Big picture: analysis of DDoS attacks map – systems and network, cloud computing, SCADA systems, and IoT

Saeed Salah

Department of Computer Science,
Al-Quds University,
P.O. Box 89, Jerusalem, Palestine
Email: sasalah@staff.alquds.edu

Belal M. Amro*

Computer Science Department,
Hebron University,
P.O. Box 40, Hebron, Palestine
Email: bilala@hebron.edu
*Corresponding author

Abstract: Distributed denial-of-service (DDoS) attacks are among the toughest security issues nowadays. These attacks are launched at any time and can impact any part of a network's operations or IT resources. Because of the seriousness of these attacks, many countermeasures have been developed by both the private sector and the research community. Despite the availability of many research efforts that suggested DDoS attacks classifications, the multitude, diversity, and variety of both the attacks and their countermeasures have the consequence that no standard taxonomy exists. In this paper, we introduce an updated and structured taxonomy of both DDoS attacks and their countermeasures. The novelty of this work stems from the fact that it covers different dimensions of tackling DDoS attacks in the four main technology areas: systems and network, cloud computing, SCADA, and IoT, with the main aim of providing an all-in-one comprehensive reference for ongoing and future security research.

Keywords: distributed denial-of-service; DDoS; internet of things; IoT; supervisory control and data acquisition; SCADA; systems, network; cloud computing.

Reference to this paper should be made as follows: Salah, S. and Amro, B.M. (2022) 'Big picture: analysis of DDoS attacks map – systems and network, cloud computing, SCADA systems, and IoT', *Int. J. Internet Technology and Secured Transactions*, Vol. 12, No. 6, pp.543–565.

Biographical notes: Saeed Salah is an Assistant Professor and researcher at the Department of Information Technology, Faculty of Dual Studies at Al-Quds University in Jerusalem. He received his BSc in Electrical/Computer Engineering from the Al-Najah National University in 2003, his MSc in Computer Science from the Al-Quds University in 2008, and his PhD from the Department of Signal Theory, Telematics and Communications of the University of Granada in 2015. His research interests are focused on network management, information and network security, machine learning, data mining, MANETs, routing protocols, e-leaning, and natural language processing.

Belal M. Amro is an Assistant Professor at the College of IT, Hebron University, Palestine. He has received his PhD in Computer Science and Engineering from the Sabanci University, Istanbul, Turkey in 2012. In 2004, he received his MSc in Complexity and its Interdisciplinary Applications from the IUSS, Pavia, Italy. His BSc was awarded from the Palestine Polytechnic University in Computer Systems Engineering in 2003. He has served as technical program committee member for different international conferences and journals, and reviewed more than 50 papers in the field of information technology including privacy and security. Currently, he is conducting research in network security, wireless security, and privacy preserving data mining techniques. He has published more than 18 papers in international journals and conferences in the field of computer security and privacy.

1 Introduction

Due to the rapid development of telecommunication technologies over the past decade, users are currently relying on internet-based services to carry out most of their daily activities. Due to the intrinsic nature of the internet structure, which primarily focused on improving services' functionality, rather than security, it inherently suffers from many security problems that can easily facilitate the perpetration of various types of attacks. Examples of such security issues are

1 Interdependency; its vulnerability to DDoS attacks is a global issue, and it is not depending on a specific network or machine.

2 Resource limitation of the internet entities; i.e., end-user devices, network devices, and services have very limited resources that can be quickly overloaded.

3 Attacker vs. victim resources; coordinating distributed attacks makes them more effective if the number of resources available to attackers is larger than those available on the victims' machines.

4 Internet resources and intelligence are not streamlined; the intelligence which is required to guarantee service-level agreements (SLAs) is sited at the end-user machines. Nevertheless, attackers can maliciously use the available resources of the intermediate network to facilitate the attack activities.

5 Accountability lack of enforcement; some attacks provide the attacker with robust mechanisms to be anonymised.

6 The internet is a distributed control system; there are no standard security mechanisms or policies being deployed worldwide, each service provider can deploy various local security policies, selected by its management team.

One of the many types of internet-based services attacks, that can be described as mysterious with a big challenge to alleviate is the denial-of-service (DoS) attack, and things become more sophisticated if such attacks are distributed (DDoS) (Dahiya and Gupta, 2021; Mishra et al., 2021; Baskar et al., 2021). DDoS attacks can be launched anytime from anywhere, to target the network's operations or IT resources, leading to massive amounts of service/s interruptions and big financial losses. Norton Inc. (https://www.norton.com) claimed that DDoS attacks are one of the most harmful and

powerful armaments to internet-based services. Amazon Inc. (https://www.amazon.com) stated that during the first quarter of 2020, they experienced 2.3 Tbps DDoS attacks traffic. Also, in the Cisco Annual Internet Report 2018–2023 (https://www.cisco.com), it is stated that the peak DDoS attack size is increased by (63% – Y/Y), 776% growth in DDoS attacks between (100 to 400 Gbps – Y/Y), the global frequency of DDoS attacks went up by (39% – Y/Y), and 23% of the attacks' traffic exceeded 1 Gbps, which is enough to take most companies completely offline. NETSCOUT Arbor's (https://www.netscout.com/) stated that about 87% of the actual network threats experienced on internet service providers (ISPs) are DDoS attacks.

DDoS attacks can be launched by attackers for different purposes including disrupting legal network operations, device malfunctioning, denying critical services for legitimate users, overloading a network by degrading throughput, etc. Furthermore, some attacks may exploit programming flaws, software bugs, loopholes, and misconfigurations in software services to slow down or crash ordinary network services (Ravi and Shalinie, 2020; Singh and Behal, 2020).

DDoS attacks are mainly launched through a network of hundreds or even thousands of controlled machines, named 'zombies'. Grouping a huge number of zombies constructs what is the so-called 'botnet'. The larger the botnet size, the greater the magnitude of the attack and the more severe the effect of that attack. Those zombies are coordinated on a large-scale basis and the attacker injects her code into these machines so that she can remotely control them (see Figure 1).

Figure 1 A typical structure of a DDoS attack (see online version for colours)

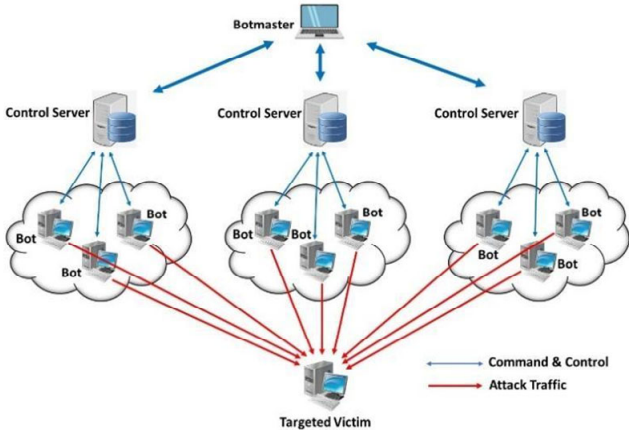
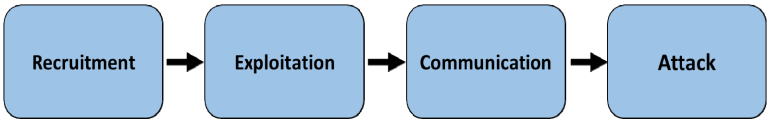


Figure 2 depicts a simplified block diagram of a typical DDoS attack (Mirkovic and Reiher, 2004; Douligeris and Mitrokotsa, 2004; De Donno et al., 2018). Any DDoS attack needs to go through four stages to be struck: *recruitment*, *exploitation*, *communication*, and *attack*. During the recruitment process, with the help of vulnerability scanning tools, the attacker scans for vulnerable machines to be used in perpetrating the attack. This process can be performed manually or automatically. During the exploitation stage, the discovered vulnerabilities are exploited by injecting malicious codes and are added to the botnet. Next comes the communication stage where the hackers use the command and control (C&C) communication infrastructure to manage the botnet, which includes scheduling attacks as well as upgrading the agents when required. Finally, in the

attack stage, the attacker starts the attack by instructing zombies to perform malicious activities against the victim. Some attack attributes – as target ID, attack duration, and some attributes of the malicious traffic – can be tuned in this stage. It is worth noting here that this process is iterative in such a way that the output of any stage could be fed as an input to the next stage.

