ANALYSIS OF DENIAL OF SERVICES ATTACK ON SENSOR NETWORK

Shubham Kumar [1], Yogesh Kumar [2]
M. Tech Scholar [1], Assistant professor [2]
Department Of Computer Science Engineering
School Of Engineering & Technology
A Unit of Ganga Technical Campus, Soldha, Bahadurgarh M. D. University, Rohtak, Haryana (India) [1,2]

Abstract: Wireless sensor networks are currently used in various fields. Security issues are very important because the information sent over the wireless sensor network is very sensitive. A denial of service (DOS) attack is a fundamental threat to wireless sensor network functionality. This article discusses the most common DOS attacks and their potential defenses. Case studies show interference attacks, one of the most common attacks on wireless sensor networks. In the introduction of this article, the author assumes that attack interference may cause serious damage to wireless sensor networks. This hypothesis has been demonstrated in simulation scenarios and case studies with simulation results. In this sense, DoS, especially DDoS, not only threatens the Internet, but it is also widely used in cybercrime, threatening the security of citizens. Therefore, it is important to fully understand the characteristics of the DDoS problem and to study corresponding defense mechanisms that make important contributions not only to academia and industry but also to social security and emergency management agencies. And help the ability. Stakeholders make the right decisions in the face of DDoS threats. In existing research work, various types of issues, such as detection of DoS attacks, can be modeled by modeling normal traffic and attack traffic and treating the issues as network conditions (rather than single packets or other units) it is based. Classification Problems the current state of the network as good or bad to detect attacks when they occur. The other is that transmission failures and deadline errors can lead to process interference and reduced overall control performance. In the future, all these will be solved by DSR algorithms of DSR attack detection and wireless sensor network encryption and BS, CH WSN. As the number of communication rounds increased, this proposed an energy depreciation form of network energy. Levels tend to fall, approach the final scenario and go to zero. A comparison and conclusion of initial energy loss is that energy loss decreases rapidly after WSN dos and DDoS attacks. So anomalous energy savings tell us that we should perform DOS and DDOS attacks on our network. At the end of the simulation, another Run button on the GUI is the result of comparing the DoS initial and suggested tasks. It is clear that the proposed study is better than previous ones.

Key Word: DOS, DDOS, WSN, MATLAB ,Attack

1. Introduction

DoS attacks can be implemented as flood attacks or logic attacks. Flood DoS attacks are based on brute force attacks. If possible, please send the victim the truthful but unnecessary data. The result is wasted network bandwidth, unneeded disk space (spam, junk files, intentional error messages, etc.) fills up, and fake information in the host software's fixed-size data structures. It fills up and wastes processing power. To amplify these effects, DoS attacks may work together from multiple sources simultaneously (Distributed DoS, DDoS). Logical DoS attacks are based on intelligent exploitation of vulnerabilities in the target. For example, well-crafted segmented Internet Protocol (IP) data can cause a system crash due to a major failure of the operating system (OS) software. Another example of a logical attack is to exploit the lost authentication requirements by inserting incorrect routing information to prevent traffic from reaching the victim's network. There are two main reasons why DoS attacks are attractive to attackers. The first reason is that expertise is not always necessary, as there are effective automation tools that can be used to attack the victims. The second reason is that attackers cannot usually find out without extensive human intervention or most routers on the Internet do not have new features. DoS attacks exploit vulnerabilities in end hosts, routers, and other systems connected to computer networks. Populations with the same vulnerability can grow in size. In July 2003, a vulnerability was discovered in Cisco routers and switches running any version of Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets. This vulnerability blocks the interface and can cause a DoS condition without triggering an alert. Another common example is the Microsoft Windows Metafile (WMF) vulnerability. This was discovered in December 2005 in all versions of Windows 98, 98SE, ME, 2000, and XP. The vulnerability could allow malware to be installed on these hosts, for example to send DoS attack traffic. However, exploiting this vulnerability requires user interaction.

