An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs

Neelam Khemariya
Poornima College of Engineering
Jaipur (Raj.)
India

Ajay Khuntetha
Poornima College of Engineering
Jaipur (Raj.)
India

ABSTRACT
Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. They plays significant role in real life applications such as military applications, home applications etc. these networks are threatened by a lot of security attacks such as Modification, Denial of service attack, Fabrication attack etc. Black hole attack (also called Selfish node attack) is a dangerous active attack on the mobile Ad hoc Networks (MANET). In this research paper an efficient approach for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack. The beauty of the algorithm described in this paper is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

General Terms
Mobile Ad hoc Networks, Routing protocols, Security Threats, Active attacks, Passive attacks, Reactive Routing protocol, Algorithm.

Keywords
AODV, Black hole Attack, Destination Sequence Number, Idle node, Proactive, Reactive, Selfish Node, Wormhole Attack.

1. INTRODUCTION
Wireless network enables communication between computers using standard network protocols, without network cabling. These networks use radio waves or microwaves as a communication medium. These networks are widely used nowadays because of their great advantages over a wired network.

Wireless Networks can be classified 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. The access points also works as a bridge.

An Infrastructure less Wireless Network does not have any fix infrastructure for the communication. Each node can communicate directly with other node and there is no requirement of the access point. An important thing about these networks is that these networks do not have routers, the wireless nodes work as routers. These networks don't have any fixed or static topology.

A mobile Ad hoc network consists of mobile nodes that use wireless transmission for communication. In these types of networks the nodes can move from one place to another. The motion of the mobile nodes may be random or periodical. Thus, these networks have no fixed infrastructure, no fixed configuration and other controlling device such as router etc [1]. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time. The routers are free to move randomly.

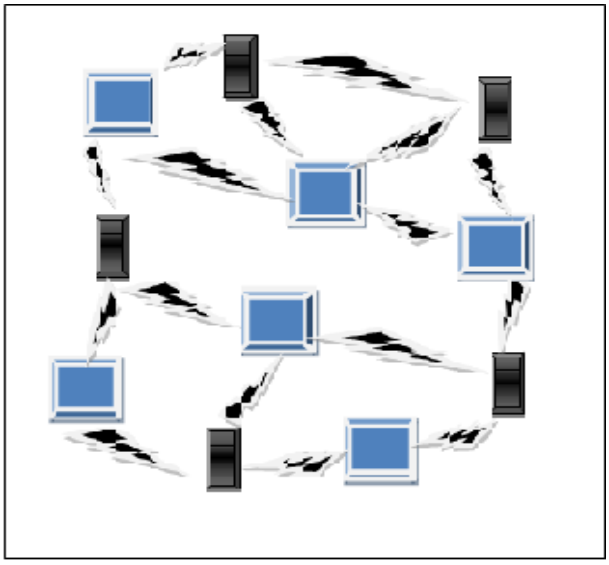

Fig 1: Mobile Ad hoc Networks

2. ROUTING PROTOCOLS FOR MANETs
The routing in the Ad hoc networks is a very critical task because of the absence of any central coordinator or base station and the dynamic topology [1]. In order to facilitate communication in these networks a routing protocol is used to discover the routes between nodes [2]. The greatest challenge for the Mobile Ad Hoc Networks (MANET) is to come with a robust security solution even in the presence of malicious nodes, so that MANET can be protected from various routing attacks. Mobile Ad Hoc Networks (MANET) has not got clear cut security provisions; it is accessible to any of the authorized network users and malicious attackers.

A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes. Many protocols have been suggested keeping applications and type of network in view.

2.1 Classification of Routing Protocols
Mobile Ad Hoc Networks routing protocols can be classified into three categories, as shown in fig. 2.

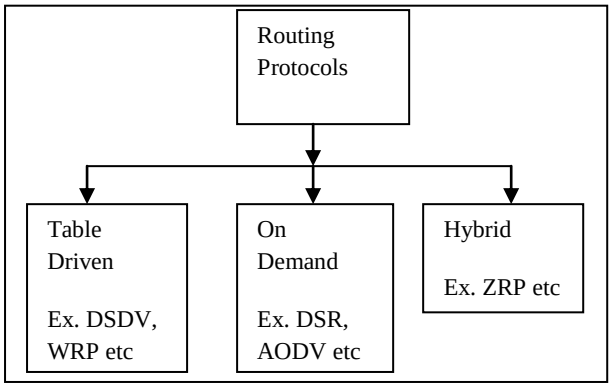

Fig 2: Classification of Routing Protocols for MANETs

2.1.1 Table Driven Routing Protocols

In Table Driven routing protocols each node maintains one or more routing tables containing routing information about all other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP etc [3].

