

A Survey on Detecting Black Hole Attack in MANETs

Nikhil G. Patel¹ Ms. Avani Dadhaniya²

^{1,2} Department of Computer Engineering

^{1,2} L.D.R.P Institute Of Technology and Research, Gandhinagar, India

Abstract— Mobile Ad hoc Network (MANET) is a collection of mobile nodes that dynamically form a temporary network without infrastructure. It has many numbers of applications mainly in the areas of Sensor Networks (SN), medical, military and rescue operations. Routing is an important component in mobile ad hoc networks and it has several routing protocols, which are affected from different attacks. Ad hoc on demand Distance Vector (AODV) is one of the most suitable routing protocols for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is called as black hole attack. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack. In this paper, we have surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks.

Key words: MANETs, AODV, Malicious node, Sequence Number

I. INTRODUCTION

MANETs being an emerging technological field is an active area of research and has found usage in a variety of scenarios like emergency operations, disaster relief, military service and task forces. Providing security to the nodes and their data Communication in such scenarios is critical. A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network [1, 3]. Mobile Ad hoc Network (MANET) [1] is a set of mobile devices like laptops, PDAs, smart phones which communicate with each other over wireless links without a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network using single hop or multi hop communication. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks,

including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [11, 12, 13]. The characteristics of MANET like dynamic topology, lack of fixed infrastructure, vulnerability of nodes and communication channel, lack of traffic concentration points, limited power, computational capacity, memory, and bandwidth make the task of achieving a secure and reliable communication more difficult. Attacks like sleep deprivation, jamming transmission channel with garbage packets, Black hole, Grey hole, Wormhole and DoS. The selfish nodes may not participate in routing and forwarding packets leading to loss of packets. This paper is a survey of different Intrusion Detection System proposed for MANETS based on their architecture.

II. ROUTING PROTOCOLS IN MANETS

Routing is the process of information exchange from one host to the other host in a network [4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself [3].

Different Strategies:

Routing protocol for ad-hoc network can be categorized in three strategies.

- 1) Pro- active routing protocol.
- 2) Re- active routing protocol.
- 3) Hybrid protocols

A. Proactive (table-driven) Routing Protocol

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbor's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol [5] and Optimized link state routing (OLSR) protocol [6].

B. Reactive (on-demand) Routing Protocol

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare

to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: - Ad hoc on-demand distance vector (AODV) [7] and Dynamic source routing (DSR) [8] protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [9] and Temporally-ordered routing algorithm (TORA) [10].

III. AD HOC ON DEMAND ROUTING PROTOCOL (AODV)

AODV combines some properties of both DSR and DSDV. It uses route discovery process to cope with routes on-demand basis. It uses routing tables for maintaining route information. It is reactive protocol. It doesn't need to maintain routes to nodes that are not communicating. AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbor nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause bypassed node to allocate route table entries for reverse route.

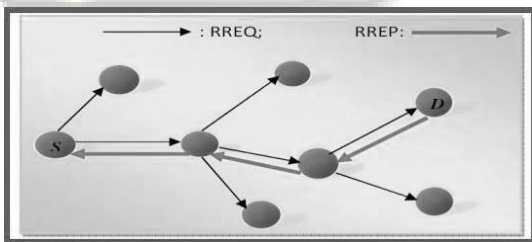


Fig. 1: AODV routing protocol with RREQ and RREP Message

The destination node unicasts a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route. Figure (Fig.1) shows, AODV routing protocol with RREQ and RREP message [14].

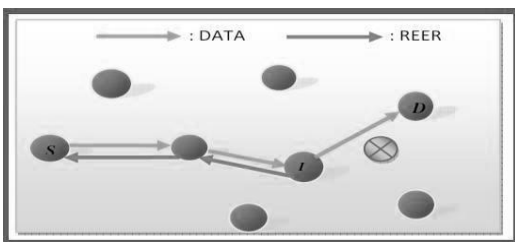


Fig. 2: AODV routing protocol with RERR message

For route maintenance nodes periodically send HELLO messages to neighbour nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node. When a node receives a RERR message it will indicate a new source discovery process. Figure (Fig.2) shows AODV routing protocol with RERR message [14].

