# Performance Examination of Black Hole and Gray Hole Attacks in MANETs

**Mahendra Pd. Sharma**

***Abstract*: *Security is a very difficult issue for ad hoc ad networks. The first step is to developa good security solution to understand the current attack method.The presence of malicious nodeswill affect the functionality and network integrity. In the Black hole attack, malicious nodes will lower the package instead of moving forward. Thus, Black hole attacks reduce networkperformance. Utimetly as a black hole this paper analysis over other attacks individually or inintegrated manner. It is quite easy to verify the behaviors of black hole attack on individual basis.But in case of gray hole attack it is too much difficut to analysis the nature and behaviors of the network. The quality of tarnsmision is unpredictable and the overall performance get badlyaffcted with the such kind of attack. These attacks is the basic of the earlier known attack butwhen it come in pair or more than its behaviorss is very hard to detected on the basis of thepresent knwledge. In this paper we analyse blackhole and Grayhole attack s that executed underthe NS2 plateform run on the linux operating system. The analysis formwithsome set of nodesand whole excution focused on three parameters i.e E2E, PDR and Throughput.***

***Keywords*: *AODV-Adhoc On demand Distance Vector,DoS-Deniel of Services,MANET- Mobile Adhoc Network,E2E-End to End,PDR-Packets Delivery Response, WLANs- Wireless Local area Networks***

## I. INTRODUCTION

The ad hoc network is a collection of wireless mobile nodes that can form a temporary network without any centralized management. In such an environment, due to the limited transmission range of the wireless network interface, the mobile node may need to reach other hosts to send host packets [1]. Not only does every mobile node act as a host, it also serves as a backward packet in the network that does not go directly to other mobile nodes in the range. Because each node is participating in a suspicious routing protocol, the network can explore multidirectional routes within another node. This philosophy of ad hoc mobile networks is also called low network infrastructure because network nodes create a path for building networks in it [2].The Ad-hoc mobile network is an autonomous and decentralized wireless system. MANET consists of mobile nodes that are free in incoming and outgoing network traffic. Network nodes are systems and devices and mobile phones, laptop computers, personal digital assistants, MP3 players, and personal computers. These nodes can act as both host routers. They can create all the land based on mutual network connection. Dedicated to the development of IP routing protocols, Internet Engineering Task Force (IETF), A MANET (WG) working group. The routing protocol is a research challenge and an exciting area. Many routing protocol MANET have been developed for AODV in ADOV networks, OLSR, DSR, etc. The security of mobile Ad-Hoc networks is the most important consideration for the core functions of the network. You can ensure that by ensuring security issues, ensuring network availability, data privacy and integrity. MENET is often due to a lack of open environment, dynamic land changes, monitoring and centralized management, collaborative algorithms, and security attacks with clear defense mechanisms. These factors changed the situation of the MANET fights against security threats [3,4].

## II. WIRELESS NETWORK

Wireless networks are becoming more popular today because users want wireless connectivity regardless of their geographic location. Wireless networks allow consumers to communicate and send data without media. One of the reasons for the spread of these networks is the widespread use of wireless devices. Wireless applications and devices focus on wireless local regional networks (WLANs). There are two main modes of operation, the existence of a control module (CM) without connection to Ad-Hoc base stations and control modules. The ad network does not agree with the fixed infrastructure for its operation. Such network mode of operation is independent or the cellular network can be connected to one or more points to provide Internet and connectivity [5].

## III. ATTACKS IN MANET

Current ad hoc mobile networks allow for many different types of attacks. Although similar attacks exist in wired networks, it is easy to fix the infrastructure in such networks. Current partners are mainly dangerous against two types of attacks, active and passive attacks. Active attacks are attacks when unnecessary nodes to perform dangerous behaviors must bear some energy price. On the other hand, inappropriate attacks are mainly due to lack of cooperation to save self-energy. Nodes that bring about a network saving to destroy other nodes, aggressive attacks considered nods, and a harsh attack on communication to save battery life. In this chapter considered to be poor, we are in danger, focusing on the current advertising network. We rank as attack, counterfeit, manufacturer, fraudster, and attack on

**Revised Manuscript Received on July 22, 2019.**

**Mahendra Pd. Sharma**, CSE Department, IIMT College of Engineering, Greater Noida, India

cooperation [6].

