Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/2023376

Research on the reliability of bloom filters to defend a distributed denial-of-service

Jiaran Liu

Miami University, Ohio, 45056, United States

liuj150@miamioh.edu

Abstract. Distributed denial of service (DDoS) attacks are one of the threats to network security, and reasonable means of defense are sought. Bloom filter is a commonly used detection method, the research have listed different attacks in the paper and made it possible to compare it with other detection methods by analyzing how Bloom filter works. The research shows that the Bloom filter works by comparing the element to be queried with an already stored vector. If the query result is zero then the element does not exist, if it is one then it means that in most cases the element exists, but false positives are not excluded causing the element to be judged as existing. In this paper, the comparison with other methods also needs focus, the time complexity of inserting, searching, and deleting data is an important feature to consider when Bloom filters outperform other methods. The research also shows that the Bloom filter is to some extent better than other detection methods in terms of insertion, search, and deletion time. At the same time, the research showed that the use of Bloom filters in response to DDoS attacks is also very impressive, for the detection of link flooding attacks and the detection and processing speed of packets is commendable, can take up less memory to achieve better results.

Keywords: Link Flooding Attacks, Protocol Attack, Application Layer Attacks, Wrap-around Counting Bloom Filter.

1. Introduction

Distributed Denial of Service (DDOS) has become a concern in network security over time, as a serious DDoS attack can cause incalculable damage to an enterprise. So finding an effective means of defense is the goal of enterprises. For DDOS defense methods, the basic defense method is divided into three main, black and white list protection, network infrastructure security facilities, and defense with the offensive way [1]. Although there are many defense mechanisms, it is also very important to judge whether a defense mechanism is valid or not. We need to analyze a method from different perspectives so that we can accurately determine its effectiveness. In this paper, we will discuss the effectiveness of bloom filter protection against distributed denial of service attacks and how it compares with other protection methods. The study will determine whether bloom filters are efficient in defending by the comparative analysis method. In the process of comparison, this paper will judge the reliability of the methods mainly based on the speed of retrieving attacks and the effectiveness of filtering attacks by different methods. The significance of this study is that it can help to use the need to defend against DDoS attacks whether the impact of the attack can be minimized using Bloom filters. It can be used as

© 2023 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/4/2023376

a judgment criterion for those who want to use Bloom filters as a defense weapon, helping people to be able to make a faster choice between Bloom filters and other methods.

2. The comparison between two different attacks in DDoS

DDoS attacks are classified as one of the four major security threats to networks, and threat participants use resources from multiple remote locations to attack an organization's online operations to implement distributed denial-of-service attacks [2]. The purpose of a distributed denial-of-service attack is to disrupt normal traffic to the target's servers, and it is a malicious means of flooding the target or the surrounding infrastructure with a large amount of Internet traffic. To a certain extent, a high-intensity distributed denial-of-service attack can force a web page to shut down [3]. DDoS attacks are divided into a variety of ways, and such attacks with different names can be summarized into two main categories, which are Application Layer attacks and Protocol Attacks as the more common types of attacks. In this type of attack, the system will often be difficult to respond.

2.1. The Application Layer attacks

Application Layer attacks are a common and deadly type of attack, its attacks are designed to disable or slow down services by using the application layer, and they use application functionality to cause severe damage rather than exploiting the capabilities of the attacking machine itself [9]. It mainly targets the software that provides the service. It attacks the server with minimal computer resource startup and evades detection of detection systems by mimicking merged traffic, where the two main types of detection systems are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) [4]. According to statistics, while network layer attacks decreased by 50% in the fourth quarter of 2017, application layer attacks nearly doubled [7].There are two common application layer attacks, one is called HTTP flooding attack and "low and slow" attack, HTTP flooding attack is mainly botnet by sending too many requests on the server, making the server crash and unable to respond. In a "low and slow" attack, it does not send any real data, but sends a small amount of traffic to keep the channel between itself and the server open [9].

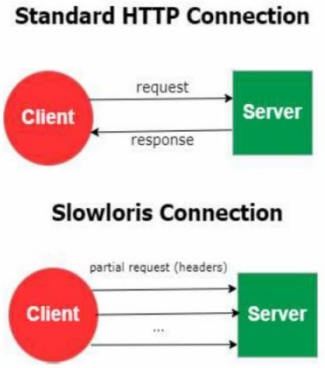


Figure 1. Low and Slow attacks keep connections open without completing the request, thus keeping server threads busy waiting for nothing and never sending the final response [9].

As more and more outstanding requests appear in the server and clients, this often causes a busy line in the system, making it impossible for the system to respond in a timely manner and thus crashing the server.

