Quantitative Detection of AODV against Black Hole and Worm Hole Attacks in MANET

Neha Malhotra
Lecturer
Lovely Professional University
Phagwara

Rachit Garg
Associate Professor
Lovely Professional University
Phagwara

Rajiv Mahajan
Professor
Global Institute of management and Emerging Technologies,
Amritsar

ABSTRACT

Security is very essential in both wired and wireless network communication. An ad hoc network is a collection of number of wireless computers having dynamically changing topology due to which the security issues are more in case of wireless networks. In this paper the aim is to provide a quantitative analysis of all the security challenges that effect the performance of MANET protocols by analyzing the effects on AODV (Ad hoc on demand vector routing protocol). The current paper willexplain the concern of black hole, worm holeattacks and presents the impact on AODV routing protocol.

Keywords
Ad hoc network, protocol, AODV, black hole, worm hole, wireless network, packets

1. INTRODUCTION

Mobile and ad hoc networks exhibits dynamic topology which leads to the dynamic behavior of all the nodes present in the network at that time. Security is one of the major concerns in dynamic nodes where the location of the nodes is not fixed at all. Wireless networks transmits radio waves in the air which act as medium to transfer data instead of having any physical cabling among the nodes. Mobile ad hoc network is based upon the mobile hosts and each host is used for maintaining information about its neighbors and to send and receive data in the network. Now based on the routing information that each node maintains further classify them into different types of protocols namely Reactive, Pro-active and Hybrid protocols. Now all these protocols are vulnerable to different types of attacks that may occur in the network. These attacks may decrease the performance of the network or it may also decrease the efficiency of the nodes to connect to each other in a dynamic environment.The use of wireless networks has become more and more familiar these days. A Mobile Ad-hoc Wireless Network (MANET) which is also known as collection of various autonomous mobile nodes and other nodes that can communicate with each other by forming a multi-hop network, and by maintaining connectivity in a decentralized manner. It consists of mobile nodes which communicate with each other using wireless link. The nodes in a MANET can be laptop, Mobile phone, PDAs, or any other device that has been capable of transmitting and receiving data (signals). There are different types of routing attacks availableand these are as follows:

a. **Attacks using Impersonation**
b. **Attack using Fabrication**
c. **Attack using Modification**
d. **And denial of service**

Attack using Fabrication
In this type of attacks [1], an intruder will generate false routing information which can be in the form of false route error messages (RERR), another will be routing updates that may disturb the network operations or consume node resources. Some of the fabrication types of attacks are Black hole attack, worm hole attack and gray hole attack.

The current paper discusseson the use of different attacks on different protocolthat falls into the category of reactive routing protocol such as Ad hoc On-demand Distance Vector (AODV) routing protocol. As these falls into two basic categories of Reactive and Proactive protocols. AODV is reactive protocol[18]. Ad hoc on demand Distance vector routing protocol is vulnerable to most of the security attacks and it needs more consideration to be taken care of.

The effect of two major types of attacks namely Black Hole Attack and Worm Hole Attack has been detected and presented the preventive measures against these attacks in AODV.

2. LITERATURE REVIEW

Agrawal, D.P [1] has proposed one of the solution for the prevention of black hole attack in the network. The solution works by modifying the AODV protocol. The solution says that if each and every intermediate node keep the address of the next hop node in it’s receive reply packets (RREP) then the black holes can be detected easily in the network.

Kute D.S., Patil A.S., Pardakhe N.V. and Kathole A.B[5] has discussed different types of security attacks that can affect the performance of all the routing protocols.

Irshad Ullah and Shoaib Ur Rehman[4]also gave his contribution to discuss the effect of black Hole attack on different reactive and proactive protocols.

Neha , Tarun Gupta, Rachit Garg [9] has already discussed the functionality of all the multicast routing protocols. It has been clearly mentioned that there are certain security risks in each and every protocol and those risks two security attacks namely black hole and worm hole attacks on AODV protocol will be discussed in this paper along with their detective and preventive measures.

M.Yoo, S. and Park, S [8] proposed the solutions against black hole attacks in the network. Each node in the network needs to maintain at least two tables which will be used to store the sequence numbers of every last packet sent to each and every node and also last packet received from every sender respectively and afterwards there is a need to compare the last sequence number which will be extracted from the route reply packet (RREP) at source node. If it matches the data will be forwarded to that route but if it will not match an alarm message will be broadcasted to intimate about the malicious node in the network.

Tamilselvan, L., Sankaranarayanan, V. [15] has also discussed that the source node is going to wait for other replies with next hop information without sending the data packets to the destination. Once it receives the first receive reply packet (RREP) it sets the timer in the “TimerExpiredTable‟, to collect the RREP‟s from different nodes.

