International Journal of Advanced Trends in Computer Applications
www.ijatca.com

VARIOUS DDOS PREVENTION TECHNIQUES: A SURVEY

[1]Navjot Singh, [2]Sarabdeep Singh
[1]Research Scholar, CEC, Landran, Mohali
[2]Asst. Prof., ECE, CEC, Landran, Mohali

Abstract: *Security and Privacy are two important parameters that need to be considered when dealing with Wireless Sensor Networks as WSN operate in an unattended environment and carry sensitive information critical to the application. However, applying security techniques that consume minimum resources is still a challenge and this paper makes an attempt to address the same. One of the major attacks in sensor network is Denial of Service(DoS) attack that not only diminishes the network capacity but also affects the reliability of information being transmitted. Distributed Denial of Service attack is a coordinated attack, generally performed on a massive scale on the availability of services of a target system or network resources. Due to the continuous evolution of new attacks and ever-increasing number of vulnerable hosts on the Internet, many DDoS attack detection or prevention mechanisms have been proposed. In this paper, we present a comprehensive survey of DDoS attacks, detection techniques.*

Keywords: *DDoS, Wireless Sensor Network*

I. Introduction

WSNs deployed in non-deterministic environment are usually prone to Distributed Denial of Service attacks (DDoS) that not only diminishes the network performance but also affects the reliability of information. Detecting DDoS threat is more crucial than recovering from the attack. Generally, attackers launch DDoS attacks by directing a massive number of attack sources to send useless traffic to the victim. The victim's services are disrupted when its host or network resources are occupied by the attack traffic. The threat of DDoS attacks has become even more severe as attackers can compromise a huge number of sensors by spreading worms using vulnerabilities in popular operating systems. A revolution came into the world of computer and communication with the advent of Internet.

Today, Internet has become increasingly important to current society. It is changing our way of communication, business mode, and even everyday life [1]. Almost all the traditional services such as banking, power, medicine, education and defense are extended to Internet now. The impact of Internet on society can be seen from the fig. 1 which shows exponential increase in number of hosts interconnected through Internet [2]. Internet usage is growing at an exponential rate as organizations, governments and citizens continue to increase their reliance on this technology A DDoS attacker uses many machines to launch a coordinated DOS attack against one or more targets [5]. It is launched indirectly through many compromised computing systems by sending a stream of useless aggregate traffic meant to explode victim resources. As a side effect, they frequently create network congestion on the way from a source to the target, thus disrupting normal Internet operation. The number of DDoS attack has been alarmingly increasing for the last few years [6]. Many of today's DDoS attacks are carried out by organized criminals targeting financial institutions, e-commerce, gambling sites etc [7].

A classification of a wide range of DDoS attacks found in the wild is presented in [4, 8] that Internet providers and users need to be aware of. Usually, it can be launched in two forms [9]. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to use massive volumes of legitimate looking but garbled packets to clogs up computational or communication resources on the target machine so that it cannot serve its legitimates users.

The first publicly reported DDoS attacks appeared in the late 1999 against a university [10]. These attacks

quickly became increasingly popular as communities of crackers developed and released extremely sophisticated, user friendly and automated toolkits to carry them out. At present, even people with little knowledge can use them to carry out DDoS attacks. The impact of DoS attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business.

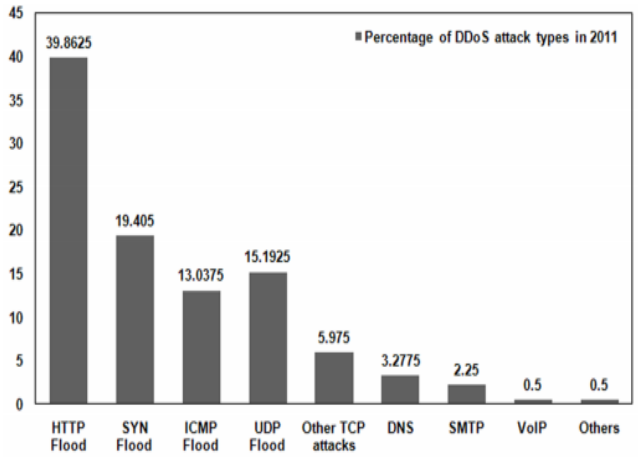

Figure. 1 Statistics of DDos attacks

This paper will present the various DDos prevention techniques. The remainder of the paper is organized as follows. Section II contains overview of DDoS prevention methods in past years. Section III will give overview of DDos attacks, Section IV will give the various prevention techniques, Section V will give the conclusion of this paper.

II. RELATED SURVEY

This section presents the work of eminent researchers in the field, highlighting the challenges in the existing solutions.

Flooding DoS attack poses a great threat as it generates large volume of traffic that prevents the legitimate user from accessing the service. It causes the links to be blocked and nodes to crash resulting in decreased network performance and even more sensors become useless due to depletion of energy in sending useless packets. A number of approaches have been proposed to counter the attack.

