Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Advanced Ddos Detection & Mitigation Technique At Data Center Level!

[1]Naveen Sharma , [2]Dr. Keshav Dev Gupta

[1]Ph.D Scholar, Sr. Assistant Professor Computer Science & IT APEX University, Jaipur.

[2]Ph.D Scholar, APEX University, Jaipur.

ACKNOWLEDGMENT

I would like to express my gratitude to Dr. KD Gupta Sir, Sr. Assistant Professor Computer Science & IT, APEX University, Jaipur, for providing me with full support and guidance in writing my Ph.D. synopsis and discussing the aim of the related article. Furthermore, I would like to thank all colleagues from the Computer Science & IT Department at the university campus for all the advice given and for proofreading the article and letting me publish it.

ABSTRACT

A Distributed Denial of Service (DDoS) attack addresses a significant danger to specialist organizations. All the more explicitly, a DDoS assault intends to disturb and refuse any assistance to real clients by overpowering the objective with countless malicious requests. A cyberattack of this sort is probably going to bring about colossal monetary misfortunes and economic loss for organizations and specialist co-ops because of expanding expenses.

Lately, AI (ML) strategies have been generally used to forestall DDoS attacks. For sure, numerous protection frameworks have been changed into intelligent smart frameworks using ML methods, which permit them to overcome DDoS attacks. This research article dissects ongoing examinations concerning DDoS identification strategies that have adjusted single and cross breed ML approaches in current systems administration conditions.

Furthermore, the article talks about various DDoS safeguard frameworks in view of ML procedures that utilize a virtualized climate, including distributed computing, programming, advanced cybersecurity technologies, AI, ML characterized organization, capacities, and virtualization conditions. As the advancement of the Internet of Things (IoT) has been the subject of critical exploration consideration lately, the article additionally talks about ML approaches as security arrangements against DDoS assaults in IoT conditions.

Moreover, the paper suggests numerous bearings for future exploration. This paper is planned to help the examination local area with the plan and advancement of powerful protection frameworks by Data Centers fit for defeating various sorts of DDoS attacks.

KEYWORDS

DDoS Attack, DDoS attack types, DDoS attack examples, DDoS attack taxonomy, DDoS attack detection techniques, DDoS attack prevention and detection, DDoS attack detection mechanism, DDoS protection strategy, DDoS protection techniques, DDoS attack Prevention, DDoS attack mitigation, DDoS prevention and solution, DDoS prevention limitation, DDoS monitoring, protect DDoS attack, DDoS prevention hybrid solution

INTRODUCTION

The internet in straightforward terms is characterized as an interconnected system of computer networks. The extent of the internet in everyday life is immense; it gives a wide scope of resources, information, services that permit all areas to be all around connected. As the requirement for the internet is developing with time, different issues about its security come into understanding.

The justification for internet insecurity is its design because the first concern was its functionality rather than its security. Henceforth a few types of attacks and dangers are the justification behind worry towards the security of the internet. The issues connected with internet security are authentication, confidentiality, integrity, availability, and non-reputation.

In this article, the principal center is around security and availability, availability implies that the information, the computing systems, and the security controls are generally accessible and operable in a serious state, at some irregular moment too. Among all DDoS (Distributed Denial of service) attacks are those which impede clients, users to access all benefits of services available to them from the server-side.

The DDoS attack brings about long system timeouts, lost revenues, huge volumes of work to recognize attacks and to get ready satisfactory response measures. A refusal of service (DoS) attack is a Distributed Denial of service (DDoS) attack since it is launched simultaneously to various machines. DDoS attacks are not another aggravation to the internet, they came late in August 1999 and after that perpetually their seriousness is developing.

A few perceived DoS attacks are SYN Flood, tear, smurf, and ping of death. There have been huge scope attacks focusing on some high-profile business sites like Twitter, Facebook, Amazon, and so on. There are assortments of DDoS attacks. Nonetheless, the most well-known type of DDoS attack is a bundle flooding attack, in which countless apparently authentic TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) parcels are coordinated to a particular objective.

