A Review of the Common DDoS Attack: Types and Protection Approaches Based on Artificial Intelligence

N. A. Majeed alhammadi [*], K. Hameed Zaboon, A. Abdulhadi Abdullah

Department of computer sciences, shatt al-arab University college, Al Basrah, 61001, Iraq

Emails: Nafeaalhamadi@yahoo.com; Khalid.Hameed842@gmail.com; ammarabdulhadiabdullah@sa-uc.edu.iq

Abstract

Recently, technology become an important part of our life, and it is employed to work together with Medicine, Space Science, Agriculture, industry, and more else. Stored the information in the servers and cloud become required. It is a global force that has transformed people's lives with the availability of various web applications that serve billions of websites every day. However, there are many types of attacks that could be targeting the internet, and there is a need to recognize, classify and protect thesis types of attack. Due to its important global role, it has become important to ensure that web applications are secure, accurate, and of high quality. One of the basic problems found on the Web is DDoS attacks. In this work, the review classifies and delineates attack types, test characteristics, evaluation techniques; evaluation methods, and test data sets used in the proposed Strategic Strategy methodology. Finally, this work affords guidance and possible targets in the fight against creating better events to overcome the most dangerous Cyber-attack types which are DDoS attacks.

Keywords: SYN Flood; ICMP; Flood; UDP flood Protection Methods.

1.Introduction

Information security is the most important part which must take into consecration during designing the systems, especially those which have contact with the internet. It comes in the field of identity risk management. It normally includes avoiding or at least minimizing the risk of unauthorized/inappropriate data access, as well as improper data usage, leakage, destruction, deletion, corruption, alteration, review, tracking, or devaluation [1]. It also requires actions directed at reducing the detrimental effects of such accidents. Encrypted records may be electronic or actual, visible (such as paperwork) or intangible such as a photograph, or knowledge.

The primary aim of information management is to balance the preservation of data's confidentiality, honesty, and availability (also known as the CIA triad) while concentrating on effective policy execution without undermining company efficiency [2]. Furthermore, several types of attacks could affect information security such as misuse, DDoS, SQL Injection, and others else. However, the most common and dangerous one of them is Misuse attack [3], [4].

The computer scene and correspondence with the advent of the Internet have changed. In this way, the Internet is becoming more and more essential in today's society. It has changed our communication and correspondence, the way we work, and even our daily lives [5]. In its early stages, the internet was used to communicate and share data

DOI: https://doi.org/10.54216/FPA.070101

between trusted individuals and organizations. Most of the internet users at that time were people in research departments of governmental organizations such as the Department of Defense (DoD) and large educational institutions such as MIT, UCLA, etc. Since computer costs were extremely high during that period, the major initial motivation for the internet was resource sharing.

Since there were only a small number of people using the internet, early network communication protocols were developed with little security in mind [6]. As more and more people started using the internet, it became less secure. In 1988, the Moris worm was released on the Internet. The first internet worm gained attention in the internet community. Though the author of this stated that the intent was not malicious, the unintended consequence was quite devastating. This event reinforced the belief that there are malicious people that will do harm to others in the internet community [2].

Consequently, the need for network security between a secure private network and the outside world became essential. Though the Morris Worm is the first recorded Distributed Denial of Service event, the DDoS attack was an unintended result of the worm. In the late 1990s and early 2000s people started to use DDoS against educational institutions, web commerce sites, and government websites. In recent years, however, DDoS has become a prominent target since hactivistsm hackers have made DDoS one of their main tools to advance their ideology. Moreover, Anonymous has launched a DDoS attack to crash the servers and disrupt the system services to websites run by organizations such as Master card, PayPal, Visa, NSA, PSN, etc. [3]. Such malicious activity has caused inconvenience to end-users who are not able to access the resources and services of these organizations and to the organizations providing service since they must resolve the DDoS attack.

These attacks can result in a large expenditure of revenue to the servicing organization. The communication channel is important for organizing an attack. An agent manager model or an IRC model can be used to communicate with each other. Agent managers using the TCP / ICMP / UDP convention should have a modular mapping between attacker and manager, handler to the manager, and vice versa. This article covers DDOS attacks, DDOS attacks and operations, DDOS attack techniques, DDOS attack tools, and various attack and protection components. Finally, it is suggested that future research should be conducted in this area.

2. Literature Review

Many well-established studies in the Field of Cyber-attacks and it is protection methods. However, in this section, the most dangerous types of DDoS attacks and it is protection approaches have been discussed and critically analyzed.

