International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Experimental Study on Assessing the Efficacy of Feature-Based Methods in Identifying DDoS Attacks Against SDN Controllers

Monika Dandotiya[1]*, Dr. Rajni Ranjan Singh Makwana[2]

Submitted: 19/01/2024 **Revised**: 28/02/2024 **Accepted**: 05/03/2024

Abstract: A Software-Defined Network (SDN) provides several benefits to the networking industry via flexibility and centralized administration; nevertheless, this centralized control leaves it vulnerable to many forms of attacks. As a common tactic, attackers often use Distributed Denial of Service (DDoS) attacks to render the controller inoperable. To detect DDoS attacks on SDN controllers, entropy-based approaches & variants are believed to be most successful. Three modules comprise this system: traffic gathering, flow table delivery, and DDoS attack detection. To be ready for traffic identification, the traffic gathering module gathers traffic parameters. A DDoS attack detection system that takes advantage of flexible & multi-dimensional features of SDNs works by having the controller take data from statistics flow tables and apply a support vector machines (SVM) method to recognize attack traffic. The flow table delivery module then uses the traffic identification result to dynamically adjust the forwarding policy, therefore defending against DDoS attacks.

Keywords: *Software-defined networking, Entropy, Controller, Attack detection, DDoS.*

1. Introduction

Network services containing crucial business and industry data are influencing modern society's production and daily lives as a result of the exponential progress of the Internet economy, the incessant improvement of network technology, and the ever-increasing network business requirements. Network services may experience disruptions as a result of DDoS attacks, which may have devastating financial and other effects. One of the most important risks to Internet network security is DDoS attacks. Finding better and faster ways to identify DDoS attacks is an important area of study in the security industry [1].

SDN is an innovative architecture comprising three distinct layers: control, application, and data [2]. Notably, the data and control planes operate autonomously from one another. Switches & routers make up the data plane, which is responsible for forwarding network traffic. NOX, POX, Floodlight, Beacon, & Open Daylight are controllers that make up the control plane. Applications that configure SDN are located in the application plane. Under a DDoS attack, the SDN controller loses centralized control and cannot react to regular traffic from the rest of the network. Because of this, DDoS attacks pose a threat to the primary advantage of SDN, which is centralized network control [3].

Most of the current research in this area has concentrated on improving either the efficiency or the accuracy of DDoS attack detection & classification utilizing a single controller and several techniques, rather than aiming for both.

Data centers must take precautions to prevent DDoS attacks on their many controllers. Different levels of network traffic are tolerated by each of these controllers. As an option for obscuring the identity of the attacker in such an attack, spoofing source (also dubbed a fake source address) is one method [4][5].

In addition, for the malicious packets to be delivered, attackers try to flood the target with fake packets. Here are the reasons for these attacks [6]: For example, in a conflict between two groups or even just two people, a DDoS attack may disable the opponent's applications and infrastructure.

In cyber warfare, which can have political or geopolitical motivations, a terrorist cell could try to attack sensitive zones to bring down the economic system.

[1*]*Research Scholar, Department of Computer Science & Engineering, Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh India*
[2]*Assistant Professor, Department of Computer Science & Engineering Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh India*
** Corresponding author's Email: dandotiyamonika@gmail.com*

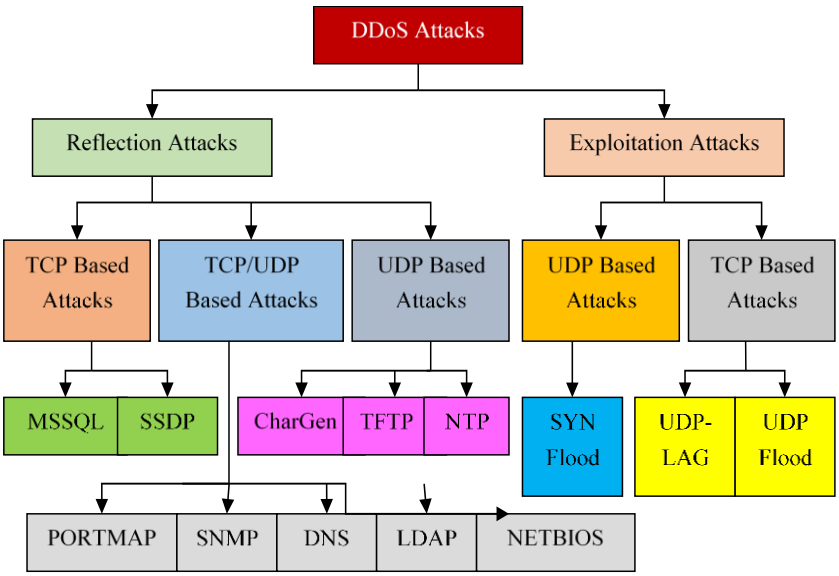


Fig 1 shows some kinds of DDoS attacks.

There are several methods for identifying DDoS attacks, categorizing them, and reducing their impact that may be found in published works. This allows us to classify the methods according to whether they depend on entropy, ML (Machine Learning), or DL (Deep Learning) [7]. In the entropy method that has been presented, the SDN controller detects IP addresses as sources and destinations and then compares their entropy flow values to specified threshold values that adjust to the dynamics of the network [8].

Entropy-based DDoS attack classification and detection using a DL model for multi-controller SDN may present the following unresolved issues: Creating more accurate and reliable models: this work suggests a model for DDoS attack detection & classification using entropy & DL, however, it might be better in terms of resilience and accuracy. Further research may be conducted to investigate alternative architectures, feature selection methods, and ML algorithms that could enhance the model's performance. Using simulated DDoS attacks, this research assesses the suggested model's functionality in a real-life scenario. Nevertheless, the model's efficacy must be tested in real-world settings with diverse traffic kinds and dynamic network circumstances. Potentially, the model's performance in real-world network settings might be investigated in further research. The problem of false positives has to be addressed since they cause needless allocation of resources or network outages while detecting DDoS attacks. Subsequent research endeavours may investigate potential strategies to mitigate the model's false positive output. Although this research primarily examines DDoS attacks in a multicontroller SDN setting, it is significant to note that DDoS attacks may disrupt a wide variety of networks, including those in the cloud and IoT (Internet of Things). Investigating how DDoS attacks affect various network types and creating models that account for their unique features might be areas of future research.

Future researchers may aid in the advancement of DDoS attack detection and classification by tackling these open issues. This will lead to the development of more efficient & effective methods for safeguarding networks from these attacks.

1.1 Software defined network (SDN)

SDN is now the most popular trend in the networking industry. SDN is distinguished by the reality that the data plane and control plane are physically separated. A representation of SDN architecture's data plane, control plane, as well as application plane, may be displayed in Figure 2.

This architecture begins with the infrastructure layer, which is made up of some network devices like OpenFlow switches & routers. The ability to forward packets inside the network is possessed by certain network devices [9]. The data plane packets include the routing information that network devices use to transmit user packets to the next switch.

