Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET

Sushil Kumar
Assistant Professor
Graphic Era University
Dehradun, India

Deepak Singh Rana
Assistant Professor
Graphic Era Hill University
Dehradun, India

Sushil Chandra Dimri
Professor
Graphic Era University
Dehradun, India

ABSTRACT
Wireless mobile ad hoc network (MANET) is a self-configuring network which is composed of several movable mobile nodes. Black Hole attack is one of the DOS attacks in MANET, which can misbehave with network, increase in network traffic, packet loss, decreases throughput, send false reply to the nodes and dropped data packets. Therefore, to analysis all these effects, a contribution has been made with modification of AODV routing protocol as a bhAODV (Black Hole AODV). To show the effect of black hole attack in AODV, result analysis is done using the comparison of AODV and bhAODV. In this paper we also contribute in AODV to provide a solution for Black Hole attack (sbhAODV). Network Simulator (NS 2.35) is used to implement bhAODV and sbhAODV, simulation and result analysis.

Keywords
MANET, AODV, bhAODV, sbhAODV, CBR, Black Hole attack, malicious node, PDR, NS-2.

1. INTRODUCTION
Wireless mobile ad hoc network (MANET) is a self-configuring network which is composed of several movable mobile nodes[1]. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In Black Hole attack, a malicious node falsely advertises shortest path to the destination node and absorbs all data packets in it. By doing this, the malicious node can deprive the traffic from the source node. It can be used as a denial-of-service attack where it can drop the packets later[2][3].

1.1 Black Hole Attack
A Black Hole attack [3][4][5] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. 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 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 reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of data packets, the Black hole node simply drops them, instead of forwarding to the destination.

1.2 AODV
AODV is categorized as a dynamic reactive routing protocol [5][6]. In a reactive routing protocol, route will be established based on the demand (upon request by source node). Ad-hoc On-Demand Distance Vector (AODV) [13] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. In AODV route discovery, there are two important control messages namely Route Request (RREQ) and Route Reply (RREP). Both control messages carry an important attribute called destination sequence number and has the incremental value to determine the freshness of a particular route.

Many researchers have conducted different detection techniques to propose different types of detection schemes. In this, we survey the existing solutions and discuss the state-of-the-art routing methods. We develop a Black Hole attack (bhAODV) for reactive ad-hoc network protocols AODV. In this paper, performance of AODV is evaluated in the presence of black hole attack (malicious node) and without black hole attack with cbr traffic under different scalable network mobility. We also proposed sbhAODV (Solution for Black Hole AODV) to prevent security threats of black hole by notifying other nodes in the network of the incident. The simulation results in NS-2.35 demonstrate that their protocol not only prevents black hole attack but consequently improves the overall performance of AODV in presence of black hole attack.

2. RELATED WORKS IN DETECTING BLACK HOLE ATTACK
There have been quite a number of works done in securing the routing protocol in MANET from the black hole attack.

M.A. Shurman [5] in his work has proposed for the source node to verify the authenticity of the node that initiates the RREP messages by finding more than one route to the destination, so that it can recognize the safe route to the destination. This method can cause routing delay, since a node has to wait for a RREP packet to arrive from more than two nodes. Ming-Yang [6] proposed an Intrusion Detection System (IDS) to solve the selective black hole attacks in MANET based on Anti-black hole mechanism (ABM). S. Yi [7] proposed a solution which looked at the Security-Aware Ad hoc Routing (SAR) using the security attributes such as trust values and relationships. N.H. Mistry in [8] has proposed for the source node to verify the RREP destination sequence number by analysing the RREP messages which arrived within the predefined waiting period by using the heuristic method. Satoshi Kurosawa [9], proposed an anomaly

detection scheme using dynamic training method in which the training data is updated at regular time intervals. S. Ramaswamy [10] proposed a solution that contain a data routing information table where 1 stands for 'true' and 0 for 'false'. Whenever a RREP is received a cross check is done to verify whether the reply is from a legitimate node or not. According to V Sankaranarayanan and L Tamilselvan [11], they projected a technique that source will verify the reply packet coming from various nearest nodes to wait and check the replies from all the neighboring nodes to discover best possible and secure route. Chin [12] used finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. Nishant Sitapara [13] used an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals assuming that the first RREP message arrived from the black hole node. Lalit [14] proposed an efficient algorithm which can be used to find the secured routes and prevent black hole nodes by the identifications of the nodes with their sequence number. Jan von Mulert [15] focused on networks using the popular AODV protocol and a secure extension to AODV, the Secure AODV (SAODV) protocol. Shashank [16] suggested a solution that is an enhancement of the basic AODV routing protocol used to avoid Black Hole attacks. [17], [18], [19] and [20] introduced the simulation the AODV routing protocol under black hole attack and the analysis of it is effect.

