Tracking Down Long ICMP Dos Attack in Wireless LAN

Geetam
Computer Science and Engineering, MITM,Jevra,Hisar Haryana,India

Vikas Malik
Computer Science and Engineering, MITM,Jevra ,Hisar, Haryana,India

Abstract. Internet Control Message Protocol (ICMP) is a query processing and error reporting protocol and it works on network layer. This protocol ensures correct data distribution, but fraudulent user may exploit this protocol to block a service or to intercept data. Security is of great concern in such networks. But before developing security mechanism to protect network against threat, it is crucial to understand the how such attacks actually works and we should have full knowledge about their characteristics and their impacts. In this paper, we present our approach to simulate the Long ICMP Dos Attack, and to analyze – how the network behaves under attack. Various parameters like Wireless LAN delay & radio receiver of mobile nodes are also discussed.

Keywords: Wireless, Protocol, Service, ICMP

I. INTRODUCTION

E-commerce & M-commerce related Transactions like online billing payment requires the exchange of confidential information like credit card number. Unauthorized user may try to attack their websites to disrupt a service. Such attacks can be denial-of-service attack [1, 10]. A denial of service attack (Dos attack) is an attack to make a computer resource unavailable to authorized users [2, 7]. To prevent or mitigate the Dos attack is not an easy job, unless how such attacks work is completely understood. Dos attacks can be classified by many criteria's [8]. Basically, there are two methods of attacking.

Semantic Attacks: Semantic attacks disrupt a particular feature of any application installed at the victim's side or exploit a specific feature of any protocol in order to consume excess amounts of its resources [3, 5].

Brute-force Attacks: Brute Force attacks are performed by sending a large amount of legitimate requests for transactions. The common targets are Web servers, DNS look up servers, switch, hub, repeater, gateway [4, 6].

II. LITERATURE REVIEW

A lot of research has been done in the field of Denial-of-service Attack.
Mitko Bogdanoski [11]. Denial of Service (Dos) Attacks in wireless network, by sending erroneous ICMP redirect packets, a malicious host can either intercept or disrupt information from a wireless access point. He presents a technique to evaluate and analysis the effects of Ping Attack on wireless network
Khaled M. Elleithy [12].Attacks techniques vary from sending of unlimited requests to a server in an attempt to crash it, flooding a server with abundant number of packets of invalid data, to send the requests with a forged IP address. In this paper he shows the analysis and implementation of three types of attack: Ping Attack, TCP SYN Flood, and DDOS. The Ping attack has been analyzed on a Windows 95 personal computer. The TCP SYN Flood attack will be simulated against a Microsoft Windows 2000 IIS FTP Server. DDOS has been analyzed by a zombie program that will carry the Ping attack. This paper will demonstrate the various damage from Dos attacks and analyze the mitigations of the damage.
Agustin Zaballos [13] presented his views as Network security now days have become important for both network implementation & design. Due of this, the need of making secure communications over the network has increased at the same pace as the accessibility to services of Internet. Although security is a delicate issue in e-business, but it may be impossible to measure its effectiveness in real life because of the network administrators fears. To find a solution to this particular problem, once more simulation opens the way to solve the problems that are difficult to fix in real life

H. Garantla-[15] this paper evaluates firewalls, their value in securing network and its functions such as performance, security and efficiency. The relation between the performance efficiency and security is presented through different scenarios and the relationship between performance and security in firewalls is evaluated.

III. METHODOLOGY

The Step-by-Step procedure for the implementation of Long ICMP Ping Flood Dos attack in a typical network is as under. We are designing two scenarios for this. Scenario1 is designed to depict the behavior of Wireless LAN network under no attack.Scenario2 is designed to depict the effect of Long ICMP Ping Flood Dos attack on Wireless LAN network. Table 1 is representing the number of malicious nodes & number of victim nodes present in scenario 1 & scenario 2.

Table 1. Number of Attackers and Victim Present In The Network.

Network Type	Number of Malicious nodes	Number of Victim
Wireless LAN (scenario 1)	**0**	0
Wireless LAN (scenario 2)	8	1

3.1 Wireless Local Area Network under No Attack

Design a wireless local area network as shown in figure1 (scenario1). In this figure, set of wireless workstations are arranged around the wireless router. The router is acting as the central node. BSS Identifier was assigned to each wireless router and same identifier was assigned to rest of the workstations. BSS identifier is used to connect the workstations to router virtually. Two separate LANs were designed and both routers are linked to switch. Connect the FTP server to switch. In this scenario, there is no attacker and no victim node. Run the simulation after setting the duration to 20 min.

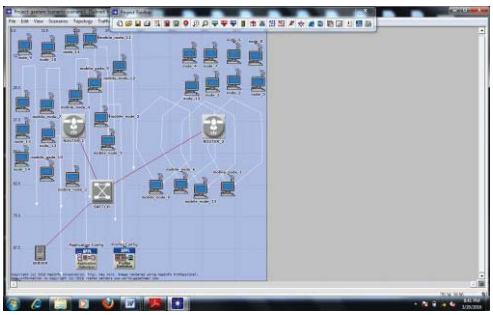

Fig. 1. Wireless LAN under No Attack (scenario1).

