A Survey on Techniques to Handle Black Hole Attack for AODV in MANET

Mr. Hardik N. Talsania
Lecturer
Department of Computer Engineering
R.C.T.I., Ahmedabad, Gujarat, India

Prof. Zishan Noorani
Assistant Professor
Department of Computer Engineering
L.D.C.E., Ahmedabad, Gujarat, India

Abstract

Providing proper security for MANETs with devices that can configure themselves without a strict intervention by network administrators is a challenging task. Due to its dynamic network topology and decentralized administration, AODV routing protocol in MANET is more susceptible to various attacks like Black Hole and Gray Hole, where a malicious node drops the packets it receives on purpose. This paper lists out and provides information about different techniques proposed by researchers to detect and/or mitigate black hole attack for AODV. The paper concludes with a summary of the techniques and the possibilities of future enhancements that can be done on one or more of the techniques mentioned.

Keywords: AODV, MANET, Black Hole Attack, SAODV, AOMSR, PBA, Packet Delivery Ratio, Throughput, End-to-end Delay

I. INTRODUCTION

There are 2 kinds of wireless networks: infrastructure-based & infrastructure-less. One of the examples of infrastructure-less network is MANET (Mobile Ad-hoc Networking) [9]. MANET's routing protocol locates routes between nodes and allows forwarding of data packets via the nodes of other network to destination [4]. Various challenges in routing of Mobile Ad-hoc Networks are found, some of them being dynamic topology, interference and lack of security mechanisms.

Two types of Ad-hoc routings algorithm are available: proactive and reactive routing algorithms. While, DSDV is a proactive routing algorithm, AODV & DSR are the examples of reactive routing protocols. AODV (Ad-hoc On-demand Distance Vector) is an on demand routing protocol, which establishes the path when it is needed [1].

A. Types of MANET Protocols:

The mobile ad hoc network (MANET) has three kinds of protocols: Proactive, Reactive and Hybrid protocols [16].

1) *Proactive Protocol:*

Proactive protocols are also known as table-driven protocols in which the nodes sustain and update the routing tables regularly even when there is no communication.

Examples: DSDV (Destination-Sequenced Distance Vector), OLSR (Optimized Link State Routing).

2) *Reactive Protocol:*

Reactive protocols or also called On-Demand Protocols are the ones in which the routes are discovered on the demand basis of the source node.

Examples: AODV (Ad-hoc On-demand Distance Vector), DSR (Dynamic Source Routing).

3) *Hybrid Protocol:*

Hybrid protocols have the combined characteristics of both the reactive and proactive protocols.

Example: ZRP (Zone Routing Protocol).

B. Types of Attacks in AODV:

Attacks can be mainly categorized into two types namely: Passive & Active Attack [5].

1) *Passive Attack:*

A passive attack is very hard to detect as it discovers valuable information by snooping on to the routing traffic without interrupting or manipulating the routing protocol [5].

2) *Active Attack:*

Malicious nodes launch an active attack to gain unauthorized access to the network by inserting fake packets or modifying the existing packet transmission.

Active attack can further be forked into external attacks and internal attacks [5].

1) External attacks are carried by the nodes that do not belong to the network. It causes congestion due to false/fake advertisements, false routing information [15].
2) Internal attacks are due to compromised nodes within the network. The compromised nodes participate in the network normally initially; as the communication goes on they act as malicious by performing some misbehavior action [15].

C. *Some Common Attacks in AODV:*

1) Black Hole:
In a black hole attack, a lethal node places itself between the communicating nodes by advertising a false optimum route to ambush the packets in the communication stream.

2) Replay:
An attacker in replay attack misuses the mobility feature in MANETs by resending previously recorded packet and causing other nodes in the network to store stale route in their routing tables.

3) Blackmail:
In this category of attacks vicious nodes attempt to blacklist legal nodes by cooking up false information which indicates that they are malignant.

4) Worm Hole:
Attackers keep the packets from reaching the destination node by always tunneling the packets between the malicious nodes.

5) Sink Hole:
Here a vicious module falsely proclaims itself as the destination to receive the entire network traffic. It then complicates the network by dropping these packets after making significant changes which inadvertently affects the network.

6) Sybil Attack:
In this type of attacks the lethal nodes create aliases of themselves to gain extravagant influence on the network.

II. BACKGROUND CONCEPTS

A. *AODV Routing Protocol in MANET:*

AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol that establishes a route on demand. In AODV, when a source wants to communicate with a destination, the source node broadcasts a RREQ (route request) message. When any intermediate node or destination node has a route to the destination node, it sends back RREP (route reply) message to the source node. If there is breakage in the link between two nodes in this route, a RERR (route error) is sent, informing the source about the lost link [14]. The routing discovery in AODV is shown in the Figure 1 below.

