Research Article


Parmod Kumar,1 Anupam Baliyan,2 K. Ramalingeswara Prasad,3 N. Sreekanth,4 Parag Jawarkar,5 Vandana Roy,6 and Enoch Tetteh Amoatey7

1Department of Electronics and Information Engineering, Jiangxi University of Engineering, Xinyu, Jiangxi, China
2Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India
3Department of EEE, Lakireddy Bali Reddy College of Engineering (A), Mylavaram, India
4Professor & HoD, Department of ECE, Malla Reddy Engineering College for Women, Maisammaguda Dhulapally Post Via Kompally, Secunderabad, Telangana, India
5Department of Electronics Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
6Professor, Electronics & Communication Engineering, Gyan Ganga Institute of Technology & Sciences, Jabalpur-482001, M.P., India
7School of Engineering, University for Development Studies, Ghana

Correspondence should be addressed to Enoch Tetteh Amoatey; eamoatey@uds.edu.gh

Received 16 December 2021; Revised 24 January 2022; Accepted 26 January 2022; Published 13 April 2022

Academic Editor: Mohammad Farukh Hashmi

Copyright © 2022 Parmod Kumar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A number of disadvantages of traditional networks may be attributed to the close relationship that exists between the control plane and the data plane inside proprietary hardware designs, as described above. The problem of security is one of the most difficult to deal with. There are a plethora of network hazards and attacks that might be encountered these days. DDoS attacks are one of the most popular and disruptive attacks on the internet today, and they affect a wide range of organisations. Despite a large number of traditional mitigation solutions now available, the frequency, volume, and intensity of distributed denial-of-service (DDoS) attacks continue to rise. According to the findings of this paper, a new network paradigm is necessary to satisfy the requirements of today’s complex security concerns. It was necessary to develop a software-defined network (SDN) in order to meet the real-time needs of the massive network that was expanding at an exponential rate. Many advantages of SDN exist, including simplicity of administration, scalability, and agility, but one of the most critical is security, which is one of the most important considerations when implementing SDN. SDS may be seen as a paradigm in which the implementation of new security regulations in the computer environment is performed via the use of protected software, which is described further below. The goal is to provide a flexible and extensible architecture for DDoS detection and prevention that is both flexible and extendable; the suggested clustering approach, which is based on the Open Day Light (ODL) Controller, is employed to carry out the experimental findings. In this section, we emphasise DDoS penetration techniques from a range of tools, and we evaluate the vulnerability against various tactics. It is necessary to use a Mininet emulation tool to construct a detection and prevention system against distributed denial of service (DDoS) attacks in order to achieve success. There is a range of other simulation tools that are utilised in conjunction with this research in order to bring it to a conclusion. Integration of industry standards such as SNORT and Flow has been accomplished in a variety of situations and parameter settings. During the creation of a framework capable of detecting and mitigating DDoS attacks at an early stage in both the control and application levels, the implementation of this framework has been shown to be crucial in the development of a framework.
1. Introduction

Putting it simply, a computer network may be regarded as a collection of nodes that are linked to one another via a network of connections. Various routes and contacts are used to link the nodes to ease the exchange of information, data, resources, and applications among several nodes [1]. To establish connections to share and exchange data or resources, cabled cabling (such as optical fibres) or wireless media may be used to convey the information or resources (such as Wi-Fi). Using computer networks, users may access the World Wide Web, send and receive an e-mail, and use a range of other services [2].

There are three types of computer networks, which can be roughly classified based on their geographical application [3]. Local area networks (LAN) are the most common type of computer network, while metropolitan area networks (MAN) are the most common type of wide area network (WAN). LAN: these types of networks have a very limited geographical range due to the nature of their design. A local area network (LAN) is a network that is situated inside a building or on a college campus [4], which is another term for a network that is placed within a building.

This is still another kind of network that is specifically designed for cities or towns, known as the MAN (metropolitan area network). As previously stated, the major purpose of this network is to provide high-speed connectivity from one end of the network to another end of the network. When considering MAN [5], the network of a communications provider is an excellent illustration.

WAN stands for wide area network. It is a kind of network in which hosts are positioned at a vast distance from one another and in which there is a provision for long-distance transmission. Among other things, this communication contains data, photos, video/audio, and other resources in addition to other components. The Internet [6] is the most well-known example of a wide-area network (WAN). It is possible to differentiate between different types of network devices that are utilised for transmission. These gadgets, which operate as middlemen between the source and the destination, act as a connection between the two. In conjunction with nodes and hosts, routers are used to determine the most optimal paths that will allow them to connect with one another and other devices on the network [7]. The following graphic illustrates the many kinds of network equipment available.

