Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks

Manjot Kaur[1] Malti Sarangal[2] Anand Nayyar[3]
[1,2]*Department of Computer Science and Engineering, PIT, Punjab Technical University, Kapurthala, Punjab*
[3]*Department of Computer Applications & IT, KCL Institute of Management and Technology, Jalandhar, Punjab*

***Abstract*— The advancement in Wireless Communication have given arise to various Wireless Networks like Mobile Adhoc Networks (MANETS), Wireless Sensor Networks and many more. MANET networks are vulnerable to various types of attacks and threats due to its unique characteristics like dynamic topology, Shared physical medium, distributed operations and many more. There are many attacks which effect the functioning of MANETS' such as denial of service which is most commonly used to affect the network is one of the types of attacks in MANETS. Jellyfish attack has gained its name recently in attack scenario in Mobile Ad hoc networks. JellyFish Attack exploits the end to end congestion control mechanism of Transmission Control Protocol (TCP).**

***Keywords*— Put your keywords here, keywords are separated by comma.**

I. INTRODUCTION

Mobile Ad Hoc Network is an autonomous system of mobile nodes which are connected by various wireless links. MANETS have varying infrastructure topology as a result it is widely effected by both passive and active attacks .Although MANETS provide vast application in emergency, rescue battlefield search and rescue operations and disaster recoveries, Context aware services, commercial and civilian services it still faces various security issues. And in which each node behaves as a router so as to forward the packet data to the neighbouring node. In MANETS the link between the nodes when ever gets break the affected nodes request for new routes and thus new links are established. MANETS have property in which nodes move freely and can organize themselves randomly which makes this network scalable in nature. MANETS work on TCP/IP structure in order to have connectivity between nodes. The traditional TCP/IP model is redefined or modified in order to compensate the MANETS mobility in order to have better functionality. Routing Protocols such as Dynamic source Routing (DSR), Destination Sequenced Distance Vector Protocol (DSDV), Ad hoc on Demand Distance Vector (ADOV) are used for forwarding the packets from one node to another and to establish the network connectivity. [1]

In this paper, Simulation Based study of Jellyfish Periodic Attack in Mobile Ad Hoc Networks is represented using topology of wireless networks with nodes , transmission of packets between the nodes is done using DSR (Dynamic Source Routing Protocol) , parameters such as end to end delay, throughput, packet delivery ratio, energy spent is calculated and represented through X-Graphs.

The following Sections are dived into II, III respectively where section II represents the security issues in Mobile Ad Hoc Networks and Section III represents the review of Jelly Fish Attack in Mobile Ad Hoc Networks.

Overview of Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets. It uses source routing which means that the source must know the complete hop sequence to the destination. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. Each node maintains a route cache, where all routes it knows are stored. The route discovery process is initiated

only if the desired route cannot be found in the route cache. To limit the number of route requests propagated, a node processes the route request message only if it has not already received the message and its address is not present in the route record of the message. Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. [2]

JELLY FISH in Mobile AD Hoc Networks

Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. Jelly fish attacks are targeted against closed loop flows. TCP has well known vulnerabilities to delay, drop and mis-order the packets. Due to this, nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack [3].

This attack which follows all TCP rules has characteristic in which jellyfish node diminish the good put, which can be achieved by dropping some of packets or delaying some packets or reordering some packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. It targets TCP's congestion control mechanism.

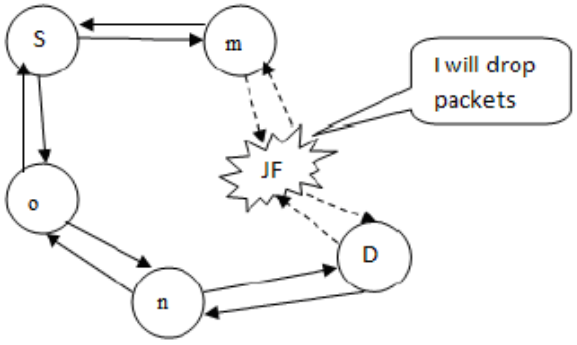

Figure1: Jellyfish Attack Scenario

As shown in Figure 1, node JF is a Jellyfish, and node S starts to communicate with node D after a path via the Jellyfish node is established. Then the Denial of service attacks launched by node JF will cause packet loss and break off the communications between nodes S and D eventually. [8].