## IV. BLACK HOLE ATTACK

The cross-well attack is carried out in two steps. In the first step, the malicious node uses the mobile ad hoc routing protocol (such as AODV) to declare itself as having a valid route to the destination node, even if the route is false, intercepting the packet. In the second step, intrusion packets are intended for use and will not be completed. In advanced form, an attacker pushes or changes some nodes extracted from a node, but data from other nodes is not unexpected [7, 8]. Therefore, an attacker forgets neighboring nodes to monitor continuous packets. As shown in Figure 1.8, Node 1 want to send a data pack to acquire a node and wishes to start a discovery pass. We understand that node 3 is a bad node, it asserts that it receives a RREQ packet and immediately sends a reply to the node when it has a RREQ packet. 1. When node 3 reaches node 1, node 1 recognizes that all other response messages are ignored when the search is complete and the packet is sent to the node. As a result, all packages passing through the abused node are consumed or lost [9,10].

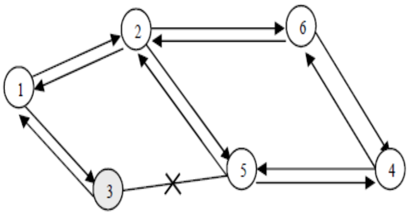

Fig:1 The black-hole problem

## V. SIMULATION

This set is executed under the NS2 plateform run on the linux operating system. The indivisual analysis form as below with some set of nodes.the whole excution performed under when attack has been excuted .

## VI. ANALYSIS OF BLACKHOLE ATTACK

Simple AODV Set up of 20 nodes for the AODV protocol under the arena of NS2 plateform. The whole execution as shown below. Now the attack (black hole) has been executed for the different set as discussed above.

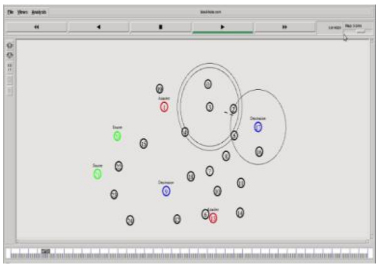

Fig: 2 Detection of Black hole AODV 25 nodes

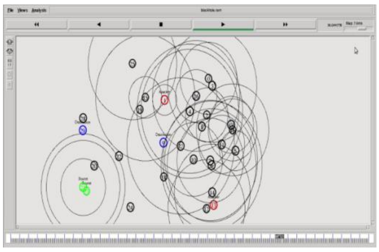

Fig: 3 Detection of Black hole AODV 30 nodes

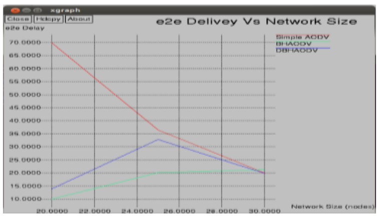

**Fig:4 E**2E delivery-black hole Detected

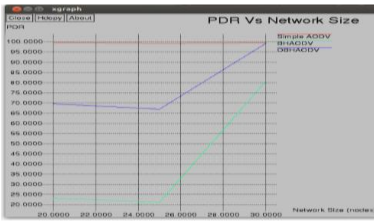

Fig: 5 PDR-black hole Detected

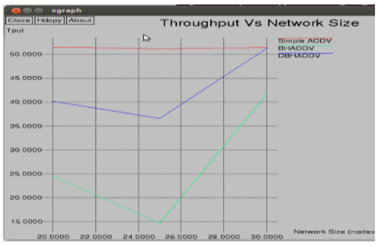

Fig: 6Through-Put Detected

Table 1: Comparative Analysis After detection of black hole

| | DBH-AODV 20 | DBH-AODV 25 | DBH-AODV 30 |
|---|---|---|---|
| E2E | 13.94 | 32.79 | 19.98 |
| PDR | 69.65 | 67.05 | 99.19 |
| Throughput | 48.22 | 36.61 | 51.23 |