Routers are devices that are used to transport data packets across many computer networks in the field of information technology (IT). This device, which may be virtual or physical, connects two networks together by acting as a gateway. In the Open Standard Interface (OSI) paradigm of computer networking, it is sometimes referred to as a layer-3 device or a third-level device. The source and destination address of each data packet received by the router are attached to the packets by the router [8]. As a consequence, data packets are more likely to reach their intended destination as a result of this.

The hub is a layer-2 device in the Open Systems Interconnection (OSI) design, connecting two or more computers. It is responsible for distributing frames (layer-2) to all devices connected to a computer networking system. LANs often make use of hubs to combine all of the parts of the network. Because it is made up of multiple ports, once a packet arrives at one port, it is copied to the other ports, enabling all segments of the LAN to see all of the boxes that have arrived. The inflow of unnecessary traffic results in congestion and memory loss [9]. This is the fundamental reason for the delay in the transmission of data packets from the source location to the destination location from the source site. The hub is the most common configuration when it comes to small-scale networks.

Switch: a switch, also known as an intelligent hub, is another key networking piece of equipment that is utilised in a variety of circumstances around the world. Despite the fact that it functions at layer-2 of the OSI model, it maintains a record of all media access control (MAC) addresses of the devices that are connected. This means that every time the same device sends a request for transmission, the switch checks its record to see if the MAC address of that device has already been recorded. If this has already been done, the data is transmitted immediately; if it has not, the data is recorded and transmitted immediately as well as previously transmitted data [10]. This feature boosts the efficiency of a switch in comparison to that of a hub. A bridge is a networking device that connects two different networks together by providing a connecting connection between them. They provide functions that are comparable to those of hubs and repeaters. Due to the fact that they are named bridges, these devices are used for broadcasting info to every single node connected to the network. Bridges update the media access control (MAC) address database as soon as they discover new segments, guaranteeing that subsequent transmissions are only sent to the specified receiver [11].

In an era where the Internet’s development is increasing at an exponential rate, one of the most disruptive network assaults is the distributed denial of service (DDoS) attack [12], which is becoming more common. Intruders are using cutting-edge methods and strategies to target websites and perform distributed denial of service (DDoS) attacks against these systems. With this attack, the purpose is to produce a disturbance in the usual flow of traffic in a network by directing a large volume of traffic towards a server. As a consequence, legitimate users are unable to use the aforementioned services and applications [13]. During an assault, attackers overwhelm the targeted web server with unexpected traffic that originates from a number of sources. It is not just the system that has been targeted that is a victim of a DDoS assault, but also any other systems that have been purposefully targeted. The hacker supervises and manages the whole operation from a distant location on the internet. According to some estimates, a targeted web server may be bombarded with traffic from a hundred or even thousands of different sources, all coming from different IP addresses [14]. As a result, banning a single source IP address is not now a practical option. One of the most difficult duties a network administrator must do is to monitor network traffic in order to distinguish between legitimate network traffic and DDoS attack activity [15]. Every day, new forms of DDoS...
attacks are being developed, and some of the most prominent classed types of DDoS attacks are shown in Figure 1 below, along with their respective frequencies.

As a consequence, the server/bandwidth network gets overwhelmed [16], resulting in the server/bandwidth network crashing. These attacks often take advantage of the protocols that are being utilised or the present state of the network to their advantage. Among the types of flooding attacks that occur at the application layer, HTTP (Hyper Text Transfer Protocol) flooding attacks are the most common. Conventional networks are comprised of static elements and various fixed functions, which are implemented in the form of switches, routers, and other networking equipment, as well as other networking components. Their creators have programmed these gadgets to do just the tasks they are designed to be capable of. Anyone wanting to change or adjust their root configuration will do so because of the lack of flexibility. This will be an obstacle to technological growth. When it comes to keeping things operating properly, traditional networks rely on specialised hardware. For the most part, the specialised hardware platform contains the network’s intelligence (code and traffic transmission rules), as well as the network architecture that underpins the network. The new framework presented in this thesis has been tested with the help of a methodology that is made up of a variety of tools and platforms, as described in this thesis. Emulation is a common approach for experimenting and for constructing network topologies, both customised and default, in order to test new ideas in an emulated environment. The Mininet tool [16] was used in this thesis to create a realistic virtual network environment, which was a requirement for the project. In a matter of seconds, you can build and run the actual kernel, switch, and application code on a single computer (VM, cloud, or native), with a single command. It is an emulation tool that allows you to build and run the actual kernel, switch, and application code on a single computer (VM, cloud, or native), with a single command on a single computer (VM, cloud, or native). A real-time packet analyzer, Wireshark, is used to monitor and analyse communication transfer between hosts while testing is taking place. In addition, the Iperf tool and a number of other criteria were used to evaluate the performance of ODL and ONOS, which are covered in further depth in Chapter 3 of this report. It is necessary to analyse the vulnerability of a centralised SDN controller using a variety of penetration tools, such as the ones described in Hping3 [17], Nping [18], XORes, and Tor Hammer [19]. The successful HTTP-based and TCP-SYN flood DDoS attacks on the three-node ODL cluster and ONOS controller are shown in this section. It is necessary to use the SNORT [20].