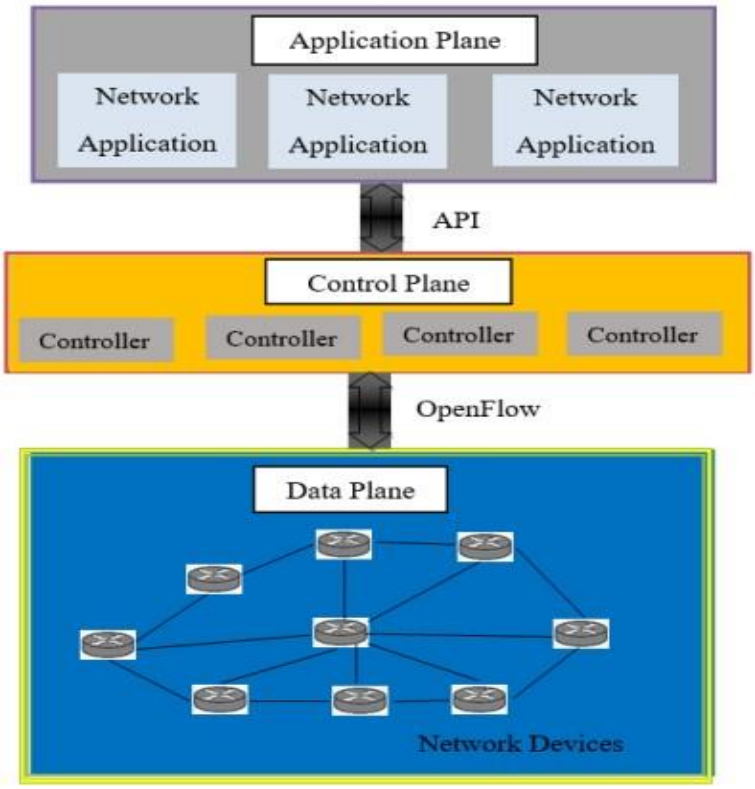


Fig. 2 SDN architecture

The network operating system, responsible for configuring network devices, makes up the second layer. Several controllers, such as Open DayLight, Open Flood Light, Maestro, Ryu, and the Open Network Operating System (ONOS), are located on the control plane. The SDN networks rely on these controllers, which are like their brains. The configuration and forwarding determination of new flows are the responsibility of the central controller [10]. At its core, the southbound protocol is SDN-related to the OpenFlow protocol. The ONF (Open Network Foundation) is responsible for maintaining the first standards that were released by Stanford's clean slate programme. The application layer, the third tier of software-defined networking, is where the programmes that run the forwarding process interact with the SDN controller [11]. A decision-making abstract network view may be created by an application by aggregating data from the controller.

1.2DDoS in SDN environment

DDoS attacks have emerged as a major concern for SDN network security in the last decade. In addition to destroying the network, it may also block legitimate users from accessing & using its resources [12]. It is therefore critical to safeguard SDN networks against DDoS attacks.

Attackers build zombie host groups by combining many hosts to suit their attack criteria. The target system uses lots of resources, such as CPU & bandwidth, processing all meaningless data packets sent by these zombie hosts. After the burden is exceeded by a significant amount of data packets, the target host will cease to function properly and be incapable of processing valid data packets. DDoS attacks are favoured by attackers due to their simplicity of execution.

The switch receives attack packets and compares them with flow entries one by one when a controller is under attack. The invalid attack packet cannot correspond to the flow table entry in the flow table. In this specific case, the packet is sent to the controller using a switch, which encapsulates it as a packet-in message. Finally, the data packet's destination is decided upon by the controller [13]. As a result of the attackers' extensive transmission of attack packets, the controller is incessantly inundated with packet-in messages, which consume a considerable quantity of controller resources. Consequently, the controller is rendered incapacitated or malfunctioning, unable to process legitimate traffic data.

As demonstrated previously, security problems related to SDN must not be underestimated. Despite its revolutionary nature and numerous advantageous features, the hidden security vulnerabilities present a significant hazard to the progress and implementation of this technology. To encourage the continued development of SDN, it is critical to conduct additional research into the security flaws of SDN architecture and design suitable countermeasures.

There are numerous varieties of DDoS attacks, consisting of ICMP flood, TCP flood [14], and UDP flood [15]. By operating the attack source, an assailant dispatches a

substantial volume of junk traffic toward the target network, thereby drastically diminishing the accessible bandwidth and impeding the target host's ability to establish external communications. Massive volumes of TCP and UDP packets are utilized in TCP flood & UDP flood attacks, respectively. To execute an ICMP deluge, normal traffic destined for the target host is disrupted through the display of ICMP request packets. The attacker transmits a significant volume of forged IP address packets to target host in TCP flood attack. The response from the originator is inaccessible to destination host due to forgery of IP addresses of packets. One notable distinction between TCP flooding attacks and UDP flooding attacks lies in the connectionless nature of UDP, which is widely implemented in audio and video applications [16]. Through UDP flooding attacks, an assailant stops the target from responding to legitimate users by generating an excessive no. of UDP packets that are directed to arbitrary ports on the destination host.

The consequences of a DDoS attack on a controller have a more severe effect on the SDN. Consequently, the significance of effective detection methods for attack detection and response cannot be overstated. Numerous techniques have been developed thus far to detect DDoS attacks against SDN controllers. Regarding architecture, scheduling, and parameters, each technological approach has a distinct design & definition.

In an SDN environment, two main ways to detect DDoS attacks are flow-based detection & packet-based detection. While a flow-based DDoS attack detection system looks at the switch's flow tables, a packet-based system should inspect every packet on the network. The pre-set trigger mechanism in the flow-based method can initially determine whether a network attack is present before initiating the attack detection algorithm. Although the attack may or may not have occurred the package-based method must nonetheless inspect all network packets.

Table 1. Techniques used for detecting DDoS attacks

S. No.	Techniques	Description
1.	Cluster analysis [17]	The goal of cluster analysis is to find patterns in data by grouping objects that share similarities while being significantly different from one another. If attack variables are comparable, we may utilize cluster analysis to separate both regular traffic & each phase of the DDoS attack.
2.	Correlation analysis [18]	The term "correlation" is employed to denote a degree of similarity between two processes. It could, nonetheless, imply no connection in certain cases. A phase difference exists between the two flows, even though they are completely interdependent.
3.	Genetic algorithms [19]	A heuristic search technique known as a genetic algorithm emulates the processes of natural evolution. As a subset of evolutionary algorithms (EA), genetic algorithms seek to solve optimization issues by mimicking the processes of natural selection via the use of mutation, crossover, inheritance, and other techniques derived from evolution.
4.	K-nearest neighbors [20]	One feature space prediction method is the k-nearest neighbour methodology, which predicts flow classes by looking at the k-closest training samples. Classification of flows is based on the majority vote of their neighbours, where k is a small positive integer.
5.	Hop-count filtering [21]	To get the right hop count for this IP address, a source IP address is utilized as an index in the database. Once the calculated hop count equals the stored hop count, a packet is considered authenticated.
6.	JDR (Joint Deviation Rate) [19]	The JDR is a novel metric for characterizing the dispersion of network traffic state rates. At its core, JDR is a compilation of all variants of the many features included in NTS (Network Traffic State).
7.	Fuzzy logic [22]	A fuzzy estimator is applied to mean packets between arrival times. While the model effectively interprets principles, it is limited in its ability to autonomously learn them.
8.	Hidden semiMarkov model(HsMM) [23]	A HsMM attack detection and stochastic process characterization tool for use during flash crowd events in detecting App-DDoS attacks.

