MINOR PROJECT REPORT

On

"Literature survey of different mitigation technique of DDoS attack"

Submitted in partial fulfilment of the requirements for the award of

Bachelor of Technology (B.Tech)

In the department of

Computer Science & Engineering

Submitted by:
Pragya Das (UG/02/BTCSE/2019/013)

Soumya Roy (UG/02/BTCSE/2019/014)

Deblin Ray (UG/02/BTCSE/2019/023)

Anindan Mondal (UG/02/BTCSE/2019/041)

Under the Guidance of

Mr. Sayantan Singha Roy

School of Engineering & Technology
ADAMAS University, Kolkata, West Bengal

CERTIFICATE

This is to certify that the Internship report entitled “Literature survey of different mitigation technique of DDoS attack”, submitted to the School of Engineering & Technology (SOET), **ADAMAS UNIVERSITY, KOLKATA** in partial fulfilment for the completion of internship of the degree of Bachelor of Technology in the department of Computer Science & Engineering, is a record of bonafide work carried out by Pragya Das (UG/02/BTCSE/2019/013), Soumya Roy (UG/02/BTCSE/2019/014), Deblin Ray (UG/02/BTCSE/2019/023)., Anindan Mondal (UG/02/BTCSE/2019/041), under our guidance.

All help received by us from various sources have been duly acknowledged.
No part of this report has been submitted elsewhere for award of any other degree.

Mr . Sayantan Singha Roy

_____

Guide Name
(Assistant Professor)

Dr. Pranav Kumar

_____

Internship Coordinator
(Assistant Professor)

Prof. (Dr.) Sajal Saha

_____

HOD CSE

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mentioning of the people whose constant guidance and encouragement made it possible. We take pleasure in presenting before you, our Internship, which is the result of a studied blend of both research and knowledge.

We express our earnest gratitude to our Mr. Sayantan Singha Roy (Guide designation), Department of CSE, for their constant support, encouragement and guidance. We are grateful for their cooperation and valuable suggestions.

Finally, we express our gratitude to all other members who are involved either directly or indirectly for the completion of this Internship.

DECLARATION

We, the undersigned, declare that the Internship entitled ‘Internship Topic, being submitted in partial fulfillment for the award of internship certificate in Bachelor of Engineering Degree in Computer Science & Engineering, affiliated to ADAMAS University, is the work carried out by us.

Pragya Das
(UG/02/BTCSE/2019/013)

Soumya Roy
(UG/02/BTCSE/2019/014)

Deblin Ray
(UG/02/BTCSE/2019/023)

Anindan Mondal
(UG/02/BTCSE/2019/041)

TABLE OF CONTENTS

ABSTRACT

DDoS attack[1] has been one of the most prominent security threats for the network servers throughout the world. These DDoS attacks are now happening at an unprecedented rate all over the world. Every existing server faces the probability of being attacked by someone sitting hundreds of kilometers away. The main reason these attacks are so effective is because of the difficulties in differentiating the attack traffic from regular traffic in the server. So by the time realization of the attack comes, the server has already been saturated with requests from the DDoS traffic. In our report we try to find the ways to mitigate these attacks that renders the servers useless from time to time. We have studied the different technologies used to mitigate these attacks and resolve the issue. These attacks can be brought under control through NFV and blockchain technologies. Multilevel frameworks can be created to mitigate the attacks and also Anycast has huge potential in mitigating the DDoS attacks. After going through various kinds of DDoS mitigation techniques, we can safely say that once the attack traffic has reached the server, it is impossible to get rid of the attack traffic without compromising the functionalities of the server with the current technologies. The server will shut down for a certain amount of time even with the help of the fastest mitigation techniques.

INTRODUCTION

1.1 Background

The DDoS attacks has possibly been the one of the biggest security issues in servers for quiet some time. The first known distributed denial of service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood. We dived into the techniques about how these attacks are being stopped. DDoS attacks has a wide variety so it is difficult to identify and mitigate. In 2022, network layer DDoS attacks increased by 109% YoY. Activity increased steadily from 731 attacks per day on average in April to 845 in may, to 1195 in June. June 20 and 21 were the most turbulent days with 1815 and 1735 attacks[2]. Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023[13]. DDoS Protection Services enable organizations to keep their applications/ websites available round the clock by monitoring traffic and preventing distributed denial of service attacks. DDoS Protection helps organizations to be well-equipped for the lurking threat of DDoS attacks[14].

