Mitigation and Prevention Methods for Distributed Denial-of-Service Attacks on Network Servers

Kwitee D. Gaylah[1](✉) and Ravirajsinh S. Vaghela[2]

[1] Cyber Security, Marwadi University, Gujarat, India
kwiteed.gaylah.115593@marwadiuniversity.ac.in
[2] Marwadi University, Gujarat, India

Abstract. Present-day Different network-based attacks increased rapidly as internet-based communication increased. Recent DDoS attacks noticed throughout the Ukrainian government, defense, and banking websites. DDoS attacks become a major threat because the different vectors of malicious attacks increased this year with different motivations. This paper shows a cutting-edge overview of DDoS attacks, defense strategies, and migration methods. This article gives a systematic analysis of DDoS attacks that include the classification of different sorts of DDoS attacks and their mitigation and preventative methods. This research study examined well-known preventative and mitigation approaches. Additionally, it provided an overview of various attack kinds, filtering strategies, and attack detection approaches. It outlined the salient aspects of the attacks as well as the benefits and drawbacks of various forms of defense.

Keywords: Denial-of-service · Autonomous System (AS) · Botnet · Distributed denial-of-service · Load balancing · Log analysis · Filtering

1 Introduction

Distributed denial-of-service (DDoS) attacks, one of the numerous forms of illegal activities that take place online, can overwhelm even the biggest servers with too many requests, causing them to crash. Figure 1 represents a DDoS attack.

Current conflicts between Russia and Ukraine, which accounted for a major portion of all DDoS-related news in these nations in mid-January, had a big impact on the DDoS trend in 2022 [35]. The Internet sector, followed by cryptocurrency and later retail was the second most targeted. On March 1st, 2022, a DDoS attack on Kyiv Mayor Vitali Klitschko's website, and several Ukrainian ministries' websites were hacked [17]. The Ukrainian Ministry of Defence's website, the online services of Oschadbank and Privat Bank, as well as the hosting company Mirohost, were all subject to DDoS attacks in the middle of February [29]. Customers of Privat Banks reported receiving phone SMS messages regarding inoperable ATMs around the same time, which appeared to be sent to cause panic. On the 2 of February, a new DDoS attack consumed Ukrainian government

The original version of this chapter was revised: the 30th reference line has been updated. The correction to this chapter is available at https://doi.org/10.1007/978-3-031-23095-0_21

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022, corrected publication 2023
S. Rajagopal et al. (Eds.): ASCIS 2022, CCIS 1760, pp. 70–82, 2022.
https://doi.org/10.1007/978-3-031-23095-0_5

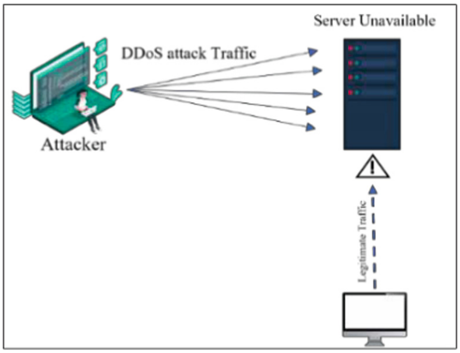

Fig. 1. DDoS attack

resources, and in late February and early March, the State Special Communications Service of Ukraine reported a mass of ongoing attacks [17].

DDoS attacks have grown in scale and regularity over the past few years. According to Kaspersky's Securelist blog, a percent of all recorded DDoS attacks in Q1 2022 occurred in the US. China and Germany, which were affected by 9.96% and 4.85% of recorded attacks during the same period, were closely behind it [36] (Fig. 2).