3.2 Wireless LAN under Long ICMP Ping Flood Dos Attack

Design a wireless local area network as shown in figure2 (scenario2).The design view of scenario2 is similar to scenario1 but apart from that, assign unique IP Address to each work station & ftp server. Configure the Long ICMP Ping flood traffic in the entire wireless LAN. The nodes chosen for disrupting a service are attackers and fileserver is a victim. In this scenario, there are 8 attackers (wireless workstations) and 1 victim node (ftp server). Run the simulation after setting the duration to 30 min.

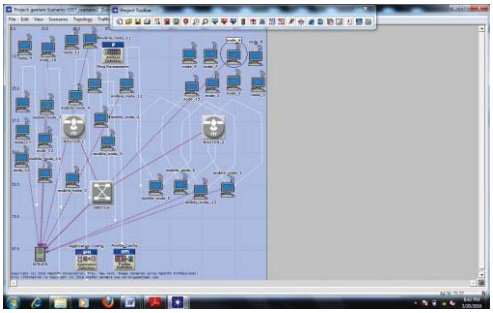

Fig 2. Wireless Local Area Network under Dos Attack (scenario 2).

IV. RESULTS AND DISCUSSIONS

This section describes the simulation results. Opnet tool is used for analyzing the typical network performance under long ICMP Dos attack at low cost. In network simulation, the various statistics need to be chosen. Here, we are choosing node statistics & global statistics. Inside the global statistics Wireless LAN is chosen & inside the node statistics radio receiver is chosen. These statistics are described as under with the help of graphs.

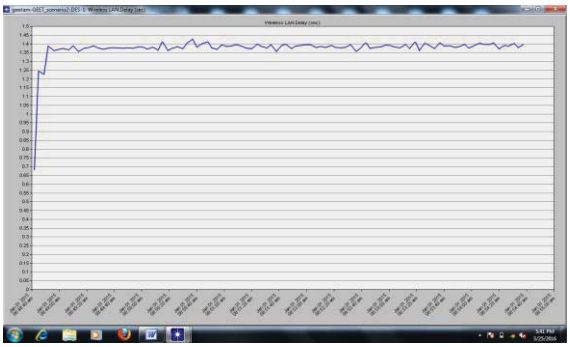

Fig.3 Wireless LAN Delay under Attack

The figure 3 shows the graph obtained after the completion of simulation. It shows the delay during transfer of IP packets between nodes and server. The Wireless LAN delay is measured in second. Initially, the IP packets were received with delay 0.7 sec. After that, most of the nodes are receiving packets with delay 1.4 sec. At last, blue line indicating Wireless LAN delay disappears (figure 4). It disappears because server is completely under ping attack. The server fails to respond. No packets were exchanged after attack so in turns no delay.

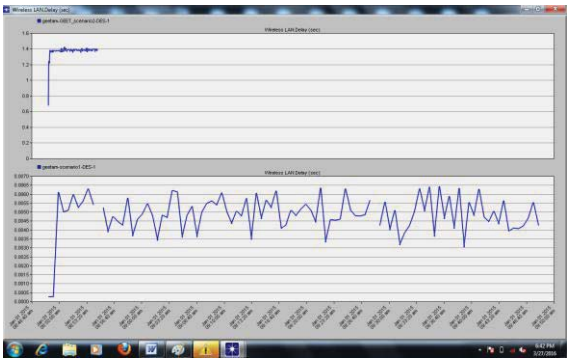

Fig.4 Wireless LAN Delay comparison under Attack and no attack

The graph in figure 4 is just depicting the comparison between two networks. One is under ping attack(figure 3) & other is not under attack(figure 5).

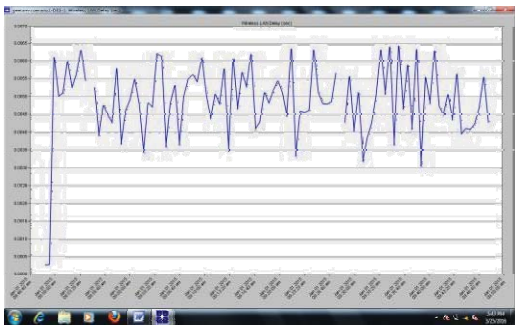

Fig.5 Wireless LAN Delay Under No Attack

In this graph as shown in fig 5, blue line is indicating the overall wireless lan delay between workstation and server . We can easily see that the nodes are receiving IP packets within the range of 0.0032 sec to 0.0062 sec. Therefore, the delay in this network (figure 5) is very much less than in the network under ping attack (figure 5).