Many researchers are working in many different areas of SDN, but only a small number have sought to extract the security feature of SDN and put it to the greatest possible use in a practical setting. The use of software-defined networking (SDN) to offer network security helps to solve the many difficulties that traditional networks face. For the most part, researchers have relied on SDN controllers that are not in use in the real world, such as those from the NOX and POX families as well as RYU and Floodlight, among others, to include security. Current SDN-based collaborative schemes and solutions for mitigating DDoS assaults rely only on SDN-based controllers that are not already in use by enterprises, according to the authors.

A work in progress is the self-detection of each low-rate and high-rate DDoS attack, which is still being worked on.

III SDN controllers now in use do not have graphical user interface (GUI) capabilities or platform compatibility with either Windows or Mac operating systems. Because the most majority of these controllers (including POX, NOX, RYU, and Floodlight) are Linux-only, they use a traditional DDoS mitigation technique that necessitates the usage of additional network computing resources to function properly.

Ongoing efforts are focused on the development of a framework that can handle and survive distributed denial of service assaults, use open-source APIs, and support many vendors. The absence of noncommercial APIs may be used by any company and adjusted by adding security rules to the network as required.

2. Background Analysis

Availability, integrity, secrecy, authenticity, and undeniable are some of the most fundamental and significant features of secure communication networks, and they are listed in no particular order [21]. When it comes to network security, network administrators must protect their sensitive data, various networking equipment (such as routers and switches), and the communication channel, which acts as a link between the various nodes of the whole network. In particular, one of the most fundamental improvements enabled by the SDN [22] is the separation of the underlying network architecture from the core intelligence of the network. Any new alterations to the network architecture, on the other hand, must comply with the network security criteria that have already been established. In their study of the various security parts of the new model of SDN architecture, notably its separation, Ujjan et al. [23] observed...
the evolution of SDN in its early phases of development and made extensive observations of the distinct security elements. They proposed a new kind of architecture known as SANE in 2006, and it has since gained widespread acceptance. The centralised SDN controller, which handles the logical operations for various network security needs such as authentication and permission, is essential to this system. The evaluation of the security requirements in their proposed design is the last step in this process and will be addressed in the next section. For many firms and organisations, meeting these standards, they claim, will be a challenging undertaking to do [24].

In 2007, Haider [25] was included in the SANE research, which resulted in an expansion of the original study. When it came to this expansion, a different approach was used, in which the need was satisfied with just a modest number of changes to the existing network infrastructure. For network control, two fundamental components are required: a centralised SDN controller, which is responsible for implementing the overall network policy, and a range of ethylene switch devices that may be used throughout the network to provide access to various network resources. It is possible to regulate the network by using these two components. Using the traffic flow rules that are specified in their flow tables, it is just essential to use these ethane switches in order to route data packets from the relevant source to the appropriate destination [26]. Due to the simplification of the network design as well as the centralization of its management, the network now has more programmability and flexibility as a consequence of these changes. A more in-depth investigation of the interaction between SDN and the OpenFlow protocol is enabled by the design of the Ethane architecture due to its modularity. However, at this point, the proposed design was impeded by a number of limitations and limits that were not yet addressed. According to one limitation, SDN applications (such as firewalls and load balancers) may be used to alter the network policy that has already been defined [27].

