IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 2, February 2016.
www.ijiset.com
ISSN 2348 – 7968

A survey on Denial of Service (DoS) attack on wireless network

Prof. Sarang Kulkarni[1], Prof.Atul Mali[2] and Prof. Dhanaraj Yerate[3]

1,2,3 Asstt.Prof., Dept of CSE,Karmayaogi Engineering College, Shelve- Pandharpur, MH, India.

Abstract

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Many users can use this alternative to enlarge their available wired network or to go completely wireless. Security is one of the most important factors for every mobile communication network. Network security is a big concern for individuals and organizations because vital information is available on the network and most difficult process of the business are completed through the Internet. If a network is to fail or security is compromised an organization could be completely crippled. For example, if Wal-Mart was to lose their cash register network than they would suffer a huge loss of business and would take, depending on the severity of the breach, several hours to days to fix.

A different types of attacks have been confirmed through the earlier days. According to our thinking, most of the attacks were targeting wired network that much extended. The commodity of the intermediate in wireless networks makes it simple for an adversary to initiate a Wireless Denial of Service (WDoS) attack. A DoS is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Denial of Service attacks is termed one of the worst attacks and is next to impossible to track. Some things that can be done to reduce the risk of being stung by a denial of service attack include: (windowsecurity.com)

a) Not running your servers at a level too close to capacity.
b) Using packet filtering.
c) Keeping up-to-date on security-related patches.

All existing research work exhibits that such attacks can easily be accomplished. For example a jammer can continually transmit a radio signal in order to block any access to the medium by legitimate wireless nodes.

Keywords: Wireless Denial of Service (WDoS) attack, packet filtering,Wal-Mart, security patches.

1. Introduction

In the present days wireless networks gain more ground day by day with the advances in wireless technology. They are becoming more reasonably priced and easier to be built. They are much easier to be compromised than any wire-line network is the main disadvantage of wireless networks [1]. For an adversary to launch an attack the commodity of the medium used for wireless data transfers makes it extremely easy. On the other hand, in wireless networks there are many circumstances where the attack can be much easier for an opponent [3]. It is practical to even obstruct any sense of communication connecting two wireless capable nodes. Jammers can exist in more intellectual ways to achieve their task without being identified. The discovery of the transmission of a control packet and the jammer to preferentially acquire interference intend at corrupting that meticulous packet [2]. In order to take in hand these threads, safety experts must deploy more well-organized methods for detecting and put off the attackers.

A variety of simple jamming models have been obtainable. Despite their openness these models have been established to be very effective. The jamming situation will best tell us the suitable standard to use in order to compare two different jamming methods for a meticulous case. In all works that have to contract with jammers there are two main metrics that are being used. The jamming is divided into two categories as Physical and Virtual Jamming attacks. The physical jamming is launched by continuous transmissions and/or by causing packet collisions at the receiver. Virtual jamming occurs at the MAC layer by attacks on control frames or data frames in IEEE 802.11 protocol.

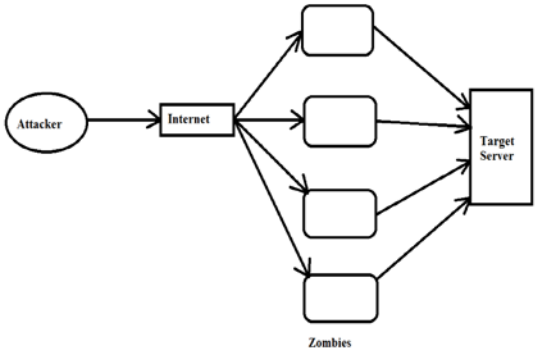

Figure 1: Denial of Service Attacks.

For instance, energy competence may be the most significant metric for sensor networks where nodes are accepted to live for an extensive time. In all cases a jammer wants to be energy proficient and to have low likelihood of discovery in order to be cautious. This can be attaining by maintaining constancy with MAC layer behaviors. We can also define metrics that enumerate the competence of a jammer. The quantitative metrics that we will use to explain the effectiveness of a jammer must be

ISSN 2348 – 7968

connected with the aptitude of the wireless device to transmit or receive data [4] [5].

1. RELATED WORK

In this paper a method is designed with a well effective framework oriented strategy where there is an effective implementation of the system takes place
in a well efficient manner respectively [6][7]. Here the design orientation of the present technique is shown in the below figure in a well oriented fashion and shown in the block diagram representation and explains in a elaborative fashion respectively. Here the present designed technique is implemented in a well efficient fashion where it supposed to analyze the problems related to the previous methods followed by the proper analysis made on these particular oriented strategy where it is supposed to analyze the problems related to the several previous methods in a well efficient manner and also effectively improve the performance of the system in a well oriented fashion respectively [8][9]. Here we finally tell that the present designed technique completely overcome the problem related to the several previous methods and rapidly improve the
performance of the system in a well analogous fashion oriented scenario [10].

2. CONCLUSION

Wireless networks are very common in the workplace as well as in the home. Technology has been created to store, transmit and receive data through networks at very high rates of speed. Networks have become essential to completing daily business tasks and most business, those who rely heavily on information technologies, would be crippled without their networks.

Advances in networking storage have allowed for organizations to use their networks not only for the sharing of resources but to store large pools of data to be used for data analysis. Companies can now store detailed profile information for customers at a very low cost. In the future, the speed of networks will increase as they have in past years. The cost of networks will continue to decline and using a network will be essential for every organization. As computing technology increases in power, and decreases in size, the price of creating a high-powered full featured network will decrease rapidly.

References

[1]MithunAcharya, Tahu Sharma, David Thuente,David Sizemore, Intelligent Jamming Attacks in 802.11bWireless Networks, in Proceedings of theOPNETWORK-2004 Conference.

[2]WenyuanXu, Wade Trappe, YanyongZhang,Timothy Wood, The Feasibility of Launching andDetecting Jamming Attacks inWireless Networks, MobiHoc 05, May 25-27, 2005, Urbana-Champaign,Illinois, USA, pp 46- 57.

[3]WenyanXu, Ke Ma, Wade Trappe, YanyongZhang,Jamming Sensor Networks: Attacks and Defense Strategies, IEEE Network, May/June 2006.

[4] Y. Law et al., Link-Layer Jamming Attacks on SMac,Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 21725.

[5] G.Noubir, On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility, Technical Report, December 2003.

[6] Y. Law et al., Link-Layer Jamming Attacks on SMac, Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 21725.

[7] A. Wood and J. Stankovic, Denial of Service in Sensor Networks, IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 5462.

[8] G.Noubir, On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility, Technical Report, December 2003.

[9] Curtis D. Schleher, ElectronicWarfare in the Information Age, 1999, Norwood, Artech House.

[10] G.Noubir, G.Lin, Low Power DoS Attacks in Data Wireless LANs and Countermeasures, in Proceedings of Poster: ACM MobiHoc 2003. Annapolis, MD: ACM Press.