Latha Tamilselvan, V. Sankaranarayanan, [6] has also proposed a solution which also deals with the modification of the AODV protocol, by which we can avoid the effect of cooperative multiple black holes in the network. This approach deals with the usage of the Fidelity table in which every participating node will be provided with a given a fidelity level which will provide reliability to that node. After this we will check the fidelity level of each and every node. The level 0 indicates that the node is malicious and needs to be eliminated from the network. We can update the fidelity levels of all the nodes based upon their trust value in the network.

3. AODV AND ITS SECURITY RISKS

AODV (Ad hoc on demand Distance vector) is suitable for both unicast and multicast routing. In this protocol a user can also append the sequence numbers which are basically used to check the staleness and freshness of the routes. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.

3.1. PROTOCOL OVERVIEW

AODV uses RREQ and RREP messages as it used this concept in unicast routing also and now same is used in multicast also. The concept is to use the sequence number concept for every route in unicast routing but in multicast routing, a node is selected to generate and update the multicast group sequence number and this node will be termed as “multicast group leader”.

```
Algorithm At Source Node: AODV

// RREP (receive reply), DSeq (Destination sequence
number), RT (Routing Table), SSeq (Source Sequence
Number, Packet P)
    1.  Destination Node sends RREP (Packet P)
            a.  if('P' has an entry in 'RT') then
            b.  select 'DSeq' from 'RT'
            c.  if(P.DSeq> DSeq)then
            d.  update 'P' in 'RT' and
            e.  unicast data packets to the route
                specified in RREP
            f.  endif
            g.  elseif (P.DSeq<DSeq) then
            h.  Discard the RREP packet
            i.  end
        endif
    2.  else
    3.  if(P.DSeq >= SSeq) then
    4.  Enter the value of 'P' in 'RT'
        end
    5.  else
    6.  Discard the RREP packet
        end
    7.  End
```

Algorithm 1: Functionality of AODV at source node

In the algorithm [19] described above for each and every Receive reply (RREP) message received, the source node available in the network would first check whether it has an entry for the destination in the route table or not. If the entry exists and it will find one then the source node would check whether the destination sequence number in the incoming control message is higher than one it sent last in the RREQ message or not. If the destination sequence number is higher, the source node will update its routing table with the new RREP control message; otherwise the RREP control message will be discarded. In Route Maintenance phase, if a node finds a link break or failure, then it sends RERR message to all the nodes that uses the route.

4. BLACK HOLE ATTACK AND ITS IMPACT ON AODV

Black hole attack [2] is one of the major security threat available in which all the traffic means all the routes and its related information is redirected to such a specific node that in actual does not exist in the network. **It completely resemble to black hole that is existing in universe in which things disappear.**It is a kind of denial of service in which a malicious node can attract all packets towards itself and then that node absorb all the packets without forwarding them to the destination.The malicious node advertises itself as it is having the shortest path available to the node whose packets it wants to intercept.

Black hole node is having the property of replying first to the request of source node. So it will respond first when any source node sends its RREQ (Route request) message.In networking terms black hole are the places where the incoming traffic is discarded by the node. These black holes are invisible and that is the main reason why they used to drop the packets that are forwarding to them by the source node.There are different forms of black holes available; some of them are as listed below:

a. **Dead Address:** one form of black hole is very common and that is a host machine that is specified by an IP Address but the machine is not running or it is an IP Address to which no host has been assigned.
b. **Firewalls and Stealth Ports:** some of the fireless have been configured to discard the packets coming to them which results in their becoming of black holes.
c. **Black Hole email addresses**: a black hole email message is the one to which all messages sent can be automatically deleted.

4.1. Impact on AODV

AODV [7] protocol suffers from two types of black hole attacks which can be termed as Internal and External Black Hole Attack.Internal Black Hole Attack is the one that has already been discussed before in which the malicious node exists within the network between source and destination and accepts the incoming messages from the source and then discard the packets.External Black Hole Attack is the one which exists outside the network.

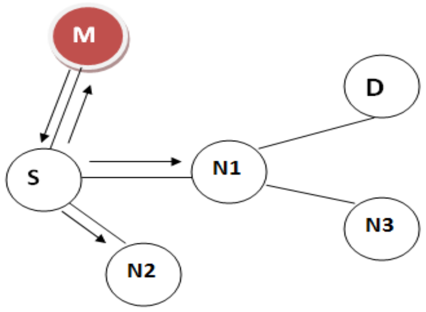

Fig1: External Black Hole Attack

Fig1. Explain an external black hole attack in AODV protocol, here the node M is being attacked by the Black Hole and becomes Malicious Node then it enters into the network by listening to the conversation between Source (S) and Destination (D).Here in this **Fig2**. Black hole attack with two black holes has been depicted in AODV protocol in which the source node is denoted by S and destination node is denoted by D. Nodes N1 to N3 act as the intermediate nodes.

