iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58025

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Deciphering the Surge: A Focused Review of Flooding Attacks and Proactive Defense Mechanisms using Anomaly-Based Detection Strategies

Aparna Khare[1], Pradnya Kashikar[2]
[1]*National Informatics Centre, Ministry of Electronics & IT, Government of India, India*
[2]*Birla Institute of Technology, Pilani, India*

Abstract: ***Flooding attacks, a taxonomical classification of the denial-of-service attacks, are a brute force attempt of overloading and incapacitating the target by consuming the entirety of the bandwidth reserved for ensuring availability. Over the years, flooding attacks have evolved, in both mode of delivery as well as attack surface parameters. Today, they pose a very serious threat to critical infrastructure and services across the globe. This paper presents a concise and focused review of flooding attacks, their expanse on the global cyber landscape alongside some recent case studies and security mechanisms adopted by industry as standards to tackle with them, followed by a review of the detection strategies using anomaly techniques for a proactive defense and the challenges faced.***

Keywords: ***flooding attacks, volumetric attacks, denial-of-service attacks, attack detection, anomaly techniques for detection, anomaly-based intrusion detection.***

I. INTRODUCTION

The cyber landscape today is encountering flooding attacks of unprecedented volume. The sheer bandwidth of these attacks can overload very robust infrastructures and this strength in the attacks is attributed to several factors, primarily being the distributed nature of these attacks. Critical infrastructures, businesses and services that cater to a large population, need to be able to detect a flooding attack from a genuine surge in peak consumption. Given flooding attacks are launched with an intent of incapacitating the bandwidth with no direct goal of accessing a service, anomaly techniques have been utilized to detect and diffuse any such malicious attacks. In the coming sections, a brief review of the cyber threat landscape in the current context shall be discussed to bring forth the types of mechanisms that have been used and their effectiveness. The review will then focus on the detection techniques that use anomaly detection to handle distributed flooding attacks in the current scenario.

II. CURRENT THREAT LANDSCAPE WITH RESPECT TO DENIAL-OF-SERVICE ATTACKS

Denial-of-service attacks have grown and evolved over decades; and in that duration, they have exploited various vulnerabilities in a number of ways. Distributed Denial-of-Service (DDoS) attacks though comparatively newer, have grown nefarious in multiple forms. The first documented large-scale DDoS attack occurred in August 17, 1999, when Trinoo[1], a DDoS tool was deployed in at least 227 systems (114 of which were on Internet sites) to flood a single University of Minnesota system that swamped the target network and rendered it unusable for more than two days [1]. Trinoo consisted of a network of compromised machines called “Masters” and “Daemons,” allowing an attacker to send a DoS instruction to a few Masters, which then forwarded instructions to the hundreds of daemons to commence a UDP flood against the target IP address. CERT Incident Notes from 1999 recorded these attacks [2].

On February 8, 2000, Yahoo.com suffered a three-hour flood from a distributed denial-of- service (DDoS) attack and lost its capacity to serve Web pages to visitors. The next day, the same technique was extended to Amazon.com, eBay.com, Buy.com, and CNN.com. Investigations located a fifteen-year-old child named Michael Calce, a high school student from Quebec, who was found responsible for the series of highly publicized denial-of-service attacks [3].

[1] Trinoo or trin00 is a distributed tool that was used to launch coordinated UDP flood denial of service attacks.

©IJRASET: All Rights are Reserved

A very significant DDoS attack that probably had the highest impact, occurred on October 21, 2002, when all the thirteen Internet Domain Name System's root name servers[2] sustained a distributed denial of service attack, all of them targeted simultaneously. Attack volume was approximately 50 to 100 Mbits/sec (100 to 200 Kpkts/sec) per root name server, yielding a total attack volume was approximately 900 Mbits/sec (1.8 Mpkts/sec) [4]. The attack lasted for over an hour.

While over the years, DDoS attacks have continued to hit in various forms including amplification attacks and reflection attacks, the era brought upon by the global covid-19 pandemic has changed the scenario even more drastically. It was reported that the year 2021 saw 9.7 million DDoS attacks in total, that was a 14% increase from 2019 [5]. The largest attack for 2021 was reported to be targeted at a German ISP reaching up to 1.5 Tbps[3].

