Distributed Denial of Service Attack with Large Language Model

Haojun Wang*

Chongqing Nankai Secondary School, Chongqing, China

*Corresponding author: shangdi3525@gmail.com

Abstract. Distributed Denial of Service (DDoS) attacks take full advantage of distributed networks by sending a relentless barrage of requests to a target server to disrupt the regular operation of the server. The main difference between a DDoS attack and a traditional Denial of Service (DoS) attack is its decentralized nature. This characteristic increases the attack's impact and thus creates incredible difficulty in prevention. Traditional DDoS strategies cover flooding attacks (e.g., TCP SYN and UDP floods), protocol usage techniques (e.g., SYN floods and the infamous Ping of Death), and resource exhaustion strategies (e.g., HTTP floods). Each of these proposed strategies relies on large amounts of bandwidth, and recent results achieved on detection systems provide more efficient mitigation means. A significant change in the pattern of modern DDoS attacks shows the rise of amplification attacks, an attack strategy that cleverly exploits weaknesses to increase traffic beyond its initial scale. In addition, the phenomenon of hybrid attacks has become more prominent, which integrates various DDoS tactics into more sophisticated and powerful attacks, e.g., combining application-layer attacks and traffic flooding, thereby crippling both the application and network layers. As network threats become more sophisticated, we must innovate our defence strategies to ensure their effectiveness. In order to gain a deeper understanding of the potential threat of DDoS, it is critical to delve deeper into traditional attack tactics, analyze specific case studies in depth, and explore the impact of emerging technologies. This article delves into traditional DDoS attacks, current threat perceptions, and how artificial intelligence can play a role in the face of these cold attacks.

Keywords: DDoS attack; Large Language Model; Artificial Intelligence; Machine Learning.

1. Introduction

Distributed Denial of Service Attack (DDoS), that is, distributed denial of service attack, is an attack mode that uses the distributed network to launch many requests to occupy the target server or network resources, thus causing the target system to fail to provide services typically. DDoS attacks send many useless network requests to a specific target by manipulating multiple computers or machines (usually called "botnets"), which will overwhelm the target server, service or network, making it impossible for legitimate users to access or use. Compared with the traditional DoS (Denial of Service (DoS) attack, DDoS attacks adopt a distributed attack mode, which makes the attack more powerful and challenging to prevent.

Traditional DDoS attacks use various types of code to exploit network vulnerabilities. Although these methods were once effective, they have certain limitations: Flood Attacks: Traditional flood attacks, such as TCP SYN floods or UDP floods, involve overwhelming the target with excessive traffic. These attacks exploit the target's bandwidth and processing capacity but often require substantial bandwidth from the attacker's side [1]. Protocol Vulnerabilities: Protocol-based attacks are mainly implemented with the help of vulnerabilities existing in network protocols. For example, the SYN flood attack sends massive connection initialization requests to the server, causing the server to be overloaded with resources and unable to respond effectively to regular user requests. In severe cases, the server can be overwhelmed and unable to process legitimate connections.

Ping of Death attacks involves sending oversized packets to disrupt network services [2]. Resource exhaustion: HTTP flooding attacks cause severe degradation or even a crash of the server by sending massive HTTP requests to the target server to exhaust its CPU and memory resources or consume all available connection slots[3]. Despite their previous effectiveness, these methods have several

drawbacks: High Bandwidth Requirements: Traditional attacks often require considerable bandwidth, limiting their effectiveness against targets with high-capacity networks [4]. High Bandwidth Requirements: Traditional attacks are often limited by large bandwidth requirements, a characteristic that significantly reduces their effectiveness and utility against targets with high-bandwidth network facilities [4]. Detection and Mitigation: The continued evolution of intrusion detection technologies and firewalls has significantly simplified recognizing and responding to traditional Distributed Denial of Service (DDoS) attacks. Modern systems can detect attack patterns and execute appropriate defence strategies universally [5].

Traditional DDoS attacks have undergone a profound transformation, evolving from both their modern variants and traditional methods. The complexity of the technology has elevated the primary technical means, such as the flooding events of the underlying TCP SYN. For example, amplification attacks exist in modern times. A variant of this is called amplification attacks. The attacker enhances the attack traffic by using specific network protocols. This technique quickly generates large data streams from relatively simple requests by fully exploiting the potential shortcomings of services such as DNS and NTP. There is a growing trend toward hybrid attacks, a strategy that blends multiple DDoS techniques to create more complex and intense strikes, such as fusing application-layer and volumetric attacks to suppress both the application layer and the network layer simultaneously. The DDoS attacks reveal a clear direction toward the increasing sophistication of cybersecurity issues. Due to the increasing sophistication of the attackers' behaviour, the means of dealing with these new intrusions also need to be constantly updated and improved. Traditional DDoS mitigation strategies are losing effectiveness in dealing with these modern challenges, highlighting the need to develop novel protection techniques to solve the problem constantly.