9.	Firewall [24]	The defender may choose a threshold value that, like the preceding firewall function, causes all packets in a flow to be deleted.
10.	Cuckoo search [25]	The approach was influenced by the parasitic behavior of some cuckoo birds. Breeding cuckoos are unable to finish their life cycles unless they find an appropriate host.

The table above displays the results of ten studies that provide methods for detecting DDoS attacks. This method has the greatest use because of its computational & logical capacity to identify irregularities between data flow items.

2. Related Work

There have been several studies and research papers on DDoS attacks in SDN environments. Here are a few notable works:

N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo [2023] outlines an SDN security architecture that can automatically identify, monitor, & mitigate slow-rate DDoS attacks. The hardware utilized to implement the framework is sourced from European Experimental Facility Smart Networks for Industry physical network. With a reduction efficiency ranging from 91.66% to 100% for several situations including the number of offenders and victims, the findings demonstrate that the framework efficiently minimizes harmful connections. Additionally, the SDN-SlowRate-DDoS dataset is provided, which comprises several tests of slowrate DDoS attacks conducted on an actual testbed. The tools included in this security dataset help corporate and scientific communities create and assess useful intrusion detection system solutions [26].

M. Sinha, P. Bera, and M. Satpathy [2023] Utilize a thorough experimental investigation to evaluate the susceptibility of DDoS attacks in several SDN controllers, including Floodlight, POX, OpenDayLight as well as Ryu. This investigation has shown that the routing rules of the stated controllers have a varied impact on how much CPU and memory are used. The results of this research will assist network administrators in selecting the best defense against DDoS attacks in SDN controllers [27].

A. N. H. Dhatreesh Sai, B. H. Tilak, N. Sai Sanjith, P. Suhas, and R. Sanjeetha [2022] provide a technique for stopping the Slowloris DDoS attack in an SDN environment. The recommended method necessitates communication between the detection and mitigation method and the controller of SDN to collect data for the detection & mitigation of low and slow DDoS attacks. DDoS attacks may target certain protocols, keep connections open for an extensive time, use up resources, or flood a target server with a lot of packets to make it unavailable [28].

R. Raj and S. Singh Kang [2022] analyze the different ML techniques utilized in SDN environments to find DDoS attacks. The SDN splits the control network from the data plane. Software Defined Networks provide a clear & simple technique for network management, but they have also introduced novel security risks. These hazards include things like DoS attacks, man-in-the-middle attacks, also other threats [29].

M. I. Kareem and M. N. Jasim [2021] investigate the most well-known techniques for detecting DDoS attacks from various sources & analyze them to show the path to interested researchers in the area. It also presents a study on security developments in SDN environments. Due to their ease of use and difficulty in detection, DDoS attacks are one of the most significant dangers to networks. This study area is thus ripe for developing effective methods to identify and counteract these attacks. By enhancing network programmability, SDN, one of the smartest technologies, makes network administration and setup simple [30].

J. E. Varghese and B. Muniyal [2021] examine the trend in the SDN architectural defense against DDoS attacks by examining the different DDoS detection techniques utilized in SDN. This comparative analysis of several SDN frameworks for DDoS detection covered the advantages & disadvantages of every SDN architectural style. DDoS attacks have contributed significantly to cybercrime for several decades, and the SDN architecture's DDoS detection solutions provide flexible solutions for shifting network conditions [31].

R. Li and B. Wu [2020] offers a DDoS attack detection technique for SDN networks that depends upon entropy. Entropy may increase feature differences between regular and abnormal data and alter associated parameters in response to network circumstances, making it simpler to spot attacks in the early phases of DDoS traffic creation. This study first presents the fundamental characteristics of entropy, then uses mathematics to show that -entropy may be used to identify DDoS. Finally, we utilize Mini-net to do simulation tests to compare the impacts of DDoS detection with Shannon entropy [32].

M. Klymash, O. Shpur, N. Peleh, and O. Maksysko [2020] Using the Kulbak-Leibler strategy to measure traffic behavior and identify flow abnormalities

throughout a session, provide a method to identify DDoS. In this instance, we'll contrast the typical session length with the time it takes for certain IP addresses to contact the server. ML database will keep track of results. If the comparison's outcome was inconclusive, the time spent using the service over the previous 7 days is contrasted. KL value is similarly derived and entered into the ML database. By examining the duration of service and access to the controller's prescribed rules, KL accumulation values in an ML will be able to spot irregularities in the flow of admission requests. SDN controller would restrict IP domains from which DDoS attacks are only beginning as a consequence of machine learning [33].

A. Ahalawat, S. S. Dash, A. Panda, and K. S. Babu [2020] suggested a DDoS mitigation strategy based on rate restriction and entropy for effective service delivery. We tested Mininet as the emulator, Ryu as the controller, and an OpenVswitch switch. The results were better in terms of bandwidth use & hit ratio, which use up network resources to create DoS. A new networking architecture, such as SDN, which depends on a central controller and separation of control & data planes, has been implemented to make the network secure and adaptable. However, because of its centralized controller, it is vulnerable to DDoS attacks since it decides whether to transmit packets depending on the rules that the OpenFlow protocol has loaded in the switch [34].

3. Research Gaps

In recent years, there has been lots of research on DDoS attacks in the context of SDN. However, there are still some unresolved issues in this field. The following are examples of research gaps:

3.1 Detection and mitigation techniques

A significant research gap exists in the development of efficient & effective approaches for detecting & mitigating DDoS attacks in SDN environments. More robust & scalable methods are needed to make use of SDN programmability and flexibility for attack detection and mitigation.

3.2 SDN-specific attack vectors

DDoS attacks may be conducted with the use of new attack vectors and vulnerabilities introduced by SDN. Recognizing and countering these attack vectors that are unique to SDN is crucial. More study is required to determine whether vulnerabilities in SDN setups might be exploited by attackers to conduct DDoS attacks.

3.3 Impact assessment

Understanding and assessing the consequences of DDoS attacks in SDN environments is an additional area of research that is deficient. One aspect of this is comprehending how DDoS attacks impact SDN-based systems' resource utilization, service availability, and network performance. Better defenses may be designed with the use of approaches that assess the effect of DDoS attacks in SDN.

3.4 Resilient SDN architectures

Ongoing research focuses on designing SDN systems with resilience to survive DDoS attacks. To make SDN systems more resistant to DDoS attacks, researchers should look at architectural upgrades that make them more resilient and fault-tolerant. This could potentially entail the creation of novel fault-tolerant control plane designs, traffic engineering mechanisms, or routing algorithms.

3.5 Evaluation frameworks

The efficacy of DDoS defence systems in SDN must be evaluated, and this requires the establishment of thorough assessment frameworks. Several DDoS defence systems may be compared and benchmarked with the use of realistic and relevant testbeds, datasets, and performance metrics.