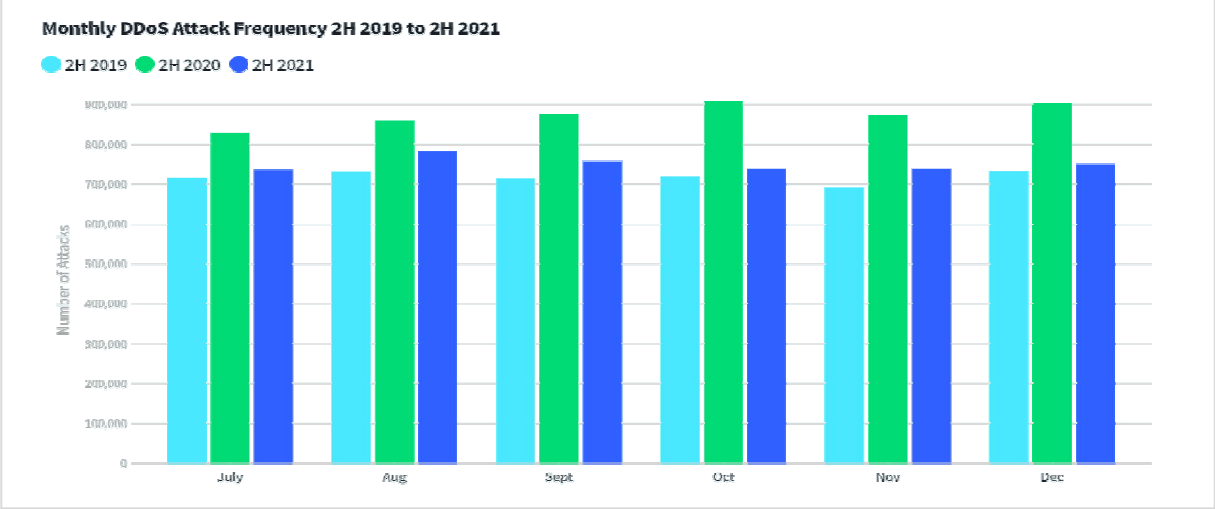


Fig. 1 Monthly DDoS Attack Frequency from second half of 2019 to second half of 2021. Source: Netscout [5]

A. Recent Case Studies

The year 2022, with the international conflict between Russia and Ukraine, that had been brewing over the years, brought forth another unprecedented methodology of war and cyberwarfare. Starting February 13, 2022, multiple direct-path (non-spoofed) SYN-flooding and UDP-flooding DDoS attacks were reported, targeting several governmental, military, and financial organizations within Ukraine on their public-facing Web sites, applications, and ancillary supporting infrastructure [6] [7]. These were identified as a targeted, orchestrated DDoS attack campaign. Observed SYN-flood attack throughput reached a maximum of ~1.2 mpps[4], while large- packet UDP flooding attacks reached a maximum of ~5.3 Gbps. By way of comparison, the largest DDoS attacks reported in 2021 were ~674 Mpps and 3.47 Tbps, respectively [6]. It was notably observed that direct-path DDoS attacks prevailed in the attacks targeting Ukraine.

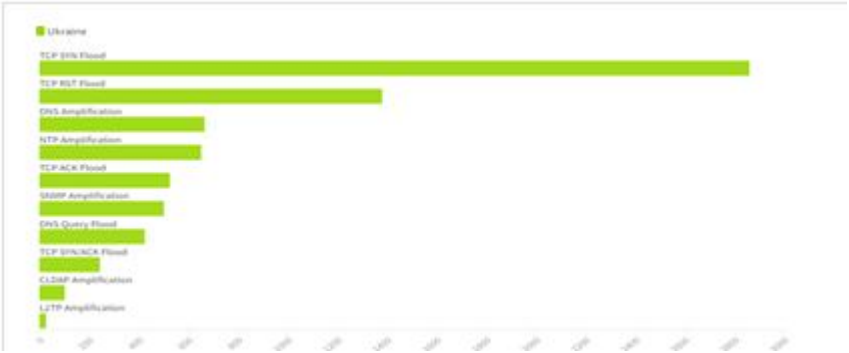


Fig. 2 Attack vectors observed in DDoS attacks against Ukraine [8]

[2] The root name servers are critical infrastructure components of the Internet, mapping domain names to IP addresses and other resource record (RR) data. Attacks against the root name servers could, in theory, impact operation of the entire global Domain Name System, and thus all Internet services that use the global DNS, rather than just specific websites.
[3] Terabits per second
[4] million packets-per-second

These attacks disrupted various online government services, banking applications and other financial services. Mirai[5] botnet was employed in most attacks that targeted government services, banks and financial institutions [9].



Fig. 3 Reported DDoS analysis data by Kentik Inc, showing simultaneous DDoS attacks against the websites of Ukraine's parliament, foreign ministry, and executive cabinet [10].

The majority of the flooding attacks were botnet based and involved five different types of botnets (mirai, gafgyt, ircbot, ripprbot, moobot) [9]. It was also noted that among the DDoS attacks that were targeted at Ukraine during the period, a vast majority of the attacks appeared to be sourced from publicly available DDoS-for-hire[6] services [11].

Soon after the DDoS attacks on Ukraine were reported, a second surge of attacks focused on targets in Russia were also observed, a big share of which also appeared to be sourced from publicly available DDoS-for-hire services. These attacks featured peak attack volumes of 454 Gbps and 173 mpps, respectively [12]. It was also noted that flooding attacks formed a major part of these targeted attacks.

