ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# Wormhole Attack Elimination in Mobile Ad-hoc Networks With OPTIMIZED Multipath Algorithm

**Waseem Ahad**[*1], **Varun Sharma**[2]
[*1,2]Department of Computer Science, CTIEMT, Jalandhar, India
khanday.waseem@gmail.com

## Abstract

Communication has different terms for different users in the technology. Wireless and Ad-hoc communication are two main communication medium which are fulfilling different domain requirement for the users. Talking about Ad-hoc networks, usually communication is based on the ad-hoc protocol policies. Most of the users in allover ad-hoc network using Ad-hoc On Demand Distance Vector Protocol (AODV) for the basic communication due to simplicity and reliability of protocol. More usage also attracts number of attackers which tends to disturb the communication. Most occurred attack in AODV network is Wormhole attack which provide lowest destination id to the source so t become the part of shortest selected path by AODV process. This attack starts proceeding by introducing the similar metrics which are taken into account by AODV while selecting the route for destination. It introduce lower number of hops and lower value of delay so that AODV will select the fake route defined by attack automatically and after attack launch, attack start decreasing the overall throughput of the network. Wormhole attack affects the network performance and overall network performance degraded a lot. To eliminate the effects of Wormhole attack, we have proposed a packet update scheme in which we fetch information from the neighbors for the enquiry of the suspected nodes in the network. Proposed scheme eliminate the Wormhole affects by finding all the malicious nodes which are present in the network and send broadcast to whole network for elimination of malicious nodes. Throughput and delay are the parameters for the performance measurements of the network. Proposed scheme provides better results with 37 % less delay as compared to the previous proposed schemes. Previous scheme provides slighter better results of 6% more throughput than our proposed scheme.

**Keywords**: Wormhole Attack, AODV, Multipath Algorithm, On Demand Routing Protocols, Route Request, Route Reply, Mobile Ad-hoc Network

## Introduction

A MANET consists of mobile nodes, a router with multiple hosts and wireless communication devices. The wireless communication devices are transmitters, receivers and smart antennas. Mobile Ad hoc Network (MANET) [1] is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. MANET is the quick remedy for any disaster situation. MANET is a spontaneous network. It is useful when dealing with wireless devices in which some of the devices are part of the network only for the duration of a communication session [2]

### AODV (AD HOC ON-Demand Distance Vector)

AODV is an on-demand routing protocol [2]. The AODV algorithm gives an easy way to get change in the link situation. [3 ] If link failure occurred then notifications are sent only to the affected nodes within range in the network. Generally after receiving this notification, it cancels almost all the routes through this affected node. [7]

Generally maintenance of AODV process is based on timely updates which suggest that entries into AODV process expired after timer expires. Further updated information is passed to the neighbors so that it can be updated about route breakage. Discovery of various routes from single source to various destinations is totally based on query and reply packets and intermediate nodes use logs to store the information of routes in route table. Various control messages which are used for the discovery and corrupted routes are as follows: [7] Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR), HELLO Messages. [7]

**Route Request (RREQ)**

Various route request packet are flooded through the network when a route is not available for the destination from source. [3][4][5]

Pair source address and request ID identify RREQ and counter is incremented every time source node sends a new RREQ. [5][6] After receiving of request message, each node checks the request ID and source address pair. The new RREQ is discarded if there is already RREQ packet with same pair of parameters. [8]

Node with no routes information to particularly destination or any destination will be discarded and information is broadcasted to update information to other routes. [9]

A route reply (RREP) message is generated and sent back to source if a node has route with sequence number greater than or equal to that of RREQ.