Figure 2 DDoS attacks generic stages (see online version for colours)



In today's scenario, DDoS attacks are becoming very serious threats to many emerging technologies in systems and networks, cloud computing, supervisory control and data acquisition (SCADA) systems, and the internet of things (IoT). To the best of the authors' knowledge, this is the first taxonomy that presents the big picture of DDoS attacks. Existing taxonomies are technology-specific, i.e., they target one or two of the aforementioned technologies. Therefore, in this paper, we propose a taxonomy of DDoS attacks and their countermeasures by comprehensively reviewing and unifying the efforts coming from the aforementioned technologies into an all-in-one comprehensive reference for ongoing and future security research targeting these promising technologies to ensure successful mitigation against these attacks.

The remainder of the paper is structured as follows. Section 2 overviews the existing DDoS attack taxonomies targeting systems and networks, cloud computing, SCADA systems, and IoT. Section 3 details the suggested DDoS attacks classification taxonomy. Section 4 explains various mitigation techniques of DDoS attacks developed for these technologies. Finally, Section 5 concludes the paper and presents some future research lines.

2 Related work

Over the past years, many DDoS attack taxonomies have been proposed in the research literature. Existing studies are technology-specific; in such a way that they targeted one or two of the following technologies with limited scope: systems and networks, cloud computing, SCADA systems, or IoT. In this section, we deeply summarise the existing DDoS taxonomies targeting the aforementioned technologies.

2.1 DDoS attacks in systems and networks

Computer systems and networks are closely related to each other, many attacks are common between them while some other attacks are either network attacks or system attacks. DDoS attacks target both networks and computers although the mechanism of each attack differs between them, the main goal is to stop the network or system from providing a service. Hansman (2003) have done much work on classifying attacks and generating robust taxonomies that may enhance the ability to better fight against these attacks. A very simple classification of DDoS attack types as well as the attack tools and

the exploited vulnerabilities was proposed by Gerber (2000). The author also provided some simple techniques to mitigate the effect of these attacks.

A more comprehensive taxonomy of DDoS attacks was presented by Mirkovic and Reiher (2004). The authors classified attacks based on multiple dimensions including a degree of automation, exploited vulnerability, rate, the possibility of identification, and impact. A different view of classification was proposed by Howard and Longstaff (1998) who created a taxonomy according to the tools used in the attack, the exploited vulnerabilities of the attack, the countermeasures carried out, the victim, and the outcomes of these countermeasures. This taxonomy was useful to understand the nature of DDoS attacks and it included all the properties of each attack. Campbell (2005) categorised DDoS attacks into four classes namely: partner (spoofing), flood, trip (shut down), and intervene (interception). These classes were presented in an expanded tree structure where potential vulnerabilities are presented as well.

In a way to better understand DDoS, Bhatia et al. (2018) provided a two-dimensional view of these attacks where they divided them into two classes namely: semantic, and high-rate flooding. Their taxonomy classified DDoS attacks according to the layers in which attacks are taking place and provided some examples of such attacks as well as techniques. They pointed out that although there exist robust DDoS taxonomies, these taxonomies did not fit into the ever changing DDoS attackers. The authors also provided detailed descriptions of prevention methods that might be used to mitigate and stop such attacks.

A taxonomy of network attacks and related tools was provided by Hindy et al. (2020). The authors provided a combination between datasets used to improve intrusion detection systems (IDS), and the attack taxonomy, which they claim will improve the creation of more realistic datasets, and hence improve the efficiency of next-generation IDS. The classification of DDoS attacks was in three classes namely: flood, amplification, and protocol exploit. DDoS attack techniques were also presented according to both TCP/IP and OSI communication models. A similar work was carried out by the same author with others (Hindy et al., 2018) where they combined the taxonomy of the attacks with IDS to improve IDS and create more realistic datasets.

Aiming at generating a good understanding of attacks by combining these attacks with their corresponding tools, Nagpal et al. (2015) provided a classification with a combination of the tools related to each attack as well as identifying various mitigation techniques used against these attacks. Similar work was carried out by Kumar and Kumar (2016). In this work, the authors focused on DDoS attacks at the application layer and summarised the major DDoS tools used to launch these attacks as well as mitigation techniques. A taxonomy of attack tools was also provided by Hoque et al. (2014). A discussion of the pros and cons of each tool was provided in a structured way that might help network defenders as well as hackers. Mahjabin et al. (2017) presented a survey of DDoS attacks and their mitigation techniques. They relied on a taxonomy where DDoS attacks are divided into two classes namely: resource depletion and bandwidth depletion. Resource depletion is split into protocol exploits, and malformed packets. Where bandwidth depletion is split into protocol exploit attacks and amplification attacks. A Detailed description of attack techniques was provided for each of the subcategories as well as mitigation techniques. The taxonomy they used was similar to the taxonomy provided by Prasad et al. (2014). To better classify and understand DDoS attacks, some researchers focused on investigating attacks that target a particular layer such as an

application layer. Jaafar et al. (2019) conducted a review of HTTP DDoS attacks and their detection methods. Similar work was conducted by Alomari et al. (2012) where they studied and classified the DDoS attacks that target the web server. They have also reported some recent web server DDoS attack incidents.

2.2 DDoS attacks in cloud computing

Cloud computing is an emerging technology where users can store data and use software and services over the internet. Most companies are now using the cloud to scale up without having to invest in new infrastructures or purchasing software licenses. A cloud computing structure is divided into three main categories (Darwish et al., 2013) – infrastructure as a service (IaaS) – where users can access physical resources like networks and storage; platform as a service (PaaS) – where users can access various platforms with different operating systems; and software as a service (SaaS) – where users can access many applications and software programs.

Hindy et al. (2018) highlighted different DDoS attacks in the cloud and their countermeasures. They classified attacks in the cloud in four basic classes: browser level, application level, server level, and network level. They listed many DDoS attacks in the cloud that are similar to network and systems attacks, these attacks include ping of death, teardrop, smurf, land attack, SYN flood, and many others. The authors also presented defence mechanisms against these attacks. Similar work was done by Mahjabin et al. (2017), where the authors listed DDoS attacks in the cloud as well as mitigation techniques along with their drawbacks. They classified the attacks as resource depletion and bandwidth depletion. Then they presented DDoS detection techniques and their effectiveness in cloud computing.

Kesavamoorthy et al. (2020) explained DDoS attacks in cloud computing and proposed a taxonomy similar to what we have seen in networks and systems. Similarly, Nagpal et al. (2015) presented DDoS attacks in the cloud and their mitigation techniques. They classified DDoS attacks in the application layer (HTTP) and the network layer (flood, reflection, and amplification). Dedicated work on IaaS DDoS attacks was carried out by Alomari et al. (2012), where the authors classified attacks-including DDoS – on IaaS based on impact and detectability, they have also listed DDoS countermeasures. Jaafar et al. (2019) investigated the most used methods to mitigate DDoS attacks in the cloud as well as prevention and recovery techniques. They listed the types of DDoS attacks in the cloud including flooding, protocol exploitation, fragmentation, ping of death, and many other attacks.

2.3 DDoS attacks in SCADA systems

SCADA are systems' frameworks with built-in monitoring stages, advanced communications, and sensors that provide prompt alert warnings to the central stations in process control. SCADA systems comprise many components such as end-user devices, terminals, sensors, programmable logic controllers (PLC), communication facilities, and graphical user interfaces (GUI) for high-level processing, and supervisory management of project-driven-processes. SCADA systems are now designed to work in a standalone way and relied on air-gapped networks and proprietary protocols for securing the system. Modernisation of the SCADA system, standardisation of communicating protocols, and increase of interdependence have greatly increased cyber-attacks that targeted SCADA

systems. Such types of attacks are becoming highly sophisticated to perpetuate classical cybercrimes.

Pliatsios et al. (2020) made comprehensive state-of-the-art SCADA systems. They discussed the general SCADA architecture, along with a detailed description of the SCADA communication protocols, and certain high-impact security incidents, objectives, and threats. Furthermore, they carried out an extensive review of the security proposals and tactics that aim to secure SCADA systems. Cherdantseva et al. (2016) examined twenty-four risk assessment methods applied in the context of SCADA systems. They analysed these methods in terms of the aim of the application domain, stages of risk management addressed, key risk management concepts covered, impact measurement, sources of probabilistic data, evaluation, and tool support. They also suggested an intuitive scheme for the categorisation of cybersecurity risk assessment methods for SCADA systems.

