An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks

Vrutik Shah
Research Scholar,
Department of Computer Science
Karpagam University, Coimbatore, India.

Nilesh Modi, PhD.
Professor and Head,
S.V. Institute of Computer Studies
Kadi, Gujarat, India.

ABSTRACT

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes that can has no fixed or predetermined topology, with mobile nodes and dynamic membership changes. A self-organizing network is a network that can automatically extend, change, configure and optimize its topology, coverage, capacity, cell size, and channel allocation, based on changes in location, traffic pattern, interference, and the situation or environment. MANETs due to complete autonomy of the member nodes and lack of any centralized infrastructure are particularly vulnerable to different types of attacks and security threats. Packet drop attack is one of them. In this paper mechanism has been proposed to detect and defend against packet drop attacks. Simulation has been done using ns 2.34 to evaluate the conventional AODV and proposed algorithm when packet drop attack is injected in network. The Result indicates that our proposed solution gives significant better performance then AODV in concern of Packet delivery ratio & Throughput with tolerable increase in routing overhead, End to End delay.

Keywords

Black hole attack, AODV, Routing Security, MANETs, Packet drop attacks

1. INTRODUCTION

This Wireless ad-hoc networks are self-possessed of sovereign nodes that are self- managed devoid of any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can effortlessly link or abscond the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes conversing with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV[1] (Ad-hoc On-Demand Distance Vector) in category of reactive protocol[1][2], DSR (Dynamic Source Routing) and DSDV (Destination- Sequenced Distance-Vector).Due to dynamic nature of MANETs, nodes may exhibit various types of misbehavior. Node misbehavior may be categorized into two broad types: Malicious behavior and Selfish behavior. : Malicious behavior intention is to attack and damage the network and Selfish behavior intention is to save power, memory and CPU cycle.

Malicious misbehavior can be of two types: Forwarding misbehavior and routing misbehavior. Forwarding misbehavior intention is to packet dropping, modification, fabrication, timing attack, silent route change etc. where ad Routing misbehavior intention is to route salvaging, dropping of error messages, fabrication of error messages, unusually frequent route updates, sleep deprivation, black hole, gray hole, wormhole etc.

Black hole attack is a routing misbehavior attack, In this attack attacker replies to each RREQ packet of route discovery with the greatest sequence number that it can. Then source node selects the greatest RREP sequence number and also selects the route contained in that RREP packet. Attacker tries to spoof ID of destination node and by using a high sequence number in RREP, flows all data packets to itself.

2. Black Hole Attack and Classification

A Black Hole attack [3][4][5] is a sort of denial of service where a malicious node Adversary selectively drops only data packets, but still participates in the routing protocol correctly using method to pull towards all packets by incorrectly declaring a fresh route to the destination and then absorb them without forwarding them to the destination. Cooperative Black hole means the malicious nodes act in a team [6][7]. When Source node initiates the transmission a data packets to a destination, as a process first sends the route discovery packet (RREQ) to all its neighbors' node. Malicious nodes is actively participates in routing process receives the RREQ as a consequences Black hole nodes have the characteristic of responding it immediately send out the RREP Packets. The RREP from the Black hole reaches the source node, well at the forefront of the other RREPs. Now on receiving the RREP from the Black hole node, the source initiates transmitting the data packets. On the reception of data packets, the Black hole node simply drops them, instead of forwarding to the destination. In an ad-hoc network that uses the AODV protocol, a black hole node perform as if to have brand new enough routes to all destinations requested by all the nodes and sop up the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes as per the nature of the algorithm. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without inspecting its routing table for a fresh route to a destination.

Mainly black hole attacks classify in two broader categories Single black hole attack and collaborative black hole attack

2.1 Classifications of Black hole attack

The method is indicating how malicious node hysterics in the data routes varies. Fig. 1 shows how Single black hole problem arises, here node "S" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all he data packet will be lost consumed or lost. Where Fig 2 shows collaborative black hole problem arise when multiple malicious node are performing in coordination with each other. from refers to one if its squad mates M2 as the next hop as depicted in fig 2 when S node initiate the route discovery process, as a result S will consider that S-4-M1-M2 is the secure route towards the destination. After getting packets from "M1" its team mate "M2" simply drops the packets.

