ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Black Hole Detection in MANET Using Modified AODV Protocol

Vinay Singh[1],Sanjay Kumar[2]

Student of M.Tech, Dept. of CSE, Faculty of Technology, Uttrakhand Technical University Campus, Uttrakhand India.[1]

Assistant Professor, Dept. of CSE.,Uttrakhand Technical University Campus, Uttrakhand India.[2]

ABSTRACT: This paper represents a method of detecting black-hole attack in mobile ad hoc networks, which are extremely vulnerable to attacks compared to conventional wired networks due to its mobility and broadcast in nature. In this case black-hole attacks can be easily deployed by the adversary. To defend against this attack, we use an approach to detect whether there is present a black hole and a path (routing) recovery protocol to set up a correct path for the real destination. Our method has a remarkable advantage that it can be implemented with a slight modification in basic AODV protocol without much affecting the efficiency, throughput and end to end delay. This is one of the efficient methods that can find out black hole node if any exist in the network.

KEYWORDS: Mobile ad hoc network, Black hole attack. Ad hoc on-demand distance vector routing protocol.

I. INTRODUCTION

Mobile ad hoc Network is a autonyms network consisting of nodes working cooperatively in ad hoc manner without a fixed network infrastructure. Each node in a MANET is mobile and is free to move in anywhere random fashion. The salient differentiating feature of MANET is the dual behaviour of each node, as it acts as both a router and a host. MANET (mobile ad hoc network) nodes include cell phones, laptops, PDA, GSM devices etc. typically having limited computation, communication and energy resources for their use.

A MANET is much more vulnerable to attacks as compared to a wired network due to the following factors:

- Nodes have limited energy due to which complex security solutions cannot be implemented.
- There is no central management node, which makes it difficult to ensure that all nodes participating in the network are friendly.

Transmission of routing and data packets is done in wireless medium, which is shared and generally unreliable to makes eavesdropping more likely. Even if the channel is reliable, the communication may still be unreliable due to the broadcast nature of MANETs.

- Mobility of nodes plays a very important role in the network, which makes routing even more challenging as the topology keeps changing regularly.

Attacks can be launched from all layers of network protocol stack but the routing layer attacks are the most damaging. Routing layer attacks can be categorized as outsider attacks and insider attacks. Outsider attacks are those in which the attacker has no authentication information about the control and data packets. These attacks can easily be dealt with using cryptography and authentication schemes. The most typical insider attacks on the routing layer are black hole, selective forwarding, hello flood, RREQ flood, sinkhole, denial of service, wormhole etc.

In this paper we proposed a mechanism that deal with the security breakdown due to the black hole attack, and can easily identified the black hole nodes and prevent it further.

I. The paper is arranged as follows. Section 2 Give an overview of the route discovery method of AODV protocol and its explanation contain the characteristics of a black hole attack. Section 3 contains the related works that are used in detection and prevention of black hole nodes within a network. Section 4 carries our proposed work that presents an approach for detection of black hole node in given topology. Methodology used for evaluation is done in section 5. We finish our work with future work in Section 6.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

II. BLACK HOLE ATTACK IN AODV

A Overview of Route Discovery Process In AODV

In case of reactive routing protocol, control packets (*Route Request* messages) are broadcast by source node in order to discover the optimal route path to the destination node in given topology. The destination sequence number is an important attribute in *Route Request* that is used to find out the freshness of a particular node. After receiving the *Route Request* packet (control message) a node have two option : i- Reply to the source node with a *Route Reply* packet if it contain the knowledge of the destination node or it contain intermediate node with 'fresh enough' route discovery information to destination node. OR

ii) Forwards the *Route Request* packet to its neighbour node if it is not containing the above-mentioned nodes detail.

An intermediate node is specified to have a fresh enough route nodes to the destination and the destination sequence number in its routing table record is greater than or equal to the destination sequence number of the *Route Request packets.* Once the source node finds the *Route Reply packet,* then it maintains a route path to the destination. The *Route Reply* message normally has the increased value for the *Route Request* packet destination sequence number, normally increased by one [1]. Fig.1 represents a route discovery process as described above.

