International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 6, December 2021, pp. 5327~5341
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i6.pp5327-5341

Distributed reflection denial of service attack: A critical review

Riyadh Rahef Nuiaa[1], Selvakumar Manickam[2], Ali Hakem Alsaeedi[3]
[1]Department of Computer/College of Education for Pure Sciences, Wasit University, Iraq
[1,2]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia
[3]College of Computer Science and Information Technology, Universitas of Al-Qadisiyah, Iraq

Article Info

Article history:

Received Oct 29, 2020
Revised May 17, 2021
Accepted Jun 12, 2021

Keywords:

Amplification attack
DDoS attack
DRDoS attack
Reflection attack
TCP/UDP attacks

ABSTRACT

As the world becomes increasingly connected and the number of users grows exponentially and "things" go online, the prospect of cyberspace becoming a significant target for cybercriminals is a reality. Any host or device that is exposed on the internet is a prime target for cyberattacks. A denial-of-service (DoS) attack is accountable for the majority of these cyberattacks. Although various solutions have been proposed by researchers to mitigate this issue, cybercriminals always adapt their attack approach to circumvent countermeasures. One of the modified DoS attacks is known as distributed reflection denial-of-service attack (DRDoS). This type of attack is considered to be a more severe variant of the DoS attack and can be conducted in transmission control protocol (TCP) and user datagram protocol (UDP). However, this attack is not effective in the TCP protocol due to the three-way handshake approach that prevents this type of attack from passing through the network layer to the upper layers in the network stack. On the other hand, UDP is a connectionless protocol, so most of these DRDoS attacks pass through UDP. This study aims to examine and identify the differences between TCP-based and UDP-based DRDoS attacks.

Corresponding Author:

Selvakumar Manickam
National Advanced IPv6 Centre
Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: selva@usm.my

1. INTRODUCTION

The phenomenal growth of internet use over the past decade illustrates the increasing social importance of the internet. This growth proves that the internet is not only a valuable tool for researchers but also a major part of the infrastructure of global society. This growth can be attributed to changes in traditional roles for doing the business by using the internet, which allows all transactions conducted on the internet. The government uses the internet to provide its citizens and the world at large with information and governmental services. The internet enables companies to share and exchange information among their divisions, suppliers, partners, and customers to increase operational efficiency [1]. Research and educational institutions depend on the internet as a medium for collaboration to enhance their research discoveries.

If we consider the previous years, specifically 1995, when the internet was used by the global population and analyze the growth curve until 2020 [2], we find that the percentage jumps dramatically in Figure 1. Amid this increase in the number of internet users [3], security challenges have started to grow [4] and internet penetration has increased in the 2009–2018 period at 24%-51%. The service provider wants to offer services to customers in the best and most secure ways. Thus, they take care of the field to provide secure services by addressing vulnerabilities on the service side. However, this task is nearly impossible to

achieve because of the difficulty of controlling the network resources [5]; then, they go ahead to another way represented in the security companies but this also needs some time to update their [6].

Unfortunately, with the growing dependence of business on the internet, security problems have begun to pose major obstacles to the future development of the internet. With increasing Internet use, the number of attacks on the internet has also increased rapidly. The internet is particularly vulnerable to attacks because of its public nature and because it has no centralised control. Therefore, network attacks have become more sophisticated because the attackers have shifted from physical (direct sabotage of digital resources) to remote (disruption or disabling of one or more targets) methods.

DDoS attacks are observed as the most devastating and prevalent in the current era, regardless of whether one has resources in the cloud environment or not. DDoS attacks alone have caused extensive damage to various businesses worldwide; among the major affected targets were Sony PlayStation Network, the Hong Kong Stock Exchange, Zorz, Visa, MasterCard, and PayPal. According to DDoS security vendor Prolexic, DDoS attack incidents reported in 2019 were more than the total number of attacks reported in 2018. Arbor Worldwide Infrastructure reported DDoS as a top security threat on the cloud [7], and the number of incidents more than doubled compared with 2017, as shown in Figure 2.

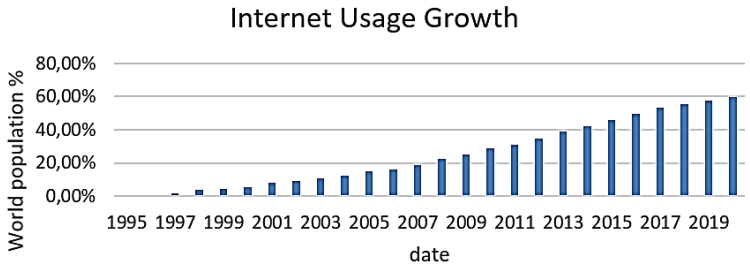

Figure 1. Growth of internet users

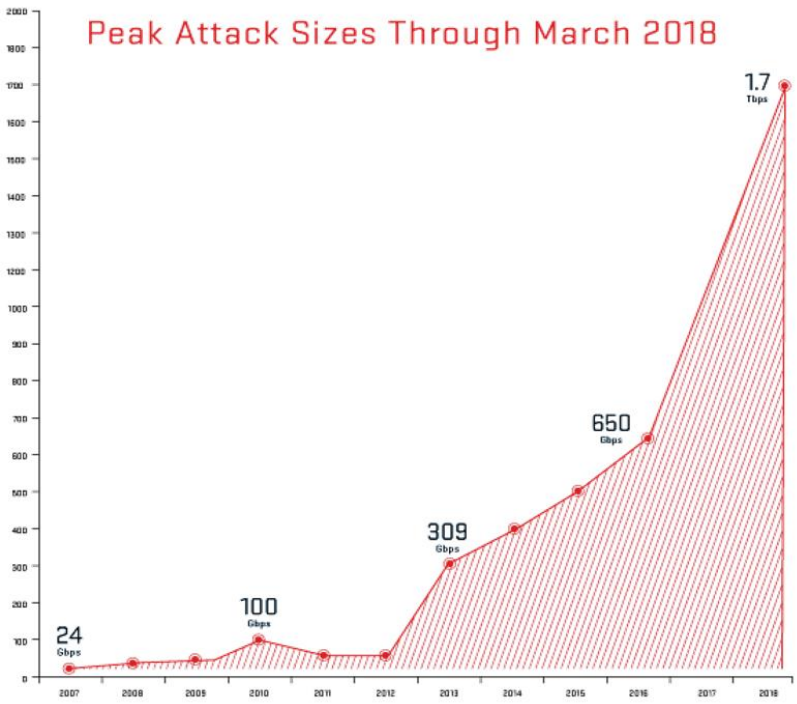

Figure 2. DDoS attack trends in 10 years

The major security companies are monitoring the digital world to analyze the threats on internet users and protect them from possible violations. Thus, every year, quarterly reports analyze and evaluate the

risk on network resources and propose possible solutions to minimize or reduce losses of the assets. Each report is represented as Q with numbers from 1 to 4 depending on its sequence in the report.

Paper organization: The remaining sections of this paper are as follows: Section 2 explains a brief history of DDoS Attacks and show last trends in 10 Years for the attacks, brief display for a mechanism of DRDoS attack then Classifying these attacks are presented in section 3 and 4 respectively, The conclusion of the work is shown in section 5.