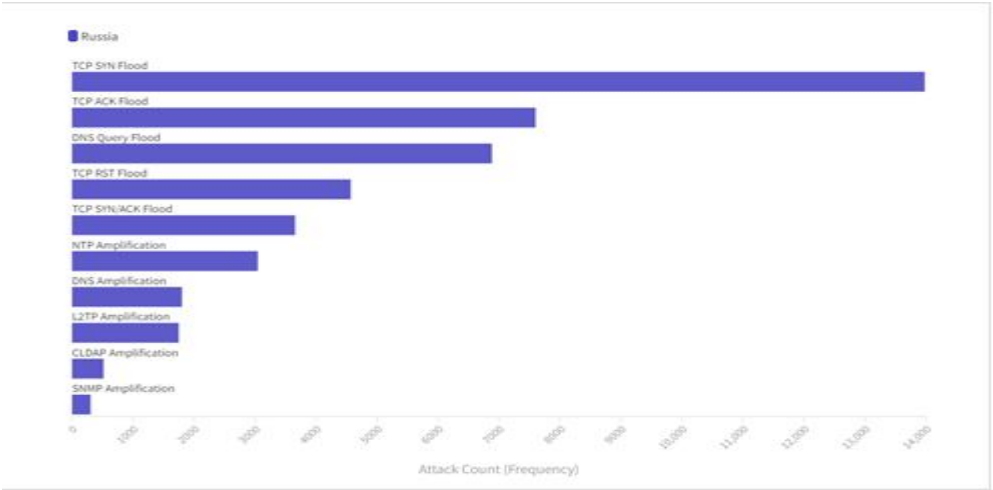


Fig. 4 DDoS attack vectors observed in DDoS attacks against Russia reported by Netscout [12]

[5] Mirai is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.
[6] DDoS-for-hire is a service that allows anybody to perform a DDoS attack for a price.

B. Attack Motivations

While the motivations for attackers to launch DDoS attacks have always been along the similar lines of any malicious actor, the current cyber threat landscape has witnessed a large number of attacks influenced by global crisis and conflicts. It has become a weapon in the hands of malicious actors with motivations ranging from extortion to cyber warfare. The big attacks are now seen as highly targeted, backed with DDoS attack services for hire as well as an immensely powered army of botnets [5].

Financial/economical gain, revenge, ideological beliefs, intellectual challenge, and cyber warfare form a broad categorization of the motivations for launching DDoS attack by a malicious actor. [13]. And by far, financial gain/profit has been a significant motive in most attacks against enterprises in 2018 [14].

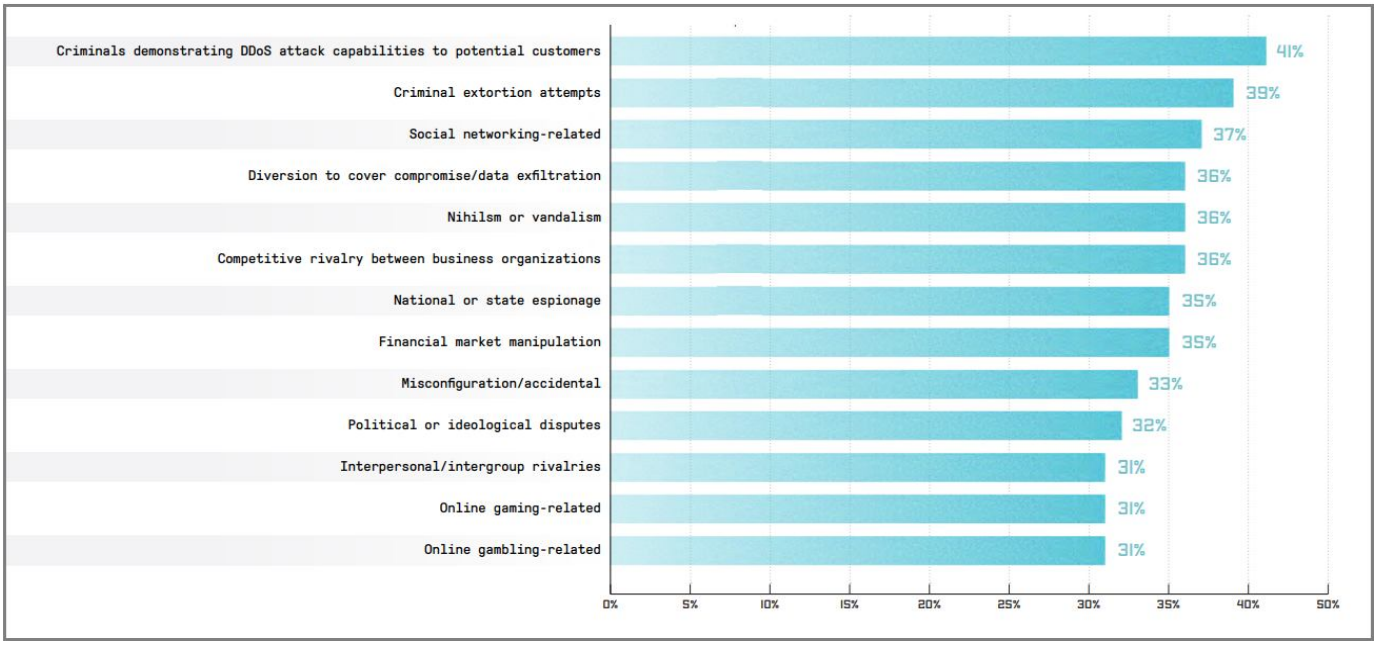


Fig. 5 DDoS Attack Motivations against enterprises in 2018 [14]

However, research from Kaspersky Lab and B2B International have also pointed out that often cyber criminals use DDoS attacks as smokescreen while hackers sneak in through other channels. Furthermore, a DDoS attack has often been found to be an integral part of the cyberattack kill-chain, wherein an adversary customizes the attack by including multiple tactics, techniques and procedures and executes them in multiple phases as a part of the attack strategy.