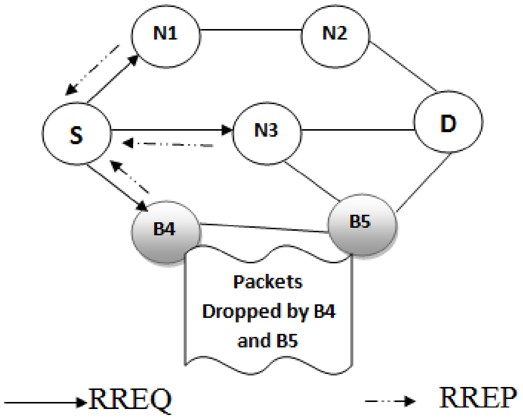

Fig 2: Black Hole Attack with two Black Holes

In Fig2: B4 and B5 act as two malicious nodes also known as cooperative black holes in the network.When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes (black holes) being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the destination or B1 forwards all the data to B2. B2 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

4.2. Algorithm to detect the presence of Black Hole in the Network

In this method [10], a certified token will be given to each and every node in the network which ensures the trustworthiness of the node in the network. All the nodes in the network must contain the token and the node which is not having any token will be considered as malicious node (Black Hole) and will be discarded from the network. Each node in the network will take care of all of its neighboring nodes by following a maintenance phase in which they have to check continuously about the token state of their neighbors and if any node will suspect any unfair thing in its neighboring node, then the issue will be reported to the source node 'S' and the suspected node if found to be malicious will be discarded from the network.In the solution provided, the presence of black hole in the network can be detected [14]in the following way:

Step1: The source node (S) which wants to send data to destination node (D) will first send a 'Hello' packet to all the neighboring nodes in the network. As depicted in Fig3 where the source node 'S' is broadcasting 'Hello' packet.

Step2: Upon receiving the 'Hello' packet all of the nodes which exist in the network as its neighbors will respond back with the acknowledgment along with all the routing information necessary to establish a route.

Step 3: Each and every node will respond back to the source node with its **'Token serial number'.**

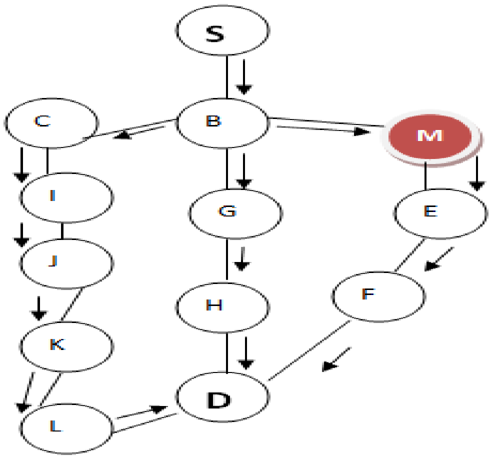

Fig3: Hello packet from source to all other nodes

Step 4: Source node will verify all the nodes based upon their 'Token serial number'

Step5: The nodes which will acknowledge to the source node will help in the establishment of the active routes from where the transmission can take place.

Step4: The source node will then check the availability of all the shortest routes available.

Step 5: Then the Destination node send the RREP through one of the shortest path. RREP must validate the Token serial number upon visiting each and every node in that path.

Step 6: If a match occurs with the token serial number that RREP had with the token serial number that node had, only then the RREP will travel through that path otherwise if there will be a mismatch the node considered to be malicious node (Black Hole) in the network.

Step 7: If there will be any malicious node available in that route then it will not send the RREP packet to next node which is depicted in Fig4 shown below and, then the transfer will be terminated and the destination node will resend the information through the next shortest possible route.