2.1 The Most common types of Attacks

- **SYN Flood Attack**

An SYN attack occurs when the system is hit by an SYN packet and is initiated by an incomplete communication request that no longer satisfies the actual communication requirements resulting in a denial of service (DOS) [4], [5]. The bellow Figure 1 demonstrates the SYN Flood design.

DOI: https://doi.org/10.54216/FPA.070101

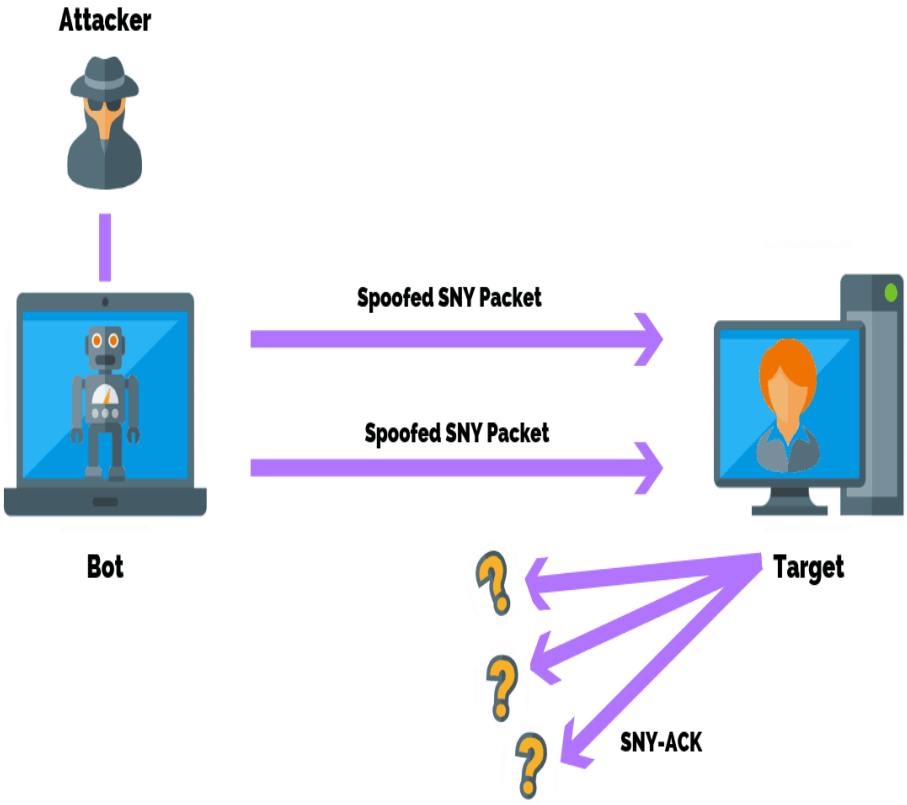

Figure 1: The architecture of SYN Flood Attack [5]

- **ICMP Flood**

ICMP flooding occurs when the ICMP overloads a system with so many repeating echoes that the system is expanded and then all resources fail until high system traffic can no longer be processed. By strengthening ICMP flood security, the Board of Directors can set thresholds that require ICMP floods when reviewed [5]. The architecture of the ICMP attack is illustrated below in Figure.

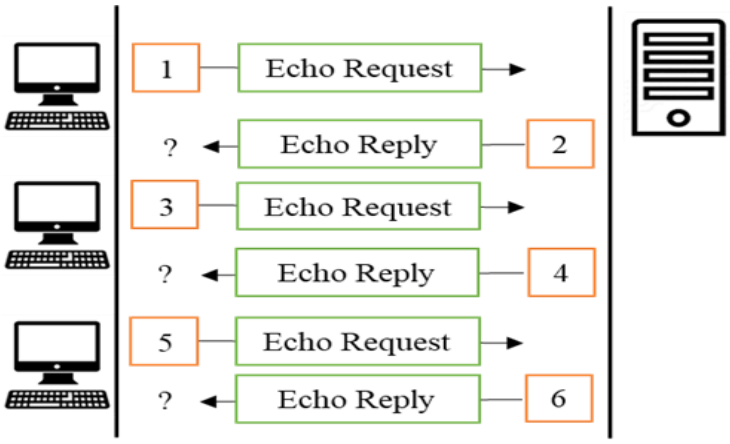

Figure 2: ICMP Flood Attack [3]

DOI: https://doi.org/10.54216/FPA.070101

- **UDP Flood Attack**

As with the ICMP flood, UDP occurs when UDP packets are started to block the system until it can no longer process valid legitimate connections. With increased UDP flood security, managers can define a threshold that exceeds protection against UDP flood attacks. [6]. The architecture of the UDP attack is presented in bellow Figure.

