrastructure , in general there is tow type of network:

- Infrastructure network such as (LAN,WLAN,WAN,PAN,MAN, WIMAX) .
- ad-hoc wireless networks .

ad-hoc as expression is an old Latin word which means (For This Purpose), in communication word the ad-hoc network is a kind of mobile wireless network without any infrastructure or any prepared configuration or administration, ad-hoc is a temporary wireless network that we can use for temporary purpose like communicate in disaster area such as earthquake, flood and of course in military communications.

Ad-hoc consisting of connected portable devices or mobile nodes, so we call it Mobile Ad-hoc wireless network (MANET), those mobile device communicate in limited geographic area via shared wireless medium without any need for access points. Each ad-hoc node has its own network configuring and in this case communicate nodes will not need a dedicated router or centralized administration, each node will represent a network router and dependence on the transmission range between sender node and destination node ad-hoc network may have multi routers node (multi-hop)[4][5].

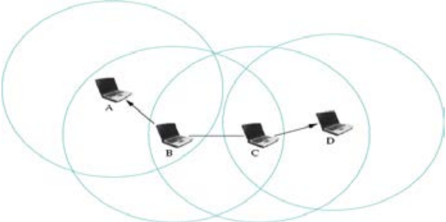


Figure 6: ad-hoc wireless networks

MANET nodes are mobility nodes and the neighbor nodes can communicate directly if the sender node and the destination node in the transmission range, if the destination node out off transmission range and there is another intermediate node in the transmission range then this node will act like network router. So the topology of the MANET network will be change dynamically, This incessant change brings different challenges in network performance and security issue. Hackers and attackers can have an immense advantage to find out a gap or a hole to attack an ad-hoc network nodes. The (Black hole) is the most known attack in ad-hoc networks, Black hole attacker aim to counterfeit the ad-hoc network routing protocol, The counterfeited routing data will disturb and exhaust the network resource and case serious damage to the network topology ,and of course losing the transmission data[4][5].

3.1. Comparison of Infrastructure and Ad-hoc Networks

Infrastructure Networks	AD-HOC Networks
Nodes are required to be in the coverage area of the access point.	Node can transmit data to another node as long as there is a neighbor node which can cover both of them.
Nodes Mobility is limited with the distance between the access point and the Node	Nodes Mobility is limited with the distance between the neighbors and the Node
access points can handle power optimization for its Nodes, If node is in power saving mode then access point can buffer data for it.	power consumption is higher, since node transmit data, that do not concern themselves.
Data is forwarded via access points , access points is the route.	Data is forwarded via intermediary nodes using one of the ad-hoc network routing protocols and broadcasts message.
Security Considerations and Information are secured.	Security is an essential problem. Information must pass over other intermediate nodes.

Table1: Comparison of Infrastructure and Ad-hoc Networks

3.2. Ad-hoc routing protocols

We can classify the Ad-Hoc routing protocols into three categories based on the routing information update mechanism

3.2.1 Proactive Protocols (Table-Driven Protocols)

Proactive Routing Protocols maintains fresh lists of nodes and their routes by periodically distributing routing tables throughout the network, each node try to keep up-to-date the routing tables by propagates the update messages to the network when the network topology changes, so each node has information about the network topology, Proactive Routing Protocols have a lot of disadvantages and problems like[4][3][5]:

1- The continual updating of network topology Exhaust network bandwidth.
2- The continual updating of network topology keeps network Exhaust
3- The continual updating of network topology keeps all nodes wakeful and quickly exhaust their power.
4- Exhaust amount of data for maintenance.
5- Slow reaction on re-structuring and failures.

The main Proactive Routing Protocols (Table Driven Routing Protocols) are

1. **Destination-Sequenced Distance Vector Routing Protocol (DSDV)**

DSDV Protocol designed to use the node sequence numbers to attain loop freedom without any coordination. Each node in ad hoc increasing the sequence number for itself. In the same loop it maintains the highest known sequence number for each destination in the network routing table (destination sequence numbers), typically the sequence information for every node exchanged through routing updates among neighbors in distance-vector protocols, is tagged with the corresponding destination sequence number. These sequence numbers are used to determine the relative freshness of distance information generated by two nodes for the same destination node which mean the node with a higher sequence number has the more recent information.