Ferrag et al. (2020) presented a comprehensive survey of existing cybersecurity solutions for fog-based smart grid SCADA systems. They provided a classification of these solutions into four categories, including authentication solutions, privacy-preserving solutions, key management systems, and IDSs. Huseinović et al. (2020) suggested a comprehensive taxonomy of DDoS attack techniques and their countermeasures targeting smart grid platforms. The DDoS techniques are divided into six categories: jamming, resource exhaustion, data attacks, desynchronisation, routing, and reflector. Kamal et al. (2017) suggested a security taxonomy of SCADA environment based on ten categories: origin, methods, medium, level, severity, target, type, impact, vulnerabilities exploited, and threat motivation. Yadav and Paul (2021) made a survey on SCADA systems including architectures, intrusion detection techniques, testbeds, and IoT-based SCADA systems by analysing the architecture of modern SCADA systems. They classified SCADA system attacks into five categories: country, target component, attack method, impact, and attack category. They also classified IDSs into two categories: classification based on information origin, and methodology analysis.

East et al. (2009) focused on the analysis of attacks targeting the Distributed Network Protocol (DNP3), which is one of the predominant SCADA protocols being widely used nowadays. They classified the attacks based on two perspectives: targets, including control centre, outstation devices, and communication paths, and threat categories, including interception, interruption, modification, and fabrication. They also classified the operational effect of the attacks into three objectives: process confidentiality, process awareness, and process control. Zhu et al. (2011) made a taxonomy of cyber-attacks on SCADA systems, they first highlighted the main technical difference between standard IT and SCADA systems. Next, they classified cyber-attacks on SCADA systems into three categories: attacks on software (S/W), attacks on hardware (H/W), and attacks on communication stack following the TCP/IP layered hierarchy. In each category, they listed the most common vulnerabilities leading to attacks. Kim et al. (2020) made a comprehensive taxonomy of security attacks targeting nuclear power plants. They analysed the attacks using several dimensions such as attack vector, attack consequence, attack procedure, vulnerability, and countermeasures. Lankatilake (2019) conducted a data analysis of ten cases of attacks from (2003–2017) using a set of derived attributes: target industry, vulnerability, nature of the attack, payload, and physical impact, attacker profile, and motivation. Mohan et al. (2020) identified and discussed attack strategies considering various configurations of the load frequency control (LFC) system. They

classified the main attacks into cyber-layer attacks – including data integrity attacks and DDoS attacks – and cyber/physical layer attacks – including resonance attacks. They also reviewed some of the existing countermeasures. Ding et al. (2020) provided a review for secure state estimation and control of cyber-physical systems (CPSs). They summarised the latest development of secure state estimation considering different performance indicators and defence strategies. Then, they discussed the results and classified them into three categories: centralised secure control; distributed secure control; and resource-aware secure control. Rakas et al. (2020) analysed IDSs in SCADA in the period (2015–2019). They proposed an evaluation methodology considering the generic features of IDS detection technique, protocols, used tools, test environment, and performance evaluation.

2.4 DDoS attacks in IoT

IoT refers to a type of network technology to connect anything with the internet infrastructure. A set of protocols were implemented to facilitate information sensing, information exchange, and communication to achieve smart recognition, positioning, tracking, monitoring, and administration. IoT has become a famous technology in recent years because of the many benefits it provides, such as enhancing human well-being, increasing the level of autonomy in tasks, and simply, providing better experiences for businesses and consumers. The internal design structure of the majority of IoT devices does not consider the security and privacy of users. Therefore, DDoS has become more popular, a driving factor for this popularity was the increased adoption of IoT in the industry. DDoS attacks are initiated by the attacker to harvest the data or resources either to hamper the operational capabilities of IoT infrastructures or completely deny their use of them.

De Donno et al. (2018) classified DDoS attacks in IoT based on a set of dimensions including architectural model, exploited vulnerability, propagation mechanism, degree of automation, victim type, attack traffic distribution, and resources involved. They also provided an analysis of Mirai; one of the main disruptive DDoS-capable IoT malware. Roohi et al. (2019) provided a detailed overview of the existing research on DDoS attacks and countermeasures in the context of IoT. In this paper, attacks are classified according to their impact on resources, bandwidth, infrastructure, and bug impact. Sonar and Upadhyay (2014) suggested a taxonomy of DDoS attacks and defence mechanisms using the integration of IoT and cloud environments. They made a comparison of various models being widely used to detect DDoS attacks in the integration of IoT and cloud infrastructures. They also compared DDoS volume-based and application-layer attacks. Khader and Eleyan (2021) reviewed some of the security problems related to DDoS attacks and their countermeasures and classified them according to the generic layered model of IoT which consists of perception layer, network layer, middleware layer, and application layer. Considering that every layer has its own set of vulnerabilities that can be exploited by attackers, Hameed et al. (2019) identified, categorised, and discussed various security challenges and state-of-the-art efforts to resolve these challenges. They focused on privacy provisioning, lightweight cryptographic framework, secure routing and forwarding, robustness and resilience management, DDoS, and insider attack detection.

Abughazaleh et al. (2020) focused on smurf attack and SYN flood, which are two common DDoS attacks targeting the network layer of the IoT layered model and

discussed DDoS mitigation technologies implemented by IoT security companies. Veluri et al. (2021) summarised IoT security attacks and established a taxonomy based on the application domain and the layered architecture of IoT. The IoT attack is assessed according to various classification criteria. At the same time, the protection of each layer on the IoT architecture should be enforced. More studies are needed to establish a robust protection framework for the whole IoT architecture, including the implementation of IDSs and risk evaluation and mitigation. Abdul-Ghani et al. (2018) developed a taxonomy of IoT attacks based on a proposed IoT asset-based attack surface, which consists of four main components: physical objects, protocols covering the whole IoT stack, data, and software. They identified IoT attack taxonomy for each component and discussed a set of countermeasures. Salim et al. (2019) discussed the various DDoS attack methods and tools used to deploy botnet infected IoT devices in the cloud layer. They divided DDoS attacks into two categories: those affecting bandwidth (bandwidth depletion attacks) and those affecting resources (resource depletion attack). Bandwidth depletion attacks are further subclassified into amplification attacks and protocol exploit attacks, while resource depletion attacks are subdivided into protocol exploit attacks and malformed packet attacks.

Silva et al. (2020) analysed DDoS attacks based on application-layer, resource exhaustion, volumetric attacks. They also suggested a taxonomy of DDoS attack mitigation approaches featured by the software-defined networking (SDN) paradigm in IoT considering four key characteristics: mitigation process (centralised vs. collaborative); single vs. hybrid solutions; the mitigation strategy; and the targeting application. Mitigation strategies are classified based on IoT application, DDoS mitigation approach, mitigation strategy, types of attacks, and assessment methodology. Vishwakarma and Jain (2020) categorised IoT attacks into three types of attacks based on their attacking techniques: application layer, infrastructure layer, and zero-day attacks.

Referring to the aforementioned DDoS attacks taxonomies per technology, it is obvious that some attacks are very common across all technologies, i.e., in the techniques used to launch the attacks as well as the mitigation techniques used. However, for the cloud and IoT, and SCADA systems things become larger and sometimes require more complex mitigation techniques.

3 Proposed DDoS attacks taxonomy

In this section, we introduce an all-in-one inclusive taxonomy of DDoS attacks covering the aforementioned technologies: systems and networks, cloud computing, SCADA systems, and IoT. As Figure 3 shows, we divided the DDoS attacks into five attack strategies – flooding, exploitation, amplification, tampering, and jamming. The classification criteria are based on the techniques used to launch the DDoS attacks according to the following descriptions:

- Flooding attacks contain all attacks that target the systems with a huge volume of traffic.
- Exploitation attacks rely on software bugs or specific features that are used to consume system resources.

- Amplification attacks are those attacks that use protocol properties to amplify traffic toward the victim.
- Tampering attacks are based on creating and sending malformed packets to the victim.
- Jamming attacks target wireless networks by intentionally disrupting wireless communication among nodes.

For each strategy, we classify the considered attacks based on communication hierarchy by using the internet reference model (TCP/IP) and attacks per application and protocol. A description of each strategy and a list of main attacks are provided below:

3.1 Flooding

In this attack strategy, attackers try to send a very high volume of network traffic to victim machines or networked systems with the aim of bandwidth depletion. Currently, flooding attacks target most of the common internet protocols and services (Douligeris and Mitrokotsa, 2004; De Donno et al., 2018; Hoque et al., 2014; Mahjabin et al., 2017; Prasad et al., 2014; Jaafar et al., 2019; Alomari et al., 2012; Salim et al., 2019). Examples of such attacks are DNS flood and Stealth/Slow drip that targets the domain name service (DNS). *DNS flood* attempts to exhaust server-side assets (e.g., CPU, memory, network I/O, or disk I/O) with a flood of UDP requests, generated by scripts running on several compromised botnets, whereas *stealth/slow drip* uses queries sent to the attacker's authoritative domain that very slowly answers requests, just before the time out.

