International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume4, Issue-8 E-ISSN: 2347-2693

Selective DDoS Attacks in Application server and Wireless Network – Survey

Harpinder Kaur[1]* and Bikrampal Kaur[2]

[1,2]Chandigarh Engineering College, India

Available online at: www.ijcseonline.org

Received: 28/Jun/2016 Revised: 16/Jul/2016 Accepted: 13/Aug/2016 Published: 31/Aug/2016

***Abstract* -** In the current computer world, preserving the information is very difficult. Some interrupts can occur on the local organization or network based system. Without security measures and controls in place our data might be subjected to an attack .Now a day's numerous attacks are evolve. The Dos attack is the most popular attack in network and internet.This kind of attack ingests a large amount of network bandwidth and occupies network equipment resources by flooding them with packet from the machinesdispersed all over the world. Dos attacks are usually doing by following methods: 1) Send unlimited quantity of packets to the server.2) Implementing malwares.3) Teardrop attack.4) Application level flood. A DDos attack is propelled by a mechanism called Botnet through a network of controlled computers. Distributed denial of service (DDos) attack has been regularly in the works attacks that badly intimidate the stability of the internet. In accordance to CERT coordination center, there are mainly three categories of DDoS attacks: flood attacks, protocol attack and logical attack.

Keywords: DDos Attack, wireless Sensor Network, CERT coordination Centre, protocol attack and logical attack.

I. INTRODUCTION

A wireless sensor network is a group of nodes organized into a cooperative network [1]. Each node consists of dispensation capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash recollections), have a RF transceiver (usually with a single omnidirectional antenna), have a control source (e.g., batteries and solar cells), and lodge various sensors and actuators. The nodes interconnect wirelessly and often self-organize after actualitypositioned in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can transfigure the way we live and work. Currently, wireless sensor networks are beginning to be organized at an accelerated pace. It is not perverse to expect that in 10-15 [2] years that the world will be protected with wireless sensor networks with admittance to them via the Internet. This can be considered as the Internet becoming a corporeal network. This new technology is stimulating with unlimited potential for numerous application areas including conservational, medical, military, transport, entertainment, crisis management, homeland defense, and smart spaces.

Computer Security is the field which tries to keep computers safe and secure. Security means allowing things you do want, while discontinuing things you don't want from happening. Parts of this include authentication and validation (manufacture sure you are who you privilege to be), encryption (making sure data gets where you want to go, without others being able to perceive it) and physical security.

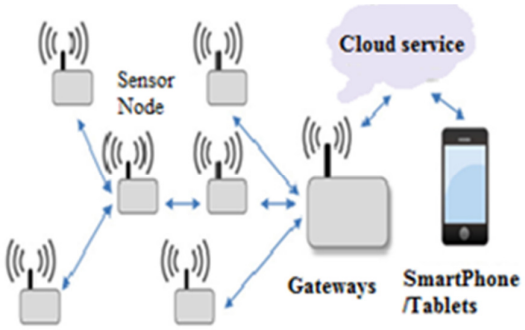

Fig 1: Wireless Sensor Network Architecture

In this section, we survey the working of the DDOS attack, wireless sensor network and analyses the work of the DDOS attacks. The strength of DDoS attacks has turned into stronger according to advancement of network infrastructure. DDoS attacks are thrown by manufacturing a tremendously large quantity of traffics and they quickly tire resources of target [5] systems, such as network bandwidth and computing power. We are describing the various types of attacks i.e. SYN attack and Flood Attacks.

II. DDoS ATTACK

Computer security mainly comprise of confidentiality, integrity [3] and availability. The major threats in security research are breach of confidentiality, failure of validity and unauthorized DDoS. DDoS attack has caused severe damage to servers and will cause even greater extortion to the development of new internet services. Traditionally,

DDoS attacks are carried out at the system layer, such as ICMP flooding, SYN flooding, and UDP flooding, which are called Network layer DDoS attacks. In Request layer DDoS attacks automata attack the victim web servers by HTTP GET requests (e.g., HTTP Overflowing) and pulling large image files from the object server in irresistible numbers. In another instance, attackers run a massive number of queries through the target's search engine or database query to bring the server down. On the other hand, a new special spectacle of network traffic called flash crowd has been noticed by researchers during the past several years. On the web, "flash meetingrefers to the situation when a very large number of users simultaneously access a popular web site, which harvests a surge in traffic to the web site and might cause the site to be virtually unreachable.