3.6 SDN security policies

A major area of study is the investigation of security rules and access control methods that might prevent or mitigate DDoS attacks in SDN environments. Improving SDN security against DDoS attacks involves investigating methods for dynamic policy adaption, policy enforcement, and anomaly detection.

To better protect SDN environments against DDoS attacks, and to build more secure SDN architectures, it is necessary to fill these research gaps.

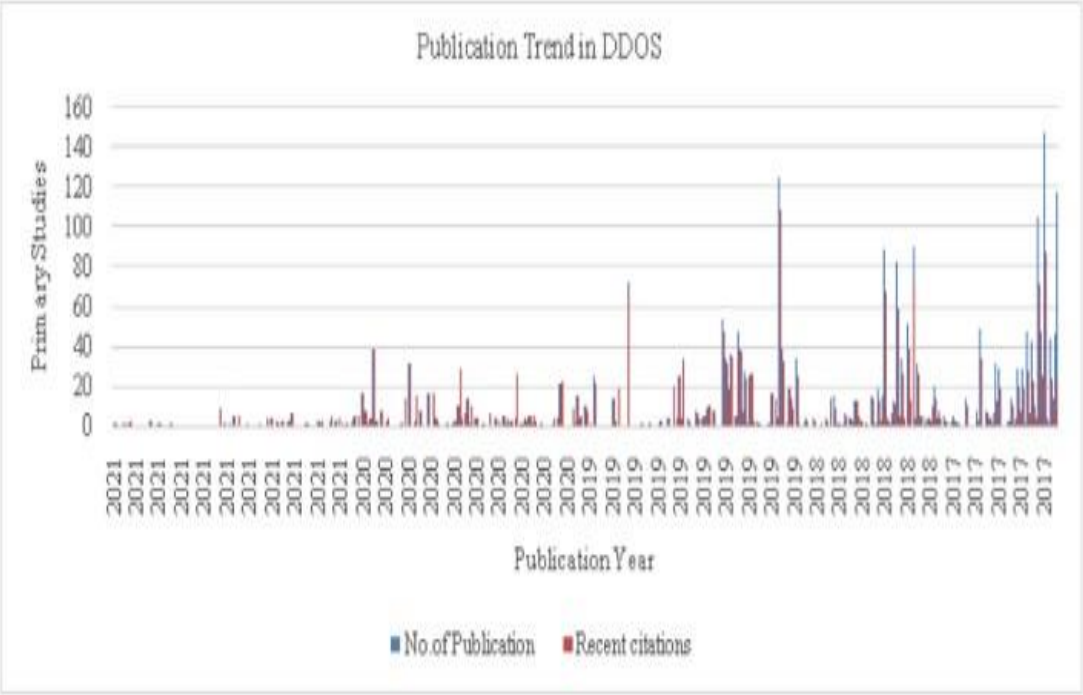


Fig. 3 Publication trends of DDoS attack in SDN

The main research of various attack traffic engineering strategies is shown in the above figure. When it comes to DDoS attacks, some significant advancements in the area of SDN include:

3.6.1. Adaptive traffic engineering

Adaptive traffic engineering techniques within SDN have been proposed by researchers as a means to dynamically redirect traffic in the event of DDoS attacks. DDoS attacks may be lessened with the help of intelligent traffic redirection by SDN controllers, which constantly scan network conditions and identify attack patterns.

3.6.2. Attack detection and classification

To detect & categorize DDoS attacks in SDN systems, several researches have focused on creating sophisticated algorithms and ML approaches. These methods may detect harmful traffic and initiate countermeasures by examining the features, flows, and behavioral anomalies of network traffic [35].

3.6.3. Programmable and scalable countermeasures

The programmability of SDN allows for the implementation of dynamic countermeasures to avoid DDoS attacks. Novel defense techniques, implementable in real-time with SDN controllers, have been presented by researchers. These include fine-grained traffic filtering, rate limitation, and traffic redirection. Implementing these precautions may effectively reduce the impact of DDoS on legitimate traffic [36].

3.6.4. Collaborative defense mechanisms

To strengthen DDoS protection in SDN, researchers have investigated the possibility of cooperation between several SDN controllers and network domains. In the event of a DDoS attack, SDN controllers may work together to react by exchanging attack details, traffic profiles, and mitigation tactics.

3.6.5. Machine learning-based anomaly detection

Researchers have built anomaly detection systems in SDN to recognize unexpected network behavior related to DDoS attacks, using ML methods. These systems are capable of acquiring knowledge of typical traffic patterns and identifying deviations that signify possible attacks, thereby enabling proactive mitigation strategies.

3.6.6. SDN-based DDoS testbeds

It has been helpful to evaluate and validate the efficacy of defence systems with the establishment of SDNbased DDoS testbeds. To study the efficacy of various SDN mitigation strategies, researchers may use these testbeds to mimic attacks with DDoS and evaluate their effects [37].

The comprehension & mitigation of DDoS attacks in SDN have been greatly enhanced by these advances. These examples show how SDN might improve network security and defend against DDoS attacks.

Table 2. Research Gaps of

Author	Title	Idea	Loopholes
A. R. Yadav, A. P. Jain, S. T, A. Rajesh, S. Perumal, and G. Eappen" [38]	"AI-based DDOS Attack Detection of SDN Network in Mininet Emulator"	SDN exposes the network to potentially more dangerous attacks than those that target conventional networks. Through this research, they want to investigate DDoS attack carried out by Artificial Intelligence (AI) on the SDN network and investigate a potential machine learning (ML)-based countermeasure.	Malicious and non-malicious packets might build up at the controller, further consuming demand & making the controller inaccessible to new packets. The SDN architecture is impacted by this occurrence, which slows down the controller.
"J. R. Dora & L Hluchy" [39]	"Detection of Attacks in SDN: *How to conduct attacks in SDN environments"	By simulating attacks on network devices, they may assess the security stance of SDN networks with demonstrate that they have several weaknesses. The reputation and financial health of the organization may be at risk if such flaws were to be exploited. As a result, they simulate the attacks utilizing Mininet and RYU controller tools to carry out the exploitation.	Due to the need that the controller instance to remain accessible at all times, the danger in the SDN environment grows. Consider how severe a DDoS attack on an SDN network might be.
"N. H. D. Sai, B. H. Tilak, N. S. Sanjith,	"Mitigation and Detection of Low and Slow DDoS	Outlines a method to stop and prevent one such Slowloris DDoS attack in an	The proposed solution is just for slowloris DDoS attacks i.e., low & slow.
P. Suhas and R. Sanjeetha" [28].	attack in an SDN environment"	SDN environment. To gather information.	
"K. V. M. Mohan, S. Kodati and V. Krishna" [40]	"Protecting the Infrastructure of Fog Networks in an IoT Scenario Using SDN from Attacks"	The SDN network is used to implement legal decisions on network enforcement made by the virtual switches. SDN switches are also often powerful computers that are used as fog nodes.	The administration of IoT becomes harder as a result of a lack of security and increasing connections. SDN has been established to control the network traffic.

4. Problem Domain

The primary issue with Software-Defined Networking with DDoS attacks, as of my most recent update in September 2021, is the increased exposure of vulnerabilities and attack surfaces.