AODV is capable of both unicast and multicast routing. Along with source and destination address, RREQ also contains the most recent sequence number for the destination. The node that has received the request packet will reply if it is the destination or it has a route towards the destination having higher sequence number. Otherwise, it rebroadcasts the RREQ to other nodes in the network. The communication starts once the source node receives the reply packet.

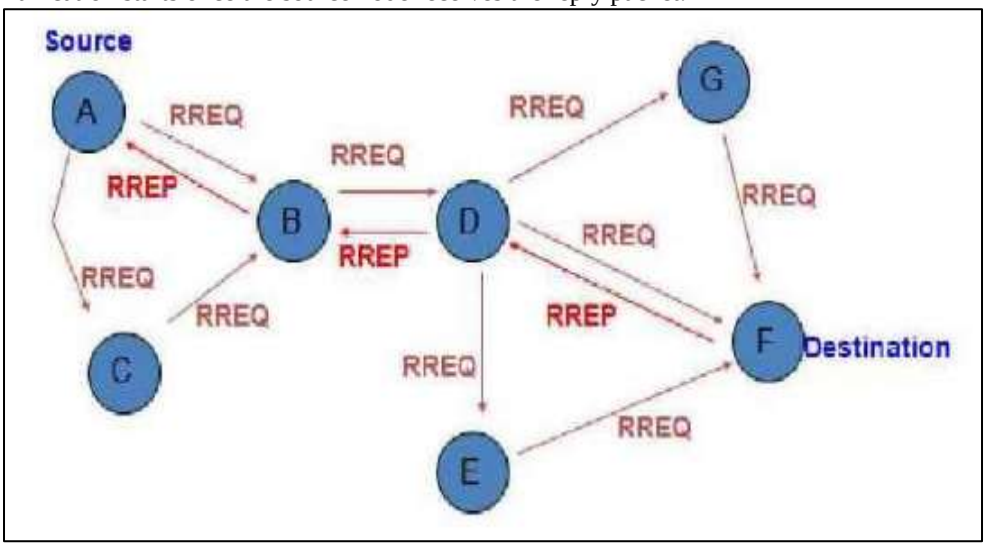

Fig. 1: Routing Discovery in AODV

Sequence number plays a key role in AODV protocol. If source node receives a reply packet (RREP) that has highest sequence number with small hop count, it updates its routing information and starts using better route. AODV is a routing protocol, hence that deals with routing table management. Routing table entry includes following fields: Destination IP Address, Destination sequence number, Next hop IP address, Life time, Hop count [15]. The Routing Table for a node in an AODV network is shown in the Figure 2 below.

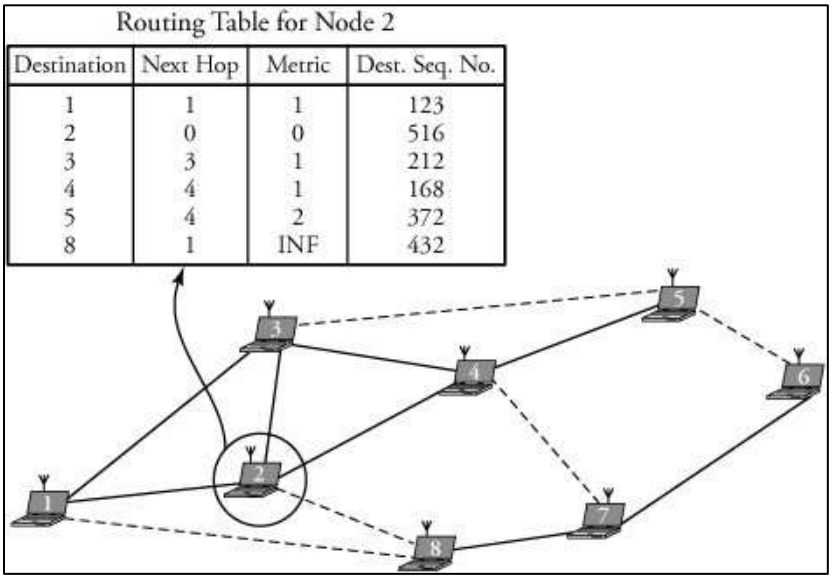

Fig. 2: Routing Table in AODV

B. Black Hole Attack in AODV:

The black hole attack in mobile ad hoc network can be classified into numerous types according to the strategy accepted by the malicious node to commence the attack [16]. Black hole attack is a well-known attack in wireless ad hoc networks that can occur especially in case of on-demand routing protocols such as AODV. It is an attack in which a malicious node acquires route from a source node to a destination node by falsification of sequence number or hop count or both. A black hole node builds a route reply with fake larger sequence number and shorter hop count (usually 1) of a routing message in order to forcefully acquire the route and then listen or drop all data packets that pass through that route [11]. Demonstration of black hole attack in an AODV network can be seen in the Figure 3 below.