3. IMPLEMENTATION OF bhAODV (BLACK HOLE AODV) ROUTING PROTOCOL IN NS 2.35

Implementation phase of Black Hole behavior to the AODV protocol is written using C++. Since the nodes behave as a Black Hole they have to use a new routing protocol that can participate in AODV messaging. All routing protocols in NS 2.35 [21] are installed in the directory of "*ns2.35*" [22]. In Figure-1 show the steps to add bhAODV and black hole behavior in NS 2.35.

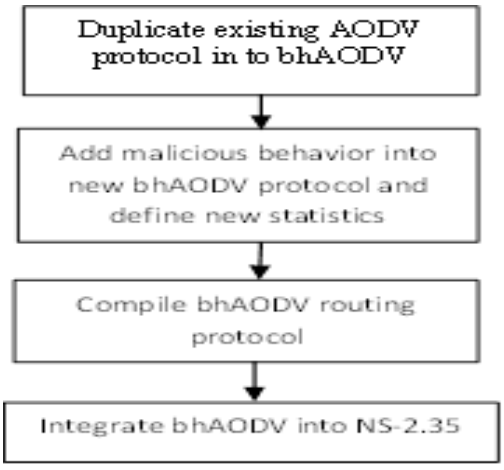

Figure-1- Steps to add bhAODV routing protocols into NS-2.35

Source node forward RREQ to all its neighbors, if there is a malicious node and receive RREQ from source node it immediately send a false RREP to the source node as shortest path or fresh rout path to deliver data packets for destination. If RREP found from the node then source node will forward data packets in RREP path. If RREP contains path of malicious node then it drop all data packets without forwarding it to the next node or destination. If no malicious node and there is actual path from source to destination then it will forward data packets on that path and destination will receive data packets without any attack.

3.1 Algorithm for Black Hole Attack Implementation

To implement black hole attack some changes are made in *bhaodv.h* and *bhaodv.cc* file. Following are the steps to make changes:

Step 1: In bhaodv.h header file we declared a Boolean variable malicious.

Step 2: In bhAODV constructor we set value for malicious variable as false.

Step 3: In command method of bhaodv.cc file, if node is labeled as blackhole then set malicious value as true.

Step 4: In Receive request method (recvRequest(Packet *p)) of bhaodv.cc file, if node is malicious then send false RREP with Max Destination Sequence Number else send Reply actual Destination Sequence Number.

Step 5: If node is not destination, but node may have a fresh enough route then send false RREP with Max Destination Sequence Number node and Lifetime as rt_expire-CURRENT_TIME, Insert next hop to RREQ source and Insert next hop to RREQ destination.

Step 6: Free packet.

Step 7: In Route Handling Functions (rt_resolve(Packet *p)) of bhaodv.cc file, if value of malicious is true then drop packets.

4. IMPLEMENTATION AND RESULT ANALYSIS OF "sbhaodv" (SOLUTION FOR BLACK HOLE AODV) ROUTING PROTOCOL IN NS 2.35

Here we contribute in AODV to provide a solution for this Black Hole attack. As the malicious node send an RREP message without checking the tables, it was assumed that more likely for the first RREP to arrive was from the malicious node. To evaluate effects of the solution, "sbhaodv" implemented same as "bhaodv". To implement the solution we modified Receive RREP function (recvReply) and create a RREP store mechanism to count the second RREP message. In RREP store mechanism, "rrep_insert" function is for adding RREP messages, "rrep_lookup" function is for looking any RREP message up if it is exist, "rrep_remove" function is for removing any record for RREP message that arrived from defined node and "rrep_purge" function is to delete periodically from the list if it has expired. In the "recvReply" function, first control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived. If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is stored before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbor.