The web service is another rich environment to conduct flooding attacks. *HTTP GET*, *POST floods*, and *slowloris* are common types of DDoS attacks targeting the web service. In GET attack, many connection requests are sent to the Web server to deplete its processing resources, *HTTP post floods* continuously request single/multiple uniform resource locators (URLs) from many botnets, *slowloris* tries to keep many connections to the Web server open by sending the request periodically, it will send subsequent HTTP headers, adding to, but never completed the request. Message and media data floods and semantic level are common types of DDoS attacks that target the session initiation protocol (SIP). *Message flood* sends abnormal SIP session packets continuously in the same process used by SIP users or service providers to introduce some service latency and jitter by making server resources wasted and depriving it of delivering service to authorised users. In semantic level attacks, the user can automatically call non-responding callers in his/her contact list impersonating himself/herself as a legitimate owner.

Index poisoning and routing table poisoning target peer-to-peer (P2P) services. With *index poisoning*, the attacker inserts fake records into the P2P index system to announce that a well-known file is located at the victim's machine. *Routing poisoning* attempts to make the targeted node a neighbour of many P2P nodes. This can result in the targeted node receiving a huge volume of maintenance traffic, and hence be the victim of bandwidth depletion.

Flooding attacks target other critical internet-based services such as simple mail transfer protocol (SMTP), network time protocol (NTP), and secure sockets layer (SSL). In *SMTP flood*, many incoming emails following some sort of catastrophic event can be characterised to stop responding to requests in a reasonable amount of time. *NTP flood*

initiates a flood of illegitimate NTP requests from different zombies. The NTP server in turn will start processing the requests, and this leads to exhaust system and network resources. *SSL flood* attacks target the SSL handshake protocol by sending worthless data to the SSL server which will result in connection issues for legitimate users.

Transport layer protocols (UDP and TCP) are vulnerable to DDoS flooding attacks. *UDP flood* works primarily by exploiting the steps that a server takes when it responds to a UDP packet sent to one of its ports. The target's resources can become quickly exhausted when a large flood of UDP packets is received. With *UDP fragmentation* attack, the attacker overbears a network by exploiting datagram fragmentation mechanisms. These attacks involve the transmission of fraudulent UDP packets that are larger than the network's MTU, (usually ~1,500 bytes). *ACK*, *ACK-PUSH*, *RST-FIN*, *SYN*, and *SYN-ACK* floods are common DDoS attacks targeting the TCP protocol. These attacks exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. They mainly use flags within the TCP header to flood the targeted server with a huge volume of SYN, ACK, or RST floods.

Both IPv4 and IPv6 can be potential targets for some types of DDoS flooding attacks. In *ICMPv4 flood or ICMPv6 flood*, attackers attempt to overwhelm victims' machines by sending many Internet Control Message Protocol (ICMP) echo request packets using many botnets. The targeted server then sends an ICMP echo reply packet to each requesting device's IP address as a response. *Routing loop attack* takes advantage of inconsistencies between a tunnel's overlay IPv6 routing state and the native IPv6 routing state. The attacker exploits this by crafting a packet that is routed over a tunnel to a node that is not participating in that tunnel. The packet is routed back to the ingress point that forwards it back into the tunnel. Consequently, the packet will loop in and out of the tunnel. *Router advertisement (RAs) floods* the local network with fake random ICMPv6 packets to force devices using a specific network prefix, and specific routes for external IPv6 requests. Once the host receives an RA, it updates its entries with the received network prefix. The hosts might also multicast a router solicitation (RS) requesting to send RAs to acquire IPv6 routes. *Neighbour discovery* in IPv6 networks provides the possibility for connected nodes to configure their IP addresses and initiate communication with others without the need for registration or authentication. The receiving node must respond to it; therefore, the attackers can flood the network with any network discovery protocol (NDP) fake packets and hosts must blindly process all these packets.

Most network access layer protocols suffer from DDoS flooding attacks. In Ethernet (802.3), a *MAC flood* targets switch by feeding many Ethernet frames, each containing different source MAC addresses. Radio frequency identification (RFID) *reader flood* causes malfunction of RFID readers or making them disrupted by others. *SMS flood* paralyses cellular communications in a certain area by overloading standalone dedicated control channel (SDCCH) that carries signalling information following mobile to network connection establishment, and channel assignment by sending enough messages to potential target lists which can be a bottleneck in cellular networks due to its limited capacity and shared characteristics. *Dropping the acknowledgment signals* tries to drop all the arriving messages to force the system for creating new temporary mobile subscriber identity (TMSI) incoming subscribers. *Authentication request flood (Wi-Fi) floods* the access point (AP) with authentication requests. Every AP has a finite number of connection requests it can handle. After reaching this number the system might stop

accepting new connections. In *random access channel (RACH) floods*, the system sends a special message called system information block (SIB) to a mobile handset and instructs it to redirect its RACH signalling to a separate or a small part of the current RACH resource. This forces the RACH resources to be overloaded by single or multiple users.

3.2 Exploitation

DDoS attacks belonging to this category exploit some software bugs or specific features of the system's protocols, applications, and services to consume an excessive amount of the victim's or network's resources (De Donno et al., 2018; Huseinović et al., 2020; Kamal et al., 2017; Roohi et al., 2019; Abdul-Ghani et al., 2018; Salim et al., 2019; Jama and Khalifa, 2016). Examples of DDoS exploitation attacks are *HTTP fragmentation* where attackers establish a valid HTTP connection with a web server and then proceed to send his/her HTTP traffic to the server in multiple packets or small fragments as slowly as possible. Some web servers (such as Apache) have improper timeout mechanisms, and therefore allows for this behaviour. *NAT-buddy exploit* might be viewed as a variant of the index poisoning attack. It exploits a network address translation (NAT) traversal. In such a mechanism, a node behind a NAT could select a public node as its 'buddy'. When the NAT node publishes a file, information about the buddy is included in its published message to the index nodes. A node controlled by an attacker exploits this vulnerability by advertising the victim as its buddy.

Buffer-overflow attack exploits a software bug called 'buffer overflow' which gives programs the ability to overwrite other memory locations adjacent to the allocated buffer that should not have been modified intentionally or unintentionally. By exploiting this vulnerability, attackers can send more traffic to a network address than the programmers have built the system to handle. *TCP shrew attacks* exploit the TCP's retransmission timeout (RTO) where the attacker sends a burst of requests to a bottlenecked router at the same time when the victim sends requests to the target server, to force the router to suspend data transmission. This leads to a massive amount of packets' retransmission that significantly slows down the TCP session. *Duplicate address detection (DoS-on-DAD)* prevents a target host from getting an IP address by constantly transmitting network advertisement (NA) packets claiming that the generated IP address is not unique. Consequently, the target host will be unable to connect to the network due to the DAD process failure. *Queensland attack* works on the physical layer of 802.11 wireless LAN, specifically 802.11b and 802.11g protocols. One attack node can make all facilities using 802.11b protocol and lose the ability to communicate in the incidence of its signal. An *unauthorised tag disabling* attack causes RFID tags to assume a state from which they can no longer function properly. This results in the tags becoming either temporarily or permanently incapacitated. *AT commands exploitation attack* provides malicious users with the ability to disconnect IoT sensors from the network, or by making them join other malicious networks, and then forward the captured data to the attackers. *In a replay attack*, the process of transmitting data is fraudulently or maliciously delayed or repeated. Attackers perform this attack by intercepting and retransmitting the valid signed messages, where their validation is confirmed by a timestamp discrepancy fixed by both source and destination.

3.3 Amplification

Amplification – also referred to as reflection – attacks exploit network protocols or services to generate a message or multiple messages they receive to amplify traffic toward the victim's machine. Attacks belonging to this category can produce a considerable response as the attackers send smaller packets. Next, they will be amplified to generate a vast number of packets transmitted to the victim (Douligeris and Mitrokotsa, 2004; Mahjabin et al., 2017; Prasad et al., 2014; Alomari et al., 2012; Huseinović et al., 2020; Salim et al., 2019; Vishwakarma and Jain, 2020; Specht and Lee, 2004; Deshmukh and Devadkar, 2015; Wani et al., 2021). Examples of these attacks are *DNS amplification* which leverages the functionality of open DNS resolvers by sending small queries that result in large responses. By having each zombie in the botnet makes similar requests, the attackers can greatly increase the attack traffic. Similarly, in *Memcached attack*, attackers send spoofed requests to a vulnerable server, which then replies by sending a massive amount of data than the initial request, amplifying the traffic volume. *Attack with unidentified URLs* keeps the web server busy most of the time by forcing it to do non-significant activities and pushes the legitimate user traffic to wait. The effectiveness of this attack appears in synchronous DNS, where a well-established synchronous DNS server can drop requests exceeding thousands of messages per second. The *distributed reflective DoS (DRDoS) attacks* exploit weaknesses found in the open BitTorrent protocol being widely used to exchange files over the internet. DRDoS allows a single BitTorrent user with only modest amounts of bandwidth to send malformed requests to other BitTorrent users.

