A COMPREHENSIVE STUDY OF DISTRIBUTED DENIAL OF SERVICE ATTACK WITH THE DETECTION TECHNIQUES

HUSAM HAMID IBRAHIM

A project report submitted in partial

fulfilment of the requirement for the award of the

Degree of Master of Electrical Engineering

Faculty of Electrical and Electronic Engineering

University Tun Hussein Onn Malaysia

JULY 2018

DEDICATION

Specially dedicated to my beloved father, mother and also brothers for their love , care and support.

ACKNOWLEDGEMENT

Foremost, all praises to Almighty ALLAH, whose give me strength and perseverance to make me able to complete this master's degree, without ALLAH I cannot do anything in this life. Therefore, he is the only one I have to be thankful for him from heart. I would like to express the deepest gratitude to my honorable Supervisor: Dr Nan bin Mad Sahar for his kind support, valuable ideas, assistance, guidance and encouragement throughout this thesis. Also, my gratitude to the cooperation given by Faculty of Electrical and Electronics Engineering (FKEE) in University Tun Hussein Onn Malaysia (UTHM). My greatest appreciation goes to all my friends and colleagues who always helped and motivated me during my master's degree and through this project.

Last but not least, with all of my love, I would like to express my honest thanks to all my family members for their love, encouragement, prayers and motivations a long all years of my life. I am deeply and forever indebted to my parents, both financially and emotionally throughout my entire study. Without them I could not have made my study. I would like to truthfully acknowledge the sincere help and the moral support of all those inspired me to complete my study

ABSTRACT

Today, net related net services are indivisible in our life. Therefore, for the success of certain types of organizations, some sustained simplification of services is essential. However, these service area units were usually hindered by the constant threat from numerous kinds of attacks. One such attack is called a distributed denial of service attack and leads to a problem starting with a temporary delay of the server in order to terminate the service's non-availability. A honeypot may be a kind of lure, but in order to prevent potential attackers from diverting, observing, preventing, and ensuring the ongoing convenience of the service. This study gives insight into the problem with distributed denial-of-service attacks. This researcher provides insight into problems caused by distributed denial of service attacks, simulates several types of attacks, analyzes the results, performs each single simulation, and shows how to prevent distributed denial of service attacks. This project explains recently introduced distributed denial of service (DDoS) and its techniques. DDoS attack method using NS - 2 simulator software. This research provides the results of four experiments related to DDoS attacks in a simulation environment with NS 2. The result of this project shows that the three main factors of DDoS attack are attack time, attack strength and pocket size. Attack time is mainly related to attack strength. Finally, it is shown that the buffer size plays a role in processing attack traffic.

ABSTRAK

Hari ini, perkhidmatan web berkaitan rangkaian tidak dapat dipisahkan dalam kehidupan kita. Oleh itu, untuk kejayaan sesetengah jenis organisasi, beberapa penyederhanaan perkhidmatan yang berterusan adalah kritikal. Bagaimanapun, unit-unit kawasan perkhidmatan ini sering terhalang oleh ancaman berterusan daripada pelbagai serangan. Satu serangan sedemikian dikenali sebagai penyangkalan penyebaran serangan diedarkan dan menyebabkan masalah dengan kelewatan sementara pelayan untuk menamatkan ketiadaan perkhidmatan. Honeypots boleh menjadi godaan, tetapi untuk menghalang penyerang berpotensi untuk beralih, memerhatikan, menghalang dan memastikan kemudahan perkhidmatan yang berterusan. Kajian ini mengkaji secara mendalam isu penyangkalan serangan serangan yang diedarkan. Para penyelidik menyelidiki masalah-masalah yang disebabkan oleh serangan penolakan yang disebarkan, menyusun beberapa jenis serangan, menganalisis hasilnya, melakukan setiap simulasi individu, dan menunjukkan bagaimana untuk mencegah penyebaran penyebaran serangan yang diedarkan. Projek ini menerangkan teknologi Penafian Pemberian Terdahulu (DDoS) yang baru dan teknologinya. Kaedah serangan DDoS menggunakan perisian simulator NS-2. Kajian ini menyediakan empat keputusan percubaan yang berkaitan dengan serangan DDoS dalam persekitaran simulasi NS 2. Hasil projek menunjukkan bahawa tiga faktor utama serangan DDoS adalah serangan, kekuatan serangan dan ukuran saku. Waktu serangan terutamanya berkaitan dengan kekuatan serangan. Akhirnya, saiz penampan paparan memainkan peranan dalam menangani lalu lintas serangan.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Research Background

The improvement in speed, reliability and accuracy of the current Internet framework's rapid technology has had a major impact on our daily lives. With the increase of Web-enabled applications, the number of important and secret information in public and private networks is increasing. Allow network design to effectively share resources among users of these networks, and Web-enabled applications play an important role in our daily personal and professional lives. [1, 21].