1.2 Objective of the Internship

The purpose of this internship is to complete a literature survey on DDoS attacks on different network layers. The purpose is to find the optimal way to prevent these attacks. The goal was to study the various ways the DDoS attacks are dealt with after it has already reached the target server. The target was to find a technique that is able to separate and to get rid of the attack traffic as quickly as possible , so that the server does not lose its functionalities for a long amount of time. Making sure that the server is back and working at its full potential soon after a DDoS attack and thus making sure that the service provided by the server is mostly uninterrupted.

LITERATURE SURVEY

2.1 An Efficient system to stumble on and Mitigate DDoS attack in cloud Environment

- PROPOSED SYSTEM

K Manju Mohan et. al. [2] have proposed a system to mitigate DDoS attacks in cloud environment proposed framework plans to identify DDoS assault in cloud conditions. And furthermore to mitigate them. In the proposed method there are mainly two phases.

- In the first phase the IP address of the packet is captured using packet capturing tool such as wireshark
- The second phase is the classification phase. In this stage the ip address is contrasted with the generally prepared classifier with recognize whether it is a typical or a went after packet. If its a normal packet, sent to its objective else it is given to the avoidance stage.

In the proposed framework the first stage is putting away the records in a sql server and afterward information is disregarded the network between a few client frameworks and server machines. Then the technique is finished. SVM characterization technique is utilized for preparing and testing the information.
DDoS assault alleviation strategy additionally executed in this proposed work. In the proposed strategy the client getting to for the cloud to download a document the client needs to get a arbitrarily produced code from the owner of the file. For this the client needs to send a request to the owner. Assuming the owner does not allowed then the client can't get to it. The qualities are put away in scrambled structure. Consequently attack can be moderated.

2.2 A study on DDoS attacks, danger and its prevention

- PROPOSED SYSTEM

Chakaraborty S. et. al. [3] have proposed a system to mitigate DDoS attacks for ISPs. Based on the findings there are recommended measures to local ISPs to strengthen security against DDoS attack in an economical manner which include – Every single user who accesses router should be given a username and password. To make sure that RPF (ingress and egress filtering) on the interface of every static connection. To Disable Telnet on vtys and allow only SSH based connections use Vtys filters to prevent public routers from getting response from your router, use TACACS (Terminal Access Controller Access Control System) for password verification. Set up security labs if not possible set aside at least one spare router and server to try a new service instead of implementing it directly on live network. Minimizing the number of transit providers possibly one must Team up with other local ISPs for benefits like leasing a scrubbing centre, out of band management and possibly setting up better security labs.

2.3 DDoS Mitigation with Router

Deephi S. et. al. [4] have proposed a technique to mitigate DDoS attacks with Router. Controls the DDoS and DoS attacks by using the already existed devices which needs a few enhancements. Router, which is the fastest performance hardware, that plays an important role during the communication in network. Router mainly consists of the routing table which specifies packet flow between source and destination addresses along with hop count.
Consider Table 1. Adding the two more fields called as timer and counter to the already existed table

Table 1 Normal routing table

Source address	Destination address	Hop count
172.2.2.141	178.3.3.165	5
157.5.78.19	172.3.6.9	12
171.2.2.224	172.3.6.9	9

Adding the two more fields called as timer and counter to the already existed table and making the MAC address [9] as visible as in the Table 2

Table 2 Proposed routing table

Source address	Destination address	Hop count	MAC address	Timer In	Timer Out	Counter In	Counter Out
172.6.0.11	172.68.0.11	3	00:13:A9:02:01:FC	–	10	–	640
172.6.0.11	172.68.6.11	3	00:13:A9:02:01:FC	–	–	–	–
172.6.0.11	172.68.6.11	3	00:13:A9:02:01:FC	–	5	–	280