Wood *et. al.* in [1] has summarized different DoS attack and their effect on the sensor network. They have listed various possible attacks in each layer which tells the importance of security features in sensor nodes. Studies [2,3] shows the survivability of wireless adhoc networks in term of link connectivity and stability between sensor nodes but they lack in considering the security of sensor network. For instance, Wang [4] and Ali et.al. [5] proposed secure packet transfer using encryption, decryption and authentication of packet header but the performance of PKC is not yet good due to resource constraint nature of sensor network. Chiang *et al.* [13] proposed architecture by adding duplicated hardware by which the reliability and availability of sensor networks can be increased but redundant hardware requires additional costs.

Researchers [6, 7] proposed security mechanisms against DoS attacks but the proposed solutions cannot handle wide range of DoS attacks.

C. Meadow [21] proposed stronger authentication between communicating parties across a network but it while attempting to prevent DoS leaves itself open to attack due to high computational load required to defend the attack wherein [22] uses payment approach and assumes that node willing to access resources would have to pay charges according to the level of service needed. This approach does not provide total solution as legitimate nodes refusing to pay would be denied of accessing service.

Authors in [8, 9, 10] use congestion algorithms to detect upsurges in traffic that can give rise to DoS but these approach may apply only simplistic signatures and also requires state information to be held on the nodes which is not a feasible solution in sensors because of limited memory. Shyne and Sterne in [11, 12] uses statistical monitoring to detect upsurges in traffic of a particular type and raise alert if something unusual is detected. Here a single alert can notify about many attack packets but it requires human intervention to monitor upsurges so is inefficient.

A critical look at the literature highlights the fact that although lot of work has been done towards the security of WSN however, nothing has proved to be so significant so as to be considered as best. Moreover, researchers have ignored the fact that software agents especially ants can be used as security staffers and can provide a protection against DDoS in WSN.

III. OVERVIEW OF DDOS ATTACKS

A Distributed Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like web, email or network connectivity, that they would normally expect to have. DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [20]. In the Fig. 2 simplified Distributed DoS attack scenario is illustrated. The figure shows that attacker uses three

zombie's to generate high volume of malicious traffic to flood the victim over the Internet thus rendering legitimate user unable to access the service.

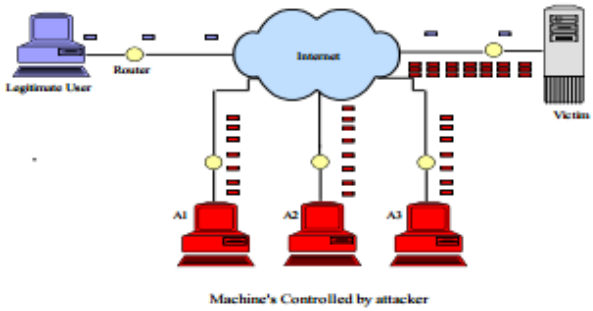

Figure.2 Ddos Attack Model

Extremely sophisticated, user friendly, automated and powerful DDoS toolkits are available for attacking any victim, so expertise is not necessarily required that attract naive users to perform DDoS attacks. Although DoS attacking strategies differ in time, studies show that attackers mainly target the following resources to cause damage on victim.

IV. DDOS PREVENTION TECHNIQUES

Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes. Attack prevention schemes are not enough to stop DDoS attacks because there are always vulnerable to novel and mixed attack types for which signatures and patches arenot exist in the database.

Techniques for preventing against DDoS can be broadly divided into two categories:

(i) General techniques (ii) Filtering techniques

A. General Techniques

1) Disabling unused services

The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks, e.g. UDP echo, character generation service.

2) Install latest security patches

Today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system.

3) Disabling IP broadcast

Defense against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will be successful only if host computers and all the neighboring networks disable IP broadcast.

4) Firewalls

Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses.

B. Filtering Techniques

1) Ingress/Egress filtering

Ingress Filtering, proposed by Ferguson et al., is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge.

2) Router based packet filtering

Route based filtering, proposed by Park and Lee, extends ingress filtering and uses the route information to filter out spoofed IP packets. It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated.

3) History based IP filtering

Generally, the set of source IP addresses that is seen during normal operation tends to remain stable. In contrast, during DoS attacks, most of the source IP addresses have not been seen before. Peng et al. relies on the above idea and use IP address database (IAD) to keep frequent source IP addresses. During an attack, if the source address of a packet is not in IAD, the packet is dropped. Hash based/Bloom filter techniques are used for fast searching of IP in IAD. This scheme is robust, and does not need the cooperation of the whole Internet communities.

