International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 6
ISSN: 2088-5334

# A Comprehensive Review of DNS-based Distributed Reflection Denial of Service (DRDoS) Attacks: State-of-the-Art

Riyadh Rahef Nuiaa [a,b], Selvakumar Manickam [b,*], Ali Hakem Alsaeedi [c]

[a] *Department of Computer, College of Education for Pure Sciences, Wasit University, Iraq*
[b] *National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia*
[b] *College of Computer Science and Information Technology, University of Al-Qadisiyah, Iraq*
*Corresponding author: *selva@usm.my*

***Abstract*— Cyberattacks significantly impact the services based on the internet that is used in our daily lives. Any disruption will make it extremely difficult for us to carry out our daily activities. Cyberattacks will disrupt online services, exploit vulnerabilities to breach databases and servers, and so on. Various systems and services contribute to the Internet's seamless functionality. The Domain Name System (DNS) is one of the most important services. DNS is used to resolve domain names into machine-readable IP addresses. DNS, like many other Internet services, is vulnerable to cyber-attacks. While DNS faces a slew of threats, one in particular appears to stand out. DNS is vulnerable to a variety of distributed denial-of-service attacks. The distributed reflection denial of service (DRDoS) attack, a flooding attack against DNS servers that renders them unavailable, disrupting domain name resolution activities, is one of the most common variants. DRDoS attacks have been on the rise in recent years. DNS lookup outages would significantly impact our online activities in the world of ultra-connectivity because they are typically the first step in establishing a connection with a server. The purpose of this paper is to present a state-of-the-art review of DRDoS attack detection and mitigation algorithms as well as the datasets on which these algorithms operate. Finally, we discussed each of these algorithms' relative merits and demerits.**

***Keywords*— DNS DRDoS attacks; DNS amplification attack; DNS reflection attack; DNS threats; DNS DDoS attacks.**

*Manuscript received 13 Feb. 2022; revised 22 May 2022; accepted 6 Jun. 2022. Date of publication 31 Dec. 2022.*


## I. INTRODUCTION

Unlike the web, email, and chat, the majority of users are unaware of DNS, even though DNS is critical to the Internet's operation. DNS' primary function is to resolve hostnames to their associated IP addresses, similar to how phone books look up and resolve names to phone numbers. Nonetheless, DNS's archaic design has left it vulnerable to cyber-attacks. Due to the unpredictable nature of these threats, they cannot be avoided or mitigated [1], [2]. Occasionally, vulnerabilities within these services may result in widespread attacks, resulting in service degradation or unavailability. While a DRDoS attack is a variant of a DDoS attack, the mechanisms for detecting and mitigating DDoS attacks do not apply to DRDoS attacks due to the complexity of attacking DNS servers. This is the most potent and destructive type of attack that attackers are capable of committing. As a result, the attackers conceal their identity and amplify responses in which the attack vector uses infected hosts to launch and maximize the damage caused by the attack. Due to the protocol's widespread use, the DNS service is vulnerable to a variety of threats [3]. Therefore, this paper focuses solely on the amplification attack on DNS issues and the difficulty in distinguishing between legitimate usage and the attack [4]. The authors used well-known publishers to prepare this comprehensive review, as shown in Figure 1, and updated references in Figure 2. Consequently, these two points are regarded as strengths of our research and a challenge in conducting a comprehensive review of the most recent research papers on DRDoS DNS attacks and analyzing them by highlighting their strengths and weaknesses. To focus researchers' attention and focus on the weaknesses and try to find solutions and improve them.

### A. Motivation

The massive and accelerating growth of DNS-targeting attacks, particularly DRDoS attacks, has become apparent to those interested in DNS security. The tactics and method of attack, as well as the effects on the victim side, distinguish these types from other DDoS attacks. In the DRDoS attacks

against the DNS, the attackers focused on exploiting security vulnerabilities in the DNS and misusing them, transforming them into a new tool for launching and maximizing their attacks.

Several mechanisms are in place to detect and mitigate the impact of these attacks. However, each of these mechanisms has both strengths and weaknesses. The detection side, the magnitude of the network traffic, the time to launch the alert when the attack occurs, and the environment in which the technique is built and implemented are all used to evaluate the mechanism. These reasons served as the foundation for this research, which provided a comprehensive review of the mechanisms used to detect and respond to these types of DNS-targeted attacks and highlighted each approach's strengths and weaknesses.

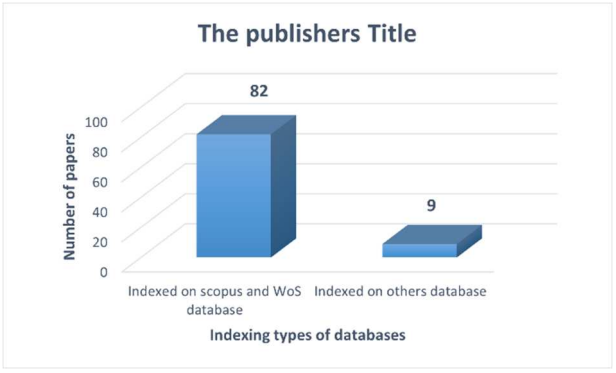


Fig. 1 The publisher


Fig. 2 The years of publishing papers

## B. Paper Organization

The remainder of the paper is organized as follows. Section II provides an overview of the different types of DNS attacks. Section III focuses on DNS Distributed Reflection Denial of Service attacks and their mechanics. Section IV describes the defense mechanisms used to detect DNS DRDoS attacks. Section V contains the conclusion.

## II. Materials and Method

To distinguish between legitimate and malicious requests, any mechanism used to prevent and mitigate such attacks must not also block access from legitimate users and issues based on the Confidentiality, Integrity, and Availability (CIA) model [5]. It is understood that DNS security issues mainly affect the availability aspect of the CIA model. Other lesser-known threats to the DNS service involve stealing user information via a stealth attack. Therefore, we classify DNS threats, as shown in Figure 3, into four categories [3],[6],[7]:

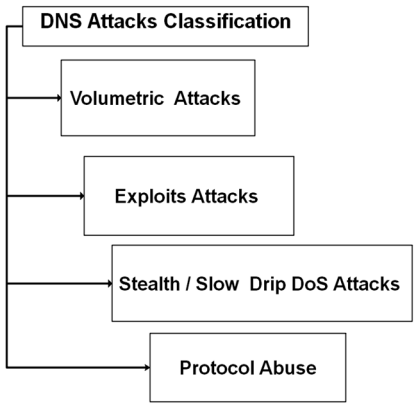


Fig. 3 DNS attacks classification

## A. Volumetric Attacks

DNS-based DDoS attacks seek to exhaust server resources, resulting in a denial of service. For example, sending a large number of requests from a single source or distributed origins in an attempt to flood the DNS server until the DNS server is saturated or overloaded with requests, at which point the service is terminated or deteriorates.