**Route Reply (RREP)**

On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node. [10]

**Route Error Message (RERR)**

The neighborhood nodes are monitored. When a route that is active is lost, the neighborhood nodes are notified by route error message (RERR) on both sides of link. [6]

**Wormhole Attack**

Wormhole attack is always launched by attacker who tunnels packets at one point to another point in the network, and then use to reply to the sender again. The wormhole attack can have dangerous effects threat in mobile ad-hoc networks, especially against many On Demand protocols for ad hoc network routing protocols. [13]

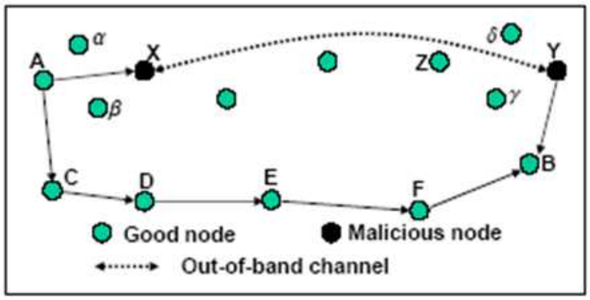


**Figure 1: Wormhole attack demonstration**

It is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. [6] [7] [8] During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. [9] [10] [11] Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand). [12]

## Problem Definition

MANET is a mobile ad-hoc network which dynamically set up temporary paths between mobile nodes which acts both as router and hosts to send and receive packets. It is mobile ad-hoc network which has dynamic moving topology, no intermediate device is there for monitoring and limited physical security so it is more vulnerable to attacks and one of them is Wormhole Attack.

The application of multi-path techniques in wireless ad hoc networks attracts a lot of attention recently because multi-path routing (MR) reduces the damages of unreliable wireless links and the constantly changing network topology. [13]

In Wormhole attack a malicious node makes use of the vulnerabilities of the route discovery packets as attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network [8].

This attack can be easily implemented in AODV during the routing discovery process. An attacker can create a wormhole even for packets not addressed to it-self, since it can hear them in wireless transmission and tunnel them to the attacker at the opposite end of the wormhole. Once the forged route has been established the malicious node is able to become a member of the active route and intercept all communication packets across that node.

The proposed work have focused on providing solution for this problem by enhancing multipath algorithm resulting in regaining of the average no. of hops as well to get normal delay by excluding the attacker nodes and these factors will be implemented using existing multipath algorithm with relevant changes as explained in research methodology portion which can prevent Wormhole attacks in MANET networks

## Methodology

This research has focused on providing solution for said problem by enhancing multipath algorithm resulting in regaining of the average no. of hops as well to get normal delay by excluding the attacker nodes.

This research has focused on the multipath algorithm to avoid the wormhole attack in MANETs.

Research has started with building a MANET network in OPNET simulator with Random Waypoint mobility Model for providing mobility with AODV as routing protocol as described in figure 2 below.

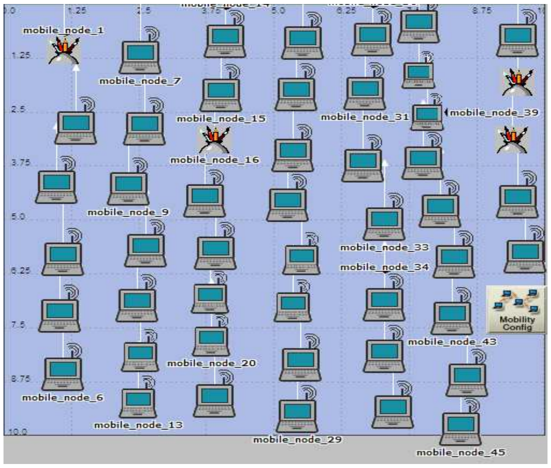


**Figure 2: Overall simulation with random waypoint model for mobility.**

After basic building, implementation of wormhole attacks has been implemented by making an attacker transmitter and attacker receiver. Implementation has shown the wormhole attack effects on normal MANET network. Both scenarios has been compared on the bases of parameters like throughput, number of hops, end to end delay and network load.