2. A BRIEF HISTORY OF DDOS ATTACKS

DoS attacks date back to the late 1980s. Launching such attacks requires technical skills and performed using powerful computer resources. In the early 1990s, DoS attacks were performed using automated tools by compromising the computing resources of a vulnerable machine. Using such tools has facilitated attacks on any target. Consequently, this condition has led to an increase in DoS attacks by the early 2000 when businesses moved to embrace the internet, and the websites of countless companies, including Microsoft and Amazon, witnessed distributed denial of service (DDoS) attacks. DDoS attacks utilize more than one machine to launch DoS attacks in a coordinated manner.

DDoS attacks are often performed using automated tools that are transformed into launching attacks through malware (Trojan or worms) that carry DoS payloads. Once a computer is compromised by malware, the infected machine initiates an attack on the defined target at a specific time. When multiple infected machines attack the target, the magnitude of attack increases considerably [8], [9].

Recent DDoS attacks appear to have more control over the compromised machines. Instead of infecting the machine with malware that performs a specific task, a new generation of malware has been developed in the form of backdoors or bots. Bots allow attackers to have complete control over computers and can issue commands to infected systems to coordinate and launch DDoS attacks [10]-[12]. A group of infected machines are usually networked together to muster strength in launching attacks. Such a network of infected machines of bots is called a botnet. Since the mid-2000s, DDoS attacks originating from botnets have grown in magnitude and effectiveness as attackers start using redefined techniques to take control of computers to initiate more effective and powerful attacks as shown in Figure 3. Since then, botnets have become one of the most significant threats to the internet especially in web-based business transactions.

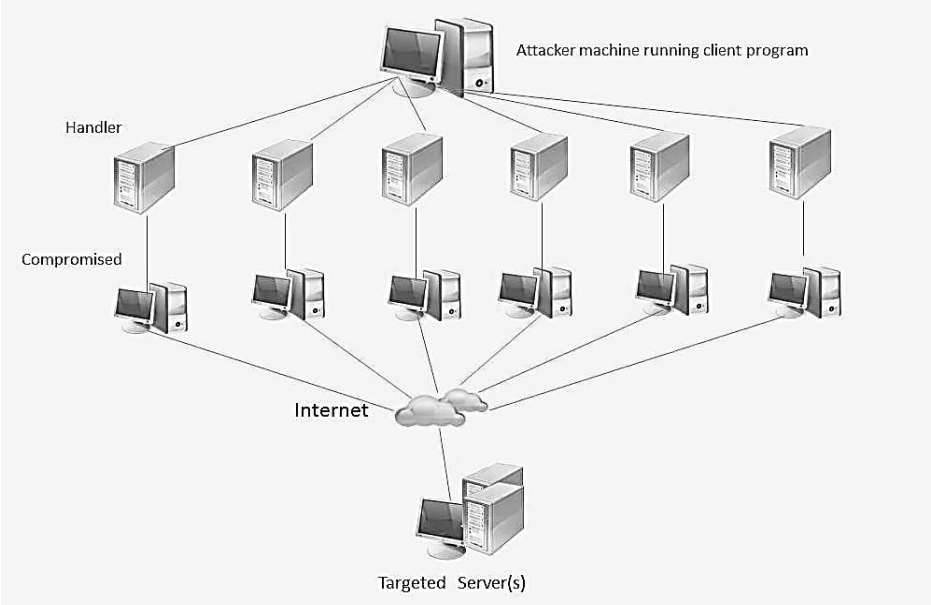

Figure 3. DDoS attack scenario

DDoS attacks aim to interrupt the supply of services by crippling network and storage capacity of the authorized users [13]-[15]. The main challenge in network security is how to ensure safety from the attacks; moreover, several types of attacks prevent legitimate users from using the services provided to them, and these types of attacks are called DDoS. The attackers update their methods to intensify the damaging effect of their actions on the victim side. Several years ago, the attackers produced an upgraded version of the

DDoS attack with huge destructive power and a new attack mechanism; this type is called distributed reflection denial-of-service (DRDoS) attack. The traditional defense techniques are helpless in a standoff against these types of attacks. Researchers have proposed several new methods to detect or mitigate the attacks. These techniques are produced based on several factors such as number of hosts in the network, architecture and speed of the network, and others. Each method has advantages and disadvantages. Some organizations or companies want to install defense methods but others may want to install it on the network side to minimize costs. Data traffic consists of two types, namely, packet or flow traffic. Thus, the data traffic and its features can influence the creation of the defense method. The defense method based on packet traffic is used in low-speed networks and focuses on one or more of these features: packet filter, packet similarity, packet size, packet per unit time, response packet size, and others. The method based on flow traffic is appropriate for transmitting a large amount of traffic through a high-speed network.

3. MECHANISM OF DRDOS ATTACK

The DRDoS attack differs from its predecessor, the DDoS attack, because it extends the DDoS attack by including IP spoofing while making the attack complex. This condition renders existing DDoS attack detection and mitigation techniques ineffective against DRDoS attacks. The distributed reflection DoS attack consists of two phases: first is IP spoofing to hide attackers by using the reflector and second is amplification used to maximize the size of responses relative to the request size [16]-[18]. The main feature of the DRDoS attack, which makes this type different from the DDoS attack, is that it does not assault the destination directly but rather sends demand packets through a go-between, an exploitable "reflector" that also involves spoofing the sender's IP address [19].

As Figure 4 shows the mechanism of amplification attack according to the following steps: the first step is the IP spoofing by the attacker by sending bots to broadcast spoofed demand packets that specify destination addresses as the prey address to the reflectors. Then, the reflectors respond to the demand with response packets and in a normal way send them to the prey. As an outcome, the prey is crushed by reflected reply packets [20].

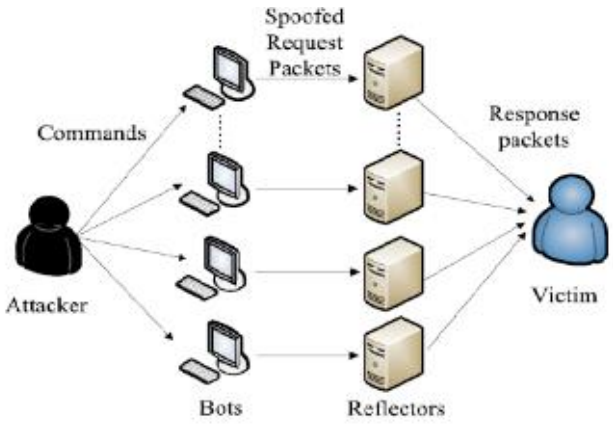

Figure 4. An illustration of the amplification attack

To make the attack strong and difficult to detect for that purpose the attacker be using the IP spoofing not only to hide identity but for the reason mention [21], in the beginning, this point and these techniques are employed in the DRDoS attack with the reflector which makes it distinct from the rest types attacks.

- The first part is the reflector, a legal host or hosts used by the attacker to flood the prey network or web server by generating slaves spoofing the prey address [22], [23].
- The second part is the amplifier (amplification), a third party used to increase the volume of traffic reflected by the victim considerably [24]. Amplification attacks cause serious challenges to network security because of their privacy and amplification characteristics [20].

The scale of the answer packet in some protocols is larger than that of a message packet. By abusing this function, attackers may generate a large volume of traffic [25] from a relatively small traffic volume. Abused servers are called amplifiers from this function [26].