C. Modern-day Attack Vectors for Distributed Denial-of-Service (DDoS) Attacks

On the basis of prevalence, three broad categories can be identified forming the modern- day DDoS attack vectors, prominent in use. A majority of DDoS attacks observed today are a varied combination of volumetric, TCP state exhaustion and application layer attack vectors.

III. DECIPHERING FLOODING ATTACKS

While intuitively the prime goal of flooding attack seems to be denying the legitimate users of a service, volumetric attacks, also called as flooding attacks have been widely used to disrupt with an intention to either create a diversion or masquerade other attacks. Simply put, flooding attacks are loads of redundant network traffic sent over a small duration of time targeted at a service with an intent to harm.

A. Common Flooding Attacks

Some of the most common types of flooding attacks are as below:

1) *UDP Flood:* In this attack, the target is flooded with User Datagram Protocol (UDP) packets with the goal to flood random ports on that target host. The host attempts to look for applications that may be associated with the datagrams, but since the requests are spurious, it eventually sends a “Destination Unreachable” packet to the sender. This leaves the host overwhelmed and eventually unresponsive.

2) *ICMP Flood:* In this attack, the target is flooded with Internet Control Message Protocol (ICMP) echo- requests (pings). This eventually strains both the incoming and outgoing channels of the network since the targeted host will attempt to send back reply messages to the spurious ping echo requests.
3) *SYN Flood:* The Transmission Control Protocol (TCP) uses a three-way handshake (SYN, SYN-ACK, and ACK[7]) when initiating connection. A SYN Flood attack exploits this connection sequence, wherein a flood of SYN requests is sent to the target, but the attacking nodes do not respond to the SYN-ACK. This eventually ties up the target hosts waiting for response ACK which never comes.
4) *HTTP Flood:* In this attack, the target is flooded with legitimately looking (Hyper Text Transfer Protocol) HTTP GET or POST requests thus saturating the server with requests.
5) *IP/ICMP[8] Fragmentation:* In this attack, datagram fragmentation mechanisms are employed to overwhelm the network. When an IP/ICMP packet is too large, it has to be divided into smaller fragments in order to be transmitted successfully. A malicious attacker can exploit IP/ICMP fragmentation to target hosts by bombarding them with spurious fragments that cannot be fragmented. This causes the target host to eventually exhaust memory resources while it waits for more fragments to successfully reassemble.
6) *Reflection Amplification:* In this attack, attackers utilize techniques to both magnify the amount of malicious traffic they can generate and obscure the identity of the sources from which the actual attack is generated. These attacks usually exploit DNS, NTP, SNMP, SSDP, and other UDP/TCP-based services.

While flooding attacks date back to more than two decades, SYN-flooding being the most popular vector for attack from 1996 to 2018 [5], Direct-path DDoS attacks in the form of direct flooding attacks have continued to make their mark known, despite the rise in reflection[9] and amplification[10] attacks.

B. Flooding Attacks as a Threat

Intuitively, flooding attacks utilize the inherent design of the Internet, wherein the intermediate network is supposed to provide the bare minimum, best-effort packet forwarding service and the sender and receiver are supposed to handle the deployment of advanced protocols to achieve desired service guarantees. However, in such a scenario, if either the sender or receiver in a two-way communication behaves maliciously, it can do arbitrary damage to its peer. No one in the intermediate network will step in and stop it, because Internet is not designed to police traffic. Intermediate networks, furthermore, are usually upgraded to high bandwidth pathways, with an intention to increase the throughput. This opens up an opportunity for malicious parties to misuse the abundant resources of the intermediate network for delivery of volumetric burst of messages to a less provisioned target. Moreover, end host resources are usually finite and consumable in nature. This implies a finite amount of bandwidth, finite amount of processing power and finite amount of storage capacities. Effectively, these can hence be exploited to the end of exhaustion.

C. Exploitability of Flooding Attacks

With the recent years, exploitability of flooding attacks has become significantly easy. The market is abundant in tools that lets even amateur attackers mount massive DDoS attacks without much know how. Referred to as DDoS-for-hire, there are services that have commoditized this class of attack and one can pay a small fee (or even free, for trial basis) to have a third party mount a DDoS attack against anyone. As of 2021, Launching DDoS attacks with illicit DDoS-for-hire services no longer requires even a nominal fee. The range of services offered by these nefarious platforms spans layers 3, 4, and 7 and targets everything from specific applications and games to methods for bypassing standard anti-DDoS measures [5]. According to just 19 out of hundreds of such sites on the dark web, they claim to have successfully launched more than 10 million DDoS attacks [5].

IV. ANOMALIES IN NETWORK TRAFFIC

When a network is under attack, be it an attempt to gain unauthorized access to resources or attempt to compromise the services altogether, anomalies in the network traffic are what typically first observed in the traffic logs. Anomalies in network traffic are network events that digress or deviate from the regular, expected, or anticipated behaviour.

