ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
South Asian Research Journal of Engineering and Technology
Abbreviated Key Title: South Asian Res J Eng Tech

| Volume-3 | Issue-6 | Nov-Dec -2021 | **DOI: 10.36346/sarjet.2021.v03i06.005**

Review Article

Black Hole Attacks Using AODV in MANET

S. Jagadeesh Soundappan[1*], Shankar Ramamoorthy[1], Ramandeep Singh[2]

[1]Department of CSE, BGIET, Sangrur, Punjab, India
[2]Department of EE, BGIET, Sangrur, Punjab, India

***Corresponding Author**
S. Jagadeesh Soundappan

Article History
Received: 27.11.2021
Accepted: 22.12.2021
Published: 30.12.2021

Abstract: Ad-hoc networks are emerging technology, due to their spontaneous nature, are frequently established insecure environments, which makes them vulnerable to attacks. These attacks are launched by participating malicious nodes against different network services. Ad hoc On-demand Distance Vector routing (AODV) is a broadly accepted network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper, a review on different existing techniques for detection of pooled or co-operated black hole attacks with their defects is presented.

Keywords: Distance Vector routing, Mobile Ad hoc Network, technology, attack.

1 INTRODUCTION

A MANET is similar to a set of mobile hosts that fulfils primary networking purposes not having the help of a permanent structures and facilities. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Security in MANET is a required component for necessary network purposes like packet forwarding and routing: network operation can be easily put in danger if countermeasures are not embedded into basic network functions at the primary stages of their design. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at centre of the security problems that are particular to ad hoc networks. As opposed to dedicated nodes of a traditional network, the nodes of an ad hoc network cannot be depending for the correct execution of serious network functions. However, similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [1]. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years. Before the development of any security measure to secure mobile ad hoc networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some common attack issues, researchers might have a better understanding of how mobile ad hoc networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them. The purpose of this study is to investigate some of the important issues that might be related to security attacks in mobile ad hoc networks and some of the existing detection and mitigation schemes. In Section II, we see how attacks against the ad hoc networks may vary depending upon in which environment the attacks are launched, what communication layer the attacks are targeting, and what level of ad hoc network mechanisms are targeted. After considering these three variations, it is also important to investigate the characteristics of attacks against the ad hoc networks. This topic explained in Section III. In this paper, we give a special attention to attacks that could be launched against the routing protocols [2]. We identified that most of the attacks against ad hoc networks routing protocols are actually launched by exploiting the routing messages.

2 Related Studies

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in [4, 7] many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of trade-offs between effectiveness and efficiency. Some solutions in [4, 7, 12] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol. The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations.

3 Classification of Routing Protocol

Since MANETs has been in an active research area and in recent years many routing protocols have been introduced. A routing protocol specifies the communication which is carried out between the routers. The choice of that route selection is done by the routing algorithm. These main routing protocols are divided into 3 categories-

- Reactive protocols/On-demand,
- Proactive protocols/Table driven,
- Hybrid protocols.

A. Reactive Protocols

Reactive protocols also called as on demand driven protocols because they discover route only when it is on demand. It only establishes the route when source node in the network wants to send a message or a packet to destination node. The main thing of this protocol is that it reduces routing table when it is overflow but the bad thing is that longer delay has been seen as it is on demand The example of this type of protocol are DSR (dynamic source routing), AODV (ad hoc on demand distance vector routing), LAR (location aided routing), TORA (temporally ordered routing algorithm).