SDN-based applications may be able to evade security restrictions in their present stage of development, but these applications are also advantageous in terms of providing network-related services in the current level of development of their architecture. This kind of technology is most often seen in network function virtualization (NFV), which is the most common example (NFV). There has been a significant amount of study undertaken on the issue of SDN security, and the findings of this research have been made public. Many vulnerabilities have been identified as a consequence of the alterations that have been made to network components and the linkages that exist between them, which have been discovered by the vast majority of them. When the OpenFlow protocol was first introduced in 2002, many academics, notably Alsmadi et al. [28], released a detailed analysis of it. The findings of this study were acquired by the use of a method known as a threat analysis model [29]. Attacks on networks such as denial of service (DoS) and information leaking have been the focus of research [30]. Additionally, several ways for minimising the attacks have been proposed, but none of them have been put into practise or proven effective. As a result of their analysis, they observed that while utilising the ProtoGENI network, a range of network attacks between clients of the testbed, as well as malicious propagation and flooding of traffic to the wider web, were all possible. It is clear from the repercussions of these researches that there is a significant level of security issue linked with the SDN system. In certain cases, a correlation may be established between the sorts of problems (for example, unauthorised access) and the different SDN layers/interfaces that are impacted by the various issues. This indicates that the most significant distinctions between the old system and the SDN are the integration of the control component and the modification of the information flow components to help in programmability, both of which are shown in this example. There has been very little research done in this area, despite the fact that this study is focused on security risks related with the control and information layers. As mentioned clearly in the next section, increasingly considerable focus has been paid to investigating the potential benefits of the SDN system in terms of organisational security improvements. According to Sánchez-Casado et al. [31], a comprehensive assessment of the general difficulties associated with the security of SDN at different levels has been split into four categories. Despite the many advantages that SDN provides, there are certain security issues linked with it as well. Among the issues still being debated, one is whether or not the centralised SDN controller is vulnerable to distributed denial-of-service (DDoS) attacks. Consequently, the underlying infrastructural layers and control logic are separated, which is the primary source of the issue. While there are several security solutions supplied by the SDN against DDoS attacks, as previously said, a centralised SDN controller remains susceptible to a broad range of different sorts of DDoS attacks owing to the fact that it is located in a central place. Many commercial providers, as well as academic researchers, must focus their attention on the many different forms of hazards that are specific to SDN-based networks in order to provide a well-defined degree of security for these systems [32]. The detection and prevention of distributed denial-of-service (DDoS) attacks on SDN infrastructure are now supported by a variety of technologies. Some of the mechanisms are illustrated in Table 1, while others are depicted in the literature section, as seen in Figure 1 of this document.

Defending against and absorbing malicious surges in network traffic and application utilisation produced by DDoS assaults, while enabling genuine traffic to pass unhindered, are the technique of DDoS mitigation. DDoS mitigation techniques and solutions are intended to mitigate the business risks provided by the complete spectrum of DDoS attack methods that may be used against a company’s network infrastructure and systems. They are first and foremost intended to maintain the availability of resources that are being targeted by attackers. However, DDoS mitigation is also intended to shorten the amount of time it takes to respond to a DDoS attack, which is frequently used by the bad guys as a diversionary tactic to carry out other types of attacks, such as exfiltration, elsewhere on the network, according to the National Institute of Standards and Technology.
According to current state of the art, many SDN-based collaborative schemes and solutions rely only on SDN-based controllers that are not presently in use by organisations to mitigate DDoS assaults. The community is currently grappling with the issue of early detection of each low- and high-rate DDoS attack, which has not yet been resolved. A graphical user interface (GUI) or cross-platform compatibility for Windows and Mac operating systems is not provided by the SDN controllers now in use [40]. All of these controllers are based on the Linux operating system. In the early phases of development, a framework that can handle and resist distributed denial of service (DDoS) assaults, make use of open-source APIs, and support many vendors is being developed. Uncertainty exists around the availability of non-commercial APIs that may be used by any company and customised to meet their own requirements by introducing security controls into the network as required.

Restricted Boltzmann Machine (RBM) is an artificial neural network (ANN) with particle swarm optimization technique, which can learn the distribution of the probability across a number of inputs. The distribution utilised is the conditional distribution of probability given I the inputs on the visible layer, and the likelihood of a hidden layer, (i) the probability of a visible 55 layer in hidden layer. The ANN is extensively used in fields such as reduction of dimensionality, characteristics education, classification, collaborative filtering, and topic modelling. RBM restricts intra-layer connections and results in efficient training and quicker learning compared to other algorithms. RBM is composed of two components, the unit visible and the unit concealed. The input features are taught for further processing in the visible layer and buried layer procedures. For connections between biased-weight units, RBM has binary-valued visible and hidden units with a weight matrix. The weight matrix depends on the network’s dynamic behaviour. The hidden layer is a softmax classifier, which classifies network traffic according to the target class. RBM supports discrete as well as continuously valued target classes.

### 3. Proposed Methodology

The Mininet consists of three distinct. The three VMs have the same hardware characteristics, i.e., 2 GB Random Access Memory (RAM), i5 CPU, and 32-bit operating system. Various IP’s are allocated to various computers. The data-centered tree topology is generated in VM-2. VM-1 and VM-3 are linked through a switch to VM-2. OpenFlow protocol was utilised for southbound API and communication. OpenFlow version 1.3 was used for experimenting. To manage the establishment and connection between different switches, hosts, and controllers, the ping connectivity test was chosen first of all to verify. Host 1 (h1) must submit a ping request from 100 ICMP data packets to host 27 (h27). The rationale for selecting these hosts (h1-h27) is the distance.