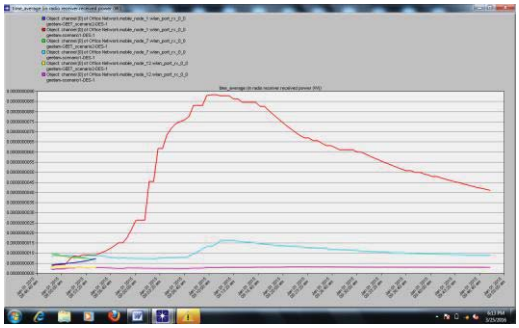

Fig.6 Radio receiver when under attack & no attack

In the network presented in scenario2 consists of fixed nodes & mobile nodes. The graph in figure 5 is depicting radio power received by mobile nodes. The recieved power was measured in Watts. The pink color, fushia color, red color line indicates radio power received by mobile nodes when not under attack. The blue color, yellow color, green color indicates the radio power received by mobile nodes when network is under attack. The radio power received by mobile node 7 for a small interval of time under attack reaches 0.0000000010 maximal point and radio power was received for a long interval of time when not under attack reaches at 0.00000000018 maximal point. The radio power was low because mobile nodes was not getting any response from server (as server's service was disrupted due to attack). Similarly, mobile node1 reaches 0.0000000090 maximal point (when under no attack) & reaches at 0.0000000007 maximal point (when under attack).). Also, mobile node 12 reaches 0.0000000004 maximal point (when under no attack) but the power was received for a long time in comparison to other network which reaches at 0.0000000003 maximal point (when under attack).

V. CONCLUSION

In this paper, the effects of the ICMP Ping Flood Attack on the wireless network were explored. To examine the behavior of a victim node when it is under an icmp ping flood denial of service attack a network is created virtually using simulation tool. Moreover, behavior of wireless networks under attack of different number of attackers is also examined. The Paper presented a few results to show how the network gets congested and node that is attacked. After examining all the graphs obtained after the completion of the simulation we conclude that as the attacking nodes continuously sent ping messages to the target node without worrying about the replies from that node to slowdown the victim node performance. A significant decrease in radio receiver has been noticed which depicts the increase in network congestion and in turn slow down the target's performance.

VI. FUTURE PROSPECTS

The concept behind the attack and its impact on the network and the network characteristics can now be very well understood. These simulations will help to build the efficient detection system using appropriate mitigation method. An efficient dos prevention and dos detection system can now be easily built once the concept behind the attack is clear. After examining the impact of attacks by virtually creating a network, better mechanisms can be proposed in order to prevent from these attacks.

REFERENCES

[1] J. Li, C. Manikupoulos, " Modeling Distributed Denial of Service attacks using OPNET Modeler‖" New Jersey Institute of Tech., University Heights, Newark, NJ 07102, USA [Online]..

[2] Shuchi Juyal , Ruchika Prabhakar," A comprehensive study of Dos attacks and defense mechanism ", Journal of Information and operation management, Volume 3, Issue 1, 2012, pp-29-33.

[3] Tao peng, "Defending against Distributed Denial of Service", University of Melbourne, 2004.

[4] Seema Gulati , "Mitigating ROQ Attacks using Flow Monitoring Method", International Journal of Engineering Trends and Technology (IJETT) , Volume 4, Issue 9, Sep 2013.

[5] Gayatri Bhatti,"A Meliorated Defense Mechanism for Flooding Based Attacks", International Journal of Soft Computing and Engineering(IJSCE), ISSN:2231-2307, Volume-3 , Issue-1,March 2013.

[6] Neha Titarmare, " DDOS Detection using Attack Model" * Priyanka Gonnade, Punam Marbate Nayan Hargule," DDOS Detection using Attack Model", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014 ISSN: 2277 128X Research Paper Available online at: www.ijarcsse.com.

[7] Monika#1, Swati Kapoor*2,"Mitigating Dos Attack in VPN",International Journal of computer trends and technology(IJCTT),volume 4 issue 5 ,Month 2013 ISSN: 2231-2803 http://www.ijcttjournal.org Page 1191.

[8] Muhammad Aamir , Muhammad Arif,"Study and Performance Evaluation on Recent Dos trends of Attack and Defence", I.J. Information technology and computer science 2013, 08, 54-65 Published Online July 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2013.08.06.

[9] SANS Institute. Egress filtering v 0.2, 2000.

[10] ARS technical, Joel hrushka. (2008, August) ,"Phlashing" attacks could render network hardware useless [Online].Avaliable: http:// arstechnica.com/security/news/2008/05/ phlashing-attacks-could-render-networkhardware-useless.ars.

[11] Mitko Bogdanoski,"Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques" International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, April 2011.

[12] Khaled M. Elleithy ,"Denial of Service Attack Techniques: Analysis, Implementation and comparison, systemics, cybernetics and informatics" volume-3 Number 1SSN:1690-4524 .

[13] Agustin Zaballos, G Corral , I Serra , J Abella ,2003," Testing Network Security Using OPNET".

[14] Subramani Rao, "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis", SANS Institute Infosec Reading room H. Garantla- "Evaluation of Firewall Effects on Network Performance".