# A Details Survey on Black-hole and Denial of Service Attack over MANET Environment

**Kamlesh Patel[1], Abhishek Thoke[2],**

[1] Scholar, Department of Information Technology, Technocrat Institute of Technology, Bhopal, India.
[2] Assistant Professor, Department of Information Technology, Technocrat Institute of Technology, Bhopal, India.

---

***Abstract* – *Security is a major challenge in Mobile Ad hoc Network (MANET) due to their features of dynamically changing topologies, frequent host movement, Multi-hop wireless links and lack of clear line of defense. Protecting the network layer of a MANET from malicious attacks is an important and challenging issue. This paper analyzes the black hole and denial of service attack which is very severe type of possible attacks in Mobile Ad hoc Networks (MANETs). In a black hole attack, malicious nodes advertise itself by sending a false route reply packet to a source node that initiates a route discovery process and drops all packets whereas DDOS attacks target the resources of these services, lowering their ability to provide optimum usage of the network infrastructure. In this paper, we are investigating the effect of black-hole and dos attack on MANET environment and recommend practical defense mechanisms against black-hole and DOS attacks. The implementation of the proposed concept is provided using the Ad-hoc on Demand Distance Vector routing protocol modification in network simulator 2 i.e. NS-2.*

*Keywords: Security, DOS, Black-hole, MANET, AODV, Routing*

## 1. Introduction

A MANET is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. A MANET is an emerging research area with practical applications. However, A 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 MANETs introduce some new security problems in addition to the ones already present in fixed networks [1]. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly [2]:

***1.1 Confidentiality:*** Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

***1.2Availability:*** Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

***1.3 Authentication:*** Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

**1.4 *Integrity:*** Message being transmitted is never altered.

***Non-repudiation:*** Ensures that sending and receiving parties can never deny ever sending or receiving the message.

### 1.1 Security Attacks in Mantes

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

***1.1.1 INTERNAL ATTACKS:*** Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [4]. Internal attacks are sometimes more difficult to handle as compare to external Attacks, because an internal attack occurs due more trusted nodes.

***1.1.2 EXTERNAL ATTACKS:*** These types of attacks try to cause congestion in the network, denial of services (DOS), and advertising wrong routing information etc. [4]. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

***1.1.3 PASSIVE ATTACKS MANETs***: are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic [4]. Detection of such type of attacks is difficult since the operation of network itself doesn't get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

***1.1.4 ACTIVE ATTACKS:*** Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [4].These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of Packets, DoS, congestion etc. In [3] [5] the authors survey attacks like flooding attack, black hole attack, link withholding attack, link spoofing attack, replay attack, wormhole attack, colluding miserly attack and gave their countermeasures using some cryptography and key management techniques in mobile ad hoc network and introduced a new attacks that is Ad Hoc Flooding Attack, which acts as an effective denial of service attack against all currently proposed ad hoc network routing protocols [3].

## 2. Literature Survey

In this paper the author presents the solution to packet drop attack and improves the performance of network. In this approach the trusted list is introduced instead of black list. As the packet drop is minor attack as proved to reduce reanalysis overhead analyzed node is or detection overhead added to trusted list. So it is skip that node's analysis in future. Hence it is reduce the calculation/ analysis or detection overhead for already analyzed trusted list to some extent trusted list is local to every node maintained as data structure in local RAM buffer. Direct reputation method using two counters [6].

Gayatri Wahane et. al. proposed a research work that suggests the modification of AODV Routing Protocol. In this paper, routing security issues in MANETs are discussed in general, and in particular the cooperative black hole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes [7].

Neetika Bhardwaj et. al. presented a new solution to detect and prevent the Black hole which does not increase routing or computation overhead and increases the performance metrics like packet delivery ratio, throughput by a huge margin. Also the false detection ratio of the approach is negligible. Black hole Attack is one of the most severe attacks because the attacker embeds itself into the route from source to destination by sending false RREP messages giving an impression that it has the freshest route to destination. Seeing its severity many researchers have addressed the problem of detecting and defending against black hole attack but the solutions presented so far suffered from one problem or the other [8].

