IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 11, November 2018

A Survey on Prevention & Elimination of MANET Attacks

Praveen Kumar Joshi[1], Anindita Saha[2]

Department of CSE, BTKIT Dwarahat[1,2]

Abstract: MANET (Mobile Ad-hoc Network) which is well known as infrastructure less network finds its application in situations where setting up of network should be impromptu. But this advantageous aspect of MANET can be used as a weakness to intrude into the system. That's why it becomes very important to tackle this scenario. In this paper two of the major attacks i.e. Black hole attack and Gray hole attack are discussed. First is active kind of attack in which malicious node participates actively whereas later one is passive attack, which is difficult to detect because malicious nodes do not drop the packets every time. So, it is quite evident that first one is eliminated and later one is prevented. This paper attempts to put forward all such aspects of MANET.

Keywords: Black hole attack, Gray hole attack, MANET

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is an on-demand network that self-configures using wireless connection. The topology of a MANET changes quickly and unpredictably. As the devices in this network are organizing all by themselves and without the interference of any user, they sets-up really fast. This is the reason why it is perfect to be used for urgent situations like rescue operations and emergency medical situations. The devices involved in MANET are part of it. This means that there is no such requirement of any pre-existing infrastructure. On the basis of these grounds it is well-known as infrastructure-less network. The advantage of dynamically changing topology is the biggest loophole of MANET as it makes it prone to several issues such as QoS (Quality of Service), scalability, security, memory overhead etc. The self-configuring property of Mobile Ad-hoc network makes it usable in variety of domains such as law enforcement; emergency search-and-rescue operations, different industries also use it for supervision purpose.

II. VARIOUS KINDS OF ATTACKS IN AD-HOC NETWORK

Although Ad-hoc networks are used in variety of applications but because of its ever changing topology they are susceptible to various attacks like traffic relaying and traffic generation. This paper discusses wo well known attacks-black hole and gray hole attack and how these traffic relaying attacks can be avoided. . The Black hole and Gray hole attacks are security attacks which falls under the network layer attacks, they exploit reactive routing protocols of MANET such as DSR, AODV etc., to drop the packets in the network [1].

A. Balck Hole Attack: It is a DoS(Denial of Service) attack. In this, an intruding node replies to the request of the source node for the best possible path. The intruding node gives an implication that shortest possible path is through it. But, as soon as it gets the packet which is to be delivered to the destination, it drops the packet straight away. This way the malicious node affects the network actively and causes the loss of information.

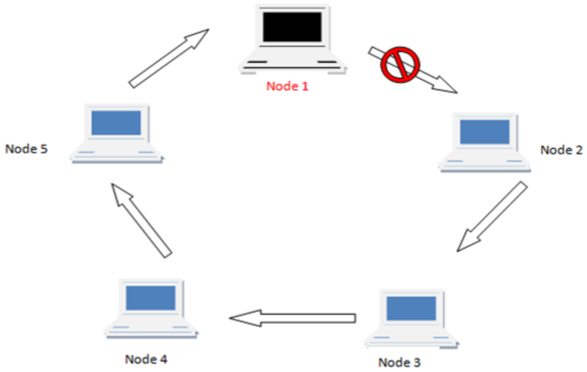

Fig. 1: Node1 is malicious

DOI 10.17148/IARJSET.2018.5114

B. Gray hole attack: Gray hole attack can said to be an extension of black hole attack. There can be completely no clue of this attack. It is so, because for some time the misbehaving node acts like every other node in the network and when packets are sent for forwarding, it drops some or all of them. One point to ponder here is that, the dropping of packet is not necessarily because of malicious nature. It should be noted that packets are dropped by the nodes because of congestion or bandwidth restrictions as well.