Volumetric attacks are a type of DDoS attack based on the size of the attacks that target the victim. The scenario for this type of attack can begin by flooding the prey with massive amounts of traffic until the server becomes saturated and unresponsive [8]. As a result, legitimate users cannot access network resources and services, or access will be very slow or intermittent. This type of attack consumes the victim's bandwidth by overloading via sending a large amount of traffic to this prey [1],[9]. The volumetric attack occurs when DNS focuses on exhausting the host's available bandwidth. When the attack is successful, the legal users do not receive any response from the DNS hosts because the legal DNS queries are dropped. Volumetric attacks are classified into four sub-types [2]. Figure 4 shows the frequency of different types of DDoS attacks from January 2020 to March 2021. As can be seen, volumetric attacks have grown rapidly in comparison to other attack types [3].

*1) Direct DNS DoS Attack (flooding)*: The server targets this type of flooding attack. The attacker sends numerous bogus requests to overburden system resources and network bandwidth. At this point, all incoming DNS server requests cannot be processed, and the server is unable to respond. A dedicated firewall detects this type of attack [4],[5].

*2) DNS Amplification Attack (DDoS):* The DNS amplification attack is a DDoS attack variant that is quite sophisticated with devastating consequences [6]. This attack is carried out on open DNS servers by overwhelming the prey's network bandwidth with the fake DNS reply traffic and its CPU or memory [7]. This reply message of DNS is more extensive than the demand in this type of attack [10]. This DNS traffic is directed at the targeted victim [11]. The IP address of the prey used to launch the attack is typically spoofed to hide the perpetrator's location [12]. To launch the attack, the attacker employs a large number of harmless intermediate nodes known as reflectors [13]. For a successful

attack, the bandwidth must be amplified during the attack, relying on botnets' DNS [14]. When a DDoS attack is based on the amplification of a DNS attack, a massive amount of traffic and the prey will be restricted to counter this attack [15],[16]. A botnet is commonly used in DNS attacks to increase the attack's effectiveness [17],[18]. As previously stated, a botnet is a global army of infected machines that primarily use social engineering techniques under the control of a botmaster to carry out numerous attacks. A botnet can be used to carry out DNS DDoS attacks in our case [19]. The recursive request function supported by the open Internet is a security problem if the server responds to it and will be employed to amplify DNS attacks [20]. Figure 5 shows the distribution of DDoS Attack Vectors, Q2 2019. We can see that DNS amplification attacks at the top of the chart are rapidly increasing compared to other DDoS attacks [21].

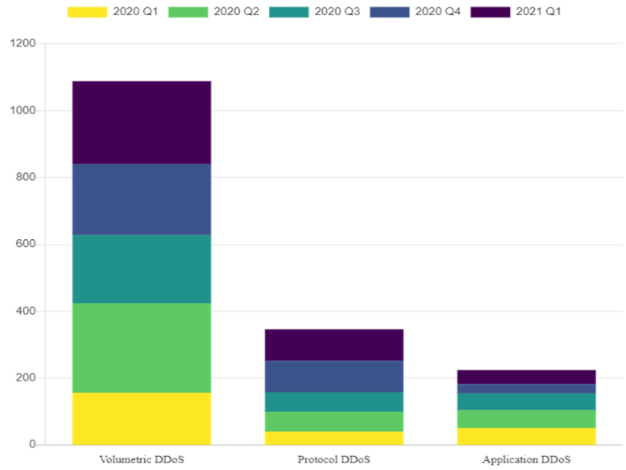


Fig. 4 Frequency of DDoS attack types, January 2020 through March 2021

*3) DNS Reflection Attack*: focuses on the open resolver and authoritative servers by flooding them with requests to consume the bandwidth and drain it. It can also be used to launch reflection attacks. It is a strategy that entails launching a DDoS attack against a DNS server in order to reduce the network's resources and infrastructure availability. The attacker must meet two requirements to execute a DNS reflection attack: the first is spoofing the IP address of the attacked endpoint, and the second is that the attacker must generate replies that are greater than the demand by multiple folds [22],[23]. The attacker gradually increases the request size by modifying the parameters of the EDNS extension mechanisms [24],[25]. As a result, the DNS servers receive a large number of DNS requests sent by the attacker with the original IP address spoofing as the prey is [26]. The exploit of low-secure resolvers, openly accessible by all Internet users, amplifies the DNS reflection attack [27]. The source address of UDP is exploited in the reflection attack on DNS, and requests and responses of DNS are asymmetric [28]. Figure 6 shows the frequency of different DDoS attack tactics from January 2020 to March 2021. As we can see, DNS Reflection attacks are constantly increasing alongside other types [3].

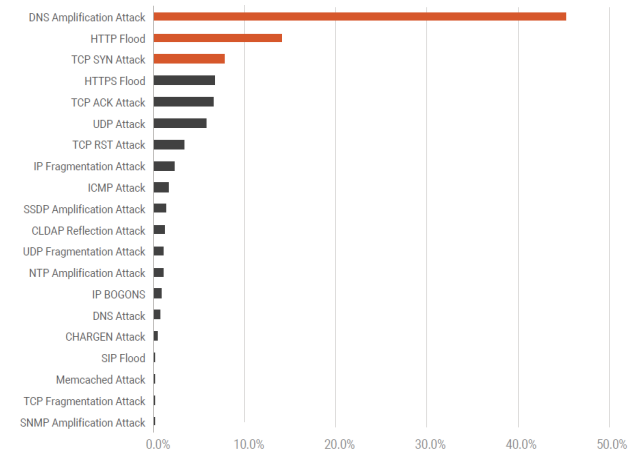


Fig. 5 Distribution of DDoS Attack Vectors, Q3 2019.

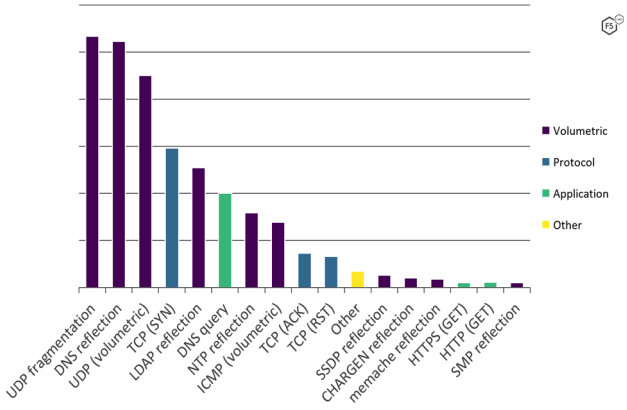


Fig. 6 Frequency of different DDoS attack tactics, January 2020 through March 2021

*4) Bogus Domain Attack (NXDOMAIN):* The NXDOMAIN attack occurred when the attacker attempted to submerge the DNS server by using false queries to resolve nonexistent domain names. The DNS server attempted to find a domain that did not exist but was unsuccessful. As a result of the NXDOMAIN, the cache becomes limited. Furthermore, legitimate requesters frequently face a response delay [29], [30]. This type of attack will overwhelm the DNS infrastructure [31]. Due to a lack of resources, the cache becomes overburdened with these malicious requests and is unable to serve legitimate requests [32].