To avoid the wormhole attack, proposed algorithm has been implemented in scenario affected by wormhole attacks and this tried to normalize the scenario to its original state. Proposed algorithm, randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as wormhole attack is done by transmitter and receiver so have to decide the transmitter and receiver. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm checked the delay of all previous routes which involve any on node of the suspicious route. The node not encounter previously should be malicious. Now to find out exact malicious node, there is need to repeat the whole algorithm if more than one node is misbehaving and that will take time and resources. So to avoid this condition, transmitter will be seeking help from directly connected neighbors. Neighbors can tell the history of particular node under suspect. The node which is not involved in any of the previous activity considered to be the malicious node. Malicious nodes have been blacklisted by the nodes and hence they are not involved in future routes.

The steps of modeling in FSM (Finite State Machine) of Proposed Algorithm are as follows:

## Proposed Algorithm

/* S is consider to be the source node and D can be consider to be the Destination Node over the network*/

{

**Step 1:** Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number updates the route in the network. Once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet then forwards it to its next node available. This algorithm process is repeated until it reaches the final destination.

**Step 2:** While receiving the RREQ packet each node update their routing table. Once the destination node receives RREQ message from neighboring nodes, it then unicasts the RREP (route reply) back to the source node.

**Step 3:** As transmission begin it will search for all the intermediate nodes called Neighbor List.

**Step 4:** If number of packet drop is large then start discovery of malfunctioning nodes.

**Step 5:** Source and destination will be decided. Randomly Generate a Number in between 0 to maximum number of nodes. Initiate a source by making transmitter node same selected.

**Step 6:** Generate the Route from selected transmitting node to any destination node with specified average route length.

```
Send packet to destination
{
Start timer (Record (Hop Count, Delay))
Counter (Threshold (Hop Count, Delay))
{
Store (Route, Hop Count, Delay)
Continue the process
```

```
}
Step 7:Wormhole Detection
{
Hop count <Threshold
Then Check Delay
}
Step 8:Malicious Node Selection
N is the number of nodes.
{
If N = 1
Thenit is the attacker
Else
Send Route Query to neighbors
{
If neighbor detect similar malfunctioning
Then mark it malicious.
Else
{
Repeat process
}
```

**Step 9:**Send worm_annoucement message to all nodes. Any node receives worm_annoucement message it removes wormhole node id from its neighbor table and Routing Table. If any forwarding node receives worm_announcement message it will send RERR message to source.

For elimination of the wormhole node, architecture based changes has been done for overtaking the effect of wormhole. The node architecture of normal scenario (Figure 3) and node architecture changes (Figure 4) are given below.

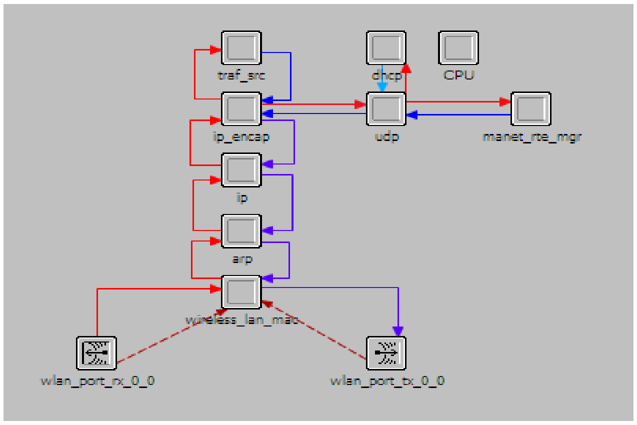


**Figure 3: Node Architecture of normal process of AODV**

Below is the changes architecture of the AODV process for eliminating the wormhole affected network.