Using the TCAM [10] mechanism (fastest memory accessing) to trace the MAC address in the packet and compare with the routing table. So by matching the each packet address with stored MAC address in the routing table, the session hijacking can be identified. The routing table stores all the details up to a particular interval of time, later refreshes it. Between this refresh intervals time, the IP address of the system in the network will be maintained constant in the router. With the help of MAC address of the system, router checks whether it came from the IP address already stored or any new IP address with the same MAC address. Whenever a packet is spoofed, its IP address changes but the actual MAC address of the packet cannot be changed easily in case of using the proxies. Counter is used to count the number of data packets flowing through the network for a

particular interval of time and to limit the packet rate in the router whenever the data count reached the max limit, after that limit again the data count initiates from starting (zero). Here, the counter limit factor depends on the timer which is an increment timer or decrement timer. A particular time range is assigned to count the packets after it initiates from starting. Both the inflow and outflow should be considered separately. Whenever data counter reaches max value within time range, then automatically the flow of the packets is delayed for particular amount of time and the data packets are stored in the router buffer and then again they are sent to the receiver after time delay. DDoS attack actually happens if the network bandwidth is completely used by single host and not allowing the others to communicate. By making the delay in packets flow, the continuous usage can be avoided and by this others can communicate. The architecture that is used to perform the analysis and perform the delay of packets. Dynamic cache (counter value dependent) and the static cache (predefined addresses) used for comparison of packets in the network and they are forwarded to the delay component for temporary storage. Delay time should be very less then only the packets can reach the destination without any loss, if the delay of the packets is more than the TTL of the packet, causing the self-destruct of the packet.

Here, static cache is used analyze the packets (for IP address, MAC address) and compare with previously identified and stored IP addresses, MAC addresses of attackers in the history database. No need to use the constant time range values to count the packets in the dynamic cache, it may vary continuously satisfying required characteristics. So, here attacker may not able to guess the actual limit value. Based on these, packets are forwarded to the network or delay component. As proposed mechanism is applied in the router ,the attack can be identified on before it is entered into network. Here, each router stores the values independently, without the consideration of other routers. If all the routers present in the network use this mechanism, then the attack can be easily identified and controlled.

2.4 DDoS Attack Detection Method and Mitigation Using Pattern of the Flow

Sanmorino A. , Yazid S. et. al. [5] have proposed a technique to mitigate DDoS attacks using pattern of the flow . The solution is the utilization of flow patterns that are sent to server. In light of this flows pattern, we can decide whether a packet is coming from DDoS assaults. The pattern of flow entries is implemented on a router or switch that became a liaison between the botnet and server that become the target of the attack.

Pattern of a flow can be gained from the data extraction of every approaching flows. The data acquired from a stream, for example, source IP, source port, destination IP, destination port, tranfer protocol, flow size, and number of packets.

One of the flow sections patterns of DDoS attack is the size of the average number of packets per flow in a determined time span. By recognizing the flow entry pattern of the request sent by the ddos traffic we can recognize and mitigate the ddos attack.

The following stage is to drop packets that are coming from the attacker. This stage includes the support of firewall as a dealing with system. In the reproductions we utilized double layer firewall.

The first firewall design incorporates a majority of network layers. The layers send packets and packet data to the primary firewall engine, keep up with and pass packet setting to resulting layers, what's more, process the packets. The primary firewall engine analyzes the packet data to at least one introduced channels and returns an activity to the layers demonstrating how to treat the packet. So it can be ascertained that the packet was able to move on only it comes from the legitimate users.

2.5 Towards Mitigation of Low and Slow Application DDoS Attacks

Shtern M. et. al. [6] have proposed a system to mitigate DDoS attacks for Low and Slow application. This section proposes the solution architecture for mitigating LSDDoS attacks aimed at applications running on SDI.

A. LSDDoS Defense Reference Architecture

This provides a standardized blueprint for a system that will detect and mitigate LSDDoS threats.

- LSDDoS Detection Sensor: It detectzs the existence of an LSDDoS attack and to identify which subset of the traffic is malicious.
- Automation Controller: It provisions the Shark Tank and then redirects malicious traffic to it. The Automation Controller is also responsible for healing the application.
- Protected Application: The application that will be defended against LSDDoS attacks.
- Monitoring System: Collects performance metrics from all components • Shark Tank: It absorbs the damage from the DDoS attacks and allows the system to learn from these attacks for future reference.

B. Performance Model-Based Approach

One way of detecting the LSDDoS attack and mitigating its effect is to have a model of the application when no attack occurs (normal behaviour) and compare it with the application characteristics under attack(abnormal behaviour).

