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

DDoS Mitigation by Software-Defined Network (SDN) in the Context of ICMP And SYP Approach

Laxmi Poonia[1], Seema Tinker*[2]

Submitted: 17/08/2023 **Revised**: 10/10/2023 **Accepted**: 22/10/2023

Abstract: DDoS attacks have never been easier than they are today, thanks to the advancement of technology and the widespread availability of the internet. The primary goal of a DDoS assault is to shut down or disrupt any internet services that could be using the victim's computer. There are a variety of reasons why it may be done, including personal gain, professional advancement, and political gain. Recent attacks include the largest ever packet per second DDoS attack on Akamai servers, the attack on Amazon, and the strikes on the US Department of Health and Human Services website One can use SDN and Blockchain to verify a legitimate IP address, and Blockchain can be used to store a legitimate user in a trust list with the support of a complicated architecture made up of several helper Blockchains. This research presents three possible network topologies that integrate the usage of Blockchain technology with software-defined networking for the prevention of DDOS attacks.

Keywords: *Advancement, Attack, Blockchain, DDoS, SDN*

1. Introduction

Over the previous decade, networking concepts have stayed mostly constant. Switches and routers of varying sophistication are used to build networks [1]. There are tens of companies developing these devices, and they all use proprietary operating systems and interfaces [1-2]. A business must engage a specialist for each router brand to build a heterogeneous network. Configuration errors are more likely to occur when multiple systems are configured at the same time. Heterogeneous networks can be difficult or expensive to administer due to the incompatibility of multiple systems from the same vendor. To make network systems more flexible, dynamic, and easier to administer, new technology is needed. These requirements could be met by programmable networks, i.e. Software Defined Networking (SDN). SDN [3] has the potential to displace conventional networking. One of the main goals of any data plane device, such as a switch, is to only forward traffic if certain rules stated in the control plane are followed. Network managers will no longer have to rely on data plane device suppliers to manage their networks. SDN control planes now manage all network devices, allowing applications to view the network as a unified logical entity [4]. In this way, software that controls the flow of network traffic can access the upper layer of the network [5].

Network attacks are likewise evolving in step with the advancements in networking technology. DDoS attacks, which aim to take down a website or service, are a real threat today. A distributed denial-of-service (DDoS) attack aims to prevent a network or server resource from being used as intended [6]. Defending against this assault is a challenge since the attacker is rarely traced back. As early as 1995, Strano Network [7] launched a DDoS attack against French government websites. By refreshing their browsers, users were able to carry out this attack. Several more or less sophisticated DDoS assaults have occurred since the original one. As of the third quarter of 2014, the average DDoS attack bandwidth had risen to 13.93 Gbps from 2.88 Gbps in the third quarter of 2013. There were 17 attacks with more than 100 Gbps of bandwidth [8]. DDoS attacks, despite the many proposed detection systems and mitigation measures, are not yet a solved problem or a major threat to the existing Internet [9].

It is still in its infancy when it comes to SDN research and SDN security. DDoS attacks will not be eliminated by the SDN [6-7]. Every new technology and level of abstraction brings with it a new set of attack vectors. A software-defined network (SDN) has many advantages [8]. Several studies [7] are examining DDoS attack pathways and mitigation approaches in SDN setups. As part of our study, we want to investigate DDoS attacks and the development of a novel DDoS attack mitigation system. We believe SDN provides us with a new and powerful instrument to counteract DDoS attacks: DDoS assaults can be detected and mitigated by networks that are more adaptive and easier to manage. SDN, on the other hand, introduces a slew of additional security concerns. SDN security research is still in its infancy, and much remains to be discovered. All the research groups are devoted to strengthening network security by leveraging

[1] *JECRC University, Jaipur-303905, India,*
ORCID ID : 0009-0003-5673-5487
[2] *JECRC University, Jaipur-303905, India,*
ORCID ID : 0000-0002-8518-6777
** Corresponding Author Email: seematinker@gmail.com*

SDN as a means to secure all of these planes of communication, which is our goal as well. A unique DDoS mitigation approach based on the advantages of Software Defined Networking will be developed as a result of our research [10]. New ways of DDoS mitigation for future networks can be created by combining existing detection methods with SDN management [8-10].