In this example, the implementation of a three-node ODL cluster is shown. The SDN network is strengthened in the event that a single controller (leader) fails or stops to operate due to the fact that other controllers (followers) will immediately take over and perform the functionality in question. Because of the capacity to function in a multicontroller environment, greater flexibility is available while dependency on external factors is reduced. The DDoS vulnerability of the three-node ODL clusters under consideration is investigated in further depth in this chapter. Several DDoS traffic penetration technologies are being employed in order to launch a vast amount of traffic at the same time. After being assaulted by a large amount of network traffic, a network controller becomes unresponsive, causing the network’s overall operation to be disturbed.

Essentially, a clustering process is a strategy that facilitates the collaboration and coordination of a range of unique activities in an organised manner. This collaborative working environment may be referred to as a single entity for the purposes of this document. The usage of clustering architecture, which is made possible by the Internet, makes it possible for multiple nodes to connect with one another. It is also feasible to interact and coordinate more readily as

<table>
<thead>
<tr>
<th>References</th>
<th>DDoS attack mechanism</th>
<th>Type of tool and SDN controller used</th>
<th>Experimental limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>[33]</td>
<td>Intrusion is detected based on statistical analysis</td>
<td>OpenFlow switch table entries attack</td>
<td>OMNeT++ Simultaneous detection cannot be performed when there is an alteration in the headers</td>
</tr>
<tr>
<td>[34]</td>
<td>DDoS detection on the basis of entropy</td>
<td>TCP SYN, UDP</td>
<td>Mininet and POX Only limited to the detection mechanism.</td>
</tr>
<tr>
<td>[35]</td>
<td>Prediction based on network bandwidth</td>
<td>DoS attacks</td>
<td>Real testbeds, floodlight Limited to only DoS attacks.</td>
</tr>
<tr>
<td>[37]</td>
<td>Traffic flow migration</td>
<td>DoS attacks</td>
<td>Mininet and Ryu Consistency issue may occur in case of multiple controllers’ environment</td>
</tr>
<tr>
<td>[38]</td>
<td>Network traffic rule-based DDoS mitigation</td>
<td>TCP-SYN traffic flooding attack</td>
<td>Mininet, ODL May increase the consumption of bandwidth and thus increasing the overhead as well.</td>
</tr>
<tr>
<td>[39]</td>
<td>Avant-guard</td>
<td>TCP-SYN traffic flooding</td>
<td>Mininet, POX For the protocols which are not based on TCP SYN, traffic.</td>
</tr>
</tbody>
</table>
a result of the linkages between various nodes. Another way to assess the effectiveness is to look at things like response time, latency, and a range of other aspects. Figure 2 depicts the clustering of the ODL data.

Figure 3 represents the clustering technique of ODL network. Clustering in ODL provides backup support as well as a reduction in the risk of a single point of failure inside the controller. Attacks against the ODL’s infrastructure, on the other hand, are growing increasingly common. It is possible that more controllers (followers) will be attacked by an intruder in the future if just one controller (say, the leader) is targeted by the intruder for a DDoS attack at a later time. This will force the whole network to come to a grinding halt, regardless of whether or not there is a multicontroller in place. When developing a system, there are a number of hazards that must be evaluated and avoided at all costs. A very serious risk in the rundown is that false activity streams will be generated and then used against the team in question. Defeating a distributed denial of service (DDoS) [41] assault is a pretty straightforward situation in which rogue components leave the system impotent. Following one of these attacks, the organization’s benefits are either halted immediately or suspended indefinitely for the hosts associated with that arrangement. It is advised that a single computer or a group of computers be used; it is possible that a single network affiliation or a group of network affiliations be used to connect to a server and transmit packets (TCP/UDP). A denial of administration attack of this kind is carried out.

**Table 2: Different machine’s specifications.**

<table>
<thead>
<tr>
<th>Input machine</th>
<th>Input address</th>
<th>Spec of the input hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine 1</td>
<td>1.193.168.205</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 2</td>
<td>1.193.168.206</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 3</td>
<td>1.193.168.203</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 4</td>
<td>1.193.168.204</td>
<td>64-bit higher-end processor</td>
</tr>
</tbody>
</table>

**Table 3: Input specification of virtual machine.**

<table>
<thead>
<tr>
<th>Input machine</th>
<th>Input address</th>
<th>Spec of the input hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine 1</td>
<td>1.193.168.201</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 2</td>
<td>1.193.168.202</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 3</td>
<td>1.193.168.203</td>
<td>64-bit higher-end processor</td>
</tr>
<tr>
<td>Virtual machine 4</td>
<td>1.193.168.204</td>
<td>64-bit higher-end processor</td>
</tr>
</tbody>
</table>
with the purpose of overburdening the server’s data measure and separating assets that include data from those that do not. It is possible that another user on the network will be unable to access the server as a consequence of this situation. Because it chooses to interrupt regular movement of a server, administration, or system by overloading the target or by combining the target with a flurry of internet activity, which is regarded malevolent, a DDoS attack has the potential to be damaging. A variety of traded-off workstation frameworks are utilised as sources of illicit activity in distributed denial-of-service assaults, which are effective due to the survivability of the targets. As instances of exploited equipment, PCs and other structured assets, such as IoT (Internet of Things) devices, will be provided. Whenever a DDoS attack is initiated from an abnormal situation, it functions as a stumbling block and produces a disruption in the functioning of the network.