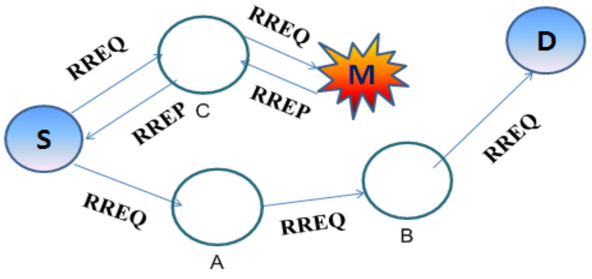


Fig 1 Single Black Hole

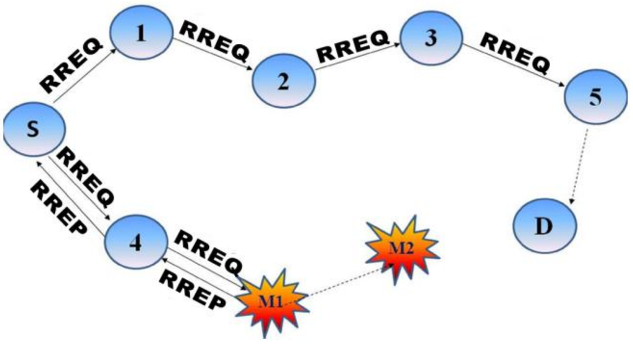


Fig 2 Collaborative Black Hole

However the case is packets are obsessive by M1 and packet drop activities of network is being compromised

3. Related Work

In this section, reviewed has been performed for the several solutions to black hole attacks. Several authors have suggested some techniques to detect and prevent multiple packet drop attack. Ming-yang at.al [8]discussed a mechanism called anti-black hole mechanism based upon abnormal difference between RREQs and RREPs transmitted from the node.Y.F.et.al[9] proposed Intruding Detection using anomaly detection(IDAD) based upon pre collected anomaly activities called audit data. In satoshi K et.al[10] have introduced anomalies detection scheme to detect black hole attack based upon dynamic training method.

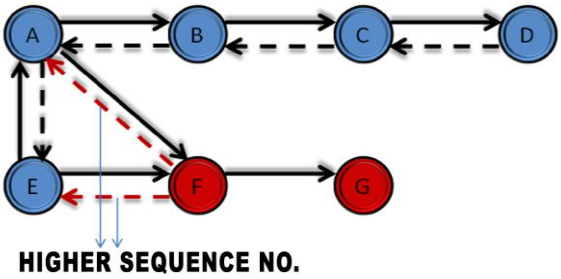
Authors	Techniques	Drawbacks
Deng H,Li W.and Agrawal[12]	Including the address of the next hop node in RREP Packet	The next hope node can response to the source node with untrustworthy routing information.
Al-shurman, M,YOO,S. and park	Source imitates ping towards the destination based upon pinging ack harmless route will be selected	Time delay and packet overhead due to ping and ack of pining.
Ramaswamy	Introducing DRI (Data Routing Information) and Cross Checking	Time Delay and network load is measurable higher.
Zhao Min,Zgou Jiju[11]	Hashing and MAC is used for authentication purpose.	counterfeit RREP with hash keys
N.Bhalaji,A.S hanmugan[3]	Route selection based upon trust value	Designed solution for DSR and Time delay is major drawback
Lalit Hirmal.et al.[13]	introducing checking sequence number of source node and opening route	Time Delay

4. Proposed Solutions

No node should be detected falsely malicious as well as no hole should be estimated as non- malicious node[15]. Keeping these two extremes in mind new fair algorithm is formed which is as bellow. In our algorithm source node will issue a inquisition message to detect malicious node only when it found no of packets received by destination is notably less than the no of packets actually sent.

We propose to modify AODV protocol by introducing two more tables which is maintained at each node. First one is observation table as described in Fig 2.2 maintain at each node. Data structure of this table is as (Source ID, To Node, No of. Packets Sent, No of Packets Received. Timestamp, status). Main purpose of this table is for calculating and monitoring packet drop activities based up on packet delivery fraction.

