International Journal of Computer Applications (0975 – 8887)
Volume 175 – No.1, October 2017

An Enhanced Detection Technique for Blackhole Attack in MANET

Nivedita Leo
[1]PG Scholar, Department of Computer Science Engineering, GGITS, Jabalpur, M.P, India

Sharda Patel
[2]Asst.Professor, Department of Computer Science Engineering, GGITS Jabalpur, M.P, India

ABSTRACT
A mobile ad-hoc network (MANET) is a self-optimizing infrastructure-less network. AODV (Ad-hoc On-demand Distance Vector) routing protocol is a loop free protocol used in ad-hoc networks. It is designed such that it can self-start in an environment where all the nodes are mobile in nature. It can also resist a variety of network behaviors such as mobility, failure of links and much more. The ad-hoc network is susceptible to black-hole attack. In a black hole attack, the router drops the packets instead relaying them and is a type of denial-of-service attack.

The proposed work enhances the AODV routing protocol for detecting a black hole attack more efficiently and hence reducing the delay and communication overhead in the MANET. In the proposed work, the behavior of the source node is modified by broadcasting the pirated RREQ which includes its own sequence number instead of destination sequence number and preprocess RREP () function is also added which makes it more secure than the existing solutions. For this the network simulation 2.35 is used. The results obtained from the proposed methodology shows that the end-to-end delay has been decreased; packet delivery ratio and throughput have been increased.

Keywords
MANET, AODV, Black hole Attack, NS-2

1. INTRODUCTION
Mobile ad-hoc network (MANET) has various properties such as operation flexibility and simple installation. Due to these properties, over the last few years, many researchers have shown their interest in MANET. In Ad-hoc network all nodes are mobile, there is no physical connection while communicating with each other. One of the main characteristics of it is its ability to operate without any central coordinator. There are many real-world applications of this network, ranging from military to civilian, in search and rescue missions, in the collection of data's, and in virtual classrooms and conferences. Multi-hop radio relaying results in frequent link breakage due to mobile nodes in the network. It also has a resource constraint like bandwidth, computing power, battery lifetime and many more. [7]. As there are various functions that take place in the MANET like packet forwarding and others, the security is one of the essential components.

One of the most popular routing protocol used in MANET is Ad-hoc on-demand distance vector (AODV) routing protocol. As compared to others, AODV routing protocol offers several benefits such as dynamic in nature, self-starting, and multiple-hops routing. Furthermore, it can adapt various functions of MANET such as the change in topology, loop-free, and can automatically reject the inactive routes [2]. Unfortunately, AODV routing protocol is vulnerable to many attacks. Among them, the blackhole attack is one of the most critical attacks in AODV based MANET. This attack occurs by sending false routing information to the victim nodes to cause fake route entries of nodes in the routing tables [11]. As a result, many fake routes come into existence and cause a bottleneck in the communication channels.

Figure 1: Mobile Ad-Hoc Network

1.1 Overview of AODV Protocol
AODV routing protocol is an on-demand/reactive protocol. A new route is formed when it is needed from source to destination. A source node broadcast route request (RREQ) packet to find a route to the destination node. If RREQ reaches a destination node either by itself or by a fresh route generated by an intermediate node, then it is said to be an authentic route. The fresh route is considered as an authentic entry if a sequence number of the destination node is greater than that of the RREQ sequence number. The route will be detected if any links break, and reply with a route error (RERR) packet, this packet is used to notify other participating nodes in the network [6][10].