DDoS attacks can't be detected and stopped effectively because different techniques are used by an attacker to hide attack sources. Protection against these attacks is trying for mostly two reasons. To start with, the quantity of zombie machines engaged with a DDoS attack is exceptionally enormous and the double-dealing of these zombies spans over a huge geological region.

The volume of traffic sent by a solitary zombie may be little, yet the volume of aggregated traffic showing up at the victim host is overpowering. Second, zombies ordinarily spoof their IP addresses heavily influenced by the attacker, which makes it truly challenging to follow the attack traffic back even to zombies.

In this research article, an overview of DDoS attacks and various prevention and mitigation techniques for DDoS attacks along with their advantages and disadvantages is discussed.

DDoS ATTACK TYPES & EVOLUTION

Attackers keep on tracking down new components and techniques for deceiving defense systems, subsequently exploiting the available software for illicit purposes and making damage to service suppliers. As of late, arising technologies, for instance, the IoT, have been used to launch powerful and exceptionally effective DDoS attacks.

There are enormous attacks of DDoS which are over and over targeted at a few organizations like CNN, Amazon, Buy.com, and eBay. In 2010 and 2011, just about 2,500 organizations having 75,000 computer systems were affected by DDoS attacks in excess of 100 countries with 4 million computers being attacked. Every day, 7,000 DDoS attacks are launched.

The sizes of DDoS attacks have increased throughout the last decade. For instance, in 2012, a botnet-based DDoS attack flooded a gathering of US banks with up to 75 Gbps of malicious traffic, while in 2013, a not-for-profit organization named Spamhaus experienced a huge DDoS attack including 300 Gbps of traffic.

The number of attacks that are recorded in the primary quarter of 2013 was at 48.25Gbps, being 718% more than that of the earlier the year 2012. The largest number of DDoS attacks recorded increased by around 1,000% from 40 Gbps in 2008 to 400+ Gbps in 2013. All things considered, these sorts of attacks happen in very nearly 3,000 dailies.

In 2014, an Internet service supplier was attacked by a network time protocol that created traffic of up to 400 Gbps, which prompted it to become inaccessible to clients. A Survey did uncover that consistently DDoS attacks increase by 111%. Around 85% of attacks are mitigated by VeriSign network security in the final quarter of 2014.

In 2015, the volume of the attack recorded was around 500 Gbps, and it disrupted the entire ISP network in Kenya. In addition, in the principal quarter of 2016 BBC encountered a website attack of 602 Gbps DDoS.

In October 2016, the Mirai botnet attacked Dyn, a web application security organization, with up to 1.2 Tbps of malicious traffic. Further, a momentous DDoS attack happened in 2018, when GitHub encountered a colossal flood of around 1.35 Tbps of produced traffic.

Much more terrible, the 2020 reflection-based DDoS attack terminated at Amazon Web Services (AWS) purportedly arrived at 2.3Tbps. The fast ascent of the IoT joined with the famously helpless security of connected shrewd gadgets, made ready for the development of IoT botnets that energized probably the most powerful attacks ever, with rogue traffic rates surpassing 1Tbps.

With everything taken into account, DDoS has been giving organizations and governments a heads-up for over two decades, and it isn't facilitating the grip. In Q1 2020, the quantity of these strikes multiplied contrasted with Q4 2019 and implies that the danger is raising. The accompanying passages will feature huge achievements in the evolution of this cybercrime system to show you the higher perspective.

There are two sorts of DDoS attacks, which are known as vulnerability and flooding. Flooding attacks include the setting up of a multitude of zombies by an intruder to attack packets that are going towards their destination. This is pointed toward increasing the traffic to a sum that the victim and his/her system can't control, subsequently bringing about the crashing of the victim's system.

