Everything on DDoS Attacks, DDoS incidents & DDoS Defense Mechanisms!

[1]Naveen Sharma[2]Dr. Keshav Dev Gupta
Ph.D Scholar, Sr. Assistant Professor Computer Science & IT
APEX University, Jaipur

Corresponding Author
Naveen Sharma
Ph.D Scholar, APEX University, Jaipur

ABSTRACT
Distributed denial-of-service (DDoS) is a rapidly growing problem. DDoS attacks have suddenly gained popularity in the last 10 years. Furthermore, their intensity to attack has increased and now ranges from just a normal problem to a severe illegal cyber activity.
The increasing number of malicious attacks cause a great loss of revenue who become the targets of this. For the protection of these attacks from happening, there is a sudden rise in the market for DDoS Protection Service (DPS) providers from whom the victims can easily ask for help by using their traffic diversion systems and DDoS protection measures.
The multitude and variety of attacks and the defense system approaches are flooding. This article presents various classifications of attacks and defense mechanisms. The attack classification criteria done in this article describe the commonalities among them.
Furthermore, features of attack strategies, the challenges in protecting them, and ideating a new easy-to-go hassle-free system for DDoS attack protection is another daunting task.
In this research article, based on PH.D.topic "An Approach to Protect DDoS Attack" briefly describes the happening of different DDoS attacks, their mechanism of attack, types of different DDoS attacks, and some important methods being used in protecting DDoS attacks from happening.
After finding out the limitations/drawbacks and disadvantages in the current DDoS protection measures, we will detail you with the Hybrid Approach effective and efficient in protecting and mitigating DDoS attacks without eliminating IPs and continuing the flow of legitimate traffic at servers online.

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

In recent years, we have seen a huge increase in the class of malicious attacks, especially, Distributed Denial of Service attacks (DDoS). These can generate traffic volumes in the order of hundreds of Gbps. Recent attacks reached the capability of 600-1000Gbps.

If this wasn't enough, then the rise in on-demand DDoS attacks between businesses to businesses, companies to companies gained more popularity.
As a result, now DDoS attacks are happening on household electronic gadgets, smart devices, IoT-connected machines, and more. Attacks can be of any kind; for example, volumetric attacks (choking the target's bandwidth with malicious traffic) or semantic attacks (denying the access of minimal bandwidth impacts).

The protection of a specific application, or even an entire network, can be outsourced to a DDoS Protection Services. Protection can take place on-site, using dedicated appliances, or be handled in the cloud using advanced technologies where malicious traffic is filtered or absorbed, thus effectively blocking the attack.

Traffic diversion is the key mechanism that allows traffic to be routed through established infrastructure. The most efficient method is to use the Border Gateway Protocol (BGP) to divert traffic. It is done by many DPS (DDoS Protection Services) infrastructure. However, handling traffic diversion, analysis, filtering of genuine traffic, etc. if is done manually, then it will involve multiple risks and might weak your DDoS attack prevention.

Currently, several research papers, journal articles, scholarly online articles, blogs, etc. are on the path to analyzing DDoS attacks, their techniques, and new DDoS mitigation and protection measures. To stop DDoS and keep ourselves secure in every possible way, our idea is a comprehensive and easy-to-implement, i.e., - ***"Distributed Mitigation of Attack."***

This article briefly analyzes the security challenges in DDoS attacks and the development of a new DDoS attack mitigation technique. With the firm research and analysis, we have made a new powerful technique to mitigate DDoS attacks.

The amount of flexibility, easy network management, IP address management, ease of traffic, server management, etc. acts as a powerful tool for detecting, analyzing, filtering, rerouting traffic, and mitigating DDoS attacks.

Hence, by identifying *DDoS Attack Types, Defense Systems, and A Hybrid Solution For DDoS Attack Prevention*, stopping DDoS and other cyberattacks will be possible at a high-scale level. This research article is all about detailing all the above-introduced things!