DDoS attacks may occur at both the data plane and control plane levels in an SDN network. Packet-in request messages are flooding the control plane layer with each incoming unknown traffic flow and change of flow table entries in the data plane, causing the control plane to become overwhelmed. In the control plane, the effect of a DDoS assault is greater, and as a result, service degradation is seen by end-users. This paper offers a detection method for DDoS assaults in SDN in order to address the aforementioned issues. As a result, the idea of DDoS attack detection in all network situations has emerged as a current field of study.

3.1. DDOS Detection System. A new generation of software-defined networking (SDN) is rapidly taking hold in the network sector, with Market Research Future projecting that the market will grow at a compound annual growth rate (CAGR) of 42.41 percent by 2019, resulting in a market size that will more than double from USD8.82 billion in 2018 to USD59.9 billion in 2019. The SDN market is expected to develop at a compound annual growth rate (CADR) of 26.8 percent according to another market analysis. It has created an array of new technologies such as SD-WAN and SD-Storage as well as 5G and other technologies. It is
currently being integrated with an array of new technologies such as cloud computing, intent-based networking, network security, and other technologies, to name a few examples. There are three layers in the SDN architecture: the application layer, the control layer, and the infrastructure layer, which are all interconnected.

In order to connect with SDN applications, the SDN controller takes use of data obtained from devices at the infrastructure layer. During processing and data forwarding on the data plane, it is up to the infrastructure layer to maintain control over the task and receive path-based instructions from the controller, which it then utilizes for processing and data forwarding. Due to the SDN controller’s central position and management capabilities, it is an attractive target for attackers since it manages the network architecture by sending instructions to the data plane that are route-relevant. To get access to the system’s controller, attackers try to mimic the controller. A breach of the SDN controller will allow a hacker to have complete control of the network and alter it as they see fit.

Several attacks are attempted in order to take advantage of the bandwidth and scalability restrictions of the SDN architecture. Among them are identification of DDoS attacks on a network is the first and most crucial step in dealing with these types of attacks. Researchers from all around the world have submitted their discoveries in order to spot DDoS attacks on the SDN network.

According to the results of thorough testing, it has been determined that our detection algorithm effectively recognizes DDoS attacks (HTTP and TCP SYN) in a timely way, taking into consideration the aforementioned parameters as well as a variety of network scenarios. The approach that was used to perform the testing is discussed in great depth in this section.

First and foremost, five separate virtual machines (VMs) are created. These virtual machines (VMs) will be used to host the various applications. Mininet is a component of the virtual machine I operating system. An ODL (Beryllium version) cluster of three nodes is being utilised to create a multicontroller environment for the tests, which is necessary for the success of the studies. In order to support the vast platform of the ODL controller, a substantial number of plug-ins and features are being created in VM-2. The ONOS machine is featured in the VM-3 virtual machine (Peacock version). Also included is an integration with the SNORT network intrusion prevention system, which is an open-source technology. It is used to launch the assaults since SNORT is capable of doing real-time traffic analysis and packet recording on the IP networks that have been built in VM-5. Assaults and probes are detected, and a variety of protocols are analysed. Figure 4 represents the methodology of the proposed technique.

3.2. Attack Detection in the Input Tools. In order to compare the findings, a range of network circumstances with differing features were used to defend both controllers from these attacks and then to compare the outcomes. The following are brief descriptions of each of these instruments.

In short, Xerxes is a distributed denial-of-service (DDoS) tool that runs in the most efficient manner possible. It is being developed by hackers as a means of countering denial-of-service (DoS) assaults on websites.
DDoS attacks are carried out via the use of networks of computers that are connected to the Internet in order to overwhelm a target. They are made up of computers and other devices (such as Internet of Things devices) that have been infected with malware, allowing the attacker to control them from a distance and so gain complete control over them. Bots (sometimes referred to as zombies) are individual devices that are part of a larger network of bots that work together to complete tasks. Groups of bots interact with one another in a botnet an attacker can use a botnet to initiate an attack by delivering remote instructions to each bot in the network after it has been successfully constructed. In as little as one second after discovering an individual botnet member’s server or network, each bot starts sending requests to the victim’s IP address. This may lead the server or network to become overwhelmed, which can cause genuine traffic to experience a denial-of-service. Given the fact that each bot is a legitimate Internet device, differentiating between attack activity and ordinary Internet traffic may prove to be difficult.