In light of the strategy for attack, flooding attacks have been named direct and indirect (through reflectors) DDoS. One more grouping given is that given by, who ordered these attacks in light of the protocol level that is affected; these authors arranged them as Net DDoS and App-DDoS flooding attacks.

HTTP Flood Attacks, Slow-and Low-Rate DDoS Attacks, Session Initiation Protocol, Reflector Attacks, Domain Name System Amplification Attacks, SYN Flooding Attacks, UDP Flooding Attacks, ICMP Flooding Attacks, and DHCP Flooding Attacks are some normal DDoS attack arrangements.

Having gone through decades of evolution, DDoS is currently being growingly harnessed in hybrid attacks that consolidate various techniques. Albeit sometimes these extortion endeavors are basically harmless, the use of DDoS as a scare component could be to the point of building organizations of money.

As of now, DDoS keeps on being a solid player in the cybercrime field, and organizations should add the appropriate defenses to their security condition in the event that they haven't as of now. The use of a web application firewall (WAF) and a confided in cloud-based threat mitigation service, for example, Akamai or Cloudflare can move forward the protection impressively.

Security analysts additionally suggest disregarding ransom demands in the event that evildoers threaten to thump an enterprise network offline if there should arise an occurrence of non-payment. Effective extortion urges attackers to support their unfairness. Besides, a significant number of these blackmail endeavors revolve around void threats that won't ever be satisfied.

DDoS ATTACK PROTECTION VULNERABILITIES

While researching the DDoS protection techniques, we found several limitations. Though these techniques are widely in usage, there are limitations to them. Below, we have put down all the limitations of DDoS attack prevention techniques that inspired us to offer a better solution **"A Proactive Measure To Stop DDoS Attacks,"** whose methodology is discussed in the next section.

Below are some of the limitations present in the current best techniques to protect DDoS attacks from happening:

- There is no automated way to detect DDoS attacks as soon as it gets dispatched from the attackers' side.
- No real-time exchange of threat information; filtering malicious traffic from genuine traffic is difficult.
- Due to the lack of a centralized DDoS prevention system, resource allocation & bandwidth conservation is a challenging task.
- Establishing a GRE tunnel for the data & information encapsulation is a costly measure to prevent DDoS attacks from happening.
- Improper compliance management
- Amplification of DDoS attacks cannot be prevented in an ongoing DDoS attack.
- No availability of a central platform where multiple data centers can come and form a community.
- Detection, Diversion, Filtering, and Analysis process/phases in DDoS protection techniques are weakly framed. Thus, it needs a complete holistic solution!
- Also, the current DDoS protection techniques lack granular control of the more agile response, seeing the complex and diverse DDoS attacks.
- Lack of a centralized advanced software system to protect data centers and online services hosted by them.
- Real-time monitoring, DDoS prevention system, resource allocation & bandwidth conservation is a challenging task.
- That's due to improper compliance management and legalization between data centers.
- Automatic detection systems are deployed but might raise a massive amount of false positives. Hence, there is a need for an advanced traffic monitoring and DDoS mitigation system!
- No availability of border protection against DDoS attacks
- Today, in protecting DDoS attacks, one needs too much manual protection; thus, a fully-automated software-based system is needed
- Many DDoS Mitigation solutions completely overlook small, low-threshold attacks. However, that too is a huge problem.

- During an attack web services face downtime. And in today's business model, being reliant is important for better business continuity.
- The consumption of memory, power, and manual resources increases the cost to protect DDoS from happening.

All these limitations and challenges can be overcome by architecting a hybrid solution that delivers a closed feedback loop between on-premises and cloud components, which allows for fine-tuned mitigation as well as granular reporting of attack details.

DDoS Protection at DATA CENTER Community Level

In the community-driven approach to protect against DDoS attacks, first, we need to establish a data center community. For example, we have 4 data centers (DC1, DC2, DC3, DC4) that have signed agreements upon any requirement to share the traffic load for business continuity.

All these data centers run on a firewall log analysis, AI-based alarming software that detects the DDoS attack in real-time, whenever a malicious traffic burst happens on the servers and IP addresses.