2.1.2 On Demand Routing Protocols

In On Demand routing protocols, the nodes don't maintain any routing table nut they have a route cache. Routes are find dynamically only when a node want to communicate with another node with the help of the route discovery procedure which is invoked by the source node. Some reactive routing protocols are: DSR, AODV etc [4].

2.1.3 Hybrid Routing Protocols

This type of protocols combines the best features of table driven and on demand routing protocols. In case of the intra-domain routing, these protocols uses the table driven approach, while in case of inter-domain routing these protocols uses the on demand approach[4]. Such as Zone Routing Protocol (ZRP) etc.

3. AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) protocol is one of the most popular reactive routing protocols. It is pure on demand routing protocol. This protocol 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 uses destination sequence number for maintaining each route entry. This destination sequence number is created by the destination. A requesting node always selects the route which has the greatest sequence number. AODV has three message types. Which are: Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs). When a sender wants to communicate with a node, it creates a RREQ packet and broadcast it to find a route to the destination. Frame format of RREQ packet is shown in figure 3.

Type	J	R	G	D	U	Reserved	Hop count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Fig 3: RREQ Packet

Each node receiving the RREQ message forward this message to its neighboring node and the process is continues till the destination is reached. The destination prepares RREP packet and unicast it to the source node. Frame format of RREP packet is shown in figure 4.

Type	R	A	Reserved	Prefix size	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Life Time					

Fig 4: RREP Packet

The RERR message is generated in case when there is a link break in an active route is detected; Frame format of RERR packet is shown in figure 5.

Type	N	Reserved	Dest Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

Fig 5: RERR Packet

4. BLACKHOLE ATTACK

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 with the smallest hop count. the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node. Then the attacker drops all data packets rather than forwarding them to the destination node.

As shown in Figure 6 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. When the Source node gets the route, it starts sending the buffered data packets immediately from that route which is provided by the malicious attacker node. Nevertheless, a Black hole node drops all data packets rather than forwarding them on.

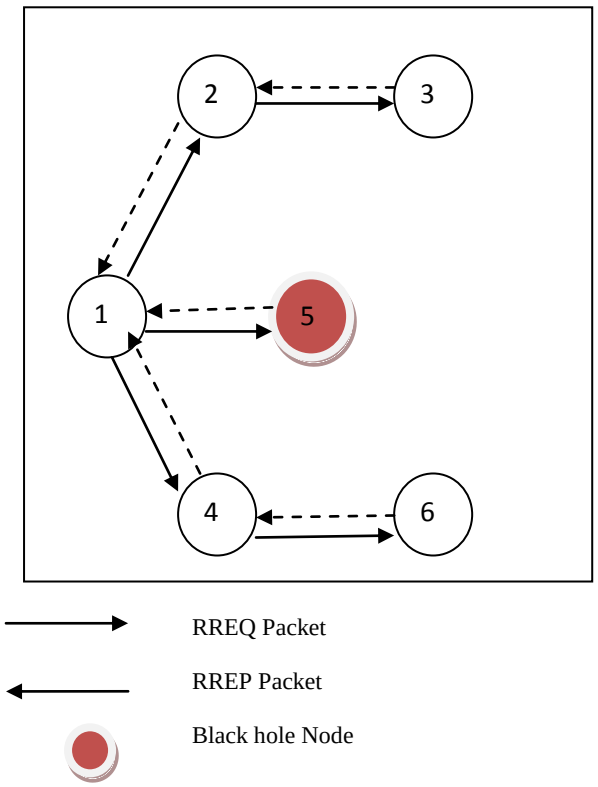

Fig 6: Example of Black hole Attack

5. LITERATURE REVIEW

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:

Deng et al. [6] proposed an approach to detect the individual black hole nodes. In this approach when any intermediate node replies for RREQ, it includes the next hop information to the destination in the RREP packet. When the source node receives this RREP packet, it sends a further request to the next hop of the replied node and asks them about the replied node and about the route to the destination. Thus we can easily identify trustworthiness of the replied node if the next hop is trusted otherwise not. Although this approach is very good for the detection of black hole- attack but it does not work in case of cooperative black hole attacks.