IV. ATTACKS ON MANETS

I will now categorize and describe possible attacks on MANETs. Most descriptions are intentionally abstract as I do not want to analyze specific protocols but list general attacks on all kinds of MANETs and protocols.

- 1) Passive Attacks
- 2) Active Attacks

A. Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard [16, 17]. There are some attacks which is particular to the passive attack brief details are given below:

1) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication [17]. The information may contain the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

2) Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to anticipate important information such as a source, destination, and source-destination pair.

B. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks [16]. There are some attacks which is particular to the passive attack brief details are given below:

1) Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole [18]. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole [17].

2) Black hole attack

In black hole attack [19] [20], a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [21].

3) Byzantine attack

A compromised with set of intermediate, or intermediate nodes that working alone within network carry out attacks such as creating routing loops, forwarding packets through non -optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network [18].

4) Gray-hole attack

This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability [18].

5) Jamming attack

Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets [17].

Now we are focusing on detecting the Black hole Attack when routing the information from sender to receiver. So here we describe the entire details of Black hole Attack in below.

V. BLACK HOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [22]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address [23].

The method how malicious node fits in the data routes varies. Fig. 3 shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

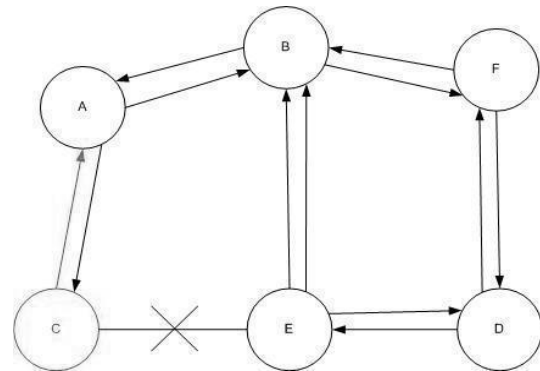


Fig. 3: Black Hole Problem

A. Black Hole Attacks are classified in to two categories [24]

1) Single Black hole Attack

In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node.

2) Collaborative Black hole Attack

In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

B. Black hole Attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

1) Internal Black hole Attack

This type of black hole attack [25] has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

2) External Black hole attack

External attacks [25] physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points:

- 1) Malicious node detects the active route and notes the destination address.
- 2) Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to

lowest values and the sequence number is set to the highest value.

- 3) Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- 4) The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
- 5) The new information received in the route reply will allow the source node to update its routing table.
- 6) New route selected by source node for selecting data.
- 7) The malicious node will drop now all the data to which it belong in the route.

VI. COMPARISON OF VARIOUS SOLUTIONS TO BLACK HOLE ATTACK

See Appendix A: Comparison of Various Solutions on Black Hole Attack [26].

VII. CONCLUSION

In this paper overview of MANET has been presented first than we define routing protocols in MANET, after we analyze detection of black hole attack in AODV. This method is very simple and efficient approach for defending the AODV protocol against. Black Hole attacks. A Black Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs with their defects is presented. Based on these performance comparisons, it can be concluded that Black Hole attacks affect network negatively. Hence, there is need for perfect detection mechanisms. The detection of Black Holes in ad hoc networks is still considered to be a challenging task. Future work, to find an effective solution to the black hole attack in AODV protocol.