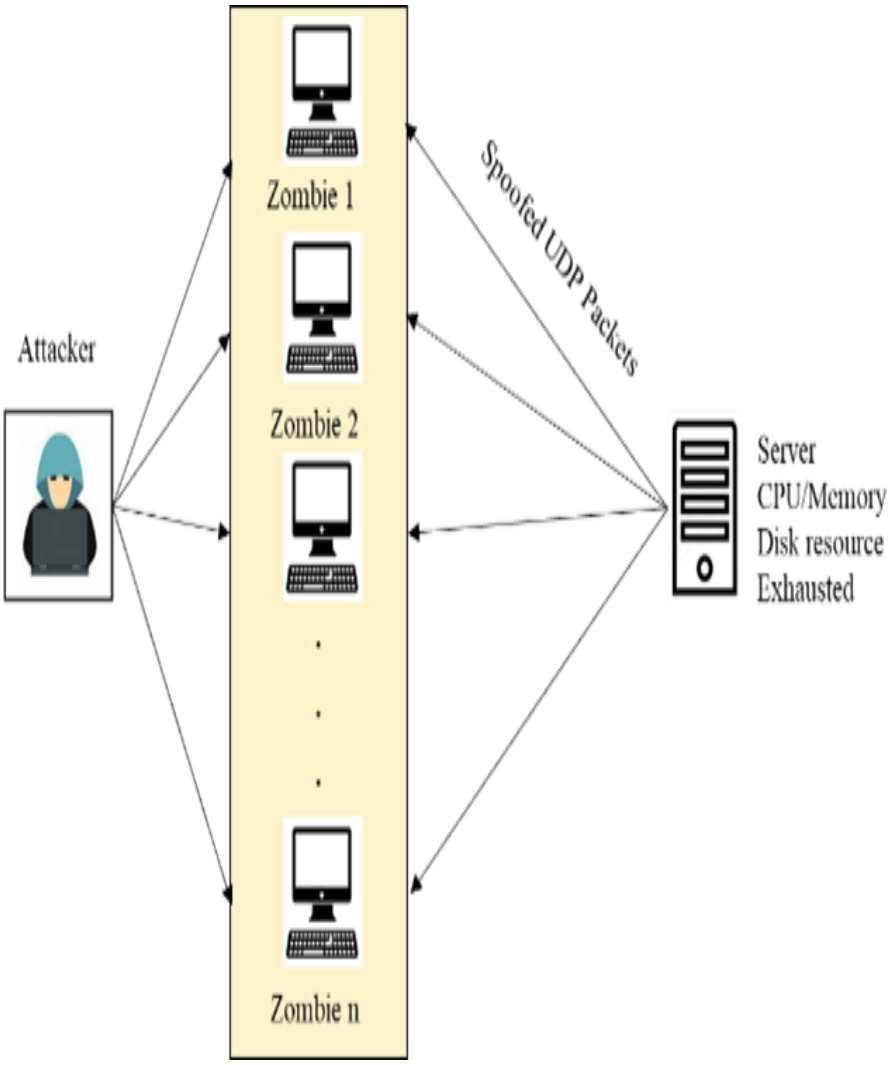

Figure 3: The Architecture of UDP Flood [6]

- **Misuse Attack**

Misuse attack is an emerging type of flooding attack. It is consuming the network resource, especially with resources that cannot be shared between multi-user, or the resources that can be shared for a limited number of users, in this attack, the attacker frees up the resources from other users and uses them for its benefits and using it for without sharing it with other users, this attack usually cases bottleneck problem, which leads to service delay or even services down of NFV network [4].