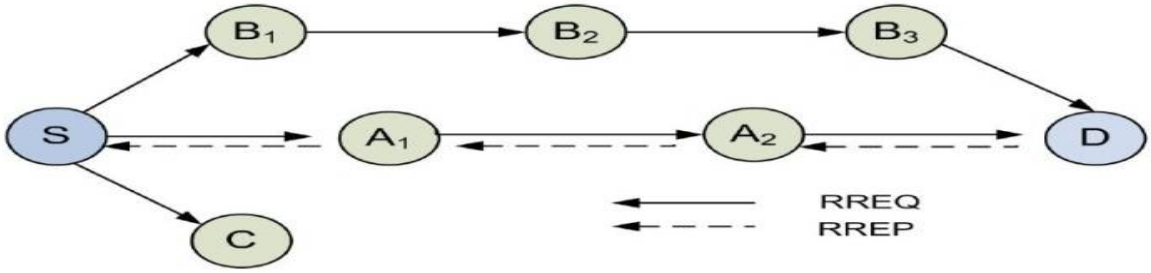

Fig.1. Route Discovery Process in AODV

A. Black Hole Attack

In on-demand routing protocol technique dropping control packets might be the more benefit to the selfish and malicious nodes. Once dropping the RREQ packets, a selfish node block to establish route path from passing through it and therefore it saves its energy for transmitting its own packets in network topology. Similarly a malicious node can drop RERR packets in order to protect the duration of use the broken routes path. As the result, Network throughput collapses sharply till no packet reaches its destination node. A precondition for a node to pitch a black hole attack is to be involved minimum in one routing path. In this way the malicious node applies the strategies mention below. As describe in Fig.2, S and D are the source and destination nodes and C is a malicious node. First of all the source node S broadcast RREQ packet to its just neighbours node and then upon receiving REEQ packet each neighbour node is assume to rebroadcast it if a route cache contain the entry towards the destination is not present. However the node C violates this condition and claims that it has a shortest path to the destination node and sends a RREP packet back toward node S. Hence if the RREP packet sent by node D or any honest intermediate neighbour node, which contain a fresh route path to D (destination) node, arrive the node S before the C's RREP packet then all works correctly. Else the source node S judge that the route passing through the node C is the shortest path, and then it starts transmitting data packet towards node C which drops them. Another method to find the attack can be described below: an intermediate node C take-offs the IP address of the destination node D, encourage the source node S to maintain the path towards C, instead of node D. To clarify that consider a network topology represent in Fig. 2, when the attacker node C got a RREQ packet it transmits a RREP packet to reply back to the node S claim that it is calculated destination node. So, it increases the Destination Sequence Number (Dst-Seq-Num) which is received in RREQ packet by a value larger than one as represent in Table 1.The node C (sets Dst-Seq-Num) to 55 rather than 41 to guarantee that the source node S chooses it as the final destination node. The method of this attacking strategy is similar to the previous one.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

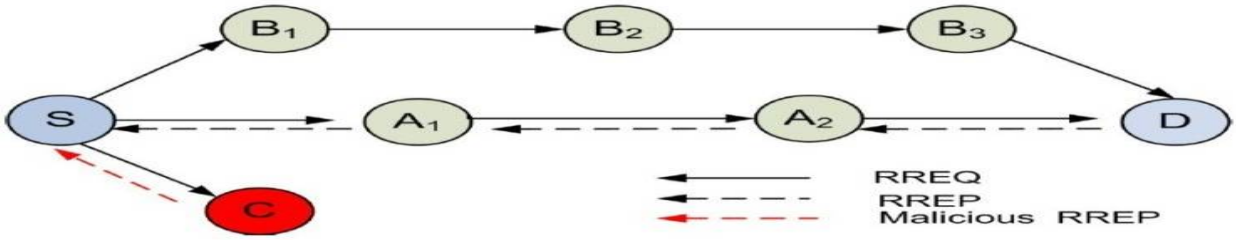

Fig.2. Black Hole Attack Condition in AODV

The Values of the different fields of RREQ and RREP packets forwarded by both authorised and malicious nodes: (I) The nodes *A*1 and *A*2 forwarded correctly the RREQ and RREP packets (II) the node *C* take-off the destination node's address (D) and augments illegitimately the DST-SEQ-NUM.

