International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 398 - 403

A Ubiquitous Solution for Mitigation of Black Hole Attack in Cognitive Radio

Girish Tiwari
Associate Professor, Department of Electronics & Communication Engineering
Ujjain Engineering College Ujjain, Sanwer Road line
Ujjain, India
tiwari_girish@yahoo.com

Nishant Doshi
PG Scholar, Department of Electronics & Communication Engineering
Ujjain Engineering College Ujjain, Sanwer Road line
Ujjain, India
nishantmdoshi@gmail.com

***Abstract*—** In the current scenario Cognitive Radio (CR) has become one of the best available solution for spectrum shortage problem. Moreover, for secure data transmission over these networks it is mandatory to make these networks robust and less vulnerable against the various types of attacks. Through this paper we have presented a ubiquitous solution for one of the attack viz. black hole attack. Its implementation and simulation in detail with PDR and Throughput. The paper deals with different type of attacks and protocols explained well here. Further there is implemention of algorithm on different parameters to achieve the improved rates than earlier solutions. The paper also deals with question of selecting AODV as it protocol used in simulation. Many aspects of attacks, secure network environment are explained here in this paper. Finally in simulation we got improved results for the parameters taken with some modification in AODV protocol.

Keywords: *Black hole, Gray hole, AODV Routing, PDR, Throughput*

*****

I. INTRODUCTION

The recent development in wireless technology and rapid deployment of wireless Networks, the industrial, scientific and medical (ISM) band has faced a considerable amount of saturation. The ISM band is also shared by license free communication devices. Due to all these factors, the band is heavily congested. On the other hand, licensed bands do not face this problem. Besides, the bandwidths that are allocated to licensed users are not used regularly which results in spectrum holes. The spectrum holes are unused spectrum space at that point in time. This discrepancy projects the inefficient spectrum allocation techniques used for both licensed and unlicensed radio frequencies. Hence a new technology is required to use the spectrum holes for communication and thus provide some relaxation to the congested bandwidth. Cognitive radio (CR) [1] technology is envisioned to solve this inefficiency problem by using the available spectrum strategically without interfering with the licensed users. It is a new paradigm in the wireless communication networks that promises reliable communication by sharing the spectrum effectively. It introduces a flexible way to optimally use the bandwidth.

Some typical types of active attacks these are as follows [2] :

1) Black hole: A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.
2) Denial of Service (DoS): A malicious node make recurrent routing requests so as the whole network sources become busy and thus unavailable to whole nodes in this whole bandwidth got trapped and hijacked.
3) Impersonation: A malicious node may pretend to be another node while sending the data packets to create an inconsistent update in the Routing Table (RT).
4) Disclosure: The malicious node release intimate address etc. If combined with some modifications its quiet harmful attack identity in the network, such as by altering the Ip.
5) Sleep deprivation: Battery powered devices always try to conserve energy by transmitting only when it is prominently needed, and malicious node requests many more possible routing or by any such means in which the battery consumption is increased.
6) Information to the licensed user in the network, and that cause the unauthorized to attack the target nodes affecting the RT.
7) Spoofing: It occurs when a node impersonate its

These are mechanisms that help prevent, detect, and respond to security attacks. There are major security goals that need to be addressed in order to maintain a reliable and secure network environment. They are mainly [2]:

1) Confidentiality: Protection of any information from being exposed to unintended entities.
2) Availability: It is much more needed feature for providing service i.e. to be always available whenever needed to the licensed user.
3) Authentication: This check is quiet useful to prevent many attacks from the attackers and become safe at the end of good authenticating system. Thus block the unauthorized user from it.
4) Integrity: Message being transmitted is never altered.
5) Non-repudiation: Ensures no conflict between sending and receiving ends so that no congestion and re-occurrence of data packets occur.
6) Assurance: It is required to commit the security measures have been properly implemented and no mal-practicing is done.

In the rest of the paper is organized as follows: In section literature review. In section III, we present types of attack in detail, followed by section IV, it presents the simulation results. In section V, we draw a conclusion and address the future work.

II. LITERATURE REVIEW

Many research have been made in order to avoid and detect Black Hole attack. This section discusses earlier works done corresponding to Black hole attack in AODV and their advantage and disadvantage.