Over the past few years, the Internet has provided a common communications and computing platform by connecting billions of computers. In addition, the connection between the Internet and wireless and mobile technologies is leading to an impressive revolution in modern devices and applications. [38]. Fig. 1.1: shows the internet users and how they increase yearly from 2005 till 2017.

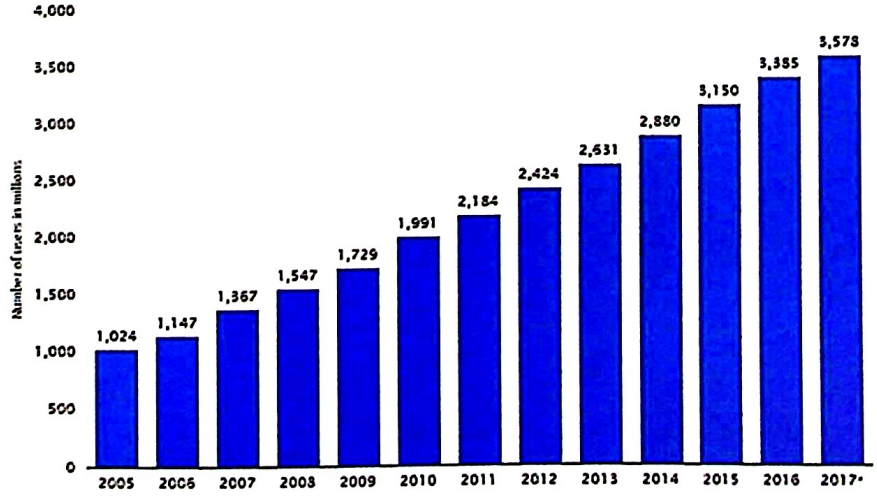

Figure 1.1: No. of Internet users till 2017 [35].

People begin to exchange and share their important information with other network users through the Internet. However, due to this high degree of dependence on the Internet, some people use the weaknesses of the Internet to locate a part of it [10]. A common example of these weaknesses in the Internet is the speed difference between core routers and edge routers. Inadequate router configuration is another major weakness of the Internet. This weakness often makes network systems the targets of attacks that attempt to gain unauthorized access to important information or damage private or professional resources. Although many passwords and firewall systems have been developed in the past few years, these systems have no drawbacks or limitations [15]. Network systems can be protected using defense mechanisms that can identify intrusions when an intrusion occurs or is about to occur. This may be another form of defense. Despite great efforts made by defenders, zero-day and other complex attacks occur almost daily. Denial of service (DoS) attacks are classified as the most common and disruptive of all threats that network maintainers need to be aware of.[32]. As shown in Figure 1.2, in the third quarter of 2017, the number of SYN DDoS attacks continued to increase, from 53.26% to 60.43%. At the same time, the percentage of TCP DDoS attacks plunged from 18.18% to 11.19%, which did not affect the rating of this attack in the second position. Both UDP and ICMP attacks have become very rare: their share has dropped from 11.91% to 10.15% and 9.38%, respectively, to 7.08%. At the same time, the popularity of HTTP attacks rose from 7.27% to 11.6%, ranking third [3].

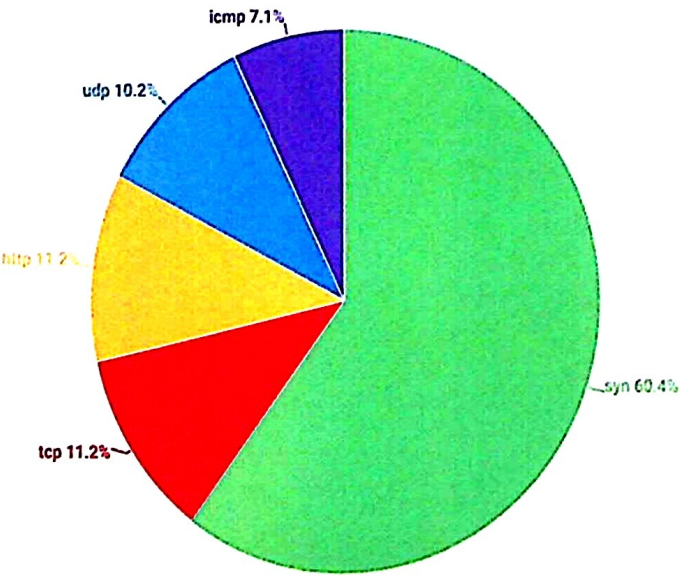

Figure 1.2: Distribution of DDoS attacks by type, Q3 2017[3]

DDoS is a coordinated attack that uses a large number of infected hosts to start. In the initial stages, attackers can identify vulnerabilities in one or more networks to install malware programs on multiple machines to control them from a remote location. Next, the next step, usually the target machine outside the infected host's original network will be exploited by the attacker. These hosts will send attack packets to them by destroying these hosts without knowing the infected hosts. [2,33]. Depending on the strength of the attack packet and the number of hosts used for the attack, there will be corresponding damage in the victim network. If the attacker can use a large number of infected hosts, the network or Web server may be interrupted for a short period of time. Some common examples of DDoS attacks are fraggle, smurf, and SYN flooding.