4.1 Algorithm for Solution of Black Hole Attack (sbhaodv) Implementation

To implement the solution for black hole attack some changes are made in sbhaodv.cc file. This algorithm describes steps to make changes:

Step 1: In Receive Reply method, set broadcastRREP by looking any RREP message up if it exit, using rrep_lookup() method.
Step 2: If destination address is equal to index then goto Step 3 else goto step 7
Step 3: If broadcastRREP is equal to NULL then goto step 4 else goto step 5
Step 4: Set count as zero and insert RREP message in routing table using rrep_insert() method.
Step 5: Set rout->count = rout->count + 1 and Set count = rout->count
Step 6: Update Rout Table
Step 7: Forward packets

5. SIMULATION PARAMETERS AND METRICS

At the physical and data link layer, IEEE 802.11 is used. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, AODV is used as the routing protocol. 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 0.25 Mbps, simulation time is 500s, pause time is 1s. The connection pattern is generated using *cbrgen* and the mobility model is generated using *setdest* utility**.** The terrain area is 800m X 800m with 10, 20, 30, 40, 50 nodes and maximum speed 20 m/s. Each data point represents an average of five runs as malicious node and without malicious node. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols.

5.1 Metrics used for Simulation

On the bases of simulation parameters [23] we calculate PDR, End to End Delay, Throughput, and Dropped packets with AODV, bhAODV (with a malicious node or Black Hole Attack) and sbhAODV (solution for black hole attack).

PDR (Packet Delivery Ratio): Packet Delivery Ratio = Total Packets Received / Total Packets Sent. The ratio of the number of data packets successfully delivered to the destinations to those generated by CBR sources. Packet delivery ratio describes the loss rate.

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. It is measured in milliseconds.

Average Throughput: The throughput is usually measured in bits per second (bit/s or bps), and data packets per second or data packets per time slot.

Dropped Packets: To evaluate dropped packets we count how many packets are sent by the sending nodes and how many of them reached the receiving nodes.

6. SIMULATION AND RESULT ANALYSIS WITH GRAPHS

To test the implementation we used three simulations cases.

6.1 First case

In first case, normal AODV routing protocol is used without any attack. Table-1 analyzed that average PDR is 87.918 %, Average End to End Delay is 0.4045 %, Throughput is 122.818 and Packet loss is 1855.

Table-1: Result analysis of AODV (without attack) for node 10 to 50

No of Nodes	10	20	30	40	50
Generated Packets	4388	9873	15358	20843	26328
Received Packets	3655	8959	14086	18816	22012
Total Dropped Packets	733	917	1276	2031	4318
Packet Delivery Ratio	83.30%	90.74 %	91.72%	90.27 %	83.61%
Average End-to-End Delay	0.591037	0.28676	0.332162	0.36037	0.452442

6.2 Second case

In second case, we implement a black hole attack by creating a node as a malicious node, for this black hole node we used bhAODV and for all other nodes AODV is used as a routing protocol. From Table-2, we analyzed that PDR is 8.928 % which decrease to 79%, Average End to End Delay is 0.3483% which decreases to 0.0563 %, Throughput is 9.878 which decrease to 102.94 %, and Dropped Packets is 14350 which increase to 12495 in comparison of first case.

Table-2: Result analysis of bhAODV with AODV (with black hole attack)

No of Nodes	10	20	30	40	50
Generated Packets	4388	9873	15358	20843	26328
Received Packets	948	716	703	1066	1606
Total Dropped Packets	3441	9158	14655	19777	24719
Packet Delivery Ratio	21.60 %	7.25%	4.58%	5.11%	6.10%
Average End-to-End Delay	0.828657	0.255202	0.138574	0.298456	0.221171

6.3 Third case

In the third case, sbhAODV protocol is used instead of AODV for all nodes and bhAODV is used for malicious node. In the test simulation, the sbhAODV protocol is used in the same scenario with Black Hole Attack bhAODV, then PDR increases 19%, Average End to End Delay increases 0.0596 %, Throughput increases 26.088 %, and Dropped Packets decreased 1999 in comparisons of AODV with bhAODV.

Table-3: Result analysis of sbhAODV with bhAODV (with black hole attack)

No of Nodes	10	20	30	40	50
Generated Packets	4388	9873	15358	20843	26328
Received Packets	3655	8899	14166	19061	21729
Total Dropped Packets	733	977	1196	1796	4607
Packet Delivery Ratio	83.30 %	90.13 %	92.24 %	91.45 %	82.53 %
Average End-to-End Delay	0.594 32	0.286 7	0.346 48	0.402 23	0.536 93

6.4 Simulation results with graph

Simulation results are described below with the help of graph.