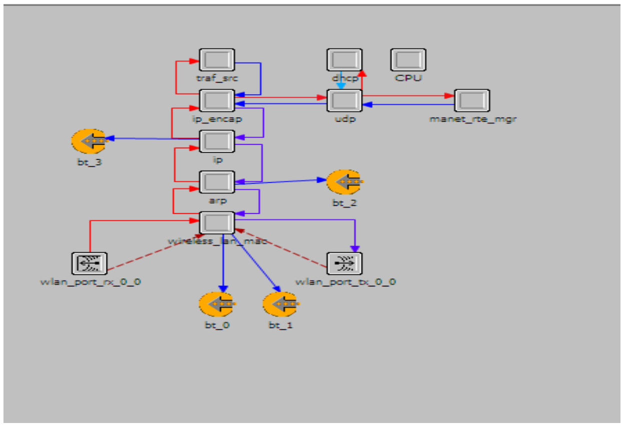


**Figure 4: Node Architecture changes done for elimination of Wormhole**

Performance of network decreases after wormhole attack and to eliminate of this attack, multipath approach of AODV protocol has been implemented by introducing logging modules on medium access layer which use to monitor average metric value used by network while communication. It maintains an average value for delay and number of hops.

Module evokes the multipath properly of AODV process and hence eliminates the nodes by introducing the query messages to the neighbors and finds the exact malicious nodes. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes.

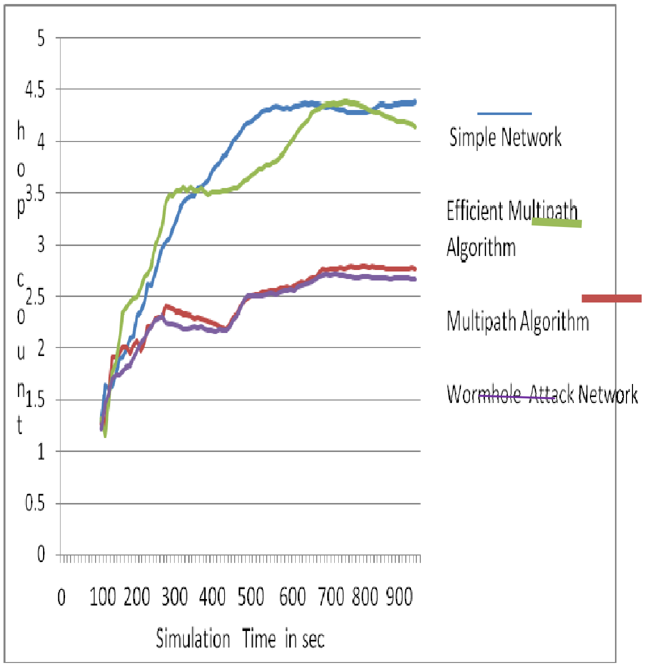
## Results and Discussion

Basic parameters used for experimentation. Some of the experimentation done for checking the behavior of AODV protocol under wormhole attacks are given below:

| Parameters | Value |
|---|---|
| Simulator | OPNET |
| Simulation Time | 900 |
| No of nodes | 50 |
| Routing Protocol | AODV |
| Traffic Model | CBR |
| Pause Time | 100 sec |
| Speed | 11 mps |

Results obtained for normal performance of AODV, Performance of AODV under wormhole attacks and performance behavior of AODV with elimination of wormhole attacks in term of throughput, delay, number of hops in AODV network for proposed and existing algorithm is discussed in the following sections basic parameters used for experimentation with OPNET simulator. Area for communication is 1500 × 1500 meters with 50 mobile nodes.

