International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 2 February 2018

A Review - Detection of Black-Hole Attack in AODV with MANET Scenario

Jaya Kushwah[1], Deepika Jain[2], Dr. Harish Patidar[3]
Research Scholar, LNCT, Indore[1]
Assistant Professor (CSE), LNCT, Indore[2]
HOD (CSE), LNCT, Indore[3]
jiyakushwah0@gmail.com[1], Deepikajainbpl@rediffmail.com[2], Harish.cs@lnctindore.com[3]

Abstract: *In current years mobile ad hoc network has a superior impact on wireless communication network. In MANET, each and every node acts as a router to establish a route and transfer data by means of various hops. MANET is more vulnerable to network security problem. When a source wants to transfer data to destination, packets are transferred through the router nodes, thus, searching and establishing a route from a sender node to a receiver node is a challenging task in MANET. Routing is an important task in MANET and for this routing it has several routing protocols. AODV is one of the most suitable routing protocols for the MANET and it is more vulnerable to black hole attack by the attacker nodes, an Attacker node that incorrectly sends the route reply (RREP) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is black hole attack. In the case of greater than one attacker nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attacker's node. There are various of efforts have been made to defend against black hole type malicious behavior, but no one a single solution looks most promising to prevent against black hole attack. In this paper surveyed and compared the existing solutions to black hole attacks on AODV protocol.*

Keywords: *MANET, AODV, Malicious behavior, single black hole and Cooperative black hole attack.*

1. INTRODUCTION

Wireless technologies such as Bluetooth or the 802.11 standards enable mobile devices to establish a Mobile Ad-hoc Network (MANET) by connecting dynamically through the wireless medium without any centralized structure [1]. MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets [2], this multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions. MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. Thus operations in MANET introduce some new security problems in addition to the ones already present in fixed networks.

According to the criterion that whether attackers disrupt the operation of a routing protocol or not, attacks in MANET can be divided into two classes: passive attacks and active attacks [3,4,5]. In a passive attack, the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. In an active attack, however, these attacks involve actions performed by adversaries, modification and deletion of exchanged data to attract packets destined to other nodes to the attacker for analysis or just to disable the net-work. Some typical types of active attacks can usually be easily performed against MANET, such as, Denial of Service (DoS), impersonation, disclosure, spoofing and sleep deprivation. Most important networking operations include routing and network management. Routing protocols can be

divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include DSDV, WRP. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes DSR, AODV and ABR. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc net-work.

2. SECURITY ISSUES

Security in Mobile Ad-Hoc Networks is an important concern for the network functioning. MANET often experience different security attacks because of its following features: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [6, 7]. These features are explained below:

- **Dynamically changing network topology**: Nodes are free and they can move arbitrarily. So the network topology changes unpredictably and frequently, which results in change in routes, frequent partitioning of network and loss of packets.
- **Lack of centralized monitoring**: MANETs does not have any established infrastructure and centralized administration. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management.
- **Cooperative algorithms**: In MANET the routing algorithms need to have trust between their neighboring nodes.
- **Bandwidth constraint**: Wireless links have lower capacity as compared to the infrastructures networks.
- **Limited physical security**: Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.
- **Energy constrained operation:** The only energy means for the mobile nodes in Ad-Hoc network is the battery power. And they also have a limited storage capacity and power.

3. BLACK HOLE ATTACK IN AODV

In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source node then starts to send out its data packets to the black hole trusting that these packets will reach the destination.

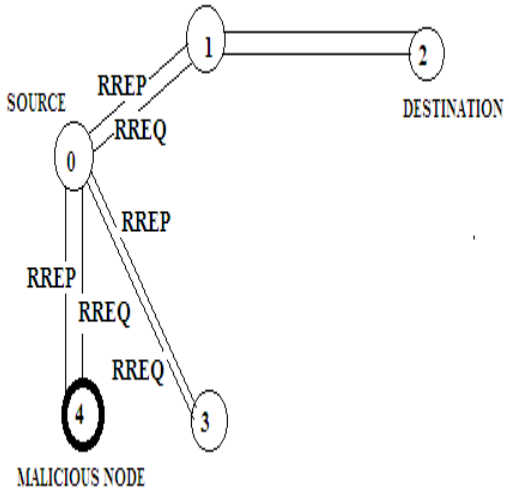

Fig.1 RREQ Broadcast

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in fig.1, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1,3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. A malicious node drops all data packets rather than forwarding them on. [8].

4. LITERATURE REVIEW

To combat the black hole attack from the wireless ad hoc network, a lot of work has been done in this field. Various researchers implemented or suggested different techniques to combat it. In this paper a literature study of the previous work is described below:

Nishu kalia, Kundan Munjal [9], present a technique which uses the Fuzzy based control, to detect and mitigate type of attack, namely malicious packet dropping, in wireless ad-hoc network. A malicious node in a network promises to forward packets but drop or delay them. In this technique, every node in the mobile ad-hoc network sends the route request and waits for the acknowledgment. The requesting node analyzes the behavior of unknown node using fuzzy technique and on the basis of result the node takes this node in the route of the packet. Subsequently, states of the nodes can also be utilized by the routing protocol to bypass those malicious nodes. Their method shows that in a dynamically changing network, the technique can detect most of the malicious nodes with a relatively high positive rate. The packet delivery rate in the MANET can also be increased accordingly.