In order to gain a deeper insight into the overall picture of DDoS attacks, it is highly critical to do an in-depth analysis of traditional attack methods, review relevant case studies and examine the potential effectiveness of emerging technologies. This section will delve into traditional DDoS, current perspectives, and the use of artificial intelligence in DDoS attacks.

2. The Overview of DDoS Attack

Mirai Botnet Attack. DDoS (Distributed Denial of Service Attack) is a malicious attack method that sends many requests to a target server or network through a distributed network to exhaust its server resources or network bandwidth, ultimately resulting in the target system being unable to provide services typically. DDoS attacks send many useless network requests to a specific target by manipulating multiple computers or machines (usually called "botnets"), which will overwhelm the target server, service or network, making it impossible for legitimate users to access or use. Compared with the traditional DoS (Denial of Service (DoS) attack, DDoS attacks adopt a distributed attack mode, which makes the attack more powerful and challenging to prevent. Figure 1 shows the botnet distribution of DDoS attacks in the DDoS attack threat report released by Tencent Security in the first half of 2022. The Mirai botnet was the most threatening botnet in the first half of the year regarding attack instructions and the number of DDoS attacks launched. In the first half of 2022, the Mirai botnet launched more than 60% of DDoS attacks, and the utilization rate of TOP20 high-risk vulnerabilities in the past two years was close to 100%. At the same time, Mirai also has about 40% of the total number of broilers, which is more than the sum of Bill Gates in second place and Gafgyt in third place.

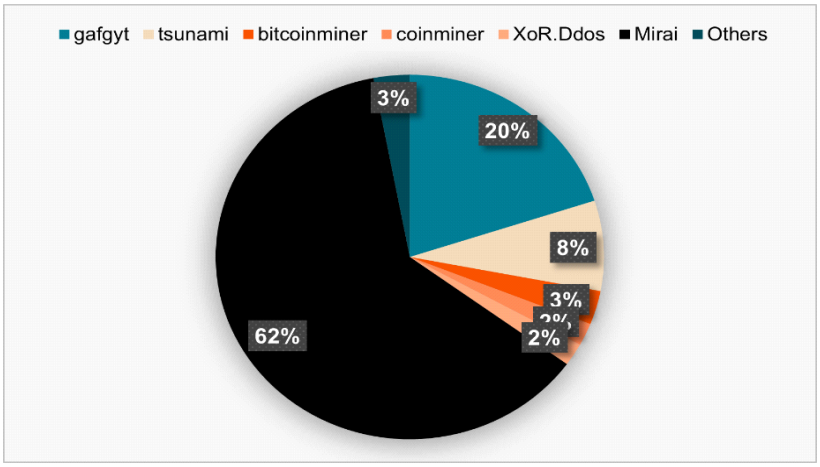

Fig.1 Botnet distribution of DDoS attack activities [6]

GitHub Attack. The GitHub attack in 2018 is noted as one of the most significant DDoS attacks, reaching 1.35 Tbps. With the Memcached protocol, an attacker utilizes an amplification attack method to unleash network traffic. The attack strategy works like this: the attack method is implemented by contacting an inappropriate Memcached server. By making subtle requests to these servers, the attacker causes a considerable increase in responses, which leads to an expansion of the attack traffic that puts a heavy strain on GitHub's infrastructure [7]. Mitigation phase: The high-speed response and traffic cleanup services provided by GitHub became a decisive factor in mitigating the negative impact of the attack. This occurrence further emphasizes the importance of maintaining exposed services and employing an efficient traffic screening system.

The nature of DDoS attacks continues to evolve, further emphasizing the urgency of ongoing research and timely adaptation. Current theoretical perspectives highlight a constantly evolving threat structure: DDoS attacks appear progressively more intricate, accompanied by the emergence of new techniques and attack vectors. Attackers continue to seek entirely new means of bypassing existing defence mechanisms. The combination of Artificial Intelligence and Machine Learning: There is a growing willingness to leverage these two technologies to optimize DDoS attack detection and mitigation methods. This set of techniques opens up new opportunities to study giant data sets and identify attack types more efficiently. Applying AI techniques to DDoS defence lines is a cutting-edge research area total of potential. While AI can improve the efficiency of identification and response, we must also be clear that it also introduces new problems, such as possible adversarial attacks on AI systems.

In Section 3, this paper presents recent advances in DDoS detection by the most popular large-scale language models in AI.

