Blackhole Prevention Algorithms for AODV in Mobile Ad Hoc Network- A Review

Devottam Gaurav, Charu Wahi

Abstract-A Wireless ad-hoc network is a temporary network where several mobile autonomous nodes can move freely in any direction. With the help of routing protocols source node finds a path to the destination node and forward data packets through intermediate nodes connected by symmetrical transmitted links. However, due to mobility and ad-hoc nature, security becomes an important issue in MANET because once malicious nodes are in the range of networks; they can join the network freely and degrades the performance by attacking it. The vulnerability of MANET is very high towards routing attacks such as blackhole, which drops all the packets instead of forwarding it to the destined node and results in data loss. This research paper focuses on analyzing the probable solutions pointed out by several eminent researchers to reduce the effects of blackhole attack in MANET.

Keywords- AODV, Blackhole, MANET.

1. INTRODUCTION

MANET itself stands for mobile ad hoc network which is an automated network consisting of several mobile nodes communicating with each other via transmission links through wireless medium. *"Ad hoc"* in Latin itself stands "**for this purpose**" where devices change its links frequently in any direction. They also forward their traffic to other devices unrelated to its own use, and therefore can be named as a router. Hence, MANET is a group of several mobile routers (and associated hosts) which are interlinked by symmetrical links and their union results in formation of arbitrary graph. Varieties of applications for MANET include disaster area, personal area network, military purpose and many more.

There are numerous issues about MANETs, such as finite transmission bandwidth, reliable data delivery, routing, quality of service, security problem etc. In recent years, researchers have extensively discussed and investigated about security threats and issues in the wired and wireless networks. Due to change in the inherent design defects of MANET, it is vulnerable to threats like snooping attacks, black hole attacks, wormhole attacks, distributed DoS (DDoS) attacks, denial of service (DoS) attacks and so on. However, one of the most popularized security threats which change the behavior of routing problem is black hole attack. Although, there are probable solutions proposed by some eminent researchers to get rid of this issue, but still unable to prevent it completely.

The remaining part of the paper is summarized as follows: Section 2 briefly describes the working of the AODV routing protocol. In section 3, we review the effect of blackhole attack and efforts of various researchers who have analyzed its performance. In section 4, we discuss some existing solution to prevent blackhole attacks and comparative analysis is done. Finally, we conclude in Section 5.

2. AODV

AODV stands for Ad-Hoc on Demand Distance Vector, is a reactive protocol in which network generates routes at initial stage of communication by building routes using a route request (RREQ) / route reply (RREP) query cycle. There is potential contribution of all nodes in the network and requires multi-hop routing [8].

2.1. Route Discovery Module

When source node "S" sends data packets to a given destination "D", S consults its routing table. On finding a valid entry (a route) towards that destination D, it uses it immediately; else a route discovery procedure is broadcasted (Figure 1) by the source node S towards neighbors which consists of a route request (RREQ) message. In order to find a fresh route, an intermediate node consults its routing table after it receives RREQ and compares the destination sequence number (DSN) of this RREQ. If it is greater than that of DSN present in routing table, modified RREQ packet with new DSN is forwarded towards the requested destination; else if both DSNs are found to be equal, metrics (hop count) comparisons are done and smallest metric is chosen. Finally, modified RREQ is forwarded to destination "D". When "D" receives the RREQ a route reply (RREP) message is sent with DSN through the pre-established reverse route towards the source S. Again comparison is done, when source S receives several RREP, it will select whose DSN is larger, if DSNs of several RREP are equal, then, hop count with smallest number will be selected [1].

IJSER

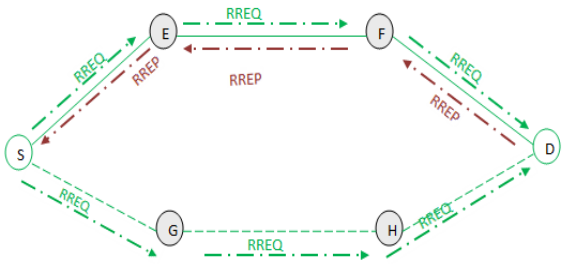

Figure 1. Route Discovery Process of AODV

2.2. Route Maintenance Module

Hello message (to ensure connectivity) is sent by each node to its neighbors and waits for Hello message in return from its neighbors. Exchange of Hello message in bidirectional way indicates a symmetric link is maintained if no interruption occurs; else a route error (RERR) message will be sent to the source node S on finding the broken link (Figure 2). This can again launch the route discovery procedure, if required. Link interruption itself indicates the breakdown of mobility of nodes in the network.