### *B. Exploit Attacks*

This type of DNS attack focuses on zero-day vulnerabilities or weaknesses inherent within DNS services' design. Once cybercriminals identify these vulnerabilities, they can be exploited for malicious purposes. Therefore, the proper functioning of DNS is critical in mitigating the exploitation of the vulnerabilities to start a massive DDoS attack after bringing the service down [22],[33]. The attack is launched by abusing a vulnerability in the DNS mechanism [34], which produces malicious responses and necessitates a high level of technical ability [35].

*1) Zero-day Vulnerability:* The zero-day attack occurred via an exploit of the protocol stack, which can be used to confuse, crash, and compromise DNS servers. Through previously undiscovered vulnerabilities in the DNS server

software. Zero-day attacks can be used to exploit low-security systems [36],[37]. DNS administrators should classify and observe modern flooding attacks in order to identify and understand the vulnerabilities of zero-day attacks [38].

*2) DNS- based Exploits Attack*: these types of attacks happen when there are bugs/flaws in the services of DNS that can be exploited, and the services of DNS running on an operating system and the protocol can all be exploited. The attackers exploit the DNS vulnerabilities to maximize visits to their websites by maliciously redirecting the traffic [39]. In addition, attackers can take advantage of flaws in the user interface given by domain registrars. This drawback allows for DNS record manipulation in the zone file. It is possible that when exploited, DNS vulnerabilities and features will be used to launch large-scale DDoS attacks that disrupt services [22].

*3) Protocol Anomalies:* DNS protocol anomalies rely on distorted queries. Since these anomalies are not very common, they are difficult to analyze and detect. The flow, bytes, packet size, and bits/second do the same [40]. DNS queries Packet spoofing is abnormal behavior in the DNS protocol [41].

*4) DNS Rebinding:* this type of attack is commonly used on devices like the IoT that lack strong security mechanisms. This type of attack is growing fast due to the increasing number of IoT devices. The Internet of Things (IoT) is expected to have 500 billion devices connected by 2030 [42]. The attacker has gotten around the firewall and communicates directly with network devices via the victim's browser [43]. IoT devices provide a vast landscape for rebinding DNS attacks by getting access to the individual networks because of the security mechanisms used [44]. Using social engineering to lure the prey via the website through the small ads for visiting it [45].

### C. Stealth / Slow Drip DoS Attacks

This type of attack produces a nonexistent subdomain called the attacked domain of a common second-level domain (SLD). At the attack stage, all queries belong to SLD as a subdomain. To avoid dropping their traffic, attackers may use open resolvers to publish their traffic across a large IP range. Furthermore, IP spoofing limits mitigation and conceals the identity of the attackers [46]. Finally, this type of attack targets the authoritative DNS server [47].

*1) Sloth Domain Attack*: When a trustworthy, authoritative domain is hacked and taken over by an attacker, legitimate users request it. The response should be extended to meet these requirements before timing out. This time-out exhausted the victim's recursive server and its capacity. This cyber-attack is idle while spreading and hiding [19].

*2) Phantom Domain Attack*: the attacker creates domain nameservers for that domain but will configure it never to listen or reply to any queries. The resolver will receive many queries from that phantom domain, so it wastes most of its resources and time responding, which never happens [48]. At the DNS, both the request and reply are not encrypted to become vulnerable to several attacks [49].

*3) Pseudo-Random Subdomain Attack (PRSD)*: In this type of attack, many nonexistent subdomains are generated that are identical to the original domain. This attack is known as a pseudo-random subdomain attack [50] and has two-fold features: attracting the victim's attention or avoiding inconsistency with the current domains [51],[52]. The value of the length average of the long-spun pseudo-random subdomain is approximately close to zero [53]. Moreover, the DGA produces domain names that are truly pseudonyms after employing meeting points with the command-and-control servers [54].

### D. Protocol Abuse Attacks

This type of attack takes advantage of the DNS protocol and modifies it for malicious purposes, resulting in parasitic behavior. There are numerous purposes, such as phishing, hijacking, data exfiltration, and so on. Furthermore, DNS decentralization can be abused while allowing for scalability [53]. Finally, one of the DNS violations, known as DNS poisoning, directs prey to the malicious site [55].

*1) DNS Tunnelling Attack*: the victim data is divided into tiny chunks, encoding them inside the DNS queries, called DNS tunnelling. After that, the victim communicates with the attacker tool via queries of DNS [33]. DNS tunnelling can be employed for many purposes, such as carrying data for the packets of DNS [45]. The attacker exploits DNS tunnelling to exfiltrate data from the enterprises hacked into [56]. When the attacker bypasses the edge firewall of the enterprise, the tunnel can be used to execute a command or copy data through the domain name exploit in DNS queries and similar DNS replies [57]. Because DNS traffic is not encrypted, it can be easily exploited for malicious activities [14].

*2) DNS Cash Poisoning (spoofing):* vulnerabilities in DNS can be exploited by redirecting legitimate website traffic to a phishing website. This attack is called DNS cache poisoning attacks [39],[58] or mismatch between the true domain name and the provided IP address specifically for the attack [59]. Several entries of the DNS query are replaced with irregular values by spoofing the packet [41]. It can be considered a source for enhancing the effectiveness of the threat [60].

*3) DNS Hijacking Pharming*: the malware hosted at a local machine can change its server's TCP/IP configurations. This change allows for traffic redirection to the malicious website. When employing DNS servers, the attackers become malicious servers relative to the legitimate users. The infected hosts work like proxies for the attackers to publish their malicious software [61].

*4) DNS Hijacking-Phishing*: redirects users to malicious websites using legitimate domains but with the IP address of a dubious server. All this happens through records of DNS at the registrar being modified. Phishing attacks sometimes involve session hijacking and the replacement of DNS addresses [62],[63]. DNS hijacking can be done in a variety of ways. Malware or a bot has already infected the victim's machine and changed the DNS settings without the user's permission. [64].

*5) Subdomain Hijacking*: This type of vulnerability occurs in organizations when they assign their

domain/subdomain of the DNS entries, particularly the canonical name "CNAME" or record, to a third-party service while changing several services, such as cloud services. In some cases, the administrator may have overlooked changing the DNS configuration of the aforementioned domain/subdomain. The attacker exploits this vulnerability, i.e., occupation of the particular subdomains, by creating an account on the same outer service [65]. Their relationship will be very independent [66]. Hijacking tries to hijack a subdomain by logging into the administration and management account of the domain [67].

*6) Domain Squatting*: occurs when an attacker registers a domain that is similar to the legitimate domain and hosts phishing or malware-laden websites. Users' errors, such as misspellings and typos, cause them to visit malicious websites [68]. The attacker registers their new domain to be very close to well-known domain names with minor variations [69], [70]. As a result, end-user traffic may be unintentionally redirected to unintended destinations [71]. When one program overlaps with another via distributed synchronization objects, it is a type of DoS attack [72].