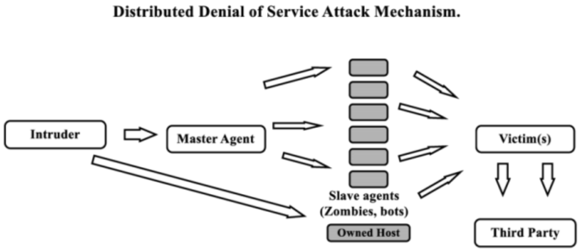

Fig 1.1: DOS attack in WSN

2. Distributed Denial Of Service Attack

Try to prevent or reduce resource availability by sending attack traffic using multiple source hosts at the same time. Typically, DDoS attack participants form a hierarchical DDoS network in which an attacker controls multiple hosts (or handlers), which in turn control a large number of agents (or daemons, zombies, bots). Real Attack Victims These definitions are:

✓**Agent (or daemon or zombie or bot):** Infected host used to send attack traffic in DoS attacks.

✓**Master (or handler):** A damaged hosts are used to control the operation of many agents.

✓**DDoS network:** A hierarchical owner groups and people groups can more easily control attacker DDoS attacks. DoS attacks are destructive or derivative.

✓**Destructive DoS attack:** Block resource availability completely.

✓**Degradative (non-destructive) DoS attack:** Reduce the performance of resources. For example, a harmful DoS attack can result in a system crash or a full disk partition. In such cases, recovery usually requires human intervention. Usually, downgraded DoS attacks cause only temporary problems, and the system recovers automatically when the attack is over. An example of a downgrade DoS attack is a flood attack that overloads a network link or host central processing unit (CPU). However, long, high-bandwidth flood attacks can produce unexpected results, such as system crashes.

✓**Deployment phase:** Installation a malicious programs on a set of infected hosts for later use as a source of DoS attack traffic.

✓**Attack phase:** Coordinate the transmission of attack traffic to the victim.

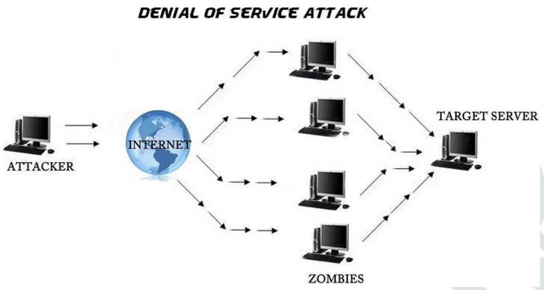

Fig 2.1: DOS attack through different routers

3. Problem Formulation

This study is designed to help all network users mitigate DoS attacks and DDoS in IP-based networks. This white paper focuses on the following: You need to understand existing attack mechanisms and available defense mechanisms, and have a general understanding of the benefits of each defense mechanism (best case performance). Possible dependencies of defense mechanisms should be recognized, and if there are multiple defense mechanisms for a particular attack type, the most appropriate defense can be selected.

4. Methodology

The main contribution here is to study the resiliency of the three ad hoc routing protocols against fall-off range attacks. This is a new DoS attack on ad hoc routing. The routing protocols are destination sequence distance vector (DSDV), ad hoc on demand distance vector (AODV), and dynamic source routing (DSR) protocols. The research method is based on the use of the ns-2 network simulator to analyze transmission delays in small ad hoc networks. The enemy performs range attacks using nodes in an ad hoc network.

5. Simulation Layout and Execution Result

The following figure is displayed after running MATLAB. The simulation was run in MATLAB 2013a and the results are shown below. This clearly shows the proposed scenario and method.

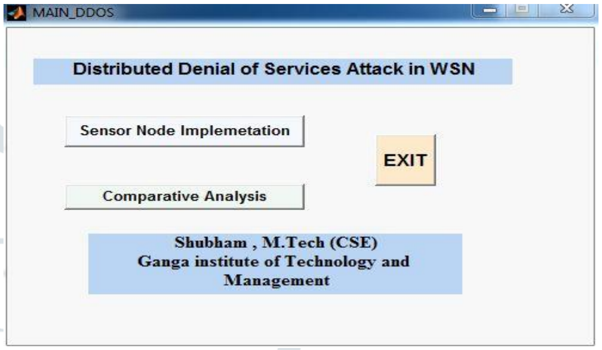
MAIN_DDOS
Distributed Denial of Services Attack in WSN
Sensor Node Implemetation
Comparative Analysis
EXIT
Shubham , M.Tech (CSE)
Ganga institute of Technology and
Management

Figure 4.1: The basic layout built in MATLAB 2013 has two buttons

This proposed an energy depreciation form of network energy as the number of communication rounds increased. Levels tend to fall, approach the final scenario and go to zero. Comparing energy loss between the above two tables, it can be concluded that energy loss decreases rapidly after Dos and DDoS attacks on WSN. So anomalous energy savings tell us that we should perform DOS and DDOS attacks on our network.