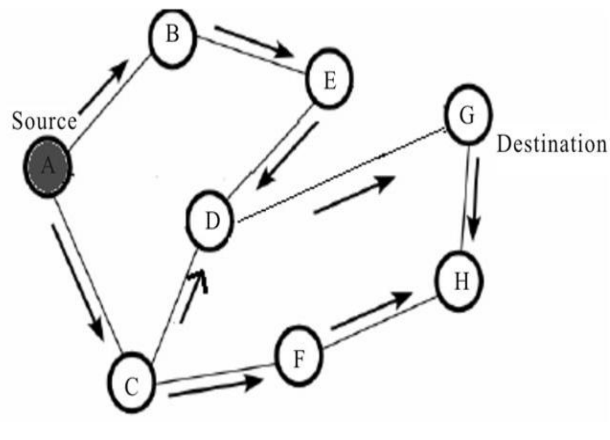

Figure 2: Propagation of RREQ

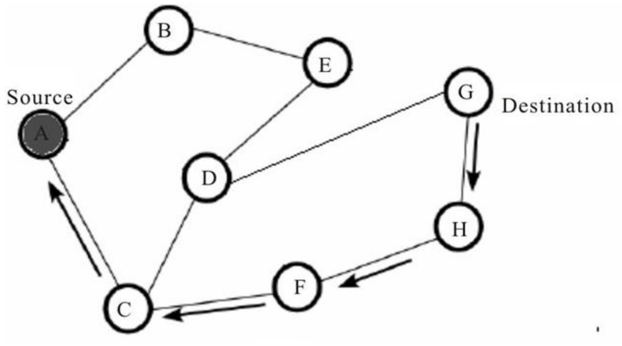

Figure 3: Route determination from source to destination

1.2 Black Hole Attack

Black holes in the network refer to the location where an incoming or outgoing packet is silently discarded (or "dropped"), a source has no information about the data that did not reach its intended recipient. The black hole intruder enters to the broadcast group and tries to separate the packets from the multicast. This type of attack deletes one or more of the recipient packets instead of sending them, as a result the packet delivery rate becomes low [5, 12]. The black hole node waits to receive a RREQ. It answers to the RREQ node before the other nodes do, without verifying its routing list and thereby introducing itself as a fittest path from all the other nodes in the whole network and succeed in gaining all network packets, and can destroy entire network paths and prepare a DOS attack [15, 3, and 4].

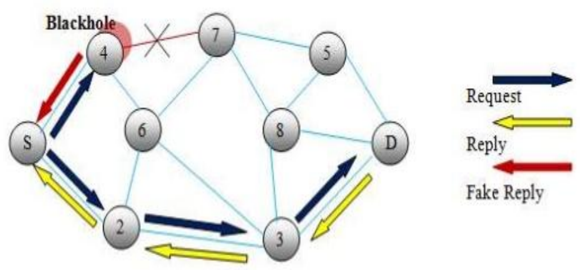

Figure 4: The black hole attack

2. RELATED WORK

To identify the black hole attack, various researches have been conducted, to design methods of intrusion detection systems. Black hole attack is a critical active attack on Ad-Hoc networks. Here in this section, the work done in the field of the black hole attack in AODV protocol is discussed.

In Chavan et al. [1] proposed a modification in AODV, in which the performance of AODV in presence of black hole node is improved. But here routing overhead is more as compare to unmodified AODV.

Poongodi et al. [14] proposed a localized secure routing architecture against cooperative black hole node in MANET. They have proposed a methodology, in which a novel LSAM protocol is designed to provide a security in MANET. It is shown that the proposed protocol is more secured and efficient. Limitation: It increases the overhead from 1 to 4 %on proposed routing protocol.

In Nishukalia et al. [9] proposed a Modified AODV Routing Mechanism for detectinga multiple Blackhole node", here they have used a fake RREQ packet which include source sq. no. instead of destination seq. no. Limitation: In the absence of timer it increases end-to-end delay and also increases the network overhead.

Dhama et al. [13] proposed a detection of black hole attack and prevention mechanism for mobile ad-hoc networks. In this paper they introduce a cross layer queue at the transport layer so that when black node is detected or when a link is broken the packets can be buffered at transport layer queue mean while the nodes will find a new route to the receiver.

Limitation: Improvement over protocol is required so that even when mobility of nodes is increased, the through put will remain same.