SDN makes network administration more flexible & programmable by separating the data plane from the control plane. While SDN has several advantages, such as automated administration and centralized network control, it also has some possible drawbacks:

4.1 Single point of control

The controller governs the entire network's behavior; therefore, a DDoS attack that targets the controller could have severe consequences due to the centralized control plane of SDN. Services may be interrupted or the network may become unavailable entirely if the controller is overloaded by the attack.

4.2 Limited flow table capacity

SDN devices, like switches, have limited flow table capacity for storing forwarding rules. These tables may

be filled up fast in large-scale DDoS attacks, which can cause packet drops and even network instability.

4.3 Lack of visibility

Dedicated security appliances can detect and mitigate DDoS attacks in traditional networks. Deploying such security appliances efficiently and achieving complete visibility into network traffic may be problematic in SDN because of the separation of the data plane and control plane.

4.4 Flow-based control

The controller manages and enforces network policies by SDN's flow-based control. However, the controller's capacity to adjust network regulations and protect against DDoS attacks could be compromised if it is overloaded during an attack.

4.5 Inadequate security mechanisms

DDoS attacks may not be adequately protected in all SDN deployments. For instance, blackhole routing, rate limiting, and access control lists may not be adequate to defend against sophisticated and large-scale DDoS attacks.

4.6 OpenFlow vulnerabilities

Attackers may be able to execute DDoS attacks and interrupt network operations by exploiting vulnerabilities in SDN protocols like OpenFlow.

Organizations should take proactive measures to safeguard their SDN environments against DDoS attacks to tackle these difficulties. This may entail the deployment of dedicated DDoS mitigation appliances, the utilization of flow analysis tools to identify anomalies, and the establishment of rate-limiting mechanisms at key points within the network. Furthermore, SDN security is an area that is always being researched and improved upon to make SDN networks more resistant to DDoS attacks.

5. Experimental Approach

The suggested methodology entails communication between mitigation & detection applications and SDN controllers for data acquisition or mitigation. Using Mininet, the SDN environment is configured. Ryu Controller serves as the control plane. A network is constructed comprising hosts, switches, and controllers. A PHP software that displays "Hello World" was created. Apache serves as the host for the PHP programming. To run the server, a computer on the network is used. The attack traffic is directed to the target server via two hosts. A library called Slow HTTP Test is used to transmit the malicious data. It employs a Slowloris DDoS attack strategy, which is slow and unreliable.

5.1 Proposed Algorithm

Step 1: Require: totalPacketCount, number Of Hosts[]

Step 2: Require: wiresharkAttackCapture[], allHosts[]

Step 3: Require: number of ConnectionsPerHost

Step 4: expected Attack Hosts ← []

Step 5: attack Hosts ←[]

Step 6: average Packet Count← fractotal Packet Count number Of Hosts

Step 7: for host ← all Hosts do

Step 8: if number Of Connections Per Host [host] > average Packet Count then

Step 9: expected Attack Hosts ← host

Step 10: end if

Step 11: end for

Step 12: for host expected Attack Hosts do

Step 13: i ←0:

Step 14: Difference of 0:

Wireshark Attack Capture [host] [PSHPackets] Step 15: wireshark Attack Capture[host][FIN Packets]

Step 16: if i > 100 then Step 17: attackHosts ← host

Step 18: end if

Step 19: end for

Step 20: Mitigation

Step 21: for host ← attackHosts do

Step 22: Droppackets fromhost

Step 23: end for=0

5.2 Proposed Flowchart

There will be two distinct phases to the research project. As a first step, we'll create an authentication mechanism that will prevent unauthorised nodes from accessing services. Phase two focuses on identifying and countering DDoS attacks launched by verified nodes. An attack database and a model built on neural networks will form the basis of the attack detection system. It is possible to utilize simulation tools to confirm the detection and mitigation outcomes.

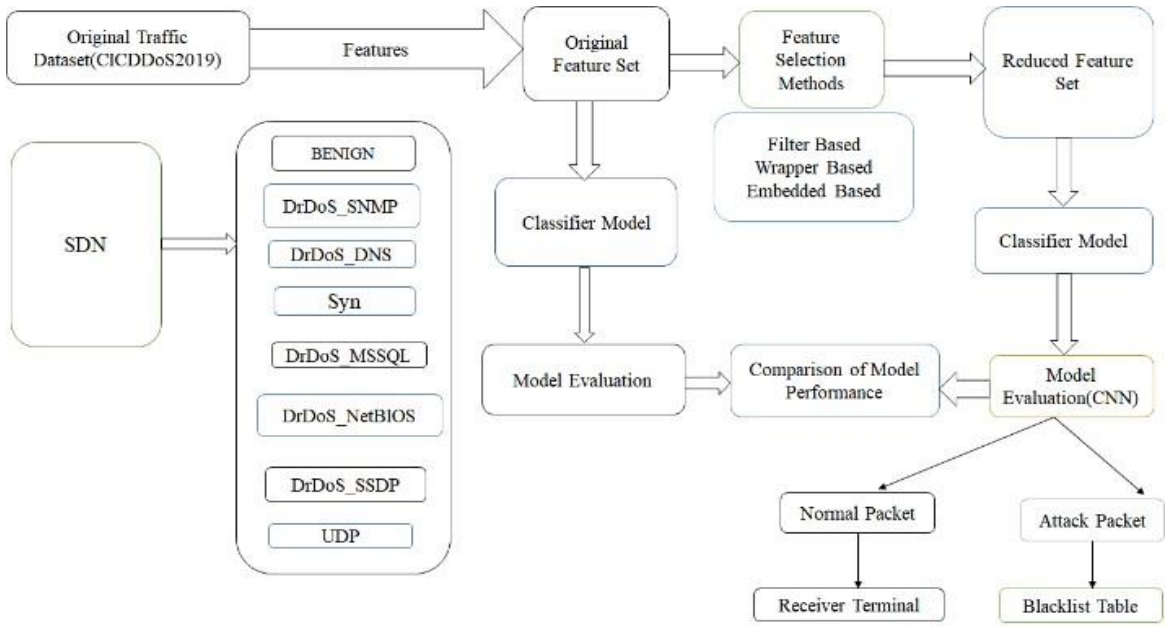


Fig 4 Flowchart of proposed approach

A flowchart of the proposed methodology is depicted in the above figure. Evaluate potential authentication situations for several criteria, such as authentication process speed (complexity), throughput following reliability methodologies, and network overhead. Evaluate the findings in light of other methods.

6. Experiment

This SDN-based DDoS detection approach should be better suited for real-world business applications that require lengthy simulations, a larger population of optimization candidates, and more optimization iterations, such as complex process interactions or a large number of potential solutions.