OVERVIEW: DDoS Attack Types & Detection Mechanisms

There are many ways to commit a DDoS attack. Attackers follow one frequent approach, i.e., sending a stream of malicious traffic to a target. This stream takes on your key resources like IP, routers, servers, machines, etc., and makes them unavailable to the victim's legitimate customers and clients.

One more conceivable approach is to vandalize machines in a network. Usually, attackers start a DDoS attack by exploiting a device's vulnerability. The attacker's system turns into the DDoS expert and starts recognizing other weak systems to launch a massive attack.

The objective behind such attacks is to flood servers with malicious traffic and utilize their accessible internet, RAM, or CPU to disturb the bandwidth and servers.

Nowadays, cybercriminals use powerful DDoS attacks as shadow/disguised attacks and launch critical data and security breaches or ransomware attacks among them.

Home routers, mobile devices, laptops, digital assistants, smart security cameras, and other IoT devices infected with malware are extremely into usage for launching DDoS attacks too.

As a result, DDoS sometimes is a bluff to target another vulnerability. Below we have mentioned 33 types of modern DDoS attacks that happened previously or are happening today:

***32 Types of Modern DDoS Attacks**:*

Application-Level Attacks	Zero-Day (0day) DDoS	Ping Flood
IP Null Attack	CharGEN Flood	SNMP Flood
NTP Flood	SSDP Flood	Fragmented HTTP Flood
HTTP Flood	Single Session HTTP Flood	Single Request HTTP Flood
Recursive HTTP GET Flood	Random Recursive GET Flood	Multi-Vector Attacks
SYN Flood	SYN-ACK Flood	ACK & PUSH ACK Flood
ACK Fragmentation Flood	RST/FIN Flood	Synonymous IP Attack
Spoofed Session Flood	Session Attack	Misused Application Attack
UDP Flood	UDP Fragmentation Flood	DNS Flood
VoIP Flood	Media Data Flood	Direct UDP Flood
ICMP Flood	ICMP Fragmentation Flood	Amplified DDoS Attacks

"***Some More Famous DDoS Attacks:*** The 2007 Estonia Attack, The 2000 Mafiaboy attack, The 2013 Spamhaus Attack, The 2013 Spamhaus Attack, The 2015 GitHub Attack, The 2015 GitHub Attack, The 2016 Dyn Attack, The AWS DDoS Attack in 2020, The Mirai Dyn DDoS Attack in 2016, The Six Banks DDoS Attack in 2012, The GitHub Attack in 2018, Occupy Central, Hong Kong DDoS Attack in 2014, The CloudFlare DDoS Attack in 2014, and The Facebook DDoS Attack in 2021"

Best Techniques to Stop DDoS Attacks!

Den Mechanism To Prevent High Malicious Flood Of Traffic

The flood attack detection strategy employs an identity detection mechanism to block the traffic from a source beyond the threshold limit. The technique used is the UDP Flood Attack Detection technique. Due to the requirement of more energy, it can't block the DDoS attack entirely.

Preventing SMURF Attack By Increasing Bandwidth

Smurf attack minimization is achieved by simply reserving the bandwidth to reduce the attack percentage of incoming malicious unwanted traffic. The technique used is the Smurf DDOS Attack Detection technique. Due to the requirement of more bandwidth, blocking or mitigating the DDoS can fail, if TBs of malicious traffic coming to the server passing ISPs. Resource degradation and wastage must be tackled. This can be achieved by dividing the entire bandwidth into channels and blocking channels having malicious traffic.

SYN Flood Prevention Mechanism

Stopping this attack needs the approach of TCP connection and we can prevent attack by using a blocking-based strategy, where we block the malicious traffic before it reaches the website. The technique used is the SYN Flood DDOS Attack prevention technique. Estimating malicious traffic manually can go wrong; you must make a centralized threat detection system. Filtering strategy to pre-process the traffic could be used to reduce execution time for attack detection

Stopping Malicious Pings When They Are Transmitted To Servers

In this attack, multiple malicious pings are transmitted to the server to block the services provided by the server. Memory buffer overflow is a problem that is handled efficiently by putting a constraint on memory utilization through the request by a single client. The technique used is the Ping Of Attack Detection Strategy. In this, memory buffering can be a challenging task.Blocking contents to be stored within memory must be accompanied by compaction to increase the access rate.