4. CLASSIFICATION OF DRDOS ATTACKS

The DRDoS attacks can be classified into two kinds depending on the transport layer that we have used, as shown in Figure 5. Attacking nodes create several requests in which the IP address of the source is replaced by the IP address of the host being targeted. Such requests are sent to servers or other tools that can be used to represent network traffic. The responses to these questions are sent to the target node. The traffic reflection process increases the difficulty of finding the true source of the attack [27].

This study on the DRDoS attack based on the TCP protocol is found in the SYN and BGP, whereas the DRDoS attack based on UDP [28] protocol is found in DNS, NTP, SNMP, and SSDP. The DRDoS attack preferred the UDP on TCP because the three-way handshake method is used in the TCP/IP to check if the legality of the traffic is confirmed using a three-way handshake such that the amplification is not possible. The packet size is not amplified to the large size in the DRDoS attack because this type of attack cannot pass through the TCP/IP protocol. If it passes through this protocol, then the effect is minimal compared with the effect of this attack if amplification occurs. As shown in Figure 6, the most common DRDoS attack classes are shown by both the TCP and UDP protocols.

Increasingly rampant DDoS attacks, particularly attacks by DRDoS with UDPs, have become a global problem [29], [30]. DRDoS attacks, which focus on UDP reflection and amplification, can produce hundreds of gigabits per second of attack traffic, and has become a major threat to internet safety [31]. These attacks violate UDP-based network protocols that send a higher response compared with the request size. Many studies have also shown that UDP-based bandwidth amplification of DRDoS attacks can expand traffic by a factor of 500 [32], [33].

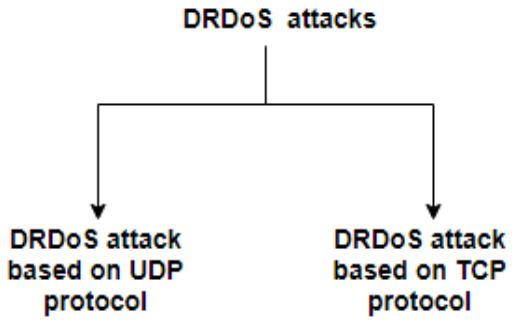

Figure 5. DRDoS attack classification

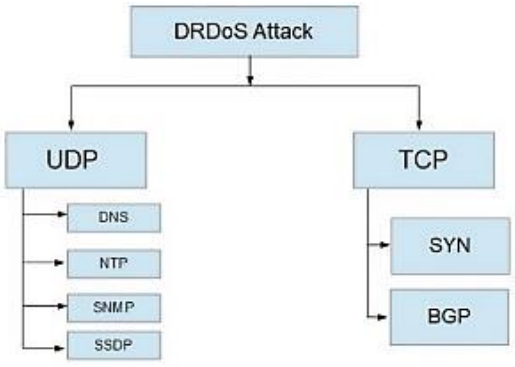

Figure 6. DRDoS attack in both TCP/UDP

4.1. DRDoS attacks based on TCP protocol

Many researchers have worked to improve the border gateway protocol (BGP) and enhance it by using various techniques to detect or mitigate attacks, especially DRDoS attacks. Thus, in our research area, we aim to shed light on the techniques used to detect and mitigate the BGP protocol by DRDoS attack. TCP-based DRDoS attacks were studied, but they only occur during the link establishment step due to the three-way handshake procedure and have no major amplification impact [31]. The protocols based on TCP, such as FTP and Telnet, have the highest number of amplifiers, as shown by data from scanning a random IP address for the popular protocols [34]. In Table 1, the authors review the strengths and weaknesses of each research paper discussed as well as the methods that were used.

Li *et al.* [35] the new kind of HTTP amplification assault is called Range-based Amplification assault. Two types of range-based amplification (RangeAmp) assaults are presented in this study, which enables attackers to exploit the vulnerabilities of Range implementation and harm CDNs' DDoS security mechanisms. Specifically, small byte range (SBR) and overlapping byte range (OBR) attacks are included in the RangeAmp attacks. In this type of attack not only the outgoing bandwidth of the origin servers deployed behind CDNs, but also the bandwidth of CDN proxy nodes can be massively depleted by attackers. The mitigation mechanism consists of three sides: server-side, CDN-side, and protocol-side. At the server-side, a local DOS defense is enforced. Requests for attacks are no different from harmless requests and come from CDN nodes that are widely spread. It is difficult for the source server to effectively protect against it without disrupting normal services. In the CDN-side, modify particular implementation on requests for range. Based on the characteristics of RangeAmp attacks, CDNs can detect and intercept malicious range requests but the important approach is to enhance the Range header handling policy. The SBR attack is triggered by the deletion policy and expansion policy. The Laziness strategy can therefore be followed by

CDNs to fully protect against the SBR attack. But this also makes it difficult for CDNs to benefit from spectrum demands. A safer approach is to follow the strategy of extension, but not to expand the range of bytes too far. At the protocol-side: A Revise an RFC that is well-defined and security-aware. RangeAmp risks are basically caused by vague definitions and inadequate security considerations of the specifications. On the mailing list of the HTTP working group, we will continue to address this threat. We believe that in a future updated RFC, particularly for the HTTP middle-boxes, a more precise limit of the Range header should be specified CDNs, like.

Miller and Pelsser [36] try to classify the attack that happened in BGP by using the Nlacholing technique in the BGP to mitigate DDoS attacks. The autonomous system (AS) is the part in which the internet consists of single or multiple networks controlled by one entity. However, BGP is a routing protocol with less authentication on the path source and checks the validity of the paths. The ASes can declare illegal paths for pseudo they do not have, pull part of the traffic to these prefixes or all.

Table 1. DRDoS research papers based on TCP protocol

No.	Ref	Collected security data	Analysis methods	Year	Target protocol	Advantage	Disadvantage	Detection location	Remarks
1	[35]	Request, Response, Response Traffic	Deletion and Expansion policy	2020	HTTP	improve the vulnerability points of the CDN.	the flaws of CDN increase worsen this vulnerability	Network side	detect and mitigate the RangeAmp assaults
2	[36]	IP source, IP destination	BGP blackholing	2019	BGP	emphasize the need for BGP community authentication, either through an extension to BGPsec or another mechanism.	still, there are some problems with BGPsec and may diverge from predictions, and from AS to AS. in some time legitimate traffic will be dropped off	Individual router	Detect BGP DRDoS attack only
3	[37]	Numbers of hops, TTL value, IP packet	Hop count filtering (HCF) based on analyze TTL	2016	BGP, NTP	the attacker cannot guess the number of hops between the host who wants to hack it and the receiver of the packet.	TTL is considered a security vulnerability for the system based on it	Multiple routers	Detect DRDoS attack in several protocol like PGB and NTP
4	[38]	Source MAC, destination MAC, srcIP, dstIP, sport, dport	ETD-BiRe: Evil Twin Detection -BiRe	2020	SYN/ ACK TCP/IP	it's can detect multi-model of ETAs (evil twin attack). no need to modify on the firmware and existing drivers.	it can't distinguish between evil twins and LAPs apart in parallel scenes without any previous information about LAPs	Client side	Detect SYN reflection and ETA

Backes *et al*. [37] proposed a solution based on the idea that the assailant cannot guess or juggle the number of leaps between the amplifier and victim. Hop-count filtering (HCF) technique is used to analyze the time-to-live (TTL) of entering packets. The authors investigated the assumption that the attacker does not discover the valid TTL value. By using a mixture of BGP data and trace routing, we construct analytical models that perform checks and evaluates the TTL within a threshold value. The drawback of the technique is that the assailant uses a mixture of BGP and trace routing data to construct analytical models in the threshold TTL value for the victim.