DOI: https://doi.org/10.54216/FPA.070101

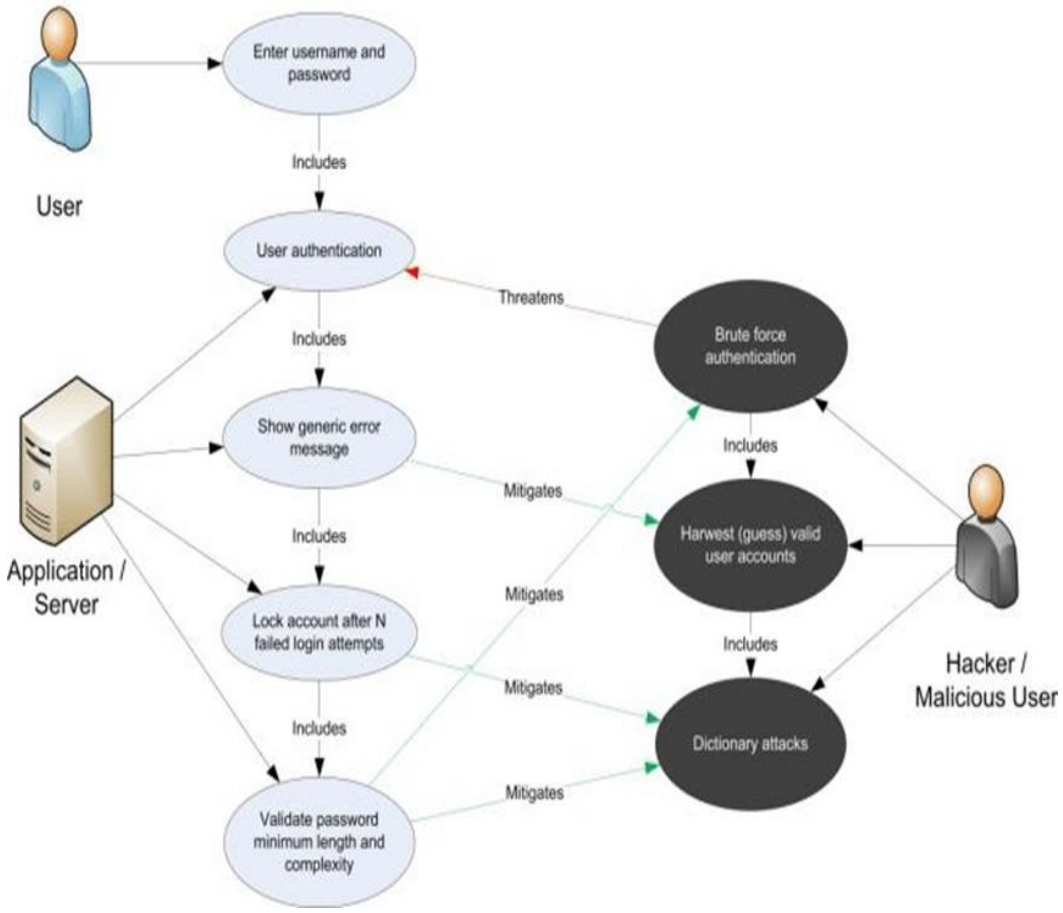

Figure 4: Misuse Flood Attack Architecture [5]

3. DDoS attack Defense Methods

DDoS attacks face many problems and challenges that are very difficult to solve and understand. In principle, unusual DDoS attacks do not have regular and recognizable features.

In the prior work of Shiaeles et al. [7], the DDoS attack detection point is complete and the boundaries are improved as much as possible using non-characteristic estimates for hairy attacks. The evaluation takes place on standard packages between the arrival times. The problem is divided into two parts, namely the detection of a DDoS attack and the IP detection of the victim. The location of the attack is carried out using actually severe thresholds, and the victim's IP address is recognized with moderate allowable requirements that can be used to quickly identify the victim's IP address. This in turn requires a hostile program that attacks the host computers and uses the appearance of time as a package as an essential measure for the detection of DDoS attacks.

The previous work of Rahul et al. [8] utilizes GA to distinguish real users and reduce the distance between the VoIP and SIP flood. The VoIP Flood Guidance Framework (VFD) is used to recognize both SIP and TCP flood attacks on SIP devices using the Hellinger separation rapid method. Moreover, in these methods and techniques, a Jacobi Quick Guide and Hellinger distance computational calculation, a numerically inconsistent technology, are used to correct as much as possible and find traffic anomalies.

Chambers etc. [9] provide an advanced NLP neural system program to detect DDOS attacks using only the Internet network as support. The system's private networks usually delay detecting attacks. In this way, a system that uses free information to define a system can better respond to a large-scale attack on various administrative services. The NLP model is considered a significant percentage of system management status for using web-based life. They

DOI: https://doi.org/10.54216/FPA.070101

show two educational models for this: the forward neural system and the incomplete LDA framework. Both models produced past work with high margins (20 ٪F1 scores).