Now, take an example that 1 out of 15 IP Pools of DC1 gets traffic from the ISP (Internet Service Provider). A cybercriminal, cyber attacker, or hacker is sending the traffic to your particular IP in DC1 to interrupt the application, software, and services working online.

The DC1 can handle 1Gbps bandwidth traffic. The attackers start sending more traffic in real-time. However, when the incoming traffic crosses a pre-defined bandwidth threshold, the AI-based software system sends alarms to the data center managers.

In real-time let's suppose that the attacker sends 2Gbps bandwidth of traffic. The software system monitoring and managing the DC1 will identify it as load traffic, and categorize it as an unwanted abnormal traffic flow. Here, it means your IP is under attack and most probably the attack is DDoS!

The first phase in the community-driven DDoS Mitigation Technique is the **DETECTION** of extra traffic (the malicious, botnet-based traffic in real-time).

Here comes the importance of a secondary datacenter (DC 2) which can share bandwidth to handle large-scale volumetric traffic and is located in another location. Furthermore, the BGP routing is always on via ISP and active between DC 1 and DC 2.

As soon as DC 1 detects a DDOS attack, the software starts looking for another data center within the community of 4 data centers that are ready to share its bandwidth.

Therefore, DC1 can ask for a little bandwidth from another datacenter, suppose 500MB to shift the genuine traffic there such that the IP remains live. The software selects the DC2, and sends

the request to share the load traffic. And instantly the DC2 accepts the request because the DC2 is part of the community of 4 datacenters.

The second phase in the community-driven DDoS Mitigation Technique is the **ACTION** to be taken upon DDoS attack. DC 1 is the primary data center on which the attack was done. The first thing the software does for DC1 is to get the attacked IP Pool additionally routed through BGP (Border Gateway Protocol) with another DC to share the traffic load.

DC2 adds this IP Pool in the BGP Advertisement to the internet service provider. As a result, the **traffic DIVERSION** takes place from DC1 to DC2 based on the same IP Pool and clients reach the destination IP in this pool to the lowest distance DC as per routing table metric.

Now both DC1 and DC2 do the **traffic FILTERING** and weed out the malicious traffic. In this case, the attacker sends higher traffic now which is above the combined bandwidth capacity of DC1 and DC2.

The AI-software system first alerts the data center managers of DC2, then analyzes which data center to take next help. As a result, the DC2 sends the request to DC3 and starts sharing the traffic load with the DC3 also via BGP advertisement.

Since DC2 stopped the DDoS and blocked the malicious traffic, the system logs and analytics at the secondary data center can help gather information about the attack, both to identify the offender(s) and to improve future resilience. It is the **traffic ANALYSIS** part!

Lastly, if you remember, then the traffic originally came to DC1. Therefore, we have to reroute the filtered, genuine, and safe traffic back to DC1 from DC2 and DC3.

For this, a secure GRE Tunnel (Generic Routing Encapsulation, a kind of VPN active between DC1, DC2, and DC3) comes into use. With this tunnel, the **REROUTING of traffic** is done from DC3 to DC1, and also DC2 to DC1.

Data Center COMMUNITY PLATFORM

As I told you, I have 4 data centers in my contact, where I performed my previous practicals and lab experiments. But, they have a manual ROA (Route Origin Authorization)!

A ROA is a cryptographically signed object that states which Autonomous System (AS) is authorized to originate a particular IP address prefix or set of prefixes. ROAs may only be generated for Internet number resources covered by your resource certificate.

A ROA is composed of a ROA name, an AS number (ASN), a validity date range, and one or more IP Addresses that are to be shared between two data centers. This ROA certificate is authorized by the internet regional registries.

Also, ROA is signed only when two DCs are ready to do it. This created a problem, i.e., finding DCs for ROA is difficult. Thus, we need an online platform for this purpose. What if a website resolves this issue?