Lu *et al* [38] proposed a new mechanism that focuses on the reflection of SYN/ACK based on TCP protocol. This mechanism can detect the evil twin attack (ETA) in WLANs. The proposed mechanism consists of three stages: target access point (AP) set selection, reflection component, and judgment component. The first stage includes the search for the APs, and then selecting two or more that have an identical SSID; these select points are the entrance to the next stage. The second stage is the most important and is the core of the new mechanism to regulate the structural link between objective APs by using the TCP handshake through the demand–reply reflection of SYN/ACK packets. To start our mechanism, two co-op

WNICs on the client side are used to individually begin the TCP handshake and observe the obscurity of the predictable SYN/ACK packets in both directions. The result of this observation is the input to the next stage to execute the closing ETA confirmation. This mechanism is called bi-directional SYN reflection because it employs the reflection in the second stage. The last stage is responsible for deciding the presence of an ETA and distinguishes diverse ETA models depending on an outcome of bi-directional SYN reflection achieved by the second stage. The network environment can be classified by this stage into three states: a safe network, an unsafe network with series ETA, and an unsafe network with parallel ETA.

4.2. DRDoS based on UDP protocol

An attacker who plans to launch attacks such as a DRDoS attack exploits the UDP protocol to perform their attack because of UDP properties, which sometimes enable the abuse of vulnerabilities in the protocols. The DRDoS attackers exploit the policy and rules of UDP communication, especially those that belong to the increased size of the response for the request, and maybe a DRDoS attack that is employed to drive through these points and start their attack [16]. In Table 2, the authors review the strengths and weaknesses of each research paper discussed as well as the methods that were used.

The UDP provides many services through several protocols based on UDP as a transport protocol, and the policy does not verify the IP addresses of sources when responding to any request; thus, many servers, which are called "reflectors" due to their functionality, will be abused [26]. The UDP protocol allows the amplification/reflection of the response that will lead to producing hundreds or thousands of gigabits per second of attack traffic. Thus, the DRDoS attacks become an influential threat to internet security [31]. The huge UDP traffic is amplified by the attacker, and the attacker is directed to the target by flooding the bandwidth of the victim by using P2P networks to store agent attack data before the attack process [39].

Gao *et al*. [16] suggested a new approach that detects a DRDoS attack. When many packets appear frequently in shortened time and these packets consist only IP header without TCP or UDP header portion, as a result, that will lead to appear huge quantities of UDP packets with major volume. The amplification used in the DRDoS attack produces a gap between the size of the response to the request to be greater than the normal response size. The packet amplification factor in the DRDoS attack is larger than the bandwidth amplification factor based on the gross number of all sent packets to the destination at the period.

This behavior leads to difficulty in discovering the attack based on the total UDP packet volume. One protocol used to launch the DRDoS attack means that only one port is used to perform the attack and all packets pass through this port, thereby generating maximum traffic. This system consists of three parts: implementation, calculation of features, and detection. In each part, steps include collecting the data and focusing on the display of the packet states and the influx of the feature volume extract. Detection is based on a timer to decide whether an attack has occurred or not.

Wei *et al*. [17] suggested an algorithm called rank correlation-based detection (RCD), which has two scenarios: one attacker and many reflectors. In both scenarios, one of the attackers falsifies requests to the inverter and randomly arranges the first scenario with a steady rate, e.g., leaving bandwidth and the second scenario with a depressed but changing rate. The alarm is switched on 10 seconds after the occurrence of the attack. to distinguish the proportion of packet rate of assaulting from the legal streams by using a threshold; it's found that: We can distinguish the two correlation types with the wide domain of assault packet rate. The false negative and false positive can be fulfilled in low value. Once fishy streams are discovered, RCD begins to calculate the rank correlation between stream couples and produces a crucial warning depending on the preset sill.

Huang *et al.* [29] suggested a new solution called "increasing expenses and weak authentication" (IEWA) to protect the NTP protocol, which is a UDP-based protocol, from DRDoS attacks. The new method focuses on several factors such as communication overhead, server storage costs, client storage costs, computation costs of the server, and computation costs of the client. The Monlist can be abused by the attacker in the NTP protocol when it is enabled. Moreover, it contains the IP addresses of the last 600 clients. The proposed method IEWA is a strategy that combines growing expenses and low authentication.

The steady-state opportunity in the system when using the IEWA increases from 0.93 to 0.98. Two scenarios are assumed: First is that the number of client demands is not restricted, and second, we have restricted the number of client demands even though the client makes endless service demands that do not appear as a DoS attack. The IEWA strategy in this situation is proof against both DRDoS and DoS attacks.

The traditional or classical techniques for attack detection may be ineffective sometimes especially with the network that has huge data because of the impact of large network traffic that floods important signals of assaults. Therefore, Jing *et al* [20] suggested a method that uses sketch techniques to detect amplification assaults. The authors plan a reversible sketch based on Chinese remainder theorem (CRT-RS), which has been used to immediately gather network traffic and thereafter observe the unforeseen differences in a one-to-one mapping among demand packets and reply packets to distinguish amplification assault traffic.

At each row in CRT-RS, when the occurrence of aberrant buckets is discovered, the addresses of the reply packets are counted and blacklisted as a malignant provenance. To check if the incoming source address was in the blacklist, we use the abloom filter, and then if the IP address exists, then traffic filtering is performed. This study mainly aims to detect an amplification attack to utilize CRT-RS by analyzing traffic behavior and reconstructing the aberrant IP addresses in a reverse manner. This approach is a good and effective solution for large network traffic. This simple method is not needed as a requirement for recording the complex features of traffic. The final results show that this method carefully detects amplification assaults.

Lukaseder *et al*. [40] proposed a mechanism that works on classifying legal or illegal reply packets in DRDoS attacks. The packets receivable from the target host can be classified into four kinds: legal demands and replies and illegal demands and replies. The demand packets are isolated from the reply packets, which are based on UDP protocol. The malicious replies should be filtered because DRDoS attacks can only come from replies. The mitigation scheme of DRDoS analyzes and filters only these reply packets based on the analysis of the incoming replies to distinguish between legal and illegal replies. The replies are legal if and only if the destination host sends comparable demands in advance. For this purpose, modified NAT is applied when the attack occurs. NAT is activated and the origin IP address of the assault goal is a substitute through the alias IP address outside UDP-based demands. The second differentiator isolates the demands from the replies to be eligible for use NAT only for the outside demands not for outside replies.

The pseudonym IP address has to be more complex to be guessing, so it's not comfortable potential for an attacker to shift their assault to the pseudonym IP address. However, the attacker can disclose the pseudonym IP address if the network traffic is monitored at the goal. For this reason, one can change the address in an orderly manner through a grace period.