Ramaswamy et al. [7] proposed an approach to detect the cooperative black hole attacks. They studied multiple black hole attacks on mobile ad hoc networks and only considered black holes which have no collaboration between them. The main problem with their approach is that they provide no simulations or performance evaluations

W. Kozma et al. [8] proposed an approach to detect the black hole attach, which is based on Audit Procedure. In this approach, if the destination node detects a heavy packet drop, it calls the source node to initiate the audit procedure. For this procedure, Source node selects an audit node and generates behavioral proof for it. The source node prepares behavioral proof for itself. .then it compares results and finds the malicious nodes are detected. The main Drawback of this approach is that it is a reactive approach and works only when detects the decrement in packet delivery ratio.

Yibeltal Fantahum Alem et al. [9] 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.

Lalit Himral et al. [10] proposed an efficient and very simple approach for the detection of the black hole attack in the mobile ad hoc networks implemented on the AODV protocol. This method prevents from the black hole attack by the identifications of the nodes with their sequence number. The identification is made for whether there is large difference between the sequence number given by the source node and the sequence number given by the intermediate nodes who has sent back RREP message. In General RREP is sent by the malicious node with high destination sequence number than the other nodes and this entry is stored as the first entry in the Route Reply Table. It Then compare the first destination sequence number with the source node sequence number and if there exists much more differences between them, then that node definitely is the malicious node, and the source node immediately remove that entry from the Route Reply Table. When the malicious node is identified, the routing table information sent from the malicious node, are discarded from the network.

Watchara et al. [11] proposed an efficient solution for the detection of Black hole attack in the AODV based MANET. They proposed a new approach called CAODV (Credit based AODV). A credit based mechanism is very efficient to detect

the Black hole attack is AODV because the Black hole attack can be detected before it occur in the network.

Shashank Khare et al. [12] proposed a solution to improve the basic working of the AODV routing protocol, to detect and remove the Black hole attacker nodes in the MANET. In this proposed solution for the reduction of the probability of the Black hole attacker node it is proposed to wait for all the replies coming from the neighboring nodes and then check these replies so that a reliable route is found. So in this approach a node sends data to another node only when it has the replies from the entire neighboring node and detects the reliable route among the all routes given from the neighboring nodes. A 'Timer Expired Table', is used for collecting the requests from the neighboring nodes, 'sequence numbers', and the time at which the packet arrives.

Firoz Ahmed et al. [13] 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.

Golak Panda et al. [14] proposed a secure algorithm for the detection of the Black hole attack in AODV protocol in Mobile Adhoc networks. In this proposed algorithm a key mechanism process is used. For the generation of the key some extra phases are added in the normal AODV protocol So that the process of key generation and key comparison can be done efficiently. The source node encrypts the message with the encrypted key and the destination node can detects the encrypted message. Thus if any attacker node gets the message it cannot understand that because it doesn't have the decryption key.

Amol Bhosle et al. [15] 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.

Sowmya K.S. et al. [16] proposed a simple and efficient mechasnism for providind the security againt 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.

Sarita Choudhary et al. [17] provides an efficient approach for the detection of black hole and Gray hole attack in Mobile Ad hoc Networks based on the AODV routing protocol. In this approach malicious nodes are listed locally by each and every node when the nodes act as a source node. The protocol uses the concept of Core Maintenance of the Allocation Table. In the Allocation table when a new node joins the network, broadcast message for the request to get the IP address as it want to be a part of that network. The nodes, also called as the backbone nodes which receive this message chose an free IP address randomly and unicast this IP address to the requesting node. When the requesting node get this allotted IP address sends back an acknowledgement to the Black hole node. Thus the allocation is only done through the Backbone node and it has the overall control the malicious node can be easily detected.

M. Umaparvathy et al. [18] 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.

6. PROPOSED WORK

In this research paper a secure efficient algorithm for the detection of the Black hole attack is described. This algorithm firstly identifies the black hole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. The algorithm is implemented in a popular reactive routing protocol, called AODV (Ad hoc On demand Distance Vector Routing). The beauty of the proposed algorithm is that it works in both the cases when there is no communication (i.e., a node is idle) and when a node is communicating (node is not idle).