Eliminating IPs To Prevent DDoS

This attack attacks the specific server and makes some specific services down while other ports are unaffected. This attack is detected and avoided by eliminating more than one connection from the client-side. The technique used is the Slowloris Detection & Prevention. The detection of VPN attacks of DDoS is challenging. Preemption in the resource allocation could solve the problem of slow loris.

More DDoS Attack Prevention Techniques:

- *Ingress Filtering:* A Router is set to drop traffic with an IP address that is not matched to the domain prefix.
- *Egress Filtering:* Makes certain that only assigned IP address space leaves the network. An outbound filter is used.
- *Route Based Distributed Packet Filtering:* Uses routing information. It works on basis that for every link on the internet, there is a limited number of source IP addresses from which traffic comes.
- *History-Based IP Filtering:* A pre-built IP address database is used and an edge router acknowledges the incoming packets accordingly.
- *Load Balancing:* Simple approach that enables network providers to increase the provided bandwidth on critical connections and prevent them from going down in the event of an attack.

- *Honeypot Technique:* Allow the attacker to attack the honeypot and not the actual system; they also help to gain info of the attacker by storing their records, the type of attack, and the type of software used.
- *Throttling Technique:* Traffic passing through the router to the source is rate limited to the throttle rate. Only aggressive flows which do not respect their rate shares are punished and not other flows. This method is still in the experimental stage.

BGP & GRE Usage in DDoS Attack Prevention

DDoS protection services use BGP to divert traffic. This requires the DPS to announce an IP subnet of its customer, such as a /24. All traffic destined for the customers is then routed to the DPS infrastructure for scrubbing.

After scrubbing, traffic is sent back to the customer's network using, e.g., a Generic Routing Encapsulation (GRE) tunnel. A (Border Gateway Protocol) BGP-based approach is typically used to protect entire networks, servers, and IP pools from an attack.

In this article, we have discussed all types of DDoS attacks, their numerous attack techniques, and their pros and cons. Due to an alarming increase in the rapidly happening DDoS attacks and internet security breaches, these attacks are now a more vulnerable issue.

Now, we have a detailed and clarified view / required knowledge about the attack, attacking mechanisms, the effective countermeasures to stop DDoS from happening, and the latest ongoing fight against these attacks. Now is the time, to find out the -

LIMITATION In DDoS PROTECTION TECHNIQUES!

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 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 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.

A HYBRID SOLUTION To Stop DDoS Attacks!

The hybrid approach is all about connecting different organizations like Data Centers and already existing cyber-security companies. In this approach, every company can continue its existing DDoS protection measure; however, a unique and centralized system is still necessary to stop DDoS attacks.

Here, we have designed software that is a combination of different systems such as Attack Detector, Firewall System, Log Analyzer, Traffic Manager, DDoS Mitigation System, integrated with AI and Data-based logics. All the organizations connected to each other run on this central DDoS attack protected system, which is basically an AI-based system.

This system detects the DDoS attack in real-time, whenever a malicious traffic burst happens on the servers and IP addresses. Among different organizations, if one gets a DDoS attack, the attack would interrupt the application, software, and services working online.

The software system monitoring and managing the organizations' network will identify the incoming malicious traffic as load traffic, and categorize it as an unwanted abnormal traffic flow that also includes legitimate traffic. If such traffic breaks in, then it is probably a *DDoS attack!*

Our DDoS Mitigation Technique is based on 4 different steps -

DETECTION: The attacker sends the malicious traffic along with the legitimate traffic. The AI system's first job is to detect unwanted traffic and alarm the other organizations in the network.

