# EFFICIENT MULTIPATH ALGORITHM IN MANETS TO PREVENT WORMHOLE ATTACK

Waseem Ahad[1], Manju Bala[2]
Research Scholar, CTIEMT, Jalandhar[1]
Department of Computer Science, CTIEMT, Jalandhar[2]

## Abstract:

Modern communication is containing different types of wireless networks as backbone for various applications used for different users. Mobile Ad-hoc Networks is the type of network which contains many mobile devices and provide good solution for many type communications for different applications military, industry and remote areas (flood hit areas, nuclear hit areas etc). In most of cases the networks which are limited with energy carrying capacity are more vulnerable to breakdowns and attacks which can be harmful for given network communication. Wormhole attack is a type of attack which affects various types of networks starting from variation of wireless standards to various wired networks. Wormhole attack is the most occurring attack in mobile ad-hoc network communication with different types according to the sequence of the attack generated. Wormhole attack is very dangerous and active in case of Reactive Protocols such as Ad-hoc On Demand Distance Vector Protocol. In this paper, we have proposed multipath neighbor help mechanism to detect and prevent the effect of wormhole attack from mobile ad-hoc network. The proposed mechanism successfully isolates the wormhole attack with 50 nodes in wireless mobile ad-hoc network communication.

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

## 1. Introduction

In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is the most dangerous and sort of hidden attack. Wormhole attack usually has two attacker nodes which create a tunnel by skipping other nodes and start transfer information to other end of attacker node. Malicious nodes have different range and can be placed on different locations which perform a tunnel of high speed link via a secrete channel. [15]
These nodes can act as router or host or both at same time. They can form random topologies depending on their connectivity with each other in the network. [16] These nodes have the ability to arrange themselves and because of their self-configuration ability, they can be deployed immediately without the need of any infrastructure. The major performance constraint comes from path loss and multiple path fading. Many MANET routing protocols exploit multiple paths to route the packets.

## 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 than 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)**

© 2013 IJAIR. ALL RIGHTS RESERVED

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]

## 3. 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. [14]

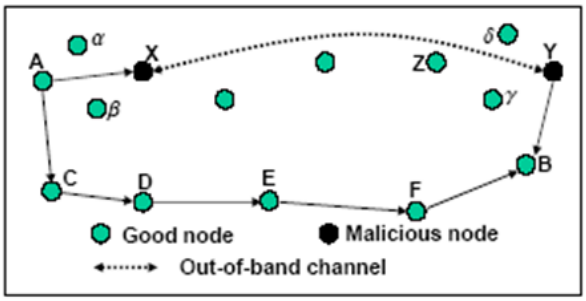


Figure 1: Wormhole attack demonstration

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]

## 4. 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. [14]

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

## 5. 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.

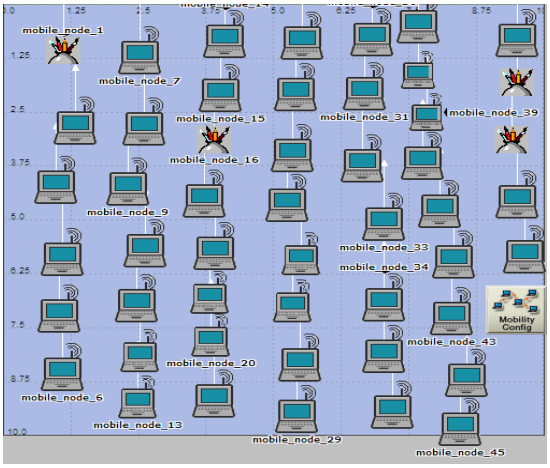


Figure 2: Overall simulation with random waypoint model for mobility.

After basic building, implementation of wormhole attacks has been implemented by making an attacker transmitter and attacker receiver. Implementation has shown the

© 2013 IJAIR. ALL RIGHTS RESERVED

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. 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 takes more 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:

**WormHole (S,D)**

/* 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
Then it 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.