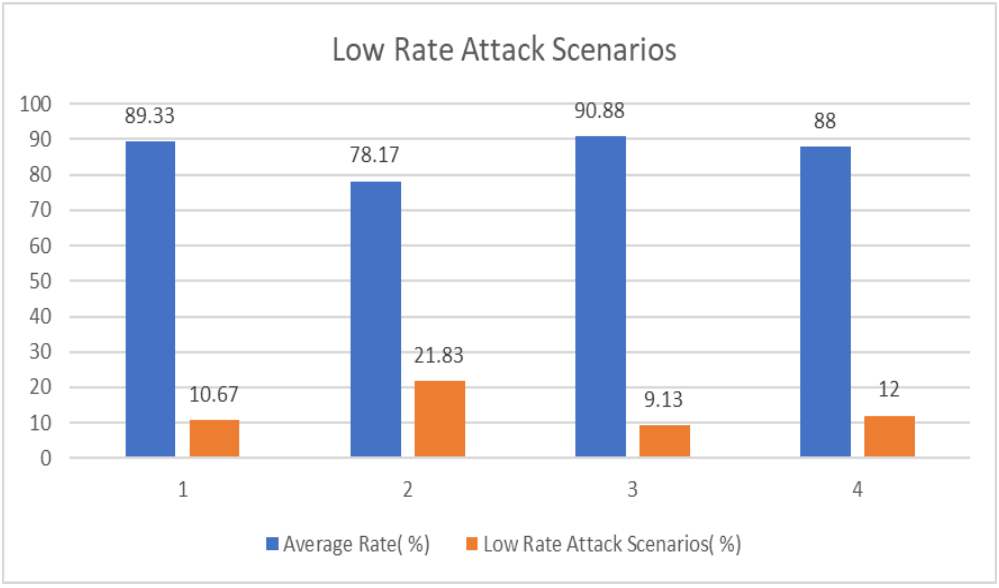


Fig. 5 The low rate attack scenarios of SDN-based DDoS

The above figure shows the Low Rate Attack Scenarios of SDN-based DDoS. The variation of DDoS attack traffic rates in every scenario allows for fluctuation between the average rate and low-rate attack scenarios, as shown in Fig. 5.

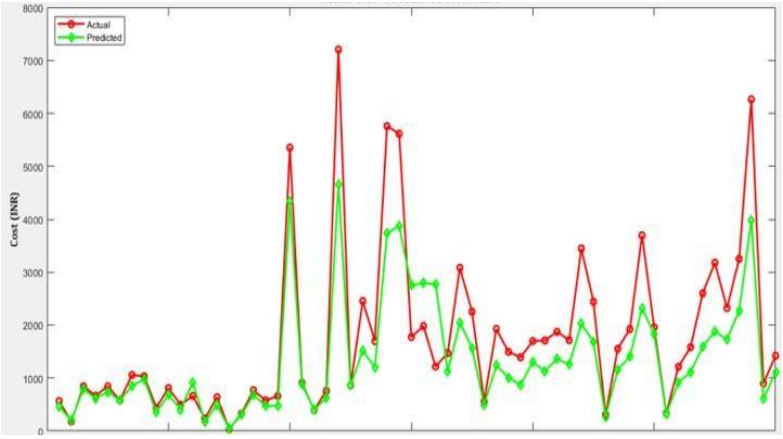


Fig. 6 The actual vs predicted cost of SDN-based DDoS

The following Figure 6 shows the actual vs predicted cost of SDN-based DDoS where the y-axis displays the cost in INR from 0 to 8000. Projected costs are costs that are predicted depending upon sales & spending from the prior period of DDoS detection. predicting future cost levels using aspects of past attack behavior.

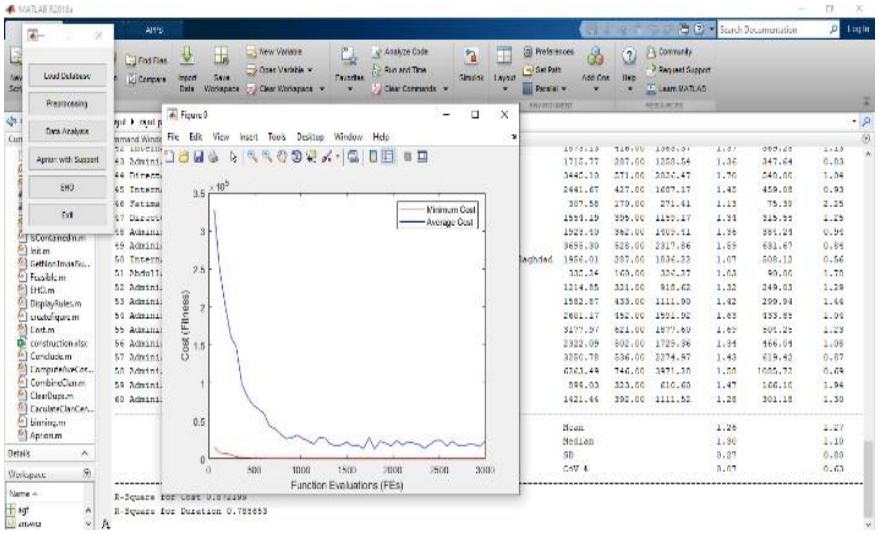
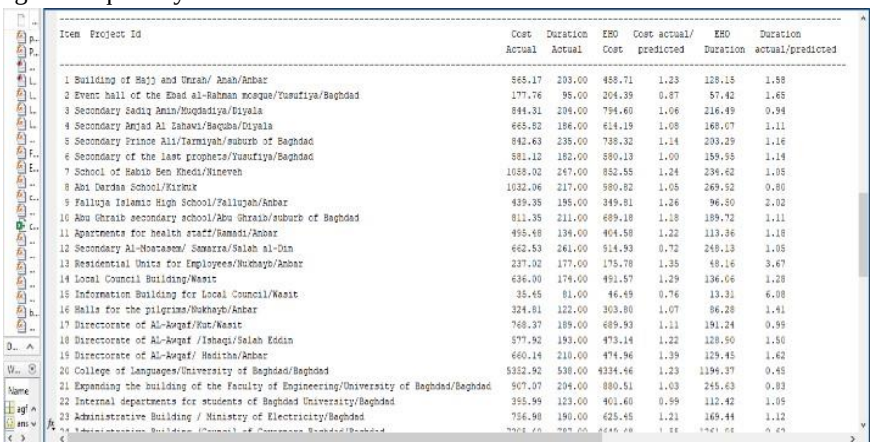


Fig. 7 The model evaluation of CICDDoS2017 dataset

Figure 7 displays the results of the CICDDoS2017 Dataset model evaluation. In all simulated scenarios, the detection method exhibited superior performance compared to competitors in identifying high-rate DDoS attacks. This superiority was attributed to the method's capacity to collect a greater quantity of statistical data regarding newly incoming network traffic, which was augmented by the high traffic rate.