Related work in [3], R. Yeneni and Anil Sarje modified RREP & RREQ as MRREP & MRREQ making an extra packet which uses random numbers for control packet, which cannot be changed by malicious node thus are caught here. But this comes with drawback of more time consumption more than earlier.

In [4],K.A. Jalil, Z. Ahmad and 1. Manan introduced a Enhanced Route Discovery AODV (ERDA) in which it makes the database all received REPs for this it neglects first REP and start the database from second REP but there is problem if the REP itself is black hole then it creates problem.

K. Lakshmi et al. proposed a solution in [5], it is assumed that an exceptionally large sequence number is the reply from malicious node, but it is always time specific thus it won't work all the times.

In [6], L. Himral et al. enhanced the work of [5]. They deleted queue of incoming REPs for waiting. Thus time limit problem is solved.

R. Dr. S. Tamilarasan in [7], followed algorithm as in [5] and [6]. And in this REP with exceptiona;;y large random number will be considered as black hole doesn't provide then algorithm fails.

A novel solution in [8], is proposed by Shalini Sharma and Girish Tiwari et al. the algorithm of IDS in this they opt for high destination sequence number (DSN) and forward it, if black hole gives low then it lowers down the output.

III. TYPES OF ATTACK

We will discuss here different kinds of attacks generally found in any network Wormhole, Black hole and Gray hole attacks[9].

A. *BLACK HOLE ATTACK*

Black hole attack is a sort of attack that generates and disseminates fabricated routing information. In this attack, a intruding node sends fake RREP, RREQ etc information, which appears to be the shortest and congestion free route and thus it compels to pass all data packet through it in network. Like in AODV, the intruder sends a fake RREP to the source node, introducing itself as having the shortest and right route to the destination node. Thus source node has to select the route that passes through the intruder. Therefore, all data packets will be routed through the intruder, and therefore, it can exploit or drop the information packets of the network traffic.

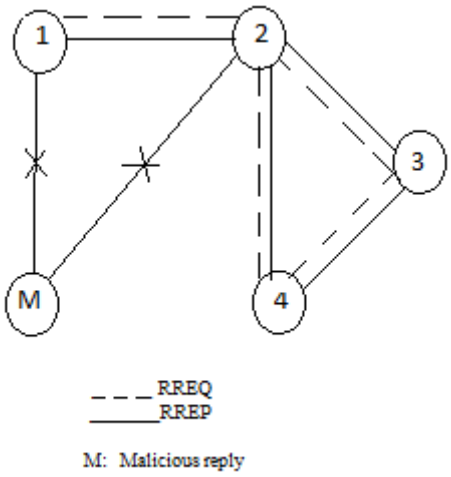

Figure 1. Black Hole Attack

B. *WORMHOLE ATTACK*

A wormhole attack is one of the most dangerous form of black hole attack. In wormhole attack, the intruders pair keep record of packets at any location and reply them back to another location using their own private high speed network. The dangerous part of this attack is that it is valid and can be run for all communication systems that provide confidentiality & authenticity. Figure 2 depicts the wormhole attack for reactive routing protocol.

In this attack, intruder connects with two distinct points in the network, and from that point it replies back. Figure 3 depicts the wormhole attack with certain conditions. There are 2 end-points of the wormhole established connection (called as wormholes). In Fig. 2, the attack is assumed between the 2 node neighboring nodes. This link of wormhole can be setup by many sorts like by using Ethernet cables, an optical link in wired medium and long-range wireless transmissions. This attack records packets at any one end-point in the network and transfers them to another end-point.

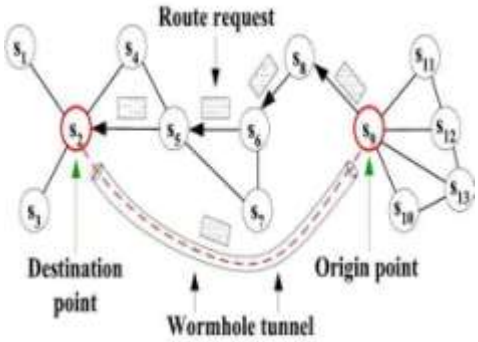

Figure 2. Wormhole Attack[19]

C. *GRAYHOLE ATTACK*

Gray hole attack is a modification or advancement of Black hole attack in which a behavior of intruder is highly unpredictable.