© 2013 IJAIR. ALL RIGHTS RESERVED

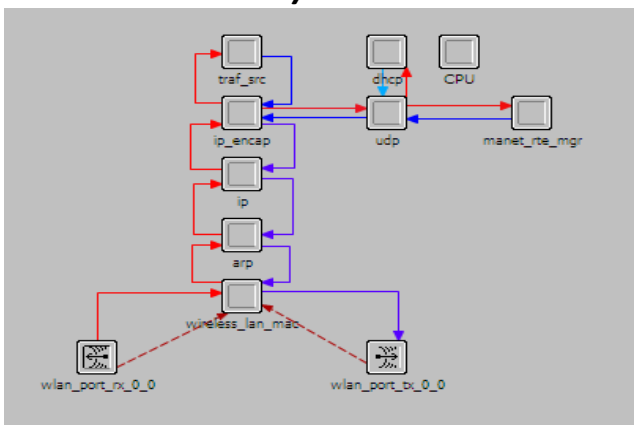


Figure 3: Node Architecture of normal process of AODV

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

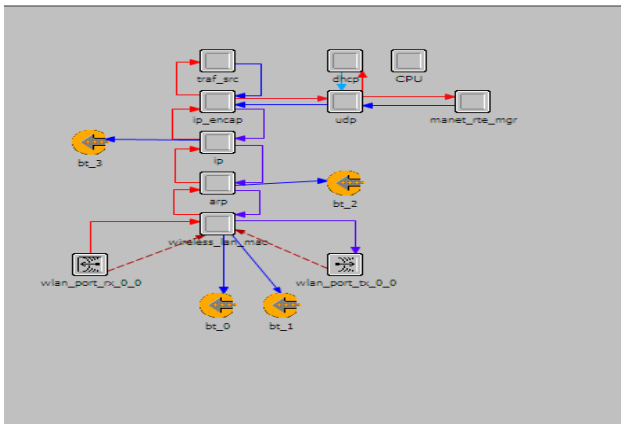


Figure 4: Node Architecture changes done for elimination of Wormhole

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.

## 7. Experimentation

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 and Traffic Received in AODV network is discussed in the following sections.

**Performance of AODV with Throughput of three Scenarios**

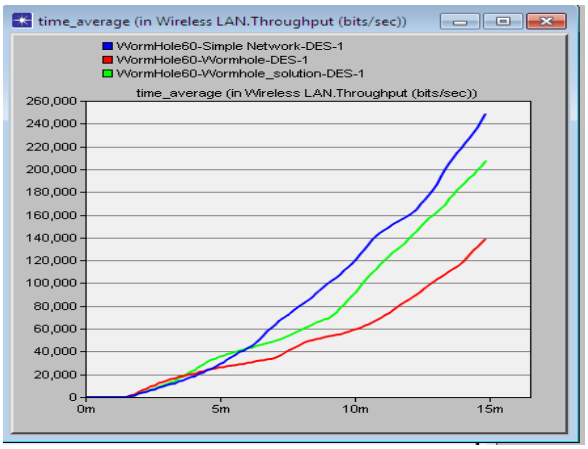


Figure 5: Throughput (bits/sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 5) and it show that the upper blue line of the throughput for normal AODV scenario. Bottom Red line shows the decrease in the throughput in case of wormhole attack scenario. Middle curve shows the normalization process of the network as in case of elimination of wormhole throughput gradually increase and tends towards the normal throughput. It is clear from the graph that elimination of wormhole provides great results.

**Performance of AODV with Traffic Received of three Scenarios**

© 2013 IJAIR. ALL RIGHTS RESERVED

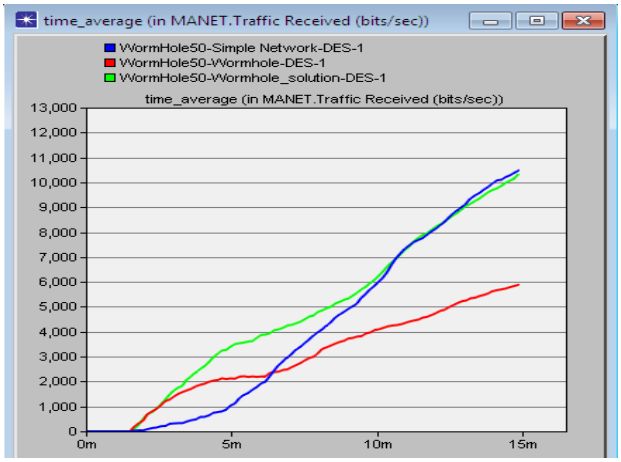


Figure 6: Traffic Received (bits/sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 6) and it show that the wormhole scenario decreases the traffic received by the normal process of the AODV and wormhole elimination scenario normalized the traffic received similar to the state of traffic received by the normal AODV process.