[7] SYN, SYN-ACK, and ACK stands for SYNchronize, SYNchronize-ACKnowledgement, and ACKnowledge respectively.
[8] Internet Protocol (IP)/Internet Control Message Protocol (ICMP).
[9] A reflection attack involves an attacker spoofing a target's IP address and sending a request for information, primarily using the User Datagram Protocol (UDP) or in some cases, the Transmission Control Protocol (TCP). The server then responds to the request, sending an answer to the target's IP address.
[10] Amplification attacks generate a high volume of packets that are used to overwhelm the target website without alerting the intermediary.

It is important to note that from a security perspective, anomalies are suspicious and may even be the indication of an intrusion attempt to access information or a denial-of-service attack beginning to happen.

Network anomalies can arise due to various causes such as malfunctioning network devices, network overload, malicious denial of service attacks, and network intrusions that disrupt the normal delivery of network services. Intuitively, anomalies in a network may be due to two basic types of categories, namely, performance-related (including network failures) and security- related.

The security related network anomalies can range from very low throughput, for example in scenarios where a vital network service such as DNS[11] Name Server lookups are compromised, to heavy traffic loads such as in cases where an attempt is made to overwhelm the network bandwidth completely by flooding the network with unnecessary or redundant traffic.

A flooding attack is a security related network anomaly wherein an intruder attempts to flood the network with requests, either to starve the bandwidth resources or the resources of the target. In order to be able to mitigate such an attack, it is crucial to have efficient and resilient network anomaly detection systems in the perimeter of an infrastructure. Intrusion Detection Systems (IDS) are applications that monitor a network or for malicious network anomalies or policy violations and alert system or network administrators when such intrusions happen.

A. Exploitability of Flooding Attacks

A botnet, also sometimes referred to as the “zombie army,” is a logical collection of internet-connected devices called bots or zombies, such as computers and smartphones, which have been hijacked in the sense that their security has been compromised by infection through a malware (malicious software) and control ceded to a third party without the knowledge of the device’s rightful owner. The originator of a botnet, also referred to as a “bot herder,” or “bot master,” controls the botnet remotely, usually through intermediary machines known as the command and control (C&C, or C2) servers. Large botnets usually have multiple C&C servers and that provides the attacker a certain degree of redundancy. These C&C servers can either communicate through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP) or even through popular services such as Twitter using encoded content in feed to act as command and control.

Botnets are not just used for DDoS attacks; they can serve a number of other malicious purposes. It is significant to note that with the constant evolution of technological innovations such as the Internet of Things (IoT), attackers have evolved as well. Thingbots, the term used now to refer to botnets composed of compromised IoT devices is now the new trend. The year 2016 saw the first major IoT security incident with the emergence of Mirai, a botnet composed of IoT devices such as routers and security cameras, which was used in a number of high-profile DDoS attacks. Symantec also witnessed a twofold increase in attempted attacks against IoT devices over the course of 2016 and, at times of peak activity, the average IoT device was attacked once every two minutes. The DDoS attack on the French hosting company OVH broke all records up until September 2016, when the attack peaked at 1 Tbps[15].

V. INDUSTRY DEFENSE STRATEGIES AND MECHANISMS AGAINST FLOODING ATTACKS

Taking into consideration that protecting infrastructure from flooding attacks requires the ability to look at the outbound traffic, automated edge protection is the de facto industry defense. These automated edge protection strategies employ some combination of packet filtering and rate limiting to the inbound traffic flows. Existing industry defense strategies and mechanisms for protecting against flooding attacks at the edge involve a layered defense strategy[12] by using multiple infrastructure solutions in tandem. These include firewalls, Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), application delivery controllers and load balancers. However, each of these individually or even partially together are not adept to handle the multi- faceted flooding attacks seen in the wild. Many of them are stateful solutions that can themselves become targets of attacks.

Additionally, several solutions intend to reutilize a Content Delivery Network (CDN) to absorb flooding attacks as a way to defend. While CDNs can technically absorbing these large volumes of data, however, they are some serious considerations. Firstly, such a solution would require enough bandwidth to absorb the massive volume traffic that comes with a flooding attack, and with these attacks that are now exceeding hundreds of gigabits per second, that amounts to a hefty price for that capacity capability. Secondly, not every resource or webpage can be made to utilize the CDN. Hence it does not really provide a complete safeguard. Also, CDNs cannot really handle the application layer flooding attacks because that is not what they were built for. So, while CDN based solution may seem a simple choice, they are not as effective.

[11] DNS stands for Domain Name System
[12] This is also called Defense in depth.

Another very significant security mechanism that is often prevalent these days is Remotely triggered Black Hole (RTBH) filtering. In the given security context, black holes imply placements in network traffic where undesirable traffic can be forwarded and dropped. This filtering is a technique that employs the routing protocol and manipulates the routing tables at the edge of the network to specifically drop the undesirable traffic, often based on the source IP address [16].

Given the complexity of flooding attacks, several factors are required to be considered while building a defense strategy. These comprise of a multi layered integrated approach and may include:

1) Having diverse sources of threat intelligence including statistical anomaly detection, and fingerprints/signatures of known or emerging threats for a faster and accurate detection,

2) Ensuring both inline[13] and out-of-band[14] deployment to ensure there is not one single point of failure on the network,

3) Having broad network visibility so that traffic from different parts of the network can be effectively monitored and analysed, and,

4) Having infrastructure scalability to manage attacks of all volumes, low or high.