In [8] Sharma and Bisen, proposed a detection as well as removal of black hole attack in Manet. Here we have noticed that, there are two mechanisms based intrusion detection drop_ ratio_ analysis and trap_request for detecting and preventing blackhole attacks. Limitation: increases network overhead.

3. PROPOSED WORK

In this section, the algorithm to perform the enhanced detection technique for black-hole attack is disclosed:

a) The source node broadcasts the pirated RREQ packet by the whole of its own source sequence number and address instead of destination sequence number and destination address.
b) When an intermediate nodes receives the pirated RREQ packet, the dealer node alternately calls for Preprocess RREP () method and stores all newly created RREP in the routing table new_RREP tab. Each participant in routing table is assigned by source sequence number.
c) It compares RREP dealer sequence number from the new _RREP_ tab and RREQ source sequence number from routing table. If RREP source sequence number is around greater than RREQ source sequence number, the source node discards this position entry in the new_ RREP _ tab, the table is not empty.
d) If new_RREP_tab is not empty, it will associate the dealer sequence number in pirated RREQ packet it received by the whole of the sequence number of the source described in the table.
e) As the source node sends its own sequence number, it will be more indisputable that it will be the fresh one. The intermediate node will have the source sequence less than the described in pirated RREQ packet. So it will not reply mutually RREP packet.
f) But, if in the network there reside any blackhole node previously it advertises itself as having the shortest path with highest source sequence number and will reply with the RREP packet.
g) The source node will then detect the black hole nodes exist in the network.

Pseudo code of proposed method

Notations:

P: Packet
SN: Source_node
DN: Destination_node
IN: Intermediate_node
RREQ: Route_request
RREP: Route_reply
HC: Hop count
Hdr: Header
Src: Source
Sq. N.: Sequence Number

Drp: Drop
Rcv_time: receiving RREP time.
wait_RREP_time: Waiting time for RREP at source Node.
storeEntry: routing table entry for storing RREP_Entry.
new_RREP_tab: new routing table for storing routing table entry.

```
Step: 1-   // Incoming packets //
           // There are four types of controls packets in AODV //
            Switch (AODVTYPE_P)
            {
Handler( )
             }
             If (AODVTYPE_P_RREQ)
          {
          // if I am the source or previously seen it //
             Do ("Drp_P");}

Step: 2- // BlackHole node gets RREQ packet for Establishing a
fake route to destination //
blackholeAODV: : recvRequest (packet *p) {
Structhdr_ip *ip = HDR_IP(P);
Structhdr_AODV_request *rq =
HDR_AODV_request(p);
BlackholeAODV_rt_entry *rt; }

Step: 3-     // BlackHole node creates a RREP packet
immediately to respond this route request packet //
             Send reply (rq ->rq_src)
            // impose I am not the destination, but I may have a
fresh enough route //
Sq N = max [SqN(u_int32), rq->dst_Sq N >rq_Src_Sq N];
//Comparing of Seq.No.

Step: 4-     // when source node got RREPpacket from malicious
blackhole node //
            Preprocess_ RREP_RecvReply (packet p)
            {
RrepHeaderRREP_Entry;
             P_>RemoveHeader (RREP_Entry);
Rcv_time = receive RREP;
Set_time = Rcv_time + wait_RREP;
storeEntry.add(RREP_Entry);

Step: 5       //Store new_RREP tab entry//
While(Rcv_time<= Set_time)
              {
new_RREP_tab.add(storeEntry);
              }
Step: 6       // If new_RREP_tab is not empty//
               While (new_RREP_tab is not Empty)
              {
                If (RREP.Src_SqN.storeEntry-RT.Src_Sq N)
>(RREQ.Src_Sq N)
                 {   //Blacklist the node(Node is attacker)//
new_RREP_tab.DeleteRout(RREP_Src_SqN.storeEntry)
                  }
              }
Choose packet from new RREP tab and call normal method
RecvReply (Packet) of AODV.
            }
Step: 7    End
```