1.2 Problem Statement

In the past decade years, this unresolved issue has been actively resolved in the IT community, and there was no definitive solution. The magnitude of the impact of DDoS encouraged me to do more research on this topic and to make my own contribution. As a result of such attacks, businesses closed down, the economy declined, and the government changed. Figure 1.3 shows that the number of attacks per day during the third quarter of 2017 ranges from 296 (July 24) to 1508 (September 26).

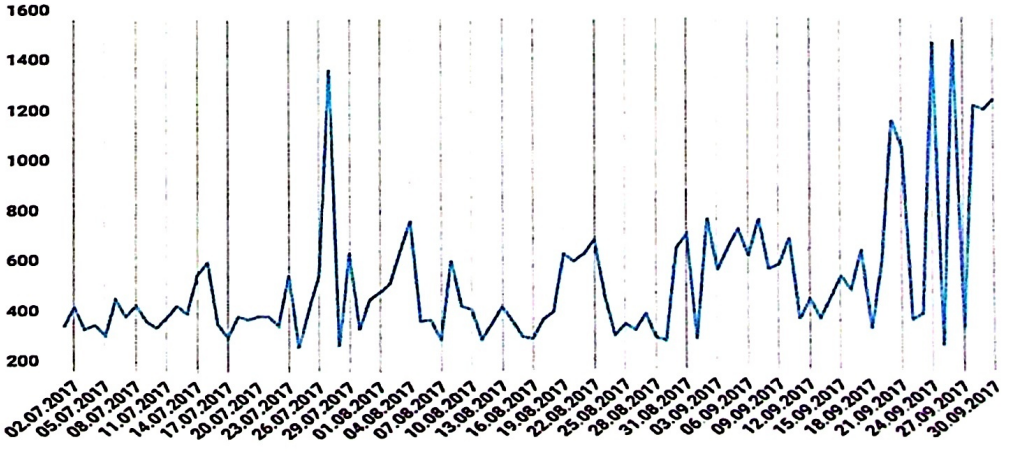

Figure 1.3: the number of DDoS attacks in Q3 2017 [3]

The highest number was registered on July 27 (1399) and September 24 (1497). There was a relative decline in July 28 (300), May 31 (240) and September 25 (297) [3].

Future warfare could cause the country to be defeated, so it will be a rocket with IP data packets. This is the result of expert prediction. In this survey, we classify and investigate the impact of DDoS attacks and their systems or services. Next, based on the DDoS attack detection function, the source detection and validity of the DDoS attack is checked. At the same time, this study uses technology to detect program anomalies and simulate DDoS attacks. This method improves the function of anomaly detection technology by combining detection of rule base and threshold value. Next, the selected DDoS attack analyzes the impact of the proposed technology as an invasion. Detect system performance.

1.3 Objectives

Based on the problem statements, there are three objectives that are going to be achieved. The objectives of this project are;

1. To investigate DDoS attack characteristics and it's detect technique effectiveness.
2. To improve and propose alternative technique for detecting DDoS attack.
3. To simulate the DDoS attack type and examine it using anomaly detection technique.
4. To evaluate the performance of proposed techniques in detecting DDoS attack.

1.4 Project Scopes

The Scopes of this project are:

1. Investigate DDoS attacks and their types; study the impact of DDoS attacks and their impact on the system.

2. Check DDoS detection technology, study its ability to detect DDoS attacks and DDoS detection
3. Simulate the three most common and powerful DDoS attack types and examine them using anomaly detection techniques.
4. Assess and validate our results together with other previous studies.

1.5 Project Structure

This is a project organization and it consists of five chapters.

• Chapter 1 discusses the research background. In addition, the problem statement, project objectives, research scope, and project structure outline were introduced.

• Chapter 2 presents a literature review that discusses the types of DDoS attacks, the impact of DDoS attacks on services or systems, DDoS detection techniques and their working principles, and reviews most of the DDoS detection capabilities.

• Chapter 3 of this chapter describes the methodology scenario and the systems and software required to simulate this project, and will review the flow chart for this project.

• Chapter 4 of this chapter will review the simulation steps and set up the test platform we studied.

• Chapter 5 of this chapter will review our simulation results and our simulation results with other relevant studies and summarize the simulations and recommendations for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

One of the serious and challenging issues is distributed denial of service (DDoS) attacks. Since a large number of insecure machines provide fertile ground for attacking zombies, attackers do not need to make any effort and can easily download and deploy automated scripts for exploitation and attack. On the other hand, due to the large number of attack machines, it is very difficult to prevent attackers or attackers from responding and tracking; using source address spoofing and the similarity between legitimate and attack traffic. Although research and business communities have designed many defense systems to deal with DDoS attacks, this problem has largely remained unresolved [30]. The comprehensive knowledge of DDoS attacks and their scenarios, objectives and detection methods are intended to be simplified in this chapter. Cosize related works were proposed and eventually developed in DDoS research.