3. DDoS Attack Detection with Large Language Model

AI technology significantly enhances detection efficiency and mitigates large-scale attacks. Machine learning models can parse network traffic patterns and identify atypical attack behaviour features, significantly reducing response time and increasing processing efficiency. CASE STUDY: Kumar and Rajasekaran (2018) revealed the efficiency of machine learning approaches in identifying anomalous behaviours associated with distributed denial-of-service (DDoS) attacks. By applying supervised learning algorithms, they significantly improved attack detection accuracy and effectively reduced false positives.

AI technologies are now incorporated into firewall systems to strengthen defences against distributed denial-of-service (DDoS) attacks. Modern firewalls use deep learning algorithms to perform on-the-fly traffic parsing, automatically recognizing and responding to anomalous traffic patterns. Case study: Google's exemplary use of machine learning to strengthen defences against distributed denial-of-service (DDoS) attacks. Google's firewall system uses artificial intelligence to

identify and block aggressive traffic, demonstrating the effectiveness of AI in maintaining a secure network architecture. Personal Perspective: AI's role in DDoS defence is transformative, offering enhanced detection and response capabilities. However, as AI systems become more central to cybersecurity, it is essential to consider the implications of their potential misuse and ensure robust security practices are in place.

Recently, the large language model has performed well in understanding unnatural languages. It has been pointed out that the traditional defence algorithm will connect the harmful information flow to the cleaning equipment after detecting it. However, the current detection is mainly based on specific rules, which can not accurately identify targeted attacks. At the same time, in the case of using a botnet, the traditional algorithm has a high delay and colossal computing power consumption.

DoLLM can detect DDoS attacks by extracting the correlation in each data stream, and at the same time, it can detect the traffic and alarm data of quintuple attacks reported by NetFlow. They sorted the obtained data first and then gave them to llmS, from which LLMS can get some parameters they set to get the results, which proved the effectiveness of their use of LLM in DDoS detection in experiments [7].

In addition, using the learning ability of the large language model, the existing work has injected domain knowledge to make the large language model distinguish different kinds of attacks. Specifically, this work divides information flow into mild and illegal traffic, decomposes illegal traffic into different classes, and classifies them based on the big language model. According to different classification results and domain knowledge injection, the large language model can generate different mitigation strategies and can directly write different codes through these strategies to mitigate attacks [8].

Some work studies leveraged OpenAI's GPT-3.5, GPT-4, and Ada models to evaluate the efficacy of Large Language Models (LLMs) in recognizing DDoS threats using two different datasets: the CICIDS 2017 and the more intricate Urban IoT Dataset. By providing context through a limited number of examples (few-shot method) or by fine-tuning, LLMs could scrutinize network data, identify potential DDoS attacks, and offer rationales for their detections. The assessments indicated that, on the CICIDS 2017 dataset, few-shot LLM approaches utilizing just ten prompt samples neared an accuracy rate of 90%, while fine-tuning with 70 samples attained approximately 95%. For the more demanding Urban IoT Dataset, particularly in scenarios of intense DDoS attacks, few-shot techniques reached 70% accuracy, whereas fine-tuning achieved nearly 96%. LLMs exhibited superior performance compared to a Multi-Layer Perceptron (MLP) model trained on a comparable number of few-shot samples. Significantly, LLMs demonstrated the capacity to articulate the reasoning behind their DDoS detections in few-shot learning scenarios and showed considerable promise. Besides, they formulate precise prompts that guide GPT-4 in analyzing attack behaviours and providing detailed explanations, as shown in Figure 2.

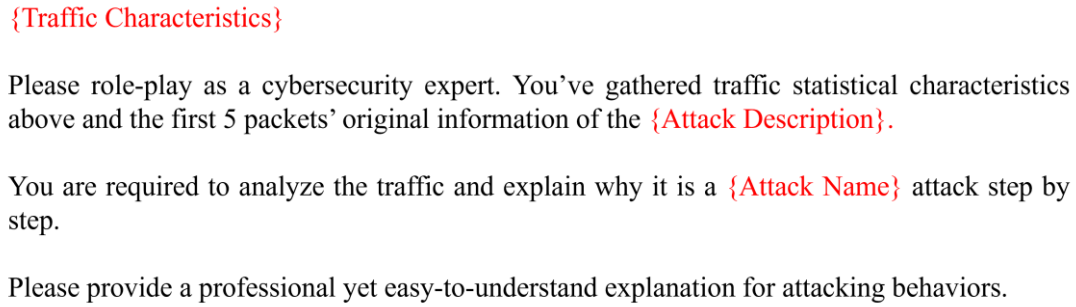

Fig. 2 The prompt template for the explanation generation [9]

4. Discussion

Although the large language model shows good discovery potential in DDoS detection, it still has limitations. The limitations of the large language model in DDoS detection are mainly reflected in the following aspects:

Lack of professional knowledge. DDoS attacks involve complex network protocols, traffic patterns, and behaviour analysis, and in-depth professional knowledge is needed to identify them accurately. Although the big language model is excellent in dealing with natural languages, it often needs more knowledge in specific professional fields, such as network security, and it is difficult to fully understand the varieties and latest technologies of DDoS attacks.