Distributed Denial of Service attacks have emerged as one of [6] the most severe threats between others. The strength of DDoS attacks has turned into stronger according to advancement of network infrastructure. DDoS attacks are thrown by manufacturing atremendously large quantity of traffics and they quickly tire resources of target [5] systems, such as network bandwidth and computing power.

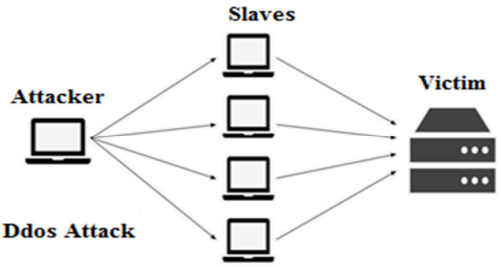

Fig 2: Distributed Denial of Services Attack Working

DDoS defenses mechanism can be classified into four classes which are prevention, uncovering, mitigation, and response. When DDoS attack occur, first step to spoil DDoS attacks is the detection and it should be done as fast as possible. However, it is difficult to differentiate between Distributed Denial of Service attack and ordinary traffics, since DDoS attack traffics frequently do not hold horrible contents in the packets. Moreover, attackers copy their source address to cover up their location and to create DDoS attacks more refined. DDoS detection schemes should assurance both short detection delay and high detection rates with low false positives [6].

Current DDoS attacks remain a high threat to IT security on the Internet. The attacks can be accepted out by attack tools [1], worms [2], and botnets [3] with attack variants of packet program such as TCP/SYN, UDP and HTTP request floods [4]. These bases of DDoS attack are powerful and can overcome any online host and server. Moreover, one of the major challenges for DDoS attack detection is flash-crowdattack. Flash-crowd attack [5][6][7] is the spectacle of a high volume of illegitimate packets from attack sources. The attack traffic is viewed the same as sincere users' traffics (called flash crowd). Attack sources pretend to be real users and pump a large volume of demand packets that flood the target victim.

III. RELATED WORKS

Theerasak Tangram et.al, 2011[1] in this paper, they proposed a behavior based detection that can distinguish DDoS attack traffic from traffic produced by real users. By using Pearson's correlation coefficient, those comparable detection methods can citation the repeatable sorts of the packet arrivals. The widespread simulations were tested for the accuracy of detection. They then achieved experiments with numerous datasets and our results affirm that the projected method can differentiate traffic of an attack source from sincere traffic with a quick response.

Jae-Hyun Jun et.al, 2011 [2] In this paper describes as, the DDoS attack, which is consuming all of the computing or communication resources necessary for the service, is known very difficult to protect. The threat posed by network attacks on large network, such as the internet, difficulties effective discovery method. Therefore, an intrusion detection system on large network is need to effectual real-time detection. In this broadside, implemented the entropy-based detection mechanism against DDoS attacks in order to agreement the transmission of normal traffic and prevents the flood of abnormal traffic. Young-Tae Han et.al,2012 [3] In this paper, presented effect of the TTL Expiry DDoS attack with the attack scenario in the tested consisted with commercialized network equipment's. V.K Soundar Rajam et.al,2013 [4] This paper proposed trace back mechanism with an actual optimization algorithm termed ACOPID in autonomous system with DPM inflicts two major advantages. They had predicted the complete attack path and efficiently tracing the DDoS attack source. Our contribution is on host IP trace back with DPM based on autonomous system to trace back the DDoS attack source with the marking information with reduced false positive rate. Ahmad Sanmorino et.al,2013 [5] In this study, they discussed how to handle DDoS attacks in the form of discovery method based on the design of flow entries and handling mechanism using layered firewall. Tests carried out using three scenarios that is simulations on normal network environment, unsecured network, and secure network. Then, analysed the simulations result that has been done. The method used successfully filtering incoming packet, by released packets from the assailant when DDoS attack happen, while still be able to receive packets from legitimate hosts .Bing Wang et.al,2014 [6] In this article, started by examined the security impact, in particular, the impact on DDoS attack defenseapparatuses, in an enterprise network where both technologies are adopted. They found that SDN technology can really help

enterprises to defend against DDoS attacks if the defines architecture is designed properly. To that end, they proposed a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to succeed attack detection and a supple control construction to allow fast and specific attack reaction.