### 3.3. DDOS Prevention System

A key feature of the VM-2 is the integration is provided as part of the VM-2 package. It is made up of Kali Linux, which also happens to be equipped with a range of penetration tools for conducting successful DDoS traffic assaults on the network. An even more detailed depiction of the technique is shown in Figure 5. The hardware requirements for the virtual machines that have been created vary. Table 2 illustrates the same point.

For each new setting in which an experiment is conducted, a new topology is created to fit the outcomes of the experiment. This process continues indefinitely. Table 3 shows the predefined that has been determined for the first circumstance. When network traffic reaches a specific threshold level, it can be observed that the remaining packets are no longer taken into account. It takes around 20 seconds for the network to reach the threshold value, which is a fair estimate.

### 4. Experimental Results

All simulations and testing were carried out on a virtual computer running on a Linux operating system. This collection of penetration tools was run from the Kali Linux virtual machine and was successful in penetrating the DDoS attacks on the VM-2 and VM-3 hosts. HTTP flood attacks on port 8181 are carried out with the assistance of Xerxes and Tor Hammer, whilst TCP SYN attacks are carried out with the assistance of Hping3, Nping, and other tools and scripts. 192.168.9.208 and 192.168.9.203 are the IP addresses of Kali Linux and the SDN controllers, respectively, since they are both on the same network and have the same IP addresses. The following are the many methods in which penetration tools are integrated with the controllers: Figure 6(a) illustrates the Xerxes tool, while Figure 6(b) depicts the hammer tool, both of which are used in distributed denial of service (DDoS) assaults, respectively. We are able to run both DDoS tools on the same Kali system since we are using the same Kali installation. It is possible for both DDoS tools to be...
running simultaneously on the same Kali Linux computer. In order to take advantage of the fact that ODL and ONOS both utilise the TCP port number 8181 for HTTP, the attack command included that port number in the command. Hping3 and Nping are two further tools used to direct traffic towards ODL and ONOS, as seen in Figures 6(a) and 6(b), respectively.

Figure 7 represents the controller design of the proposed work. Hping3 makes advantage of the following characteristics:

- The -c option specifies how many packets should be sent. Packages with the SYN prefix are represented by the letter -S. The port number is indicated by the -p option.
- In order to create a traffic jam, use the word “flood.”
- Random IP addresses are used to conduct attacks using the—rand-source command.

Among the qualities that are utilised on Nping are those that include:

- A nonprivileged TCP connect probe mode is represented by the command—tcp-connect.
- This option specifies the number of packets to transmit per second.

To terminate the programme after a defined number of rounds, use the -c option.

One less word per second – q – reduce the degree of verbosity by one word per second – q –.

In order to produce traffic during a TCP SYN flooding DDoS attack, it is required to calculate and know the IP addresses of the targets, as well as the port numbers on
which the assaults are to take place. Another need is to produce a TCP packet with a random source port that contains the victim port’s flag, the sequence of the individual packets, and a time frame to enable for the multiple packets to be transmitted at the same time as well. As a consequence of this attack, the target host will be bombarded with a large number of IP packets. Figure 8 shows that during each cycle, a new IP packet is generated, and the hping3 software is used to create the vast network flood necessary to achieve the desired outcome. Random UDP packet traffic generation, on the other hand, would flood the target host with a large number of these random UDP packets, resulting in the target host’s failure. In order to produce traffic
aimed at the victim, it is necessary to first identify the IP addresses of the target; after this has been completed, the ports of the source and destination are set to 80 and 1, respectively, during the traffic generation phase. IP packets are generated in a different manner each time. There is a preset number of ports (1000) that have been set up for the purpose of testing. The LOIC is used to achieve this purpose by using a testing and denial-of-service attack application that was printed in the C programming language. It is necessary to send the IP packets to the IP address that has been identified as the victim within the time period given after the IP packets have been created. In Figure 8 on the SDN network, you can see a thorough approach and several phases for the UDP flooding assault on an SDN network (b).

DDoS attacks from multiple sources penetrated the network prior to the initiation of 5000 packets per second of normal traffic flow prior to the initiation of DDoS attacks. As indicated in Figure 9, the average speed of ordinary traffic can be shown to be around 50 miles per hour. In this situation, the amount of legal traffic that is sent out every second is taken into consideration. In this case, the log files were obtained using Wireshark from real-time network activity and saved in a log file format. As soon as traffic starts to flow over the network from the different penetration tools seen in Figures 10 and 11, the transmission of the traffic flow via the network’s connections is initiated by the network’s operating system. According to scenario I, the network seen in Figure 11 and in Figure 10 has been increased to 1, 50,000 packets per second, which corresponds to scenario II. In this graph, it is simple to see the difference between ordinary traffic and TCP/HTTP failures, which is a good thing. The grey line in Figures 9–11 indicates normal traffic, while the blue bars in the same figures reflect TCP and HTTP failures, respectively. Figure 9: normal traffic.