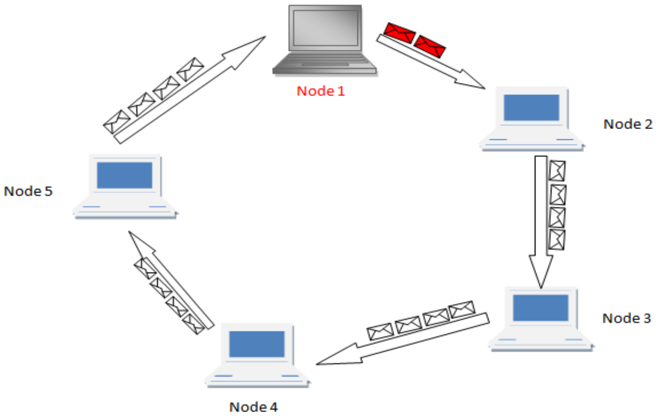

Fig. 2: Selective dropping at Node 1

III. PREVENTION AND ELIMINATION OF ATTACKS

The dynamic topology of MANETs allows any malicious node to intrude into the system. Depending on the type of scenario created by these malicious nodes; attacks are categorised as active and passive i.e. black hole attack and gray hole attack. When MANET is affected by black hole attack, participation of malicious nodes is actively seen as packets are dropped significantly. Although in case of gray hole attack participation is passive, which means packet dropping is not regular. This makes it very difficult to be detected, as congestion; low bandwidth or other factors can also cause misbehaving of packet delivery. So, opting for prevention is the best idea.

A. Existing Approaches to Eliminate Attacks: Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks [2]. This approach highlights the issues common with Mobile Ad-hoc Networks (MANETs) and proposes an algorithm for identifying chain of cooperating misbehaving nodes. For detecting the malicious nodes, each node in the network stores information of black listed nodes in its local table. The algorithm proposed in this paper tells how node can detect the malicious nodes and warn the complete network about their presence. From this information a secure path is obtained between source and destination node. So, this method helped in detecting and avoiding cooperative malicious nodes.

A Hybrid Routing algorithm against Routing attacks in Mobile Adhoc Networks (MANETs) [3] is also suggested. It utilizes the properties of proactive and reactive approaches of routing. Because of this hybrid algorithm has both better packet delivery and low overheads. This routing approach is designed for various applications like search-and–rescue operations and for army missions.

B. Existing Approaches to Prevent Attacks: The approaches of eliminating attacks in MANET are not feasible in case of gray hole attack. This is because of the deceptive nature of malicious nodes, as they drop the packets in discontinuous manner. So, it becomes next to impossible to find out whether actually there is attack or not. As loss of packets can take place due to congestion, low bandwidth and because of many other reasons. Let's have a look at some of the attack preventing approaches.

Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET attempted to mitigate the gray hole attack and proposes a credit based approach based on Ad-hoc On Demand Distance Vector (AODV) routing protocol. This paper proposed and implemented an algorithm named as Credit Based AODV (CBAODV). In this approach, initially each and every node assigns a fixed value for its every neighbor node as the neighbor credit value. This credit value is incremented by when it receives a Route Request Packet (RREQ) and decrement when it receives the route reply (RREP) packet. When a node finds credit for one of its neighbors as a negative value, then it identifies the gray hole node. Also it removes all existing paths from its routing table going through that node [4]. Further in the paper, Detection of Gray hole in MANET through Cluster Analysis speaks about gray hole detection by using cluster of three nodes and its performance with varied mobility and number of nodes [5].

DOI 10.17148/IARJSET.2018.5114

CONCLUSION

It is obvious from the discussed approaches that there is notable distinction between black hole attack and gray hole attack. So, as far as active and passive participation of malicious nodes is concerned, elimination approach is followed for first type of attack and prevention approach for the later type. A hybrid approach fulfilling both measures with better efficiency can be developed as the future work.

REFERENCES

[1]. Rashmi, Ameeta Seehra, " Detection and Prevention of Black-Hole Attack in MANETS", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Jul-Aug 2014, ISSN: 2347-8578, Page 204-209.

[2]. Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3]. Swati Kapoor, Poonam Saini "A Hybrid Routing algorithm against Routing attacks in Mobile Adhoc Networks (MANETs)", International Conference on Computing, Communication and Automation (ICCCA2015), ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE.

[4]. Deepali A. Lokare, A.M Kanthe, Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", International Journal of Computer Applications (0975 – 8887) Volume 88 – No.15, February 2014.

[5]. S D Khatawkar, Nitin Trivedi, "Detection of Gray hole in MANET through Cluster Analysis", 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).

DOI 10.17148/IARJSET.2018.5114