REFERENCES

- [1] S. R. Murthy and B .S .Manoj,” Ad Hoc Wireless Networks”, Pearson Education, 2008.
- [2] Y. Xiao, X. Shen, and D.-Z. Du,” A Survey on Intrusion Detection in Mobile Ad Networks”, pp. 170 – 196 c 2006 Springer.
- [3] Amit Shrivastava, Aravinth Raj Shanmogavel, Avinash Mistry , Nitin Chander ,Prashanth Patlolla, Vivek Yadlapalli “Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols”.
- [4] Humayun Bakht, “Computing Unplugged, Wireless infrastructure, Some Applications of MANET”, issue200410/00001395001.html, April-2003.
- [5] Perkins CE, Bhagwat P (1994),”Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, Paper presented at the ACM SIGCOMM’94 Conference, London, United Kingdom, August 31- September 2, 1994.
- [6] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) ,“Optimized Link State Routing Protocol for Ad Hoc Networks”, Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001.
- [7] Perkins CE, Royer EM (1999),”Ad-hoc On-Demand Distance Vector Routing”, Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25-26 February 1999.
- [8] Johnson DB, Maltz DA (1996),”Dynamic Source Routing in Ad Hoc Wireless Networks”, In: Imielinski T, Korth H (eds) Mobile Computing, Vol 353. Kluwer Academic Publishers, pp. 153–181.
- [9] Haas ZJ, Pearlman MR, Samar P (2002),” The zone routing protocol (ZRP) for ad hoc networks”, IETF Internet Draft.
- [10] Park V, Corson S (1998),” Temporally-Ordered Routing Algorithm (TORA)”, Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group.
- [11] M. G. Zapata, “Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing,” ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.194.
- [12] Y. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’02), pp. 3-13, June 2002.
- [13] Y. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks,” Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom’02), pp. 12-23, September 2002.
- [14] Dr. S. Tamilarasan, “Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 1 Issue 5, July – 2012.
- [15] Martin Schütte, “Detecting Selfish and Malicious Nodes in MANETs”.
- [16] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET”-Internet Communication International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).
- [17] Pradip M. Jawandhiya MANGESH M. GHONGE ,DR. M.S.ALI ,PROF. J.S. DESHPANDEA “Survey of Mobile Ad Hoc Network Attacks” International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.
- [18] Priyanka Goyal, Sahil Batra, Ajit Singh,” A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.
- [19] E. A .Mary Anita and V. Vasudevan, “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining”, International Journal of Computer Applications (0975 – 8887) Vol. 1, Issue 12, pp. 21-28, 2010.
- [20] Umang S, Reddy BVR, Hoda MN, “ Enhanced Intrusion Detection System for Malicious Node

Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption”, IET Communications Vol.4, Issue17, pp2084–2094. Doi: 10.1049/ietcom. 2009.

- [21] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.
- [22] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, ”A Novel Approach for Gray Hole and Black Hole Attacks in Mobile Ad-hoc Networks”, 2012 Second International Conference on Advanced Computing & Communication Technologies.
- [23] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006.
- [24] Himani Yadav, Rakesh Kumar,” A Review on Black Hole Attack in MANETs”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp.1126-1131.
- [25] Irshad Ullah, Shoaib Ur Rehman, “Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols”.
- [26] Sarita Badiwal, VandnaVerma,” Survey of IDS in MANET against Black Hole Attack”, International Journal of Application or Innovation in Engineering & Management (IJAEM) Volume 2, Issue 5, May 2013 ISSN 2319 – 4847.

Akanksha Jain	Trust based	Single black	Minimum	Poor	AODV
---------------	-------------	--------------	---------	------	------

Table. 1: Comparison of available solutions to black hole attacks on AODV

VIII. APPENDIX A

Technique proposed by	Techniques	Type Of Black hole attack	Merits	Demerits	Routing Protocol
Payal N. Raj1 And Prashant B. Swadas2, 2008	Compares The RREP Sequence numbers with threshold value using dynamic learning method	Single And multiple black hole	Increases PDR With Minimum Increase in Average end-to-end delay	Higher Routing overhead and can't detect cooperative black holes	AODV
Y.Zhang And W.Lee,2000	Introduces the CREQ and CREP to avoid black hole	Single Black hole	Low cost	Time delay and false positives	AODV
Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Nov. 2007	A New detection method based on dynamically updated training data.	Single Black hole	Detection rate And false positive rate improve	Network delay	AODV
Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, Sept. 2010	An Anti-Black Hole Mechanism (ABM) using IDS	Multiple black holes	High detection rate	Time delay	AODV