2.6 Mitigation using Nfv

- THE PROPOSED MITIGATION TECHNIQUE

Alharbi T. et. al. [7] In this paper a two-stage DDoS mitigation framework by leveraging NFV and SDN is proposed.
This framework consists of a traffic screening stage and a service stage. The traffic screener will analyse the traffic and determine what next-stage processes are needed for a traffic flow. Network-layer security, applicationlayer security, and/or certain network services are applied to a traffic flow according to the screening and analysis. The proposed DDoS mitigation scheme can be deployed in the organization's datacentre at the premises to reduce latency and achieve better privacy and security.

Screening mechanism

In some cases, the increase in incoming traffic is due to special events and seasons, and is not an abnormal flood. The traffic screener inspects the traffic using the algorithms and policies based on traffic pattern and packet features. It makes a decision whether a traffic flow is likely benign or malicious, and generates the outputs . In case of malicious flood, the traffic screener requests instantiation of the required network and/or application layer VSF from the orchestrator. However, if the high volume of the incoming traffic is due to legitimate requests, the traffic screener requests an increase in the capacity of the needed VNF such as DNS server or other functions to handle the traffic.

Resource allocation

To adapt to the changing demand for computing, storage, and bandwidth resources, the resource allocation module will specify the needed resources for any VNF, any VSF, and the traffic screener. Before the traffic screener sends an instantiation request of any virtualized function to the orchestrator, the resource allocation algorithm is invoked to determine the allocated resources based on the demand and availability. If more resources are needed for a VNF or VSF, the resource allocation module will work with the orchestrator to scale up the resource for the virtualized function or generate another instance.

2.7 Anycast and its potential for DDoS mitigation

 PROPOSED TECHNIQUES

De Vries B. W. et. al. [8] have proposed a system to mitigate DDoS attacks using Anycast to configure multiple sever with same IP address. With this we can confine the attack to a limited area. So the server might be unavailable to a fraction of its users, rather than becoming totally unavailable.
IP any cast reduces data redundancy. and provides high availability. It is widely used in DNS and CDN.
As there are multiple server with same If there's no single point of failure. So Anycast is effective against DDoS attack, as it cannot shut down whole server at once.
For example on november 2015, the DNS root servers received so many requests that it saturated some of their network connection, but it was.
limited as 11 out of 13 root name servers are Anycasted.
The goal is to optimize the Anycast But in a way where nee have maximum security against DDoS attack.
The approach will be focused on talking with operators, to understand their procedure to make an optimized, tailor made system for them.
An experimental anycast- testbed will be deployed, comparable to PEERING. It will announce and withdraw IP prefixes.
RIPE Atlast framework will be used to perform active measurements.
Passive measurement data will be provided by BGPmon and RIPE'S RIS. With the obtained data we attempt to find ways of optimizing the placement of the nodes.
Sources of DDoS attacks will be analyzed to see if it is coming from a certain area , it will further assist the optimization of the anycast catchment. Sleeping / inactive instances may be added, which will be activated in case of a DDoS attack.

2.8 Multilevel DDoS mitigation framework in IIOT devices

Yan Q. , Huang W. et. al. [10] have proposed a system to mitigate DDoS attacks using multilevel framework to safeguard IIOT devices from a security threats posed by these attacks.
Fog computing level:

It consists of IMCU. IMCD is cluster of SDN controllers and application. Frenetic Language is used to achieve security task. Security functions are programmed in the SDN application plane.
North bound and southbound APIs are used.

DDoS Attack are depended in three phases:

• collect -detect- mitigate (CDM):

collects data in the IMCD management range. IMCD collects traffic data through s flow on net flow. The data will be analyzed in real time and based on analysis and predefined policy an attack will be mitigated.

•honeypot-detect-react (HDR):
Finds out about what techniques are being used by the attackers. It helps capture malware, exploits and catches security breaches.
IMCU can direct the honeypot using SDN.

• cloud- detect- fog- mitigate (CDFM):
A co-operation between edge, fog and cloud computing level . Detecting an attack is easier near to the victim and stopping is easier close to the attacker. With powerful data analysis ability of cloud, doing real time analysis is possible.

Cloud computing Level:

It provides high computing power . It is highly scalable. DDoS detection and mitigation system framework (DDMF) can be used through cloud to handle big data. Because of high processing power neural networks and deep learning algorithms can be used to detect DDoS attack at this level.