2. **Wireless Routing Protocol (WRP)**

In WRP protocol, every node is updated with the shortest path spanning tree of each of its neighbors. Each node uses the cost of its neighbors links along with shortest path trees reported by neighbors to update its own shortest path tree, the node reports changes to its own shortest path tree to all the neighbors in the form of updates containing distance and second-to-last hop information to each destination[4][3][5]:.

3.2.2 Reactive Protocols (On-Demand Protocols).

Reactive on-demand protocols finds a route on demand by flooding the ad hoc network with route request packets, When the sender node wants to connect to the destination node, it send the route request packet as a broadcasted message to its direct neighbors (first level) if the destination node found in the neighbors and received the router request it will reply with a replay packet . But if the destination node not in the first level of neighbors then downright the neighbors of the sender node will forward the broadcasted router request packet to their neighbors (level 2) and this action is happen until the destination is found. And sends the replay packet the sender node in the shortest path. The route remains in the route tables of the nodes through shortest path until the route is no longer needed.

The main disadvantages of Reactive Protocols are:

1. High latency time in route finding.
2. Excessive broadcasted can lead to network clogging.

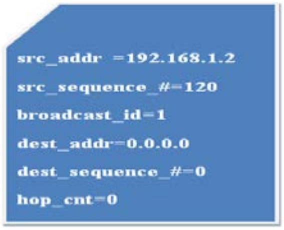
The main Reactive Protocols (On-Demand Protocols) is

Ad hoc On-demand Distance Vector (AODV)

In AODV protocol , each ad-hoc node maintains at most one route per destination so the destination replies only once to the first arriving router request during the route discovery operation . AODV is a single path protocol, it has to invoke a new route discovery whenever the only path from the sender to the destination fails. When network topology changes frequently, route discovery needs to be initiated often which can be very inefficient since route discovery flood is associated with significant latency and overhead. AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes are not in the transmission range and cannot hear the other node. Each node can communicate with other nodes in its neighborhood by using local broadcasts known as hello messages. And the neighbor routing tables organized the response time to local movements and provide quick response time for new routes requests[4][3][5]:.

(AODV) Path Discovery steps

1. initiate when sender node needs to communicate with another node , it broadcast to the neighbors a route request packet (RREQ).
2. Every node maintains two counters:
   - node_sequence_number
   - broadcast_id
3. The RREQ has the following data:



src_addr =192.168.1.2
src_sequence_#=120
broadcast_id=1
dest_addr=0.0.0.0
dest_sequence_#=0
hop_cnt=0

Figure 7: The RREQ

- src_addr (sender address)
- src_sequence_# (sender sequence number)
- broadcast_id (is incremented when sender node send a RREQ)
- dest_addr
- dest_sequence_#
- hop_cnt (hop counter)

4. Each neighbor either assure the RREQ, by sending back a routing reply (RREP), or rebroadcast the RREQ to its own neighbors after increasing the hop_count by one.
5. If a node receives a RREQ that has the same <src_addr, broadcast_id> with a previous RREQ it drops it immediately
6. Each node records the address of the neighbor from which it received the first copy of the RREQ.
7. These entries are maintained for at least enough time, for the RREQ to traverse the network and produce a reply .
8. As RREQ travels from sender to many destinations, it automatically sets up the reverse path, from all nodes back to the sender.
9. The sender can begin data transmission as soon as the first RREP received [4][3][5]:

3.3. Ad-hoc Black Hole Attack

Black hole attack in ad hoc network is a malicious node that present itself as having the shortest path to all nodes in the network environment and it has all the time the fresh sequence number, The black hole node often occupy the center of ad-hoc network in order to be in the transmission range for all nodes and intermediate all RREQ , and to catch all RREQ, the a malicious node waits for ad-hoc nodes to send RREQ messages. When the malicious node receives the RREQ message, it will immediately and without checking its routing table sends a fake RREP message giving a route discovery destination over itself, a RREP with a high sequence number to cheat the routing table of the sender node, before other nodes send a true RREP. Therefore the sender node assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node, so all the transmitted data will go to the black hole for ever[4][5] .

4. AD-HOC Networks Simulation

This simulation is for educational purpose to simulate an Ad-hoc network with AODV protocol black hole attack and the, our software has a user-friendly graphical user interface and has been written in java language with the following features:

- interactive user interface so user can add new node and change nodes details .
- user can test ad hoc data transmission
- The software imitate the AODV path discovery
- User can select the black hole node and the destination node.
- The software imitate the black hole attack.