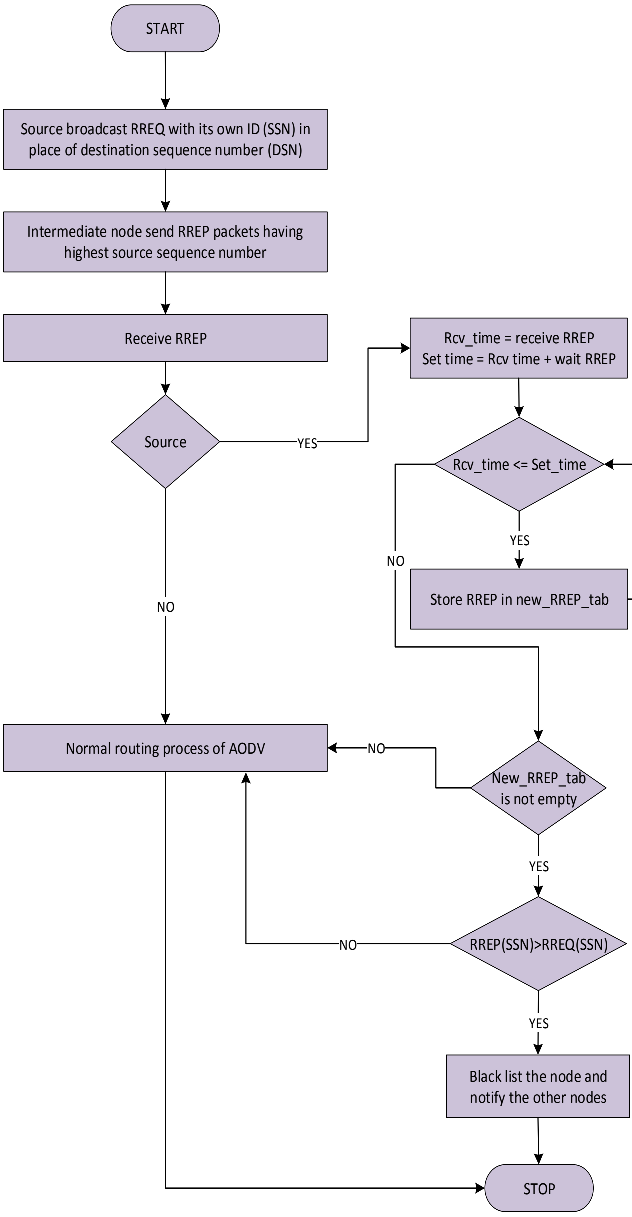

Figure 5: Flowchart of proposed work

4. PREVENTION OF BLACKHOLE ATTACK THROUGH MODIFIED AODV

The changes are done in the AODV protocol. By doing so, the effect of the Blackhole node attack is decreased the overall throughput and packet delivery ratio is increased. To implement it, the simulation of blackhole node attack in AODV is done by using Network Simulator (version 2.35). A new protocol is implemented after modifying AODV in which the data packets are bypassed. For evaluating the performance of new protocol, the various simulation parameters are needed such as, traffic mobility model and many more. The following parameters are used in performing the simulation.

Table 1 Simulation Parameters

Parameters	Value
Channel_type	Wireless_channel
Radio_propogation_model	Two_ray_ground
Mac_type	802.11
Antenna_model	Omni directional antenna
Number_of_mobile_nodes	50
Routing_protocol	AODV
Queue Length	150
Simulation Area	1000*1000
Mobility speed	0-10 m/s
Paused time(seconds)	1-2s
Traffic	CBR(Constant bit rate)
Packet size	512 bytes
Simulation time	300s

5. RESULTS AND GRAPHS

In this section, the results obtained from simulation on various scenarios are presented and discussed in detail. The Blackhole attack is simulated and the effect of an attack on the basis of performance metrics such as Packet Delivery Ratio (PDR), Throughput, End-to-End Delay (EED) is determined by varying mobility speed and number of nodes. Simulation parameters used to build the scenarios are shown in table 1. Simulations are performed using NS-2(version- 2.35)

The comparison of AODV, Black hole AODV and Enhanced Detection Technique (EDT) AODV is evaluated on the basis of Packet delivery ratio, throughput, and end-to-end delay. In figure 6, the packet delivery ratio is evaluated on the basis of mobility. The packet delivery ratio in case of EDT AODV improves over Blackhole AODV.