IV. ANALYSIS

Then we analyse the impact of the combinedtechnologies on the network protection against DDoSattacks.

i) Software-Defined Networking

Unlike the well formatted data plane abstractionin the OSI model, the control plane of the Internet is composed of various complex protocols for variousnetwork functions. Managing these protocols ina distributed manner becomes incompetent and errorprone.SDN is a network architecture that decouples thecontrol plane and the data plane of network changesand moves the control plane to a central applicationcalled network controller. The network controller is in charge of the entire network through a seller independentinterface such as Open Flow [8], which definesthe low-level packet forwarding behaviours in thedata plane. Developers then can program the networkfrom a higher level without regarding the lower leveldetail of packet processing and forwarding in physicaldevices.

ii) Impact of SDN on DDoS attack defence

The most important two concepts of SDN are *control plane abstraction* and *network function virtualization*. They introduce following properties.

a) *Centralized network control:* The centralized network operating system connects toall the alterations in the network directly. Thus, NOS can provide a global network topologyalong with the real-time network status.
b) *Simplified packet forward:* The data plane inSDN [9] simply forwards packets based on theforwarding policies generated by control programs.
c) *Software based network function implementation:* Network functions originally implementedwithin a switch or a middle-box areinstigated as control programs in SDN.These control programs reside above the NOSand communicate with switches remotely [10].

V. CONCLUSION

DDoS attack is one of the most serious threats in Internet at present. Tracing back to the DDoS attacker and reconstructing the attack path can facilitate responding the DDoS attack, thus the DDoS attack can be mitigated effectively. But the existing DDoS trace back schemes have high false positive rate, or require large number of packets for reconstruction, or high overhead of network and router etc. Aiming at these disadvantages, a novel packet marking scheme based on space-code Bloom Filter for trace back DDoS attack is planned.

REFERENCES

[1] Thapngam, Theerasak, et al. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns." Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011.
[2] Jun, Jae-Hyun, Hyunju Oh, and Sung-Ho Kim. "DDoS flooding attack detection through a step-by-step investigation." Networked Embedded Systems for Enterprise Applications (NESEA), 2011 IEEE 2nd International Conference on. IEEE, 2011.
[3] Han, Young-Tae, et al. "Vulnerability of small networks for the TTL expiry DDoS attack." Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, 2012.
[4] SoundarRajam, V. K., et al. "Autonomous system based traceback mechanism for DDoS attack." Advanced Computing (ICoAC), 2013 Fifth International Conference on. IEEE, 2013.
[5] Sanmorino, Ahmad, and SetiadiYazid. "Ddos attack detection method and mitigation using pattern of the flow." Information and Communication Technology (ICoICT), 2013 International Conference of. IEEE, 2013.
[6] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal Kumar Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.
[7] Anantvalee, Tiranuch, and Jie Wu. "A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security. Springer US, 2007. 159-180.
[8] Chhabra, Meghna, and B. B. Gupta. "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)." Research Journal of Applied Sciences, Engineering and Technology 7.10 (2014): 2033-2039.
[9] Alqahtani, Sarra, and Rose Gamble. "DDoS Attacks in Service Clouds."System Sciences (HICSS), 2015 48th Hawaii International Conference on. IEEE, 2015.
[10] Jae-Hyun Jun, Hyunju Oh, andSung Kim. "Real time detection and classification of DDoS attacks using Enhanced SVM with string kernels." Recent Trends in Information Technology (ICRTIT), 2015 International journals on. IEEE, 2015.