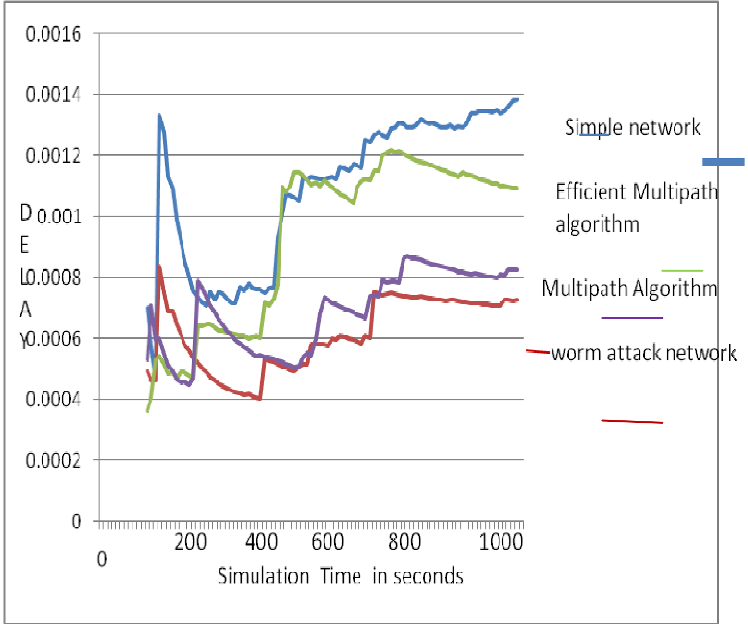
### Performance of AODV With HOP Count



**(a)** Hop count variation of proposed and existing algorithm:

In the above fig (a) the hop count results for simple network, efficient multipath algorithm, multipath algorithm and wormhole attack network is shown. It has been observed that hop count value of simple network is 4.4 after 900 seconds, in presence wormhole attack the hop count value is 2.7 therefore, it has reduced about 38%from simple network. By implementing efficient multipath algorithm the hop count value is 4.2 which is 5% less than simple network, and total recovery is about 34% from attack. By implementing multipath algorithm the hop count
Value is 2.8 it is 37% less than normal and total
Recovery is about 2% from wormhole attack.
Thus it is clear from the above figure (a) above that the recovery and improvement is more in presence of Efficient multipath algorithm which is about 32% more than previous multipath algorithm

### Performance of AODV with Delay



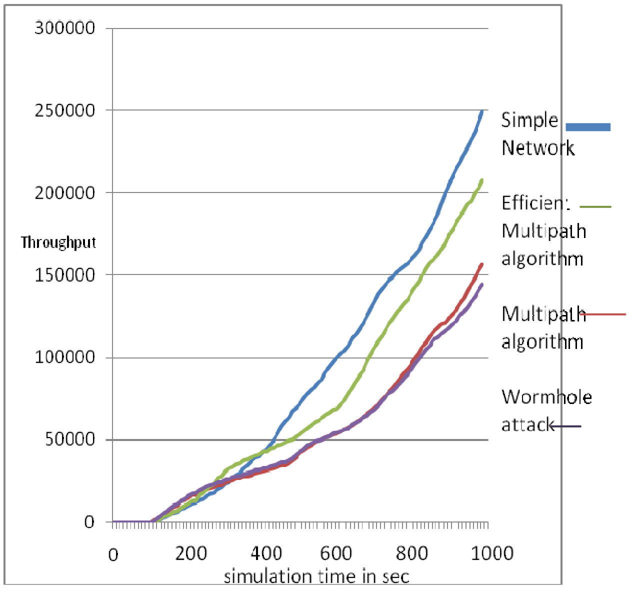
**(b) Delay variation of proposed and existing algorithm:**

In the above fig (b) the Delay results for simple network, Efficient multipath algorithm, multipath algorithm and wormhole attack network is shown. It has been observed that Delay value of simple network is 0.0014 after 900 seconds, in presence wormhole attack the Delay value is 0.0007 therefore, it has reduced about 50%from simple network. By implementing Efficient multipath algorithm the Delay value is 0.0011 which is 22% less than simple network, and total recovery is about 28% from attack. By implementing multipath algorithm the Delay value is 0.0009 it is 36% less than normal and total recovery is about 14% from wormhole attack. Thus it is clear from the above fig (b) that the recovery and improvement is more in presence of Efficient multipath algorithm which is about 14% more than previous multipath algorithm

**Performance of AODV with Throughput**

Throughput variation of proposed and existing algorithm

.