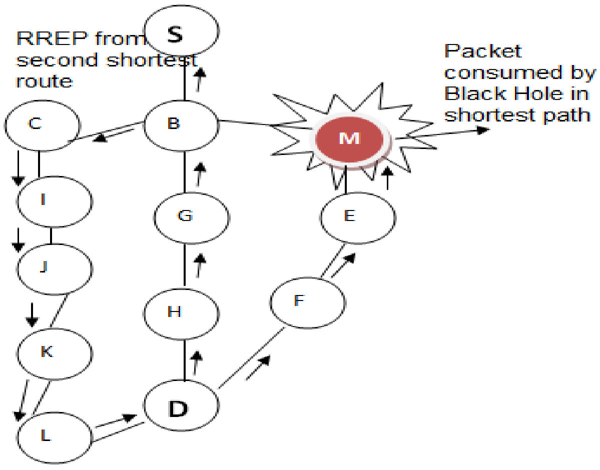
RREP from second shortest route
S
Packet consumed by Black Hole in shortest path
C
B
M
I
G
E
J
H
F
K
D
L

Fig4: Black hole detected on first shortest path

```
Algorithm: To discover different routes the algorithm is as follows:
//S=Source node, N= Neighboring nodes, D=Destination node, RREQ=Route request, RREP=Route receive reply, Token serial number= TN
    1. Send a 'Hello' packet as a 'RREQ' to 'N' in search of "D"
    2. The entire 'N' will append its'TN' in the header of RREQ.
    3. This 'TN' will be validated at each and every node.
    4. Each 'N' will further broadcast RREQ to its neighbors
    5. Upon reaching at 'D', transmission of 'RREQ' stops
    6. 'D' will extract the routing information from RREQ received.
    7. From the first RREQ received , 'D' will send RREP to 'S' through that route only
    8. Each node in that route will validate its 'TN' with the one in RREP header
    9. If 'TN' matches
        a. There will be no black hole and the routing continues
        b. Transmission continues from this path only
    10. Else
        a. Node is malicious and can be considered as black hole
        b. Route Terminates
```

Algorithm 2: To detect Black Hole in the Network

5. Worm Hole Attack and its impact on AODV

Wormhole attack**[3]** is a kind of attack in which two attackers are going to place themselves strategically in the network. Then the attackers will keep on hearing the network and will record the wireless data.

The attackers will establish a link between them which is known as **"WORMHOLE LINK"** and then they advertise this link in the entire network [11] as one of the shortest route available.

Impact on AODV

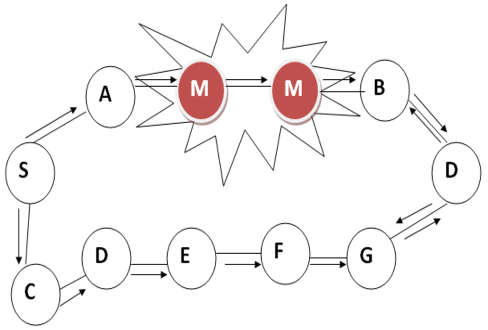

Fig 5: Worm Hole in AODV

In Fig3: when the source node (S) is going to send data to destination node (D) it will forward the Route request (RREQ) packet to all of its neighbors such as A and C. Then A and C will further send the RREQ to its neighbors and M being the malicious nodes connect themselves with A and get the RREQ from A and then places it on the high speed data bus and then send it to B which further send it to D through the route **S-A-M-M-B-D**and destination node D will get the RREQ from another route also which is **S-C-D-E-F-G-D.** So it is obvious that destination D will send the route reply packet (RREP) only to the shortest route available which will be the one with the malicious nodes.

In this way the network gets damaged by the malicious nodes through the wormhole tunnel established by the malicious nodes.

5.1. Detectionof Worm Hole in AODV

Pratik Singh, Aman Dutta,[12] has proposed a solution for the detection of worm hole in the network. According to the solution the nodes in the network can send the RREP in respond to RREQ within a stipulated period of time. If the response from the other node will exceed that time limit it will detect a worm hole presence in the network. As according to author, there should be one Worm hole presence timer (WPT) and if to send the RREP the nodes will take more than WPT/2 time, and then the worm hole can be expected in the network.

Reshmi Maulik and Nabendu Chaki [13] also suggested one feasibility in the source node that it can have all the information related to the nodes in the network and to the nodes which are further sending RREQ to its neighbors.

In the suggested solution, worm hole attack can be detected in the network in the following manner also:

a. As it has been already discussed that the malicious nodes send the data on a high speed bus that's why a shortest route is maintained, so it clear that a large and spontaneous decrease in the route length can be used as one of the measure to detect worm hole in the network.

b. **Strength of the malicious node:** It is defined as the amount of traffic which got attracted to the malicious link which was advertised by the colluding nodes.

c. **Distance between Actual Path and Malicious Path:** Larger is the difference between the actual path and the advertised path more will be the anomalies that can be observed in the network.

d. **Robustness of the wormhole:** The robustness of a wormhole in the network refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network.

e. **Packet Delivery Ratio** can also be considered as one of the metric in detecting worm hole attack.