Sender	**RREQ**			**RREP**			
	S	A1	A2	D	A2	A1	C
IP-src	S	A1	A2	D	A2	A1	D
Dst-adr	D			S			S
	40			41			55

Table 1 The Values of the different fields of RREQ and RREP packets send.

II. RELATED WORK

Many approaches to detect the black hole attack and to defend the MANET from the attack have been proposed [2]-[8]. According to the algorithm by Deng et al. [2], every node crosses check with its next hop node on the route to the destination on receiving a RREP packet. If the next hop node does not have a path to the node that sent the RREP, then the node that sent the RREP is assume as malicious. This solution assumes that there exists at most one malicious node and thus cannot cover the case with two or more malicious nodes, which is quite possible in real situations. An algorithm presented in [3] claims to detect the black hole attack in a MANET which is based on relationships of a certain trust level among the nodes. However, in the real network, it is very difficult to set an appropriate value for the trust level. In the method [4], every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of the criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. This method only provides detection of a single black hole attacker and cannot detect a chain of malicious nodes which cooperate with each other. The method [5] provides a data learning scheme to detect a black hole attacker. In this scheme, every node has knowledge of the current value of SN by the exchange of route messages such as RREQ and RREP. If a node receives a RREP message with a SN that is much larger than a threshold plus the current SN value, this node will believe that the RREP message is generated by a malicious node. Obviously, this method depends on the value of the threshold and may lead to a high rate of misjudgement. The methods [6], [7] provide protection against black hole attacks using some special mechanisms such as PKI, threshold and trust level. Thus, the disadvantages of all these conventional methods are obvious. First of all, it is difficult to distribute public keys safely in a MANET, which will imply that such a method with PKI is not practical. In the second place, it is not easy to calculate and set an appropriate threshold value and trust level because of the features of the MANET. In addition, most of the above methods can detect only one black hole attacker and do not provide an effective mechanism to cover the situation with more than one attacker in the network. It should be noted that the second and the third disadvantages lead to large false negative rate due to the inability to detect attackers in some cases. Sun, Guan, Chen and Pooch [8] developed a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

neighbourhood based approach to detect as well as respond to the black hole attack. The core of their approach is outlined as follows.

1) *Concept*: Once the normal path discovery process is finished, the source node sends a special control packet to request the destination to send its current neighbor set.

2) *Neighbor set*: The *neighbor set* of a node is defined as all nodes that are within the nodes radio transmission range. They claim this metric provides a good "identity" of a node, that is if the two neighbor sets receive at the same time are different enough, it can be assume that they are generated by two different nodes. They verified their claim through the following two experiments:

i) They measured the neighbour set difference of one node at different time instants *t* and *t*+1 seconds under different moving speeds and network sizes. The result shows that there is not much change of a nodes neighbour set during a route discovery process.

ii) They examined the neighbor set difference of two different nodes at the same time, that is (({A"s neighbor set} U {B"s neighbor set}) – ({A"s neighbor set} ∩ {B"s neighbor set})). The result shows that the probability that node A"s neighbor set is the same as that of node B is very small.

3) *Detection*: After source node receives the neighbor set information, it analyses them by measuring the neighbor set difference. If the difference is larger than the predefined threshold values, the source node knows that current network has black hole attacks and responds to it accordingly [8] .

III. PROPOSED ALGORITHM

Step 1- Mobile ad hoc network (MANET) node initiate with sendhello ( ) call for checking the presence of its neighbors nodes.

Step 2- Neighbors node receive sendhello request and reply with recvhello packet. After that nodes maintain its link with neighbor nodes.

Step 3- After maintain the link with neighbors node source node initiate with broadcast RREQ packets to his neighbor nodes.

Step 4- RREQ packets are receive by the different types of node like destination node, fresh node, intermediate nodes.

Step 5- If(node = = Destination node) then Check
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
{ set rt_seqno = 0 and send updated RREP packet)
Else (send normal RREP packet)

Step 6- If (node = = Fresh node) then Check
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
{ set rt_seqno = 0 and send updated RREP packet)
Else (forword RREQ packet)

Step 7- If (node = = intermediate nodes) then check
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
{ set rt_seqno = 0 and send updated RREP packet)
Else (forword RREQ packet)

Step 8- After receiving RREP packet routing table update with maximum destination sequence number and minimum hop count value.
rt->rt_seqno = max(rt->rt_seqno, rp->rp_dst_seqno);
rt->rt_hop_count = min(rt->rt_hop_count, rp->rp_hop_count);

Step 9- After updating routing table source node unicast RREQ packets to the destination node, fresh node and intermediate nodes.