## III. Results and Discussion

This section introduces the techniques and mechanisms used as countermeasures for DRDoS attacks. Previously, we defined the attack types discovered while researching the types of attacks in DNS. Although DNS can be attacked, each type of attack relies on security vulnerabilities in the DNS to launch their malicious attacks. As a result, this section focuses on the most common types and their impact on the DNS's efficiency and accuracy.

Cybersecurity researchers say DDoS attacks have become more common in recent years. DDoS attacks have also significantly impacted the functioning of companies and organizations worldwide, causing financial and technical damage due to their destructive effect while sabotaging DNS infrastructure [73]. The DNS amplification attack is more popular than other DNS attacks because the attacker prefers attacks with a high effect and a low cost. Furthermore, DNS reflection attacks have a significant and dangerous impact due to their attack-specific characteristics [74]. The poll in 2016 [75] included a question about the techniques used for reflection/amplification Figure 7. Although reflection attacks have been discovered in all these protocols this year and have become more prevalent, DNS remains the most commonly used.

DNS is the dominant protocol in reflection/amplification attacks because the attack numbers are greater than all other attack vectors combined, and the packet size of the response is larger than the demand. In recent years, there has been an increase in this type of attack, particularly in protocols that can be abused to amplify packet sizes, such as DNS and other protocols.

According to Nexusguard Limited Company, the distribution of DDoS attack factors in 2019 from Q1 to Q4 is DNS amplification/reflection: the Q1 DNS amplification attack factor is 42.94% (6398), the Q2 DNS amplification attack factor is 65.95% (8382), the Q3 DNS amplification attack factor is 45.21% (4448), the Q4 DNS amplification attack factor is 50.97% (4470).

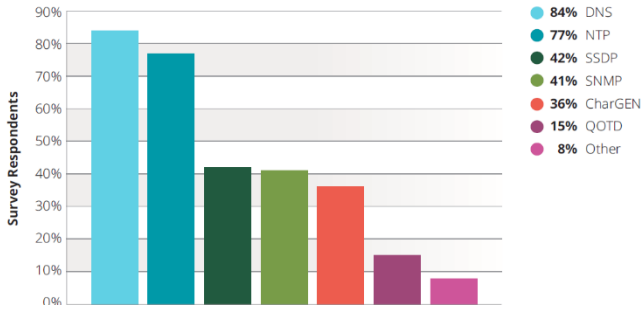


Fig. 7 Protocols Used for Reflection/Amplification

### A. The Mechanics of DRDoS Attacks

As previously stated, DRDoS is a DDoS attack targeting DNS servers by flooding them with bogus requests. Furthermore, some attackers have combined amplification and reflection, resulting in a new type of attack known as a distributed reflection denial of service (DRDoS).

This type of attack is classified into two types based on the protocol used in the attack: TCP-based DRDoS assault and UDP-based DRDoS assault, which consists of two parts: amplification and reflection [73]. As a result, some attacks are protocol-dependent, while others are protocol-independent. Figure 8 represents the mechanism for DRDoS DNS attacks that occur.

*1) Amplification*: In some protocols, the response is more significant in packet size than the demand. Thus, attackers can leverage this feature to generate massive traffic from almost minimal traffic. The servers that abuse this feature is referred to as amplifiers. The difference between the size of the request and response packets is obvious at DNS, and therefore, it amplifies the DNS attack [76].

*2) Reflection:* Verifying the origin IP address of the packet is not yet a built-in mechanism in the internet protocol. As a result, the UDP does not verify the source of the packets requested when returning the reply packets. The servers that abuse this feature are called reflectors, and the reflectors are legitimate hosts that flood the target server with many reply packets by spoofed IP addresses [77].

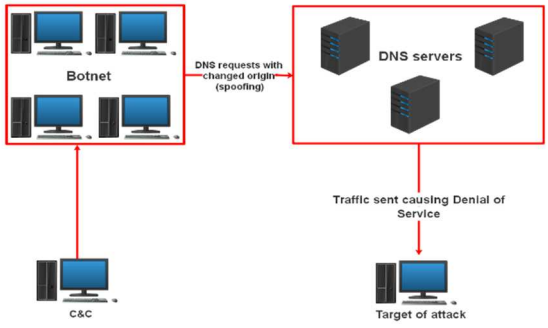


Fig. 8 DNS DRDoS attack diagram

The defense techniques used differ from one attack to another, depending on the attack mechanism. Therefore, when planning to build a security defense for any organization, the first option is to detect the attack, or the method used for that purpose. The intrusion detection system is used to detect

several types of attacks, and the IDS can be a device or software.

Lukaseder et al. [78] studied the very well-known reflective attacks that can be mitigated by using packet filtering based on NAT as a reliable method. There are four categories of messages receivable via the destination host: legitimate and illegitimate requests/response. The response which must be filtered is the illegitimate response to the DRDoS attacks. Then the first step is to separate the requests from the responses. DRDoS attacks are typically launched using UDP. As a result, only the UDP response packets are analysed by the DRDoS mitigation system. This system must classify inbound responses as legitimate or illegitimate. The NAT modified form is used. NAT is activated during the attack, and the IP address of the assault destination is replaced in outbound UDP requests by a pseudonym IP address. When using this method, it is difficult to replace their IP addresses. This system correctly distinguishes between legitimate and illegitimate replies without monitoring the attack traffic. When the system is available, a second differentiator classifies demands from replies. Only outbound requests are routed through NAT.

El-Houda et al. [6] employed the Brain Chain approach. The Brain Chain model is divided into two phases: the first is a model to detect DDoS using machine learning, which aims to reveal illegal flows (illegal DNS demands) in real-time, and is comprised of three schemes: FS, ES, and BF. These three schemes operate at the application layer (SDN controller) and make use of sFlow, the network traffic statistics collected by FS. The other two schemes detect illegal flows automatically. The second phase, the DNS mitigation scheme (DM), aims to mitigate the effects of illegal streams in order to restore the network immediately. They assessed the BF machine learning algorithm's performance using the detection and false-positive ROC curve rates. Furthermore, the BF was tested with two different sizes of attempts, causing the accuracy and rate of false positives to vary.

According to Gupta and Sharma [79], the proposed method includes a collection of geographically distributed routers known as the Barrier of Routers (BoR). The network that needs to defend itself should route all inbound and outbound traffic through the BoR. The BoR terminates all attack traffic. This method can help mitigate the attack's traffic with DNS amplification attacks. When attacked, the Anycast-Barrier is more vulnerable than the Proxy-Barrier. These factors all affect the BoR's performance: the number of routers, the level of the network, the size of the level network, the type of network, and the location of the BoR in relation to the borders.