Item	Project Id	Cost Actual	Duration Actual	EHO Cost	Cost actual/ predicted	EHO Duration	Duration actual/predicted
1	Building of Hajj and Umrah/ Anah/Anbar	565.17	203.00	458.71	1.23	128.15	1.58
2	Event hall of the Emad al-Rahman mosque/Yusufiya/Baghdad	177.76	95.00	204.39	0.87	57.42	1.65
3	Secondary Sadiq Amin/Muqdadiya/Diyala	844.31	206.00	794.60	1.06	216.49	0.94
4	Secondary Amjad Al Zahawi/Baquba/Diyala	665.82	186.00	614.19	1.08	168.07	1.11
5	Secondary Prince Ali/Tarmiyah/suburb of Baghdad	842.63	235.00	738.32	1.14	203.29	1.16
6	Secondary of the last prophets/Yusufiya/Baghdad	581.12	182.00	580.13	1.00	159.55	1.14
7	School of Habib Ben Khedi/Nineveh	1038.02	267.00	852.55	1.24	236.62	1.05
8	Abi Dardaa School/Kirkuk	1032.06	217.00	980.82	1.05	269.52	0.80
9	Falluja Islamic High School/Fallujah/Anbar	439.35	195.00	349.81	1.26	96.30	2.02
10	Abu Ghraib secondary school/Abu Ghraib/suburb of Baghdad	811.35	211.00	689.18	1.18	189.72	1.11
11	Apartments for health staff/Ramadi/Anbar	495.48	134.00	404.58	1.22	113.36	1.18
12	Secondary Al-Mostasem/ Samarra/Salah al-Din	662.53	261.00	514.93	0.72	248.13	1.05
13	Residential Units for Employees/Nukhayb/Anbar	237.02	177.00	175.78	1.35	48.16	3.67
14	Local Council Building/Wasit	636.00	174.00	491.57	1.29	136.06	1.28
15	Information Building for Local Council/Wasit	35.45	81.00	46.49	0.76	13.31	6.08
16	Halls for the pilgrims/Nukhayb/Anbar	324.81	122.00	303.80	1.07	86.28	1.41
17	Directorate of AL-Awqaf/Kut/Wasit	768.37	189.00	689.93	1.11	191.24	0.99
18	Directorate of AL-Awqaf /Ishaqi/Salah Eddin	577.92	193.00	473.14	1.22	128.90	1.50
19	Directorate of AL-Awqaf/ Haditha/Anbar	660.14	210.00	474.96	1.39	129.45	1.62
20	College of Languages/University of Baghdad/Baghdad	5352.92	538.00	4334.66	1.23	1196.37	0.45
21	Expanding the building of the Faculty of Engineering/University of Baghdad/Baghdad	907.07	204.00	880.51	1.03	245.63	0.83
22	Internal departments for students of Baghdad University/Baghdad	395.99	123.00	401.60	0.99	112.42	1.09
23	Administrative Building / Ministry of Electricity/Baghdad	756.98	190.00	625.45	1.21	169.44	1.12

Fig. 8 The duration of actual/predicted value

The duration of the actual value compared to the predicted value is shown in the figure above. The number of attack sources and how they change their attack traffic rates influences the network's DDoS attack rate. A DDoS attack can potentially be initiated by either a single host attack or multiple host attacks (many attackers).

Table 3. Detection mechanisms of DDoS attack that showed best ratios

Studies	Datasets	Detection Rate (%)
[41]	CAIDA, DARPA & TUIDS	99.76
[42]	DARPA 2009, BONESI-generated, CAIDA 2007	98.45
[43]	KDD Cup1999	98.34
[44]	Knowledge Discovery & Data Mining (KDD) Cup 1999	97.31

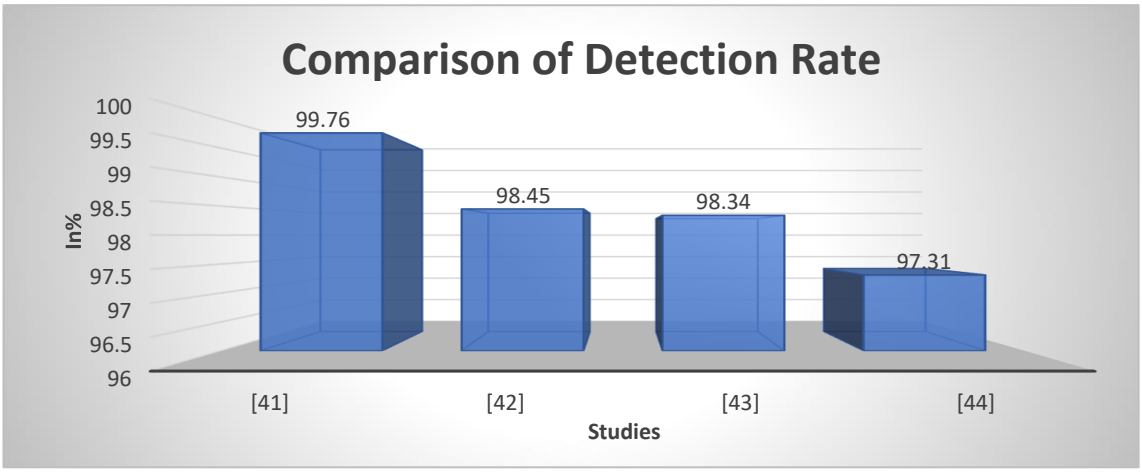


Fig. 9 Comparison among different studies in terms of several datasets

Several studies have reported the detection rates of different intrusion detection systems (IDS) using different datasets. Table 3 and Figure 9 summarise these rates. The first study [41] uses CAIDA, TUIDS, and DARPA datasets and achieves a detection rate of 99.76%. The second research [42] uses datasets from CAIDA 2007, DARPA 2009, and BONESI-generated to reach a slightly lower detection rate of 98.45%. The third research [43] finds a detection rate of 98.34% using the KDD Cup 1999 dataset, while the fourth study [44] employs the same dataset to get a detection rate of 97.31%. The findings show that the model performs well in terms of detection on various datasets, with the first research obtaining the best detection rate compared to the others. The KDD Cup 1999 dataset is used in two of the studies, and while there are small differences in detection rates, it consistently shows that it is beneficial to evaluate IDS.

7. Conclusion and Future Roadmap

When developing new 5G protocols, attack resistance must be taken into account. Questionable authentication techniques, such as username/password, should be phased away. The emerging dangers, on the other hand, underline the need for quantitative security assurance and compliance, or validating the presence, accuracy, and sufficient of security functions. The two-stage security model can improve the authentic use of services from the server and also neural network-based prediction can provide better blocking of DDoS attacks in the SDN environment. We hope that our work is based on an effective framework for DDoS attacks in the SDN environment. We plan to test the model in a computer network that has a flow that the model has never previously seen. An evaluation of the model will be part of this deployment. Depending on the findings, we may suggest using the acquired data in a model training phase.

References

[1] H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li, and C. F. Cheang, "A Survey on Security-Aware Measurement in SDN," *Security and Communication Networks*. 2018, doi: 10.1155/2018/2459154.

[2] T. Wang, Y. Feng, and K. Sakurai, "Improving the Two-stage Detection of Cyberattacks in SDN Environment Using Dynamic Thresholding," 2021, doi: 10.1109/IMCOM51814.2021.9377395.

[3] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in softwaredefined networking," 2015, doi: 10.1109/ Trustcom.2015.389.

[4] L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race, "Tennison: A distributed SDN framework for scalable network security," *IEEE J. Sel. Areas Commun.*, 2018, doi: 10.1109 /JSAC.2018.2871313.

[5] H. D. Zubaydi, M. Anbar, and C. Y. Wey, "Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller," 2017, doi: 10.1109/PICICT.2017.26.

[6] N. Ahuja and G. Singal, "DDOS Attack Detection Prevention in SDN using OpenFlow Statistics," 2019, doi: 10.1109/IACC48062.2019.8971596.