Step 10- If(node = = Destination node) then Check
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
{ send black hole RREP packet)
Else (send normal RREP packet)

Step 11- If (node = = Fresh node) then Check

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

```
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
    { send black hole RREP packet)
Else (forword RREQ packet )
```

Step 12- If (node = = intermediate nodes) then check

```
If (rt->rt_seqno >= 3 * NETWORK_DIAMETER + rq->rq_seqno)
    { send black hole RREP packet)
Else (forword RREQ packet )
```

Step 13- After receiving RREP packet routing table update his routing information by creating a path between source node to the destination node by avoiding black hole node in the routing path.

Step 14- Source node initiate forwarding the data packet to destination node avoiding black hole nodes in the path.

A. Control Packets Format Use in The Proposed Approach

Type	J	R	Reserved	Hop count
Broadcast_Id				
Dest_IP_Addr				
Dest_Sequence_No				
Source_IP_Addr				
Source_Sequence_No				

Table 3: RREQ Packet Format

Type: xx
J Join flag: set when source node wants to join multicast group.
R Repair flag: set when a node wants to initiate a repair to connect two previously disconnected portions of the multicast tree.
Reserved: Sent as 0, ignored on reception.
Hop Count: The number of hops from the Source IP Address to the node handling the request.
Broadcast ID: A sequence number identifying the particular RREQ uniquely when taken in conjunction with the source node's IP address.
Destination IP Address: The IP address of the destination for which a route is desired.
Destination Sequence Number: The last sequence number received in the past by the source for any route towards the destination.
Source IP Address: The IP address of the node which originated the Route Request.
Source Sequence Number: The current sequence number for route information generated by the source of the route request.

Type	L	Reserved	Hop count
Dest_IP_Addr			
Dest_Sequence_No			
Source_IP_Addr			
Lifetime			

Table 4: RREP packet format

Type: xx
L flag: If the 'L' bit is set, the message is a "hello" message and contains a list of the node's neighbors.
Reserved: Sent as 0, ignored on reception.
Destination IP Address: The IP address of the destination for which a route is supplied.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Destination Sequence Number: The destination sequence number associated to the route.
Source_IP_Addr: The IP address of the node which originated the Route Request.
Lifetime: The time for which nodes receiving the RREP consider the route to be valid.

IV. SIMULATION RESULTS

For the simulations, we use NS-2 (v-2.33) network simulator. NS-2 provides faithful implementations of the different network protocols. At the physical and data link layer, we used the IEEE 802.11 algorithm. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 0.2 Mbps. The connection pattern is generated using *cbrgen* and the mobility model is generated using *setdest utility*. *Setdest* generates random positions of the nodes in the network with specified mobility and pause time. The terrain area is 800m X 800m with number of nodes varying from minimum 10 to maximum 80 with chosen maximum speed up to from 10 m/s to 70 m/s. The simulation parameters are summarized in table 6. Each data point represents an average of ten runs. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols.

Parameter	**Value**
Simulator	Ns-2 (ver. 2.33)
Simulation Time	100 s
Number of nodes	10 to 60
Routing Protocol	AODV
Traffic Model	CBR
Pause Time	2 s
Mobility	10 – 70 m/s
Terrain area	800m × 800 m
Transmission Range	250 m
Type of Attack	Black hole attack

Table 6: Simulation Parameters

V. METRICS USED FOR SIMULATION

To analyse the performance of our solution, various contexts are created by varying the number of nodes and node mobility. The metrics used to evaluate the performance of these contexts are given below.
Packet Delivery Ratio: The ratio between number of packets received by the CBR sink at the final destination and the numbers of packets originated by the "application layer" CBR sources.
Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