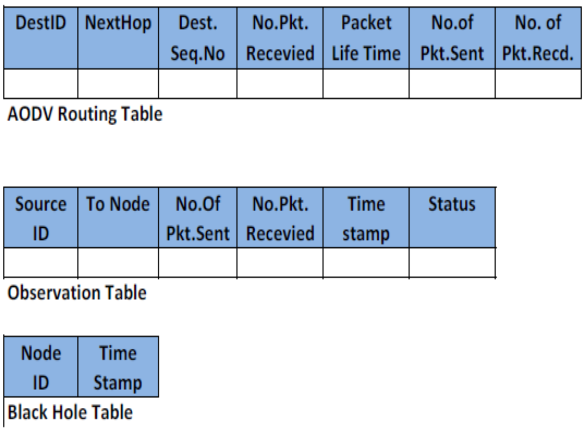
Another table is Black hole list table as shown in Fig 4 which keeps the track of nodes who have been declared and broadcast as a black hole node with timestamp information.



.

Fig 3: Network Topology

In Addition, it has been modified the routing table of the AODV by adding a new fields called Source Id,No of packets sent,no of packets drop. which will track updated information of each node in the routing table. the new proposed AODV routing table as shown if Fig 3 and 4. As a data structures {Desti.IP,Next Hope IP,Dest. Seq No, Path Life time, no of packets sent, no of packets received}.The Counter is managed based on the no of packets sent and no of packets drop, when ACK does not comes via next node within the allowable time limit the counter of no of packet drops incremented by 1. The rest working of AODV were kept as it is.



DestID	NextHop	Dest. Seq.No	No.Pkt. Recevied	Packet Life Time	No.of Pkt.Sent	No. of Pkt.Recd.

AODV Routing Table

Source ID	To Node	No.Of Pkt.Sent	No.Pkt. Recevied	Time stamp	Status

Observation Table

Node ID	Time Stamp

Black Hole Table

Fig 4: Data Structures of Routing Table

Whenever Source node wish to commence the black hole detection and removal process it broadcasts a query message to all its neighbors and set timers for the receipt of the result message from the monitoring nodes. The result comes as per the observation table which is managed by all nodes.

Let ∞ be the threshold probability of non malicious packets drop by each node then each monitor node check if (ni (1-∞)<=dataCount) then it is not a suspected node. If at the next node data loss is ∞ then the next node actually forwards ni (1-∞)*(1-∞) as a result total data loss via packet drop is (ni –ni (1-∞)N) where N is the total number of nodes in the route. Therefore,

$$\infty=1-(1-\infty)N$$

Case A:

In AODV the node that receives the RREP, checks the value of sequence number in routing table and accepts if it has a higher RREP seq_no than the one in routing table, Extra Method has been added to check whether the RREP seq_no is higher than the threshold value (A value that is updated dynamically in time intervals). As the value of RREP seq_no is found to be higher than the threshold value, the node is suspected to be malicious and added to the Observation List with the status field Su The threshold value is dynamically updated using the data collected in the time interval. If the initial training data were used it is implausible for the routers to adapt changes in environment. This case will detect black hole attack if it is in form of Single black hole attack.

```
Procedure :
Begin
If status filed is $S_u$ then
        [Check packet drop activities.]
        Packet drop ratio=packet sent/packet
drop.
                If packet drop ratio> $\infty$
                  Where $\infty = 1-(1-\infty)^N$

                    THEN
        ADD the Node ID in to Black hole list.
        Broadcast to all neighbors
        Go to End
 ELSE
        Go to End
 End
```

Case B:

In case of Collaborative black hole attack Case A will not be sufficient. Assume the observation table as per below.

Source ID	To Node	No. of PKT sent	No of PKT received	Time stamp	Status
A	C	50	30	101	NN
A	F	40	25	52	NN
C	A	30	20	74	NN
C	F	20	15	76	NN

Fig 5: Observation table of B

Source ID	To Node	No. of PKT sent	No of PKT received	Time stamp	Status
A	G	50	0	101	NN
A	G	40	25	52	SN
E	G	30	0	74	NN
A	E	20	10	78	SN

Fig 6: Observation table of F

Here Status filed indicates reliability of node. Let's assume all node are non malicious node F and node B As per the table F as depicted in fig 4.4 routing table have clear cut sign that if G is a next node irrelevant of source node the packet drop ratio is much more higher than 1-(1-∞)N. from the table it has been observed A-G and E-G two routes having highest packet drop ratio. it is clear cut indication that node G is malicious node with the pair with some another node. Now there will be possibility of A,E of F(node itself) might be paired with G. The Entire algorithm depended upon combination of Source node and Next node. Hence F's status Su will broadcast to all neighbors. The same case with table where B's observation table is depicted. In table tolerable packet drop ratio is there so B's status Nn will broadcast to all neighbors. Each node will tell reliability (Status Filed) of its by calculating the bellowed procedure.

```
Procedure:
Begin
If status filed is $S_u$ then
        [Check packet drop activities.]
Packet drop ratio=packet sent/packet drop.
                If packet drop ratio> $\infty$
                    Where $\infty =1-(1-\infty)^N$

                 THEN
                 [Calculate the status of this node]
  Where Source node might be anything and next node is same.
  Return status to all other node: Su
   Broadcast status to all neighbors.
        Go to End
 ELSE
        Go to End
   End
```