Deli *et al*. [41] suggested a fully automatic analysis tool. When measuring the amplification factor for several protocols, the researchers show that these protocols and servers are vulnerable according to their mechanism. The measurement and identification both rely on traffic information from specific ISP, and distinguishes the questionable traffic stream that has a particular style, such as height amplification factors. The model suggested by the authors consists of three parts: attacker, amplifier, and victim. Each part complements the others to complete the work of this model. The first part (attacker) wants to tuck the maximum bandwidth of the prey by reflecting a massive volume of amplified traffic by using the second part. Then, in the second part, some protocols attract the attacker because of their vulnerable points that build-up in the server, and most of these protocols are based on UDP in transmissions. When a server replies to the request from the client, sometimes the size of the reply packet is larger than the request size and appears to be an abnormal reply. This feature can be exploited when spoofing IP address is potential from the first part side. When the first part sends the data, the third part is not the immediate goal. However, the prey undergoes overcrowding in traffic, which is sent from the second part.

Mittal [42] focuses on the NTP protocol and how to protect this protocol from DRDoS attacks. To detect and mitigate the DRDoS attacks, the suggested model uses a graphical processing unit (GPU) with the prey machine called hybrid computing system. The results showed that the hybrid (CPU–GPU) computing machine is better than the simple machine (CPU only) and more effective in amplification response. When this model was tested, five systems were employed: attacker, compromised, reflector (NTP server), prey machine, and legal user. The attacker uses the Metasploit tool to establish a link with the weak machines after searching for the weak points in the system. When this link is found, the connection is obtained. The attacker starts posting demands to synchronize with the reflector by sending UDP demand packets to the NTP server through IP spoofing. The attacker uses Bit-Twist tool to capture the aforementioned packets and modifies the origin IP address. The Monlist contains the last 600 hosts that link to the NTP server. This leads to the creation of 600 modified packages, which are sent to NTP through the compromised system through Monlist rule by Bit-Twist tool help. Huge traffic floods the NTP server by using the Bit-Twist tool, which generates a new Monlist content that is posted with details to the prey linked to the NTP server. Three main influential factors (CPU, main memory, and bandwidth) are used to compare the hybrid and normal systems before and after the attacks. Our hybrid machine system shows that the CPU consumption decreases and response is better during the DRDoS attack when using the system rather than a normal machine. Also, memory in the hybrid machine is less than what is needed in the normal machine. However, our hybrid machine cannot reduce the effectiveness of the DRDoS attack on the bandwidth. During the occurrence of the attack, the legal users were unable to use services as a result of the large traffic that saturates the bandwidth. Nevertheless, the hybrid machine in the experiment is better than the normal machine. The attacks in the past years have shown a new mechanism and numerous effects on the victim's side. A critical aspect is the reflection/amplification assault, which has many types, including store and forward DRDoS (SF-DRDoS) based on the idea of store and flood at peer-to-peer networks. These attacks demonstrate a large amplification factor.

Fraiwan *et al.* [39] proposed a new method to detect and mitigate these types of attacks based on crawling and filtering. The new defense strategy is based on distinguishing potential reflector nodes by simulating the attackers' demeanor besides foiling their actions. It is possible to get information concerning potential reflector nodes through crawling Kad in every limited period time. In this condition, a Bloom filter is used to discover anomalous traffic at this moment with large filenames. Then, after the filtering is completed to exclude the onslaught packets, the crawling techniques that exist in the literature can be classified into two classes: iterative and recursive. Often, the iterative crawling fails to find some nodes and crawls to the identical nodes. This situation leads to wasted bandwidth and increment ID space. Two critical metrics are used in the crawling process evaluation: accuracy of the crawler and traffic cost-effectiveness (TCE). Based on the aforementioned metrics, the recursive crawling is best in detecting potentially large numbers of nodes than the iterative crawling with high TCE value. When one of the specific inputs is equal to 0, the filter does not filter the nodes and allows packets to push through. When they are all 1, the node is presumably inserted into the filter without any false positives.

Chen *et al*. [43] have employed two modern techniques, namely, SDN technique and ML algorithm, to produce and design a new system that is able to detect and prevent a DRDoS package automatically. The proposed system consists of two main components: detection agent and open networking operating system (ONOS). The first component, i.e., the detection agent, consists of two parts: the first part is responsible for observing the network by using netmate tool, and the second part is created through a machine learning algorithm called a classifier. The second main component, which is the ONOS, works in a manner similar to the SDN controller. It provides an OpenFlow protocol and allows various RESTful APIs to determine specific vectors in a limited time interval. Then, the result is used to teach a prototype by ML algorithms to classification by using a netmate tool. The next step is training the ML model. In training, both regular and malignant flows of DNS requests and responses are required. During the reflection attack, the increase of the stream to the victim occurs by posting a huge amount of demands in a short time. This operation to produce huge response packets to the reflect, continuously the attacker asking for special domain names plus several fixed orders. The standard deviation from the attackers' side in packet size appears to be zero. The pattern of traffic is dissimilar to that of normal ones. As the average volume of response packets is larger than regular and the standard deviation is near zero ... so by chosen, each feature is linked to backward packets. Only the chosen packets are checked, and this feature decreases the load on the detection agent.

Meitei *et al.* [44] employed two important techniques: machine learning (ML) algorithms and attribute selection algorithms. The first part is the ML algorithms, which uses four supervised ML algorithms: decision tree, multilayer perceptron, naïve Bayes, and SVM. Furthermore, they used three attribute selection algorithms: information gain (IG), gain ratio (GR), and chi-square, which are applied to the chosen parameters. The main task of this study is to analyze the DNS queries.

Three important steps taken to complete the suggested scheme are the method of how to select parameters, how to train and test ML algorithms, and the way of parameter diminution. chosen eight elected statistical feature dataset i.e. arrival time of the packet, occurrence of IP per unit time, answer and authority and additional of resource records, and minimum and maximum and an average of packet size. The next step is training and testing by using the classification and clustering algorithm for the selected features by selecting the same number of IP addresses for both normal and attack DNS queries. By using the feature selection algorithms IG, GR, and chi-square to diminish repetitive parameters and drop unnecessary features, both operations minimize computational time and exhibit high detection accuracy.

To detect DNS amplification attacks, Cai *et al*. [45] focus on three features that affect the detection method according to their vision. These features are used in the DNS server to discriminate the normal a certain time from that abnormal. These features are recurrence of DNS demands, rate of amplified data traffic at a certain time (reply traffic/demand traffic), and amount of grown packet in a certain period. The third feature, which is the ratio of the number of the response packets to that of demand packets in one unit time, not only increases the accuracy of detection however it be easier to determine real-time data. A K-means machine-learning algorithm is used to distinguish between the normal and abnormal packets by classifying them into abnormal and normal clusters, after classifying the packets into clusters through K-means algorithm from the detection model and determining the reference points. The main drawback of the study may be the method of determining the weight per feature and placing the same weight on the three features.

Böttger *et al*. [24] suggested a model for detection amplification attacks; this model relies on observing and distinguishing traffic. When a client wants to connect to the server, a PairFlow is formed. Many UDP flows are also produced by aggregating those collections of flows. The PairFlow appears and contains the client IP, IP and port of the server, payload dispatch to the server, payload dispatch to the client, and recording period interval for the PairFlow to determine average rates. In the test stage, we select a certain time, i.e.,10 minutes for the PairFlow, as active/inactive in that time interval.

Additional criteria are used to detect amplification attacks, i.e., request and response packet size similarity, request and response payload, similarity, unsolicited messages, and IP spoofing. The attacker sometimes attempts to avoid detection, i.e., low traffic generates a low attack factor less than our detection threshold. If payload entropy and demand packet lengths can be adapted, then the mass of attack traffic need not be diminished. Minimizing the detection threshold is possible to detect the low attack factor but at the same time increases the false positive alarm.