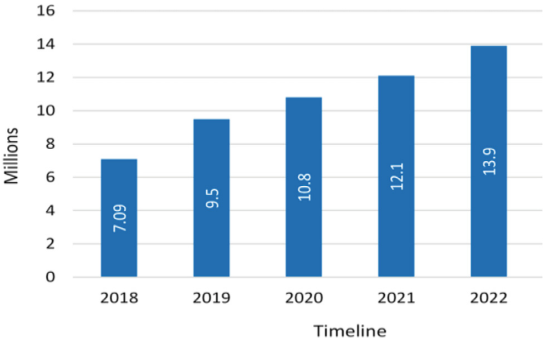

Fig. 2. DDoS attack trends

2 Proposed Survey

The Internet's architecture offers users the best-effort, packet-switched services. This leads to resource sharing amongst several users. As a result, one user's actions could interfere with another user's ability to access the services [21]. DDoS attack often seeks to obstruct authenticated users' access to services by depleting the system's resources. DDoS attack packets typically lack any glaring characteristics that would allow people to tell the difference between the bad stream from legitimate ones.

This paper shows a cutting-edge overview of DDoS attacks, defense strategies, and migration methods. This article gives a systematic analysis of DDoS attacks that include the classification of different sorts of DDoS attacks and their mitigation and preventative methods.

2.1 Motivation for DDoS Attacks

Check Point study shows that they track more than 1000 significant, diverse DDoS attacks every day globally [35]. These DDoS attacks can be directed at anyone, from an individual user at home to an entire government. The desire for financial gain is one of the main drivers behind attacks on these users [37]. However, pornographic or gambling websites can be tempting targets for a DDoS attack. Additionally, DDoS attacks frequently target governments and political organizations. DDoS attacks can also target financial markets and gaming websites, as demonstrated in Fig. 3.

In Cloudflare Lab quarterly report, we observe that most manufacturing, business services, and gaming are most affected by DDoS attacks [38].

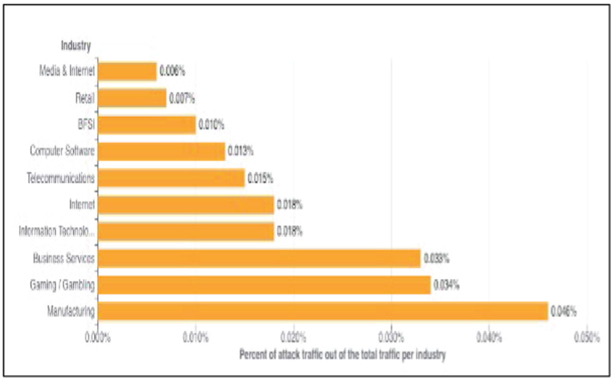

Fig. 3. Attack by organizations

- *Show of power:* This category of attackers performs DDoS attacks to show their skills.
- *Revenge:* Another motive for DDoS attacks is when some irate (and less technically proficient) individuals carry them out as revenge for perceived oppression.
- *Cyberwarfare:* This is another crucial attack motive that puts its targets in danger and has a big negative economic impact. An attack of this kind is often carried out by a few well-trained members of a military or terrorist organization.
- *Financial benefit:* This category of DDoS attacks is thought to be the most dangerous, they aim to earn some financial benefit from the hacks.

2.2 Attack Strategies and Phases

Figure 4 shows the DDoS attack's composition. A victim or target machine, numerous control masters, slaves, agents, and an attacker make up the components of a DDoS attack [13].

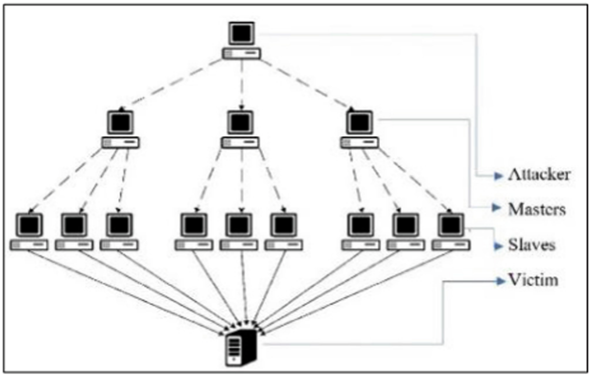

Fig. 4. DDoS attack components

- *Phase one:* The hacker acquires a good number of infected machines during the early phase. These infected devices are referred to as the masters because they direct other compromised machines into the attacking army [16].
- *Phase two:* The second step starts if enough devices have been enlisted in a compromised army. The term for this hacker army is a botnet. The attacker prepares for the attack by sending all essential information to the master armies in the second phase. The master armies then send the information to all slave armies.
- *Phase three:* In the last stage, the army of the attacker launches and executes attacks [33].