**Performance of AODV with Delay of three Scenarios**

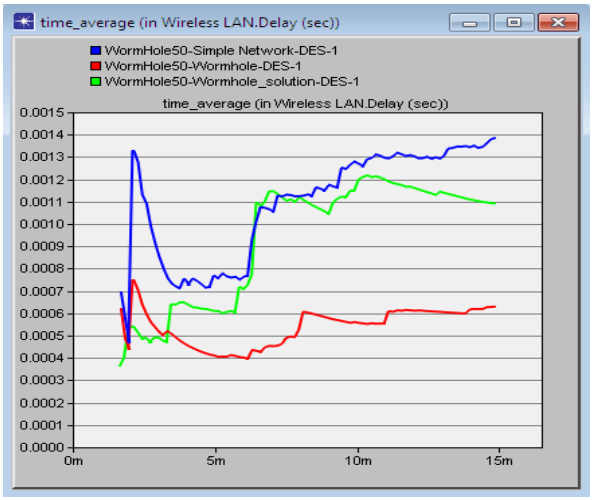


Figure 7: Delay (sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 7) and it show that the upper blue line shows` the delay of the normal network and bottom red line shows the decrease in the delay which is in case of wormhole attack as in wormhole attack delay introduced by attacker is always low as compared to normal network. Middle curve shows the delay normalization process with elimination of wormhole in third scenario.

**Performance of AODV with Number of Hops of three Scenarios**

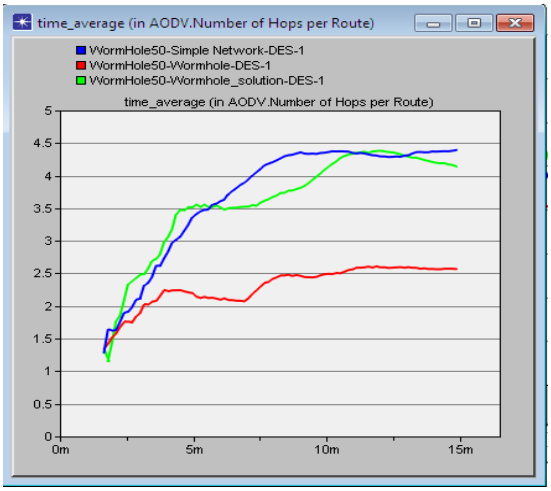


Figure 8: Number of hops per route comparison of all three scenarios

The performance of network is compared in above figure (Figure 8) and bottom Red curve shows the wormhole case which use to fake the hops count as lower than normal so that AODV would send data by considering lowest hops count as best path. Upper Blue curve shows the number of hops per route of normal AODV scenario and normalized value of hop count shown in middle curve shows elimination of wormhole scenario.

The overall simulation performance is presented in nutshell in the following table, which indicates that the elimination of wormhole attack scenario provides the better results and try to normalize the wormhole effected network to its normal state as close as possible.

## 7. Conclusion

In this work, the performance of the Ad-hoc on demand distance vector routing protocol has been summarized. 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 traffic received. In doing so, a wormhole scenario has been created and four wormhole attacker nodes have been generated. These malicious nodes provide false information to the network and AODV consider the path defined by malicious nodes as best routing path available and start communication through it. 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. After

© 2013 IJAIR. ALL RIGHTS RESERVED

implementation of this module, it finds the malicious nodes because the metric values of malicious nodes are very less as compare to normal metric value. A summary of suspected nodes has been forwarded to the upper layer where another module has been added to find the sequence of attack. If any sequence found, it is sent to network layer where another module is added to find the solution for attacks. Module use to evoke the multipath properly of AODV process and hence eliminate the nodes by introducing the query messages to the neighbors and find the exact malicious nodes. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes.

In nutshell, elimination of wormhole attack has been done so that ad-hoc communication can be normalized as normal communication.

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] Reshmi Maulik, Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, Vol. 3, No. 1, pp 271-279, January 2011.

[14] Gajendra Singh Chandel, Priyanka Mur, "Manet Threat Alarming Based On System Statistics & Support Vector Machine", International Journal of Engineering Research and Applications, Vol.2, No. 4, pp 1722-1726, August 2012.

[15] A.Shevtekar, K.Anantharam, N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communication Letters, Vol.9, No. 4, pp 363–65, April 2005.


© 2013 IJAIR. ALL RIGHTS RESERVED

[16] Amol A. Bhosle, Tushar P. Thosar, SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications , Vol.2 , No. 1, pp 325-331, February 2012.

.

© 2013 IJAIR. ALL RIGHTS RESERVED