International Journal of Computer and Communication Technology

Volume 3 | Issue 4 Article 14

October 2012

# A counter measure to Black hole attack on AODVbased Mobile Ad-Hoc Networks

Subash Chandra Mandhata
*Krupajal Engineering College, DRIEMS, Cuttack Bhubaneswar*, smandhata@gmail.com

S .N. Patro
*Dhaneswar Rath Institute of Engineering and Management Studies Tangi, Cuttack, Orissa-754022, India*, snpatro@gmail.com

Recommended Citation
Mandhata, Subash Chandra and Patro, S .N. (2012) "A counter measure to Black hole attack on AODVbased Mobile Ad-Hoc Networks," *International Journal of Computer and Communication Technology*: Vol. 3 : Iss. 4 , Article 14.
Available at: https://www.interscience.in/ijcct/vol3/iss4/14

# A counter measure to Black hole attack on AODV-based Mobile Ad-Hoc Networks

**Subash Chandra Mandhata , Dr.Surya Narayan Patro**
*Krupajal Engineering College, DRIEMS, Cuttack*
*Bhubaneswar,*
*Email-smandhata@gmail.com, snpatro@gmail.com*

***Abstract: Security is a major threat and essential requirement for mobile Ad Hoc network. Due to its inherent characteristics, it has many consequent challenges, which needs to be taken care of. In this paper we analyse the black hole attack in MANET using AODV as its routing protocol. Black hole is a type of routing attack where a malicious node impersonates a destination node by sending deceived route reply packet to a source node that initiates a route discovery process. By doing this, the malicious node can deprive the traffic from the source node. We propose a solution that makes a modification in existing AODV routing protocol.***

***Keywords: Ad hoc Networks, Routing Protocols, AODV, Black Hole Attack***

## 1. Introduction

Needless to say a mobile ad-hoc network ( MANET ) is an autonomous system of mobile nodes connected by wireless links. Two nodes can communicate with each other when they are within the transmission range but need cooperation of intermediate nodes by forwarding packets when they are multi hop away from each other. Although mobile Ad-Hoc networks have many advantages over wired network, it also suffers from many non trivial challenges to the security design as they are vulnerable than wired networks[1]. The complexity of security issues arises due to the factors such as i) open network architecture, ii) highly dynamic network topology caused by node mobility, node joining and leaving the network, iii) limited resource constraints[2] such as processing power, storage , battery power of the nodes, iv) lack of centralized management. In contrast to the wired network , each node in Ad Hoc network acts as a host as well as a router that forwards the incoming data packet to its neighbor node towards the destination. Routing protocols play an imperative role in creation and maintenance of virtual set of connections between the nodes that need to deliver data bits. Many different routing protocols have been devised for Ad Hoc networks and have been mainly classified into two categories such as proactive (periodic) and reactive (on demand). In a proactive routing protocol, nodes periodically exchange routing information with other nodes in order to have current routes to all destination [3]. In a reactive protocol the route to the destination is obtained as and when a node has data bits to send to that destination [4].

Security in network layer plays an important role in the security of the entire network. The wireless channel is accessible to both legitimate network users as well as to malicious attackers. There are different types of attacks by malicious node that can have a network and make it unreliable for communications. These attacks can be classified as active and passive attacks [5]. A passive attack is one in which the information is snooped by an intruder and does not disrupt the network operation on the other hand an active attack disrupts the normal operation of the network. Attacks can be further classified as external and internal attacks. External attacks are carried out by nodes that do not form the part of network, while compromised nodes that were once legitimate part of the network are cause of internal attacks

A black hole attack is a type of routing attack in which malicious node advertise itself as having shortest path to destination in a network by sending fake route reply to the source node. It can be used as Denial of Service (DoS) by dropping the received packets. The malicious node can deprive the traffic from the source node.

The rest of the paper is organized as follows. Section 2 discusses the theoretical background of AODV. Section 3 presents black hole attack. Related work on prevention of black hole attack is discussed in section 4. Proposed solution to the black hole attack are presented in section 5 , Section 6 of this paper discusses the simulation environment used and results for our proposed solution Last section presents the conclusion.