To check if a node is idle, we set a threshold value (T_h) of 1000 mseconds for the Communication Interval (CI). And if the CI is more than this threshold value then we start the procedure for the detection of the malicious node. For this, the node see the entries of the recent paths stored in its route cache and then sends RREQ packets to them and waits for the reply. Based on the reply it stores the entries in terms of the DSN in decreasing order and then calls the Black hole detection procedure. The important thing in this approach is that the RREQ packets are sent in Fibonacci series pattern till the Flow count Threshold F_{th} is not reached. In this algorithm value of F_{th} is set to 34 mseconds.

When a Node is node is not Idle, then simply the Blackhole_Detection procedure is invoked.

The description of the Blackhole_Detection Procedure is given as : If DSN is so much greater than SSN then consider this node as the suspicious node and then retrieve the second entry from the routing table and if the DSN for this node is so much greater than the SSN then consider this node also as a suspicious node and the process continued until we reach at a point where there is a sufficient difference between the source node and the destination node and after this call the route discovery procedure second time and if it finds that suspicious nodes are again appearing in the R-R table with the Highest SSN, then treats these nodes as the Black hole node.

The algorithm is described below:

Algorithm:

Step 1: Root Discovery Process
The source node S starts the route discovery phase by broadcasting the RREQ packet to the neighboring node.

Step 2: Collecting Replies
The Source node store all the replies arrived from the destination node or the intermediate nodes in terms of their DSN and NID and arrange them in terms of the decreasing DSNs in RR – Table

Step 3: Identification of Black hole Node

Case 1: When a node is Idle:
If ($CI > T_h$)
{ Idle node Prepares 3 packets and send them as 0, 1 and 1 msec, respectively. i.e., $Fcnt_{src1}$=0; $Fcnt_{src2}$=1; and $Fcnt_{src3}$=1;
Do
{Call the procedure (Blackhole_ Detection)
$Fcnt_{src\ 1}$= $Fcnt_{src\ 2}$;
$Fcnt_{src\ 2}$= $Fcnt_{src\ 3}$;
$Fcnt_{src\ 3}$= $Fcnt_{src\ 1}$+ $Fcnt_{src\ 2}$;}
While ($Fcnt_{src3}$ <= F_{th})}
Else
{Reset $Fcnt_{src}$ with the initial value}

Case 2: When a node is not Idle:
Source node retrieves the top entry from RR-Table.
Call the Procedure **Blackhole_Detection**

Procedure (Black hole_ Detection)
If (DSN >>> SSN)
{
Set x[Node_id] =1;
}
Else if(x[Node_id] = =1)
{Malicious node= x[Node_id];
Go to step 4}
Else
The node is not an attacker node

Step 4: Removal of Black hole Node
Remove the Entry of the entire malicious node (s) from the R-R table detected through **Blackhole_Detection** Procedure in step 3
Step 5: Node Selection Process for Secure Routing
Sort the contents of RR-Table entries according to the DSN in decreasing order and select the node which has highest DSN.

Step 6: Continue Default Routing Process
Continue with the normal procedure of AODV Protocol.

The Abbreviations used in the above algorithm are:
SSN - Source Sequence Number
DSN -Desination Sequence Number
NID - Node ID CI - Communication Interval
T_h - Threshold Value for CI R-R Table-Route Reply Table
F_{th}- Flow count Threshold
x[Node_Id]=Suspicious or Black hole Node

7. IMPLEMENTATION AND RESULTS

7.1 Parameters

The parameters are defined in the table 1 below:

Table 1 Simulation Parameters

Parameter	Value
Simulator	NS-2
Version	NS 2.34
Number of Nodes	30
Topography Dimension	670 m x 670 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	50
Channel	Wireless Channel
Max/Min Movement Speed	50 m/sec.
Min Movement Speed	10 m/sec
Pause Time	10 sec.
Seed	125

7.2 Simulation Results

Figure 7 is showing the simulation scenario of the 30 mobile wireless nodes.