2.2. The protocol attacks

The purpose of the protocol attack is to consume the server's resources and make it wait for a response and thus crash. Protocol attacks typically occur at OSI layers 3 and 4 to manipulate traffic [1]. The protocols are mainly divided into IP protocols as well as TCP protocols, one of the most typical examples of using TCP protocols is the SYN flooding attack, in which the attacker sends data to the server via a forged IP address and waits for the client to respond because the service area needs to comply with the terms of the network. However, the attacker never replies, which causes the server's resources to be

DOI: 10.54254/2755-2721/4/2023376

taken up by a large number of useless resources, which leads to a breakdown. Protocol attacks make the server have an unbearable pressure, and too much traffic often makes it difficult for the server to handle. SYN flooding attacks are mainly based on the three handshake protocols of the TCP protocol. SYN attacks capture the guidelines of the handshake protocol in the TCP protocol making the whole process incomplete and thus leading to a denial of service.

2.3. The way to defend against DDoS attacks

The main way of DDoS attacks is to use spoofed source IP addresses. Many researchers have researched countermeasures for this attack method. The main way is to mark the packets with a backtracking mechanism. The victim can use this information to reconstruct the path the packet took through the acquisition. This mechanism from this backtracking helps the victim to install network filters upstream to stop the attack traffic [10]. Among the choices of network filters, Bloom filters can be very efficient in accomplishing the task, and a closer look at how Bloom filters operate to enable DDoS attacks to be successfully defended against in a later study.

3. The reliability of Bloom filters in DDoS

DDoS attacks are very frequent, and the emergence of Bloom filters has helped to counter these attacks. However, the effectiveness of Bloom filters is a topic that needs to be explored. A study by Ripon found that Bloom filters are dump data structures that can largely cope with DDoS attacks, and that there are many types of Bloom filters that can be modified to help prevent DDoS attacks. We can see that the effectiveness of Bloom filters is very considerable. Although Bloom filters have a silly data structure, most researchers have designed a DDoS defense system by Bloom filters [6]. In addition to the use of Bloom filters at the level of some turn-out data structures, their performance against DDoS in the Internet of Things is also very impressive. The study found by Gang showed that IoT devices are generally small and resource-constrained, and common Information-Centric Networking (ICN) is not applicable to new DDoS attacks like Interest Flooding Attacks (IFA). In contrast, a mitigation mechanism based on Bloom filters can effectively reduce memory costs while ensuring detection accuracy and latency, in addition to better defending against attacks brought by DDoS.

3.1. The way Bloom filters work in DDoS

A Bloom filter works by entering a set with n elements. In the Bloom filter a certain bit of vector is assigned, setting them all to zero, and then the input is read through different loops, through which we set the vector to one at a specific position. If we need to use a Bloom filter, we will compare the element to be queried with the vector in the Bloom filter, and if any bit of the query results in zero then the element does not exist.

```
Input: Set of n elements;
Output: Bloom filter A;
A = allocate m bits initialized to 0;
for each x_i in the set do
    for j ← 1 to k do
        A[h_j(x_i)] ← 1;
```

Figure 2. Pseudocode for programming phase [11].

```
Input: An element y;
Output: True/False;
for j ← 1 to k do
    If A[h_j(y)] = 0 return False;
return True;
```

Figure 3. Pseudocode for querying phase [11].

In the pseudo code, the Bloom filter collects different inputs and finally changes all identified bits to 0. Then, after comparing the searched data with the stored bits, it returns true if it exists and false if it does not. Bloom filter is a structure based on probabilistic data, which can search for the desired element in

DOI: 10.54254/2755-2721/4/2023376

a collection of elements quickly, it is very fast, basically the search can be completed in constant time. Bloom filter mainly returns true and false, and its results are also divided into true positives, and false positives. For a few cases, Bloom filter will also give wrong results. The reason for giving an incorrect result may be that when looking for a specific element, the bit in the Bloom filter is accidentally set to 1 when looking for other elements before, which can easily lead to an incorrect result because the element does not actually exist.

3.2. Filtration effectiveness of Bloom filter

The filtering performance of Bloom filter has remarkable effectiveness in defending against different attacks, especially for DDoS attacks, which greatly helps to relieve the pressure on the server. A research found by peng showed that if eighty percent of the attacks are detected as well as resolved in real time, then the link can remain in good condition, and in their detection of link flooding attacks, the detection accuracy of Bloom filters from this we can see that Bloom filters can achieve good filtering effectiveness for link flooding attacks in DDoS and can filter most of the attacks. Bloom filters not only have great filtering effectiveness for link flooding attacks, but also do not have delays in processing requests while maintaining multiple Bloom filters. During a DDoS attack, there will be a large number of packets transmitted compared to the normal case, there is an effective data structure called Wrap-around Counting Bloom Filter (WCBF) to minimize the number of packets required and also as a variant of Bloom Filter can be used for packet marking. In the face of DDoS attacks, we can use multiple WCBFs for defense. With the use of multiple Bloom filters we can still make the system handle a large number of requests smoothly, thanks to the fact that Bloom filters are a space-saving data structure, so even multiple Bloom filters can keep the memory consumption low. The most important thing is that Bloom filter insertion and search are always kept at O(1). So the effectiveness of Bloom filters to successfully filter DDoS attacks is very impressive [5].

4. Comparison of other methods with the bloom filter method

Bloom filters appear to be more efficient than other defenses against DDoS.