## 2. The Routing Protocol : AODV

The Ad Hoc On-Demand Distance Vector (AODV) is a state of the art reactive routing protocol suitable for dynamic link condition and is an adaptation from DSDV protocol. Every node in a Ad Hoc network maintains a routing table and whenever a source node needs to communicate with another node, it sets up a route on-demand at the start of the communication session for which it has no routing information and makes use of the route till it breaks. Route discovery process being the part of AODV uses control messages such as Route Request (RREQ), Route Reply (RREP). AODV is also able to handle changes in route if there is an error through the control message Rout Error (RERR). Nodes that communicate directly with another is considered to be its neighbor and a node keeps track of its neighbors by listening to a HELLO message that each node broadcast at regular intervals.

When one node needs to send a message to another node that is not its neighbor, it broadcast a RREQ containing several key bits of information: The source, the destination, the lifespan of the message and a sequence number which serves as a unique ID. Each neighboring node responds to the RREQ message by sending a RREP message back to the source node if it knows a route to the destination or the neighbor itself is the destination node otherwise it rebroadcast the RREQ to its own set of neighbors after increasing the hop count field. If a source node does not receive the RREP in a set amount of time, it rebroadcast a new RREQ with new ID and longer lifespan. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup [6]

The destination sequence number serves as time stamp and allow intermediate nodes to compare how “fresh” their information on other nodes. Every time node sends out message increases its own sequence number. A higher sequence number signifies a fresher route. If a node receives more than one RREPs, it updates its routing information and propagates the RREP only if RREP contains either a greater destination sequence number than in the previous RREP or same destination sequence number with a smaller hop count and discards all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then updates the routing information later for better route to the destination. Nodes stores or updates following information in their route table:

- Destination node address
- Source node address
- Hops up to destination
- Next hop to destination node
- Destination sequence number
- Active neighbors for the route
- Route expiration time

The routing protocol typically assumes that all nodes are cooperative in the communication process and at the same time malicious attackers can disrupt the network operation. In this paper, we discuss the black hole attack in particular and propose a solution to it.

## 3. Black hole attack

MANETs are vulnerable to various attacks due to the factors described in the introduction section of this literature. These attacks directly pose threat to the important network layers such as physical, data link and network layer which are responsible for routing mechanism of the network, Attacks in network layer can either cause Denial of Service (DoS) by not forwarding the packet or add and modify the routing parameters such as hop count and sequence number in control messages, When the malicious node is chosen as route to the destination, it stops forwarding the data packets.

In black hole attack, the malicious node waits for its neighbor to send a RREQ packet. Upon receiving the RREQ packet, the malicious node immediately sends a forged RREP to the source node with a modified higher sequence number. In such a case, the source node assumes that the node is having a fresh route towards destination. The source node discards the RREP packets it receives from other nodes having genuine route and send data packets through malicious node. A malicious node takes all routes towards itself and does not allow forwarding any packet. This attack is called black hole as it swallows (drops) all objects; data packets [7].

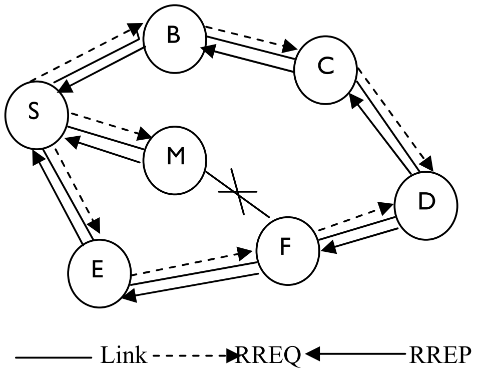

Figure 3.1

In figure 3.1, S and D are assumed to be source and destination nodes respectively. Let M be the malicious node. S being the source node would initiate the route discovery process and broadcasts a RREQ that is received by the nodes B, M and E being the neighbors of node S. Upon receiving the RREQ from the node S, node B and E makes a search to their cache for a fresh route to the destination. Non-availability or older entry in their route table causes nodes to rebroadcast the RREQ and this process is continued till the RREQ arrives at node D. But node M claims to have the fresh route to destination and sends RREP packet to the source node S. The reply from the malicious node reaches the source node much earlier than other legitimate nodes, as the malicious nodes does not have to check its routing table. Nodes those have route to the destination would update their route table with the accumulated hop count and the destination sequence number of the destination node and generate a RREP control message. The destination sequence number that determines the freshness of a route is a 32-bit integer associated with every route [8]. The malicious node claims to have a fresher route by including a very high destination sequence number in RREP packet. The source node chooses the path provided by the malicious node and starts sending the data packets, which are dropped by the malicious node.