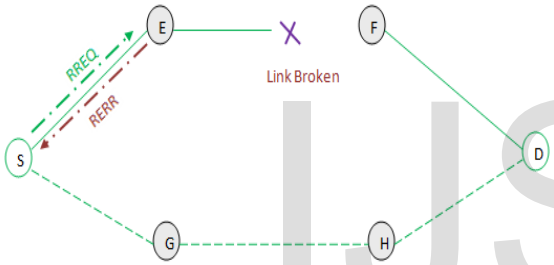

Figure 2. Route Maintenance Process of AODV

3. Security Issue in Mobile Ad Hoc Network

Security provides an essential service for both mediums of network communications (i.e., wired and wireless) and ad-hoc network's success strongly depends upon it. In mobile ad hoc networks security is difficult to achieve because adversaries must access the network medium by crossing many defense lines such as firewall and gateway before their malicious activities attacks the targets in case of wired networks, but, in case of wireless networks, adversaries can communicate with the nodes of adhoc network or join the network once they are in the range of it and may reduce the network performance by attacking it. The vulnerability of MANET is very high towards routing attacks such as blackhole.

3.1. Blackhole Attack

An intermediate node works alone or a group of intermediate nodes works in collusion to carry out blackhole attack. The performance of the routing services are degraded due to the creation of routing loops, forwarding of packets via non optimal paths or selectively dropping of packets by the attacker node. (Figure 3) shows how blackhole attack happens; route discovery process is initiated by having the communication between node "S" and node "D" and then, data packets are forwarded between the two. When route discovery process is completed, node "M" (malicious node) claims that it has a shortest and active route to the destined node and then, sends the route reply packet (RREP) with the highest sequence number back to the source node "S". When RREP packet of malicious node "M" reaches source node "S", then all remaining replies are rejected by "S" and forwarding of packets takes place between "S" and "M". Further, malicious node "M" drop all packets, due to which the packet loss increases and destination node neither knows nor receives packet and source node also never get to know about this. Thus, performance of network degrades due to the problem created in the network, so called black hole problem [2].

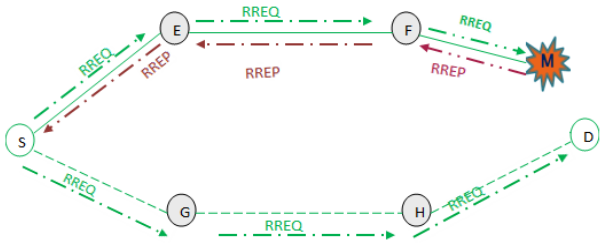

Figure 3. Blackhole Attack Problem

3.2. Effects of Blackhole Attack on AODV

Various researchers have evaluated the performance of Mobile Ad-Hoc network to analyze the effect of blackhole attack on the working of AODV using different simulators like NS-2, QualNet etc. Some of their works are:-

- Pramod Kumar Singh et.al [3], have carried out the simulation of Blackhole attack using QualNet 5.0.1. They have created a network of 30 nodes with CBR traffic. The simulation results showed that throughput drastically reduces to 40% in case of AODV with blackhole attack.
- Nital Mistry et.al [4], have carried out the simulation of Blackhole attack using NS-2 tool having maximum transmission of 1000 packets to the destination node from source node. All the data packets are CBR with 0-2 Mbps packets transmission rate. Number of nodes is varied from 10 to 80 moves with a maximum speed up to 70m/s. There is drop in PDR by 81.812% in presence of blackhole attack. By varying the mobility of nodes, PDR of AODV drops by 70.867% in presence of blackhole attack.
- Anu Bala et.al [5], have carried out the simulation on Blackhole attack using NS-2 simulator tool. They have created a small size network with 7 nodes with a terrain of 670*670m. The results revealed that blackhole node increases the data loss by 86.88%. There is increase in average end-to-end delay without the effect of blackhole attack. This is due to the immediate reply from the malicious node because it doesn't check its routing table.
- Ei Ei Khin et.al [6], have carried out the simulation of Blackhole attack using NS-2 tool, with 20 nodes. The evaluation showed that the PDR of AODV without attack is is 97.99% when the nodes move at a speed of 10m/s and decreases to 69.03% in presence of

IJSER

blackhole. There is significant increase in routing overhead from 50.63 to 229.62 at 40s pause time.