Gray hole attacks are of three kinds mainly.

1. In this the intruding node may or may not drop some

packets from any nodes and can forwards all other packets.

2. In this attack, a node may mischief for a limited time period only, and late on it become normal node like present in the network and functions properly.
3. In this type of attack, both types of attack as defined above in 1 & 2 can be used at a time is the third type attack. And because this reason gray hole attack is not an easy task to be detected and mitigated easily. This in effect disturbs very much to network and its proper functioning.

In Figure node 4 is the source node and 2 is the Destination Node. M node treats as a malicious node for node 2 and it act as a normal node for some time and drop the packet some time.

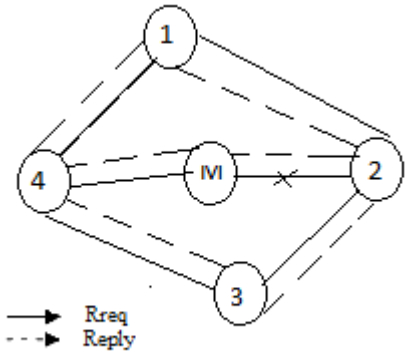

Figure 3. Gray hole Attack

IV. AODV PROTOCOL

The work of proactive protocol is to regulate and update the routing information of every node and it is updated throughout the network periodically or when topology changes. Each node here is required for storing and exchanging routing information with each other nodes frequently so that they can have update about all the current routes and their information of every route i.e. destination sequence distance vector (DSDV) Protocol. While in reactive or source initiated on demand protocols, a node is active only on demand whenever it is required it don't take pain of finding the route periodically i.e. Ad hoc on demand distance vector (AODV) Dynamic Source Routing (DSR) etc. Moreover, Hybrid protocol makes use of both proactive and reactive kind of techniques i.e. Zone Routing Protocol (ZRP).

The paper is focused on AODV protocol which is one of the reactive routing protocols. AODV is a protocol which best suits our requirement and therefore many researchers use because of its dynamic features and adaptability for any type environment. As it is applicable for both type of routing i.e. Unicast & Multicast. It is self-starting protocol & loop-free protocol. It activates whenever the route is needed by network nodes.

The Ad hoc On Demand Distance Vector (AODV) is a routing protocol designed for MANETs. AODV setup connections between mobile nodes and maintains the routes when demanded.

Route Discovery Process: Control messages establishes the route between the nodes AODV i.e. RREQ and RREP. RREQ is broadcasted through source node for Route Discovery. RREQ have broadcast ID, source node's IP, present destination sequence number and Time-To-Live (TTL) value. Updation of neighboring nodes through their routing table, record backward route and forwarding of RREQ is done for it, if they don't have any route to destination.

A node sends RREP after receiving RREQ if:

1. It is itself a destination node, else
2. The route towards destination is having with a large sequence number than or equals to that in received RREQ.

In AODV nodes maintain all the information which is needed about new routes. And the processing of RREQ cannot be done again. When any RREQ is fetched by a node which has been found by it earlier then this RREQ is discarded.

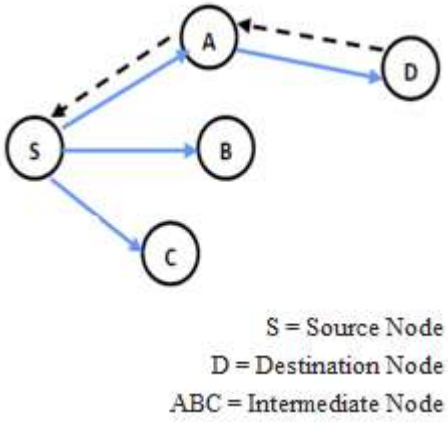

Fig. 4. Basic AODV mechanism[5]

Source node initiates transmission of data packet to destination whenever REP is received by it. Thus updating of routing table is done if :

A). RREP got new sequence number, or

B). It receives a RREP afterwards with little hop count but the sequence number is same.