2.2 DOS Attack Scenario

Victims receive a malicious stream of packets that can exhaust some critical resources. This happens in denial-of-service (DoS) attacks; this leads to denial of

service to legitimate customers of the victims (Tuomo Penttinen, 2005).

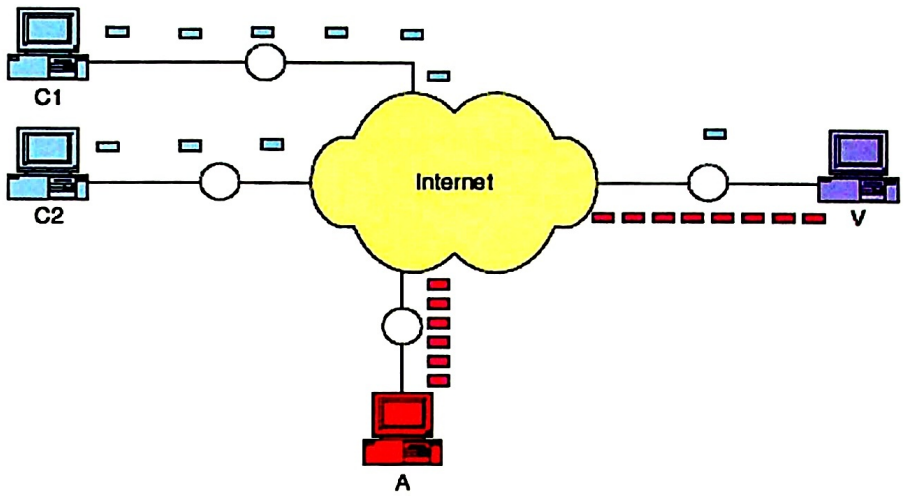

Figure 2.1: DoS attack scenario [25]

In a typical denial of service attack scenario, attacker A sends a malicious packet flow to victim V and refuses to provide services to legitimate clients C1 and C2, as shown in Figure 2.1. Machine A is actually an agent machine, an unwitting participant destroyed by the attacker, because the attacker rarely uses his own machine to perform the attack. By misusing a vulnerability in the software that runs on the victim, the attack may exhaust key resources (vulnerability attacks)[34] or simply send more traffic than the victim (flood attack)[38] .

Contain data packets of a particular type or content to exploit exploits that are normally included in exploits. [29].The number of exploits is small because the vulnerabilities can often be exploited by a small number of data packets. Both of these features (special types of packets and low capacity) can simplify the handling of vulnerability attacks - the target can patch its vulnerabilities or discover special types of packets and process them separately.

A large number of floods overwhelmed the victim's resources. Because malicious packets can be of any type or content, and high capacity hinders detailed traffic analysis, this strategy is more difficult to counteract. A common approach to defend against flood attacks is to provide victims with a wealth of resources because DoS attacks involve only one attack aircraft. To perform a successful attack, an attacker needs to find and subvert better-configured machines. With the amount of resources allocated to victims, the attackers find it more difficult to find enough agent machines [24].

2.3 DDOS Attack Scenario

A simple denial of service attack is performed from a number of subverted machines (agents), so-called Distributed Denial of Service (DDoS) attacks [27]. All machines are used at the same time and begin to generate as many data packets as they can send packets to victims, which is exactly what happens in Scarecrow and the most common scenarios. Due to the moderate functionality of the proxy machine, a large number of participating agents allow the attacker to overload the highly configured victims' resources.

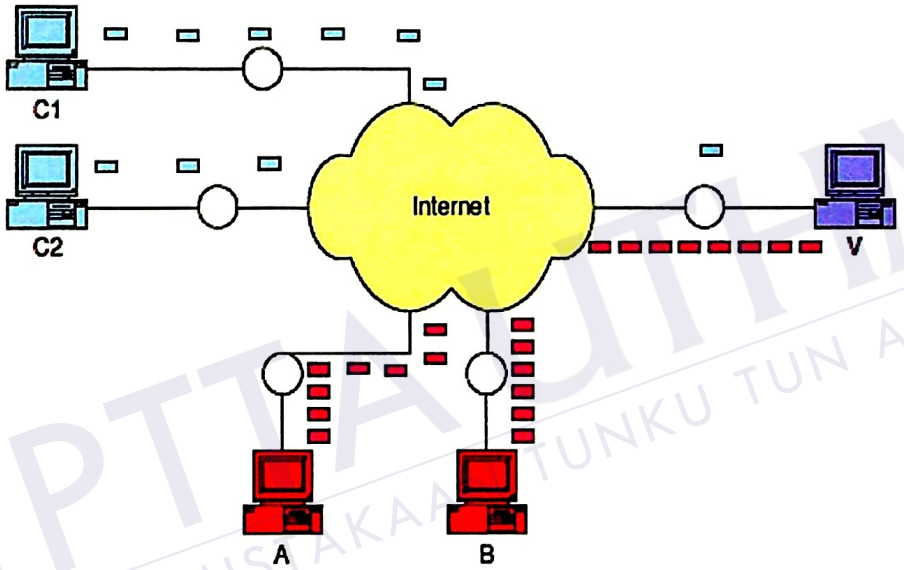

Figure 2.2: DDoS attack scenario [25]

