© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

# Detection and Analysis of Black Hole Attack on MANET Using IDS on NS-2: A Review

**Tehreem Nishat[1], Prof. Hansa Acharya[2]**

Radharaman Institute of Technology & Science, Research Scholar, RGPV Bhopal, Madhya Pradesh, India

## ABSTRACT

Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to that of the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack others nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication that is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Previously the works done on security issues in MANET were based on reactive routing protocol like Ad Hoc on Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET. Black hole attack found in network layer pretends that it has a shortest route to reach to the destination but actually consumes all the packets sent by the source. For this, Intrusion Detection System is implemented using NS-2 by modifying the original AODV protocol and removing the black hole node, which drops the maximum packets. We also proposed a method of activating the promiscuous mode by selecting the path of highest sequence number, which is helpful in achieving the better Quality of Services (QoS).

**Keywords :** MANET, Black Hole, AODV Routing protocols, IDS, NS2

## I. INTRODUCTION

In today's fast and rapidly growing world of technologies, MANET can turn the dream of networking at any place and at time into reality. We are almost there by the way such as Bluetooth enabled mobile phones such as 3G. MANET provides lots of feature and now more and more businesses understand the advantages of usage of computer networking. Depending on the firm's size and resources, it might be a small LAN containing only a few dozen computers; however in large corporations the networks can grow to enormous and complex mixture of computers and servers. A computer network is a system for communication between two system and computers. These networks may be fixed (permanent) or temporary. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless.

## II. METHODS AND MATERIAL

### 1. Infrastructure Less Network : MANET

In any but the most trivial networks (point-to-point links), some mechanism is required for routing the packets from the source to the final destinations. This includes discovery and maintenance of routes along with associated costs. In what is called an 'infrastructure based' wireless network, the job of routing is assigned to dedicated nodes called access points (AP). Configurations of the APs are much less dynamic than there, possibly mobile, end-point nodes. APs are like base stations which keep track of nodes' associations/disassociations, authentication etc. and control the traffic flow between their clients as well as between fellow APs. The AP may also be connected to the Internet thereby providing Internet connectivity to its clients.

The term Ad Hoc comes from the fact that there is no fixed infrastructure for forwarding/ routing the packets. Figure 1.1 [2] shows an infrastructure-based and an Ad Hoc wireless network.