A. *Simulation Result and Analysis*

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

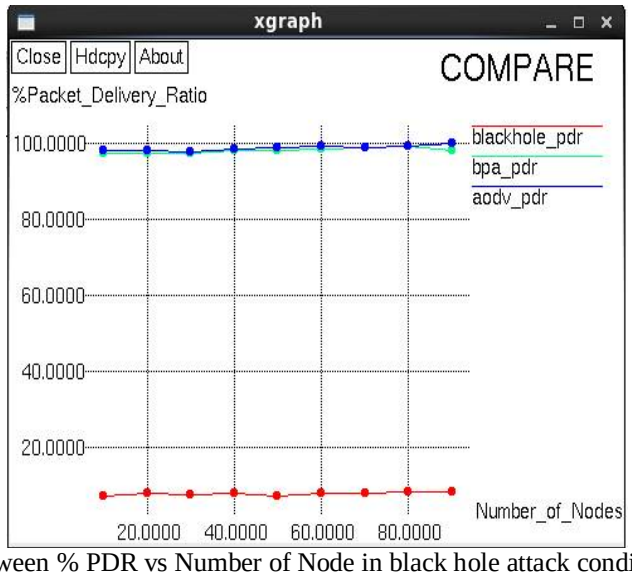

Fig. 3 (a) Comparison between % PDR vs Number of Node in black hole attack condition, standard AODV and proposed algo (bpa_pdr).

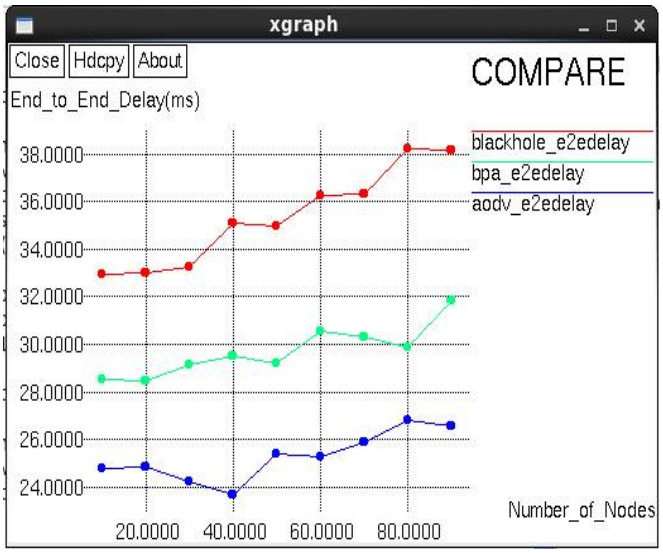

Fig. 3 (b) Comparison between End to End Delay vs Number Of Node in black hole attack condition, standard AODV and proposed algo(bpa_e2edelay).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

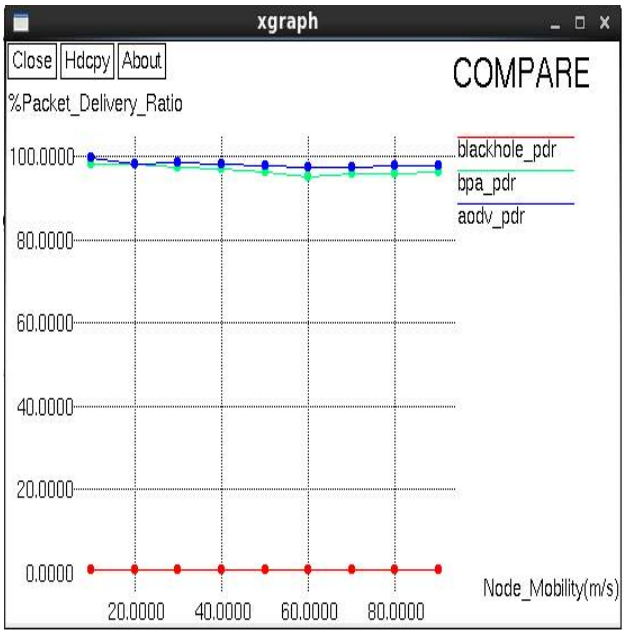

Fig. 3 (c) Comparison between % PDR vs Node Mobility(m/s) in black hole attack, standard AODV and proposed algo(bpa_pdr).