In a simple distributed denial of service attack scenario, attackers A and B send the malicious packet stream to victim V, denying its service to legitimate clients C1 and C2 shown in Figure 2.2 [8].

The vast majority of packets are sent from multiple attack sites to the victim site, which is what the DDoS attack contains. These data packets reach such a high volume that some of the key resources on the target (bandwidth, buffer, CPU time for calculation response) are quickly exhausted [14]. Victims either crash or spend a lot of time managing the traffic that cannot participate in their actual work [23]. Distributed denial of service attacks are widely considered to be the main threat to the Internet. Therefore, as long as the attack continues [16], legitimate customers are deprived of the victim's services. They have adversely affected the main Internet commerce sites, single machines and even services of core Internet infrastructure

services. Because very large-scale DDoS attacks occur irregularly (usually as a byproduct of viruses), Internet-wide communications are spreading for hours or worms). These incidents still caused major disruptions to users, costing the victims website millions of dollars, and the service resumed immediately after the attack subsided. In addition, the Internet is used daily for important communications such as stock trading, financial management, and even some infrastructure services [15].

Due to the DDoS attacks, many transactions must be processed in time and may be severely delayed. The impact of this attack is greater than the threat. Any immature user may locate and download DDoS tools and allow them to perform successful large-scale attacks. The attacker has almost no risk of being discovered.

- There are two types of DDoS attacks that prevent the design of more effective defenses: DDoS traffic is very similar to legitimate traffic. Attacks usually occur in large quantities and consist of legitimate data packets. It cannot be distinguished on a data packet by packet basis because they completely integrate a small amount of legitimate client traffic. All victim-targeted packets can be grouped into higher-level semantic structures (for example, "all data streams exchanged between two IP addresses", "all HTTP data streams", and "supplied source IP address" by the defense system. "Etc.," then detects high-capacity or anomalous communications, performing many statistics on the dynamics of these structures. Afterwards, packets belonging to the suspicious structure will be supervised, and packets belonging to structures with legal behavior will be forwarded [26].
- Distribution of DDoS traffic. Attack flows only converge near the victims and are generated from many attacking machines throughout the Internet. In order to reduce the denial of service to the victims, the defense system must control most of the attacks. This indicates that the distributed system that the defense node covers an important part of the Internet or the system must be a single point system located near the victim. [19].
- The goals of this paper are: Studying DDoS attacks and current detection techniques, simulating the most powerful attacks of DDoS attacks on anomaly detection techniques, and studying the effects of DDoS attacks and other research validation results and their Impact on the system, investigate DDoS detection technology, study its availability for detecting DDoS attacks and DDoS detection capabilities.

Several characteristics of DDoS attacks present challenges to the design of successful defenses [20]:

• IP source spoofing use. During an attack, source address spoofing is often used by attackers - they forge information in the IP source address field in the attack packet header. Tracking the proxy machine is very difficult and it considers the attacker to gain an advantage from IP spoofing. Therefore, it brought a few terrible consequences. The information stored on it (i.e., the access log) does not help you find the attacker yourself because the tracking risk of the agent machine is low. As a result, the DDoS incident was very encouraging. Moreover, attackers can reuse the proxy machine's address by hiding them for future attacks. Finally, attack packets appear to come from many different sources because they carry a wide variety of addresses; fair sharing technology is a direct solution to resource overload problems and can be defeated. The ability to perform reflector attacks [Pax01] is another advantage that IP spoofing offers to attackers. The attacker (in the name of the victim) asks the public service to generate a large number of replies to specific small requests (magnification effects). The source addresses of the victims are forged and sent to the public server: so that the attacker can generate as many service requests as possible based on his resource license [23]. These servers can direct the number of replies to the victim (thus reflecting and increasing attack power) and overloading their resources. [CERe] describes the common case of reflector attacks. Using the victim's spoofed source IP address, the attacker sends a large number of UDP-based DNS requests to the name server. The name server response may be much larger than the DNS request, so there is the possibility of bandwidth amplification. This is why any name server response is sent back to the fraudulent IP address as a destination. Even if Retrospective Problem 1 is resolved, reflector attacks will not help. Public servers are uninformed participants and their legitimate services are abused in attacks. They do not have any information about the attacker [25]. In addition, because this can cause harm to many other customers, their services cannot be disabled (i.e., stop the attack). They can prevent reflector attacks by limiting the amount of replies they are willing to generate for a particular IP address based on the resources and requests of these servers. It may consume a lot of memory resources because this method requires the server to cache the request address.