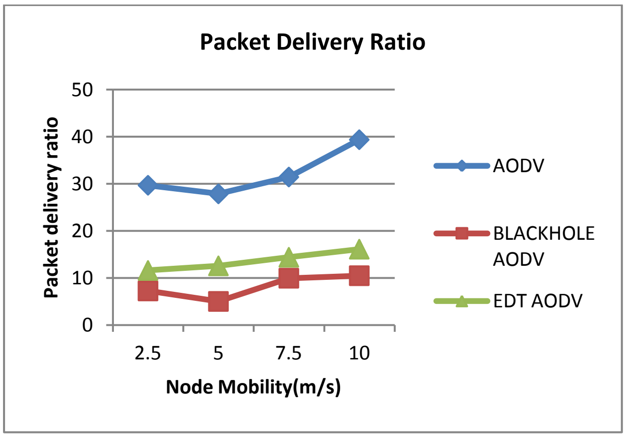

Figure 6: Mobility speed v/s Packet delivery ratio

Throughput: In a given amount of time the data packets transmitted across the network from one end to another end is known as throughput. As compared to the black hole attack in AODV the throughput of EDT AODV is improved.

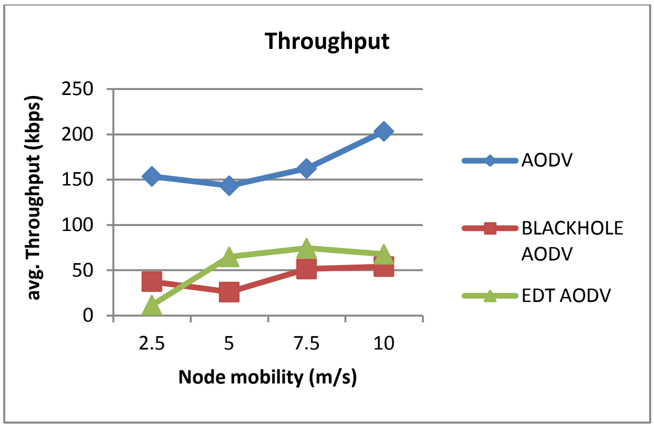

Figure 7: Mobility speed v/s avg. Throughput

End to End delay: It is described as the average time taken by the data packet to be transmitted from source to destination. The end-to-end delay in case of EDT AODV decreases as compared with blackhole AODV.

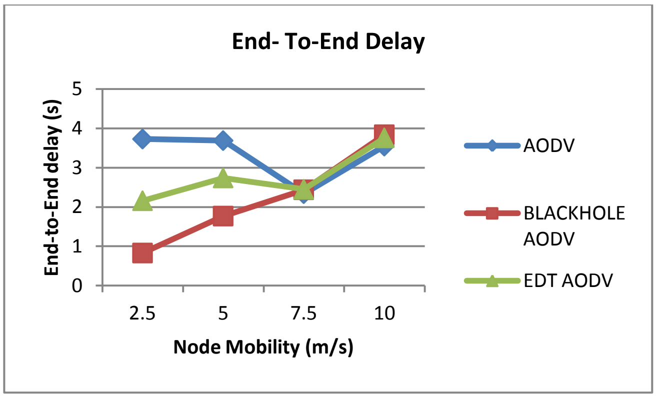

Figure 8: Mobility speed v/s avg. End-to-End Delay

Figure 9 shows the results of attack with increase in number of nodes in the network. As the number of nodes increases, the PDR of EDT AODV becomes greater than AODV because the enhanced detection technique discussed is able to identify a malicious node which greatly increases the network PDR.