The major steps in the simulation code are

1. We use the java JLabel to present the network nodes with image icon and name refer to node name and text refer to node IP.

2. We measure the transmission range for node by 300 pixel.
3. To find out if neighbor node is in the transmission range we used this equation:

```
Transmission_range=300
X=Sender_ x_location - Destination_ x_location
Y= Sender_ y_location - Destination_ y_location
Path=SQR(X^2*Y^2)
If (Path>= Transmission_range)
Add node to neighbor
Else
Next node
```

Equation 1. if neighbor node is in the transmission range

4. With overlapping Loop statement we get the routing path for the Destination node ,we can handle five level of neighbor.

5. With the same step ,we test the black hole attack.

4.1 User Guide

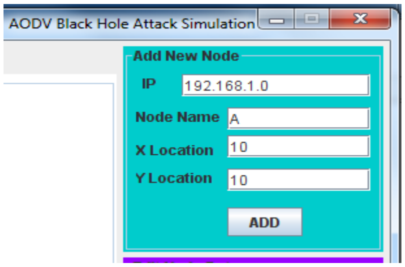
4.1.1 How to run the software

User can click the JAR(AODV_Black_Hole_S.JAR) file to run the software.

4.1.2 How to Use

First step to add new node with entering the following data :

- Node IP
- Node Name
- Node X location
- Node Y location



AODV Black Hole Attack Simulation

Add New Node

IP 192.168.1.0

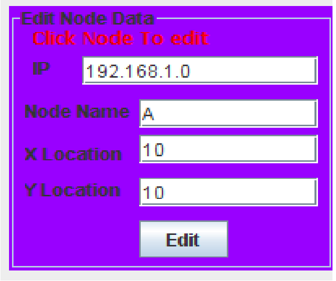
Node Name A

X Location 10

Y Location 10

Figure 8: Add New node Section

User can edit any exist node by click node icon to be selected and after that he can change the node data in edit section .



Edit Node Data

Click Node To edit

IP 192.168.1.0

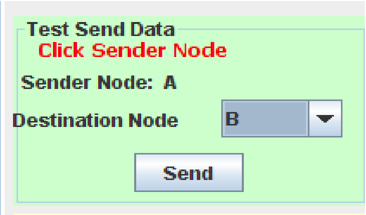
Node Name A

X Location 10

Y Location 10

Figure 9: Edit node Section

After adding all the nodes user can test AODV data transmission by click the sender node from the interface and select the destination node from the destination compo box. And finally click send button .



Test Send Data

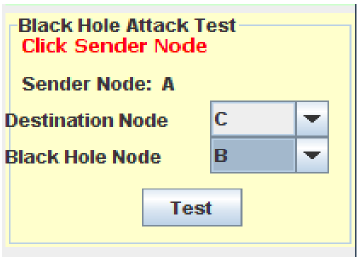
Click Sender Node

Sender Node: A

Destination Node B

Figure 10: Test Send Section

To test the black hole attack user should click the sender node and after that to select the black hole node from black hole compo box and to select the destination node from the destination compo box and finally click test button .



Black Hole Attack Test

Click Sender Node

Sender Node: A

Destination Node C

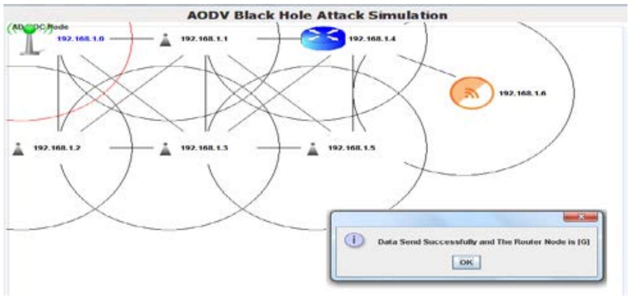
Black Hole Node B

Figure 11: Test Black Hole Section

4.1.2 Software limitation

This software coded to handle five level of neighbors node , if the destination node over five level neighbors from the sender node the software will give one result **"Path Not Found and there is no router".**

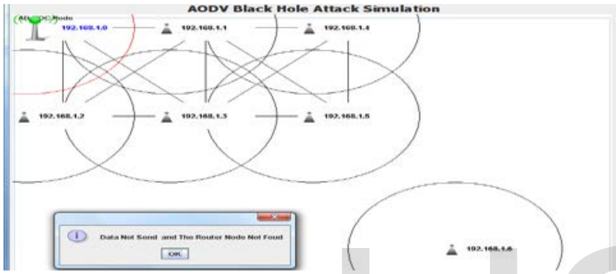
a. Data Transmission Test


AODV Black Hole Attack Simulation

Data Send Successfully and The Router Node is [G]

Figure 12: Test Send succeed

In the Figure 12 we test the simulation by sending data from node A with IP=192.168.1.0 to Dis Node with IP=192.168.1.6 and the transmission succeed and the router node was G with IP=192.168.1.4 as smart path.