[7] J. Pei, Y. Chen, and W. Ji, "A DDoS Attack Detection Method Based on Machine Learning," 2019, doi: 10.1088/1742-6596/1237/3/032040.

[8] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*. 2023, doi: 10.1007 /s00500-021-06608-1.

[9] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN)," *J. Comput. Networks Commun.*, 2019, doi: 10.1155/2019/8012568.

[10] O. Rahman, M. A. G. Quraishi, and C. H. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," 2019, doi: 10.1109/ SERVICES.2019.00051.

[11] M. M. Joëlle and Y. H. Park, "Strategies for detecting and mitigating DDoS attacks in SDN: A survey," 2018, doi: 10.3233/JIFS-169833.

[12] D. Melkov and S. Paulikas, "Security Benefits and Drawbacks of Software-Defined Networking," 2021, doi: 10.1109/eStream53087.2021.9431466.

[13] J. H. Cox *et al.*, "Advancing software-defined networks: A survey," *IEEE Access*, 2017, doi:

[14] 10.1109/ACCESS.2017.2762291.

[15] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong, and Y. K. Sanjalawe, "Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller-A Review," *IEEE Access*, 2020, doi: 10.1109/ ACCESS.2020.3013998.

[16] S. Deore and A. Patil, "Survey Denial of Service classification and attack with Protect Mechanism for TCP SYN Flooding Attacks Atul Patil," *Int. Res. J. Eng. Technol.*, 2016.

[17] Rajkumar and M. Nene, "A Survey on Latest DoS Attacks : Classification and Defense Mechanisms," *Int. J. Innov. Res. Comput. Commun. Eng.*, 2013.

[18] V. Jean Shilpa and P. K. Jawahar, "Advanced optimization by profiling of acoustics software applications for interoperability in HCF systems," *J. Green Eng.*, 2019.

[19] P. Radha and B. Meena Preethi, "Machine learning approaches for disease prediction from radiology and pathology reports," *J. Green Eng.*, 2019.

[20] K. . Higgins, "Researchers to Demonstrate New Attack That Exploits HTTP," 2010.

[21] http://www.darkreading.com/vulnerability-management/167901026/security/attacksreaches/228000532/index.html.

[22] Y. Wu, V. Suhendray, H. Saputra, and Z. Zhao, "Obfuscating Software Puzzle for Denial-of-Service Attack Mitigation," 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.45.

[23] M. Kowsigan, "Data Security and Data Dissemination of Distributed Data in Wireless Sensor Networks," *Int. J. Eng. Res. Appl.*, 2017, doi: 10.9790/9622-0703042631.

[24] K. Bhuvaneswari and H. Abdul Rauf, "Edgelet based human detection and tracking by combined segmentation and soft decision," in *2009 International Conference on Control, Automation, Communication and Energy Conservation*, 2009, pp. 1–6.

[25] K. J. Poornaselvan, T. Gireesh Kumar, and V. P. Vijayan, "Agent based ground flight control using type-2 fuzzy logic and hybrid ant colony optimization to a dynamic environment," 2008, doi:

[26] 10.1109/ICETET.2008.85.

[27] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *Int. J. Comput. Appl.*, 2012, doi: 10.5120/7640-0724.

[28] R. Kanmani and A. Jameer Basha, "Performance analysis of wireless OCDMA systems using OOC,

PC and EPC codes," *Asian J. Inf. Technol.*, 2016, doi: 10.3923/ajit.2016.2087.2093.

[29] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo,

[30] "Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset," *IEEE Access*, 2023, doi: 10.1109/ACCESS. 2023.3274577.

[31] M. Sinha, P. Bera, and M. Satpathy, "DDoS Vulnerabilities Analysis in SDN Controllers:

[32] Understanding the Attacking Strategies," 2023, doi: 10.1109/WiSPNET57748.2023.10134518.

[33] A. N. H. Dhatreesh Sai, B. H. Tilak, N. Sai Sanjith, P. Suhas, and R. Sanjeetha, "Detection and Mitigation of Low and Slow DDoS attack in an SDN environment," 2022, doi:

[34] 10.1109/DISCOVER55800.2022.9974724.

[35] R. Raj and S. Singh Kang, "A Review on DDoS attack Detection in SDN using ML," 2022, doi:

[36] 10.1109/ICAC3N56670.2022.10074330.

[37] M. I. Kareem and M. N. Jasim, "The Current Trends of DDoS Detection in SDN Environment," 2021, doi: 10.1109/IT-ELA52201.2021.9773744.

[38] J. E. Varghese and B. Muniyal, "Trend in SDN Architecture for DDoS Detection-A Comparative Study," 2021, doi: 10.1109/DISCOVER52564. 2021.9663589.

[39] R. Li and B. Wu, "Early detection of DDoS based on \varphi-entropy in SDN networks," 2020, doi: 10.1109/ITNEC48623.2020.9084885.

[40] M. Klymash, O. Shpur, N. Peleh, and O. Maksysko, "Concept of Intelligent Detection of DDoS Attacks in SDN Networks Using Machine Learning," 2021, doi: 10.1109/PICST51311.2020.9467963.

[41] A. Ahalawat, S. S. Dash, A. Panda, and K. S. Babu, "Entropy Based DDoS Detection and Mitigation in OpenFlow Enabled SDN," 2019, doi: 10.1109 /ViTECoN.2019.8899721.

[42] C. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou, and C. Campbell, "Detection of DDoS Attacks in Software Defined Networking Using Entropy," *Appl. Sci.*, 2022, doi: 10.3390/ app12010370.

[43] S. M. Mousavi and M. St-Hilaire, "Early Detection of DDoS Attacks Against Software Defined Network Controllers," *J. Netw. Syst. Manag.*, 2018, doi: 10.1007/s10922-017-9432-1.

[44] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2018.07.017.

[45] A. R. Yadav, A. P. Jain, T. Shankar, A. Rajesh, S. Perumal, and G. Eappen, "AI based DDOS Attack

[46] Detection of SDN Network in Mininet Emulator," 2023, doi: 10.1109/ViTECoN58111.2023.101 57074.

[47] J. R. Dora and L. Hluchy, "Detection of Attacks in Software-Defined Networks (SDN) $*$: $*$How to conduct attacks in SDN environments," 2023, doi: 10.1109/SACI58269.2023.10158584.

[48] K. V. M. Mohan, S. Kodati, and V. Krishna, "Securing SDN Enabled IoT Scenario Infrastructure of Fog Networks From Attacks," 2022, doi: 10.1109/ICAIS53314.2022.9742727.

[49] T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2004, doi: 10.1007/978-3-540-24693-0_63.

[50] J. Cheng, J. Yin, C. Wu, B. Zhang, and Y. Liu, "DDoS attack detection method based on linear prediction model," 2009, doi: 10.1007/978-3-642-04070-2_106.

[51] J. Udhayan and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," *Int. J. Netw. Secur.*, 2011.

[52] G. Öke and G. Loukas, "A denial of service detector based on maximum likelihood detection and the random neural network," *Comput. J.*, 2007, doi: 10.1093/comjnl/bxm066.