Pooja Jaiswal et. al. proposed a method for finding the secure routes and prevent the black hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the Route Request Table (RRT). Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RRT [9].

Distributed Denial of Service (DDoS) attacks remain a major security problem the mitigation of which is very hard especially when it comes to highly distributed botnet based attacks. The early discovery of these attacks, although challenging, is necessary to protect end users as well as the expensive network infrastructure resources. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture and algorithms of FireCol. The core of FireCol is composed of Intrusion Prevention Systems (IPSs) located at the Internet Service Providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as its support for incremental deployment in real networks [10].

Distributed Denial of Service (DDOS) flooding attacks are one of the biggest concerns for security professionals. DDOS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). In this paper, explore the scope of the DDoS flooding attack problem and attempts to combat it. Authors categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, we highlight the need for a comprehensive distributed and collaborative defense approach. Our primary intention for this work is to stimulate the research community into developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack [11].

Content-Centric Networking (CCN) is an emerging networking paradigm being considered as a possible replacement for the current IP-based host-centric Internet infrastructure. CCN focuses on content distribution, which is arguably not well served by IP. Named-Data Networking (NDN) is an example of CCN. NDN is also an active research project under the NSF Future Internet Architectures (FIA) program. FIA emphasizes security and privacy from the outset and by design. To be a viable Internet architecture, NDN must be resilient against current and emerging threats. This paper focuses on distributed denial-of-service (DDoS) attacks; in particular we address interest flooding, an attack that exploits key architectural features of NDN. We show that an adversary with limited resources can implement such attack, having a significant impact on network performance. We then introduce Poseidon: a framework for detecting and mitigating interest flooding attacks. Finally, we report on results of extensive simulations assessing proposed countermeasure [12].

## 3. Black-hole and Denial of Service Attack

**3.1 Black hole Attack:** In Black-hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device [13]. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack [14].

For example, in Figure 1, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

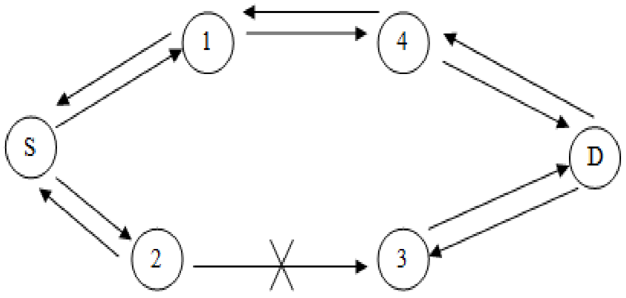

*Figure 1 Black hole attack*

**3.2 Denial of Service Attack:** DOS attacks can cause a severe degradation of network performance in terms of the achieved throughput and latency. The performance of the wireless network is degraded by DOS depends on many factors such as location of malicious nodes, their traffic pattern, fairness provided in the network resources. It attacks like routing table overflow and sleep deprivation fall. The main aim of a DoS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the networks bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients. In the not so distant past, there have been some large - scale attacks targeting high profile Internet sites. [15].