2.3 Attack Methods

Understanding DDoS attack classification methods are essential for comprehending DDoS attack studies. This study's goal is to investigate each attack taxonomy and give a complete, straightforward classification scheme. Figure 5 presents a classification scheme.

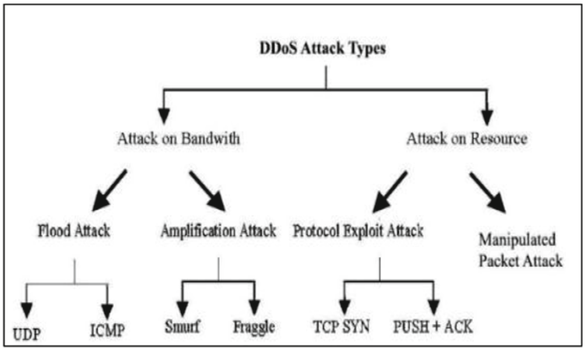

Fig. 5. Attack methods

- *Resource Depletion Attacks:* These attacks' purpose is to overload or crashes the system's significant resources, including memory, sockets, and CPU [9]. Initially, the attacker makes use of certain protocols along the application, transport, and network levels. Spoofed packets are employed as a second method of attack.
- *Protocol Exploit Attacks:* The weaknesses in the various network layer protocols are used by known protocol-based attacks. This attack causes the victim to use all of its memory while carrying out various memory-demanding tasks [22, 23].

Flood Attack. An example of resource depletion is a flood attack, in which a victim is attacked using the application layer protocol HTTP [19]. The HTTP GET and HTTP POST requests are specifically manipulated in this form of attack while a server or particular application is being communicated with (Fig. 6).

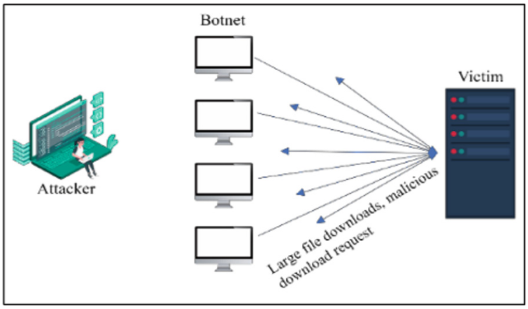

Fig. 6. Flood attack

TCP SYN Hack. The client sends an SYN packet to a server in three-way handshaking to start the handshaking. The server responds by delivering an SYN+ ACK packet. Finally, the client sends back the final ACK packet which completes the handshake and establishes the TCP connection [7]. By taking advantage of this functionality, the attacker can overwhelm the server's memory, which finally causes legitimate users to refuse connection attempts. The attacker starts a large number of connections but does not finish the handshaking procedure, flooding the victim's memory (Fig. 7).

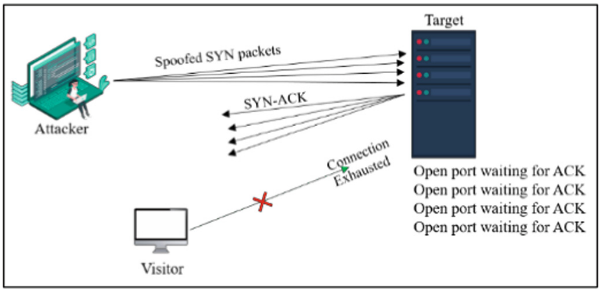
Target
Spoofed SYN packets
Attacker
SYN-ACK
Connection Exhausted
Open port waiting for ACK
Open port waiting for ACK
Open port waiting for ACK
Open port waiting for ACK
Visitor

Fig. 7. TCP SYN attack

DNS Amplification Attack. The goal of the most prevalent cyberattacks in the world is the network bandwidth of the victim. In this instance, the goal of the attacker is to leverage a DNS's weak points to scale up an intrusion significantly [3]. This exploit is also an illustration of a reflection attack that floods a victim with a large number of UDP packets by using several open recursive DNS servers [3, 25, 33] (Fig. 8).