This study was able to tell current attacks apart using three different sorting criteria. The first is a vulnerability that has been exploited. Semantic or brute-force attacks can be used in response to this condition. Program attacks, or semantic assaults, abuse a feature or implementation of a protocol or application to get access to sensitive data. TCP SYN flood is the simplest example [11]. Known as "flooding attacks," brute force attacks generate a lot of traffic that appears to be legitimate. The legitimacy of the source address is the second requirement [12]. Packets emerging from the assault traffic can have a real or fake source IP address. Because packet modification functions are not available or the attack requires certain request/reply exchanges, such as the Slowloris attack [13], attacks using legitimate IP addresses are utilized. In most cases, faked IP addresses are used as the source of attacks [14]. Using a faked IP address prevents victims from being able to identify and block the source of the attack. Any genuine server might be used to mirror these attacks. The final criterion is whether or not the subject can be characterized [15]. Attack traffic may or may not be identifiable. The traffic may be identifiable, but it may not be filtered [14].

Building and administering computer networks follows a basic principle that hasn't altered much since the days of the early adopters [10]. As far as communication service providers (CSPs) were concerned, the most important thing was to provide a single service – whether that service was a voice, video, or data access. Customers of single-service connections can be reached by cable or radio towers installed by CSPs. Changes in service demand and changes in the OSI model have increased CSP infrastructure. To provide a wide range of services to clients, it was required to expand the physical infrastructure (voice and data, voice and video, etc.).

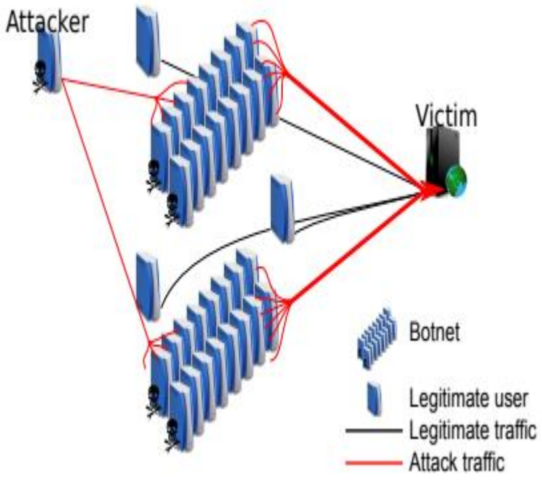

Fig 1. DDoS attack [11]

This model was quickly discovered to be unsustainable. Thus, layer 2 virtualization, such as Asynchronous Transfer Mode, was developed by the industry (ATM). New technology enabled CSPs to provide several services over the same physical infrastructure [12].

The next service that users requested was Internet access. To take advantage of the already established infrastructure, a new virtualized layer has to be added on top of the already existing layer 2. IP connectivity was provided to clients by CSPs without increasing infrastructure expenses. With their infrastructure speeding up and capacity increment, the CSPs became predominantly Internet service providers in the late 2000s (ISPs) [13].

It is tough to administer, complicated, and highly proprietary depending on the vendor of the networking hardware in use in today's networks. Increased demand for bandwidth, scaling, huge data transfers, and dynamic architecture changes are putting fresh pressure on ISPs [10]. To respond to these demands while maintaining a sustainable infrastructure and keeping prices down, more enhanced technologies on the top layers of the OSI model are required. The technologies of programmable networks appear to be the answer to these consumers' and providers' expectations. Computer networks underwent a paradigm shift in the early 1990s with the advent of programmable networks. Flow control is abstracted from network hardware by software in programmable networks. With this abstraction, re-configuration of the network is made easier [8]. A common API means that network administrators are not tied to a single network hardware vendor [13-14].

As a result of these changes, network costs will be reduced, network resources will be more dynamically allocated, transparency will be boosted, and privacy and security technologies will benefit. In the next paragraphs, we'll discuss two of the most common programmable network technologies [15]. Both SDNs and NFVs (network function virtualization), are briefly discussed in this article (SDN).

SDN and NFV aren't competing for technologies; in fact, they're best served by collaborating. New technologies bring with them new ideas for network planning and management. Data plane virtualization may benefit from the NFV technology that SDN uses for network virtualization. SDN-based network management, on the other hand, could aid NFV implementation [16].

1.1. Software Defined Networking

Software Defined Networking (SDN) is another area of interest in programmable networks. Because of the increasing need for scalable and adaptable networks, SDN has been reawakened, particularly in data centers. In 1996, [17] introduced the basic concept of SDN. SDN, on the other hand, has recently piqued the interest of academics as well as business leaders.