LDAP amplification attacks leverage the lightweight directory access protocol (LDAP) being widely used in Microsoft Active Directory for authentication purposes. The attackers can send very small requests to a vulnerable LDAP server to generate amplified replies, reflected to a target LDAP server. In *RPC amplification*, attackers exploit vulnerabilities found in the RPC Portmapper, where victims are sent copious amounts of responses from Portmapper servers, saturating bandwidth, and keeping web-based services unreachable. In *NTP amplification*, attackers send small NTP requests to the servers using spoofed IP addresses, resulting in a large number of NTP responses that flood the victim's NTP server. *SNMPv2 amplification* attacks target the simple network management protocol (SNMP) being widely used for network management. Many SNMP queries can be sent by attackers using spoofed IP addresses to a large number of connected devices that, in turn, respond to that faked address.

NetBIOS reflection targets the NetBIOS services, which is a software interface and a naming convention that includes a name service, often called WINS on Microsoft Windows operating systems. This attack generates more response traffic sent to the target than the initial queries sent by the attacker. *Simple service discovery protocol (SSDP) reflection* is a type of DDoS attack that targets the SSDP network protocol that leverages the Plug and Play (UPnP) mechanism that allows devices to send/receive massive amounts of information using the UDP. Vulnerable network devices will send a reply UPnP packets to the spoofed IP address of the victim's network to overwhelm it. *CLDAP reflection* attack leverages the advantage of the connectionless lightweight directory access protocol (CLDAP) by sending CLDAP requests to an LDAP server with a spoofed source IP address. The LDAP server will reply with bulked-up responses to the target's device. *CharGen reflection* attacks leverage the character generation service, in which

attackers can send a massive number of CHARGEN requests to many publicly accessible systems offering that service.

UDP amplification attacks exploit the stateless property in UDP protocol. An attacker can send a spoofed UDP packet to an intermediate server. The server is then instructed to send the response back to the victim's IP address instead of the attacker's IP. *Smurf attack* attempts to flood a targeted server with ICMP (ICMPv4 and ICMPv6) packets. By making requests with the spoofed IP address of the targeted device to one or more machines, the computer networks then respond to the targeted server, amplifying the initial attack traffic and potentially overwhelming the target, rendering it inaccessible. In a *routing header attack*, attackers can maliciously use IPv6 type (0) routing headers to bypass IPv6 access-list policies or anycast addressing and routing. These headers can be used to perform amplification attacks (ping-pong attacks that can cause link saturation and potential performance issues). *rSmurf attack* sends ECHO request packets from a multicast IPv6 address to deny the services from all targeted networks. The destination device, if exists, will reply by sending an ECHO reply packet using a multicast address. In *demand for a synchronisation* attack, the attacker can impersonate simultaneous and repeated requests to resynchronise the data flow for a group of users; it will then overwhelm the home resource register (HRL).

3.4 Tampering

The basic structure of these attacks is to send incorrectly formed IP packets – not following the protocol specifications – to the victims' machines to force them to demand additional processing resources for analysing the arriving traffic (Huseinović et al., 2020; Abdul-Ghani et al., 2018; Jama and Khalifa, 2016; Wani et al., 2021; Krishnan and Oliver, 2019). Examples are *HTTP malformed packets*, in which an attacker could exploit this flaw by creating a malicious HTTP packet and sending it to the target device, this might cause a buffer overflow condition on the target device, *SIP malformed* exploits VoIP services by sending non-standard messages (malformed SIP) with an intentionally wrong input. A *deregistration attack* sends a spoofed 'unregister' message to a SIP server and cancels the registration of the victim at that server. This prevents the victim user from receiving any calls.

Zero-day attacks exploit vulnerabilities previously unknown to security experts. If used when talking about popular software products, the term refers to security bugs of which their developers were previously unaware. In *land attacks*, attackers can send spoofed TCP SYN packets to the victim using the same port number for both source and destination. This forces the victim machine to send many replies to itself continuously. In *fragmented ACK attacks*, attackers send packets of 1,500 bytes long to the vulnerable server. This will give the attacker the ability to send a few packets with irrelevant information through the routers to consume all available bandwidth in the network. In a *TCP NULL attack*, attackers exploit the flags set in the TCP header format to send malformed packets with invalid TCP segment flags set information. The *ping of death* involves sending a malformed ICMP echo request (ping) that is larger than the maximum size of an IP packet. A *teardrop* is an attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap, leading to systems' crashes. In *IP null attack*, attackers send packets whereby the IPv4 header specifies the transport layer protocol and sets this field value to zero. In a *type of service (ToS) attack*,

attackers use the type of service 'ToS' in an IP header to spoof ECN packets to degrade the throughput of identical connections. The attacker can also utilise the differentiated services flags to leverage the priority of the malicious traffic over that of benign traffic. In an *ICMP fragmentation*, attackers send largely fragmented – greater than 1,500 bytes – and highly spoofed ICMP packets at a high data rate. Consequently, these useless packets cannot be reassembled at the destination side causing a large waste of computing resources.

In *IP packet option field attack*, attackers can produce incomplete or malformed packets by misconfiguring some of the IP header option fields. *Redirect attack* is the ability to cause packets to be sent to a place that is not tied to the transport and/or application layer protocol's notion of the peer. An attacker might learn the contents of a particular flow by redirecting it to a location where the attacker changes the packets and then forwards them to the ultimate destination. *Malformed router header attacks leverage* RS messages and RA messages to flood the network with malformed prefix advertisements that can cause traffic interruption and routing storms. *IPv6 fragmentation attack* abuses the IPv6 fragmentation mechanism in such a way that IPv6 header chain of the attackers' packets is fragmented into multiple fragments, where the first one might not contain the required information about the upper layer protocols such as UDP and TCP.

Deauthentication attack works at the data link layer and tries to send, using a spoofed victim's MAC address, unencrypted deauthentication frames to a wireless access point (WAP). Here, attackers only need to know the victim's MAC address which can be easily obtained using sniffing tools. *Authentication modification* exploits the radio network controller (RNC) by getting malformed messages from the attackers to terminate the connection between the legitimate users and the subscriber. *Baseband processor attacks* exploit Baseband vulnerabilities by giving attackers the possibility to craft a mobile phone's communications to extract some sensitive information, send some premium SMS messages, or cause a huge volume of data transfers unperceived by the phone's user.

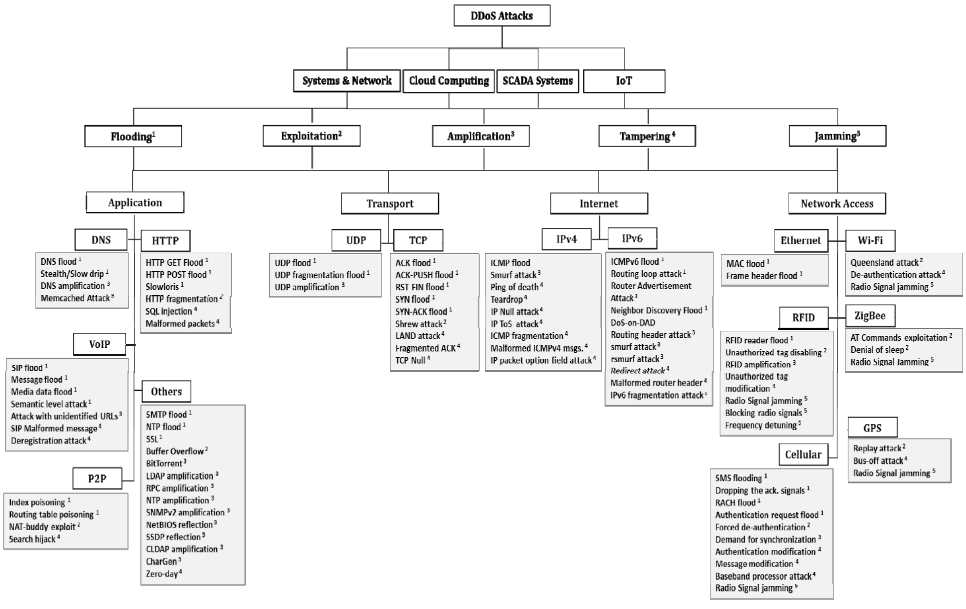
3.5 Jamming

Since most wireless devices are using radio frequency (RF) signals to communicate with others, this signal can be jammed with other stronger signals with intentional disruption of communication. The attacker intercepts and denies communication between the sensor, or tag, and the reader of transmitted data. In this electromagnetic jamming is done to prevent tags from communicating with the reader. Jamming attacks rely on modification of signals transmitted between communicating devices which may, on the receiver/sender side, result in a malfunction due to false interpretation of signals (Huseinović et al., 2020; Sonar and Upadhyay, 2014; Khader and Eleyan, 2021; Abughazaleh et al., 2020; Abdul-Ghani et al., 2018; Manju and Sasi, 2012; Džaferović et al., 2019).