Jellyfish Attack Classification

Jellyfish attack is further classified into three sub categories

- Jellyfish recorder attack
- Jellyfish periodic dropping attack
- Jellyfish Delay variance attack.

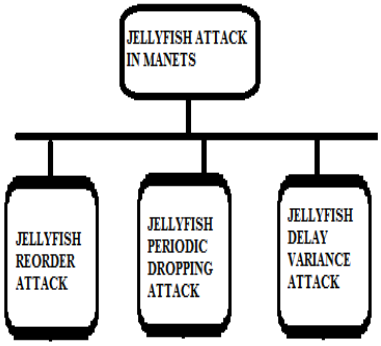

Figure 2: Jellyfish Classification

Jellyfish Reorder Attack

Jelly Fish Reorder attack is possible due to well-known vulnerability of TCP. Jelly fish attacker uses this vulnerability to record packets. This is possible because of factors such as route changes or the use of multi path routing.

Jellyfish Periodic Dropping Attack

Periodic dropping is possible because of sarcastically chosen period by the mischievous node. This kind of periodic dropping is possible at relay nodes. Suppose that congestion losses force a node to drop α% of packets. Now consider that the node drops α% of packets periodically then TCPs throughput may be reduced to near zero even for small values.

Jellyfish Delay Variance Attack

In this type of attack, the malicious node randomly delays packet without changing the order of the packets.

Effects of Jelly Fish Attack

This attack compliance with all data and control protocols as a result its detection and diagnosis is quite difficult to detect. This attacks effects mainly closed- loop flows as such these flows respond to network conditions like packet loss and packet delay. [8]

Conclusion

This paper gives review about the most recent establish attack in wireless networks which is very difficult to detect as it follows all the rules of Transmission Control Protocol (TCP). Strong novel mechanism is the need of hour to develop in order to overcome this attack in the network. We will be using Genetic Algorithm as technique to combat the attack and optimize the network and provides defence to Mobile Ad Hoc Networks against this technique.

References-

[1] Aad and J.P. Hubaux, E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM Transactions on Netwroking,vol.16,pp.791- 802,Aug.2008.

[2] Dhiman Deepika, Nayyar Anand, "*Complete Scenario of Routing Protocols, Security Leaks and Attacks in MANETs*",in Journal Proceedings of the IJARCSEE Volume 3, Issue 10, October 2013

[3] Hetal P. Patel, Prof. Minubhai. B. Chaudhari, *"Survey: Impact of Jellyfish On Wireless Ad-Hoc Network"*, in proceeding of INJCR'10, Volume.10, issue.5, no.2pp. 5-9, 2010

[4] Hepikumar R. Khirasariya, "*Simulation Study of Jellyfish Attack in MANET (mobile ad hoc network) using AODV Routing Protocol*", in proceeding of AISec'10, pp. 1-3, 2010

[5] Kaur Manjot, Nayyar Anand "A Comprehensive Review of Mobile Adhoc Networks (MANETS)" in International Journal of Emerging Trends & Technology in Computer Science (ISSN2278-6856), Volume 2, Issue 6, November - December 2013

[6] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group; Jan 2004.

[7] Perkins, C.: AODV routing implementation for scalable wireless ad-hoc network simulation (SWANS). http://jist.ece.cornell.edu/docs/040421-swans-ao

[8] I.Aad and J.P.Hubaux , E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks" , IEEE/ACM Transactions on Networking , vol.16 pp.791-802, Aug 2008