4. EXISTING SOLUTIONS TO PREVENT BLACKHOLE ATTACK

4.1. Based on timing information

Rajdipsinh Vaghela et.al [9], proposed a solution in which the requesting node forwards DATA packets to destined node and halts for other replies from other neighboring nodes. As soon as it receives request, a timer is set in the "Timer Expired Table" to collect further requests from different nodes. "Collect Route Reply Table (CRRT)" stores the "sequence number" and packet arrival time and at the end, timeout value is calculated based on the packet arrival time of first route request. After that, it checks CRRT for any repeated next hop node in the reply routes. If found, it considers those paths to be correct or malicious paths are reduced.

4.2. Modification of AODV by control messages

In this paper [10] next hop information is added in RREP message along with two control messages: Further route request (FRREQ) and Further route reply (FRREP). After receiving RREP message with next hop information at source node, FRREQ message to next hop is broadcasted from which it receives RREP and in return, next hop nodes reply back with FRREP message to source node. After receiving FRREP at source node, data packets are routed to the destination node with the shortest path in it. If the next hop node is black hole node, then, the next hop never receives FRREQ and FRREP is not replied back to the source node. At last, data packets are not sent by the path suggested by black hole node from source node.

4.3. Real Time Monitoring

Durgesh Kshirsagar et.al [11], have proposed a solution in which the suspected node, i.e., neighbor of a RREP node is identified first. Neighbor node is instructed to listen the packets sent by suspected node. Two counters are maintained by neighbor node: Fcount and rcount. Fcount increases by 1 when neighbor node forwards the packet to suspected node. Similarly, rcount increases by 1 when suspected node forwards packet to neighbor node. To check node is malicious or not, source node sends packets to destined path. Neighbor node continues to forward packets to the suspected node until fcount reaches the threshold value; thereafter, only if rcount is 0. RREP creator will identify itself as a malicious node and will be blocked [12].

4.4. Opinion based proposal

Monika Y. Dangore et.al [13], have proposed a solution where honesty of a node depends on its participation in communication. When any node first receives the RREP message, it forwards data packets to the source node and different opinions are given by the neighbors of RREP originator node to check its honesty. When it receives reply from all neighbors, it checks whether packets are delivered to the destination from RREP originator node. If found, it considers the node as an honest node. If many packets are received by RREP originator node but packets are not forwarded further or it has sent many RREP packets, it is a malicious node. Further additions of such nodes in the quarantine list leads to blockage [12].

4.5. Based on Destination Sequence Number (DSN)

Pooja Jaiswal et.al [14], have provided a probable method in which all RREPs are collected by source node in Route reply table (RRT) and the source node marks the first reply as first entry in the table. Comparison is done between DSN of first reply and sequence number of source node and if the comparison results in large difference between two, then, the node is malicious node and elimination from the RRT takes place. Remaining entries in the RRT are arranged according to DSN and path of that node is selected based on the highest DSN [12].

4.6. Pre_ReceiveReply Method

N. Mistry et.al [4], have proposed a solution where an additional function Pre_ReceiveReply (Packet P), a table Cmg_RREP_Tab, two timers MOS_WAIT_TIME, RREP_WAIT_TIME and a variable Mali_node is used in the data structures of AODV protocol. All the RREPs are stored in the newly created table, viz., Cmg_RREP_Tab until the time, MOS_WAIT_TIME. When heuristics function is used, MOS_WAIT_TIME is found to be half of the value of RREP_WAIT_TIME – (is the time during which the source node makes a halt for other RREP control messages before regenerating RREQ). As source node receives first RREP control message, it waits for the MOS_WAIT_TIME, during which the source node will save all the incoming RREP control messages in Cmg_RREP_Tab table. Thereafter, the source node makes an analysis of all other stored RREPs from Cmg_RREP_Tab table, and rejects the one having very high destination sequence number and node is considered as malicious. Remaining entries in the Cmg_RREP_Tab table are arranged according to DSN and path with the highest DSN is selected after the identification of the malicious node. It does so, by calling our own method viz. the Pre_ReceiveReply() method. Identity of the malicious node is maintained properly as Mali_node, so, in future, any control messages coming from that node will be discarded and routing table for that node will not be maintained as well as no messages will be forwarded from the malicious node in the network. Freshness is maintained, by flushing the Cmg_RREP_Tab once an RREP is chosen from it.

4.7. ALARM Control Packet

In this paper [15], the time interval data help in updating the threshold value dynamically and an additional checking is done to find out whether RREP_seq_no is greater than threshold value or not. When node is detected malicious it is blacklisted and an ALARM

control packet is send to its neighbors, so that, RREP packet coming from the malicious node is blocked and no processing is done. It simply ignores the reply coming from that node. Hence, routing overhead is less and isolation of malicious node from the network is done by the ALARM control packet which results in no update in the routing table for that node, or no packets are forwarded to any another node. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet [16]. Updating the threshold value depends upon the receiving of RREP packet by the newer node by time to time.