## 4. Related work

Several researchers have studied the vulnerabilities of MANETs and black hole attack in particular. Black hole attack is one of the active DoS. Many researchers have proposed their solutions which are available in literature.

The solution proposed in[9] require that the requesting node should wait for a predetermined set time to receive RREPs with next hop details instead of from other neighboring node sending data packets immediately after receiving a reply. After the time out, it first checks in CRRT table whether there is any repeated next hop node. If any next hop node is present in the reply path it assumes the path is correct or the chance of malicious path is limited .Extra overhead is added in the process of finding repeated next hop and adds a delay.

In[10] author has suggested anomaly based detection technique through dynamic learning method .IN this approach , the normal state of the network view is updated periodically to adopt to the frequent network changes and “clustering-based ” technique is adopted to identify the nodes that deviate from the normal state.

As per this approach the characteristics considered to express the normal state of network are (i) total number of RREQs sent out .(ii) total number of RREPs received

(iii) average of destination sequence number difference between the RREP sequence number and the one held in the list in each time slot .The network state in time slot ; is expressed by three –dimensional vector $x_i=(x_{i1},x_{i2},x_{i3})$.

The mean vector values of these features are calculated as in (1) where D is training data set for N time slots.

$$\bar{x}^{D}=1/N \sum_{i=1}^{N} xi \qquad (1)$$

Hence the initial training data refer to the data collected in first interval of the network i.e$\Delta T_{0.}$

The distance of each input data sample x to the mean vector for each time slot is calculated as shown in (2)

$$d(x)=\|x- \bar{x}^{D}\|^2 \qquad (2)$$

From the learning data set , the distance with the maximum value is considered as Threshold $T_h$.

$T_h$ =d($x_1$), where I=$\arg_i$ max d($x_i$) $x_i$ €D

When the distance for any input data sample is larger than the Th, it is considered as deviding from the normal traffic and hence judged as attack else . By using data collected in initial time $\Delta T_0$ , the calculated mean vector is used to detect next period time interval i.e $\Delta T$ .If $\Delta T$ is considered as normal , the corresponding data set else it is treated as data with attack and consequently discarded.

[The solution proposed by the author suffer from the network resource limitation such as battery power, storage and processing. Every time interval $\Delta T$, the input data set need to be collected & processed resulting additional overhead]

In [11], source node verifies the authenticity of node that inititate RREPs by finding more than one route to the destination. when source node receives RREPs , if routes to destination shared hops , source node can recognize the safe route to destination.

In [12], the author has developed a neighborhood approach capable of detecting the black hole attack. Once the root discovery process initiated by the source is over, the source node sends a special control packet to request the destination to send its current neighbor set. If the two neighbor sets received at the same time are different enough, it can be considered that they are generated by two different nodes. The claim for the same is substantiated with the following observation.

(i) Considering the node mobility and size of the network, the neighbor set difference of one node at different time instants t and $t_{+1}$.The results shows no much change in neighbor sets during route discovery.

(ii) 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 }) has the probability that node A’s neighbor set is the same as that of node B is very small.

So when the source node receives the neighbor set , it and analysis them by measuring the difference with a predefined threshold values . If the difference is larger , the source node concludes that the current network has black hole attack and responds to it accordingly.