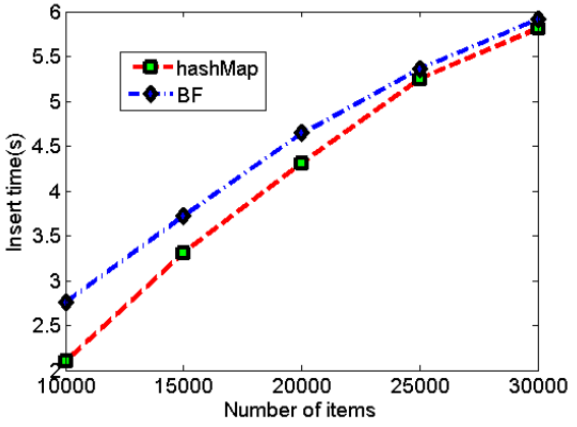


Figure 5. The comparison of methods on detect processing [8].

Comparing the hash map with the Bloom filter under link flooding attack, although the Bloom filter takes longer to insert values, the Bloom filter has a faster detection time because the hash map is slower than the Bloom filter in terms of search speed. So compared to the Bloom filter based on different ways of retrieving data, making it more efficient compared to other means of defense against DDos [8]. In addition, when we need to store pairs of key-value pairs, Bloom filters are compared with linked lists (queue) and search trees. The time complexity of both insertion and search of Bloom filter remains in O(1), but the time complexity of insertion, search and deletion of the other two is in O(log(N)) [5]. Compared to other methods, Bloom filter is more advantageous in terms of processing data streams, which can be solved with more efficient processing speed while occupying less memory. Therefore, Bloom filter is superior when other methods are compared with Bloom filter.

DOI: 10.54254/2755-2721/4/2023376

5. Conclusion

In this research, the research introduced what has distributed denial of service attacks and listed the different ways of attack. DDoS attacks are a major concern in network security, so the reliability of Bloom filters becomes one of the key points to be explored. Application layer attacks and protocol attacks are very common types of DDoS attacks, and both of them can make the server crash. Among the protocol attacks, SYN flood attacks are also one of the culprits that make it difficult for servers to withstand great pressure. After analyzing how the bloom filter works and the effectiveness of successful filtering, it is found that the reliability of the bloom filter is very high and it is able to defend well against some DDoS attacks. Especially for packet detection and link flooding attacks are extremely important to help, more than 80% of attacks can be detected, while under DDoS attacks, a large number of packets can also be handled by Bloom filter in a smooth way. Compared with other defenses, the performance of the bloom filter is more excellent in terms of detection data time, which is mainly attributed to the different operation methods of the bloom filter compared with other defenses. The shortcoming of the study is that there is no analysis of the performance of Bloom filter under other attacks, and in the future Bloom filter can be placed under more attacks for comparison. In addition, the paper does not focus on volume-based attacks, which can be carefully analyzed in the future.

References

[1] Dzurenda, Petr, Zdenek Martinasek, & Lukas Malina. "Network Protection Against DDoS Attacks." International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems [Online], 4.1 (2015): 8-14. Web. 17 Aug. 2022

[2] "What Is a DDOS Attack and How Does It Work: Cybersecurity: Comptia." Default, https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works.

[3] Case Study: Distributed Denial of Service Attacks (Ddos) - the Engine Room. https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf.

[4] J. D. Ndibwile, A. Govardhan, K. Okada and Y. Kadobayashi, "Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication," 2015 IEEE 39th Annual Computer Software and Applications Conference, 2015, pp. 261-267, doi: 10.1109/COMPSAC.2015.240.

[5] S. Saurabh and A. S. Sairam, "Increasing the effectiveness of packet marking schemes using wrap-around counting bloom filter", Security and Communication Networks, vol. 9, no. 16, pp. 3467-3482, 2016.

[6] Srinahyanti, Srinahyanti, et al. "Influence of Gadget: A Positive and Negative Impact of Smartphone Usage for Early Child." EUDL, 12 Aug. 2019, https://eudl.eu/doi/10.4108/eai.3-11-2018.2285692.

[7] "Q4 2017 Global Ddos Threat Landscape." Resource Library, 18 July 2022, https://www.imperva.com/resources/resource-library/reports/q4-2017-global-ddos-threat-landscape/?redirect=Incapsula.

[8] P. Xiao, Z. Li, H. Qi, W. Qu and H. Yu, "An Efficient DDoS Detection with Bloom Filter in SDN," 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 1-6, doi: 10.1109/TrustCom.2016.0038.

[9] S. Black and Y. Kim, "An Overview on Detection and Prevention of Application Layer DDoS Attacks," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022, pp. 0791-0800, doi: 10.1109/CCWC54503.2022.9720741.

[10] A. Yaar, A. Perrig and D. Song, "Pi: a path identification mechanism to defend against DDoS attacks," 2003 Symposium on Security and Privacy, 2003., 2003, pp. 93-107, doi: 10.1109/SECPRI.2003.1199330.

[11] Geravand, Shahabeddin, and Mahmood Ahmadi. "Bloom filter applications in network security: A state-of-the-art survey." Computer Networks 57.18 (2013): 4047-4064.