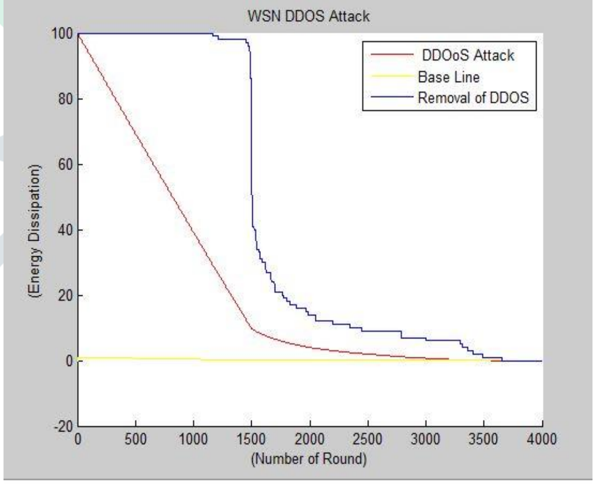

Fig 4.2: Energy Dissipation Vs. Number of Rounds

Table 1: Energy Dissipation (Attack) vs. Energy Dissipation (Removal)

Number of Rounds	Energy Dissipation (Attack)	Energy Dissipation(Removal)
0	0	0
500	25	0
1000	60	0
1500	90	60
2000	96	12

2500	99	8
3000	0	5
3200	0	4
3500	0	0

Energy dissipation of DDoS attack in respect to number of round of communication shown above. The compare the fall in Energy dissipation when DDoS attack with Removal of DDoS is very clear. The fall of dissipation rate very fast during the attack and normal without attack. The base line is when there is no communication. The above figure will be displayed after the end of the simulation. This is the result of comparing the initial work of DDoS with the proposed work. It is clear that the proposed study is better than previous ones.

6. Conclusion & Future Scope

DoS Attacks and Distributed DoS are part of an organizations overall risk management strategy. Organizations need to identify the most important DoS risks and implement cost-effective defense mechanisms against the types of attacks that have the highest risk of business continuity. According to research and news on real-world DoS attacks, these attacks are not only one of the most common cyber security risks, but they also prevent the entire organization from leaving the internet during an attack. In the future, DoS attacks will occur because the number of connected hosts on the internet will increase, access lines will become faster, software products will become more complex, and security for ordinary home users and many people will be difficult to organize. Problems will increase the more hosts on the internet, the more likely they will be used for DoS purposes. The strength of the DoS attack also increases as more hosts can generate more traffic through faster internet access lines. As software becomes more complex, there will be more of those vulnerabilities that can be used to compromise a host. The fast pace of new revisions does not make the situation easy. Finally, it is still difficult to assess the security risks of existing computer systems, especially for the average person.

6. REFERENCE

[1] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[2] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[3] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.

[4] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer journal of IEEE Communications Magazine, Vol. 40, no. 10, pp. 42-51, 2002.

[5] R. Puri, Botsand Botnet an overview, Aug.08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.pdf

[6] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ ddos–whitepaper.html

[7] CERT, Denial of Service Attacks, June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html

[8] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures, EURASIP Journal on Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.

[9] Yahoo on Trial of Site Hackers, Wired.com, Feb. 8, 2000, [online] http://www.wired.com/news/business/0,1367,34221,00.html

[10] Powerful Attack Cripples Internet, Oct. 23, 2002, [online] http://www.greenspun.com/bboard/q–and–a–fetch–msg.tcl?msg id=00A7G7

[11] Mydoom lesson: Take proactive steps to prevent DDoS attacks, Feb. 6, 2004, [online] http://www.computerworld.com/s/article/89932/Mydoom lesson take proactive steps to prevent DDoS attacks Taxonomy ID=017