DDoS Attacks: Detection Techniques

By Alice Lin

AUTHOR BIO

Alice is a student at Nobles and Greenough school, in Dedham, Massachusetts. Her primary academic interest is computer science, and she is also interested in mathematics and physics. She appreciates the practical applications of computer science, and has completed research in the past on the usage of machine learning in different areas of healthcare. She hopes that with research she is able to explore different areas of computer science and gain more experience and knowledge about what she would like to pursue as a career. Outside of academics, she enjoys spending her time reading, running, and baking.

ABSTRACT

As we become more reliant on technology, we also become more vulnerable to cyberattacks. One of the most common types of cyberattacks is DDoS attacks, or Distributed Denial of Service attacks. These attacks are carried out to make certain servers or web pages unavailable, or very slow to update. One of the reasons DDoS attacks are very effective is that it is very hard to catch the attacker while the DDoS attack is occurring. Therefore, one of the crucial steps to protecting oneself against DDoS attacks is to develop a way to distinguish between DDoS traffic and normal traffic, so that the normal traffic is not affected when the DDoS traffic is being dealt with. This paper provides an overview of what DDoS attacks are, as well as some of the methods people have researched to detect DDoS attacks and distinguish between the different types of traffic.

Keywords: Distributed Denial of Service, DDoS, Cybersecurity.

INTRODUCTION

Distributed denial of services attacks, or DDoS attacks, occur when an attacker overwhelms a target so that it is not able to address legitimate traffic, rendering it unavailable to users. DDoS attacks are carried out through multiple devices, making them harder to detect. They are almost always carried out using bots, or zombies, which are devices with malware which allows the attacker to control them. A group of these bots are referred to as a botnet.

DDoS attacks have become more and more of an issue in our digital world. From 2021 to 2022, the number of DDoS attacks worldwide increased by 150% (Radware). There can be many motivations for an attack to launch a DDoS attack, ranging from financial, to political, to personal. Financial motives can have an attacker who demands the victim pay a fee before they stop the attack, or could be an attack between rival businesses. Political motives could be launched at oppressive governments or protestors, it could also be used to cause confusion in military troops or civilians when there is political unrest. These attacks can target large companies, small companies, or even personal web pages – no one is exempt. Following is a couple of major DDoS attacks in history:

On April 27, 2007, there was political conflict in Estonia between the Russian-speaking Estonians and ethnic Estonians. There was a surge in cyberattacks, most of them being DDoS. People were using ping floods and botnets to attack financial institutions, government departments, and media outlets.

On July 20, 2008, the government of the Republic of Georgia experienced a DDoS attack right before being invaded by Russia. This attack highlights how cyberattacks have and can be used alongside physical attacks.

On March 18, 2013, the Spamhaus incident occurred, sometimes also called "Attack that Almost Broke the Internet." Spamhaus added a group called Cyberbunk to their blacklist, and the group responded with a DDoS cyberattack. The attack even managed to take down Cloudflare, which was an internet security company which was designed to combat DDoS attacks.

On February 28, 2018, there was a DDoS attack on GitHub, which was viewed as the most prominent developer platform. The attackers spoofed GitHub's IP address in order to send huge traffic towards them. However, it only took GitHub 10 minutes to get back online, as they routed the traffic through scrubbing centers.

In February, 2020, Amazon Web Services were attacked with a DDoS attack. It took Amazon Web Services three days to get back online and running. This attack was the largest to its date, 2.3 Tbps, while previously these attacks had only reached 1.7 Tbps. (CompTIA)

As DDoS attacks become more common and damaging, it becomes more important for people to be aware of these attacks, as well as how to protect themselves from them. One of the first steps someone can take to protect themselves from DDoS attacks is being able to detect when one is occurring, and when it is occurring knowing what traffic to ban and what traffic to let through. This paper attempts to highlight some of the methods people have researched to detect and separate DDoS traffic and normal traffic.

Types of DDos Attacks

DDoS attacks take advantage of the natural connection that occurs between devices and networks. These connections can

be modeled by the OSI model, which divides the network connection into 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

1. The first or bottom layer is the Physical Layer. This layer refers to the physical or electrical components, and is where raw data bits are transmitted. Examples of what is encompassed in this layer include cable types, pin layouts, voltages, network adapters, etc.

2. The second layer is the Data Link Layer. This layer is where data is packaged into frames, as well as where error correction for the physical layer occurs. It then transmits the data through node-to-node connections.

3. The third layer is the Network Layer. This is the layer where the routers are. It determines the route the data will take to get to the correct IP address as its destination.