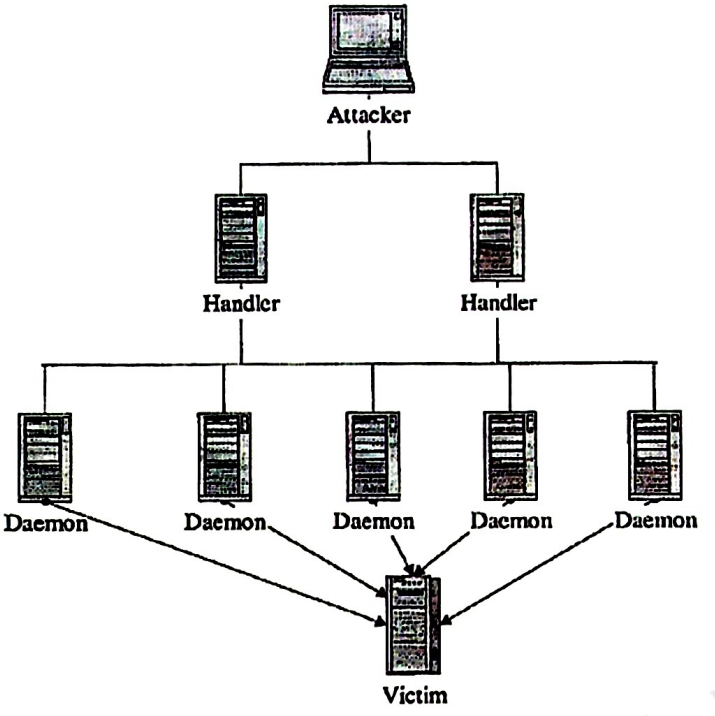

Figure 2.3: DDoS attack architecture [13]

• A large number of proxy machines. Even if it is possible to successfully perform backtracking in the case of IP spoofing, it is difficult to say what actions can be taken for hundreds or thousands of proxy machines. Such a large number prohibits any rough automatic reply, designed to prevent attack traffic near the source.

• Attacks on legitimate traffic similarities. To perform a successful denial of service attack, you can use any type of traffic to accomplish this. Compared with other traffic types, some traffic types have higher attack success rates than others, and attacks on different content and types of data packets target different resources. On the other hand, if the goal is merely to stifle the actions of the victim, then it can be achieved by sending a sufficiently large amount of traffic and blocking the victim's network. Blurring malicious traffic in legitimate traffic, attackers tend to generate legitimate data packets to perform attacks. Because malicious packets cannot stand out from legitimate packets, it is not possible to filter legitimate traffic from attack traffic based solely on inspection of individual packets. In order to extract transactional semantics from the packet flow, the defense system must retain a certain amount of statistical data to distinguish certain legitimate traffic (e.g. belonging to lengthy, well performing transactions) from attack traffic.

2.4 DDOS Attack Targets

A single Web server connects to the entire university, the entire city and even the entire country's Internet connection, all of which may be the target of DDoS attacks. In general, DDoS attackers will choose any of the four generic targets in the victim's network, [6] as described below.

2.4.1 On Infrastructure

By targeting its infrastructure, many DDoS attackers are targeting network systems. Globally or globally, the DNS can range from the smallest wireless access point to a large public key infrastructure. The impact of a DDoS attack depends on the coverage of the infrastructure.

2.4.2 On Link

This link is a common target for DDoS attacks. By sending a large number of coordinated channels to completely expel the link, an attacker can successfully initiate a DDoS attack. As a result, many legitimate data packets may be dropped.

2.4.3 On Router

DDoS attacks usually target IP routers. By filling the routing table with a large number of routes, the CPU power is insufficient or the router memory is exhausted. This is a common method of launching a DDoS attack on a router. In order to launch such attacks, many attackers also exploited the weaknesses of routing protocols.

2.4.4 On OS

To protect resources from application DDoS attacks, the operating system (OS) can play an important role. Many attackers therefore target the operating system itself. It

may cause serious damage to all applications running on the operating system if such an attack can be successfully initiated [4].

2.4.5 On Defense Mechanism

The defense system may be the target of the DDoS attack itself. DDoS attackers usually target firewalls and DDoS detection mechanisms. The goal of the firewall is to exhaust resources by sending a large amount of traffic. This traffic may be stateful or stateless. This may cause the firewall to maintain an excessive state and may eventually lead to insufficient memory. However, in the case of a defense mechanism, the impact or consequences of a DDoS attack will be different. Producing a large number of false alarms may be the result of a failure to implement the mechanism correctly.