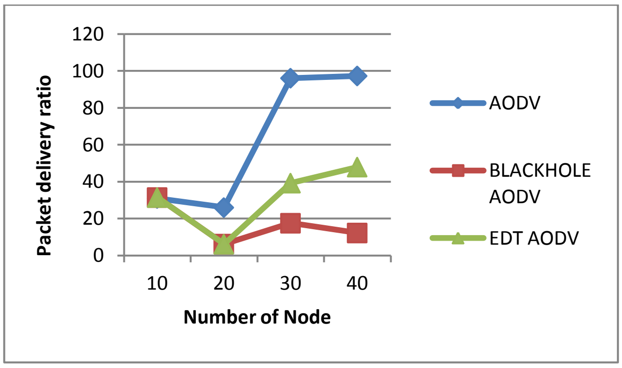

Figure 9: Number of Nodes v/s avg. PDR

Figure 10 shows the effect of AODV under attack and EDT AODV on average end-to-end delay. It can be observe from the figure that the EDT AODV significantly decreases average end-to-end delay.

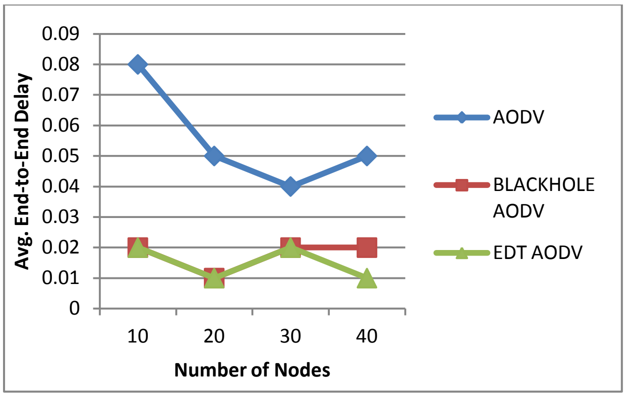

Figure 10: Number of Nodes v/s avg. end-to-end delay

Figure 11 specifies that throughput increases in case of EDT AODV as compare to blackhole AODV.

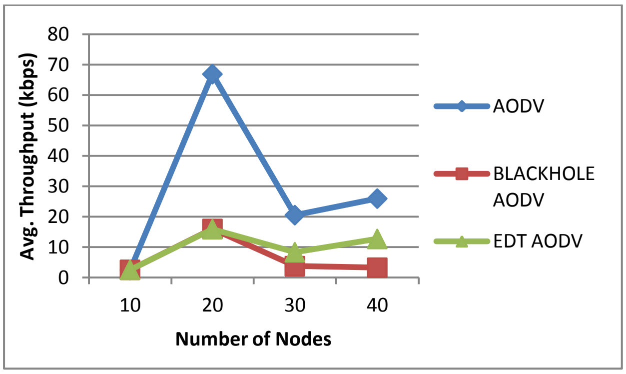

Figure 11: Number of nodes v/s avg. Throughput

6. CONCLUSION

In this thesis, the performance of AODV, Blackhole AODV and EDT AODV routing protocols is analyzed. The EDT AODV is an Enhanced Detection Technique which is effectively implemented using NS 2.35 simulator. The scenarios simulated are with varying number of nodes such as 10, 20, 30, and 40 and with queue length 150. Along with this the nodes mobility speed has been varied between 0-10 m/s, on the basis of three parameters i.e. Packet delivery ratio, average throughput, and average End-to-End delay. In this research, the proposed mechanism handles the blackhole nodes attack in MANET. To tackle the black hole nodes attack, it assume that the source node is an intelligent node which uses the sequence number concept to detect the intruder nodes in MANET and use timer and RREP(). In previous work [9], the source sequence number was used by the source node to detect the black hole attack without the timer. In the absence of time, the source node will not know that how much time it will take to detect the blackhole node. After the blackhole attack has overcome and route resuming is done, it is observed that:-