4. The fourth layer is the Transport Layer. This layer regulates the data transfer, meaning it determines how much data is being sent, how fast, the destination, etc. There are a number of different methods that can be used, the most common being Transmission Control Protocol (TCP) which is built on top of the Internet Protocol (IP).

5. The fifth layer is the Session Layer. This is the layer that maintains sessions between computers or other devices. The sessions are set up, managed, and terminated at this layer.

6. The sixth layer is the Presentation Layer. This layer makes sure that the data is in the correct format for the next step. Most of the time it is switching the data from application format to network format, or vice versa. Data encryption also occurs at this step.

7. The seventh, and final, layer is the Application Layer. This layer receives information from the users and also displays data to the user. This is where the human and the computer interact directly.

There are three main types of DDoS attacks: Application Layer, Protocol, and Volumetric attacks.

Application Layer attacks, also sometimes called Layer 7 attacks, are the most common type of DDoS attack. The attack targets the Application Layer of the network connection, where web pages are generated from HTTP requests. The attacker can initiate an HTTP flood, overwhelming the server with HTTP requests so that legitimate traffic cannot get through. There are multiple types of HTTP Flood attacks, one being GET attacks. During GET attacks, attackers utilize a botnet to send a large number of GET requests for large files to overwhelm the victim. Another type of HTTP flood is a Single Session or Single Request attack, where attackers will use only one HTTP packet, but include a large number of requests.

Protocol attacks target the third and fourth layer (Network and Transport Layers) of the OSI model, and is the second most common type of DDoS attack. One type of Protocol attack is the IP Null attack. All packets are expected to specify what transport protocol to use for the packet (ex: TCP, IMCP, etc.), but attackers can set the value to “null,” causing the server to consume resources to try to determine how it should deliver the packages. Another type of Protocol attack is the SYN Flood, where the

attacker sends many SYN request packets, but the final acknowledgement (ACK) never comes, leaving the server waiting. Slowloris is another type of Protocol attack which sends a large number of partial HTTP requests to a web server, in order to hold open many sessions to consume the server's resources.

Volumetric attacks create a ton of network traffic to overwhelm the server. The attack is usually carried out using amplification or a botnet. One type of Volumetric attack is a UDP flood attack, which is when a two-way session is not established, but instead the UDP sends data packets to the server without waiting for a reply. Another type of Volumetric attack is an ICMP (Ping) Flood. The Echo Request and Echo Reply commands are used to test network connectivity, and together the two of them form the "ping" command. The attacker will send a large number of Ping packets without waiting for the response from the server, which will consume the incoming and outgoing bandwidth of the server.

A common trick that attacks will use to carry out their attacks more effectively is spoofing. This is when they disguise their address as something else, making it easy for them to trick devices into sending packets to a victim that never requested them.

Detection

One of the most challenging parts to protecting against DDoS attacks is differentiating between legitimate and attack traffic. There have been multiple studies on the detection of DDoS, and this paper will go over some proposals.

Doshi et al. (2018) used multiple machine learning techniques to test the accuracy of each in distinguishing between normal and DoS attack packets. They used the K-nearest neighbors (KN), support vector machine with linear kernel (LSVM), decision tree using Gini impurity scores (DT), random forest using Gini impurity scores (RF), and a neural network (NN). The results showed that the LSVM performed the worst, and the decision tree and K-nearest neighbors both performed the best with an accuracy of 0.99. They also noted that the neural network was expected to do better if there had been more training data available. They also noted that in their feature importance testing, stateless features performed much better than stateful features.

Lee et al. (2008) used cluster analysis on a selection of parameters in order to recognise and classify each phase of a DDoS attack. The parameters they selected for detection were: the entropy of source IP address and port number, entropy of destination IP address and port number, entropy of packet type, occurrence rate of packet type, and number of packets. The cluster method used was hierarchical clustering. They divided the data set into five groups: normal, phase 1, phase 2, attack, and post-attack. They were able to detect three of the five phases.

Idhammad et al. (2018) used a semi-supervised machine learning approach. There were five steps to their proposal: dataset preprocessing, estimation of network traffic Entropy, online co-clustering, information gain ratio computation, and network traffic classification. To estimate the entropy they used the flow size distribution (FSD) features, source and destination packets count, and the source and destination bytes count. They also used a co-clustering technique to eliminate some of the normal traffic to avoid the noise it provides. They tested their method on three different datasets, and obtained accuracies of 99.88%, 98.323%, and 93.74%.

Saied et al. (2016) used an artificial neural network (ANN) for detecting DDoS attacks. They compared their neural network

approach to a couple of previous approaches, and found that their accuracy of 98% was the highest among them. They also compared the results of their network trained on old datasets compared to new ones, and found that the new datasets (with an accuracy of 98%) surpassed the old datasets (with an accuracy of 92%).