## VII. ANALYSIS OF GRAYHOLE ATTACK

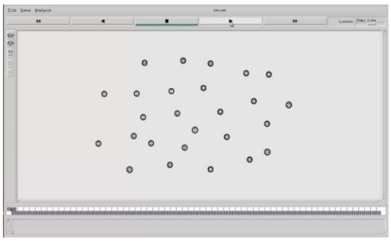

Fig: 7 25 nodes under NS2

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

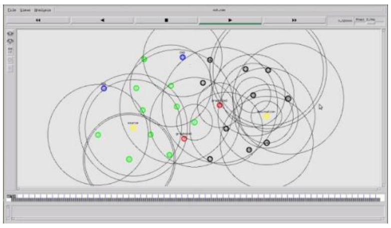

Fig: 8 Start simulations of 25 nodes

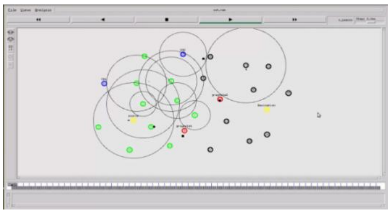

Fig: 9 Drop Packet during Simulation

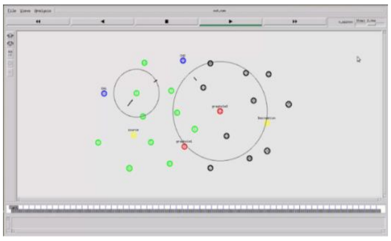

Fig: 10 Data Transfer from source to destination

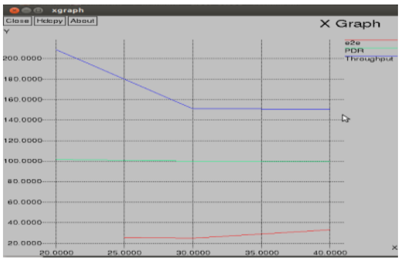

Fig: 11 Graph e2e, PDR, Throughput gray hole attack

Table 2: comparative result of grayhole attack

| Nodes | 25 | 30 | 40 |
|---|---|---|---|
| e2e | 25.7744 | 24.7383 | 33.0175 |
| PDR | 101.68 | 99.84 | 99.58 |
| Throughput | 208.8 | 151.18 | 150.77 |

## REFERENCES

1. Abusalah, L., Khokhar, A. A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. IEEE Communications Surveys and Tutorials, 10(1-4), 78-93.
2. Akyildiz, I. F., & Wang, X. (2005). A survey on wireless mesh networks. IEEE Communications magazine, 43(9), S23-S30.
3. Alem, Y. F., & Xuan, Z. C. (2010, May). Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 3, pp. V3-672). IEEE.
4. Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. D. (2015, January). An intrusion detection system against malicious attacks on the communication network of driverless cars. In Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE (pp. 916-921).
5. Al-Kahtani, M. S. (2012, December). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on (pp. 1-9). IEEE.
6. Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 56(2), 940-965.
7. Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 56(2), 940-965.
8. Bai, F., Sadagopan, N., & Helmy, A. (2003, March). IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of Rou-Ting protocols for Adhoc Networks. In INFOCOM 2003. Twenty-second annual joint conference of the IEEE computer and communications. IEEE societies (Vol. 2, pp. 825-835). IEEE.
9. Barbera, M., Lombardo, A., Panarello, C., & Schembra, G. (2007, June). Active Window Management: an efficient gateway mechanism for TCP traffic control. In Communications, 2007. ICC'07. IEEE International Conference on (pp. 6141-6148). IEEE.
10. Bellofiore, S., Foutz, J., Govindarajula, R., Bahçeci, I., Balanis, C. A., Spanias, A. S.,& Duman, T. M. (2002). Smart antenna system analysis, integration and performance for mobile ad-hoc networks (MANETs). IEEE Transactions on Antennas and Propagation, 50(5), 571-581.

## AUTHORS PROFILE

**Mahendra Sharma** - b.tech-it, m.tech-cse.,assistant professor in department of cse, iimt college of engineering greater noida, he constantly proved excellence in teaching & research and all academic work. he has started his career in the year 2005 and he is having more than 14 years of experience in teaching and educational filed. he has handled more than 15 subjects for ug, more than 05 subjects to pg..