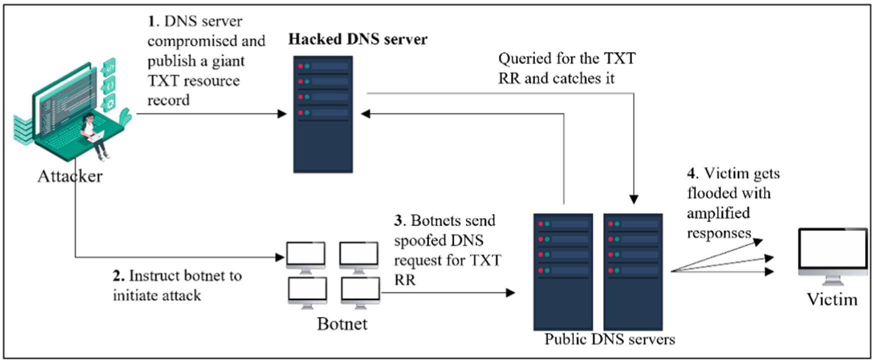
1. DNS server compromised and publish a giant TXT resource record
Hacked DNS server
Queried for the TXT RR and catches it
Attacker
4. Victim gets flooded with amplified responses
3. Botnets send spoofed DNS request for TXT RR
2. Instruct botnet to initiate attack
Botnet
Victim
Public DNS servers

Fig. 8. DNS amplification attack

Infrastructure Attack. The purpose of this attack is to seriously harm essential components of the Internet. As a result, it also targets the resources (memory, CPU) of the targeted system in addition to the network bandwidth [14]. Infrastructural attacks, for instance, target the DNS, particularly the root. A botnet sends standard UDP requests to the DNS server throughout a DNS flooding attack [2]. But because there are so many of them, the system becomes overwhelmed, and eventually, all of the resources are used up.

Zero-day Attack. Using some undiscovered security flaws or vulnerabilities, a zero-day attack takes place on day 0 [27, 34]. A "zero-day" is the first day after an attack when the system's vulnerabilities are discovered. For exposing zero-day vulnerabilities, many private software businesses or security organizations offer incentives and prizes [15] (Table 1).

Table 1. DDoS attacks summary

Attack Type	Description	Impact
HTTP flood	Exploits HTTP POST and GET request	Deplete all server resources
DNS flooding	Uses an exploit to boost the DNS response message	Flood network bandwidth

(*continued*)

Table 1. (*continued*)

Attack Type	Description	Impact
TCP SYN attack	Exploits the three-way handshaking of TCP	Deplete all server resources
ICMP flood	Exploits ICMP request	Flood network bandwidth
IP packet option field	Forms a packet larger than the allowed data packet size on the server	Buffer overflow and system crash
IP packet option field	Sets one to each quality-of-service bit	Inundates processing ability of the victim
DNS amplification	Uses an exploit to boost the DNS reply message	Flood network bandwidth
Land attack	Use the victim's IP as the source and destination address	Creates an infinite loop for the victim
HTTP fragmentation	Split an HTTP packet into tiny pieces and deliver them at the slowest rates possible	Consumes all sockets
Slow read	Reads the response as slowly as possible	Consumes all connections in the connection table
Slowlories	Opens the HTTP connection for the longest feasible time	Consumes all sockets
R.U.D. Y	Exploits the form submission field by sending data with the smallest packet size possible	Consumes all the connections
UDP flood	Sends a significant volume of UDP packets to a target's chosen or random port	Consumes network bandwidth

3 Prevention Methods

The best defensive strategy against DDoS attacks is to prevent them from happening (Fig. 9).