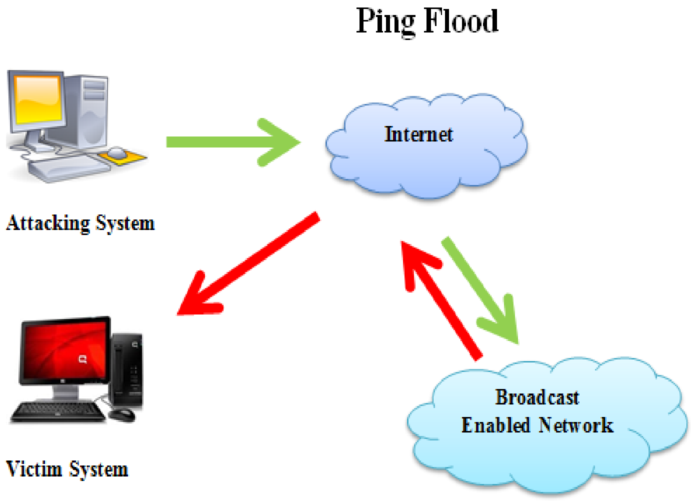

*Figure 2 Denial of Service Attack*

**3.2.1 Significance of DOS:** A common technique of attack involves saturating the target machine with communications requests, by which target machine cannot respond to legitimate traffic, or responds slowly. In other terms, DDoS attacks are deployed by forcing the targeted machine to reset or consuming its resources by which that machine no longer provide its services. There are two chief classes of DDoS attacks: bandwidth depletion and resource depletion attacks [16].

**3.2.2 Bandwidth Depletion:** Bandwidth depletion attack is designed to flood the victim network with unwanted traffic by sending that stops legitimate traffic from reaching the victim system. Bandwidth attacks can be separated to flood attacks and amplification attacks.

**3.2.3 Resource Depletion:** Resource depletion attack is an attack that is planned to tie up the resources of a victim system. This is done by developing the TCP protocol and sending will fully incorrect semantic IP packets to crash the victim system. This type of attack can be separated to protocol exploit attacks and malformed packet attacks.

## 4. Problem Formulation

There does number of framework exist for finding the malicious attackers is available and most of techniques are providing solutions for single attack. If the solution is formulated as a classic model to secure the network from more than one attacker using single solution is more effective. Thus an effective technique is required to adopt more parameters by which the other kinds of attackers are also distinguished. The proposed security technique involves the following issues to resolve in the proposed solution.

- ➔ Due to DDOS attacker and Black hole attack injects routing overhead is increases significantly. The routing overhead directly impact on the network performance in terms throughput and packet delivery ratio and end to end delay also.
- ➔ The energy of the network nodes is limited due to the limited power source. The DDOS attacker tries to consume the node energy and Black-hole attacker the data packets. Thus energy consumption is increases and packet delivery ratio becomes too low.

## 5. Proposed System

The proposed security model is a paramete based security framework and promises to provide a secure communication model. Therefore the following security solution is required to implement.

- ➔ To provide efficiency during the route discovery this process is taken place
- ➔ Obtain some essential network parameters that help to design the attribute based rules to improve the performance during the attack.
- ➔ Design of a fuzzy algorithm that helps to identify the Black-hole and DDOS attacks in networks

### 5.1 Methodology

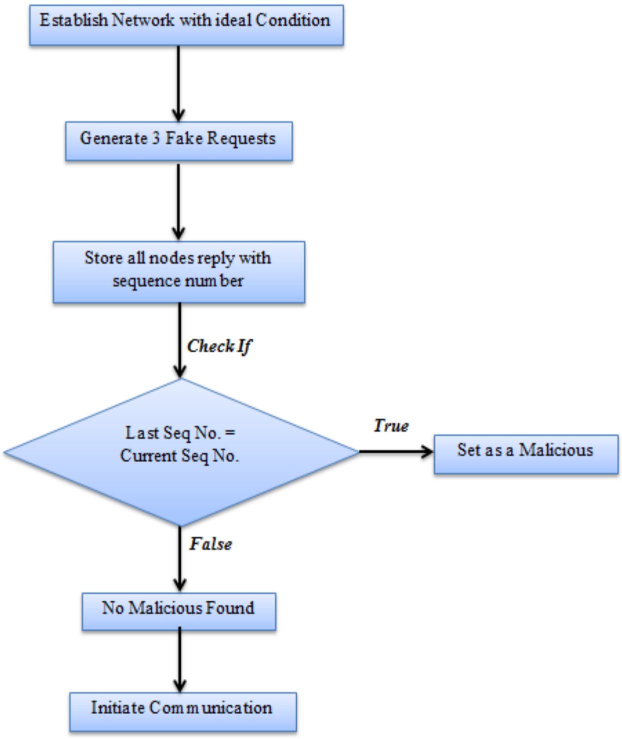
Establish Network with ideal Condition
Generate 3 Fake Requests
Store all nodes reply with sequence number
Check If
Last Seq No. = Current Seq No.
True
Set as a Malicious
False
No Malicious Found
Initiate Communication