6. Summary

Type of Attack	**Detection**	**Protocol**
Black Hole Attack	Each and every intermediate node keep the address of the next hop node in its receive reply packets (RREP) then the black holes can be detected easily in the network.	AODV
Black Hole Attack	By maintaining fidelity table which specifies the fidelity level of all the nodes that depends upon the trustworthiness behavior of the node in the network	AODV
Black Hole Attack	By maintaining the timer expired table which consist of the timestamp delay in sending the RREP packets of each and every node in the network.	AODV
Black Hole Attack	Proposed algorithm which will validate the nodes based upon their token serial number. If it validates then the route is not having any black hole but if it is not having then the route consists of malicious nodes in the network.	AODV
Worm Hole Attack	Each node will send its Route Request (RRREQ) messages to destination by viewing their neighboring table. If the source node will not receive back the RREP message within a stipulated amount of time, it will automatically detect the presence of wormhole in the network	AODV
Worm Hole Attack	A large and spontaneous decrease in the route length can be used as one of the measure to detect worm hole in the network.	AODV
Worm Hole Attack	Moreover there will be one feasibility in the source node that it can have all the information related to the nodes in the network and to the nodes which are further sending RREQ to its neighbors.	AODV
Worm Hole Attack	Also with the available advertised path information in the network, if in any case the end-to-end path delay for that path cannot be explained by the sum of hop delays of the hops present on that advertised path then also the existence of wormhole in the network can be suspected.	AODV

Table1: Summary of all the detective and preventive measures of black hole and worm hole attack

7. Conclusion

This paper presented has amalgamated a lot of work done in the field of mobile and ad hoc network to detect and prevent two major attacks on AODV protocol namely black hole attack and worm hole attack.There are many authors who already discussed various methods to detect black holes in the network. A method can be discovered which can be used to detect the presence of black holes in the network based upon the validation of the token serial number. Along with detection parameter an additional parameter such as "timer" can also be used with each and every RREQ and RREP packets and keep the entry of the every visit of these packets to each and every node. The timer table will help a lot in detecting the node which is consuming the packets or which is not sending the packets to other nodes and will be helpful to detect the presence of black holes in the network.

8. Future Work

A lot of work has been done on the detection and prevention of black hole attack on specifically AODV(Ad hoc on demand Routing Protocol) but a very less work has been done on all other protocols namely DSDV, TORA etc. A lot of research can be made on the detection and prevention of black hole and worm hole on other mobile ad hoc routing protocols. Secondly, efforts can be made to design a protocol that is completely secure from black hole and worm hole attack.Moreover we can also study the effect of cooperative black holes in the network since the proposed solution is dealing with only one black hole node in the network.

9. References

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

[2] Bala, A., Bansal, M., and Singh, J. 2010. Performance Analysis of MANET under Blackhole Attack. First International Conference on Networks and Communications 141-145.

[3] Bintu Kadhiwala and Harsh Shah, " Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks" International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887)

[4] IrshadUllah and Shoaib Ur Rehman, Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols

[5] Kute D.S., Patil A.S., Pardakhe N.V. and Kathole A.B., International Journal of Wireless Communication

[6] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008

[7] Madhusudhananagakumar KS, G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET"International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

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

[9] Neha , Tarun Gupta, Rachit Garg," A Quantitative survey of mobile and ad hoc multicast routing protocols" International Journal of Emerging Technology and Advanced Engineering

[10] 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.

[11] Nidhi Nigam and Vishal Sharma, "A Novel Approach for Wormhole Detection in MANET"International Journal of Computer Applications (0975 – 8887) Volume 63– No.7, February 2013

[12] Pratik Singh, Aman Dutta, Flood Tolerant AODV Protocol (FT-AODV),International Journal of Computer Applications (0975 – 8887) Volume 53– No.6, September 2012

[13] Reshmi Maulik1 and Nabendu Chaki2, " A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279

[14] Sharma, N., and Sharma, A. 2012. The Black-hole node attack in MANET. Second International Conference on Advanced Computing and Communication Technologies 546-550.

[15] Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[16] Thind.T., & Garg.R., "Mobile distributed system: concepts, issues, challenges", National Conference on Emerging Trends in Computer Science & Engineering (ETCSE-2012) , 11th-12th May,2012, Guru Kashi University, Talwandi Sabo, Punjab, India

[17] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009

[18] Y.-C. Hu, A. Perrig, D.B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, 11(1-2), pp. 21–38, 2005.

[19] NitalMistry, Devesh C Jinwala, Member, IAENG, MukeshZaveri"Improving AODV Protocol against Blackhole Attacks"