Jamming attacks target the first two layers of the TCP/IP reference model, namely the physical and the medium access control (MAC) layers. Most media access protocols suffer from radio signal jamming that disturbs data transmission by broadcasting interference signals to a wireless channel. Examples of DDoS jamming attacks are radio signal jamming [Wi-Fi, RFID, ZigBee, cellular, global positioning system (GPS), *blocking radio signals*, and *frequency detuning*]. By emitting very strong interference signals, the jamming attackers can significantly decrease the signal noise ratio (SNR),

which in turn prevents the receiving node from correctly detecting intransient packets. In physical-layer attacks, the jamming attackers are not required to follow the wireless protocol. Whereas in MAC-layer attacks, both the sending node and the jamming attackers operate on the same channel, with the overall aim is to introduce packets' collisions. Under jamming attacks, packets transmitted to the receiving node might get corrupted and produce invalid checksum used in the protocol. Frequency detuning also operates in an inherently noisy and unstable environment, their communication is susceptible to possible signal interference and collisions from any source of radio interference that impairs or even blocks the radio signal and leads to RF detuning.

Figure 3 The proposed taxonomy of DDoS attacks



4 DDoS attacks countermeasures

DDoS attack countermeasures were classified according to different criteria. The main criterion was based on the phases of the actions related to the time the attack occurs (Mahjabin et al., 2017; Ramanauskaite and Cenys, 2011; Papadie and Apostol, 2017; Gupta and Dahiya, 2021). Accordingly, we classify DDoS countermeasures according to the time the countermeasure is applied related to the time the attack is launched. Hence, we adopted four categories namely prevention, detection, response, and tolerance. These categories are described below.

4.1 Prevention

It involves the steps carried out to avoid DDoS attacks before they occur. Many techniques are used in this stage including filtering, load balancing, honeypot,

demilitarised zone (DMZ), and awareness as well. Prevention techniques are described below (Ramanujan and Varghese, 2021).

- *Filtering* is the process of dropping out packets to ensure that only legitimate traffic passes through routers. This technique works for spoofed IP addresses and has some limitations regarding actual IP addresses (Patgiri et al., 2018; Pack et al., 2016). Ingress/egress, hop count, history-based, packet score, router-based filtering, and source address validity are filtering methods used in DDoS prevention.
- *Load balancing* refers to balancing the load between different systems to ensure that no system is overloaded, it requires a bandwidth increase and a sufficient number of replicate servers (Belyaev and Gaivoronski, 2014; Zebari et al., 2020).
- *Honeypot/honeynet* establishes an attractive and less secure system to lure the attacker to attack it instead of the actual system. However, the static and passive nature of honeynet may cause the attacker to learn that fact (Gupta and Gupta, 2017; Hasan and Hassan, 2020).
- *Security overlay/demilitarised zone* (*DMZ*) builds a network on top of an IP network to work as a buffer between external networks and the inner private network. It is only applicable for private networks and does not fit for public servers (Patel, 2020).
- *Awareness* takes preventive measures by generic users in their systems, and it is a user-centric approach. Awareness tips may include changing IP address, disable unused services, patches, etc. (Li et al., 2020).

4.2 Detection

It involves the steps carried out to detect DDoS attacks that are running. The techniques are either anomaly-based or signature-based detection methods that aim at reporting an active DDoS attack being carried out (Khraisat et al., 2019; Wu et al., 2018). Signature-based detects an attack by comparing well-known attack signatures, or patterns, against monitored traffic signature and is fast in detection time and detects most known attacks, however, it has low false positive (FP) rates. Signature-based methods include MIB, SNORT, and spectral analysis (Badotra and Panda, 2021). *Anomaly-based techniques* compare the network traffic behaviour against previous normal traffic behaviour, it requires training and can detect unknown attacks, but it has higher FP rates. Behaviour-based methods include Multops and DWARD (Kaur et al., 2017; Prasad et al., 2020).

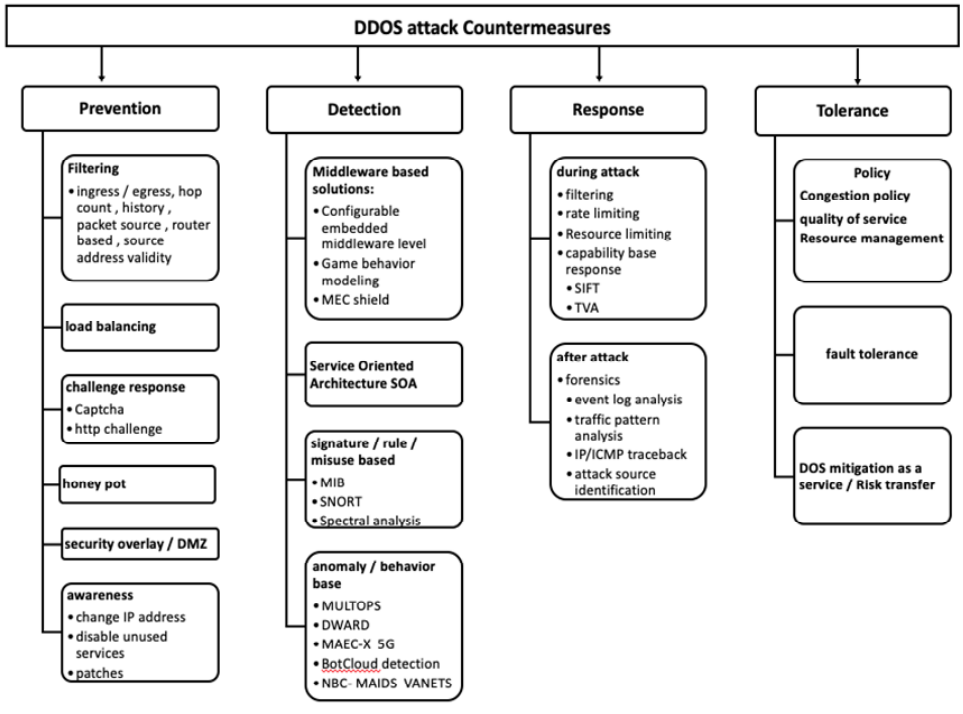
4.3 Response

It involves the steps carried out to counterfeit DDoS attacks and stop them. The response process can be divided into two stages based on the time the response is carried out, during attack response, and after attack response. These techniques are described below:

- *During attack response* is the response carried out during the attack and it involves filtering (Gulihar and Gupta, 2020), rate-limiting (Nur, 2021), and capability-based response which includes stateless interflow filter (SIFT) (Pascoal et al., 2017) and traffic validation architecture (TVA) (Osterweil et al., 2020).

- *After attack response* is carried out after the attack has occurred and mainly focuses on Forensics to identify the intrusions and their sources. It involves inspecting malicious activity and examining networks and systems for anomalous traffic to identify intrusions. Sometimes, this stage is called the deterrence stage. Methods include event log analysis, traffic pattern analysis, IP/ICMP traceback, and attack source identification (Tu et al., 2012; Sarmento et al., 2021).

Figure 4 The proposed taxonomy of DDoS attacks countermeasures



4.4 Tolerance

It is the last stage and implies strategies carried out to reduce the effect of DDoS attacks when the previous steps are of no use. This stage focuses on providing the maximum possible quality of service (QoS) while minimising the effect of the attacks, it mainly deals with congestion policy and fault tolerance techniques. Methods include congestion policy (re-feedback) and NetFense (Deka et al., 2021), and fault tolerance (Bergs et al., 2021).

To provide an overall picture of the DDoS countermeasures, we summarise the aforementioned stages and techniques in Figure 4 which form the basis of the DDoS countermeasure taxonomy we explained.

5 Conclusions and future work

In this paper, we conducted an intensive survey about DDoS attacks, their taxonomy, and countermeasures. To come up with a clear understanding and come up with a big picture for DDoS taxonomy, we conducted our survey on four emerging technologies: systems and networks, cloud computing, SCADA systems, and IoT. In this survey, we investigated most of the state-of-the-art works about DDoS attacks in these four technologies and their countermeasures.