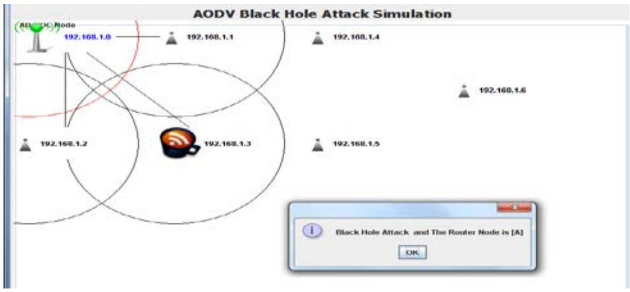

AODV Black Hole Attack Simulation

Data Not Send and The Router Node Not Foud

Figure 13: Test Send out of transmission range

In the Figure 13 we test the simulation by sending data from node A with IP=192.168.1.0 to Dis Node with IP=192.168.1.6 and the transmission unsuccessful because node Dis is out of any neighbor range .

b. Black Hole Attack Test:


AODV Black Hole Attack Simulation

Black Hole Attack and The Router Node is [A]

Figure 14: Test Black Hole attack

In the Figure 14 we test the simulation by sending data from node A with IP=192.168.1.0 to Dis Node with IP=192.168.1.6 and we have black Hole node which is node D with IP=192.168.1.3 the transmission unsuccessful because node D reply with a RREP contains a high sequence number .

5. Conclusion

In this paper , we tried to explain the ad hoc network and the AODV routing protocol, after that we moved to see how the malicious node cause the black hole in an AODV ad-hoc Network. The main purpose of this paper is to simulate the ad-hoc network data transmission and the black hole attack over AODV routing protocol , Our simulation software has two level:

First level is to implemented the AODV protocol when data transmission over ad-hoc network , and to see how AODV Path Discovery work to find the destination node and the router node. In the java code there are many multiple overlapping Loop statement to get the smart path for the destination node. In order to find the smart path we must start from the sender node and to located all its neighbors node , if we are lucky the destination node is one of the direct neighbors to the sender. Else we must find the neighbors of neighbors for all node in multi level until we get the destination node.

The second level in our simulation is to test and to imitate the black hole attack on AODV ad-hoc network , also here we used the same number of overlapping Loop statement to check out if the transmitted data will receive the destination node or it will disappear forever in the black hole node.

6. Future works:

In this paper, we try to simulate the ad-hoc data traffic routing and the black hole attack , in our simulation, we focused on (On-demand Distance Vector)-AODV protocol .Our future work will be about clustering in ad-hoc networks, while ad-hoc networks do not use specialized routers for path discovery and data traffic routing , and to get ad-hoc efficient communication between nodes we must recognize or form the backbone nodes of network, after that we can divide the ad-hoc into multi sub network depending on the backbone and its members nodes , these sub networks called ad-hoc clusters and each cluster has cluster-head node which has the responsibility for routing.

7. LIST OF REFERENCES

[1] Richard C. Dorf ,"Broadcasting and Optical Communication Technology" ,CRC Press, 2006

[2] Karl Piper, Wendy Michael, William Cronin " FDDI: An Introduction to Fiber Distributed Data Interface", 1992.

[3] http://en.wikipedia.org/wiki/Personal_area_network," Personal_area_network".

[4] PRASANT MOHAPATRA , SRIKANTH V. KRISHNAMURTHY ," AD HOC NETWORKS -Technologies and Protocols", 2005.

[5] Songbai Lu, Longxuan Li, Kwok-Yan, Lingyan Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack",2009

[6] D. P. Agrawal , Q.-A. Zeng, "Introduction to Wireless and Mobile Systems", Cole Publishing, Aug. 2002.