DETAIL REPORT ON DDoS MITIGATION USING IP-ANYCASTING

3.1 IP-ANYCAST

- IP-anycast is a type of IP addressing in which a single IP address can be accessed from multiple Internet locations and refers to multiple distinct hosts. as opposed to the usual unicast IP addresses, which are associated with just one host. An anycast site or instance is a place where the anycast IP address can be accessed. It can be one server or a group of servers. The global routing system, Border Gateway Protocol (BGP), determines which topologically closest instance is presented to users who attempt to reach the anycast IP address.
- Anycast catchment for a service is largely dependent on the operation of BGP, which determines which instance traffic from each network reaches. Based on a shortest path calculation, BGP moves traffic from one network, an autonomous system in BGP terms, to its destination.
- The main benefit is reduced latency due to traffic localization, but this is not provided automatically and requires careful configuration and planning. Due to the replication of the service, IP-anycast also offers the advantages of scalability and resilience.
- The domain name system (DNS) is one application of IP-anycast. Because it is stateless and typically only requires a single request message and a response, the DNS protocol is ideal. Twelve of the 13 root DNS operators, which are named after the letters A-M, employ IP-anycast.

3.2 CATCHMENT MEASUREMENT

- The methods to determine the catchment of an anycast service can be roughly divided in two categories:

    1. Passive Measurements:
       Passive methods register all source IP-addresses reaching each site at the site itself. This results in the catchment among all IP addresses that connected to the anycast service and is almost always incomplete or biased towards the user population of the anycast service.
    2. Active Measurements:
       Active methods use some kind of vantage points (VPs) to actively send some message to the anycast prefix and infer the anycast site reached from the response.

- Another method to measure the catchment of an anycast service is by sending ICMP echo request with anycast prefix as the source and listening for the responses on the anycast instances.

3.3 CONTROLING CATCHMENT

With BGP, anycast operators have few options for influencing the capture of anycast instances. Choosing the upstream AS and entering into peering agreements can have an impact on the catchment. or by artificially lengthening the path to a particular instance using, for instance, AS-path prepending. However, due to their trial-and-error nature, these strategies frequently result in unanticipated outcomes.
We map the attack traffic on anycast instances to determine the impact of a DDoS attack on a specific anycast deployment configuration. Each instance's catchment, which maps a significant portion of the IPv4 address space to instances, is combined.

3.4 ANYCAST TESTBED

Utilizing ICMP Echo requests and responses, or "ping," the testbed is able to determine the catchment of each of its instances. The anycast prefix will be used as the source IP address each time one of the instances sends an ICMP Echo request to a particular IP address. BGP will route the response to the "closest" anycast instance and address it to the anycast prefix. The ICMP Echo response will be sent to the instance that is closest, and the source IP address of the response will be determined to belong to this instance's catchment.

3.5 MEASUREMENTS

The measurements aim to determine the most effective AS-path prepending mitigation strategies for various DDoS attack combinations and anycast deployment scenarios. We evaluate the effects of various AS path-prepending strategies for each combination, select those that have a positive effect, and possibly refine them.

3.6 ANYCAST DEPLOYMENTS

The following properties are taken into consideration when defining anycast deployments: the anycast service's objectives and guidelines, the number of anycast sites, and each site's capacity.
For anycast services, we define two types of policies:

1. Maximum accessibility for everyone, with no discrimination against users, and the service ought to be made available to as many people as possible
2. Minimum required performance, or a certain level of performance, is valued more than user accessibility.

- This study's DDoS attacks are captured by services known as Booter or Stresser . Without requiring any technical expertise in DDoS attacks, these DDoS for hire services can carry out massive DDoS attacks.
- The testbed's total number of anycast sites can only support so many instances. The DDoS attacks, on the other hand, are not actually carried out against the testbed; rather, they are simulated using the mapping of source IP addresses on the anycast testbed's catchment.

CONCLUSION

Through this project, we have found out the ways to mitigate DDoS attacks on different network layers. We have learned about various different technologies that are applied to stop these attacks. We have found out how difficult it is to identify the attack traffic from regular traffic, making these attacks lot more lethal than they should be. The mitigation techniques come into action only after the attack has happened. So it means the attack has done some damage to the target server, exposing the security threats that these attacks possesses.