## 5. Proposed Solution

Though there are many solutions proposed by various authors to deal with black hole attack, some of them are reviewed in this literature and found to exhibit the effect on performance in terms of increase in delay and overhead,

In this literature considering the limitations (battery power, storage and processing power ) of nomadic computing paradigm, we devise an algorithm that prevents from black hole attack at the cost of only marginal processing overhead. The proposed algorithm is simple and does not affect workings of either intermediate or destination node. It does not even modify the working of normal AODV but calls a preprocess called Pre_Process_RREP. The Process continues to accepts RREP packets and calls a process called Compare_Pkts(packet p1, packet p2) which actually compares the destination sequence number of two packets and selects the packet with higher destination sequence number if the difference between two numbers are not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node and an ALERT message containing the node identification is generated which is broadcasted to neighbor nodes so that any message receive from such malicious node is discarded. A list of such malicious nodes can be maintained by the nodes participating in communication which can be used to prevent black hole attack. The algorithm is given in following fig.

```
Pre_Process_RREP(){
t=CURRENT_TIME+WAIT_TIME;
while (CURRENT_TIME < t){
    packet Old_pkt=Cur_Pkt=Sel_Pkt=NULL;
    Cur_Pkt=Compare_Pkts(packet New_Pkt, packet Old_Pkt};
    If(Cur_Pkt!=NULL && Cur_Pkt!=Sel_Pkt){
            Process_RREP(Cur_Pkt);
            Sel_Pkt=Cur_Pkt;
    }
    If(Cur_pkt!=NULL && Cur_pkt =New_Pkt)
            Old_Pkt= Cur_pkt;
    Cur_Pkt=NULL;
}//End of while
}//End of Pre_Process_RREP()
```

*Fig.-1 Proposed Algorithm: at source node*

```
Compare_Pkts(packet p1, packet p2){
    Packet Selected_Pkt=NULL;
    if(p1!=NULL && p1.dest_seq_no is exceptionally high){
            generate ALERT message;
            p1=NULL
    }
    if(p2!=NULL && p2.dest_seq_no is exceptionally high){
            generate ALERT message;
            p2=NULL
    }
    If(p1!=NULL && p2!=NULL)
            Selected_Pkt=Packet containing higher dest_seq_no.
    else
            If(p1!=NULL)
                    Selected_Pkt=p1;
            else
                    Selected_Pkt=p2;
    return Selected_Pkt;
```

*Fig.-2 Proposed Algorithm calls Compare_Pkts.*

## 6. Conclusion

Black hole attack is one of the major security challenges for MANETs. It is one of the active DoS in which a malicious node impersonates a destination node by sending a forged RREP to the source node. Although there exists many variants of black hole attack, in this paper we just studied the black hole attack by the existence of single malicious node in the network and its solution proposed by various authors. Review of the proposed solutions suggests that the performance of the routing protocol is affected in terms of additional overheads, end-to-end delay and packet delivery ratio. In our future work, we would carry our research in optimizing the performance of a network having black hole attack.

## References:

***[1] Hao yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications, February 2004.***

***[2] D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.***

***[3] Shree Murthy and J.J. Garcia-Luna-Aceves. "An Efficient Routing Protocol for Wireless Networks". Mobile Networks and Applications, 1(2):183-197, 1996.***

***[4] Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc On Demand Distance Vector Routing". In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90-100, February 1999.***

***[5] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, Vol.13, No.6, Nov./Dec. 1999, pp. 24-30.***

***[6] C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000, http://www.ietf.org/internal-drafts/draft-ietf-manet-aodv-05.txt***

***[7] Dokurer, Semih "Simulation of Black hole attack in wireless Ad-Hoc networks" Master's thesis, Atihm University, September 2006.***

***[8] Santoshi Kurosawal, hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV – based Mobile Ad Hoc Networks by Dynamic Learning Method" in International Journal of Network Security, Vol.5, No.3, pp.338-346, Nov.2007.***

***[9] Latha Tamilselvan, V sankaranarayanan, "Prevention of Blackhole Attack in MANET". In Proceedings of The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.***

***[10] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto " Detecting Black hole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method", Intl. Journal of Network Security, vol 5, no 3 Nov 2007, Pp 338-346.***

***[11] M.A. Shurman, S.M. Yoo, and S. Park, "Black hole attack in wireless Ad Hoc networks", in ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr-2004***

***[12] B. Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.***