2.5 Source End Detection

Because the anti-DDoS mechanism may make it impossible for them to get rid of the source defense, the overall requirements and features of the DDoS attack detection and defense system close to the source end cannot compete with the victim end defense itself [5]. The advantages of DDoS are:

• Congestion avoidance: Internet resources can be preserved by restricting the flow of attacks in the vicinity of the source. These attack flows will be exhausted by the attack traffic.

• Small collateral damage: The smallest legitimate user may be negatively impacted by rate restrictions or traffic filtering near the source.

• Simpler backtracking: By approaching the source of information, it is possible to simplify attackers backtracking and simplify post-attack investigations.

• Complex detection strategies: Put more router resources into DDoS defenses, making routers closer to relay routers that are likely sources of relay traffic closer to [28].

The disadvantage of DDoS is [12]:

• Defense effectiveness: Attack packets are very similar to benign packets. The number of input/output connections, traffic or input/output packet rates are the

traditional methods based on detection. However, because only a small portion of the attack traffic can be observed at the source, these methods may not be available.

• The source response must be selective.

The issue of deployment incentives has also been improved. Although deploying tools that can detect outgoing DDoS attacks will cost the owner of the source network, the protection is still provided to the victim. Therefore, one of the ideal attributes of source defense is low deployment cost and low false alarm rate [17]

2.6 Intrusion Detection Technique

2.6.1 Anomaly Based Detection

By observing deviations from the normal behavior of network traffic, attacks can be detected, as assumed by the anomalous DoS detection technique. The first one is extracted from the normal traffic observed in the past or is known as a synthetic traffic without attacks, which is an overview of normal behavior. The observed network traffic will be checked against the established profile of the traffic behavior, which will happen in later detection modes. How to generating an alert when traffic deviates from a profile that exceeds the threshold. In monitored network traffic, the occurrence of a worm is detected by analyzing the byte distribution of the payload of the packet and looking for deviations from the established profile. Since no a priori knowledge of a particular attack is required, unpredictable attacks can be detected, which is an advantage of anomaly detection. However, because the entire range of network traffic behavior during the learning phase may not be covered, the observed anomalies do not necessarily indicate an attack, and the false alarm rate may be high.

2.6.2 Signature Based Detection

DoS detection decisions are formed on the basis of accumulated knowledge of known attacks or system vulnerabilities, that is, they occur during signature detection. Security experts describe patterns of known attacks that generate signature libraries. Identify DoS attacks. These signatures are then matched against the observed traffic and an alert is raised whenever a match is found. Security experts can use signature

REFERNCES

[1] Abliz, M. (2011). Internet denial of service attacks and defense mechanisms. University of Pittsburgh, *Department of Computer Science, Technical Report,* 1-50.

[2] Akamai, state of the *internet security* Q2 2017 Report. [Volume 4/Number 2].

[3] Khalimonenko, A., Kupreev, O., & Ilganaev, K. (2017). DDoS attacks in Q1 2017. *securelist. com.*

[4] Álvarez, G., & Petrović, S. (2003). A new taxonomy of web attacks suitable for efficient encoding. *Computers & Security*, 22(5), 435-449.

[5] Beitollahi, H., & Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications,* 35(11), 1312-1332.

[6] Bhattacharyya, D. K., & Kalita, J. K. (2016). Ddos attacks: Evolution, detection, prevention, reaction, and tolerance. *Chapman and Hall/CRC.*

[7] Bhaya, W., & EbadyManaa, M. (2017, March). DDoS attack detection approach using an efficient cluster analysis in large data scale. In *New Trends in Information & Communications Technology Applications (NTICT),* 2017 Annual Conference on(pp. 168-173). IEEE.

[8] BUKAČ, V. (2012). *Detection of flooding denial of service attacks on the source client hosts* (Doctoral dissertation, Masarykova univerzita, Fakulta informatiky).

[9] Conti, M., Gangwal, A., & Gaur, M. S. (2017, October). A comprehensive and effective mechanism for DDoS detection in SDN. In *Wireless and Mobile Computing, Networking and Communications* (WiMob), (pp. 1-8). IEEE.

[10] Deka, R. K., Bhattacharyya, D. K., & Kalita, J. K. (2017). DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment. *arXiv preprint arXiv:1710.08628..*

[11] Diovu, R. C., & Agee, J. T. (2017, June). A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In *PowerAfrica, 2017 IEEE PES* (pp. 28-33). IEEE.

[12] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 44*(5), 643-666.

[13] Fan, Y., Hassanein, H., & Martin, P. (2003, May). Proactively defeating distributed denial of service attacks. In *Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on (*Vol. 2, pp. 1047-1050). IEEE.

[14] Guiton, E. (2003). of the Thesis*: A Rate-Limiting System to Mitigate Denial of Service Attacks.*

[15] Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing and Applications,* 28(12), 3655-3682.