Liu *et al*. [46] one of the main reasons for increasing the reflection attacks on SSDP is the proliferation of IoT devices. Previously many approaches were suggested to detect and mitigate the Reflection attacks on SSDP but this method is more effective and modernity because it employs the bots as defense methods and this approach is called a multi-location defence scheme (MLDS). Three principal features that distinguish it from other approaches are: the mechanism of the MLDS begins from assault source to prey via assaulting link, also not based on detection of assaults, and the main and novelty key is to utilized bot as defenders. The deployment of various protection strategies to multiple locations from the above study will make the defence work efficiently in the entire attack link, from the source initiating the attack to the victim. This is why we are developing the MLDS.

Kim *et al*. [47] proposed a method to prevent the DNS amplification attacks. by utilizing the history queries of DNS based on SDN they proposed a method to prevent the DNS amplification attacks. This technique proactively and reactively acts to reduce the effects of these attacks on native DNS servers. there are two kinds of DNS packets are A and ANY, the A for normal packets, and ANY for the attacker packets. The proposed mechanism relies on a one-to-one technique, i.e., for each response, a corresponding request exists. The orphan pairs are classified as suspicious immediately, thereby enabling the protection of the local DNS servers. it contains two principal components are switch and SDN controller. Understanding the behavior of any attack is important to produce the perfect technique to detect or mitigate from that type of attack.

Thus, Huistra [48] focuses on the fingerprints of the attack, and because the attacks that are attacking the DNS are the most famous types of DRDoS attack, this work focuses on DNS attacks and how to distinguish and analyze the behavior of the DNS attacks. When designing a detection scheme for DNS reflection attack, this work needs much information to obtain excellent results. Some of the information include the IP address of both the host and the server, the request and reply time of DNS, the size DNS request and its response, and source, destination port for DNS query. The scenario of this approach depends on the consistent size of both the request and response. When the size of the request and response is inconsistent, the attacker exploits this feature. Furthermore, the attacker can employ a small or large number of DNS servers for the attack. In the NetFlow scenario, some information is lost, i.e., the size of every packet and individual capture time because of the aggregation method. This study does not include detection of attacks that use various sizes of requests.

El Houda *et al*. [49] the suggested model called WisdomSDN that used to detect and mitigate the DNS amplification attacks.the restricted and monitoring on DNS requests/responses by using a one-to-one technique to recognize the illegitimate DND demands and replies. the results show that the WisdomSDN achieves a high rate of detection and a low rate of false-positive. Dodia and Zhauniarovich [50] this method focus on filtering garbage traffic to prevent upcoming amplification demands from accessing amplifiers inside the provider network, protecting vulnerable services from abuse. this prototype will track spoofed traffic and filter it out at the ISP network's edge. This eliminates garbage traffic caused by network amplifiers, saving ISPs and their customers time and money.

5. CONCLUSION

This study focused on cybersecurity because the number of internet users is growing dramatically and the various devices connected to the internet are the main challenge in the field of security. When it is denial legitimate user from the services that are provided. The DoS attack is a popular form of these challenges. The more effective version is the distributed DoS attack, but attackers improve the DDoS attacks to produce robust attacks with devastating effects on the victim’s side. This attack is called the DRDoS attacks, which has been the focus of network security research in previous years because of the volume of attacks and their effects. This type of attacks prefers the UDP protocols. Thus, most of the papers focused on the services that rely on UDP protocols. We compared the papers in terms of method used and the feature selection as well detection performance. To the best of our knowledge, our paper is the first to classify this type of attack based on transport protocols, such as DRDoS attacks based on TCP protocol and DRDoS attacks based on UDP protocol. We aim to focus on a special protocol in the future, which is the most popular among other protocols that have been and will continue to be the target of DRDoS attacks.

APPENDIX

Table 2. DRDoS research papers that based on UDP protocol

No.	Ref	Collected security data	Analysis methods	Year	Target protocol	Advantage	Disadvantage	Detection location	Remarks
1	[20]	packet header, sum of packet sizes, number of packets,	Chinese Remainder Theorem based Reversible Sketch	2019	Any protocols abuse by amplification	it is efficiently used for huge size network traffic at the prey end. it's less complex and is not sensitive to the detection interval.	its consume more time in detection.	Victim end	Detect amplification attacks
2	[40]	Source IP, destination IP, source UDP port, destination UDP port	NAT packet filtering with SDN	2018	Any UDP protocols abuse by DRDoS attack	It's a good defense mechanism for DRDoS attacks.	it's not suitable for application protocol. Its not detection method	Reflector end	Defense method for DRDoS attack
3	[41]	Origin IP flow , destination IP flow , origin port flow , destination port flow,	Flow analysis	2017	Multi protocols	reduce the statistics errors.	because our analysis relies on the traffic, for this reason, there is no guarantee of the accuracy of identification. it will allow low amplification to pass	Victim end	Detect DRDoS attack
4	[17]	Flow rate	The similarity of packet rate	2013	Protocol independent	effectively and efficiently it can distinguish between legitimate and reflection flow.	not suitable for attackers to share a different set of reflectors.	Victim end with multiple routers	Detect two typical scenarios of DRDoS attack
5	[16]	The number of packets, packet size.	SVM algorithm	2016	UDP based protocol	The detection method based on packet counting has been improved. the detection performance has been improved compared to the previous methods	it employs to protect a specific target not full network	End-user	Detect DRDoS attacks under a certain assumed condition
6	[44]	Packet size, packet arrival time, and IP occurrence rate,	Machine Learning Classification algorithm	2016	DNS	It achieves 99.3% accuracy by using the decision tree. Reduce the number of parameters and time testing.	the result some time may be inaccurate because it uses a statistical method. Not suitable for the encrypted packets.	Victim end	Analyze only DNS query traffic
7	[45]	The number of packets, packet size, Respons size, Request size	K-means algorithm	2016	DNS	write down an IP address for every packet is not necessary. it increases the accuracy of detection in real-time data	the way of calculating the weight about per feature. sometimes the point is overlap or the distance between them is not clear. There is no timestamp.	Network end	Specify attack pattern using three features
8	[24]	Packet size, TTL values, number of packets	Match attack rule	2015	NTP	Added new features to enhance the detection model. detection method has enhanced to thwart new DRDoS attacks	Can't detect low attack factor. when the amplification traffic comes encrypted this approach will fail. this approach not suitable for the multiplied uplinks.	Network end	Use some additional features to detect DRDoS attacks