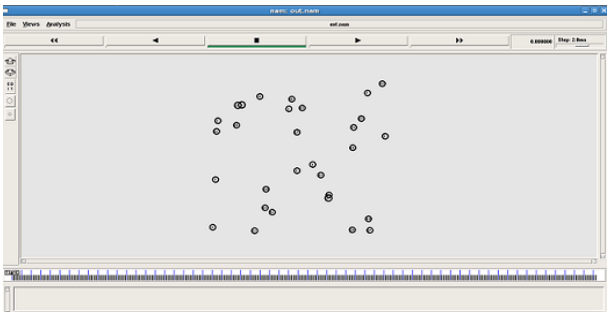

Fig 7: Simulation of 30 Mobile Nodes Implementing AODV Protocol

7.3 Simulation Graphs

Two graphs Throughput Graph and Packet Delivery Ratio Graphs are used to show the simulation results for the case when There is Only one Attacker Black hole node present in the network, While three graphs Throughput Graph, Packet Delivery Ration Graph and End to End Delay Graph are used to show the simulation results for the case when there is more than one attacker Black hole nodes are present in the network.

In both of the cases, every graph has two sub graphs: first graph is for showing the results when there are attacker nodes in the AODV protocol and we have no prevention algorithm there. This graph is shown by the red color and names as AODV. While the second graph is for showing the results when there are attacker nodes in the networks and we implemented our prevention algorithm for the identification and removal of these attacker nodes. This graph is shown by the green color and named as NAODV.

7.3.1 Case 1: When There is only one Attacker Node

7.3.1.1 Throughput Graph

This metric is basically used to describe the total number of bits send to the physical layer per second. So it is always measured in kbps. This Graph is drawn between Mobility (in m/sec) in X Axis and Throughput (in Kbps) in Y-Axis.

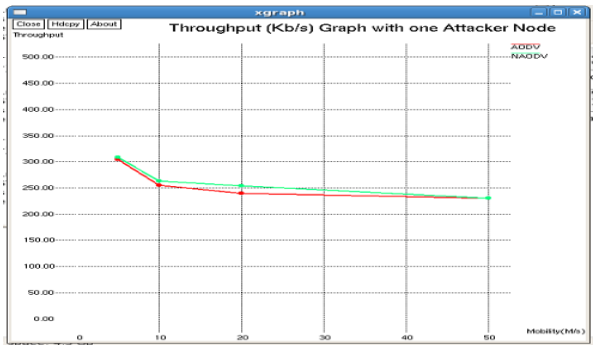

Fig 8: Throughput Graph with one attacker node

7.3.1.2 Packet delivery Ratio Graph

Basically this graph is used to describe the Packet delivery ratio which is the ratio of total incoming packets and actual received packets by the destination. This Graph is drawn between Mobility (in m/sec) in X Axis and PDR in Y-Axis.

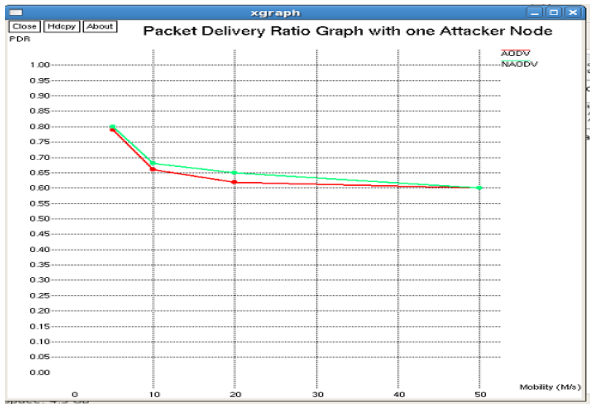

Fig 9: Packet Delivery Ratio Graph with one attacker node

7.3.2 Case 2: When There are More than one Attacker Nodes (in our case 5)

7.3.2.1 Average End to End Delay Graph

This metric is basically used to describe the average time to send a packet from source to the destination. It is always measured in seconds. This Graph is drawn between Number of Black hole Nodes in X Axis and Avg. End to end Delay (in milliseconds) in Y-Axis.