4.8. Solution based on reliability

Latha Tamilselvan et.al [17], has proposed a solution which uses Fidelity table where every node's participation has a fidelity level where reliability will be given to that node. Node is eliminated from the network upon having 0 fidelity level and marked as malicious. Updating the fidelity level of node relies on trusted participation of the node in the network. Each RREP's fidelity level is checked and highest level is selected upon equalization of two levels. Selection of valid route is based on the received threshold value. An acknowledgement is sent to the destination node by the source node only if, data packets are received which results in incrementing the intermediate node's level; else intermediate node's level will decrement. The main drawback of this solution is occurrence of processing delay in the network [18].

4.9. Packet Sequence Number

In this article [19], every node maintains last-packet-sequence-numbers for the last packet sent to every node in one table and last-packet-sequence-numbers for the last packet received from every node in second table. Updating the table is based on the arrival or transmission of data packets. Either the intermediate node or the destination node includes the sequence number of last packet received from the RREQ originator node (i.e., source node) in RREP phase. Source node extracts the last packet sequence number when it receives and then comparison is made with the most recent value saved in its table. If matching occurs, the transmission takes place; else node is considered as malicious node and an alarm message is sent to every node to block the packets coming from this malicious node [20].

The following table summarizes different approaches used by researchers to mitigate the effect of blackhole attack on AODV.

Table 1. Comparative Study of Existing Solutions

Sl. No.	Paper Title	Author	Publishing Year	Features	Simulator	Limitations
1.	Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network [10]	Romina Sharma, Rajesh Shrivastava	3 March, 2014	Working of AODV protocol is modified by addition of next hop information in the RREP message along with two control messages which includes further route request (FRREQ) and Further route reply (FRREP).	NS-2	Co-operative black hole attack can't be prevented. Increase is observed in routing overhead because of two extra control messages.
2.	Blackhole attack prevention and detection by real time monitoring[11]	Durgesh Kshirsagar and Ashwini Patil	4-6 July, 2013	Cooperative Blackhole node is detected using real time monitoring with the help of two counters: Fcount and rcount.	NS-2	Malicious node's identification is based on threshold value because false positive detection can increase.
3.	Detecting and overcoming Blackhole attack in AODV protocol [13]	Monika Y. Dangore and Santosh S. Sambare	15-16 November, 2013	Different opinions given by the neighbors of RREP originator node decide the honesty of the node.	NS-2	The methods works well for Blackhole attack but unable to detect more than one Blackhole node.
4.	A Survey on Approaches towards the Black Hole Attack in Manet [9].	Rajdipsinh Vaghela,Divyesh Yoganand, Monika Changela	December, 2012	Collect Route Reply Table (CRRT) stores the sequence number and packet arrival time. A timer is set in Timer Expired Table.	NS-2	Ineffectiveness is achieved when the attacker agrees to forge the fake reply packets.
5.	Prevention of Black Hole Attack in MANET [14]	Pooja Jaiswal, Dr. Rakesh Kumar	October, 2012	The Route Request Table (RRT) stores route reply coming from malicious node with high destination sequence number as the first entry in it.	NS-2	If sequence number is not extremely large, no detection of Blackhole node is observed.
6.	Improving AODV Protocol against Blackhole Attacks[4]	Nital Mistry, Devesh C Jinwala	17-19 March, 2010	An additional function Pre_ReceiveReply (Packet P), a table Cmg_RREP_Tab, two timers MOS_WAIT_TIME, RREP_WAIT_TIME and a variable Mali_node is used in the data structures of AODV protocol.	NS-2	It does not entail any hidden overhead on either the intermediate nodes or the destination nodes.
7.	Prevention of Blackhole	N.H.Mistry, D.C.Jin	July, 2009	Threshold value is dynamically updated every	NS-2	Works well only in presence of

	Attack in MANETs [15]	wals, M.A.Zaveri		time and an ALARM control message is sent if RREP_seq_no is higher than threshold value.		single malicious node, and performance degrades in case of multiple malicious nodes.
8.	Prevention of Co-operative Black Hole Attack in MANET [17]	Latha Tamilselvan, V. Sankaranarayanan	5 May, 2008	Elimination of any node from the network is based on 0 fidelity level and marked as malicious node.	NS-2	Processing delay occurs in the network.
9.	Black Hole Attack in Mobile Ad Hoc Networks [19]	Mohammad Al-Shurman, Seong-Moo Yoo	2-3 April, 2004.	No addition of overhead is done to the channel because every packet itself contains the sequence number in the base protocol as well as provides an efficient way to detect the suspicious reply.	NS-2	Can only detect cooperative black hole attacks and time delay is increased, because source node halts for other route replies.