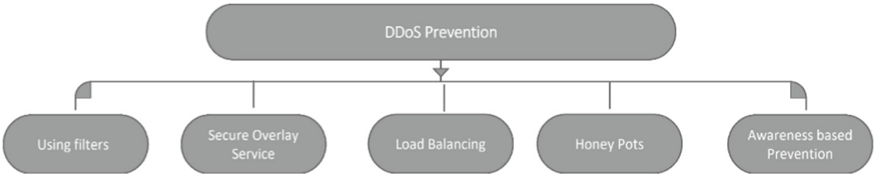

Fig. 9. DDoS prevention

3.1 Prevention Using Filters

Filtering strategies primarily shield a victim from attacks and keep an offender from being an unwitting victim. In essence, all filtering methods are used on the routers to guarantee that only authorized traffic can enter a system. This section will discuss several filtering strategies.

Route-based Packet Filtering. Route-based Packet Filtering uses routing information to evaluate whether a packet will reach a route [26]. An IP packet with a source address that differs from a set range of addresses is rejected by the core routers since it seems faked to the router [4].

According to Kihong Park and Heejo Lee's research, route-based packet filtering occurs on two timescales: packet forwarding based on table lookup at the fast time, and filter table update the slow one. As a result, its forwarding/discard function can be executed nearly at line speed subject to general processing overhead. That is, the core filtering function itself is not subject to a DoS attack [26].

Access Control Lists (ACL). This method can only be used for a brief period of historical time because it requires a lot of computing power. Markus et al. provided a fresh approach to reducing DDoS attacks based on collected information in their research. Instead of trying to identify DDoS attacks, the system aims to automatically create filter rules for IP firewalls. By doing so, the server will be able to continue serving legitimate users even when it is being heavily attacked by Denial-of-Service Attacks. [12].

Ingress Filtering. Egress filtering is the idea of firewalling traffic that originates on a local network but is going to a distant network. Like most other comparable for-profit and open-source solutions, pfSense includes a LAN rule that permits all traffic from the LAN to the Internet. However, this is not a good approach. Since most people anticipate it, it has been the de facto default in most firewall implementations. The common belief is that anything on the internal network is "trustworthy," so why bother screening?[10] RFC 226768's definition of ingress filtering permits network traffic that corresponds to a present range of the network's domain prefix to enter [30]. As a result, if an attacker uses a spoof IP address that does not match the prefix, the routers will disregard it. These filtering algorithms guarantee protection from a sizable number of DDoS attacks that employ faked IP [11].

Source Address Validity Enforcement Protocol (SAVE). The previously described RPF protocol has been improved with the SAVE protocol. It mandates that all destination routers linked to a source receive messages containing the most recent source information from the routers [20]. Each router then utilizes its forwarding table, which has been updated with the most recent data, to filter packets according to RPF's techniques.

Hop-count Filtering. This method doesn't ensure complete detection, but it can reject the majority of the spoof IP packets that make up the attack flow. The HCF Mechanism uses the IP header information, which is difficult to fabricate, to distinguish between faked and genuine packets [8]. To stop an attack, the filter discards packets that it recognizes as being part of a flow of faked packets.

History-based Filtering. To distinguish between legitimate traffic and malicious traffic, an efficient method (history-based IP filtering (HIF)) was proposed [24]. This method examines several DDoS attack features as well as regular traffic to extract traits that reveal information about the DDoS attack's occurrence. An attack is anything that deviates from the regular traffic profile.

3.2 Secure Overlay

The aim behind this method is to build an overlay network over the main IP network [32]. This overlay network serves as the gateway for outside networks to connect to the secured network. It is expected that safety can be attained if a network utilizes a distributed firewall or hides its IP addresses [18, 31].

3.3 Honeypots

An intriguing DDoS protection method is a honeypot. A honeypot is a network-attached system that hackers use to identify and research the tactics and types of attacks they utilize [9, 33]. On the internet, it serves as a potential target and alerts the defenders to any unauthorized attempts to access the information system. The actual system is thus kept secure [39]. The problem with this approach is skilled attackers can quickly recognize it because it can be distinguished from production systems [21].