Juneja et al. [10] propose a multi-agent plan to differentiate, protect and track the source of DDoS attacks. This provision explains where the DDoS attacks come from, but some operators are bound to achieve the best results. The table shows the analysis of defense technology.

Table 1: THE ANALYSIS OF THE DEFENSE METHODS

Ref.	Model	Advantage	Disadvantage
Shiaeles et al. [53]	Real-time DDoS attack detection approaches	It has the ability to detect DDoS and identify malicious IPs in real-time.	It is inefficient in handling FC. Also, it the difficulty to detect the attack at the source before the attack
Rahul et al [60]	VoIP Flood Detection System	It is fast and accurate in detecting DDoS attacks.	It is inefficient against FC.
Chambers et al. [69]	The neural language processing model	It is very effective in defending against DDoS attacks.	It is limited to dealing with some types of attacks.
Juneja et al. [73]	An agent-based framework to counterattack DDoS Attacks	It has the ability to trace a distant source of different types of DDoS attacks.	It is still unsure about how many software agents shall be employed to work optimally.

4. Conclusion

The purpose of this article is to understand current security issues and a brief overview of the offered solutions for different protection systems and approaches. Moreover, the research covers a total of 15 reviews and research articles. It applies to OSI network layers, servers, network management, IoT, Cloud Computing, and all devices which have an Internet connection. The brief review provides an exhaustive and detailed step-by-step study of the robust methods used to recognize and prevent DDoS attacks. Lastly, the purpose of this article is to help develop modern and effective protection strategies for defending against DDoS attacks. Additionally, DDoS attack component settings include updates and endless improvements to handle new and complex emerging threats.

The Funding of the work: "This research received no external funding"

The Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] K. Igor and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," International Journal of Computing vol. 4, pp. 113-123, 2014.

[2] K. Sharma and B. Gupta, "Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices, "International Journal of E-Services and Mobile Applications (IJESMA)," vol. 10, pp. 58-74, 2018.

[3] A. Saied, R. Overill and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," Neurocomputing, vol. 172, pp. 385-393, 2016.

[4] K. Prasad, A. Reddy and K. Rao, "DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey," Global Journal of Computer Science and Technology, 2014.

[5] N. Z., Bawany, J. A., Shamsi & K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions ". *Arabian Journal for Science and Engineering*, *42*(2), 425-441, 2017.

[6] J. Ye, Cheng, X., J. Zhu, L. Feng & L. Song, "A DDoS attack detection method based on SVM in software defined network. *Security and Communication Networks*, *2018*.

[7] Z. Tan, A. Jamdagni, X. He, P. Nanda, & R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis, ". *IEEE transactions on parallel and distributed systems*, *25*(2), 447-456, 2013.

DOI: https://doi.org/10.54216/FPA.070101

[8] J. Gonzalez, M. Anwar and J. Joshi, A trust-based approach against IP-spoofing attacks," In Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on (pp. 63-70). IEEE. (2011, July).
[9] S. Shiaeles, V. Katos, A. Karakos, and B. Papadopoulos, "Real time DDoS detection using fuzzy estimators," computers & security, vol. 31, pp. 782-790, 2012.
[10] A. H. Azizan, S. A. Mostafa, A. Mustapha, C. F. M. Foozy, M. H. Abd Wahab, M. A. Mohammed and B. A. Khalaf," A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems," Annals of Emerging Technologies in Computing (AETiC), 5(5), 2021.
[11] N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta," Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence", Journal of Network and Computer Applications, 173, 102871, 2021.
[12] D. M. Abdullah and A. M. Abdulazeez," Machine Learning Applications based on SVM Classification A Review," Qubahan Academic Journal, 1(2), 81-902021.
[13] A. Rahul, S. Prashanth, S. Kumar and G. Arun, "Detection of Intruders and Flooding In Voip Using IDS, Jacobson Fast And Hellinger Distance Algorithms," IOSR Journal of Computer Engineering (IOSRJCE), vol. 2, pp. 30-36, 2012.
[14] N. Chambers, B. Fry and J. McMasters, "Detecting Denial-of-Service Attacks from Social Media Text: Applying NLP to Computer Security," In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers) (Vol. 1, pp. 1626-1635). (2018).
[15] D. Juneja, R. Chawla and A. Singh, "An Agent-Based Framework to Counter attack DDoS Attacks," International Journal of Wireless Networks and Communications, vol. 1, p. 193, 2009.

DOI: https://doi.org/10.54216/FPA.070101