Table 2. DRDoS research papers that based on UDP protocol *(Continue)*

No.	Ref	Collected security data	Analysis methods	Year	Target protocol	Advantage	Disadvantage	Detection location	Remarks
9	[46]	TTL, SSDP Requests, SSDP Responses	Multi-location defense mechanism	2019	SSDP	Employing the bots to act as defenders to get more effectiveness and make the defense starts from the attack source via the link of the attack.	TTL value will affect the effectiveness of the defense.	Host / Network end	Detect the reflection attacks on the IoT devices
10	[47]	Source and destination IP address	SDN with history of DNS Queries	2017	DNS	The possibility of FP packets can be removed. memory limitation has Been resolved by using SDN.	when the size of DNS queries increased then the system have a communication delay	Network end	Detect DNS amplification attack at a local DNS server
11	[48]	Number of packets IP client, IP server, Time DNS request and reply, size of DNS request and reply, source and destination port of DNS query	Match attack rule	2013	DNS	show high accuracy to distinguish between the legal DNS traffic from DRDoS attacks. Depends on strict inspection of the packet	the method does not have enough flexibility to deal with requests and responses If they get together. it's not suitable for high-speed network	Network end	Analyze several scenarios of DRDoS attacks
12	[39]	Packet size, Number of the packet, file ID, file name, file size,	packets filtration	2018	P2P networks (Kad protocol)	Detect the new type of DRDoS attack called reflective amplification attacks (i.e., Store and Forward DRDoS attack.	the analysis of the packets does not give the high accurate to decide whether attack or not in some network traffic, especially in big networks traffic.	Reflector side	Analyze a specific type of reflective amplification attack called Store and Forward DRDoS attack.
13	[29]	Packet filter, MONLIST, IP client, IP destination, time-consuming	IEWA scheme with SMP	2019	NTP	the steady-state availability with the improved protocol has increased from 0.93 to 0.98	it consumes the time and this approach Only tested with 5G network	Network end	Detect NTP DRDoS attack only
14	[42]	SorIP, DesIP, SorPort, DesPort, MONLIST	hybrid system with additional Hardware	2015	NTP	it consumes less CPU and memory and the packet loss is very small	the consume of bandwidth can't be mitigated	Victim end	It uses a defense mechanism from DRDoS attack
15	[43]	SorIP, DesIP, SorPort, DesPort, protocol,	SVM algorithm	2017	DNS, NTP	it can detect known unknown attacks. The detection accuracy is high.	it cannot detect low rate attack	Victim end	Detect both DNS/NTP amplification attacks
16	[49]	source IP address, UDP port Source, and ANY DNS requests.	WisdomSDN	2020	DNS	the rate of detection is high. the rate of false-positive is low.	difficult to set a proper threshold value. the time delay between SDN and the switch may be influencing the performance of the model.	Victim network	DNS amplification attacks
17	[50]	Victim IP, Port, SDN controller	SDN and filter traffic	2019	UDP	QoS has been improved. save the resources of ISP	chose a proper value to predefined threshold is very difficult.	Network end	DRDoS attacks

REFERENCES

[1] R. R. Nuiaa and A. A. Kazm, "A Survey of Mobile Cloud Computing: Secure Channels Transmission in Mobile Cloud Computing," *J. Coll. Educ.*, vol. 1, no. 22, pp. 745–758, 2016.

[2] Miniwatts Marketing Group, "Internet world stats," 2020. [Online]. Available: https://www.internetworldstats.com/emarketing.htm.

[3] S. Setti and A. Wanto, "Analysis of Backpropagation Algorithm in Predicting the Most Number of Internet Users in the World," *J. Online Inform.*, vol. 3, no. 2, pp. 110–115, 2019.

[4] M. Meeker and L. Wu, "Internet trends 2018," Kleiner Perkins, 2018. [Online]. Available: https://www.kleinerperkins.com/perspectives/internet-trends-report-2018/.

[5] M. Salahuddin and J. Gow, "The effects of Internet usage, financial development and trade openness on economic growth in South Africa: A time series analysis," *Telematics and Informatics*, vol. 33, no. 4, pp. 1141–1154, 2016, doi: 10.1016/j.tele.2015.11.006.

[6] R. R. Nuiaa, "Energy Efficient Mobile Data Collection in Three Layered Wireless Sensor Networks," *J. Educ. Coll. Wasit Univ.*, vol. 1, no. 25, pp. 443–456, 2017, doi: 10.31185/eduj.Vol1.Iss25.131.

[7] C. Morales, "NETSCOUT Arbor confirms 1.7 Tbps DDoS attack; the terabit attack era is upon us," [Online]. Available: https//asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us.

[8] X. Yang, B. Han, Z. Sun, and J. Huang, "Sdn-based ddos attack detection with cross-plane collaboration and lightweight flow monitoring," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8254079.

[9] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/1283472.

[10] A. Wang, W. Chang, S. Chen, and A. Mohaisen, "Delving into internet DDoS attacks by botnets: characterization and analysis," *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, pp. 2843–2855, 2018, doi: 10.1109/TNET.2018.2874896.

[11] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: trends and challenges," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015, doi: 10.1109/COMST.2015.2457491.

[12] A. R. Yusof, N. I. Udzir, and A. Selamat, "Systematic literature review and taxonomy for DDoS attack detection and prediction," *Int. J. Digit. Enterp. Technol.*, vol. 1, no. 3, pp. 292–315, 2019, doi: 10.1504/IJDET.2019.097849.

[13] 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*, 2020, pp. 389–419, doi: 10.1007/978-3-030-22277-2_15.

[14] W. Zhijun, L. Wenjing, L. Liang, and Y. Meng, "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey," *IEEE Access*, vol. 8, pp. 43920–43943, 2020, doi: 10.1109/ACCESS.2020.2976609.

[15] P. Gulihar and B. B. Gupta, "Cooperative Mechanisms for Defending Distributed Denial of Service (DDoS) Attacks," in *Handbook of Computer Networks and Cyber Security*, 2020, pp. 421–443, doi: 10.1007/978-3-030-22277-2_16.

[16] Y. Gao, Y. Feng, J. Kawamoto, and K. Sakurai, "A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation," in *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, Aug. 2016, pp. 80–86, doi: 10.1109/AsiaJCIS.2016.24.

[17] W. Wei, F. Chen, Y. Xia, and G. Jin, "A rank correlation based detection against distributed reflection DoS attacks," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 173–175, 2013, doi: 10.1109/LCOMM.2012.121912.122257.

[18] I. M. Tas, B. G. Unsalver, and S. Baktir, "A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism," *IEEE Access*, vol. 8, pp. 112574–112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[19] S. B. Kumar, K. Mukherjee, and R. K. Dwivedi, "Secured Cloud System Using Deep Learning," in *Computational Intelligence in Pattern Recognition*, 2020, pp. 503–510, doi: 10.1007/978-981-15-2449-3_42.

[20] 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, doi: 10.1016/j.jnca.2019.06.007.

[21] S. N. Shiaeles and M. Papadaki, "FHSD: an improved IP spoof detection method for web DDoS attacks," *Comput. J.*, vol. 58, no. 4, pp. 892–903, 2015, doi: 10.1093/comjnl/bxu007.

[22] P. Revathi, "Flow and rank correlation based detection against Distributed Reflection Denial of Service attack," in *2014 International Conference on Recent Trends in Information Technology*, 2014, pp. 1–6, doi: 10.1109/ICRTIT.2014.6996117.

[23] T. Horak, P. Strelec, L. Huraj, P. Tanuska, A. Vaclavova, and M. Kebisek, "The Vulnerability of the Production Line Using Industrial IoT Systems under DDoS Attack," *Electronics*, vol. 10, no. 4, p. 381, 2021, doi: 10.3390/electronics10040381.

[24] T. Böttger, L. Braun, O. Gasser, F. von Eye, H. Reiser, and G. Carle, "Dos amplification attacks–protocol-agnostic detection of service abuse in amplifier networks," in *International Workshop on Traffic Monitoring and Analysis*, 2015, pp. 205–218, doi: 10.1007/978-3-319-17172-2_14.