In total, there are three layers to this puzzle. The data plane is the lowest layer of infrastructure. Simple network equipment, such as switches, make up this plane. These switches lack features that would make them easier and cheaper to use. When the flow table defined from the control plane using the southbound protocol is used, only incoming packets are dropped or forwarded accordingly. SDN's OpenFlow protocol [19] was deemed its initial standard. The data plane devices can be accessed and manipulated. Even though OpenFlow is not the only protocol available (e.g., XMPP [20]), it is regarded as a standard and is supported by numerous firms in their SDN-ready products. The control layer sits on top of the data plane, above the network devices. It connects the applications at the top of the architecture with the network devices at the bottom. An SDN controller serves as the "brain" of the control layer [17-20]. Through open interfaces, the controller gives apps access to the underlying network while still providing them with a centralized view of the network. Commercial and open-source controllers can be found [17-18, 20].

Applications that manage and secure the underlying network could make up the higher layer. The controller or the northbound API of the controller can be used to connect with the apps. All network information is stored in one place, so the controller has access to this data. There are northbound APIs in the controller that allows applications to configure and upload records into data plane flow tables based on the above information.

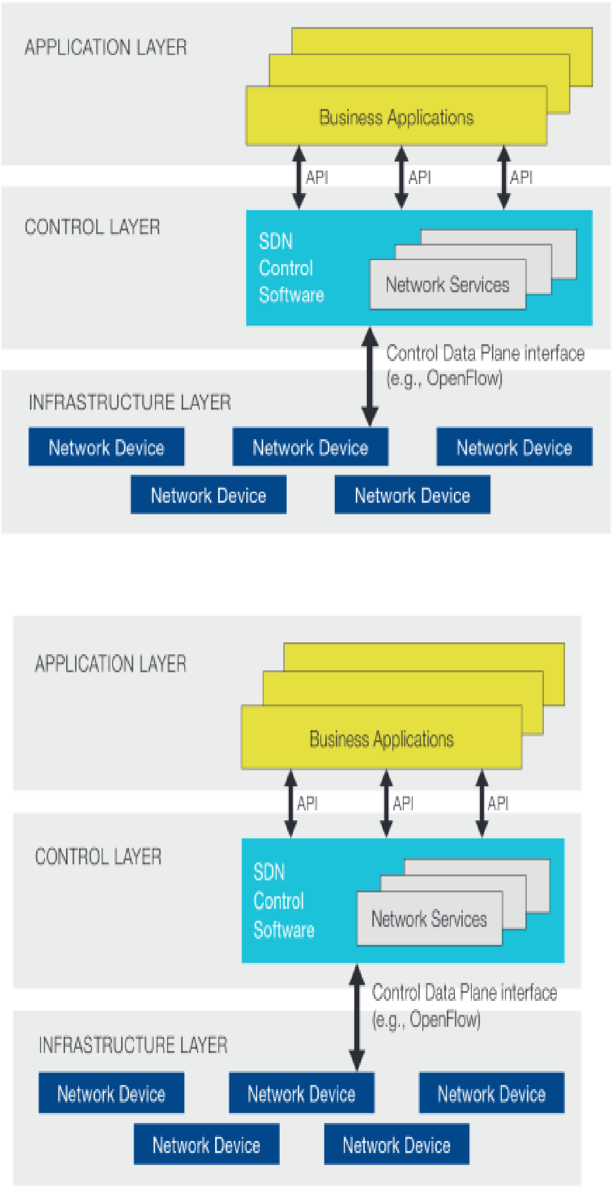

Fig 2. SDN Framework [21]

1.2. Network Functions Virtualization

A new network technology called Network Function Virtualization (NFV) is in the works (NFV). Network services are being migrated from proprietary hardware to the cloud as part of this initiative. NFV has three primary goals: using software-only solutions to reduce hardware costs, maximizing the utilization of a single network for different applications, and creating more dynamic networks[22]. Several network operators' whitepapers [23] outlined the major concepts. It's a fundamental principle to segregate network functions from specific hardware.

Network equipment like routers and firewalls might then be replaced by virtual machines that provide the same services. If this is the case, adding additional network functionality could be done without the need for a new network device to be connected. On industry standard high-volume servers and switches and storage, consolidation of network equipment is depicted in Figure Members of the ETSI1 Industry Standardization Group for NFV are proposing research and specification of this technology. Telecommunications and information technology (IT) companies are represented among the group's members [24]. The first part of the NFV definition was completed by the end of 2014. Documents explaining NFV security, for example, can be found at [25]. Furthermore, the Open Platform for NFV was established [26]. NFV ISG, an ETSI-affiliated open-source group that aims to speed up the development of NFV, is the driving force behind this new open-source project.