[16] Gupta, B. B., Joshi, R. C., & Misra, M. (2012). Distributed denial of service prevention techniques. *arXiv preprint arXiv:1208.3557.*

[17] Jia, Q. (2014). *Mitigating Denial-of-Service Attacks in Contested Network Environments* (Doctoral dissertation)..

[18] Jiang, H., Chen, S., Hu, H., & Zhang, M. (2015, April). Superpoint-based detection against distributed denial of service (DDoS) flooding attacks. In *Local and Metropolitan Area Networks (LANMAN), 2015 IEEE International Workshop on (pp. 1-6).* IEEE.

[19] Karthik, S., Bhavadharini, R. M., & Arunachalam, V. P. (2008, December). Analyzing interaction between denial of service (dos) attacks and threats. In *Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on* (pp. 1-9). IEEE.

[20] Karthikeyan, B. (2014). *Detecting and Isolating Distributed Denial of Service Attack in Smart Grid Systems. Diss.* National Institute of Technology Rourkela.

[21] Kaur, P., Kumar, M., & Bhandari, A. (2017). A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering*, 5(1), 301-320.

[22] Khadke, A., Madankar, M., & Motghare, M. (2016, January). Review on mitigation of distributed Denial of Service (DDoS) attacks in cloud computing. In *Intelligent Systems and Control (ISCO), 2016 10th International Conference on* (pp. 1-5). IEEE.

[23] Kumar, K. (2007*). Protection from distributed denial of service (ddos) attacks in isp domain.*

[24] Liu, Z., Huang, X., Hu, Z., Khan, M. K., Seo, H., & Zhou, L. (2017). On emerging family of elliptic curves to secure internet of things: ECC comes of age. *IEEE Transactions on Dependable and Secure Computing*, 14(3), 237-248.

[25] Mirkovic, J. (2003). *D-WARD: source-end defense against distributed denial-of-service attacks* (Doctoral dissertation, University of California, Los Angeles).

[26] Mirkovic, J., & Reiher, P. (2005). D-WARD: a source-end defense against flooding denial-of-service attacks. *IEEE transactions on Dependable and Secure Computing, 2(3), 216-232.*

[27] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34(2), 39-53.*

[28] Mirkovic, J., Robinson, M., Reiher, P., & Oikonomou, G. (2005). Distributed defense against DDOS attacks. *University of Delaware CIS Department technical report CIS-TR-2005-02, 1-12.*

[29] Papp, D., Ma, Z., & Buttyan, L. (2015, July). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In *Privacy, Security and Trust (PST), 2015 13th Annual Conference on (pp. 145-152). IEEE.*

[30] Penttinen, T. (2005). *Distributed denial-of-service attacks in the Internet.*

[31] Poisel, R., Rybnicek, M., & Tjoa, S. (2013, March). Game-based simulation of Distributed Denial of Service (DDoS) attack and defense mechanisms of Critical Infrastructures. In *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference* on (pp. 114-120). IEEE.

[32] Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. *Global Journal of Computer Science and Technology.*

[33] Singh, K., Singh, P., & Kumar, K. (2017). Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. *Computers & security,* 65, 344-372.

[34] Tzang, Y. J., Chang, H. Y., & Tzang, C. H. (2015). Enhancing the performance and security against media-access-control table overflow vulnerability attacks. *Security and Communication Networks*, 8(9), 1780-1793.

[35] Vadlamani, N. S. (2013). *A survey on detection and defense of application layer DDoS attacks*.

[36] Wahab, O. A., Bentahar, J., Otrok, H., & Mourad, A. (2017). Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. *IEEE Transactions on Services Computing*, (1), 1-1.

[37] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials,* 18(1), 602-622.

[38] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials,* 15(4), 2046-2069.

[39] Zhou, W. (2012, June). Keynote: Detection of and Defense Against Distributed Denial-of-Service (DDoS) Attacks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. lxxxii-lxxxii). IEEE.*

[40] Thomas, M. S., Ali, I., & Gupta, N. (2012, October). A secure way of exchanging the secret keys in advanced metering infrastructure. In *Power System Technology (POWERCON), 2012 IEEE International Conference* on (pp. 1-7). IEEE.

[41] Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. P. (2012). A survey of communication/networking in smart grids. *Future Generation Computer Systems*, 28(2), 391-404.

[42] Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Im, E. G., Yao, Z. Q., & Wang, H. F. (2012*). Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems.*

[43] Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1(1), 99-107.

[44] Shila, D. M., Cheng, Y., & Anjali, T. (2009, November). Channel-aware detection of gray hole attacks in wireless mesh networks. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* (pp. 1-6). IEEE..

[45] Lee, M. J., Zheng, J., Ko, Y. B., & Shrestha, D. M. (2006). Emerging standards for wireless mesh technology. *IEEE Wireless Communications*, 13(2), 56-63.

[46] Karlof, C., & Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 *IEEE International Workshop on* (pp. 113-127). IEEE.