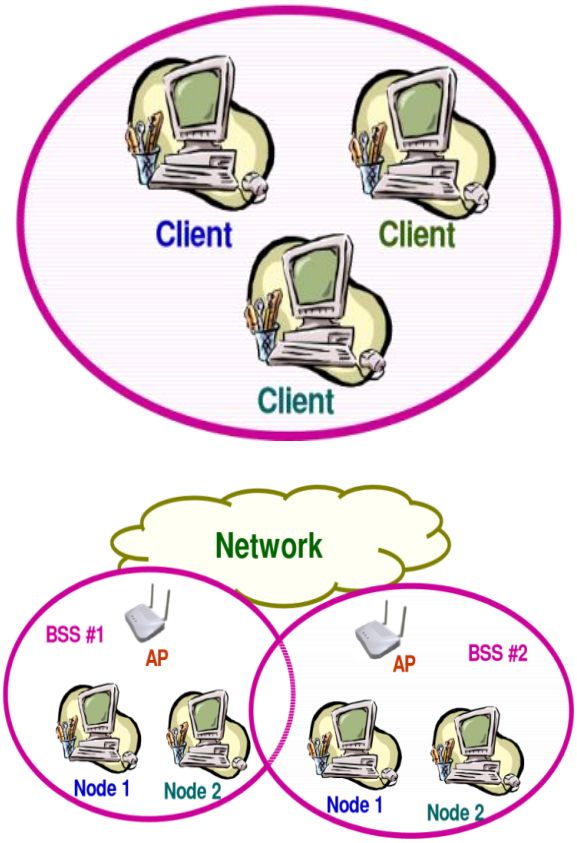


**Figure 1-1.** Ad Hoc and Infrastructure Network Topologies

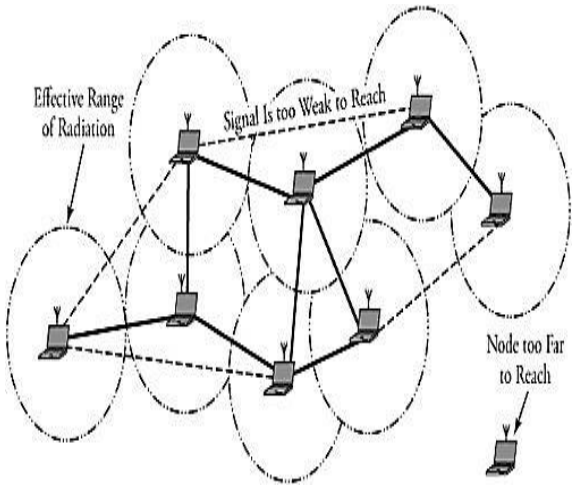


**Figure 1-2 –** A Typical MANET

A typical MANETs (Mobile Adhoc Networks) is shown in Fig 1-2 [6]. The circles indicate communication ranges of individual nodes. In the real-world, this boundary is never likely to be a perfect circle and the links in fact can even be unidirectional in many cases – node 'A' can reach node 'B' on link 1 but node 'B' may not be able to use this link to reach node 'A'. This can happen due to the signal strengths of the two transmitters being unequal or can even be based on the transmission path.

In Ad Hoc networks, each node is willing to forward data to other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to the infrastructure-based networks in which designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make Ad Hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc. An Ad Hoc network is formed for a purpose by participating wireless nodes and is then torn off.

These networks introduced a new art of network establishment and are well suited for environments where either the infrastructure is lost or where deploying an infrastructure is not cost-effective.

**Advantages of Mobile Ad-Hoc Network:**

The advantages of a mobile Ad-Hoc network include the following

- ✓ Independent and decentralize control.
- ✓ Self-configurable network.
- ✓ Each node may act as simple node and router.
- ✓ Less expensive in the comparison of wired network.
- ✓ Scalable and flexible network due to mobility factor.
- ✓ Very robust and useful network

## 2. AD-HOC on Demand Routing Protocol (AODV)

To understand the problem of black hole attack on AODV routing protocol first we understand the some common characteristics and it's working of AODV routing protocol in mobile environment. After that we take a look of the black hole attack, attacking mechanism in the AODV routing protocol. Ad-hoc on-demand distance vector (AODV) routing protocol uses

an on demand approach for finding routes for communication such a route is established only when it is required by a source node for transmitting a data packet. It allows all mobile nodes, to pass messages through their neighbors to the node which are not in radio frequency range for communication. AODV protocol does this by discovering the routes along which message and information can be send. AODV protocol take precaution for such routes that they do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in route and can create new routes if there is an error. AODV defines three types of control message for route maintenance: There are three types of control messages in AODV which are discussed below.

1. Route Discovery
2. Route Reply (RREP)
3. Route Maintenance

RREQ- When one node needs to send a message to another node that is not its neighbor it broadcasts a Route Request (RREQ) message. RREP- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a correct route to this address. RERR- Node monitors the link status of next hops in active routes and when a connection breakage in an active route is detected, a RERR message can be used to notify to the other nodes of the loss of the link.AODV uses sequence numbers to ensure loop freedom.

### 3. Black-Hole Attack

In this attack, a malicious node advertises itself as having the shortest path to other nodes of the network. Nevertheless, as soon as it receives packets destined for other nodes, it drops them instead of forwarding to the final destination. In our simulation scenario, each time a malicious black hole node receives a Route Request packet; it sends a Route Reply packet to the destination without checking if it really has a path towards the selected destination. Thus, the black-hole node is always the first node that responds to a Route Request packet. Moreover, the malicious node drops all Route Reply and Data packets it receives if the packets are destined to other nodes.

1. Highest Sequence Number with Min. Hop Count.
2. Route Table Modification (Update Wrong Route Message).
3. Wired Connection.
4. Adapting techniques of other Security Threats i.e. Wormhole Attack .

### 4. Intrusion Detection

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection is the process of identifying and responding to malicious activities target at computing and network resources. This identification introduces the notion of intrusion detection as a process, which involves technology, people and tools. Intrusion detection is an approach that is complementary with respect to mainstream approaches to security such as access control and cryptography.