Özdinçer and Mantar [80] has identified and reduced DNS amplification, a type of DRDoS attack. It has the effect of developing an SDN-based system. The proposed system separates the attack detection and attack mitigation stages. Many factors influence this system's performance, including request size, reply to packets, and variations in the TTL value in the IP header; as well as using a predefined threshold and only statistical changes. The system used in the attack detection stage is known as YARASA, and it is divided into two stages:

The first stage involves monitoring the amplification factor, which has two thresholds, lower and upper; if the lower threshold is exceeded, the YARASA goes directly to the second phase to avoid the overthrow of the legal queries. However, if the upper threshold is exceeded, the process proceeds directly to the mitigation stage. The second stage entails tracking the variation in the hop count. The TTL values change in the IP header for requests from the client's DNS to a server with a high AF value. The mitigation stage: when a DNS server acts as a reflector, this stage is activated and prevents the prey from responding in order to reduce inbound traffic from that server. Legal requests made through the prey are sometimes ignored.

Khooi et al. [81] suggested model is called the Distributed In-Network Defense Architecture, or DIDA. While still offering much more precise and quicker detection and protection against AR-DDoS attacks by relying on a completely distributed solution that operates entirely on the data plane. This model focuses on the data levels that are programmable and effective data structures, and it can be leveraged to observe and track the connections per user. The network is controlled by applying DIDA, an automated and distributed method, without overwhelming. DIDA's detection and mitigation accuracy for AR-DDoS attacks is very high. Furthermore, it necessitates only a limited number of resources.

According to Zhang and Cheng [82], traffic throttling employs reinforcement learning RL, and the RL agent allows the traffic throttling technique by obtaining traffic data. The basic router is deployed dynamically in this model. The goal is to reject attack traffic while retaining as much legal traffic as possible by filtering router traffic to prevent amplification. Thus, it is smarter and more efficient than the traditional system of port-based traffic throttling.

In contrast to centralized base defensive systems, DDM introduces a distributed mechanism to detect and prevent DNS reflection/amplification attacks with less impact on network computational resources [83]. DDM adds a security layer to DNS by introducing an authentication method for DNS queries. Furthermore, DDM employs a classification filtering approach that is only activated when malicious traffic is detected.

Lyu et al. [84] present a method for detecting distributed DNS attacks that combines machine learning with a hierarchical graph structure to monitor DNS activity at three levels: host, subnet, and autonomous system (AS). Our method detects dispersed assaults at low rates and in subtle patterns, and we discovered critical characteristics that successfully differentiate malicious entities from ordinary external users. Our dynamic data structure also used anomaly detection algorithms (trained/tuned using benign and attack traffic).

Xu et al. [85] suggested a new strategy for detecting and defending against distributed denial-of-service (DDoS) assaults on the Internet of Things (IoT) as the number of connected devices grows. Via network nodes that evaluate DRDoS request and response packet statistics. The HDTI host based DRDoS threat index is presented based on the definition of these processed and integrated properties. The suggested approach's high accessibility to modern network nodes gives it enough confidence to use the detection model and HDTI as a major factor in its detection scheme and as the trigger for the defense method presented shortly in this study. Testing and experiments had been used to establish our

proposed detection method's validity, efficiency, and accuracy.

A previous study has characterized DRDoS attacks using multiple protocols and carpet bombing [86]. Developing MP-H, a honeypot that collects data using nine different protocols commonly used in DDoS assaults. Over 731 days, the honeypot was subjected to over 1.4 million DRDoS assaults, including over 13.7 thousand multiprotocol attacks. When comparing multiprotocol attacks to monoprotocol attacks that happened in the same time period, our honeypot saw many strikes described as carpet bombing. DNS and Memcached requests are routed through real servers in MP-H, but the honeypot imitates all other protocols, which generates fake answers with created content.

According to Arthi and Krishnaveni [87], IDS are currently automated and dynamically configured with the help of machine learning and deep learning models. In most cases, the model's performance is heavily influenced by the data used to train it. As a result, the primary goal of this article is to examine the impact of current datasets in the IoT environment. An IoT-based data collection system for DNS amplification attacks is proposed as an alternative. The network packets of a DDoS attack are recorded using port mirroring. The study investigates DDoS attacks on the Internet of Things, including amplification attacks, in the numerous available datasets. Finally, this study explains how to obtain real-time data for DNS amplification attacks.

A proposed developed system depends on the behavior of a biologically inspired particle swarm optimization algorithm [88]. Each consortium member is frequently used in its private chain, with no information exchanged between members. Moreover, the anomalous data is stored on the public chain, which enables a business to monitor the attacker's activity. The public chain contains all the anomalous data without the need for a trustworthy third party. Likewise, this prohibits tampering with the public chain's anomalous information and enables members to acquire accurate information. Especially, the blockchain's powerful encryption technology ensures data security and prohibits tampering. According to the research, smart contracts can distinguish DDoS data and generate anomalous chains on each node.

SDN-based architectures can recognize DDoS attacks at the transport and application layers by utilizing a variety of Machine Learning (ML) and Deep Learning (DL) models [89]. They evaluated the machine learning/deep learning models using two up-to-date security datasets, CICDoS2017, and CICDDoS2019. They demonstrated a modular SDN-based architecture composed of interchangeable components. The proposed approach was validated in an emulation environment using Mininet and the ONOS controller. The highest detection rates are achieved by the GRU and LSTM models. DL models outperformed ML models in terms of detection rates for all types of attacks studied in this work.

The deep neural network (DNN) is proposed as a deep learning model for detecting DDoS attacks on a sample of packets recorded from network traffic [90]. Because the DNN model's structure incorporates feature extraction and classification methods and has self-updating layers, it can operate rapidly and accurately even with little data.

Thorat, Parekh, and Mangrulkar [91] extended the binary classification problem of detecting DDoS attacks to a multi-classification problem of locating the vulnerable protocol. Knowing the attacker's precise protocol helps strengthen security management systems and respond faster to malicious packets entering the network. The TaxoDaCML technique detects and classifies 11 significant DDoS assaults with an accuracy of 85.8%, using taxonomy to break a larger classification problem into seven smaller classification problems. Table I shows the comparisons between the techniques that are used to detect DRDoS attacks.

TABLE I
DETECTION METHODS FOR DRDOS ATTACKS.