Acknowledgement by source node if RREP with highest sequence number is received and also if multiple RREPs are received

type	flags	Reserved	Hop count
RREQ(Broadcast) id			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Figure 5. RREQ[10]

type	A	reserved	Hop count
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

Figure 6. RREP [10]

Destination IP address

 ISSN: 2321-8169
398 - 403

Destination sequence number
Hope-count
Next-hop
First-hop
Valid bit
Count

Figure 7. Fields of AODV routing table[10]

V. PROPOSED SOLUTION

In AODV the selection of route is done on the basis od highest destination sequence number. In this the malicious black hole node will easily be qualified for the route selection process and hence the performance of this is degraded thus.

In the proposed methodology there are some changes in the protocol as extra bit is added as Check field (CF) so as to ensure the proper detection of black hole solution and thus removal of malicious node from the network.

Primarily an extra bit is added which in turn is CF has the formula of 2h+1 as h is here hop count so it directly relates the Routing table here so that from nowhere there can be a chance of intrusion entrance in the network. It is its unique feature here. As RREQ is circulated the process of finding the path for destination node starts and then we get RREP thus we get hop count and update CF with the help of its formula here. As the CF is updated we move further to update RT with following entries as in AODV and CF as an extra bit. Now, if any malicious node try to send fake RREP then it will be caught as it is not aware about the CF and if then don't know the formulae used in this solution.

Steps involved in Proposed Solution

A) Source node begins process of finding route and thus REQ is circulated to the neighboring nodes.

B) RREP replied by destination node contains hop count and check field (CF).

C) Now by using the hop count (h) for extra bit CF RREP will calculate CF=2h+1.

D) Destination sends back with CF=2h+1, resets its value to NULL.

E) Now, destination node reply has replier with updated hop count & CF to source node.

F) Updating of RREP's database with CF value.

G) Now entries in database are to checked and the entries which is not having any field of CF will be considered as malicious node.

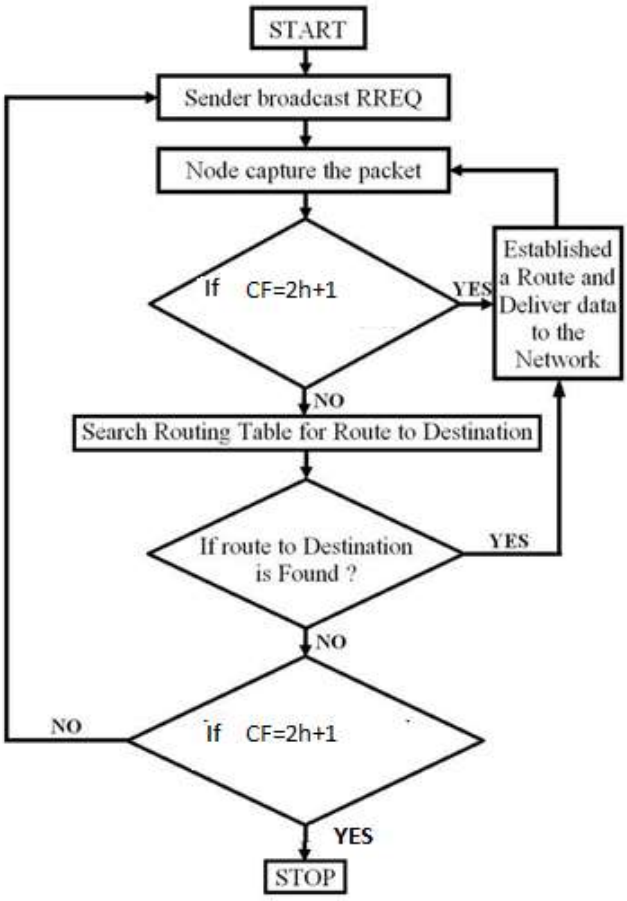

Figure 8. Flowchart

H) Now, if black hole will reply with any false RREP, it will not be aware of extra CF field and thus caught and removed from the network.

In this way malicious node will be removed and thus network will perform properly.