After receiving status of each node imitator or neighbor node will follow the procedure as per follows.In case of non receipt of status message wait until the tolerable time and threshold value. Due to network nature appropriate number of endeavor is required before classifying nodes as misbehaving. For this cause Every of the nodes are given MT(Maximum tolerance) number of opportunities before they are attributed as Black hole node in case of non receipt of status field.

```
Procedure:
Begin
If status filed is $S_u$ then
  THEN
        ADD the Node ID in to Black hole list.
        Broadcast to all neighbors
        Go to End
         ELSE
                Go to End
If status filed is $N_n$ then
                 THEN
Consider node as a Non malicious node
 ELSE
                Go to End

   End
```

In case of non receipt of status message wait until the tolerable time and threshold value. Due to network nature appropriate number of endeavor is required before classifying nodes as misbehaving. For this cause Every of the nodes are given MT(Maximum tolerance) number of opportunities before they are attributed as Black hole node in case of non receipt of status field..

5. Simulation Setup

In our evaluation, Comparison has been made for the performances of AODV and AODV-GAP using Network Simulator – 2.34 (NS-2) [14]. The details of simulation environment and the performance metrics are specified in the following subsections. About ten scenarios with different node positions, mobility and speed have been simulated and tested. The network parameters were measured with the presence of 0 to 10 malicious nodes. The network parameters Packet delivery fraction (PDF), End-to-End delay(E2Ed) and Network Routing Overload(NRL) and route discovery time (RDT) has been taken as evaluation parameters.

At the lower layer means physical and data link layer, it has been used IEEE 802.11 with Two Ray Ground radio propagation model. Consideration of the traffic of Constant Bit Rate (CBR) data packets over UDP at the transport layer in a of 1000m x 1000m with the total number of nodes varies as per scenarios forming the ad hoc network.

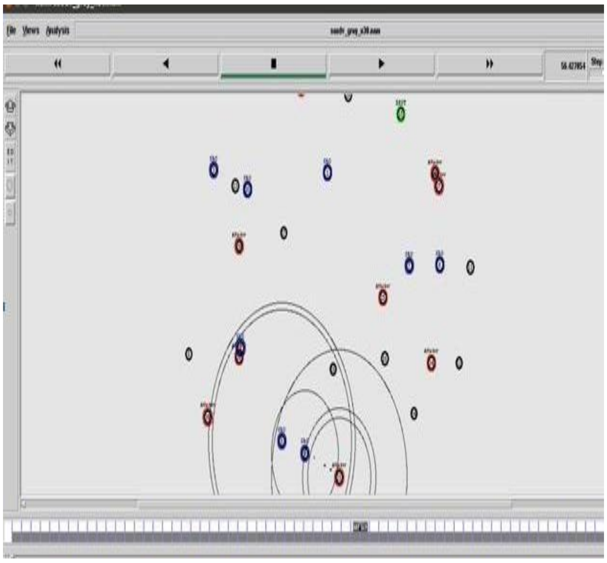


Fig 7: Simulation Topology in NS 2.34

Table 1:Simulation Parameters.

Simulation	Value
NS Version	2.34
AODV	NS2 default
BlackholeAodv	Customized variations in NS2 default AODV
No of Nodes	50
Traffic Type	UDP
Data Type	CBR
Data Packet Size	512 Bytes
Scenario	Random Motion models generated using "setdest"
MAC Protocol	IEEE 802.11
Radio Propagation	Two Way Ground
Simulation Time	100

Node Speed	50 m/s
Interface Queue	Queue/DropTail/PriQueue
Simulation Area	1000 x 1000 m
Animator	NAM
No of Attackers	10

6. Result Analysis

Ns-2 creates agents for the various network objects, including the router, CBR source, physical interface and so forth. Each of these agents log data which contains at least the minimal information in trace file .(tr file).