1. **Ad-Hoc on Demand Distance Vector Protocol (AODV):** AODV is commonly used reactive protocol in MANET. It establishes a route to a destination only on demand i,e node does not discover and maintain route until it demand. It is also a distance-vector routing protocol. AODV uses three main messages to determine a route they are RREQ, RREP, and RERR as follows: Route Request Message (RREQ): When a source node wants to communicate with another node, but does not have a route to reach that node Source node broadcasts a route request (RREQ) packet to all of its neighbors. The source creates an RREQ packet contains the source node IP address, current sequence number, destination IP address, last known destination sequence number, a broadcast ID, which is incremented with each RREQ and a Hop Count field. Route Reply Message (RREP): If a node receives an RREQ packet and it has a route to the target destination, then it unicast a route reply packet (RREP) to the neighbor that sent the RREQ packet. route reply message packet for the source include IP address, sequence number & hops to source and IP of neighbor from RREQ received Route Error Message (RERR): When the packet is not reached to the destination node or the link break happens then the host delete the route from the routing table and send the route error (RERR) message to the corresponding neighbors.
2. **Dynamic source Routing (DSR):** It is a reactive protocol that generates a route on demand using source routing protocol. In Dynamic Source Routing, each source determines the route to be used in transmitting its packets to selected destinations. This protocol floods a route request message in the network to establish a route and there are two main components, called Route Discovery and Route Maintenance.

B. Proactive Protocol

Proactive protocols are also called as table driven routing protocol because they maintain the routing table of the entire network. In proactive each node has to maintain its tables for storing routing information and also update the table i,e changes is done whenever the network changes. If any changes in topology as each node will send a broadcast message to entire network so it will affect the routing table for maintaining the routing entries. For large network proactive routing protocol not be suggested because for each node maintaining the table causes more bandwidth consumption and overload to routing table .the examples of proactive routing protocol are DSDV (destination sequence distance vector) and OLSR (optimised link state routing).

1. **DSDV:** The Destination-Sequenced Distance-Vector (DSDV) routing protocol based on the Bellman-Ford algorithm. In which each node maintains a routing table which stores next hop, destination and a sequence number that is created by the destination itself. In DSDV each node increment and add its sequence number periodically while forwarding routing table to its neighbors.
2. **OLSR:** The OLSR protocol is more efficient in networks with high density and high rarely traffic but the situation is when it is used in between a large number of hosts. OLSR requires that it continuously have some bandwidth in order to receive the topology updates messages.

C. Hybrid Protocols

It is a combination of both reactive and proactive routing protocols. To overcome the weakness of reactive and proactive routing protocol the hybrid is mostly used. In hybrid routing protocol network is divided into zones. It is the most suitable routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state).

4 Securities in MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism.

- ✓ **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. Both passive and active attacks can be made on any layer of the network protocol stack.
- ✓ **Passive Attacks:** Passive attacks are the attack that does not disrupt proper operation of network. Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is Also able to interpret data gathered through snooping .Detection of this attack is difficult since the operation of network itself does not get affected.

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 [3, 4]. These features are explained below:

1) **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.
2) **Lack of centralized monitoring:** MANETs does not have any established infrastructure and centralized administration. MANET works without any pre-existing 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.
3) **Cooperative algorithms:** In MANET the routing algorithms need to have trust between their neighboring nodes.
4) **Bandwidth constraint:** Wireless links have lower capacity as compared to the infrastructures networks.
5) **Limited physical security:** Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.
6) **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.

A. Black Hole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [15]. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely. Figure 1 is an example of single black hole attack in the mobile ad hoc networks. Node 1 stands for the source node and node 4 represents the destination node. Node 4 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the netwoek operation is suffered from this problem.