Here, Node3 is a malicious node on the network. When it receives the RREQ message, it replies immediately to the source node (Node1) with its RREP message without following the routing protocol. The black hole's RREP message includes S_Addr and D_Addr values that are copied from the RREQ message, the lowest Hop_Count (shortest path), and the highest DSN value [17]. To instigate the black hole attack, the primary step for a malicious node is to find a way that permit it to get mixed up in the routing/forwarding path of data/control packets [16].

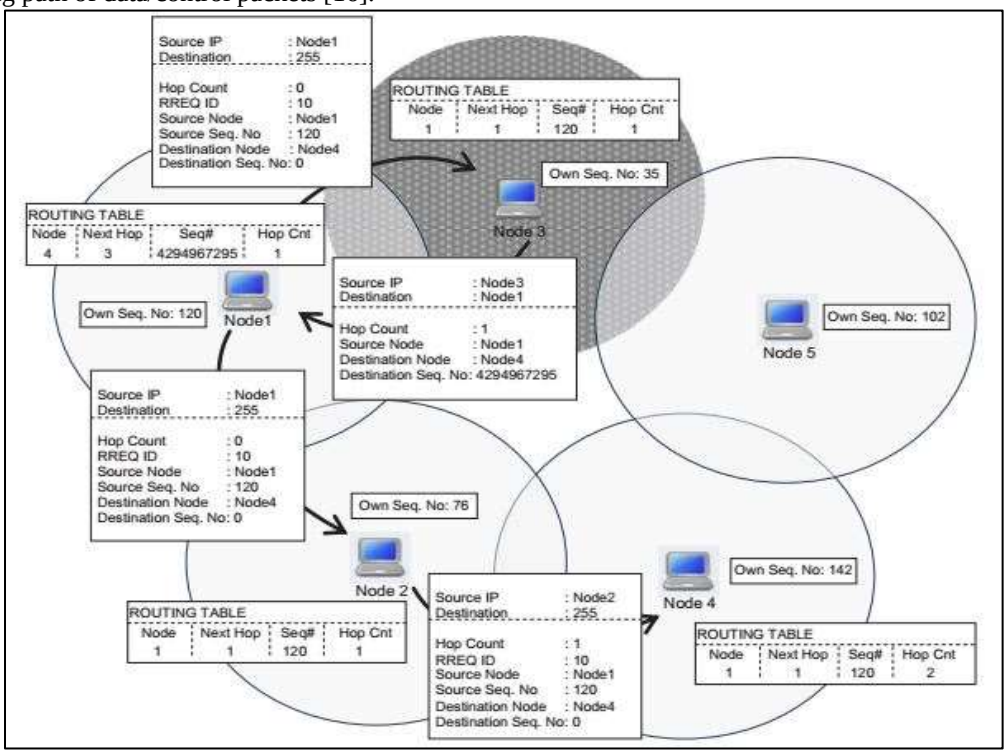

Fig. 3: Black Hole Attack Demonstration [17]

III. LITERATURE SURVEY

As a part of literature review, existing research and survey papers were studied related to research area of the thesis.