5. Conclusion

In this paper, effect of Blackhole attack in an AODV Network is analyzed and comparison is done among different solutions proposed by different researchers but yet none of them are perfect in terms of effectiveness and efficiency. Thereafter, the fact is that AODV protocol is susceptible to the Blackhole attacks. Although research is still being carried out to modify the existing solutions for their viability in order to reduce the malicious effect of blackhole attack in the given network.

References

[1]Monika Roopak, Prof. BVR Reddy, May-2013, "Blackhole Attack Implementation In AODV Routing Protocol," International Journal of Scientific & Engineering Research, Volume 4, Issue 5, 402, ISSN 2229-5518

[2]CH.V. Raghavendran, G. Naga Satish and P. Suresh Varma, 2013, "Security Challenges and Attacks in Mobile Ad Hoc Networks," Information Engineering and Electronic Business, 3, 49-58 Published Online September 2013 in MECS.

[3]Pramod Kumar Singh, Govind Sharma, 2012, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[4]Nital Mistry, Devesh C. Jinwala, 17-19 March, 2010, "Improving AODV Protocol against Blackhole Attacks," Preceding of the International Multi Conference of Engineers and Scientists 2010, Vol II, IMECS 2010, Hong Kong.

[5]Anu Bala, Munish Bansal, Jagpreet Singh, 2009, "Performance Analysis of MANET under Blackhole Attack," First International Conference on Networks & Communication, IEEE.

[6]Ei Ei Khin, Thandar Phyu, May-2014, "Impact Of Blackhole Attack On AODV Routing Protocol," International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2.

[7]Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Nov-2007, "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.

[8]Charles E Perkins, E M Royer, Sameer R. Das, 2001, "Ad hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, draft-ietf-manetaodv- 09.txt.

[9]Rajdipsinh Vaghela, Divyesh Yoganand, Monika Changela, December 2012, "A Survey on Approaches towards the Black Hole Attack in Manet," Volume: 1, Issue: 12, ISSN - 2250-1991.

[10]Romina Sharma, Rajesh Shrivastava, 3 March 2014 "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network," IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3.

[11]Durgesh Kshirsagar and Ashwini Patil, 4-6 July, 2013, "Blackhole attack prevention and detection by real time monitoring," 4th ICCCNT.

[12]Sakshi Jain, 2014, "Review of Prevention and Detection Methods of Black Hole Attack in AODV- based on Mobile Ad Hoc Network," International Journal of Information and Computation Technology, ISSN 0974-2239 Volume 4, Number 4, pp. 381-388.

[13]Monika Y. Dangore, Santosh S. Sambare, 15-16 November, 2013, "Detecting and overcoming Blackhole attack in AODV protocol," Internation conference on cloud & ubiquitous computing, IEEE.

[14]Pooja Jaiswal, Dr. Rakesh Kumar, October 2012, "Prevention of Blackhole attack in MANET," IRACST.

[15]N.H.Mistry, D.C.Jinwala, M.A.Zaveri, July 2009, "Prevention of Blackhole Attack in MANETs," In Proceedings of EPWIE- 2009, Gujarat, India, pp 89-94.

[16]Prof. Dhaval Thakar, Prof. Nainesh Prajapati, Oct 2013, "A Modified AODV – Algorithm for prevention of Black hole attack in Mobile Adhoc Networks," International Journal of Conceptions on Electrical and Electronics Engineering, Vol. 1, Issue 1, ISSN: 2345 – 9603.

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

[18]Ashwani Singh, Mohd. Haroon, Mohd. Arif, October-2014, "Routing Misbehavior in Mobile Ad Hoc Network," Volume-4, Issue-5, ISSN No.: 2250-0758, International Journal of Engineering and Management Research, Page Number: 31-36.

[19]Mohammad Al-Shurman, Seong-Moo Yoon, Seungjin Park, 2-3 April, 2004, "Black Hole Attack in Mobile Ad Hoc Networks," ACMSE'04, Huntsville, AL, USA.

[20]Akanksha Saini, Harish Kumar, 19-20 March, 2010, "Comparison Between Various Blackhole Detection Techniques In MANET," NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, India.

IJSER

Author Details:

Devottam Gaurav
M.Tech Scholar
Birla Institute of Technology
Noida-201301
U.P., India
gauravpurusho@gmail.com

Charu Wahi
Assistant Professor
Birla Institute of Technology
Noida-201301
U.P., India
charu@bitmesra.ac.in