| No. | Title | Year | Algorithm | Dataset | Advantage | Disadvantage |
|---|---|---|---|---|---|---|
| 1 | [6] | 2020 | BrainChain | Private dataset | The approach can detect DNS amplification attacks and mitigate, with high accuracy and low FPR. | Sometimes a fixed threshold classifies legitimate requests as illegal requests. |
| 2 | [78] | 2018 | By implementing the packets filtering that based on NAT in the SDN | private dataset | An alias IP address has been used, and this method is very difficult to guess by the attacker | If the network traffic has been hacked, this approach will be ineffective |
| 3 | [79] | 2018 | A barrier of Routers (BoR) and DNS Amplification Attacks Detector (DAAD) | Private dataset | the traffic of attack can be mitigated in high accuracy in a specific geographic area. | The system is affected by two important factors: the attack bandwidth and the number of routers. |
| 4 | [80] | 2019 | YARASA system | AmpPot dataset | consuming fewer resources. The system shows the high performance when used to mitigate the attack affects the victim side. | The system is affected by how selecting the proper values of the threshold. Sometimes the legal requests via the prey are dropped |
| 5 | [81] | 2020 | Distributed In-network Defense Architecture (DIDA) | Private dataset | The DIDA achieves high detection accuracy and consumes very few resources from memory. | The predefined threshold will drop some legitimate request/response or allow some request/response illegitimate. |
| 6 | [82] | 2019 | reinforcement learning | Private dataset | This mechanism achieves High performance by maintaining legal traffic to | The static threshold used in the model will affect the detection accuracy and decreases it. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | identify and discard attack traffic. | |
| 7 | [83] | 2020 | distributed-based defense mechanism (DDM) | Private dataset | The DDM reduces the time it takes for network computational resources to be used. | Number and location of nodes. The size of the network traffic will affect the DDM performance. |
| 8 | [84] | 2021 | hierarchical graph structure | Private dataset | the model achieves high accuracy detection. | Using information-gain lead to an overfitting issue. |
| 9 | [85] | 2019 | host-based DRDoS threat index (HDTI) | WRCCDC 2018 dataset | HDTI model can detect and mitigate DRDoS attacks with a higher detection rate and a lower false alarm rate. | The location of the HDTI model and network traffic load balance are influential on the performance of HDTI. |
| 10 | [86] | 2021 | multiprotocol honeypot | Private dataset | A new method for understanding and detecting multiprotocol attacks | maybe some of the output MP-H generates fake answers with created content. |
| 11 | [87] | 2021 | | Private dataset | It seems a new and powerful IDS method in IoT for detecting and protecting from amplification attacks. | The tested model is limited to IoT and can't run on other environments. |
| 12 | [88] | 2020 | biologically inspired particle swarm optimization algorithm and blockchain | CICDDoS2019 | This method achieved a detection accuracy of 89.8% and a perfect false positive is equal to zero. | The size of data used in training the system is very small, and maybe when the size of data is increased, the detection accuracy and false-positive will be affected. |
| 13 | [89] | 2021 | intelligent SDN-based DoS/DDoS attacks detection | CICDDoS2017 and CICDDoS2019 | This method achieved a perfect and high detection accuracy of 99.97%. | Employing a large number of features in the detection mechanisms leads to a high false-positive. |
| 14 | [90] | 2021 | Deep Neural Network (DNN) | CICDDoS2019 | This method achieved a perfect and high detection accuracy of 99.99% | Several features are removed before training the model, and then only 69 features are used in the training. Therefore, those removed features may have an effect on the obtained detection accuracy. |
| 15 | [91] | 2021 | TaxoDaCML | CICDDoS2019 | It is important to quickly notice the onset of a DDoS attack so that secure information management infrastructure may be quickly restored. | This method achieved a very low detection accuracy of 69.8% when detecting DNS-based DRDoS attacks. |

## IV. Conclusion

DNS threats are becoming so widespread and rapid that they are affecting the quality of services provided to clients. Many studies are being conducted in order to find the perfect solution to these problems. Therefore, we reviewed the literature on the most important attacks targeting domain name systems, DRDoS attacks. The novelty of this study is in the form of categorizing the solutions in research papers based on the techniques used into two parts: protocol-independent and protocol-based techniques such as DNS. These proposed methods can be used to detect and mitigate DNS attacks, as well as both. As a result, each strategy has advantages and disadvantages. These proposed approaches depend on several factors when designed to produce the desired results. The well-known one is based on requests and responses, filtering them using various techniques or focusing on orphan replies.

## References


[1] J. J. C. Gondim, R. de Oliveira Albuquerque, and A. L. S. Orozco, "Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols," Futur. Gener. Comput. Syst., vol. 108, pp. 68–81, 2020.

[2] J. Bushart and C. Rossow, "DNS unchained: amplified application-layer DoS attacks against DNS authoritatives," in International Symposium on Research in Attacks, Intrusions, and Defenses, 2018, pp. 139–160.

[3] David Warburton, "DDoS Attack Trends for 2020 | F5 Labs," 2021. https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020 (accessed Aug. 31, 2021).

[4] I. Georgiev and K. Nikolova, "An approach of DNS protection against DDoS attacks," in 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), 2017, pp. 140–143.

[5] D. Boro and D. K. Bhattacharyya, "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks," Microsyst. Technol., vol. 23, no. 3, pp. 593–611, 2017.

[6] Z. Abou El Houda, A. Hafid, and L. Khoukhi, "BrainChain-A Machine learning Approach for protecting Blockchain applications using SDN," 2020.

[7] L. A. Trejo, V. Ferman, M. A. Medina-Pérez, F. M. A. Giacinti, R. Monroy, and J. E. Ramirez-Marquez, "DNS-ADVP: A Machine Learning Anomaly Detection and Visual Platform to Protect Top-Level Domain Name Servers Against DDoS Attacks," IEEE Access, vol. 7, pp. 116358–116369, 2019.

[8] K. S. Niraja, K. K. Chennam, and R. Madana Mohana, "A Survey on DDoS Attacks from Compromised Devices to Enhance IoT Security," in Computational Intelligence in Machine Learning, Springer, 2022, pp. 265–269.

[9] Y. Nosyk, M. Korczyński, and A. Duda, "Routing Loops as Mega Amplifiers for DNS-Based DDoS Attacks," in International Conference on Passive and Active Network Measurement, 2022, pp. 629–644.

[10] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, "BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web," J. King Saud Univ. Inf. Sci., vol. 32, no. 1, pp. 73–87, 2020.