Given the majority of flooding attacks today utilize botnets, it also becomes crucial to develop a defense strategy that can also cope with the variability factor that comes with compromised devices included in bot armies. Determining the kind of devices that make request for resources by analysing their network profile, helps in gaining useful insight and helps identify the networks where compromised devices reside. It is significant to note that such an edge protection requires the ability of viewing defense both from outside in as well as inside out, thus ensuring that while malicious traffic is blocked and legitimate traffic is efficiently serviced, no internal devices become compromised and get vulnerable to be misused in a botnet elsewhere.

While all the factors considered above are important when considering implementing an effective defense against flooding attacks, detection and developing a sound threat intelligence rest at the core of any effective defense security mechanism against flooding attacks. It becomes imperative to be able to distinguish between a malicious flooding attack traffic and flash events[15] to ensure that the quality of service (QoS) is not hampered. Intrusion detection is hence a crucial step to defend against flooding attacks.

Industry Intrusion Detection Systems (IDS) today, utilize one of the two methods as per current standards to detect attacks, namely,

a) *Intrusion-Signature based:* Intrusion-signature based detection utilizes matching the packet signature with existing attack signatures in a database. This method however fails when the attack signature is not present in the database.

b) *Anomaly based:* Anomaly based detection characterizes what is considered as normal and abnormal traffic, setting threshold values, and checking traffic parameters against those set thresholds. This is intuitively a continuous learning process so that the method can effectively address changing request patterns.

One of the major benefits of anomaly-based intrusion detection is the scope for detecting new attacks, unlike intrusion-signature based detection which can only detect attacks whose signatures are present in the detection database.

VI. DETECTION USING ANOMALY TECHNIQUES

Anomaly techniques predominantly rely on network behaviour. Anomaly-based intrusion detection consists of observing and recognizing deviations from normal behaviour, which has been captured and maintained in electronic profiles. To ensure that the false positive rate is kept minimum, observations to populate these electronic profiles of network activity must be made across and time and across domains.

Furthermore, to capture anomalies in the network, it is necessary to identify the sources of data that can be utilized. These are inherently dependent on the type of network. Intuitively it is prudent to first categorize what must be considered normal network traffic and at what time. Being able to accurately identify and define this information is the first step in generating an algorithm that can effectively detect any occurrence of flooding attacks by measuring network anomalies.

With respect to effectiveness, an anomaly-based intrusion detection technique must be able to, first, maintain a high detection rate and, second, ensure a low false detection. Various parameters are utilized to meet these two criteria and many approaches make use of statistical models and tools to ensure the criteria are met.

A common anomaly-based network IDS has the following functional stages defined [17]:

1) *Formation of attributes*: Herein attributes are pre-processed based on the target system,

[13] Also called in-band, it implies accessing infrastructure from within the network.
[14] Out-of-band implies a secure and dedicated alternate access method into an IT network infrastructure for the purposes of administration
[15] Flash events, also called flash crowds refer the surge of traffic created by legitimate requests.

2) *Observation stage*: Herein a model is built and analysed with regards to the behavioural features of the target system, and,
3) *Functional stage*: This is the actual detection stage where traffic is observed against the model developed.

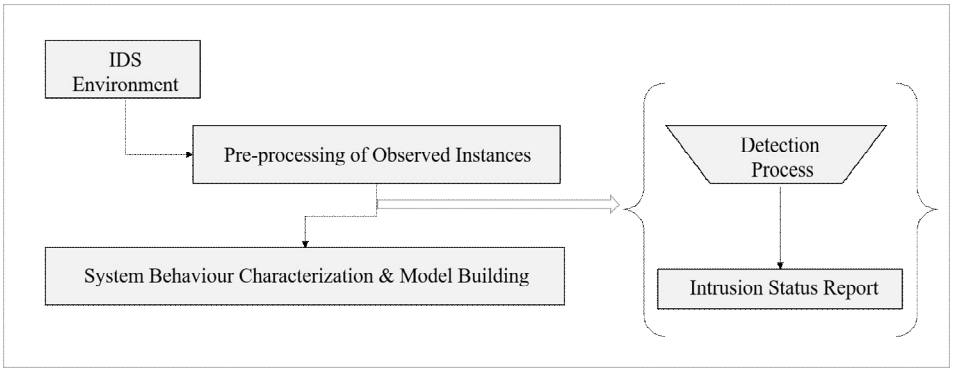


Fig. 6 Common Network Based Anomaly Intrusion Detection System

Anomaly based intrusion detection techniques can be categorized on the basis of what tools are used to build the detection model and profile. Most prominent of these are statistical based, cognition (or knowledge)-based, machine learning-based and data mining-based. User intention identification[16] and computer immunology[17] also form a basis of categorization.