Real-time challenge DDoS attacks are usually sudden and rapid, which requires the system to respond quickly and take measures. The training data of a large language model is static and can not be updated in real time to reflect the latest attack methods and characteristics. Therefore, there may be a lag in detecting new DDoS attacks.

Computational complexity and performance bottleneck. DDoS detection must deal with a large amount of network traffic data and requires accurate judgment quickly. Large language models may face computational complexity and performance bottlenecks when dealing with large-scale data, especially in real-time detection scenarios, which may affect the accuracy and timeliness of detection.

False positives and false negatives. DDoS detection needs to improve the detection rate as much as possible while ensuring a low false positive rate. When generating predictions, large language models may be influenced by noise and bias in training data, resulting in false positives or false negatives in DDoS detection. In addition, the model cannot identify complex attack patterns and may not accurately distinguish regular traffic from malicious traffic.

The acquisition and understanding of information is continuously learning to meet more diverse contextual needs. DDoS attack detection usually needs to comprehensively consider the network traffic data and the contextual information of the entire network environment to make judgments and identifications. When parsing network traffic data, large language models need to fully grasp the traffic characteristics and the background knowledge of the network ecosystem in which they are located. This process directly affects the accuracy of the detection results. For example, it may be difficult for the model to accurately recognize whether specific seemingly abnormal traffic flows constitute distributed denial-of-service (DDoS) attacks.

5. Conclusion

Distributed denial-of-service (DDoS) attacks take advantage of distributed networks by submitting impatient requests to a given server, thereby severely disrupting its regular operation. The main difference between DDoS attacks and regular denial-of-service (DoS) attacks is their degree of decentralization, which further increases the impact of DDoS attacks and the difficulty of preventing their spread. Difficulty. Traditional DDoS (DDoS) methods consist primarily of flooding (e.g., TCP, SYN, and UDP floods), protocol-based techniques (e.g., SYN floods and the infamous Ping of Death), and resource exhaustion approaches (e.g., HTTP floods). While recent advances in our detection capabilities have provided us with more efficient buffering, these tactics still often require immense bandwidth reserves. Today, the pattern of DDoS attacks has changed dramatically, as evidenced by the rise of amplified aggressive behaviour, which skillfully employs attack weaknesses to augment traffic far beyond the scale and utility of its early days. In addition, hybrid attack approaches have become particularly important, combining DDoS methods with other attacks to generate more advanced and powerful attacks, such as combining application layer attacks with traffic flooding tactics to destroy both the application and network layers. Given the increasing complexity of cybersecurity issues, continuous innovation in defence strategies is necessary to maintain their effectiveness. In order to delve deeper into the global nature of DDoS threats, the core step is to delve deeper into the traditional means of attack and further investigate the various implications of new

techniques by analyzing specific cases. This paper delves into traditional DDoS attacks, current security threat perceptions, and how artificial intelligence can counter these persistent attacks.

References

[1] Ahmed Bakr, A. A. Abd El-Aziz, Hesham A. Hefny. A survey on mitigation techniques against ddos attacks on cloud computing architecture. International Journal of Advanced Science and Technology, 2019, 28(12): 187-200.

[2] Jelena Mirkovic, Peter Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[3] Jasmeen Kaur Chahal, Abhinav Bhandari, Sunny Behal. DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges. Computer Science Review, 2024, 53: 100644.

[4] Georgios Kambourakis, Constantinos Kolias, Angelos Stavrou. The mirai botnet and the iot zombie armies //MILCOM 2017-2017 IEEE military communications conference (MILCOM). IEEE, 2017: 267-272.

[5] Mizuki Kondo, Rui Tanabe, Natsuo Shintani, et al. Amplification Chamber: Dissecting the Attack Infrastructure of Memcached DRDoS Attacks//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: Springer International Publishing, 2022: 178-196.

[6] https://security.tencent.com/index.php

[7] Qingyang Li, Yihang Zhang, Zhidong Jia, et al. DoLLM: How Large Language Models Understanding Network Flow Data to Detect Carpet Bombing DDoS. arXiv preprint arXiv:2405.07638, 2024.

[8] Tongze Wang, Xiaohui Xie, Lei Zhang, et al. ShieldGPT: An LLM-based Framework for DDoS Mitigation//Proceedings of the 8th Asia-Pacific Workshop on Networking. 2024: 108-114.

[9] Michael Guastalla, Yiyi Li, Arvin Hekmati, et al. Application of large language models to ddos attack detection//International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles. Cham: Springer Nature Switzerland, 2023: 83-99.