First, I want to make an online website, where multiple data centers can come, register, and sign ROAs with the other data centers as per their needs and feasibility.

In the user platform, a DC can register with a login ID/Password after filling necessary form fields like:

- Datacenter name and tier level
- Datacenter Geographical location
- Required compliance, inventory, resources, IP availability

After the data centers, successful registration, they first have to download software from the available link in their user panel. Once the download is done, the data center can access the platform and select from the list of other data centers and agree upon signing ROA from the 5 regional registries discussed above.

From then, the AI-based software will manage!

Now, if ever a DDoS attack happens, the software

- First will detect the incoming traffic in the real-time
- If the traffic crosses the threshold limit of the bandwidth capacity, the software will identify and alarm the attacked data center with the DDoS traffic.
- Now the software will automatically let you select the other data center with whom you have your agreements and ROA.
- Next, the best ROA signed DC will host the attacked IP.
- The software installed in both the data centers will manage and divert the traffic to the required DC.
- Malicious traffic is cleaned, the traffic is filtered, and rerouting the genuine traffic back to the attacked DC is done by the software.

Now, this whole process will be automatically based upon the downloaded software. And the data center managers just have to monitor the process. That entire process was discussed in the third 6-months report - “Mitigating Traffic Safely and Efficiently At Datacenter Levels; Protecting DDoS Attacks!”

In this software, we will have multiple data centers and ROAs among them. I believe such an online platform and software will be a revolutionary change in the IP routing facility, Load traffic sharing, and DDoS Mitigation methods that are my primary aims behind this Ph.D. research on “A Community-Driven Proactive Measure To Stop DDoS Attacks!”

CONCLUSION

Each data center can make reforms, rules, and regulations, and can decide their pricing to help each other at the time of need. One can implement the sync monitoring and managing system not only in a particular area but nationwide and globally.

Here, I have discussed only the 4 data centers, but in reality, such traffic diversion, filtering, and rerouting, while protecting against DDoS attacks can happen between multiple data centers. Furthermore, thousands of data centers globally can connect and become one community to not only stop DDoS but to stop other attacks too.

My research was about finishing the DDoS attack, mitigating it, transferring it back to the attacker, and finally protecting your ISP, Servers, GRE Tunnel, IP Addresses, VPNs, and clients who have their business-related services on your servers. This research article has presented just glimpses of it. Lastly, the importance of software automation in traffic channeling and IP routing is the key that helps protect against DDoS attacks

This can only be achieved if each country's IT cell, government & private data centers form a cybersecurity community to help out each other at the perilous times of DDoS attacks.

Hence, the solution which I had proposed is **A community Driven Approach!**

REFERENCES

1. DDoS Incidents and their Impact: A Review - By Monika Sachdeva, The International Arab Journal of Information Technology
2. A taxonomy of DDoS attack and DDoS defense mechanisms - Jelena Mirkovic , Peter Reiher (ACM SIGCOMM Computer Communication Review Volume 34Issue 2)
3. Measuring the Adoption of DDoS Protection Services - Mattijs Jonker, University of Twente | Anna Sperotto, University of Twente | Roland van Rijswijk-Deij, University of Twente
4. An approach to detect DDoS attack with A.I. - TowardsDataScience.com
5. A Review on DDoS Attack Prevention and Mitigation Techniques - By Deepika Mahajan Shaheed Bhagat Singh State Technical Campus, Ferozpur, Punjab, India | Monika Sachdeva Shaheed Bhagat Singh State Technical Campus, Ferozpur, Punjab, India
6. D. G. Andersen. Mayday: Distributed filtering for internet services | Usenix Symposium on Internet Technologies and Systems
7. H. Balakrishnan, M. F. Kaashoek, and R. Morris. Resilient Overlay Networks | In Proceedings of 18th ACM SOSP
8. T. Anderson, T. Roscoe, and D. Wetherall. Preventing internet denial-of-service with capabilities | In Proceedings of Hot Nets