2. Background Information: in the Context of Literature Investigation

2.1. Recent Examples

Before going into detail on how DDoS assaults are currently detected and mitigated, let's take a look back at some of the more notable attacks from the past few years. We chose the Spamhaus DDoS attack, as well as DDoS strikes against Czech organizations. Spamhaus was the target of a DDoS attack in 2013 that peaked at over 300 Gbps [27]. So far, this was the largest wild animal attack. The assault was reflected by DNS servers that had been incorrectly set up. Taxonomists classified it as a type of application attack because of the spoofing of the source IP address. However, at this level of traffic, neither the exploited vulnerability nor the potential for characterization matters. This attack took the use of a flaw in the DNS server [28]. Since it was first documented several years ago, this "vulnerability" remains an outstanding topic. Since then, the attack's focus has changed. Spamhaus was the target of the initial attack. CloudFare's mitigation technology shifted the attack to their network, where it was more intense. Finally, the attacker targeted the bandwidth providers used by CloudFare. In the last phase, more than 300 Gbps of traffic was detected. This rate of attack impacts not just the victim's network, but also non-Spamhaus sites that use the crowded infrastructure to communicate with each other. A second example is the 2013 DDoS attack on different Czech Republic institutions. Online media, banks, and telecommunications companies were all targeted throughout the four-day assault. The attack had a peak throughput of one gigabit per second. It was a smaller attack than Spamhaus, but administrators in the Czech Republic had a difficult time dealing with it. TCP SYN flood assault was reflected as well, however, this was much easier to detect an attack. Taxonomically it was a brute-force attack with a faked source IP address, as defined by the taxonomy Reflectors on the Internet are crucial to the success of reflected attacks. used as a mirror on any device that is linked to the internet. Even though honeypots are designed to make the Internet a more secure place, they have been abused as very specialized and effective reflectors. place. BCP38 [29] discusses how to stop attackers from faking IP addresses in the same way as recursive DNS servers do. By removing BCP 38 from the Internet of Things, A mirrored DDoS assault could include your brand-new refrigerator. ATMs and credit card readers were also knocked offline as a result of these attacks. To keep track of DDoS attacks around the world, they've set up a digital map [26-28].

2.2. Mitigation of DDoS attacks

DDoS defense is a difficult problem to solve. Identifying whether the attack saturates the victim's Internet connection or overloads its servers is critical from a DDoS mitigation perspective [1-4]. There may be no choice but to move your mitigation closer in order to protect yourself from an overwhelming attack. While this can be done with the help of many network administrators, it does so only if they are all working together [2-3]. As a result, Internet service providers (ISPs) stress the need for network neutrality and to avoid interfering with traffic. An organization's mitigation strategy, incorporating DDoS protection systems, can be used to neutralize other DDoS attacks [17, 18, 21, 22, 25, 27]. However, these mitigation solutions are frequently constrained to a perimeter device, such as a firewall, which quickly becomes a bottleneck in terms of performance. It is challenging in today's networks to distribute this load among all devices in the business that can filter traffic. Software Defined Networking (SDN) offers a way to improve this [11, 17, 19].

A third-party organization can also mitigate both threats. DDoS protection services are available from several commercial providers like Incapsula, Prolexic, CloudFlare, and Radware. There are three parts to minimizing the impact of an attack. There are several ways to mitigate the effects of a distributed denial of service (DDoS) assault. Second, the mitigation firm's scrubbing center filters traffic. After a while, only routine user traffic is sent to its final destination with a minimal amount of delay.

2.3. DDoS Mitigation and Security in SDN

SDN security is a focus of our investigation. Currently, security research in SDN is focused on OpenFlow and the SDN architecture. You may find an in-depth analysis of current research in [12]. The concerned SDN layers' security research was covered till the autumn of 2013. As a result of the study, it was found that researchers were working to improve network security and OpenFlow protocol, for example, through an assessment of OpenFlow vulnerabilities [13] and a study of SDN's overall security [14]. DoS attacks are becoming more common, and security analysis is focusing on control-data plane concerns rather than on application-control plane vulnerabilities, according to the researchers [12-17].

SDN design difficulties, their remedies, and network security advancements are the focus of more research. This topic has been explored in depth in several studies [2, 21, 22, 31-43] It is proposed to improve network and application security. SDN-enabled networks could benefit from a security solution based on a hybridization of traditional and SDN methodologies. OpenFlow-enabled networks can be traced back to anomalies [18]. It is found that traditional networks face many difficulties in detecting and mitigating DDoS attacks.