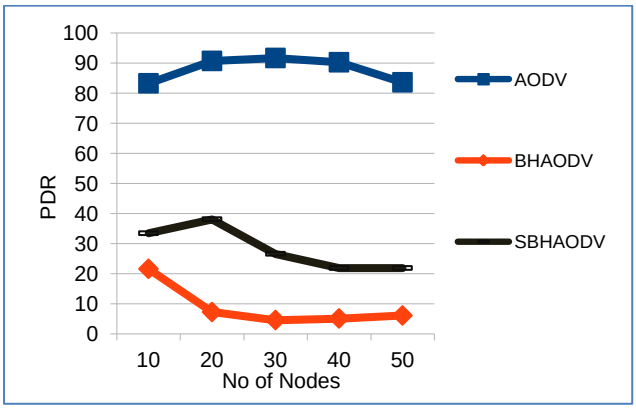

Figure-2 PDR in % with bhAODV and sbhAODV

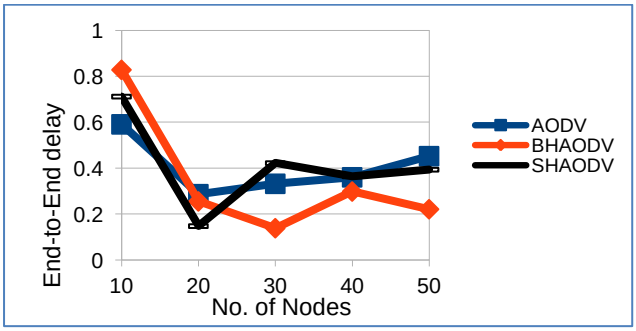

Figure-3 End to End Delay with bhAODV and sbhAODV

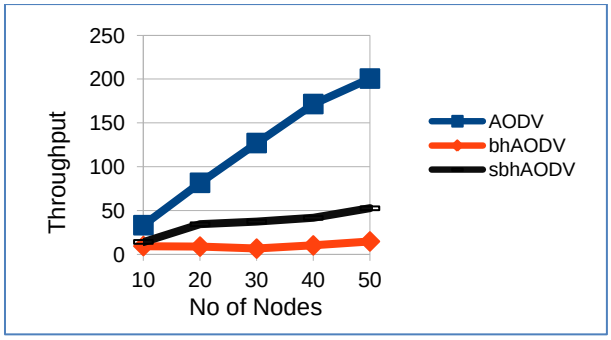

Figure-4 Throughput for sbhAODV with bhAODV

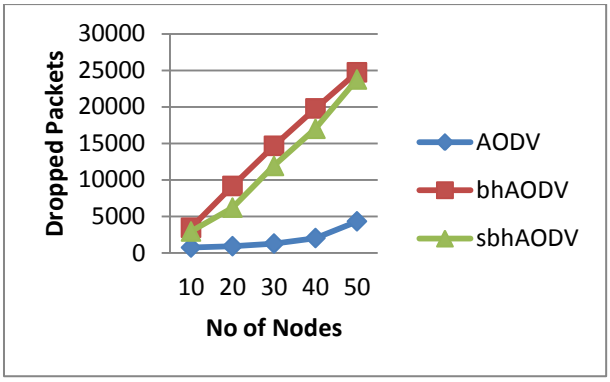

Figure-5 Dropped packets for sbhAODV with bhAODV

7. CONCLUSION

In this paper, effect of the Black Hole in AODV routing protocol is analyzed. Five scenarios are simulated for AODV, after introducing a black hole attack with bhAODV. Here a solution for black hole attack (sbhAODV) is also implemented that attempted to reduce the Black Hole effects in NS 2.35 and simulated the solution using the same scenarios as we used for AODV and bhAODV. AODV has normally 87.918 % PDR, 0.4045% Average End to End Delay, 122.818 Throughput and 1855 packet loss. If a Black Hole Attack is implemented using bhAODV then PDR is 8.928 % which decrease to 79%, Average End to End Delay is 0.3483% which decreases to 0.0563 %, Throughput is 9.878 which decrease to 102.94 %, and Dropped Packets is 14350 which increase to 12495 in comparison of normal AODV. When sbhAODV protocol is used in the same scenario with Black Hole Attack bhAODV, then PDR is 28.388 % which increase to 19%, Average End to End Delay is 0.4079% which increases to 0.0596 %, Throughput is 35.966 which increase to 26.088 %, and Dropped Packets is 12351 which decrease to 1999 in comparisons of AODV is used with bhAODV. Therefore, from analysis we conclude that sbhAODV gives good performance with bhAODV in comparisons of normal AODV and bhAODV.