### 5. Objectives

Aims and objectives of this thesis work are summarized as follow:

- The study focus on analysis of black hole attack in MANET and its consequences.
- Analyzing the Route Discovery Process
- Collecting Replies
- Identification of Black Hole
- Removal of Black Hole node and remove the entire malicious node(s) from RR-Table detected through Black Hole detection procedure.
- Node selection process for secure routing

## III. RESULTS AND DISCUSSION

### Literature Review

MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing

protocols and security measures within the networks were proposed. Previously the works done on security issues in MANET were based on reactive routing protocol like Ad-Hoc on Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET.

In 2016 Sun B et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1-Collect neighbor set information. Step 2Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify-Route Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.

**Advantages:** This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15% and the false positive probability is usually less than 1.7%.

**Disadvantages:** The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003 and the simulation is done in NS-2 simulator. [1]

In 2015 Shurman et al. propose two techniques to prevent the black hole attack in MANETs. The first technique is to find at least two routes from the source to the destination node. The working is as follow. Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP packets and after identifying a safe route it transmit the buffered packets. It represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are fast-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV.

**Advantage:** second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.

**Disadvantage:** these both techniques fail to detect cooperative black hole attacks. Technique published in year 2004 and simulator used is ns2. [2]

1) In 2014 Tamilselvan L et al. proposed a solution based on an Enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named collect route reply table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.

2) **Advantage:** the simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But end-to-end delay might be raised visibly when the malicious node is away from the source node. Simulation is done in glomosim. [3]

In 2014 Djenouri D et al. proposed a solution in year 2007 to monitor, detect and remove the black hole attack in mantes. In the monitor phase, an efficient technique of random two-hop ack is used. Regarding the judgment issue, a Bayesian approach for node accusation is used that enables node redemption before judgment. The aim of this approach is to consider and avoid false accusation attacks vulnerability, as well as decreasing false positives that might be caused by channel conditions and nodes mobility. This solution

deals with all kinds of packet droppers, including as well selfish as malicious nodes launching a black hole attack. It also deals with any byzantine attack involving packet dropping in any of its steps. This solution detects the attacker when it drops packets. Simulation is done with glomosim simulator. [4]

In 2013 Hesiri Weera singhe et al. proposed an algorithm to identify Collaborative black hole attack. In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data routing information (DRI) table and cross checking using further request (freq) and further reply (FREP). If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (route request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the dri table with all intermediate nodes between source and the destination. The simulation is done in qualnet simulator. The algorithm is compared with the original AODV in terms of throughput, packet loss rate, end-to-end delay and control packet overhead. [5].

## IV. FURTHER STUDIES

- The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols.
- A study can be conducted on the relationship between the average detection delay and the mobility of the nodes.
- More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.
- A complete system can be designed to implement intruder identification.
- A complete approach can be developed that considers more parameters such as the available queue length and the delay on a path during the route determination.
- In order to avoid traffic fluctuation, randomness can be introduced into route determination.

## V. CONCLUSION

An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification-based technique. The IDS performance in detecting misuse of the AODV protocol has been discussed. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. From the results obtained, it can be concluded that our IDS can effectively detect Sequence Number Attack, Packet Dropping Attack and Resource Depletion Attack with Incremental Deployment. The method has been shown to have low overheads and high detection rate. The implementation of the IDAODV protocol has shown its feasibility to work in real life scenarios; IDAODV performs real-time detection of attacks in MANETs running AODV routing protocol. The prototype has also given some insight into the problems that arise when trying to run real applications on an Ad Hoc network.

Simulation results validate the ability of our protocol to successfully detect both local and distributed attacks against the AODV routing protocol, with a low number of false positives. The algorithm also imposes a very small overhead on the nodes, which is an important factor for the resource-constrained nodes.

## VI. REFERENCES


[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA ’02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002,. 3–13.

[2] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.

[3] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.

[4] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackhole attackon AODV based mobile ad-hoc networks by dynamic learning

method,"International Journal of Network Security, pp. 338–346, 2007.

[5] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.

[6] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[7] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date lastviewed: 2010-05-05

[8] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-HocNetworks," ACM Southeast Regional Conf. 2004.

[9] Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[10] Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[11] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[12] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[13] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.

[14] istry N, Jinwala DC, IAENG, Zaveri M, "Improving AODV Protocol Against Blackhole Attacks", International Multi Conference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.