3.4 Load Balancing

Dividing network traffic among several servers is known as load balancing. It ensures that a single server will not be overloaded. Load balancing increases the responsiveness of an application by distributing the work evenly (Fig. 10).

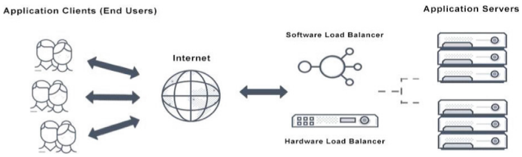

Fig. 10. Load balancing

3.5 Additional Security Patches

To prevent the system from being compromised by DDoS attacks, it is important to update software security patches regularly. The following are additional strategies to mitigate DDoS attacks.

Changing IP Addresses. Using this strategy, the computer system switches its IP address to a different one. Since the previous one could potentially be the target of DDoS attacks. However, there are other administrative costs associated with this. This strategy is effective as long as the attacker is not knowledgeable of the new IP address

Disabling Unusual Services. This is a DDoS defense technique. DDoS attacks could happen to some services, like character generator and UDP echo. By blocking these services, a system can be shielded from some DDoS attacks. Telnet and SSH remote access options to network servers should be disabled (Table 2).

Table 2. DDoS prevention using filters

Filter method	Description	Source of action
Route-based packet filtering	Uses a routing table to determine whether a packet arriving at a route is valid to the source and destination addresses	Main router
Access Control Lists (ACL)	Use a set of rules to specify which systems or users are permitted or denied access to a specific item or system resource	Main router
Ingress filtering	Uses a predetermined range of domain prefixes to filter traffic	Edge router for the victim's network
Source Address Validity Enforcement Protocol	Prevents delivery of packets based on source and destination addresses	Every inbound router
Hop-count filtering	Operates based on a packet's hop counts	The router at the victim's location
History-based filtering	The history of the normal traffic is used to determine malicious traffic	The router at the victim's location
Martian address filtering	Blocks the transmission of packets with IPs from the unallocated range of IP addresses	Every inbound router
Packet-score	A statistical technique that evaluates the profile values of each packet to award it a score	The router at the victim's location
Path identifier–based filtering	Works according to the attacker's known route	The router at the victim's location
SAVE	Makes the routers transmit messages with updated source addresses to all of the destination routers	Main router

4 DDoS Mitigation Methods

This section is crucial for defending against numerous DDoS attacks. However, despite new attack signatures and updates, DDoS attacks continue to pose a concern. As a result, there are numerous research efforts taking place in the area of DDoS mitigation, which is the next step of defense.

4.1 Detection of DDoS Attacks

It is fairly simple to detect an attack because it significantly reduces service or system performance. Sometimes a response necessitates tracing the origin of the attack, while other times it necessitates spotting the malevolent activity.

Signature-based Detection. To distinguish between legitimate traffic and malicious traffic, signature-based detection methods use known DDoS attacks to determine the attack signatures [24]. As a result, they are effective in identifying known DDoS attacks. But these detection systems fail to pick up on any variations in currently occurring attacks. This section of the paper will discuss some well-known signature-based detection mechanisms.

Log Analysis. Because they offer real-time information and statistics about your web traffic, log analysis tools are helpful software solutions for DDoS monitoring and detection. Spikes in activity suggestive of a DDoS attack can be found using tools like SolarWinds Loggly, and Splunk for instance [28]. To do this, Loggly uses an anomaly-detection program that scans servers for an excessive quantity of 503 errors.

Spectral Analysis. The methods described here use spectrum analysis to separate attack flow from regular traffic. For instance, attack flow is identified using the packets' power spectral density detection based on anomalies [1]. Attacks with new signatures and freshly discovered attacks can both be handled by anomaly -based detection mechanisms [6].

SNORT. SNORT is a highly popular tool for detecting network intrusions. It is a simple rule-based tool for detecting a variety of attacks and probes [5]. It has coupled anomaly-based security with signature-based detection to broaden the scope of attacks it can identify. However, because SNORT relies on precise pattern matching, it may cause a bottleneck in the system's performance due to the high volume of traffic and Internet speed.