[11] R. Samta and M. Sood, “Analysis and Mitigation of DDoS Flooding Attacks in Software Defined Networks,” in International Conference on Innovative Computing and Communications, 2020, pp. 337–355.
[12] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, “LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection,” IEEE Trans. Netw. Serv. Manag., 2020.
[13] M. Nooribakhsh and M. Mollamotalebi, “A review on statistical approaches for anomaly detection in DDoS attacks,” Inf. Secur. J. A Glob. Perspect., vol. 29, no. 3, pp. 118–133, 2020.
[14] C. Patsakis, F. Casino, and V. Katos, “Encrypted and covert DNS queries for botnets: Challenges and countermeasures,” Comput. Secur., vol. 88, p. 101614, 2020.
[15] J. Slupska, “War, Health and Ecosystem: Generative Metaphors in Cybersecurity Governance,” Philos. Technol., pp. 1–20, 2020.
[16] S. Saharan and V. Gupta, “Prevention of DrDoS Amplification Attacks by Penalizing the Attackers in SDN Environment,” in International Conference on Advanced Information Networking and Applications, 2022, pp. 684–696.
[17] S. Charles, Y. Lyu, and P. Mishra, “Real-time detection and localization of distributed dos attacks in noc based socs,” IEEE Trans. Comput. Des. Integr. Circuits Syst., 2020.
[18] V. R. Krishna and R. Subhashini, “Mimicking attack by botnet and detection at gateway,” Peer-to-Peer Netw. Appl., pp. 1–11, 2020.
[19] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, “A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities,” IEEE Trans. Ind. Appl., 2020.
[20] M. O’Leary, “DNS and BIND,” in Cyber Operations, Springer, 2019, pp. 165–211.
[21] ACSC, “Threat Report,” Aust. Cyber Secur. Cent., vol. 1, p. 40, 2019.
[22] G. Mittal and V. Gupta, “KarmaNet: SDN solution to DNS-based Denial-of-Service,” in International Symposium on Security in Computing and Communication, 2018, pp. 431–442.
[23] T. Ubale and A. K. Jain, “Survey on DDoS Attack Techniques and Solutions in Software-Defined Network,” in Handbook of Computer Networks and Cyber Security, Springer, 2020, pp. 389–419.
[24] J. Li, M. Liu, Z. Xue, X. Fan, and X. He, “RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things,” IEEE Access, vol. 8, pp. 36191–36201, 2020.
[25] S. Saharan, V. Gupta, N. Vora, and M. Maheshwari, “Detection of Distributed Denial of Service Attacks Using Entropy on Sliding Window with Dynamic Threshold,” in International Conference on Advanced Information Networking and Applications, 2022, pp. 424–434.
[26] C. Sun et al., “Sdpa: Toward a stateful data plane in software-defined networking,” IEEE/ACM Trans. Netw., vol. 25, no. 6, pp. 3294–3308, 2017.
[27] N. Kostopoulos, A. Pavlidis, M. Dimolianis, D. Kalogeras, and V. Maglaris, “A Privacy-Preserving Schema for the Detection and Collaborative Mitigation of DNS Water Torture Attacks in Cloud Infrastructures,” in 2019 IEEE 8th International Conference on Cloud Networking (CloudNet), 2019, pp. 1–6.
[28] P. K. Sharma, S. Singh, and J. H. Park, “OpCloudSec: Open cloud software defined wireless network security for the Internet of Things,” Comput. Commun., vol. 122, pp. 1–8, 2018.
[29] V. Rajakumareswaran and S. Nithiyanandam, “Box counting–based multifractal analysis of network to detect Domain Name Server attack,” Int. J. Commun. Syst., vol. 32, no. 7, p. e3916, 2019.
[30] L. Shafir, Y. Afek, and A. Bremler-Barr, “NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities,” arXiv Prepr. arXiv2005.09107, 2020.
[31] R. Ghannam, F. Sharevski, and A. Chung, “User-targeted Denial-of-Service Attacks in LTE Mobile Networks,” International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 2018-Octob. 2018, doi: 10.1109/WiMOB.2018.8589140.
[32] M. E. Ahmed, H. Kim, and M. Park, “Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking,” in MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 11–16.
[33] S. Shafieian, D. Smith, and M. Zulkernine, “Detecting DNS tunneling using ensemble learning,” in International Conference on Network and System Security, 2017, pp. 112–127.
[34] B. Munkhbaatar, M. Mimura, and H. Tanaka, “Dark Domain Name Attack: A New Threat to Domain Name System,” in International Conference on Information Systems Security, 2017, pp. 405–414.
[35] A. Nadler, R. Bitton, O. Brodt, and A. Shabtai, “On the vulnerability of anti-malware solutions to DNS attacks,” Comput. Secur., vol. 116, p. 102687, 2022.
[36] M. Singh, M. Singh, and S. Kaur, “Detecting bot-infected machines using DNS fingerprinting,” Digit. Investig., vol. 28, pp. 14–33, 2019.
[37] O. Somarriba and U. Zurutuza, “A collaborative framework for android malware detection using DNS & dynamic analysis,” in 2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII), 2017, pp. 1–6.
[38] S. R. Rincón, S. Vaton, and S. Bortzmeyer, “Reproducing DNS 10Gbps flooding attacks with commodity-hardware,” in 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 510–515.
[39] A. K. Jain and B. B. Gupta, “A novel approach to protect against phishing attacks at client side using auto-updated white-list,” EURASIP J. Inf. Secur., vol. 2016, no. 1, p. 9, 2016.
[40] R. Sharma, A. Guleria, and R. K. Singla, “Characterizing Network Flows for Detecting DNS, NTP, and SNMP Anomalies,” in Intelligent Computing and Information and Communication, Springer, 2018, pp. 327–340.
[41] P. Robberechts, M. Bosteels, J. Davis, and W. Meert, “Query log analysis: Detecting anomalies in DNS traffic at a TLD resolver,” in Joint European Conference on Machine Learning and Knowledge Discovery in Databases, 2018, pp. 55–67.
[42] Cisco, “Internet of Things,” 2016. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.
[43] D. Tatang, T. Suurland, and T. Holz, “Study of DNS Rebinding Attacks on Smart Home Devices,” in Computer Security, Springer, 2019, pp. 391–401.
[44] J. Spaulding and A. Mohaisen, “Defending internet of things against malicious domain names using D-FENS,” in 2018 IEEE/ACM Symposium on Edge Computing (SEC), 2018, pp. 387–392.
[45] A. Sehgal and A. Dixit, “Securing Web Access—DNS Threats and Remedies,” in Emerging Trends in Expert Applications and Security, Springer, 2019, pp. 337–345.
[46] R. Burton, “Characterizing Certain DNS DDoS Attacks,” arXiv Prepr. arXiv1905.09958, 2019.
[47] H. Sinanović and S. Mrdovic, “Analysis of Mirai malicious software,” in 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2017, pp. 1–5.
[48] R. Sommese, A. Sperotto, R. van Rijswijk-Deij, A. Dainotti, and K. Claffy, “Background research on DNS-related DDoS vulnerabilities,” 2019.
[49] A. Ramdas and R. Muthukrishnan, “A Survey on DNS Security Issues and Mitigation Techniques,” in 2019 International Conference on Intelligent Computing and Control Systems (ICCS), 2019, pp. 781–784.
[50] S. L. Feibish, Y. Afek, A. Bremler-Barr, E. Cohen, and M. Shagam, “Mitigating DNS random subdomain DDoS attacks by distinct heavy hitters sketches,” in Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies, 2017, pp. 1–6.
[51] S. Le Page and G.-V. Jourdan, “Victim or Attacker? A Multi-dataset Domain Classification of Phishing Attacks,” in 2019 17th International Conference on Privacy, Security and Trust (PST), 2019, pp. 1–10.
[52] S. Le Page, G.-V. Jourdan, G. V Bochmann, I.-V. Onut, and J. Flood, “Domain classifier: Compromised machines versus malicious registrations,” in International Conference on Web Engineering, 2019, pp. 265–279.
[53] A. Nadler, A. Aminov, and A. Shabtai, “Detection of malicious and low throughput data exfiltration over the DNS protocol,” Comput. Secur., vol. 80, pp. 36–53, 2019.
[54] A. D. Kumar et al., “Enhanced Domain Generating Algorithm Detection Based on Deep Neural Networks,” in Deep Learning Applications for Cyber Security, Springer, 2019, pp. 151–173.
[55] C. Hesselman, G. C. M. Moura, R. de Oliveira Schmidt, and C. Toet, “Increasing DNS security and stability through a control plane for top-level domain operators,” IEEE Commun. Mag., vol. 55, no. 1, pp. 197–203, 2017.
[56] N. Ishikura, D. Kondo, I. Iordanov, V. Vassiliades, and H. Tode, “Cache-Property-Aware Features for DNS Tunneling Detection,” in 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2020, pp. 216–220.