So the mitigation techniques only come into effect after the server has lost some of its functionalities[3]. It means mitigation techniques, even though very useful are not enough to completely dispel the threat that are DDoS attacks.

REFERENCE

1. DDoS mitigation - Wikipedia. (2022). Retrieved 15 October 2022, from https://en.wikipedia.org/wiki/DDoS_mitigation

2. Yoachimik, O. (2022) DDoS attack trends for 2022 Q2, The Cloudflare Blog. The Cloudflare Blog. Available at https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2 (Accessed: October 15, 2022).

3. Is it possible to prevent DDoS attacks?. (2022). Retrieved 15 October 2022, from https://www.techtarget.com/searchsecurity/answer/Is-it-possible-to-prevent-DDoS-attacks

4. https://www.researchgate.net/publication/338670829_DoS_and_DDoS_Attacks_at_ OSI_Layers - Obaid, Hadeel & Abeed, Esamaddin. (2020). DoS and DDoS Attacks at OSI Layers. 1-9. 10.5281/zenodo.3610833.

5. https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends__ebook.pdf – Accessed on 11th oct, 22 at 8:30 pm

6. https://ieeexplore.ieee.org/document/8291111 - Yan, Q., Huang, W., Luo, X., Gong, Q., & Yu, F. (2018). A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things. IEEE Communications Magazine, 56(2), 30-36. doi: 10.1109/mcom.2018.1700621

7. https://ieeexplore.ieee.org/abstract/document/6550471 - Huang, V., Huang, R., & Ming Chiang. (2013). A DDoS Mitigation System with Multi-stage Detection and Text-Based Turing Testing in Cloud Computing. 2013 27Th International Conference On Advanced Information Networking And Applications Workshops. doi: 10.1109/waina.2013.94

8. https://ieeexplore.ieee.org/document/9369635 - Yaegashi, R., Hisano, D., & Nakayama, Y. (2021). Light-Weight DDoS Mitigation at Network Edge with Limited Resources. 2021 IEEE 18Th Annual Consumer Communications &Amp; Networking Conference (CCNC). doi: 10.1109/ccnc49032.2021.9369635

9. https://ieeexplore.ieee.org/document/7868480 - Alharbi, T., Aljuhani, A., & Hang Liu. (2017). Holistic DDoS mitigation using NFV. *2017* IEEE 7Th Annual Computing And Communication Workshop And Conference (CCWC). doi: 10.1109/ccwc.2017.7868480

10. https://link.springer.com/chapter/10.1007/978-81-322-2012-1_75 - Deepthi, S., Hemanth, K., Rajesh, D., & Kalyani, M. (2014). A Novel Approach for DDoS Mitigation with Router. Advances In Intelligent Systems And Computing, 701-707. doi: 10.1007/978-81-322-2012-1_75

11. https://link.springer.com/chapter/10.1007/978-3-319-39814-3_16 - de Vries, W., Schmidt, R., & Pras, A. (2016). Anycast and Its Potential for DDoS Mitigation. Management And Security In The Age Of Hyperconnectivity, 147-151. doi: 10.1007/978-3-319-39814-3_16

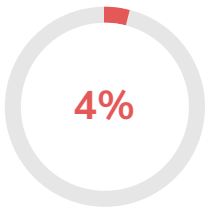
12. https://ieeexplore.ieee.org/abstract/document/6574541 - Sanmorino, A., & Yazid, S. (2013). DDoS Attack detection method and mitigation using pattern of the flow. *2013* International Conference Of Information And Communication Technology (Icoict). doi: 10.1109/icoict.2013.6574541

13. Five most famous ddos attacks and then some (2022) A10 Networks. Available at: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=A%20Brief%20History%20of%20DDoS,become%20a%20classic%20DDoS%20 attack (Accessed: October 15, 2022).

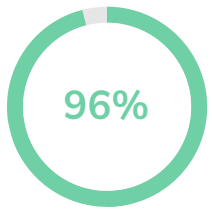
14. Top reasons that DDoS protection services is more crucial than ever (2022) Indusface. Available at: https://www.indusface.com/blog/top-reasons-that-ddos-protection-services-is-more-crucial-than-ever/? amp (Accessed: October 15, 2022).