A taxonomy for DDoS attacks in these categories was generated and populated with well-known attacks in each category. DDoS attack countermeasures were also studied, and a comprehensive model was proposed. The model was adapted to be applicable for these categories. Modern mitigation techniques related to each countermeasure classification category were proposed as well. To the best of the authors' knowledge, this work is the first work that adapted a DDoS attack taxonomy and countermeasures in systems and networks, cloud computing, SCADA systems, and IoT. The findings of this work will be used to conduct experimental results and develop metrics for DDoS mitigations techniques considering the big picture of these attacks.

References

Abdul-Ghani, H.A., Konstantas, D. and Mahyoub, M. (2018) 'A comprehensive IoT attacks survey based on a building-blocked reference model', *International Journal of Advanced Computer Science and Applications*, Vol. 9, No. 3, pp.355–373.

Abughazaleh, N., Bin Jabal, R., Btish, M. and Hemalatha, M. (2020) 'DoS attacks in IoT systems and proposed solutions', *International Journal of Computer Applications*, Vol. 176, No. 33, pp.16–19.

Alomari, E., Manickam, S., Gupta, B.B., Karuppayah, S. and Alfaris, R. (2012) *Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art*, arXiv preprint arXiv:1208.0403.

Badotra, S. and Panda, S.N. (2021) 'SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking', *Cluster Computing*, Vol. 24, No. 1, pp.501–513.

Baskar, M., Ramkumar, J., Karthikeyan, C., Anbarasu, V., Balaji, A. and Arulananth, T.S. (2021) 'Low rate DDoS mitigation using real-time multi threshold traffic monitoring system', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No. 1, pp.1–9.

Belyaev, M. and Gaivoronski, S. (2014) 'Towards load balancing in SDN-networks during DDoS-attacks', in *2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC)*, IEEE pp.1–6.

Bergs, C.J., Bruiners, J., Fakier, F. and Stofile, L. (2021) 'Cyber security and wind energy: a fault-tolerance analysis of DDoS attacks', in *ICCWS 2021 16th International Conference on Cyber Warfare and Security*, Academic Conferences Limited, p.443.

Bhatia, S., Behal, S. and Ahmed, I. (2018) 'Distributed denial of service attacks and defense mechanisms: current landscape and future directions', in Conti, M., Somani, G. and Poovendran, R. (Eds.): *Versatile Cybersecurity. Advances in Information Security*, pp.55–97, Springer, Cham, Switzerland, DOI: 10.1007/978-3-319-97643-3_3.

Campbell, P.L. (2005) 'The denial-of-service dance', *IEEE Security & Privacy*, Vol. 3, No. 6, pp.34–40.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems', *Computers & Security*, Vol. 56, pp.1–27.

Dahiya, A. and Gupta, B.B. (2021) 'A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense', *Future Generation Computer Systems*, Vol. 117, pp.193–204.

Darwish, M., Ouda, A. and Capretz, L.F. (2013) 'Cloud-based DDoS attacks and defenses', in *International Conference on Information Society (i-Society 2013)*, IEEE, pp.67–71.

De Donno, M., Dragoni, N., Giaretta, A. and Spognardi, A. (2018) 'DDoS-capable IoT malwares: comparative analysis and Mirai investigation', *Security and Communication Networks*.

Deka, R.K., Bhattacharyya, D.K. and Kalita, J.K. (2021) 'DDoS attacks: tools, mitigation approaches, and probable impact on private cloud environment', *Big Data Analytics for Internet of Things*, pp.285–319, Chapter 13, Wiley Online Library.

Deshmukh, R.V. and Devadkar, K.K. (2015) 'Understanding DDoS attack & its effect in cloud environment', *Procedia Computer Science*, Vol. 49, pp.202–210.

Ding, D., Han, Q.L., Ge, X. and Wang, J. (2020) 'Secure state estimation and control of cyber-physical systems: a survey', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 51, No. 1, pp.176–190.

Douligeris, C. and Mitrokotsa, A. (2004) 'DDoS attacks and defense mechanisms: classification and state-of-the-art', *Computer Networks*, Vol. 44, No. 5, pp.643–666.

Džaferović, E., Sokol, A., Abd Almisreb, A. and Norzeli, S.M. (2019) 'DoS and DDoS vulnerability of IoT: a review', *Sustainable Engineering and Innovation*, Vol. 1, No. 1, pp.43–48.

East, S., Butts, J., Papa, M. and Shenoi, S. (2009) 'A taxonomy of attacks on the DNP3 protocol', in *International Conference on Critical Infrastructure Protection*, pp.67–81, Springer, Berlin, Heidelberg.

Ferrag, M.A., Babaghayou, M. and Yazici, M.A. (2020) 'Cyber security for fog-based smart grid SCADA systems: solutions and challenges', *Journal of Information Security and Applications*, Vol. 52, p.102500.

Gerber, L. (2000) 'Denial of service attacks rip the internet', *IEEE Computer*, April, Vol. 33, No. 4, pp.12–17.

Gulihar, P. and Gupta, B.B. (2020) 'Cooperative mechanisms for defending distributed denial of service (DDoS) attacks', in *Handbook of Computer Networks and Cyber Security*, pp.421–443, Springer, Cham.

Gupta, A. and Gupta, B.B. (2017) 'Honeynettrap: framework to detect and mitigate DDoS attacks using heterogeneous honeynet', in *2017 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, pp.1906–1911.

Gupta, B.B. and Dahiya, A. (2021) *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*, 1st ed.; CRC Press: Boca Raton, FL, USA.

Hameed, S., Khan, F.I. and Hameed, B. (2019) 'Understanding security requirements and challenges in internet of things (IoT): a review', *Journal of Computer Networks and Communications*, Vol. 2019, article ID 9629381.

Hansman, S. (2003) *A Taxonomy of Network and Computer Attack Methodologies*, Supervisor Ray Hunt, Department of Computer Science and Software Engineering, University of Cantebury, Christchurch, New Zealand, November.

Hasan, M.M. and Hassan, M.H. (2020) 'A three layer security approach using honeypot to mitigate DDoS attack in cloud-IoT ecosystem', *International Educational Applied Scientific Research Journal*, Vol. 5, No. 12, pp.16–19.

Hindy, H., Brosset, D., Bayne, E., Seeam, A.K., Tachtatzis, C., Atkinson, R. and Bellekens, X. (2020) 'A taxonomy of network threats and the effect of current datasets on intrusion detection systems', *IEEE Access*, Vol. 8, No. 2020, pp.104650–104675.

Hindy, H., Hodo, E., Bayne, E., Seeam, A., Atkinson, R. and Bellekens, X. (2018) 'A taxonomy of malicious traffic for intrusion detection systems', in *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, IEEE, June, pp.1–4.

Hoque, N., Bhuyan, M.H., Baishya, R.C., Bhattacharyya, D. and Kalita, J. (2014) 'Network attacks: taxonomy, tools and systems', *J. Netw. Comput. Appl.*, Vol. 40, pp.307–324.

Howard, J.D. and Longstaff, T.A. (1998) *A Common Language for Computer Security Incidents*, No. SAND98-8667, Sandia National Labs., Albuquerque, NM, USA; Sandia National Labs., Livermore, CA, USA.

Huseinović, A., Mrdović, S., Bicakci, K. and Uludag, S. (2020) 'A survey of denial-of-service attacks and solutions in the smart grid', *IEEE Access*, Vol. 8, pp.177447–177470.

Jaafar, G.A., Abdullah, S.M. and Ismail, S. (2019) 'Review of recent detection methods for HTTP DDoS attack', *Journal of Computer Networks and Communications* [online] https://doi.org/10.1155/2019/1283472.

Jama, A.M. and Khalifa, O.O. (2016) 'Review of SIP based DoS attacks', *International Journal of Computer Applications Technology and Research*, Vol. 5, No. 12, pp.775–781.

Kamal, P., Abuhussein, A. and Shiva, S. (2017) 'Identifying and scoring vulnerability in SCADA environments', in *Future Technologies Conference (FTC)*, pp.845–857.

Kaur, P., Kumar, M. and Bhandari, A. (2017) 'A review of detection approaches for distributed denial of service attacks', *Systems Science & Control Engineering*, Vol. 5, No. 1, pp.301–320.

Kesavamoorthy, R., Alaguvathana, P., Suganya, R. and Vigneshwaran, P. (2020) 'Classification of DDoS attacks – a survey', *Test Eng. Manag.*, Vol. 83, pp.12926–12932.