VI . SIMULATION AND RESULTS

1. Packet delivery ratio (PDR): The ratio of total number of packets send from source node defined as S to total number of packets received successfully at each destination nodes defined as D.

$$PDR = S/D$$

2. Throughput: It is defined as the rate of successfully delivered packets in the network to the rate of received file by a host over a period of time is called as Throughput. Unit of the throughput is bits per time.

$$\text{Throughput} = \frac{\text{Total number of bits transmited}}{\text{Total time taken for transmission}}$$

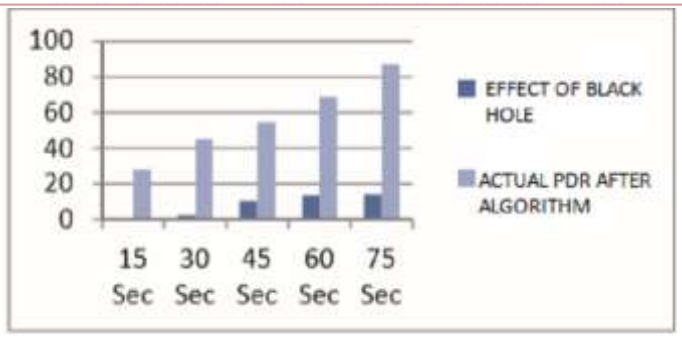

Figure 9. Comparison of PDR with effect of attack

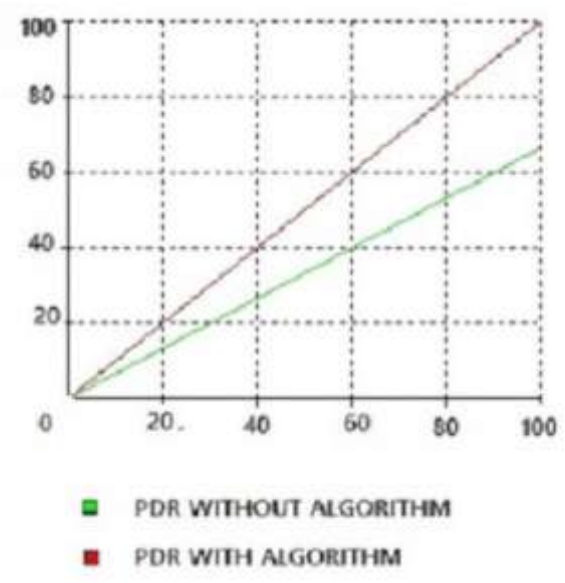

Figure 10. PDR with and without algorithm

The algorithm is simulated with the help of NS2.35 simulator and verifies that the proposed solution is serves the improved version of work done in this field on PDS and Throughput. In this paper we have also compared the results with earlier work and shown it throughout all the figures.

Simulation parameters:

Channel type: Wireless channel

Radio propagation model: Two ray

MAC type: 802.11

Topographical area: 800*800 meters

Routing protocol: AODV

Number of nodes: 100

Number of mobile nodes: 20

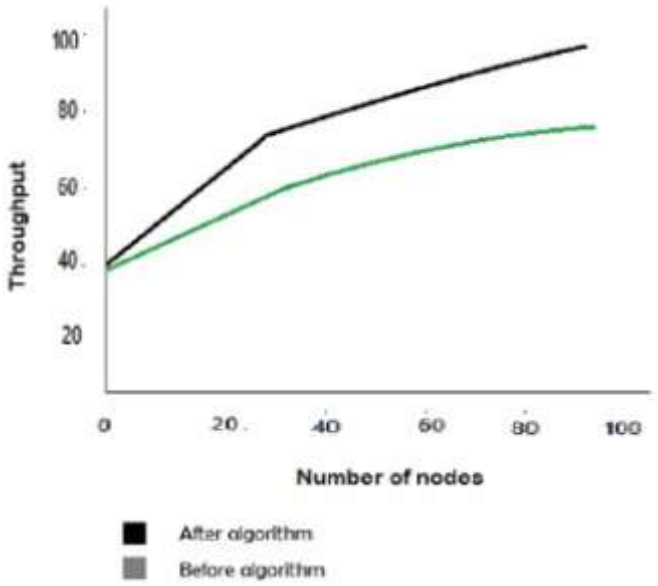

Figure 11. Throughput with earlier and applied algorithm

VII CONCLUSION

Black hole attack is one of the major security challenges for cognitive radio. We have proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to identify multiple black hole nodes cooperating with each other in a cognitive radio; and Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also we showed that the effect of packet delivery ratio and Throughput with respect to the variable node mobility. There is reduction in Packet Delivery Ratio and Throughput. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of malicious node in networks is still considered to be a challenging. Simulation show that AODV with our mechanism gave comparatively better performances as compared to AODV. As a future scope of work, the proposed security mechanism may be extended to detect other malicious nodes as gray hole and Detection of wormhole attacks in cognitive radio.

REFERENCES

[1] Ramesh babu B, Meenakshi Tripathi , Manoj Singh Gaur, Dinesh Gopalani, Dharm Singh Jat “Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact” , IEEE conference , pp 125-130, 2015.

[2] Junhai Luo, Mingyu Fan, and Danxia Ye “ Black Hole Attack Prevention Based on Authentication Mechanism” IEEE ICCS, pp 173-177, 2008.

[3] R. Yerneni and AK Sarje. "Enhncing performance of AODV against Black Hole attack," in Proceedings of the CUBE Conference intenational information Technoloy, 2012, pp. 857-862.

[4] K.A. Jalil, Z. Ahmad, J.L.A Manan. "Securing Routing Table Update in AODV Routing Protocol," in Proceedings

of iEEE Conference on Open Systems (lCOS), 2011, pp. 116-121.

[5] K. Lakshmi et al. " Modiied AODV Protocol against Blackhole Attacks in MANET." international Journal of Engineering and Technoloy , vol. 2, no. 6, pp. 444-449, 2010.

[6] L. Himral et al. "Preventing AODV Routing Protocol from Black Hole Attack." intenational Jounal of Engineering Science and Technoloy (JEST), vol. 3, no. 5, pp. 3927-3932, May 201I.

[7] Dr. S. Tamilarasan. " Securing AODV Routing Protocol from Black Hole Attack." intenational Jounal of Computer Science and Telecommunications(IJCST), vol. 3, no. 7, pp. 52-56, Jul. 2012.

[8] Shalini Sharma, Girish Tiwari "A new IDS scheme against blackhole attack to enhance security in wireless network" International journal of research in engineering and technology (IJRET) vol. 9, no. 8,pp 429-433,aug 2015

[9] Hitesh Gupta, Shivshakti Shrivastav, Sanjana Sharma " Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing " IEEE 5th International Conference on Computational Intelligence and Communication Networks , pp 380-384, 2013

[10] Neeraj Arya " Detecting and Avoiding of Worm Hole Attack and Collaborative Blackhole attack on MANET using Trusted AODV Routing Algorithm " IEEE International Conference on Computer, Communication and Control (IC4-2015)

[11] Ankur mishra, Ranjeet Jaiswal, Sanjay Sharma " A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network " 3rd IEEE International Advance Computing Conference (IACC) 2013, oo 499-504.

[12] Ume-Hani Syed " Avoidance of Black Hole Affected Routes in AODV- Based MANET " International Conference on Open Source Systems and Technologies, pp182-185, 2014

[13] P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks," In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.

[14] H. Deng, W. Li, and D.P. Agrawal, "Routing security in wireless Ad hoc networks," IEEE Communications Magazine, Vol. 40, Issue: 10, October 2002, pp .70 - 75.

[15] S. Marti, T. Guili, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In Proceedings of MOBICOM Boston, Massachusetts, United States,2000, pp. 255-265.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.

[17] S. Lu, L. Li, K-Y Lam, L. Jia, "SAODV: A Manet Routing protocol that can Withstand BlackHole Attack", Proc. of Intl. Conference on Computational Intelligence and Security (CIS '09), Dec. 11-14,Beijing, China, pp. 421-425, 2009

[18] S. Deswal and S. Singh, "Implementation of Routing Security As- pects in AODV", Intl. Journal of Computer Theory and Engineering, Vol. 2, No.1 Feb., 2010