[25] S. Karapoola, P. K. Vairam, S. Raman, and V. Kamakoti, "Net-Police: A network patrolling service for effective mitigation of volumetric DDoS attacks," *Comput. Commun.*, vol. 150, pp. 438–454, 2020, doi: 10.1016/j.comcom.2019.11.034.

[26] D. Makita, "A Study on Observation of DRDoS Attacks for Proactive Countermeasure and Real-time Response," Yokohama National University, 2017, doi: 10.18880/00010947.

[27] Y. Bekeneva and A. Shorov, "Development of protection mechanisms against DRDoS-attacks and combined DRDoS-attacks," *Vibroengineering PROCEDIA*, vol. 12, pp. 178–183, 2017, doi: 10.21595/vp.2017.18546.

[28] D. Kshirsagar and S. Kumar, "A feature reduction based reflected and exploited DDoS attacks detection system," *J. Ambient Intell. Humaniz. Comput.*, pp. 1–13, Jan. 2021, doi: 10.1007/s12652-021-02907-5.
[29] H. Huang, L. Hu, J. Chu, and X. Cheng, "An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks," *IEEE Access*, vol. 7, pp. 175970–175979, 2019, doi: 10.1109/ACCESS.2019.2957565.
[30] I. Ko, D. Chambers, and E. Barrett, "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 53–70, 2020, doi: 10.1007/s10207-019-00453-y.
[31] B. Liu, S. Berg, J. Li, T. Wei, C. Zhang, and X. Han, "The store-and-flood distributed reflective denial of service attack," in *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, 2014, pp. 1–8, doi: 10.1109/ICCCN.2014.6911808.
[32] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," *Network and Distributed System Security Symposium*, 2014, doi: 10.14722/ndss.2014.23233.
[33] L. Berti-Equille and Y. Zhauniarovich, "Profiling DRDoS attacks with data analytics pipeline," in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 2017, pp. 1983-1986, doi: 10.1145/3132847.3133155.
[34] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Hell of a Handshake: Abusing {TCP} for Reflective Amplification DDoS Attacks," *Proceedings of the 8th USENIX Conference on Offensive Technologies*, 2014.
[35] W. Li *et al.*, "CDN Backfired: Amplification Attacks Based on HTTP Range Requests," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2020, pp. 14–25, doi: 10.1109/DSN48063.2020.00022.
[36] L. Miller and C. Pelsser, "A Taxonomy of Attacks using BGP Blackholing," in *European Symposium on Research in Computer Security*, 2019, pp. 107–127, doi: 10.1007/978-3-030-29959-0_6.
[37] M. Backes, T. Holz, C. Rossow, T. Rytilahti, M. Simeonovski, and B. Stock, "On the feasibility of ttl-based filtering for drdos mitigation," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, 2016, pp. 303–322, doi: 10.1007/978-3-319-45719-2_14.
[38] Q. Lu, R. Jiang, Y. Ouyang, H. Qu, and J. Zhang, "BiRe: A client-side Bi-directional SYN Reflection mechanism against multi-model evil twin attacks," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101618.
[39] M. Fraiwan, F. Al-Quran, and B. Al-Duwairi, "Defense Analysis Against Store and Forward Distributed Reflective Denial of Service Attacks," in *2018 International Conference on Innovations in Information Technology (IIT)*, 2018, pp. 111–116, doi: 10.1109/INNOVATIONS.2018.8605972.
[40] 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.
[41] G. Deli, S. Shiqi, and M. Tran, "Automatic Identification of the Potential Amplifiers in DRDoS Attacks," *Final Report, CS6231 AY 2016/2017*, 2016.
[42] M. Mittal, "Defence Mechanism of Distributed Reflective Denial of Service (DRDOS) Attack by using Hybrid (CPU-GPU) Computing System," *International Journal of Computer Trends and Technology*, vol. 27, 2015, Art. no. 106, doi: 10.14445/22312803/IJCTT-V27P106.
[43] C. C. Chen, Y. R. Chen, W. C. Lu, S. C. Tsai, and M. C. Yang, "Detecting amplification attacks with software defined networking," in *2017 IEEE conference on dependable and secure computing*, 2017, pp. 195–201, doi: 10.1109/DESEC.2017.8073807.
[44] I. L. Meitei, K. J. Singh, and T. De, "Detection of DDoS DNS amplification attack using classification algorithm," in *Proceedings of the International Conference on Informatics and Analytics*, 2016, pp. 1–6, doi: 10.1145/2980258.2980431.
[45] L. Cai, Y. Feng, J. Kawamoto, and K. Sakurai, "A behavior-based method for detecting DNS amplification attacks," in *2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2016, pp. 608–613, doi: 10.1109/IMIS.2016.88.
[46] X. Liu *et al.*, "A Multi-location Defence Scheme Against SSDP Reflection Attacks in the Internet of Things," in *Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health*, 2019, pp. 187–198, doi: 10.1007/978-981-15-1922-2_13.
[47] S. Kim, S. Lee, G. Cho, M. E. Ahmed, J. P. Jeong, and H. Kim, "Preventing DNS amplification attacks using the history of DNS queries with SDN," in *European Symposium on Research in Computer Security*, 2017, pp. 135–152, doi: 10.1007/978-3-319-66399-9_8.
[48] D. Huistra, "Detecting reflection attacks in DNS flows," 2013.
[49] Z. A. El Houda, L. Khoukhi, and A. S. Hafid, "Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 4, pp. 2523–2535, 2020, doi: 10.1109/TNSM.2020.3014870.
[50] P. Dodia and Y. Zhauniarovich, "Poster: SDN-based System to Filter Out DRDoS Amplification Traffic in ISP Networks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2645–2647, doi: 10.1145/3319535.3363277.

BIOGRAPHIES OF AUTHORS

Riyadh Rahef Nuiaa is received a B.Sc. in Computer Sciences in 2004 from Baghdad College of Economics sciences University, Baghdad, Iraq. completed the M.Sc. In Information System/Computer sciences in the year 2014 from the college Osmania University, India. Now he is enrolled as a Ph.D. student from December 2019 in National Advanced IPv6 Centre/Universiti Sains Malaysia. He has worked as a lecturer at Wasit University/Iraq in the areas of Cloud computing, computer theory, and operation systems. His research interests network Cloud Computing, Cybersecurity, and Data Mining.

Selvakumar Manickam is an associate professor and researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He has authored and co-authored almost 170 articles in journals, conference proceedings and book reviews. He has graduated 13 PhDs and many Masters and FYP students. He has given several key note speeches as well as dozens of invited lectures and workshops at conferences, international universities and for industry. His research interest includes Cybersecurity, Cloud Computing, Software Defined Network, IPv6, Internet of Things (IoT) and Open Source Technology.

Ali Hakem Alsaeedi is completed B.Sc. in Computer Sciences in 2006 from the college of sciences at University of Al-Qadisiyah, Diwaniya, Iraq. Received his M.Sc. (master) in computer sciences in the year 2016 from the college of computer sciences at the Yildiz Technical University (YTU), Istanbul, Turkey. He has worked as a lecturer at a number of the Iraqi Universities in the areas of Artificial Intelligent, Data mining, and signal processing. He currently works as a lecturer in the University of Al-Qadisiyah. His research interests machine learning, smart optimization algorithms, and optimization of Big Data. Ali has several publications in the areas of the binary of metaheuristic optimization and data mining.