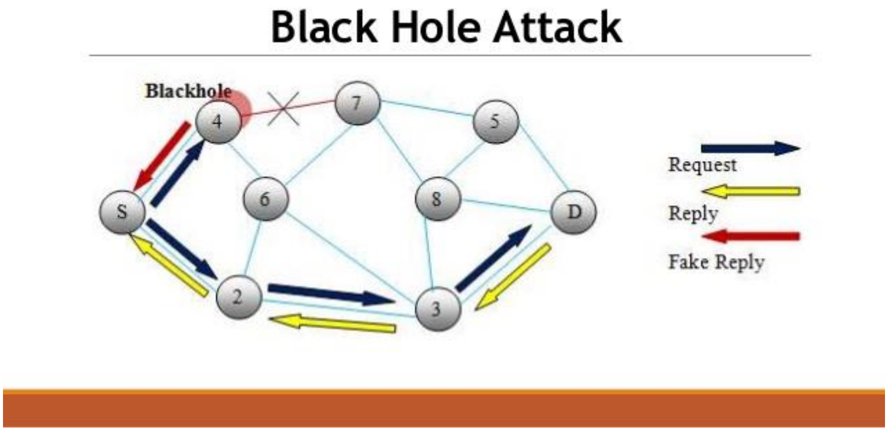

Fig. 1: BlackHole Attack in MANET

B. Pooled Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack .In recent years. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, moreover, hide from the existing detection scheme. As a result, several cooperative detection schemes are proposed preventing the pooled black hole attacks [5]. In the following, different detection schemes for the cooperative black hole attack are presented in a chronological order.

1) **DRI Table and Cross Checking Scheme [6, 7]:** Sanjay Ramaswamy *et al.*, exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology. Every node needs to maintain an extra DRI table, 1 represents for true and 0 for false. The entry is composed of two bits, “From” and “Through” which stands for information on routing data packet from the node and through the node respectively. The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN’s honesty. After that, SN sends the further request to IN’s NHN for asking its routing information, including the current NHN, the NHN’s DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path. Authors propose a detection method to overcome the multiple black hole problems and the collaborative attacks, and submit the simulation result in [7]. The experiment result shows that this solution performs an almost 50% better than other solutions. However, it wastes 5 to 8% communication overhead, and slightly increases the packet loss percentage because of the secure route discovery delay.
2) **Distributed Cooperative Mechanism (DCM) [8]:** Chang Wu Yu *et al.*, propose a distributed and cooperative mechanism viz. DCM to solve the collaborative black hole attacks. Because the nodes works cooperatively, they can analyze, detect, mitigate multiple black hole attacks. The DCM is composed of four sub-modules which shown as Figure 2. In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. A threshold viz. thr represents the maximum hop count range of cooperative detection message. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. There are reaction modes in global reaction phase. Though the first reaction mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs more operation time. In the simulation results, the notification delivery ratio is from 64.12 (thr as 1) to 92.93% (thr as 3) when using different threshold values. Compare with the popular AODV routing protocol in MANET, the simulation result shows that DCM has a higher data

delivery ratio and detection rate even if there are various black hole nodes. Even though the control overhead can be reduced due to the distributed design method, DCM wastes few overhead inevitavle.

3) **Hash based Scheme [9]:** Weichao Wang *et al.,* design a hash based defending method to generate node behavioral proofs which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems. The proposed solution is originated from an audit-based detection method videlicet REAct [12]. The vulnerability of REAct system is that cooperative adversaries can specialize in attacker identification phase by sharing Bloom filters of packets between them. The major difference between these two schemes is discussed as follows. A hash based node behavioral proofs is proposed to defend the collaborative attacks. The audited node ni is needed and settled by the source node S, and then S sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t0 is attached to the tail of every packet. The intermediate node n1 combines the received packet and its own random number r1 to calculate its value t1, and this operation is continued within every intermediate node until ni receives the packet. Nevertheless, this paper doesn't give the results, so that it's hard to figure out the enhancement.
4) **Hashed-based MAC and Hash-based PRF Scheme [10]:** Zhao Min and Zhou Jiliu propose two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are submitted to provide fast message verification and group identification, find the collaborative suspicious hole nodes and discover the secure routing path to prevent cooperative black hole attacks. The public key infrastructure (PKI) is difficult to utilize in MANET due to the inherently design disadvantages, which is no centralized infrastructure. To deserve to be mentioned, authors overcome this bottleneck and design an authentication mechanism. The key point of this solution is that each node acquires a secret key Ki, and Ki = Gk (ri). The sharing key Ki is undisclosed to all other nodes, hence, it is formulated by choosing a random number ri and repeatedly applying PRF on ri by k times. When source node receives a packet, it checks Ki-d to find whether the key used for the MAC is disclosed or not, and checks the MAC when Ki is disclosed. After checking the above two conditions, this packet is regarded as available packet and the route is confirmed as a secure route. The simulation result shows that both solutions have better data delivery ratio than AODV routing protocol. But, the detection time increases as the pause time raises, and the control overhead of both solutions is higher than the ordinary AODV.
5) **Bait DSR (BDSR) based on Hybrid Routing Scheme [11]:** Po-Chun Tsou *et al.,* design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

4 CONCLUSIONS

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. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper a survey on different existing techniques for detection of pooled black hole attacks in MANETs with their defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem.