As previously mentioned, an effective anomaly-based intrusion detection, capturing anomalies requires identifying suitable source of network data. These may include the following:

1) *Network Probes:* Probing tools such as ping and traceroute can help in obtaining definite network parameters such as packet loss and end to end delay. These are direct and instantaneous measure of how the network normally behaves. This mechanism can however provide limited value data due to many practical restrictive constraints.
2) *Filtered packets for flow-based statistics*: Network performance information can be gathered by sampling packets and analysing their IP headers. Flow based monitoring from this method can help classify unusual network flows.
3) *Data from routing protocols:* Capturing and processing routing events and related information can help gain insight into the behaviour of the network.
4) *Data from network management protocols:* Network traffic statistics can also be collected from the protocols that manage the inner workings for network, such as the SNMP (Simple Network Management Protocol). The information from such protocols is at a very granular level and hence can help characterize the network behaviour and can be used for network anomaly detection.

Once this collected information is processed and a model is built, rule-based approaches, finite state model approaches, pattern-based matching and/or statistical analysis may be performed for anomaly detection.

VII. CHALLENGES, GAPS AND WEAKNESSES

Intrusion Detection Systems (IDS) have advanced significantly over the years to handle the voluminous and varied intrusion attacks across networks and heterogenous devices. Distributed model IDSs called Distributed Intrusion Detection Systems (DIDS) are more in prevalence among organizations. DIDS work by distributing their analysis and monitoring functions across various components. This architecture as well as the significant automated response capabilities of IDSs put them at a noteworthy amount of risk of getting disabled by attackers, before an attempt is made to infiltrate deeper. Once the IDS components become the primary target for attackers, it may be possible for the attackers to completely compromise the capability of the IDS by attacking the critical components and advance with their malicious intent of attack.

Configuring Intrusion Detection Systems to be DDoS resilient in a one step closer to mitigate this challenge. Techniques may be employed to ensure that the critical IDS components stay hidden or invisible from an attacker by obscuring it from active network scanning and passive monitoring of packets. Beyond this, the critical components may be made to adapt by automatically relocating to another host in an event when they become a target of flooding attack. Additionally, two additional safeguards can help build overall resistance, namely blocking IP address spoofing and controlling the inbound traffic by traffic separation to their respective services [5].

[16] User intention identification is based on categorizing the features depending on the user or system usage to identify abnormal activities for the system.
[17] Computer immunology involves simulating the behaviour of natural immune system to develop immunologically meaningful interpretations from the characteristics of the system.

Such an architecture can help build resiliency over and above the standard defense mechanisms and provide effective resolution against flooding attacks.

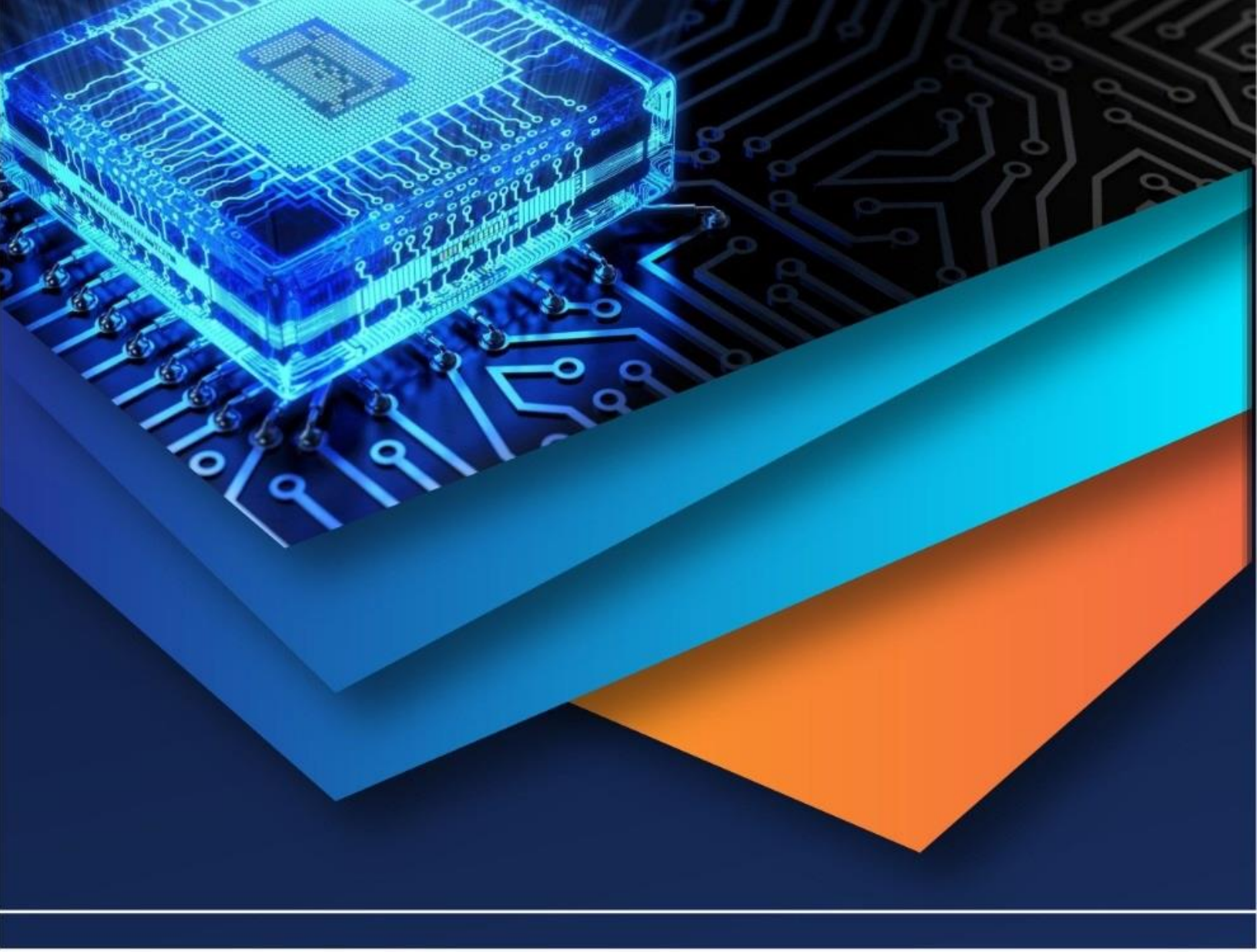
While IDSs themselves can be made resilient to detect and handle attacks, another big challenge is to handle the performance issues that infrastructures suffer with the heavy traffic inflows during an attack. Both the IDS and the network architecture must be able to recover efficiently while handling the voluminous inflows of traffic. While industries have built their infrastructures around Software Defined Networks (SDNs, an architecture that decouples the network control and forwarding functions enabling the network control to become directly programmable, so that they may have a much more efficient global view of the network with respect to DDoS protection, even those are vulnerable to several attacks. Several strategies are proposed to mitigate the issues, however, tackling all of them while maintaining scalability and efficiency remains a challenge.