The calculation of the packet delivery fraction uses the ratio of the total number of CBR packets received in the network to the total number of CBR packets sent during the simulation. The Result shows that PDF is considerable better as compare to SBH (Single Black Hole) and CBH(Collaborative Black Hole Attack) as depicted in Fig 8.

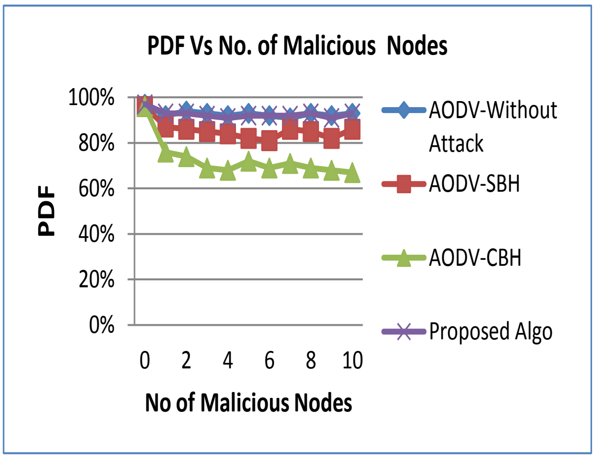


Fig 8 Graph of PDF vs No of Malicious node

The graph is showing our proposed solution is not attack proof but has high resilience as compared to AODV under attacks

Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gave the average end-to-end delay for the received packets The Results as shown in Fig 9 Avg End 2 End delay is slightly higher delay than to AODV. This is consistent if the numbers of nodes are less. However with the increase in number of node an increase in the delay of AODV occurs.

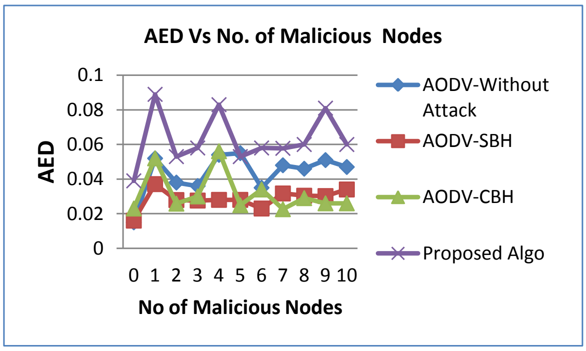


Fig 9 Graph of AED vs No of Malicious node

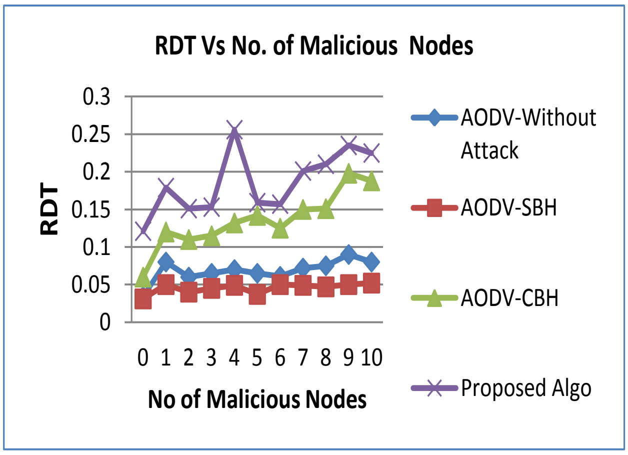


Fig 10 Graph of RDT vs No of Malicious node

The measurement has been taken for Route Discovery Time (RDT) as depicted in fig 10 because of Routing table calculations RDT is toraable higher than AODV. In case of attack the performance of RDT is slightly compromised in concern of our proposed algorithm.

Another parameter is Network Load (NRL) is more or less same as compare with AODV normal and AODV with attack. Variation comes because of Status field whenever Source node queries related to detect black hole attack in the network. As per our proposed solution source node will initiate query that time extra packets transmission has to be performed. Due to that transmission NRL is slightly higher than normal AODV protocol.