8. ACKNOWLEDGMENTS

I am very thankful to the management of Graphic Era University for always being very supportive for me and also providing such a commendable research platform for all of us.

9. REFERENCES

[1] Burbank JL, Chimento PF, Haberman BK, Kasch WT "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology". IEEE Communication Magazine 44(11):39–45, 2009.

[2] Abolhasan, M., Wysocki, T., Dutkiewicz, E: "A review of routing protocols for mobile ad hoc networks". Elsevier, Amsterdam, 2004

[3] Mahmood, R.A., Khan, A.I.: "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks". In: International Symposium on High Capacity Optical Networks and Enabling Technologies", 2007.

[4] K.A. Jalil, Z. Ahmad, and J.-L. Ab Manan "An Enhanced Route Discovery Mechanism for AODV Routing Protocol" J.M. Zain et al. (Eds.): Springer-Verlag Berlin Heidelberg, ICSECS 2011, Part III, CCIS 181, pp. 408–418, 2011.

[5] Shurman, M.A., Yoo, S.M., S. Park.: "Black hole attack in wireless ad hoc networks". In: ACM 42nd Southeast Conference ACMSE 2004.

[6] Yang Su Ming, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Elsevier Computer Communications, vol 34, pp. 107-117, 2011.

[7] Yi, S., Naldurg, P., Kravets, R.: Security-Aware Ad hoc Routing for Wireless Networks.In: Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (Mobihoc 2001), Long Beach, CA, pp. 299–302, October 2001.

[8]. Mistry, N.H., Jinwala, D.C., Zaveri, M.A.: "MOSAODV: Solution to Secure AODV against Blackhole Attack", International Journal of Computer and Network Security, December 2009.

[9] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security 5(3), 338–346, 2007.

[10] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K: "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

[11] Sankaranarayanan, V., Tamilselvan, L: "Prevention of Blackhole Attack in MANET". In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. IEEE, Los Alamitos, 2007.

[12] Tseng Chin-Yang, Balasubramanyam Poornima, and Ko Calvin, "A Specification-based Intrusion Detection System for AODV" in Proceedings of 1st ACM workshop on security of Ad Hoc and sensor networks, California, Davis, pp. 125-134, 2003.

[13] Sitapara Nishant and Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks," in International Conference on Emerging trends in engineering "ICETE-201O" , Jasingpur, 2010.

[14] Himral Lalit, Vig Vishal, and Chand Nagesh, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), vol. 3, pp. 3927-3932, 2011.

[15] Von Mulert Jan, Welch n Ian, and Winston K.G.Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," Journal of Network and Computer Applications, vol. 35, pp. 1249–1259, 2012.

[16] Khare Shashank, Sharma Manish, Dixit Namrata, and Agrawal Sumit, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET," VSRD International journal of Electrical, Electronics and Communication Engineering, vol. 2 (6), pp. 385-390, 2012.

[17] Ghonge Mangesh and S. U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANT," International Journal of Advanced Research in Computer Science and Software Engineering", 2012.

[18] Nabarun Chatterjee and Jyotsna Kumar Mandal, "Detection of Blackhole Behavior using Triangular Encryption in NS2," 1st International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA- 2013), pp. 524-529, 2013.

[19] Sharma Ajay, Babu, Ahirwar Rajesh, and Patil Smita, "Performance Evaluation of AODV under Blackhole attack in MANET using NS2 simulator," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), pp. 79-82, 2012.

[20] Su Mon Bo, Xiao Hannan, Adereti Aderemi, and James A, "A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack," in Third International Symposium on Information Assurance and Security, pp. 50-55, 2007.

[21] The VINT Project, "The NS manual", A Collaboration between researches at UC Berkeley, LBL, USC/ISI, and Xerox PARC, March 14, 2008.

[22] Eitan Altman and Tania Jimenez, "NS Simulator for beginners", lecture notes, Univ. of de Los Andes, 2003-2004.

[23] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana , "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", Paper published by *International Journal of Computer Technology & Applications,* Vol 3 (4), 1395-1399, ISSN:2229-6093, 2012.