Singh & De (2017) also used an artificial neural network, and decided to train theirs with genetic algorithms instead of gradient descent. The features they used were the number of HTTP count, the number of the IP addresses, the constant mapping function, and the fixed frame length. After testing, their method had an accuracy rate of 98.04%, when detecting an application layer DDoS attack.

Discussion

While the methods presented in this paper all seem to be effective at detecting and categorizing DDoS attacks, they are all research methods that have not yet been applied to real life. It is also important to note that detecting DDoS attacks and differentiating between traffic is an important step to take in protecting against DDoS attacks, but it is not the end. Once the DDoS traffic is detected, there needs to be an implemented way to route that traffic into a sinkhole to prevent it from using up resources.

There are some methods available online to use for protection against DDoS attacks. One such method is cloud scrubbing devices, which are inserted between the DDoS traffic and your network. THey take the traffic and route it to a different location to isolate the damage from the target. Akamai, Radware, and Cloudflare all provide cloud scrubbing devices. Some businesses will protect against DDoS attacks by using multiple internet service connections. If the business feels that they are being overwhelmed by traffic, it is possible for them to switch from one to another to avoid the negative consequences of being overwhelmed by traffic. Content delivery networks (CDN) are networks that are separated to help mitigate the effects of DDoS attacks. Since they are separated, if one gets overwhelmed by traffic, they can distribute it to the other connected networks. Web application firewalls (WAF) are usually used in conjunction with other protection techniques. WAFs filter traffic coming towards a specific web server or application.

Conclusion

As DDoS attacks become more and more prevalent and effective, the need for detecting and preventing them also becomes more pressing. This paper highlights a couple of attempts at developing detection methods for DDoS attacks, a critical step in being able to prevent them. Further research could discuss ways to make this accessible to the public, as well as combining it with mitigation techniques once the DDoS attack is detected.

REFERENCES

America's Cyber Defense Agency. (2021, February 1). *Understanding Denial-of-Service Attacks* . cisa.gov. Retrieved August 26, 2023, from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Cloudflare. (n.d.). *What is a DDoS attack?* Cloudflare. Retrieved August 26, 2023, from

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

CompTIA. (n.d.). *WHAT IS A DDOS ATTACK AND HOW DOES IT WORK?* CompTIA. Retrieved August 26, 2023, from https://www.comptia.org/content/guides/What-is-a-ddos-attack-how-it-works

Cook, S. (2023, June). *20+ DDoS attack statistics and facts for 2018-2023* . Comparitech. Retrieved August 26, 2023, from https://www.comparitech.com/blog/information-security/ddos-statistics-facts/ Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. *IEEE* . https://doi.org/10.1109/SPW.2018.00013 Eliyan, L. F., & Pietro, R. D. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems* , *122* . https://doi.org/10.1016/J.future.2021.03.011

Forcepoint. (n.d.). *What is the OSI Model?* Forcepoint. Retrieved August 26, 2023, from https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20 Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. *Springer Link* . https://doi.org/10.1007/S10489-018-1141-2

Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of Recent Detection Methods for HTTP DDoS Attack. *Journal of Computer Networks and Communications* . https://doi.org/10.1155/2019/1283472

Kime, C. (2022, December). *Complete Guide to the Types of DDoS Attacks* . eSecurityPlanet. Retrieved August 26, 2023, from https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

Lee, K., Kim, J., Kwon, K. H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. *Elsevier* , *34* (3). https://doi.org/10.1016/J.eswa.2007.01.040 Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. *Springer Link* . https://doi.org/10.1007/s00500-021-06608-1

Radware. (2023, February). *Radware Full Year 2022 Report: Malicious DDoS Attacks Rise 150%* . Radware. Retrieved August 26, 2023, from https://www.radware.com/newsevents/pressreleases/2023/radware-full-year-2022-report-malicious-ddos-attacks/#:~:text=Number%20of%20attacks%3A%20In%202022,aimed%20at

%2 0organizations%20in%20EMEA

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Elsevier* , *172* . https://doi.org/10.1016/j.neucom.2015.04.101

Shaw, K. (2022, March). *The OSI model explained and how to easily remember its 7 layers* . Networkworld. Retrieved August 26, 2023, from https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html#:~:text=The%20layers%20are%3A%20Layer%201,Presentation%3B%20Layer%207%E2%80%94Application

Singh, K. J., & De, T. (2017). MLP-GA based algorithm to detect application layer DDoS attack. *Elsevier* , *36* . https://doi.org/10.1016/j.jisa.2017.09.004