Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.623 – 626

REVIEW ARTICLE

Selective Packet Drop Attack in MANET-A Review

Anubha Goyal
Chandigarh Engineering College, Landran
anubhagoyal1991@gmail.com

Abstract-Wireless Networking is technology in which two or more computers are communicating with each other. MANET is one of the types of wireless networking. There are many types of attacks which are possible to be triggered in MANET. In this paper we will focus on selective packet drop of selective forwarding attack. This packet reduce throughput of the system. A novel technique will be proposed which will reduce packet drop problem.

Keywords- MANET; Active attacks; Passive attacks; Selective packet drop

I. INTRODUCTION

To exchange information number of computer are joined together to form networks and share resources. Networking is used to distribute information and data communication. There are two types of sharing resources that is hardware or software types. It is central administration system or supports these types of system. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables [3]. There are two types of wireless networking. First is infrastructure mode is that mode in which wireless network adaptor is used to connect with the already existing networks with the help of access point. Wireless adaptor is also known as wireless clients [4].It has a central controller. Second is Infrastructure based network, communication is takes place only between the access points and the wireless nodes. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. Ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it's a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. There are two types of attacks are present in MANET which break the security of the networks. These attacks are as follow:

1. Passive Attacks
2. Active Attacks

1.Passive Attacks:

A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection [4]. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel. Examples of Passive Attacks are eavesdropping, snooping.

2. Active Attacks:

An active attack is that attack which any data or information is inserted into the network so that information and operation may harm [4]. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing [2].

Other types of attack are as follow:

1. Internal Attack:

Internal attacks are as of compromised nodes that are part of the set of connections. In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Traffic can be analyze between other nodes and may participate in the activities of other networks like blackhole, selective packet drop attack etc [6].

2. External Attack:

The external attack is conceded out by the nodes which do not belong to network. It may cause unavailability and congestion by sending false information for the network jamming attack [1].

II. LITERATURE REVIEW

S. Sharmila and G. Umamaheswari discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node [5]. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with various mobility and receiver sensitivity of the node.

N.Bhalaji introduced [6] Ad-hoc networks are frequently targeted by participating malicious nodes to sabotage the network. A common mechanism to protect these networks is through the use of encryption and hashing mechanisms. However, the implementation of these mechanisms generally imposes certain unessential requirements, which are considered as restrictive for unplanned environments. In this paper we have discussed the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks connected to ad hoc networks. With the help of the Network simulator we were able to prove that the proposed scheme increases the routing security and encourages the nodes to cooperate in the adhoc structure. Our scheme is equipped with technique to identify and isolate the malicious nodes from the active data forwarding and routing.

Aikaterini Mitrokotsa et.al discussed [7] that evolution of wireless network technologies and the recent advances in mobile computing hardware have made possible the introduction of various applications in mobile ad-hoc networks. Not only is the infrastructure of these networks inherently vulnerable but they have increased requirements regarding their security as well. As intrusion prevention mechanisms, such as encryption and authentication, are not sufficient regarding security, we need a second line of defense Intrusion Detection. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, we briefly describe intrusion detection systems and then we suggest a distributed schema applicable to mobile ad hoc networks. This anomaly detection mechanism is based on a neural network and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance of the proposed architecture is evaluated under different traffic conditions and mobility patterns.

Jacek Cicho et.al discussed the problem of efficient alarm protocol for ad-hoc radio networks consisting of devices that try to gain access for transmission through a shared radio communication channel [8]. The problem arises in tasks that sensors have to quickly inform the target user about an alert situation such as presence of dangerous radiation, fire, seismic vibrations, and more. In this paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots.

III. SELECTIVE PACKET DROP ATTACK

Selective Packet drop is only possible when jamming attack is unsuccessful. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehavior. Post-reception dropping is fewer bendy than selective jamming because the challenger is limited to dropping only the packets routed through it. Selective policy known as the Jellyfish attack which is a compromised node that is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero. This attack can be achieve even by remind random delays to TCP packets, without dropping them, while left over protocol compliant. Similar selective dropping attacks can be construct for other network functions such as the association/de-association of STAs, and topology management [5].

IV. **PROPOSED METHODOLOGY**

Among all the attacks discussed previous selective packet drop attack is the most common active type of attacks. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been proposed to isolate Selective attacks from the network. When Selective packet attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. In our work, we work on to detect and isolate Selective Packet Drop attack In AODV Protocol. The aim of the study is to detect the Selective Packet Drop in MANET using AODV protocol. To analyzing the effects of Selective Packet drop attack in the light of Packet loss, throughput and end-to-end delay in MANET. To propose new scheme to detect malicious nodes in the network which are responsible for triggering the Selective packet Drop attack in the network. Simulation of the detection of Selective packet Drop attack using AODV protocol in MANET using NS-2 tool. In our proposed work we overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes.

V. **CONCLUSION**

In this paper we had studied various types of attack like internal attack, external attack, active and passive attack. The main concern of this paper is to focus on Selective packet drop attack. There are many problem and vulnerabilities in selective packet drop attack which can be removed with help of monitor nodes.

REFERENCES

[1] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, “End to End Delay Analysis of Prominent On-demand Routing Protocols”, IJCST Vol. 2, Issue1, March 2011

[2] ABDUL HAIMID BASHIR MOHAMED, thesis, “ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS”2004

[3] Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, “An Intrusion Detection Tool forAODV-based Ad hocWireless Networks”, 2004

[4] Sevil Şen, John A. Clark, Juan E. Tapiador, “Security Threats in Mobile Ad Hoc Networks”, 2010

[5] S. Sharmila and G. Umamaheswari, “ Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks”, *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*

[6] N.Bhalaji , “Reliable Routing against Selective Packet Drop Attack in DSR based MANET”, *JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009*

[7] Aikaterini Mitrokotsa Rosa Mavropodi, Christos Douligeris, “Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks”, *Ayia Napa, Cyprus, July 6-7, 2006*

[8] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada “On Alarm Protocol in Wireless Sensor Networks”, 2010