REFERENCES

1. Vimal, K., & Rakesh, K. (2020). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. *International Conference on Intelligent Computing, Communication & Convergence*, 48, 472-479.
2. Pradhan, D., & Priyanka, K. C. (2021). Green-Cloud Computing (G-CC) data center and its architecture toward efficient usage of energy. In *Future Trends in 5G and 6G* (pp. 163-182). CRC Press.
3. Gajiyani, R., & Ghada, W. (2018). Enhanced Intrusion Detection & Prevention Mechanism for Selfishness in MANET. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(9), 8544-8549. ISSN(Online): 2320-9801, ISSN (Print) : 2320-9798.
4. Shivam, Y. (2021). A detail survey of channel access method for cognitive radio network (CRN) applications toward 4G. *South Asian Research Journal of Engineering and Technology*, *3*(1), 31-41.
5. Briscoe, B., Brunstrom, A., Petlund, A., Hayes, D., Ros, D., Tsang, J., ... & Welzl, M. (2014). Reducing internet latency: A survey of techniques and their merits. *IEEE Communications Surveys & Tutorials*, *18*(3), 2149-2196. ISSN: 1553-877X
6. Ranjana, P., Peizhao H., Jadwiga, I., & Marius, P. (2013). Protocol for Efficient Opportunistic Communication. *38th Annual IEEE Conference on Local Computer Networks, Sydney*, ISSN: 0742-1303 Print ISBN: 978-1-4799-0536-2, DOI: 10.1109/LCN.2013.6761240, pp: 244-247
7. Ranjana, P., Peizhao, H., Jadwiga, I., Marius, P., & Saaidal, A. (2013). A Performance Study of Hybrid Protocols for Opportunistic Communications. *9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Sydney*, Print ISBN: 978-1-4799-0539-3, DOI: 10.1109/LCNW.2013.6758492, pp: 9-16.
8. Guo, J., Liu, H., Dong, J., & Yang, X. (2007). HEAD: a hybrid mechanism to enforce node cooperation in mobile ad hoc networks. *Tsinghua Science and Technology*, *12*(S1), 202-207. ISSN: 1007-0214
9. Prateek, K., Arvind, N., & Alaria, S. K. (2013). MANET-evaluation of DSDV, AODV and DSR routing protocol. *International Journal of Innovations in Engineering and Technology*, *2*(1), 99-104. ISSN: 2319 – 1058
10. Kumar, A., & Mittal, P. (2013). A Comparative Study of AODV & DSR Routing Protocols in Mobile Ad-Hoc Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5), 658-663. ISSN: 2277 128X
11. Bhalinder, K., & Sonia. (2013). Performance Evaluation of MANET Routing Protocols with Scalability and Node Density issue for FTP Traffic. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 544-548. ISSN: 2277 128X
12. Patil, P., Pawar, P. R., Jain, P. P., KV, M., & Pradhan, D. (2020). Performance Analysis of Energy Detection Method in Spectrum Sensing Using Static & Variable Threshold Level for 3G/4G/VoLTE. *Saudi J Eng Technology*, *5*(4), 173-178.
13. Rajesh, S., & Seema, S. (2013). Dynamic Source Routing Protocol (DSR). *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(7), 239-241. ISSN: 2277 128X
14. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *Int. J. Netw. Secur.*, *5*(3), 338-346.
15. Yuh-Ren, T., & Shiuh-Jeng, W. (2004). 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.*

CITATION: S. Jagadeesh Soundappan *et al* (2021). Black Hole Attacks Using AODV in MANET. *South Asian Res J Eng Tech, 3*(6): 190-195.