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. 4, April 2014, pg.199 – 203

REVIEW ARTICLE

A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks

Manjot Kaur[1], Malti Rani[2], Anand Nayyar [3]

[1]Department of Computer Science and Engineering, PIT, Punjab Technical University, Kapurthala, Punjab
[2]Department of Computer Science and Engineering, PIT, Punjab Technical University, Kapurthala, Punjab
[3]Department of Computer Engineering, KCL Institute of Management and Technology Punjab

manu.sembhi@gmail.com [1], malti_87@yaho.co.in [2], anand_nayyar@yahoo.co.in [3]

Abstract— Mobile Adhoc Networks have become a part and parcel of technology advancements due to its working as autonomous system. 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- MANETS, security, Jellyfish attack

I. INTRODUCTION

Mobile Ad Hoc Network is an autonomous system of mobile nodes which are connected by various wireless links and in which each node behaves as a router so as to forward the packet data to the neighboring node. Mobile Ad hoc has basic principal that nodes are free to join and leave the network and there is no central administration. This is the infrastructure less network. This type of networks experiences the dynamic topology. 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. The properties of MANETS have brought tremendous applications in existence. Applications such as automated battlefields, emergency services such as various relief activities, search and rescue operations and disaster recoveries, Context aware services, commercial and civilian services. 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

© 2014, IJCSMC All Rights Reserved

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.

Security is a key property in any network. Availability of network services, Integrity and confidentiality of the data can be achieved by assuring that security issues are met.

MANET functions without any central administration where node communicates with each other on the base of mutual trust. The various characteristic like open medium, dynamic topology, no central administration makes the network more vulnerable.

As this technology usage is increasing day by day in his era providing security is the major issue to this technology. These networks are commonly affected by Denial of Service (DOS) attacks which Protocol-compliant Denial of Service attacks are the most difficult to defend against [1], Aad et al. refer to such attacks as Jellyfish attack.

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.

II. SECURITY ISSUES

Security Flaws in MANETS-An Overview

There are lots of unsolved problems in ad hoc networks; securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons; amongst them are lack of secure boundaries, threats from compromised nodes within the network, lack of centralized management facility, restricted power supply, scalability [1]. Mobile Adhoc Networks have various flaws which make it more vulnerable to attacks-[5]

Non Secure boundaries- The wireless medium does not have proper boundaries outside of which nodes are known to be unable to receive network frames

Compromised Nodes- Ad hoc networks mobility makes its easier for compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity.

No Central Management-The node connects with each other on the basis of blind mutual trust on each other and thus detecting attacks and monitoring traffic is highly cumbersome.

Problem of Scalability- The nodes are free to move in and out which make it more scalable and shrinkable.

Following are the key requirements which check whether the security of network is maintained or not-

- **Availability:** Generally aims denial of service (DoS) attacks and is the ability to sustain the networking functionalities without any interruption because of security threats.
- **Integrity:** ensures that a packet is not modified during transmission.
- **Confidentiality:** ensures certain information is never disclosed to unauthorized entities.
- **Authentication:** ensures that the other end of a connection or the originator of a packet is the node that is claimed.
- **Non Repudiation:** ensures that the origin of a message cannot deny having sent the message.

TABLE I. shows the characteristics and examples of active and passive attacks. Both active and passive attacks can be launched on any layer of the network protocol stack. Table II. [6, 7] shows some examples of attacks on different layers.

© 2014, IJCSMC All Rights Reserved

TABLE I. Passive and Active Attacks

Type of Attack	Characteristics	Examples
Passive Attacks	○ Obtains information without disturbing normal network operation ○ Difficult to detect	Traffic analysis, traffic monitoring and eavesdropping
Active Attacks	○ Can be internal (attacker within the network) or external (attacker outside the network) ○ Can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node	Modification, impersonation, fabrication, jamming and message replay

TABLE II. Attacks on Different Layers of Protocol Stack

Layer	Examples of Attacks
Application Layer	○ Repudiation, Data corruption, Viruses, Worms, Malicious codes
Transport Layer	○ Session hijacking, SYN flooding
Network Layer	○ Sybil attack, Sinkhole attack, Blackhole attack, Grayhole attack, Wormhole attack, Spoofing, Flooding, Location disclosure, Route table overflow, Route table poisoning, Route cache poisoning
Data-link Layer	○ Traffic monitoring and analysis, Disrruption MAC (802.11), WEP weakness
Physical Layer	○ Jamming, Interception, Eavesdropping

III. OVER VIEW OF JELLY FISH IN MOBILE AD HOC NETWORKS

Attackers are always trying to modify messages or generate false messages and thus take down the network's operations which cause denial of service in MANETs. In this section we summary introduce JELLY FISH Attack.

Tremendous progress has been made in order to ad hoc networks by developing secure routing protocols that ensure different security concepts such as authentication and data integrity. Moreover, intrusion detection and trust-based systems have been developed to protect MANETs against misbehaviors such as rushing attack, query flood attacks, and selfish behaviors. Yet, most of the defense mechanisms are not able to detect a set of protocol compliant attacks called jellyfish (JF) attacks.

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. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. 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].

Jelly fish attacks are targeted against closed-loop flows. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. The Jellyfish attack is one of those kinds. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet

© 2014, IJCSMC All Rights Reserved

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. Reference also described that malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets.

This attack mainly targets closed-loop flows as such flows respond to network conditions like packet loss and packet delay. It targets TCP's congestion control mechanism. The main goal of the Jellyfish nodes is to reduce the good put of all the flows to near-zero by either reordering the packets or dropping a small fraction of packets. [4] These forwarding mechanisms are variants of Jellyfish attack.

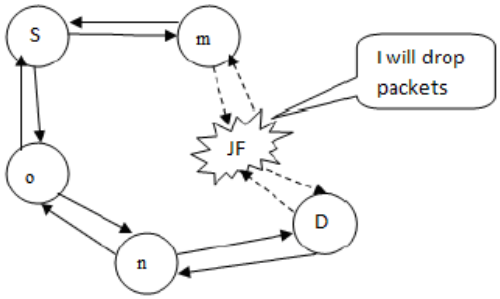

Figure2: Jellyfish Attack Scenario

As shown in Figure 2, 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. [3].

Jellyfish Attack Classification

Jellyfish attack is further classified into three sub categories

Jellyfish recorder attack, Jellyfish periodic dropping attack and Jellyfish Delay variance attack.

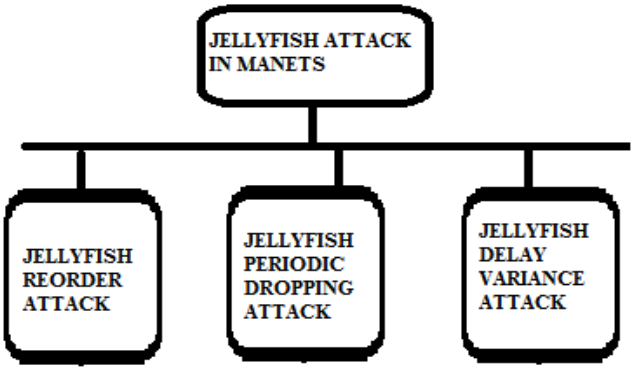

Figure 3:Jellyfish Classification

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

© 2014, IJCSMC All Rights Reserved

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]

IV. 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 defense 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

© 2014, IJCSMC All Rights Reserved