Table – 1
Summary of Literature Survey

Sr. No.	Title of Paper	Authors	Year & Publication	Traffic & Nodes	Technique Used	Result / Performance
1	Interception of Black- Hole Attacks in Mobile AD-HOC Networks	Balachandra et al. [5]	2016 IEEE	Constant Bit Rate (CBR); 20-100 Nodes	SAODV (Secure-AODV); Watch Dog Mechanism	PDR: 99.66% Throughput: 50.60% E-E Delay: 21.77%
2	Detection As Well As Removal Of Black hole And Gray hole Attack In MANET	Neha Sharma et al. [3]	2016 IEEE	CBR; 50 Nodes	Fake RREQ; Promiscuous Mode	PDR: 37.5 – 25.0 for 1 – 4 black hole nodes respectively
3	Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks	Ashish Kumar Jain et al. [9]	2015 IEEE	CBR; 50 Nodes	Ignoring first RREP	PDR: 92.86 Throughput: 142.63 E-E Delay: 1.55 Routing Overhead: 70.46
4	An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET	Dhaval Dave et al. [6]	2014 IEEE	CBR; 10-50 Nodes	Ad-hoc On-demand Multipath Secure Routing (AOMSR); Permutation-based Acknowledge-ment (PBAck)	Comparative increase in throughput and decrease in routing overhead
5	AODV Based Black-Hole Attack Mitigation in MANET	S. Banerjee et al. [12]	2014 Springer	Not given	Higher Seq. No. than the last received	Minimal overhead; Detects all types of Black Hole Nodes
6	Mitigation Algorithm against Black Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET	Anishi Gupta [8]	2015 IEEE	TCP; 20-80 Nodes	Real-time Monitoring AODV (RTMAODV); Promiscuous Mode; Use of fvalue & rvalue counters & threshold	Increased performance in terms of PDR & E-E Delay as compared to the affected AODV network
7	Detection of Single and Collaborative Black Hole Attack in MANET	Satish M et al. [2]	2016 IEEE	15-50 Nodes	Fake RREQ, seq. no. & next hop; Applicable to Single & collaborative black hole nodes	70% deacrease in E-E Delay; 12% increase in throughput; 45% increase in PDR
8	Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks	Muhammad Imran et al. [11]	2015 Springer	UDP-CBR; 50 Nodes	Use of special DPS Nodes in Promiscuous Mode & Threat_Value Counter	13-47% decrease in Packet Drop Rate

As it is found that there is a scope of improvement in the performance of some of the existing systems, a new system can be proposed by combining some of these techniques to increase the efficiency of the network in terms of both PDR and throughput.

IV. CONCLUSION

It can be concluded that various techniques have been proposed to detect and prevent black hole attack in AODV, however, performance of the affected network can be improved by proposing new techniques.

Also, the results of the techniques can be measured in terms of the parameters other than the one listed, and combination of some techniques is believed to increase the performance of the network.

REFERENCES

[1] R. Kumar, A. Quyoom and Devki Nandan Gouttam, "To mitigate black hole attack in AODV," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 307-311.
[2] Sathish M, Arumugam K, S. N. Pari and Harikrishnan V S, "Detection of single and collaborative black hole attack in MANET," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 2040-2044.
[3] N. Sharma and A. S. Bisen, "Detection as well as removal of black hole and gray hole attack in MANET," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 3736-3739.
[4] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using trust with AODV in MANET," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 470-474.
[5] Balachandra and N. P. Shetty, "Interception of black-hole attacks in mobile AD-HOC networks," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-5.
[6] D. Dave and P. Dave, "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET," 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, 2014, pp. 1690-1696.

[7] S. Dhama, S. Sharma and M. Saini, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2993-2996.
[8] A. Gupta, "Mitigation algorithm against black hole attack using Real Time Monitoring for AODV routing protocol in MANET," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 134-138.
[9] A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-6.
[10] A. Jain, U. Prajapati and P. Chouhan, "Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-4.
[11] Imran M., Khan F.A., Abbas H., Iftikhar M. (2015) "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks". In: Garcia Pineda M., Lloret J., Papavassiliou S., Ruehrup S., Westphall C. (eds) Ad-hoc Networks and Wireless. ADHOC-NOW 2014. Lecture Notes in Computer Science, vol 8629. Springer, Berlin, Heidelberg.
[12] Banerjee S., Sardar M., Majumder K. (2014) "AODV Based Black-Hole Attack Mitigation in MANET". In: Satapathy S., Udgata S., Biswal B. (eds) Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. Advances in Intelligent Systems and Computing, vol 247. Springer, Cham.
[13] Jaisankar N., Saravanan R., Swamy K.D. (2010) "A Novel Security Approach for Detecting Black Hole Attack in MANET". In: Das V.V. et al. (eds) Information Processing and Management. Communications in Computer and Information Science, vol 70. Springer, Berlin, Heidelberg.
[14] N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection mechanism," 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, 2015, pp. 1-4.
[15] K. Madhuri, N. K. Viswanath and P. U. Gayatri, "Performance evaluation of AODV under Black hole attack in MANET using NS2," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-3.
[16] H. P. Singh and R. Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol," 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2014, pp. 1-8.
[17] S. Tan and K. Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-Based MANETs," 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, 2013, pp. 1159-1164.
[18] Lo NW., Liu FL. (2013) A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET. In: Juang J., Huang YC. (eds) Intelligent Technologies and Engineering Systems. Lecture Notes in Electrical Engineering, vol 234. Springer, New York, NY.