Khader, R. and Eleyan, D. (2021) 'Survey of DoS/DDoS attacks in IoT', *Sustainable Engineering and Innovation*, Vol. 3, No. 1, pp.23–28.

Khraisat, A., Gondal, I. and Vamplew, P. (2019) 'Survey of intrusion detection systems: techniques, datasets and challenges', *Cybersecurity*, Vol. 2, p.20.

Kim, S., Heo, G., Zio, E., Shin, J. and Song, J.G. (2020) 'Cyber attack taxonomy for digital environment in nuclear power plants', *Nuclear Engineering and Technology*, Vol. 52, No. 5, pp.995–1001.

Krishnan, S. and Oliver, J.J.E. (2019) 'Mitigating DDoS attacks in software defined networks', in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, pp.960–963.

Kumar, V. and Kumar, K. (2016) 'Classification of DDoS attack tools and its handling techniques and strategy at application layer', in *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)*, IEEE, Fall, pp.1–6.

Lankatilake, K.K. (2019) 'A taxonomy-based analysis of attacks on industrial control systems'.

Li, J., Yi, X. and Wei, S. (2020) 'A study of network security situational awareness in internet of things', in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, pp.1624–1629.

Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017) 'A survey of distributed denial-of-service attack, prevention, and mitigation techniques', *International Journal of Distributed Sensor Networks*, Vol. 13, No. 12, p.1550147717741463.

Manju, V.C. and Sasi, K.M. (2012) 'Detection of jamming style DoS attack in wireless sensor network', in *The 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, IEEE, pp.563–567.

Mirkovic, J. and Reiher, P. (2004) 'A taxonomy of DDoS attack and DDoS defense mechanisms', *ACM SIGCOMM Computer Communication Review*, Vol. 34, No. 2, pp.39–53.

Mishra, A., Gupta, N. and Gupta, B.B. (2021) 'Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller', *Telecommunication Systems*, Vol. 77, No. 1, pp.47–62.

Mohan, A.M., Meskin, N. and Mehrjerdi, H. (2020) 'A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems', *Energies*, Vol. 13, No. 15, p.3860.

Nagpal, B., Sharma, P., Chauhan, N. and Panesar, A. (2015) 'DDoS tools: classification, analysis and comparison', in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, pp.342–346.

Nur, A.Y. (2021) 'Combating DDoS attacks with fair rate throttling', in *2021 IEEE International Systems Conference (SysCon)*, IEEE, pp.1–8.

Osterweil, E., Stavrou, A. and Zhang, L. (2020) '21 years of distributed denial-of-service: a call to action', *Computer*, Vol. 53, No. 8, pp.94–99.

Pack, G., Yoon, J., Collins, E. and Estan, C. (2006) 'On filtering of DDoS attacks based on source address prefixes', in *2006 Securecomm and Workshops*, IEEE, pp.1–12.

Papadie, R. and Apostol, I. (2017) 'Analyzing websites protection mechanisms against DDoS attacks', in *The 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, pp.1–6.

Pascoal, T.A., Dantas, Y.G., Fonseca, I.E. and Nigam, V. (2017) 'Slow TCAM exhaustion DDoS attack', in *IFIP International Conference on ICT Systems Security and Privacy Protection*, Springer, Cham, pp.17–31.

Patel, M. (2020) *Demilitarized Zone: An Exceptional Layer of Network Security to Mitigate DDoS Attack*, Doctoral dissertation, University of Windsor, Canada, University of Windsor Digital Archive [online] https://scholar.uwindsor.ca/cgi/viewcontent.cgi.

Patgiri, R., Nayak, S. and Borgohain, S.K. (2018) *Preventing DDoS using Bloom Filter: A Survey*, arXiv preprint arXiv:1810.06689.

Pliatsios, D., Sarigiannidis, P., Lagkas, T. and Sarigiannidis, A.G. (2020) 'A survey on SCADA systems: secure protocols, incidents, threats and tactics', *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 3, pp.1942–1976.

Prasad, K.M., Reddy, A.R.M. and Rao, K.V. (2014) 'DoS and DDoS attacks: defense, detection and traceback mechanisms – a survey', *Global Journal of Computer Science and Technology*, Vol. 14, No. 7, Ver. 1.0, pp.15–32.

Prasad, K.M., Reddy, A.R.M. and Rao, K.V. (2020) 'BARTD: bio-inspired anomaly based real time detection of under rated app-DDoS attack on web', *Journal of King Saud University-Computer and Information Sciences*, Vol. 32, No. 1, pp.73–87.

Rakas, S.V.B., Stojanović, M.D. and Marković-Petrović, J.D. (2020) 'A review of research work on network-based SCADA intrusion detection systems', *IEEE Access*, Vol. 8, pp.93083–93108.

Ramanauskaite, S. and Cenys, A. (2011) 'Taxonomy of DoS attacks and their countermeasures', *Central European Journal of Computer Science*, Vol. 1, No. 3, pp.355–366.

Ramanujan, A. and Varghese, B.A. (2021) 'A survey on DDoS prevention, detection, and traceback in cloud', in *Second International Conference on Networks and Advances in Computational Technologies*, Springer, Cham, pp.69–82.

Ravi, N. and Shalinie, S.M. (2020) 'Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture', *IEEE Internet of Things Journal*, Vol. 7, No. 4, pp.3559–3570.

Roohi, A., Adeel, M. and Shah, M.A. (2019) 'DDoS in IoT: A roadmap towards security & countermeasures', in *2019 25th International Conference on Automation and Computing (ICAC)*, IEEE, pp.1–6.

Salim, M.M., Rathore, S. and Park, J.H. (2019) 'Distributed denial of service attacks and its defenses in IoT: a survey', *The Journal of Supercomputing*, Vol. 76, No. 7, pp.5320–5363.

Sarmento, A.G., Yeo, K.C., Azam, S., Karim, A., Al Mamun, A. and Shanmugam, B. (2021) 'Applying big data analytics in DDoS forensics: challenges and opportunities', in *Cybersecurity, Privacy and Freedom Protection in the Connected World*, pp.235–252, Springer, Cham.

Silva, F.S.D., Silva, E., Neto, E.P., Lemos, M., Neto, A.J.V. and Esposito, F. (2020) 'A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios', *Sensors*, Vol. 20, No. 11, p.3078.

Singh, J. and Behal, S. (2020) 'Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions', *Computer Science Review*, Vol. 37, p.100279.

Sonar, K. and Upadhyay, H. (2014) 'A survey: DDOS attack on internet of things', *International Journal of Engineering Research and Development*, Vol. 10, No. 11, pp.58–63.

Specht, S.M. and Lee, R.B. (2004) 'Distributed denial of service: taxonomies of attacks, tools, and countermeasures', *ISCA PDCS.*

Tu, M., Xu, D., Butler, E. and Schwartz, A. (2012) 'Forensic evidence identification and modeling for attacks against a simulated online business information system', *Journal of Digital Forensics, Security and Law*, Vol. 7, No. 4, p.4.

Veluri, R.K., Raghuvanshi, A., Singh, U.K., Panse, P. and Saxena, M. (2021) 'Internet of things: taxonomy of various attacks', *European Journal of Molecular & Clinical Medicine*, Vol. 7, No. 10, pp.3853–3864.

Vishwakarma, R. and Jain, A.K. (2020) 'A survey of DDoS attacking techniques and defence mechanisms in the IoT network', *Telecommunication Systems*, Vol. 73, No. 1, pp.3–25.

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K.M., Almotairi, S. and Gulzar, Y. (2021) 'Distributed denial of service (DDoS) mitigation using blockchain – a comprehensive insight', *Symmetry*, Vol. 13, No. 2, p.227.

Wu, D., Li, J., Das, S.K., Wu, J., Ji, Y. and Li, Z. (2018) 'A novel distributed denial-of-service attack detection scheme for software defined networking environments', in *2018 IEEE International Conference on Communications (ICC)*, IEEE, pp.1–6.

Yadav, G. and Paul, K. (2021) 'Architecture and security of SCADA systems: a review', *International Journal of Critical Infrastructure Protection*, Vol 34, p.100433.

Zebari, R.R., Zeebaree, S.R., Sallow, A.B., Shukur, H.M., Ahmad, O.M. and Jacksi, K. (2020) 'Distributed denial of service attack mitigation using high availability proxy and network load balancing', in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, IEEE, pp.174–179.

Zhu, B., Joseph, A. and Sastry, S. (2011) 'A taxonomy of cyber attacks on SCADA systems', in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, IEEE, pp.380–388.