Plagiarism Scan Report

Report Generated on: Jan 05,2023



Plagiarised



Unique

Total Words:	**826**
Total Characters:	**5130**
Plagiarized Sentences:	**1.88**
Unique Sentences:	**45.12 (96%)**

Content Checked for Plagiarism

De Vries B. W. et. al. [8] have proposed a system to mitigate DDoS attacks using Anycast to configure multiple sever with same IP address. With this we can confine the attack to a limited area. So the server might be unavailable to a fraction of its users, rather than becoming totally unavailable.
IP any cast reduces data redundancy. and provides high availability. It is widely used in DNS and CDN.
As there are multiple server with same If there's no single point of failure. So Anycast is effective against DDoS attack, as it cannot shut down whole server at once.
For example on november 2015, the DNS root servers received so many requests that it saturated some of their network connection, but it was.
limited as 11 out of 13 root name servers are Anycasted.
The goal is to optimize the Anycast But in a way where nee have maximum security against DDoS attack.
The approach will be focused on talking with operators, to understand their procedure to make an optimized, tailor made system for them.
An experimental anycast- testbed will be deployed, comparable to PEERING. It will announce and withdraw IP prefixes.
RIPE Atlast framework will be used to perform active measurements.
Passive measurement data will be provided by BGPmon and RIPE'S RIS. With the obtained data we attempt to find ways of optimizing the placement of the nodes.
Sources of DDoS attacks will be analyzed to see if it is coming from a certain area , it will further assist the optimization of the anycast catchment. Sleeping / inactive instances may be added, which will be activated in case of a DDoS attack.

Yan Q. , Huang W. et. al. [10] have proposed a system to mitigate DDoS attacks using multilevel framework to safeguard IIOT devices from a security threats posed by these attacks.
Fog computing level:

It consists of IMCU. IMCD is cluster of SDN controllers and application. Frenetic Language is used to achieve security task. Security functions are programmed in the SDN application plane.
North bound and southbound APIs are used.

DDoS Attack are depended in three phases:

• collect -detect- mitigate (CDM):

collects data in the IMCD management range. IMCD collects traffic data through s flow on net flow. The data will be analyzed in real time and based on analysis and predefined policy an attack will be mitigated.

•honeypot-detect-react (HDR):
Finds out about what techniques are being used by the attackers. It helps capture malware, exploits and catches security breaches.
IMCU can direct the honeypot using SDN.

• cloud- detect- fog- mitigate (CDFM):
A co-operation between edge, fog and cloud computing level . Detecting an attack is easier near to the victim and stopping is easier close to the attacker. With powerful data analysis ability of cloud, doing real time analysis is possible.

Cloud computing Level:

It provides high computing power . It is highly scalable. DDoS detection and mitigation system framework (DDMF) can be used through cloud to handle big data. Because of high processing power neural networks and deep learning algorithms can be used to detect DDoS attack at this level.
Alharbi T. et. al. [7] In this paper a two-stage DDoS mitigation framework by leveraging NFV and SDN is proposed.
This framework consists of a traffic screening stage and a service stage. The traffic screener will analyse the traffic and determine what next-stage processes are needed for a traffic flow. Network-layer security, applicationlayer security, and/or certain network services are applied to a traffic flow according to the screening and analysis. The proposed DDoS mitigation scheme can be deployed in the organization's datacentre at the premises to reduce latency and achieve better privacy and security.
In some cases, the increase in incoming traffic is due to special events and seasons, and is not an abnormal flood. The traffic screener inspects the traffic using the algorithms and policies based on traffic pattern and packet features. It makes a decision whether a traffic flow is likely benign or malicious, and generates the outputs . In case of malicious flood, the traffic screener requests instantiation of the required network and/or application layer VSF from the orchestrator. However, if the high volume of the incoming traffic is due to legitimate requests, the traffic screener requests an increase in the capacity of the needed VNF such as DNS server or other functions to handle the traffic.

Resource allocation

To adapt to the changing demand for computing, storage, and bandwidth resources, the resource allocation module will specify the needed resources for any VNF, any VSF, and the traffic screener. Before the traffic screener sends an instantiation request of any virtualized function to the orchestrator, the resource allocation algorithm is invoked to determine the allocated resources based on the demand and availability. If more resources are needed for a VNF or VSF, the resource allocation module will work with the orchestrator to scale up the resource for the virtualized function or generate another instance.