4) Capability based method

Capability based mechanisms provides destination a way to control the traffic directed towards itself. In this approach, source first sends request packets to its destination. Router marks (pre-capabilities) are added to request packet while passing through the router. The destination may or may not grant permission to the source to send. If permission is granted then destination returns the capabilities, if not then it does not supply the capabilities in the returned packet

5) SAVE

Source Address Validity Enforcement Li et al. have proposed a new protocol called the Source Address Validity Enforcement (SAVE) protocol, which enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address. The aim of the SAVE protocol is to provide routers with information about the range of source IP addresses that should be expected at each interface. Similarly to the existing routing protocols, SAVE constantly propagates messages containing valid source address information from the source location to all destinations. Hence, each router along the way is able to build an incoming table that associates each link of the router with a set of valid source address blocks.

V. CONCLUSION

DoS attack causes either disruption or degradation on victim's shared resources, as a result preventing legitimate users from their access right on those resources. DoS attack may target on a specific component of computer, entire computer system, certain networking infrastructure, or even entire Internet infrastructure. Attacks can be either by exploits the natural weakness of a system, which is known as logical attacks or overloading the victim with high volume of traffic, which is called flooding attacks. A distributed form of DoS attack called DDoS attack, which is generated by many compromised machines to coordinately hit a victim. DDoS attacks are adversarial and constantly evolving.

In this paper, we covered an overview of the DDoS problem, and a classification of available DDoS prevention mechanisms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat.

REFERENCES:

[1] A. Wood and J. Stankovic. "Denial of service in sensor networks". IEEE Computer Vol 35, Issue: 10,Oct 2002.
[2] Avancha, S, 'A Holistic Approach to Secure Sensor Networks' , PhD Dissertition, University of Maryland, 2005.
[3] A. Chowdhury "ACO Routing in Wireless Sensor Networks", Jan 2008.
[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "Wireless sensor networks: a survey". Computer Networks, 38:393-422, 2002.
[5] H. Chan and A. Perrig. "Security and privacy in sensor networks". IEEE Computer Magazine, pages 103-105, Oct. 2003.
[6] H. Mittal A. Agarwal, I S.K. Dhurandher, S Misra,, I. Woungang, "Ant Colony Optimization -Based Congestion Control in Ad-hoc Wireless Sensor Networks", 2009 IEEE.
[7] B. Abolhassani, M. Ziyadi, K. Yasami, "Adaptive Clustering for Energy Efficient Wireless Sensor Networks based on Ant Colony Optimization", 2009 7th Annual Communications Networks and Services Research Conference.
[8] C. Karlof, D. Wagner "Secure routing in wireless sensor networks: attacks and countermeasures" 2003 Elsevier.
[9] C. K., and K. V. Viswanatha "Enhanced Ant Colony Based Algorithm for Routing in Mobile Ad Hoc Network" World Academy of Science, Engineering and Technology 46 2008.
[10] C. Li, F. Chiang, H. Chao W. Chen, "Jumping ant routing algorithm for sensor networks" 2007 Published by Elsevier B.V.
[11] D. Qian, H. Chen, W. Wu, L. Cheng, "Swarm Intelligence Based Energy Balance Routing For Wireless Sensor Networks", 2nd International Symposium on Intelligent Information Technology Application.
[12] D. Qian, Y. Wen, Y. Chen, and "An Ant-based approach to Power-Efficient Algorithm for wireless sensor networks" Proceedings of the World Congress on Engineering 2007 Vol II WCE 2007, July 2, 2007, London, U.K.
[13] D. Raymond and Scott F. Midkiff "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses" 2008 IEEE.
[14] D. Culler, D. Estrin, and M. Srivastava. "Overview of sensor networks." IEEE Computer, pages 41-49, Aug. 2004.
[15] H. Zhu, K. Xu, Y. Liu,,, and Y. Jial, "A Routing Strategy Based on Ant Algorithm For WSN", Third International Conference on Natural Computation (ICNC 2007).
[16] J. Walters, Z. Liang, W. Shi, and V. Chaudhary " Wireless Sensor Network Security: A Survey".
[17] J. Bruten, O. Holland and R. Schoonderwoerd, "Ant-like agents for load balancing in telecommunications networks" Agents'97 Marina del Rey CA USA @1997 ACM.
[18] L. Osadciw, R.. Muraleedharan and," Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence" 2006 IEEE.
[19] L. Osadciw, R.. Muraleedharan," Decision Making in a

Building access system Using Swarm intelligence and Posets" 38th Annual Conference on Information Sciences and Systems, Princeton Unversity, 2004.
[20] L. Osadciw, R.. Muraleedharan, "Jamming Attack Detection and countermeasures In Wireless Sensor Network Using Ant System"SPIE Defence and Security, Orlando, 2006.
[21] Y. Wang, G. Attebury and B. Ramamurthy "A Survey of Security issues in Wireless Sensor Nework", 2nd Quarter 2006, Vol. 8, No. 2 IEEE