5 Conclusion

Based on their successes and failures, this study examined well-known preventative and mitigation approaches for DDoS attacks. Additionally, it provided an overview of various attack kinds, filtering strategies, and attack detection approaches. It outlined the benefits and drawbacks of various forms of DDoS defense strategies. However, further research is necessary to fight new and undiscovered attacks with new signatures.

References

1. Agrawal, N., Tapaswi, S.: Low rate cloud DDoS attack defense method based on power spectral density analysis. Inf. Process. Lett. **138**, 44–50 (2018). https://doi.org/10.1016/j.ipl.2018.06.001
2. Alonso, R., Monroy, R., Trejo, L.A.: Mining IP to domain name interactions to detect DNS flood attacks on recursive DNS servers. Sensors (Switzerland) **16**(8), 1311 (2016). https://doi.org/10.3390/s16081311
3. Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., Gritzalis, S.: DNS amplification attack revisited. Comput. Secur. **39**, 475–485 (2013). https://doi.org/10.1016/j.cose.2013.10.001
4. Armbruster, B., Smith, J.C., Park, K.: A packet filter placement problem with application to defense against spoofed denial of service attacks. Eur. J. Oper. Res. **176**(2), 1283–1292 (2007). https://doi.org/10.1016/j.ejor.2005.09.031
5. Badotra, S., Panda, S.N.: SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking. Clust. Comput. **24**(1), 501–513 (2020). https://doi.org/10.1007/s10586-020-03133-y
6. Chen, Y., Hwang, K.: Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. J. Parallel Distrib. Comput. **66**(9), 1137–1151 (2006). https://doi.org/10.1016/j.jpdc.2006.04.007
7. Deng, Y., et al.: Resource provisioning for mitigating edge DDoS attacks in MEC-Enabled SDVN. IEEE Internet Things J. **9**(23), 24264–24280 (2022). https://doi.org/10.1109/JIOT.2022.3189975
8. Devi, G.U.: Detection of DDoS attack using optimized hop count filtering technique. Indian J. Sci. Technol. **8**(26), 1–6 (2015). https://doi.org/10.17485/ijst/2015/v8i26/83981
9. Erhan, D., Anarim, E.: Hybrid DDoS detection framework using matching pursuit algorithm. IEEE Access **8**, 118912–118923 (2020). https://doi.org/10.1109/ACCESS.2020.3005781
10. Baker, F., Savola, P.: Ingress Filtering for Multihomed Networks. RFC 3704 (2004)
11. Ferguson, P., Senie, D.: Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. In: Request for Comments (2000)
12. Goldstein, M., Lampert, C., Reif, M., Stahl, A., Breuel, T.: Bayes optimal DDoS mitigation by adaptive history-based IP filtering. In: Proceedings - 7th International Conference on Networking. ICN 2008 (2008)
13. Gupta, B.B., Chaudhary, P., Chang, X., Nedjah, N.: Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. Comput. Electr. Eng. **98**, 107726 (2022). https://doi.org/10.1016/j.compeleceng.2022.107726
14. Hasan, D., Hussin, M., Abdullah, A.: Effective amplification mitigation and spoofing detection during DNS flooding attacks on internet. J. Eng. Appl. Sci. **12**(3), 475–480 (2017). https://doi.org/10.3923/jeasci.2017.475.480
15. Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.N., Bayne, E., Bellekens, X.: Utilising deep learning techniques for effective zero-day attack detection. Electronics (Switzerland) **9**(10), 1684 (2020). https://doi.org/10.3390/electronics9101684
16. Huang, K., Yang, L.X., Yang, X., Xiang, Y., Tang, Y.Y.: A low-cost distributed denial-of-service attack architecture. IEEE Access **8**, 42111–42119 (2020). https://doi.org/10.1109/ACCESS.2020.2977112
17. Husák, M., Laštovička, M., Plesník, T.: Handling internet activism during the Russian invasion of ukraine: a campus network perspective. Digital Threats: Research and Practice (2022). https://doi.org/10.1145/3534566
18. Keromytis, A.D., Misra, V., Rubenstein, D.: SOS: Secure overlay services. In: Computer Communication Review (2002)