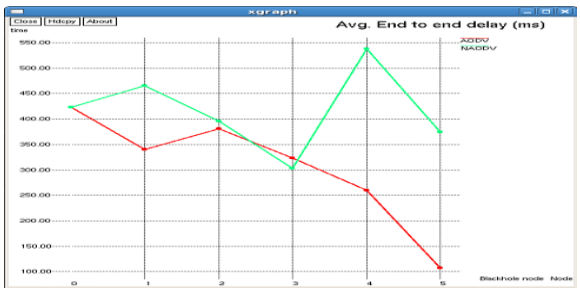

Fig 10: Average End to End Delay (in msec.) Graph with more than one attacker node

7.3.2.2 Throughput Graph

This metric is basically used to describe total number of bits send to physical layer per second. So it is always measured in kbps. This Graph is drawn between Number of Black hole Nodes in X Axis and Throughput (in Kbps) in Y-Axis.

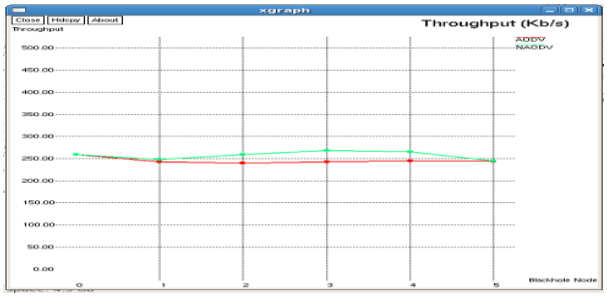

Fig 11: Throughput Graph with more than one attacker node

7.3.2.3 Packet delivery Ratio Graph

This graph is used to describe Packet delivery ratio which is the ratio of total incoming packets and actual received packets by the destination. This Graph is drawn between Number of Black hole Nodes in X Axis and PDR in Y-Axis.

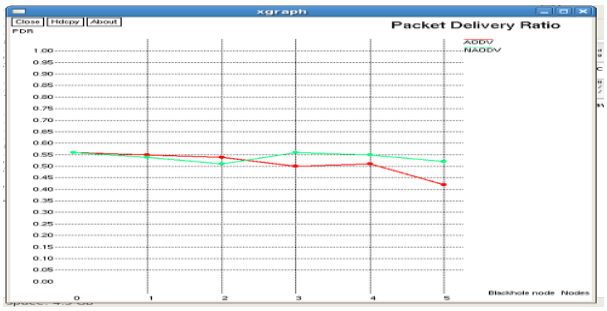

Fig 12: Packet Delivery Ratio Graph with more than one attacker node

8. CONCLUSION AND FUTURE SCOPE

In this research paper an efficient approach for the detection of the Black hole attack in the Mobile Ad Hoc Networks on AODV routing protocol is proposed. The beauty of this algorithm is that it can detects the black hole nodes in both of the cases when a node is not idle and when node is idle(i.e., there is no communication for a defined interval). And it

detects the single Black hole node and cooperative Black hole nodes.

These two implementations made the approach very secure and efficient. The comparison graphs show the results in both the cases, i.e., when there are more than one attacker nodes and when there are only one attacker node.

As the future work, this algorithm can be implemented for some other dangerous network layer attacks such as Grey hole or Wormhole attack etc.

9. ACKNOWLEDGMENTS

It is with deep sense of gratitude and reverence to **Prof (Dr.) Ajay Khunthetha, and Prof Manish Singhal** for providing all the facilities and working environment in the institute.

We want to express our deep sense of obligation to our family and God for their blessings and encouragement.

10. 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] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA

[8] W.Kozma, and L. Lazos,"REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009.

[9] 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.

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

[11] Watchara Saetang, Sakuna Charoenpanyasak ,"CAODV Free Blackhole Attack in Ad Hoc Networks", International Conference on Computer Networks and Communication Systems (CNCS 2012)IPCSIT vol.35(2012) © (2012) IACSIT Press, Singapore.

[12] Shashank Khare, Manish Sharma, Namrata Dixit and Sumit Agrawal," Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET ",VSRD-IJEECE, Vol. 2 (6), 2012, 385-390

[13] 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 .

[14] Mr. Golok Panda, Mr. Gouri Shankar Mishra, Mr. Ashok Kumar Sahoo, "Prevention of Black hole Attack in AODV protocols for Mobile Ad Hoc Network by Key Authentication"**,** IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.3, June 2012.

[15] 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.2012.2105 45.

[16] 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

[17] 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.

[18] 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