ACTION: In the meantime, the AI software will take the next step. Here, the other organizations will come and aid the attacked organization. A BGP (Border Gateway Protocol) route will be activated between both organizations. Upon activation, the attacked IP Pool is routed to another organization to share the traffic load.

DIVERSION: Now the software diverts the traffic from attacked organization to the helping organization. Furthermore, the detection is going on and the software weed out the malicious traffic.

ANALYSIS: If the attacker sends high traffic, which is above the bandwidth capacity, the next organization can come to help both organizations. The system logs and analytics at the second organization can help gather information about the attack, both to identify the offender(s) and to improve future resilience.

Lastly, a secure GRE (Generic Routing Encapsulation) is established between all the organizations, and **REROUTING** of genuine, legitimate traffic is done back to the attacked organization.

This research is all about finishing the DDoS attack, mitigating it, transferring it back to the hacker, and finally protecting your ISP, Servers, GRE Tunnel, IP Addresses, VPNs, and clients who have their websites on your servers.

This can only be achieved if each country's IT cell, government & private data center (s) form a cybersecurity community to help out each other at the perilous times of DDoS attacks. Hence, the solution is termed a ***Hybrid Approach!***

What Are The Features of Hybrid Solution?

Now, this whole process will be automatically based upon the downloaded AI software, which is centralized software. And the organization just has to monitor the process made up of logic, algorithms, programs, and codes.

In this software, we will have a network of multiple data centers, organizations, IT companies, internet security firms, and other industrial organizations. We believe such an online platform and software available will be revolutionary in the IP routing facility, Load traffic sharing, and DDoS Mitigation methods that are my primary aims.

The solution ***"Distributed Mitigation of Attack"*** against DDoS attack describes a system and infrastructure whose potential is to mitigate the attacks locally before the DDoS reaches the actual target. Instead of using the above previous methods, we should prefer to mitigate a DDoS attack with an intelligent system whose features are below:

Advanced Traffic Monitoring System

- Detects malicious traffic
- Filter malicious and genuine traffic
- Logs for analyzing traffic through the Firewall.
- Predicts, if there are again chances of malicious traffic attacks

Advanced GRE Tunnel System

- Use of multiple protocols over a single-protocol backbone
- Providing workarounds for networks
- Connection of non-contiguous subnetworks
- Being less resource-demanding than its alternatives (e.g. IPsec VPN)

Advanced DDoS Mitigation System

- No IP blocking
- Allowing affected data centers to use bandwidth capacities
- No website blocking and no website downtime
- Successful running of servers
- Protects other types of cyberattacks
- Preventing legitimate and innocent requests

The majority of commercial solutions provide threshold-based alerting mechanisms to collect meaningful information on the attack from the logs. Principal firms that provide solutions for DDoS mitigation to protect their structures from an attack are to identify normal conditions for network traffic defining «traffic patterns», this is necessary for threat detection and alerting.

CONCLUSION

The discussed DDoS protection and mitigation techniques and their limitations are now a known fact to us. Though their firewall systems and intrusion detection system works well, still these techniques are unable to defend networks from volumetric traffic attacks. The big stumbling barrier is that these attacks are unidentified. Furthermore, it is difficult to differentiate between genuine and illegitimate traffic.

Most of the proposed approaches require certain features to achieve peak performance and will perform quite differently if deployed in an environment where these requirements are not met.
Therefore we need to understand not only each existing DDoS defense approach but also how those approaches might be combined to effectively and completely solve the problem of DDoS attacks.

The potency of DDoS flooding attacks can impact your network, devices, and machine; therefore, analyzing and filtering the volume of traffic attacks is important. And the hybrid approach can help you to solve this via, ***"A Hybrid Approach to Protect and Mitigate the DDoS Attack!"***

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 given advice and for proofreading the article and letting me publish it.

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 ReviewVolume 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 HotNets