19. Kshirsagar, D., Kumar, S.: An ontology approach for proactive detection of HTTP flood DoS attack. Int. J. Syst. Assur. Eng. Manag. (2021). https://doi.org/10.1007/s13198-021-01170-3
20. Li, J., Mirkovic, J., Ehrenkranz, T., Wang, M., Reiher, P., Zhang, L.: Learning the valid incoming direction of IP packets. Comput. Netw. **52**(2), 399–417 (2008). https://doi.org/10.1016/j.comnet.2007.09.024
21. Mahjabin, T., Xiao, Y., Sun, G., Jiang, W.: A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. **13** (2017). https://doi.org/10.1177/1550147717741463
22. Manickam, S., et al.: Labelled dataset on distributed denial-of-service (DDoS) attacks based on internet control message protocol version 6 (ICMPv6). Wirel. Commun. Mob. Comput. **2022** (2022). https://doi.org/10.1155/2022/8060333
23. Manso, P., Moura, J., Serrão, C.: SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Information (Switzerland) **10**(3), 106 (2019). https://doi.org/10.3390/info10030106
24. Obaidat, M.S. (ed.): ICETE 2016. CCIS, vol. 764. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-67876-4
25. Nuiaa, R.R., Manickam, S., Alsaeedi, A.H.: Distributed reflection denial of service attack: a critical review. Int. J. Electr. Comput. Eng. (IJECE) **11**(6), 5327 (2021). https://doi.org/10.11591/ijece.v11i6.pp5327-5341
26. Park, K., Lee, H.: On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets * (2001)
27. Parrend, P., Navarro, J., Guigou, F., Deruyver, A., Collet, P.: Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. EURASIP J. Inf. Secur. **2018**(1), 1–21 (2018). https://doi.org/10.1186/s13635-018-0074-y
28. Rodrigues, K., Luo, Y., Yuan, D.: CLP: Efficient and scalable search on compressed text logs. In: Proceedings of the 15th USENIX Symposium on Operating Systems Design and Implementation. OSDI 2021 (2021)
29. Serpanos, D., Komninos, T.: The cyberwarfare in Ukraine. Computer (Long Beach Calif) **55**, 88–91 (2022). https://doi.org/10.1109/MC.2022.3170644
30. Tandon, R.: A Survey of distributed denial of service attacks and defenses (2020). https://arxiv.org/abs/2008.01345
31. Wang, X., Chellappan, S., Boyer, P., Xuan, D.: On the effectiveness of secure overlay forwarding systems under intelligent distributed DoS attacks. IEEE Trans. Parallel Distrib. Syst. **17**(7), 619–632 (2006). https://doi.org/10.1109/TPDS.2006.93
32. Yang, X., Yu, Y.: DDoS attacks defense mechanism based on secure routing alliance. Int. J. Performability Eng. **14**, 515–520 (2018). https://doi.org/10.23940/ijpe.18.03.p12.512520
33. Zhang, C.: Impact of defending strategy decision on DDoS attack. Complexity **2021**(2), 1–11 (2021). https://doi.org/10.1155/2021/6694383
34. Zoppi, T., Ceccarelli, A., Bondavalli, A.: Unsupervised algorithms to detect zero-day attacks: strategy and application. IEEE Access **9** (2021). https://doi.org/10.1109/ACCESS.2021.3090957
35. CYBER AT TACK TRENDS Check Point's 2022 Mid-Year Report
36. kaspersky.de APT trends report Q1 2022 GReAT
37. DDoS attack trends for Q1 2021
38. Network-Layer DDoS Attack Trends for Q4'20
39. Five Best Practices for Mitigating DDoS Attacks How to defend against rapidly evolving Distributed Denial-of-Service threats and address vulnerabilities at every layer