VIII. CONCLUSION

Over the years, adversaries have been nefariously crafting flooding attacks against enterprises and service providers so that the target hosts get inundated while servicing to the end of exhaustion and can no longer function. Detecting such attacks is the foremost requirement for any security mechanism in place and detection via anomaly techniques is as essential as any other. They are the most intuitive approach for detecting in-the-wild, advance persistent threats and zero- day attacks with respect to the attack category and hence extremely crucial to be implemented. Building a resilient detection system that can both fend off inbound flooding attacks and protect internal devices from getting infected is the goal towards which efforts must be focused.

REFERENCES

[1] D. Dittrich, "The DoS Project's "trinoo" distributed denial of service attack tool," University of Washington, 21 October 1999. [Online]. Available: https://staff.washington.edu/dittrich/misc/trinoo.analysis. [Accessed 26 July 2018].
[2] "White Paper | 1999 CERT Incident Notes," [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=496440. [Accessed 26 July 2018].
[3] "FBI Facts and Figures 2003," Archived from Original https://www.fbi.gov/libref/factsfigure/factsfiguresapri2003.htm, 2003. [Online]. Available: https://web.archive.org/web/20070326115414/http://www.fbi.gov/libref/factsfigure/factsfiguresapri2003.htm. [Accessed 17 July 2018].
[4] P. V. a. G. Sneeringer, "Events of 21-Oct-2002 (Archived from Original)," 24 November 2002. [Online]. Available: https://web.archive.org/web/20110302164416/http://www.isc.org/f- root-denial-of-service-21-oct-2002. [Accessed 27 July 2018].
[5] Netscout, "Netscout Threat Intelligence Report: Issue 8 2021," 2021.
[6] Netscout, "The Anatomy of the DDoS Attack Campaign Targeting Organizations in Ukraine," [Online]. Available: https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting- multiple-organizations-ukraine. [Accessed 19 04 2022].
[7] Kentik Inc, [Online]. Available: https://www.kentik.com/analysis/ddos-attacks-against-ukrainian- government-networks/. [Accessed 19 04 2022].
[8] Netscout, "DDoS Threat Landscape - Ukraine," [Online]. Available: https://www.netscout.com/blog/asert/ddos-threat-landscape-ukraine. [Accessed 19 04 2022].
[9] 360 Netlab, "Some details of the DDoS attacks targeting Ukraine and Russia in recent days," [Online]. Available: https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/. [Accessed 19 04 2022].
[10] Kentik Inc, "DDoS Attacks against Ukrainian Government Networks," [Online]. Available: https://www.kentik.com/analysis/ddos-attacks-against-ukrainian-government-networks/. [Accessed 19 04 2022].
[11] Netscout, [Online]. Available: https://www.netscout.com/blog/asert/ddos-threat-landscape-ukraine. [Accessed 19 04 2022]
[12] Netscout, "DDoS Threat Landscape - Russia," [Online]. Available: https://www.netscout.com/blog/asert/ddos-threat-landscape-russia. [Accessed 19 04 2022].
[13] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.
[14] Netscout, "14th Worldwide Infrastructure Security Report," NETSCOUT SYSTEMS, INC., 2019.
[15] [Online].Available:https://securityaffairs.com/51640/cyber-crime/tbps-ddos-attack.html. [Accessed 13 01 2023]
[16] Cisco, [Online].Available: https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf [Accessed 13 01 2023]
[17] J. Sen, Ed., Computer and Network Security. IntechOpen, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)