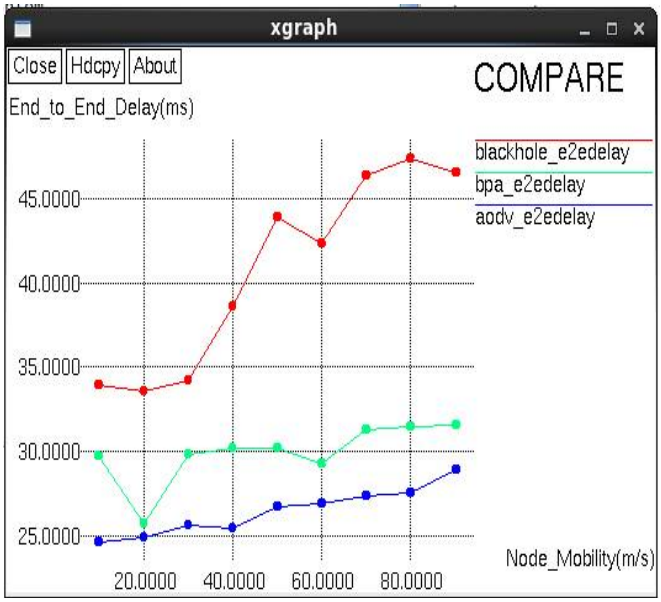

Fig. 3 (d) Comparison between End To End Delay vs Node Mobility (m/s) in black hole attack, standard AODV and proposed algo(bpa_e2edelay)

VI. Conclusion and Future Work

With the fact that the default AODV protocol is susceptible to the Black hole attacks, in this research exercise, we attempt at investigating the existing solutions for their viability. Having justified a need for further improvements, we propose an algorithm to counter the Black hole attack on the routing protocols in MANETs. From the experimental results, we conclude that the proposed solution achieves a very good rise in PDR with acceptable rise in end-to-end delay. Moreover, the proposed algorithm does not entail a much hidden overhead on either the intermediate nodes or

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

the destination nodes. We also emphasize that though the proposed algorithm is implemented and simulated for the AODV routing algorithm, it can also be further trivially extended for use by any other routing algorithms, as well. As part of our future endeavor, we aim to study the impact of varying pause time on the protocol efficiency. In addition, we would also attempt to investigate the impact of varying network size and node mobility on Normalized Routing Overhead in the protocol.

REFERENCES

[1] C.E.Perkins, E.M.B. Royer and S.R.Das, "Ad Hoc on Demand Distance Vector (AODV) routing", RFC 3561, July 2003.
[2] H. Deng, W. Li, and D. P. Agrawal: "Routing security in wireless ad hoc network". IEEE Communications Magazine, pages 70- 75, (2002)
[3] Latha Tamilselvan, V.Sankaranarayanan: "Prevention of Black Hole Attack in MANETs", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007)
[4] Mohanmmad AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004).
[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by Dynamic Learning Method", International Journal of Network Security, Vo1.5, PP.33S-346, (November, 2007)
[6] S, Ramaswamy, 1-1. Fu, M, Sreekantaradhya, 1. Dixon, and K, Nygard: "Prevention of cooperative black hole attack in wireless ad hoc networks", Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570-575. Las Vegas, USA, (2003).
[7] I. Rubin, A. Behzad, R. Zhang, H, Luo, and E. Caballero, Tbone: "A mobile-backbone protocol for ad hoc wireless networks", In Proceedings of IEEE Aerospace Conference, volume 6, pages 2727-2740, (2002).
[8] B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, *In Proc.* 5*th European Personal Mobile Communications Conference*, Glasgow, UK, April 2003.

BIOGRAPHY

Vinay Singh[1] is completed his M.Tech. Degree (2013-15) in the Computer Science & Engineering Department, College of **Faculty of Technology** Uttrakhand Technical University Campus, Uttrakhand. He completed B.Tech Degree in Information Technology (IT) in 2012 from IMS Engineering Collage, Ghaziabad (U.P.) India. Her research interests are Computer Networks.

Sanjay Kumar[2] is a Assistant Prof. in CSE Dept. Uttrakhand Technical University Campus Uttrakhand Indian .He is completed his master degree from IISc Bangalore & pursuing his Ph.D Degree from Uttrakhand Technical University. Her research interests are Computer Networks & Security.