**(c)**

In the above fig (c) the Throughput results for simple network, efficient multipath algorithm, multipath algorithm and wormhole attack network is shown. It has been observed that Throughput value of simple network is 250000 bits/sec after 900 seconds, in presence wormhole attack the Throughput value is 140000 therefore, it has reduced about 44% from simple network. By implementing efficient multipath algorithm the throughput value is 210000 which are 16% less than simple network, and total recovery is about 28% from attack. By implementing multipath algorithm the throughput value is 160000 it is 36% less than normal and total recovery is about 8% from wormhole attack. Thus it is clear from the above fig (c) that the recovery and improvement is more in presence of efficient multipath algorithm which is about 20% more than previous multipath algorithm.

## Conclusion

In this work, the performance of the Ad-hoc on demand distance vector routing protocol has been summarized. The validation of the proposed work has been done by comparing it to the results based on similar research done previously. In previous study, wormhole elimination has been done on the bases of prominent mode algorithm but concept used broadcasting which used huge resources. In this research, unicasting process has been used instead of broadcasting which can save resources and provided useful better results. In previous study similar parameters have been used and it shows that the proposed algorithm results for hop count, delay and throughput are better than existing algorithm as shown in the graphs above. The main focus was to show the performance of AODV under normal environment, under wormhole attack and performance after elimination of wormhole attack in term of throughput, number of hops per route, delay and in future this work can be extended for other parameters also. It is an important issue for the further study to implement the proposed scheme on the distributed environment of wireless ad-hoc devices. The proposed work need strong testing in scenario where energy saving is a big concern. Moreover implementation of clustering approaches with proposed scheme can be consider providing security with resources saving in the wireless Ad-hoc networks.

## References

[1] Ningrinla Marchang , Raja Datta, “Collaborative techniques for intrusion detection in mobile ad-hoc networks”, Journal on Adhoc Networks, Science Direct conference, Vol.10, No. 7, pp 1179-1190, March 2008.

[2] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, “A Cryptographic Handshaking Approach to Prevent Wormhole Attack in MANET” International Journal of Computer Applications, Vol.50, No. 2, pp 265-269, April 2012.

[3] Shang-Ming Jen , Chi-Sung Laih and Wen-Chung Kuo, “A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET”, International Journal of Engineering and Innovative Technology, sensors, Vol.2, No. 2, pp 384-389, August 2009.

[4] Routing protocols and concepts, CCNA exploration companion guide. ‘‘Introduction to dynamic routing protocols’’. Chapter three, pp 148-177.

[5] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis, “Securing Threshold-based intrusion detection in ad hoc networks and secure AODV”, International Journal of Advances in Engineering & Technology, Science Direct, Vol.1, No. 5, pp 337-341, November 2008.

[6] Imran Raza, S.A. Hussain, “Identification of malicious nodes in an AODV pure ad hoc network through guard nodes”, Science Direct Conference on Consumer Communications and Networking, pp 593 - 598, January 2008.

[7] Ningrinla Marchang, Raja Datta, “Collaborative techniques for intrusion detection in mobile ad-hoc networks”, Conference of Information Technology, Science Direct, Vol. 2, No. 2, pp 704-709, April 2008.

[8] Nikos Komninos, Dimitris Vergados, Christos Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks", Conference on Asia-Pacific Service Computing Conference, Science Direct, pp 172- 178, December 2007.

[9] Imrich Chlamtac, Marco Conti,"Mobile ad hoc networking: imperatives and challenges", International Conference on Computer Science and Network Technology, science Direct, Vol.1, No.4, pp 445-449, December 2003.

[10] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review" IRACST – Engineering Science and Technology: An International Journal (ESTIJ), Vol.2, No. 2, pp 1–5, April 2012.

[11] Shalini Jain, Mohit Jain, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol.1, No.7, pp 172 – 175, June 2010.

[12] Dr. Karim Konate, Abdourahime Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking, Vol. 4, No. 2, pp 156-158, June 2011..

[13]Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi, "Elimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol .1, No.2, pp 40-47, December 2011.