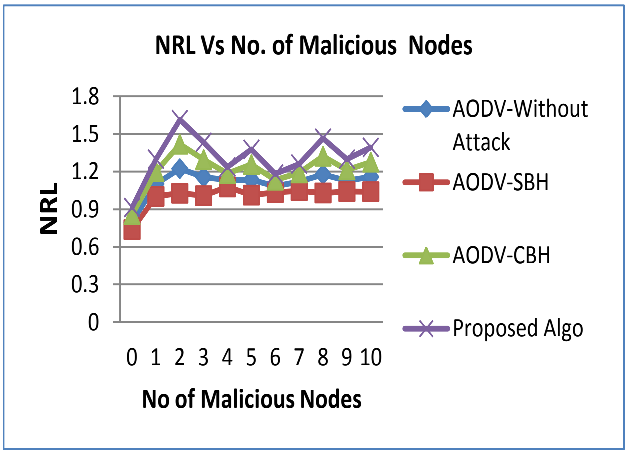


Fig 11 Graph of NRL vs No of node

7. Conclusions

In this Paper, it has been analyzed effect of the Black Hole in an AODV Network with Single Black hole attack and collaborative black hole attack. For this purpose, In this simulation implementation has been done of an AODV protocol that behaves as Black Hole in NS-2. Simulation has been done simulated several scenarios with nodes ranging from 10 to 60 that use AODV protocol and also simulated the same scenarios after introducing ten black Hole Node into the network. Moreover, implementation has been done for a proposed solution that attempted to mitigating the black Hole effects in NS-2 and simulated the solution using the same scenarios. The simulation results are analyzed below.

Having simulated the black Hole Attack, we saw that the packet loss is increased in the ad-hoc network due to nature of attack.. Its also affects the overall network connectivity and the data loss could show the existence of the black Hole Attack in the network. If the number of black Hole Nodes is increased then the data loss would also be expected to increase. These two results show that our solution mitigating the black Hole effects efficiently in stipulations of PDF, AED, Routin Discovery Time and Routing overhead

8. REFERENCES

[1] C. E. Perkins, E. M. B. Royer and S. R. Das, " Ad-hoc On-Demand Distance Vector (AODV) Routing," Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, Feb. 2003.

[2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; , "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE , vol.11, no.1, pp. 38- 47, Feb 2004.

[3] N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[4] Raja Mahmood, R.A.; Khan, A.I.; , "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on , vol., no., pp.1-6, 18-20 Nov. 2007

[5] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[6] Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes" International Journal of Advanced Computer Sciences and Applications, Vol: 2 Issue: 8 Pages: 97-102, 2011.

[7] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.

[8] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[9] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vo l.5, No .3, P P.338–346, Nov. 2007.

[11] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[12] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[13] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[14] F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf

[15] Shah Vrutik,Modi N,Patani A."aodvgap-an acknowledgment based approach to mitigate selective forwarding attacks in manet" in international journal of computer engineering & technology (IJCET) ISSN 0976 – 6367(P) ISSN 0976 – 6375(Online) Volume 3, Issue 2, July- September (2012), pp. 458-469

[16] Osathanunkul, K.; Ning Zhang; , "A countermeasure to black hole attacks in mobile ad hoc networks," Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on, vol., no., pp.508-513, 11-13 April 2011.

[17] Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[18] L. Eschenauer, V. Gligor, and J. Baras. On Trust Establishment in Mobile Ad-hoc Networks. Technical Report MS 2002-10, Institute for Systems Research, University of Maryland, 2002.

[19] X. Li, M. Lyu, and J. Liu. A Trust Model Based Routing Protocol for Secure Ad hoc Networks. In Proceedings of the Aerospace Conference, pages 1286–1295, March 2004.

[20] T. Ghosh, N. Pissinou, and K. Makki. Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad hoc Networks. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), pages 224–231, Washington, DC, USA, 2004. IEEE Computer Society.

[21] N. Pissinou, T. Ghosh, and K. Makki. Collaborative Trust-Based Secure Routing in Multihop Ad hoc Networks. In NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, pages 1446–1451, 2004.

AUTHOR'S PROFILE

Vrutik Shah was born in India in 1980; He is a Ph.D scholar in Computer Science He received his MCA degree in Computer Science and Application. His research interest includes security in wireless networks, Ad- Hoc networks, and network protocols. He is working with IITE Ahmedabad.This work is a part of Ph.D Program from KARPAGAM University, Coimbatore, INDIA.

Dr. Nilesh Modi received his MCA from Hemchandracharya North Gujarat University in 2002, and his Ph.D. in computer science from Bhavnagar University in 2006. He is currently a Professor and Head of Department at SVICS,Kadi,