The work in [10], proposed a method based on PL2 whose modification has been done in AODV protocol for ensuring the security against the Black hole attack using NS2 Simulation. This method is based on time and neighborhood parameters. This method first check for malicious activity exists, and then starts detect and remove the Black hole nodes.

In [11], analyzed the effect of black hole attack which is one of the feasible attacks in ad hoc networks. In the first phase they simulate the effect of black hole nodes in the network for AODV routing protocol. In the second phase they have modified AODV routing protocol by tuning the parameters in the RREP packet for detection of the Black hole nodes. They have done simulations by changing the various parameters like number of nodes, mobility, black hole nodes using NS2. They have compared the results with traditional AODV for simulation matrix like PDR and End-to-End delay.

In Ref. [12] proposed a neighborhood-based and routing recuperation method. This recognition method based on a neighborhood-based method to distinguish the black hole attack, and a routing recovery protocol to put together the correct path [12][13]. This method is employed to recognize the nodes which are unconfirmed .In this method, source node sends a alter Route Entry control packet to target node to refurbish routing path in the recovery protocol. In this system, not only an inferior discovery time and privileged throughput are attained, but the precise detection possibility is also achieved. The foremost restriction of this method is that it becomes useless when the attacker agrees to counterfeit the fake reply packets.

A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol [14], Harsh Pratap Singh, Rashmi Singh describe clock synchronization technique, in this paper, they proposed a technique in which broadcast synchronization (BS) and relative distance (RD) technique of clock synchronization is used to thwart the black hole nodes. In this internal and external clock node evaluate with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malicious. This method can easily identify and avoid the block-hole node.

5. COMPARISON OF SINGLE BLACK HOLE ATTACK DETECTION SCHEMES

Schemes	Routing Protocol	Detection Type	Limitations
Neighborhood Based and Routing Recovery	AODV	Single Detection	Failed when attackers cooperate to forge the fake reply packets
Repeated next hop node	AODV	Detect single Black hole node	Work same as AODV in absence of repeated next hop node, detect Black hole attack only up to single level
DRI table and cross checking using FREQ and FREP	AODV	Collaborative Black Hole	5-8% more Communication overhead of route Request
MAC and Hash based PRF Scheme	AODV	Collaborative Black Hole	The malicious node is able to forge a

			fake reply to dodge the detection
Difference in Sequence number	AODV	Detect single Black hole node	Simulations to analyze performance based on other parameters

6. CONCLUSION

In this paper we studied the information about the network, concept of wireless network, why use of wireless network. We also see the introduction about MANET and various features of MANET. In this paper we have brought out few aspects on the Black hole Attacks observed in MANETS. Then we further elaborated on the AODV Protocol and how Black Hole attacks occur in the network. The study here shows different modified versions of AODV algorithms which have been proposed and implemented to prevent and detect black hole attack. A comparison table shows the performance of methods, Used Routing Protocol, Type of black hole attack and their limitations.

REFERENCES

[1] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56, no. 2, pp. 940–965, October 2011.
[2] M. Zhang and P. H. J. Chong, "Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility," in Proc. of IEEE Communications Society conference on Wireless Communications & Networking, Budapest, Hungary, 2009, pp. 2450-2455.
[3] Deng Hongmei, Li Wei and Agrawal D.P. (2002) IEEE Communications Magazine, 70-75.
[4] Hongmei Deng, Wei Li, and Agrawal D.P. (2002) IEEE Communications Magzine, 40(10), 1704-1710.
[5] Papadimitratos P. and Haas Z. Communication Networks and Distributed Systems Modeling and Simulation.
[6] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp 338–346.
[7] Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93 B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.
[8] Ranjeet Suryawanshi,Sunil Tamhankar," Performance Analysis and Minimization of Blackhole Attack in MANET" IJERA, july-August 2012.
[9] Nishu kalia, Kundan Munjal "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.
[10] Vasanthavalli.S, R.Bhargava Rama Gowd,S.Thenappan "Peruse Of Black Hole Attack and Prevention Using AODV on MANET", International Journal of Innovative Research in Science Engineering and Technology,Vol. 3, Issue 5, May 2014, ISSN: 2319-8753.
[11] Dhaval Thakar, Nainesh Prajapati "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, Oct 2013; ISSN: 2345 – 9603.
[12] Fan-Hsun Tseng, Li-der chou and Han-chieh chao, "A survey of black hole attack in wireless mobile adhoc networks", springer journal 2011.
[13] Sun B,Guan Y and Pooch UW, "Detecting Black hole Attack in Mobile Adhoc Networks" ,Paper presented T 5th European Personal Mobile Communication Conference, April 2003.
[14] Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol", International Conference on Electronics and Communication Systems (ICECS) 2014 , Page(s):1 - 8 Print ISBN:978-1-4799-2321-2.
[15] Sun B, Guan Y, Chen J, Pooch UW "Detecting Black-hole Attack in Mobile Ad Hoc Network"s. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
[16] Al-Shurman M, Yoo S-M, Park S "Black Hole Attack in Mobile Ad Hoc Network"s. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.
[17] Tamilselvan L, Sankaranarayanan V "Prevention of Blackhole Attack in MANET". Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.
[18] Djenouri D, Badache N "Struggling Against Selfishness and Black Hole Attacks in MANETs". Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6, 2008.
[19] Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M "Developing Attack Defense Ideas for Ad Hoc Wireless Networks". Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.
[20] 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.

[21] Weerasinghe H, Fu H "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation". Paper presented at the Future Generation Communication and Networking, Jeju- Island, Korea, 6-8 December 2007.