Figure 10 represents the networking scenario, and Figure 11 represents the traffic rules. Figure 12 represents the traffic rules.

SNORT is ready to be utilised in production situations after it has been setup and is functioning in test mode by default with pre-defined ports in the SNORT startup, as seen in Figure 12. Following the successful initiation of DDoS assaults using the various aforementioned penetration tools, the SDN controllers were hammered with about 2,50,000 packets per second in a variety of situations. Rule file may be done after all controllers have been shut down and the local. Rule file has been deleted.

Our DDoS testing on these controllers, as previously indicated, has resulted in every one of them being fully brought down following a successful attack. In order to identify DDoS attacks, several SNORT rules may be employed. These rules can be configured as SDN DDoS alert rules in local rules, and as SDN DDoS alert rules in global rules. In Figure 13, you can see an example of the local ordinances that were put together. The following day, we attempted a DDoS attack using a variety of tools. As shown in Figure 14 below, which shows that network has been detected by the snort console.

Figure 15 represents the alert system of the proposed work. With a packet rate of 50,000 packets/sec in scenario I, the detection time is raised to 10 seconds as compared to the 2, 50,000 information in scenario II dependent on the quantity of packets blasted, the length of time it takes for the controllers to go down and the functioning of the whole network to be disrupted is determined. When compared to instances I and II, where packet loss ranged between 97 and 99.9 percent, it has been discovered that packet loss for scenarios IV and V is a stunning 100 percent. In all of these situations, the kind of traffic experienced by both controllers is the same.

4.1. DDOS Prevention Experimental Study

(i) The following three scenarios are investigated in the context of DDoS attack mitigation for dissimilar forms of net circulation, as detailed below

(ii) ICMP flood circulation, such as the following: the preventative system has established a threshold value that has been launched by the system in order to avoid overloading the network. After 20 seconds, the network had hit the threshold value, which was the least period of time that could have been achieved
Figure 16: Represents the input flood analysis of the proposed work.

Figure 17: Represents the traffic analysis in the proposed network.

Figure 18: TCP flood traffic.
(iii) It has been determined that there is an excessive volume of UDP flood traffic. As shown in Figure below (Figure 16); when the network’s threshold value. After 20 seconds, the network had hit the threshold value, which was the least period of time that could have been achieved.

(iv) In addition, the amount of traffic produced by TCP flooding has been restricted to 40,000 packets per second, with the protection mechanism ordered to delete packets if the threshold is surpassed. The network achieved the threshold value in the shortest period of time feasible, which was just 23 seconds, thanks to the use of high-speed connections.

Figure 17 represents the traffic analysis of proposed work in the network.

Figure 18 represents the TCP flood traffic of the proposed work. It is first explored how different penetration tools may be used to create tools, after which it is determined whether or not these attacks were successful. These packets are examined and then programmed into the ODL controller using a sFlow script in order to successfully establish a DDoS protection architecture. A new kind of DDoS traffic is taken into account for each case, with a different threshold value being applied in each instance. It has been observed that data packets are discarded once the network traffic hits a particular threshold value, which has been established, as previously mentioned.

5. Conclusion and Future Work

In a network, there are several difficulties that might develop the security. DDoS attacks are the common and outbreaks now in use; attackers are using a range of dynamic tactics to execute DDoS attacks, which are growing more successful as time goes on. Traditional security measures, according to the experts, are less effective and ineffective in dealing with these difficulties. As a consequence, the SDN has been put into operation. In a very short amount of time, it has gained significant appeal, owing to the basic notion of isolating the network’s intelligence from the underlying network architecture. Because to the adoption of SDN, control plane and data plane work are no longer separated in the network, and control plane work is now centralised in a network controller, as opposed to before. The traditional networking architecture was built on devices that had control planes and data planes combined into a single device before the advent of SDN; however, with the introduction of SDN, this architecture was transformed. Providing security is one of the most major advantages of software-defined networking (SDN). Using SDN has made it simpler and more realistic to deal with dynamic, high-rate DDoS attacks. Future extensions of this research effort might involve the use of more APIs (both southbound and northbound), as well as a broader range of real-time SDN controllers and a bigger number of network parameters, among other things. It is feasible to determine how well the proposed solution would fair in the case of a subnet attack on the network.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors of this manuscript declared that they do not have any conflict of interest.

References