1. Packet delivery ratio is far better than that of AODV with blackhole (malicious node)
2. The throughput of the network increases.
3. End-to-End delay decreases

Future work: The number of routing protocol provides different types of services to nodes in the presence of different scenario of the network. Every protocol shows different characteristics in the environment of mobile ad hoc network. In future work the stability of routing protocol in presence of multiple blackhole node needs to be studied, and should identify which type of protocol gives the best performance if the size of network will increase sustainably and also found out the simulation result in presence of different scenario in large size of the network with cooperative blackhole nodes and number of mobile nodes.

7. REFERENCES

[1] A. A. Chavan, Prof. D.S.Kuruleb, Prof. P.U.Derec. “Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against BlackHole Attack”. 7th International Conference on Communication, Computing and Virtualization 2016, Published by Elsevier B.V.

[2] Ali Dorri, HamedNikdel, “A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET”,IKT20157th International Conference on Information Knowledge & Technology, 978-1-4673-7485-9/15/$31.00©2015 IEEE.

[3] Chhabra, M.,Gupta, B., &Almomani, A. (2013). “A novel solution to handle DDOS attack in MANET’. Journal of Information Security, 4(3), 165–179.

[4] Jamali, S.B.S. (2015). “A survey over black hole attack detection in mobile ad hoc network”. International Journal of Computer Science and Network Security (IJCSNS), 15, 44

[5] Kurosawa, S.,Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2007). “Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method”. IJ Network Security, 5, 338–346.

[6] KritiPatidar, Vandana Dubey “Modification in Routing Mechanism of AODV for DefendingBlackhole and Wormhole Attacks” 978-1-4799-3064-7/14/$31. 00©20 14 IEEE.

[7] Monika Y. Dangore, Mr Santosh S. Sambare, “Detecting A Overcoming Blackhole Attack In Aodv Protocol” 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEEDOI 10.1109/CUBE.2013.23

[8] Neha Sharma, Anand Singh Bisen, “Detection As Well As Removal of Blackhole Attack In MANET”, InternationalConference on Electrical, Electronics, and Optimization Techniques (ICEEOT) –2016, 978-1-4673-9939-5/16/$31.00 ©2016 IEEE.

[9] NishuKalia, Harpreet Sharma, “Detection of Multiple Black hole nodes attack in MANETby modifying AODV protocol” International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol.8 No.5 May 2016.

[10] Piyush Khemariya, Upendra Kumar Purohit & Umesh Barahdiya, “Performance Study of Improved Aodv against Black Hole Attack In Wireless Environment”, International Journal of Engineering Research &ModernEducation,2016

[11] Satria Mandala1, Abdul Hanan Abdullah, Abdul Samad Ismail, Habibollah Haron, Md. Asri Ngadi, Yahaya Coulibaly, “A Review of Blackhole Attack Mobile Ad hoc Network”, 2013 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-

BME)339 Bandung, November 7-8, 2013, 978-1-4799-1650-4/13 $31.00 © 2013.

[12] Sina Shahabi, Mahdieh Ghazvini1, Mehdi Bakhtiarian3, “A modified algorithm to improve security and performance of AODV protocol against black hole attack”, Springer Science+Business Media New York 2015

[13] Siddharth Dhama, Sandeep Sharma, Mukul Saini, “Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks”, 978-9-3805-4421-2/16/$31.00_c 2016 IEEE.

[14] T.Poongodi, M.Karthikeyan., “Localized Secure Routing Architecture against Cooperative Black Hole Attack in Mobile Ad Hoc Networks” Springer Science+Business Media New York 2016

[15] Vimal Kumar and Rakesh Kumar, “An Adaptive Approach for Detection of Black hole Attack in Mobile Adhoc Network”, International Conference on Intelligent Computing, Communication & Convergence, 1877-0509 © 2015 The Authors. Published by Elsevier B.V. Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015) doi: 10.1016/j.procs.2015.04.122