[57] D. Kondo, V. Vassiliades, H. Tode, and T. Asami, “The named data networking flow filter: Towards improved security over information leakage attacks,” Comput. Networks, p. 107187, 2020.
[58] Z. Wang, H. Hu, and G. Cheng, “Design and implementation of an SDN-enabled DNS security framework,” China Commun., vol. 16, no. 2, pp. 233–245, 2019.
[59] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, “Detection and prevention of DNS spoofing attacks,” in 2017 Siberian Symposium on Data Science and Engineering (SSDSE), 2017, pp. 84–87.
[60] Z. Yu, D. Xue, J. Fan, and C. Guo, “Dnstsm: DNS cache resources trusted sharing model based on consortium blockchain,” IEEE Access, vol. 8, pp. 13640–13650, 2020.
[61] A. Almomani, “Fast-flux hunter: a system for filtering online fast-flux botnet,” Neural Comput. Appl., vol. 29, no. 7, pp. 483–493, 2018.
[62] D. N. Pande and P. S. Voditel, “Spear phishing: Diagnosing attack paradigm,” in 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 2720–2724.
[63] S. Chanti and T. Chithralekha, “Classification of Anti-phishing Solutions,” SN Comput. Sci., vol. 1, no. 1, p. 11, 2020.
[64] U. T. Gudekli and B. Ciylan, “DNS Tunneling Effect on DNS Packet Sizes,” 2019.
[65] S. M. Z. U. Rashid, M. D. I. Kamrul, and A. Islam, “Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme,” in 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019, pp. 1–4.
[66] D. Liu, Z. Li, K. Du, H. Wang, B. Liu, and H. Duan, “Don’t let one rotten apple spoil the whole barrel: Towards automated detection of shadowed domains,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 537–552.
[67] R. Stevens, D. Votipka, E. M. Redmiles, C. Ahern, and M. L. Mazurek, “Applied Digital Threat Modeling: It Works,” IEEE Secur. Priv., vol. 17, no. 4, pp. 35–42, 2019.
[68] Y. Hu et al., “Mobile app squatting,” in Proceedings of The Web Conference 2020, 2020, pp. 1727–1738.
[69] P. Kintis et al., “Hiding in plain sight: A longitudinal study of combosquatting abuse,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 569–586.
[70] P. Lv, J. Ya, T. Liu, J. Shi, B. Fang, and Z. Gu, “You have more abbreviations than you know: A study of AbbrevSquatting abuse,” in International Conference on Computational Science, 2018, pp. 221–233.
[71] V. Le Pochat, T. Van Goethem, and W. Joosen, “Funny accents: Exploring genuine interest in internationalized domain names,” in International Conference on Passive and Active Network Measurement, 2019, pp. 178–194.
[72] S. Chen, L. Fan, C. Chen, M. Xue, Y. Liu, and L. Xu, “GUI-Squatting Attack: Automated Generation of Android Phishing Apps,” IEEE Trans. Dependable Secur. Comput., 2019.
[73] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, “Distributed reflection denial of service attack: A critical review.,” Int. J. Electr. Comput. Eng., vol. 11, no. 6, 2021.
[74] R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari, “A new proactive feature selection model based on the enhanced optimization algorithms to detect DRDoS attacks.,” Int. J. Electr. Comput. Eng., vol. 12, no. 2, 2022.
[75] A. NETSCOUT, “14th Annual Worldwide Infrastructure Security Report, 2019.” 2019.
[76] X. Jing, J. Zhao, Q. Zheng, Z. Yan, and W. Pedrycz, “A reversible sketch-based method for detecting and mitigating amplification attacks,” J. Netw. Comput. Appl., vol. 142, pp. 15–24, 2019.
[77] M. Anagnostopoulos, S. Lagos, and G. Kambourakis, “Large-scale empirical evaluation of DNS and SSDP amplification attacks,” J. Inf. Secur. Appl., vol. 66, p. 103168, 2022.
[78] T. Lukaseder, K. Stölzle, S. Kleber, B. Erb, and F. Kargl, “An SDN-based Approach For Defending Against Reflective DDoS Attacks,” in 2018 IEEE 43rd Conference on Local Computer Networks (LCN), 2018, pp. 299–302.
[79] V. Gupta and E. Sharma, “Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers,” in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 392–400.
[80] K. Özdinçer and H. A. Mantar, “SDN-based Detection and Mitigation System for DNS Amplification Attacks,” in 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2019, pp. 1–7.
[81] X. Z. Khooi, L. Csikor, D. M. Divakaran, and M. S. Kang, “DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks,” in 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, pp. 277–281.
[82] Y. Zhang and Y. Cheng, “An Amplification DDoS Attack Defence Mechanism using Reinforcement Learning,” in 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019, pp. 634–639.
[83] R. R. H. Amin, D. Hassan, and M. Hussin, “Preventing DNS misuse for Reflection/Amplification attacks with minimal computational overhead on the Internet,” Kurdistan J. Appl. Res., pp. 60–70, 2020.
[84] M. Lyu, H. H. Gharakheili, C. Russell, and V. Sivaraman, “Hierarchical Anomaly-Based Detection of Distributed DNS Attacks on Enterprise Networks,” IEEE Trans. Netw. Serv. Manag., vol. 18, no. 1, pp. 1031–1048, 2021.
[85] R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, “A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment,” Symmetry (Basel)., vol. 11, no. 1, p. 78, Jan. 2019, doi: 10.3390/sym11010078.
[86] T. Heinrich, R. R. Obelheiro, and C. A. Maziero, “New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks,” in International Conference on Passive and Active Network Measurement, 2021, pp. 269–283.
[87] R. Arthi and S. Krishnaveni, “Design and Development of IOT Testbed with DDoS Attack for Cyber Security Research,” in 2021 3rd International Conference on Signal Processing and Communication (ICPSC), 2021, pp. 586–590.
[88] X. Han, R. Zhang, X. Liu, and F. Jiang, “Biologically Inspired Smart Contract: A Blockchain-Based DDoS Detection System,” in 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC), 2020, pp. 1–6.
[89] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, “SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning,” IEEE Access, vol. 9, pp. 108495–108512, 2021.
[90] A. E. Cil, K. Yildiz, and A. Buldu, “Detection of DDoS attacks with feed forward based deep neural network model,” Expert Syst. Appl., vol. 169, p. 114520, 2021.
[91] O. Thorat, N. Parekh, and R. Mangrulkar, “TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification,” Int. J. Inf. Manag. Data Insights, vol. 1, no. 2, p. 100048, 2021.