*Figure 3.1 Proposed Flow Work*

**Description:** To prevent black-hole attack first we make two or three fake route request which has destination within network as nature of black-hole attacker node he just reply to both node as same route reply in the form of sequence number but all the other nodes send the different sequence number of different number if we find this kind of reply we provide the key to all other nodes rest of them are safe to communicate For preventing the DDOS attack we also add the counting the number of route request without including this two nodes find out the variance of all nodes if the node sends more than the variance this is also set as attacker node and if any route request come from this node all other node will not process this request

## 6. Conclusion

It is easy to deploy DOS flooding and Black-hole attack to impersonate another node in MANET. Mobile ad hoc network has no clear line of defense, so, it is accessible to both legitimate network users and malicious nodes. This survey paper initiate key defense threats in MANET and also explore different Denial of Service attack flooding and Black-hole attack detection and prevention techniques, and how these solutions are capable to safe the network So the finally, by evaluate the pros and cons of obtainable techniques the open research challenges in mobile ad-hoc network are studied.

## References

[1] Junhai Luo, Mingyu Fan, and Danxia Ye, "Black Hole Attack Prevention Based on Authentication Mechanism", *the Eleventh IEEE International Conference on Communications Systems (ICCS),* PP. 173-177, 2008.

[2] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE and DR. M.S.ALI, "A Survey of Mobile Ad Hoc Network Attacks", *International Journal of Engineering Science and Technology,* Vol. 2(9), PP. 4063-4071, 2010.

[3] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, published in International Journal of Information Technology Vol. 11 No. 2, , pp. 83–94,

[4] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274

[5] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, IEEE Wireless CommunicatioOctober 2007 , pp. 85–91

[6] Ashok M. Kanthe , Ramjee Prasad, Dina Simunic, "The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-Hoc Networks", *international journal of recent technology and engineering (IJRTE)*, volume-2, , December 2012.

[7] Gayatri Wahane and Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack in MANET", 2014 (ICAET-2014 IOSR Journal of Computer Science (IOSR-JCE) PP. 59-67.

[8] Neetika Bhardwaj and Rajdeep Singh, "Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, PP. 376-383, 2014.

[9] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", I*nternational Journal of Computer Networks and Wireless Communications (IJCNWC),* Vol. 2, No. 5, PP. 599-606, Oct 2012.

[10] Issam Aib and Raouf Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", *IEEE/ACM Transactions on Networking*, PP. 1828-1841, 2012.

[11] Saman Taghavi Zargar, James Joshi and David Tipper," A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*", IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, PP. 2046 - 2069, volume 15, 2013.

[12] Alberto Compagno, Mauro Conti and Paolo Gasti, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", *38th Annual IEEE Conference on Local Computer Networks*, PP. 630-638, 2013.

[13] Shree Om and Mohammad Talib, "Wireless Ad-hoc Network under Black-hole Attack", International Journal of Digital Information and Wireless Communications (IJDIWC) PP. 591-596, 2011.

[14] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil, "Black Hole Attack Injection in Ad hoc Networks".http://users.ece.cmu.edu/~koopman/dsn08/fast abs/dsn08fastabs_ruiz.pdf

[15] Douligeris and A. Mitrokotsa," DDoS attacks and defense mechanisms: classification and state of-the-art", In Computer. Network, 643-666. (Apr. 2004).

[16] Stephen Specht and Ruby Lee, "Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures", Technical Report CE-L2003-03, May 16, 2003.