SDN was offered as a new mitigation strategy for DDoS attacks [31-37]. Various techniques are incorporated along with SDN such as decision tree [38], forward feature detection [39], and Unsupervised online anomaly [40], which are used to improve the DDoS attack detection capacity of SDN. The detection and mitigation of DDoS attacks are implemented using self-organizing map [41] is used. An SND-based controller is used for the detection and prevention of DDoS attacks in a smart grid [42]. Several other techniques such as collaborative approach [43], wavelet-based transform and CNN [44], and programmable switches [45] are used to improve DDoS attack mitigation.

Data plane security is the primary topic of the first section. The safety of communication between SDN planes is the focus of the second study topic. The third is focused on the safety of the plane's controls. The fourth area is the focus of our investigation. Security enhancements and the creation of SDN-enabled technologies are covered.

3. Methodology

Definite Framework

For the detection and mitigation of DDoS assaults, we believe SDN is the right platform.

It's a known fact that DDoS attacks are a problem, and several mitigation strategies could help reduce the frequency of attacks. No doubt that this issue needs to be addressed in the future as well as in current networks. We feel that adopting SDN for DDoS detection opens up new avenues. SDN ensures dynamic and configurable networks. They'd be able to respond to changes in packet forwarding more quickly and effectively. Despite its rapid development, SDN is still a relatively new field [7, 8, 27, 21, 12].

Objective

The following are the framed objectives of the proposed work:

- To evaluate the performance of SDN with respect to traditional network
- To investigate the SDN-specific security vulnerability

4. Experimental Set

The proposed DDoS attack detection framework based on SDN is tested using Mininet 2.2.2 and the network configuration is shown in Figure. The testbed's hardware requirements are as follows: 8 GB DDR4-2400 MHz RAM and Windows XP Professional operating system are required for Ubuntu 18.04's Ryu controller. S1 serves as the edge switch for the experimental network, which includes S4, S5, and S7, each of which is connected to three hosts, each of which has a unique ID number. DDoS attacks were conducted from switch s1 to host h15 after Scapy was used to inject traffic into the network as background traffic. In a regular network, background traffic has an information entropy of approximately 0.8. So we ran the simulation using Hn(X) = 0.80 and 0.20 as the values for Hn(X). When it comes to DDoS attacks, ICMP and SYN flood attacks [24 and 11] are the most common. Flow entries and information entropy are counted in real-time at the edge switch, and Wireshark keeps track of the attack port's entropy level.

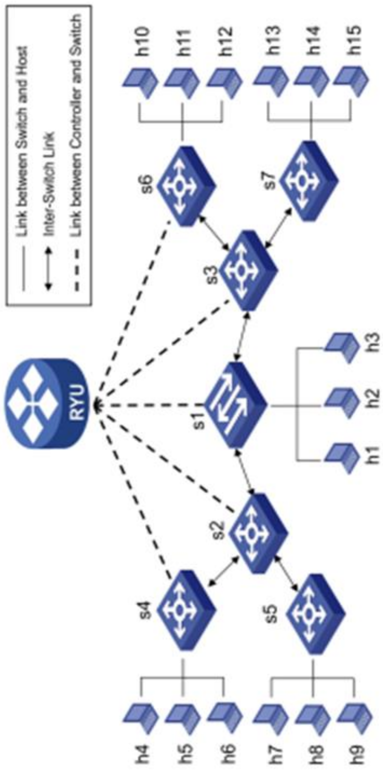

Fig 3. Architecture of DDos [10]

Table: 1. 5_Feature tuple

Average number of packets	avg_pkt_num
Average number of bits	avg_pkt_bit
Growth rate of port	Rate_port
Growth rate of flow	Rate_flow
Growth rate of source IP	Rate_sip

Table: 2. Data set of flows

Data Set	Flow type	Number of flows	Proportion
All	Normal attack	(69276993)13 920	1
Training set	Normal attack	(46184662) 9280	2/3
Test Set	Normal attack	(23092331) 4640	1/3

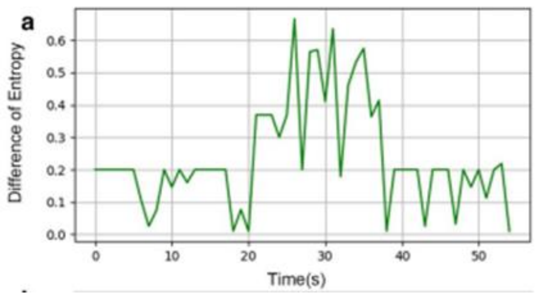

Fig 4. Results based on Information Entropy Difference (IED**)**

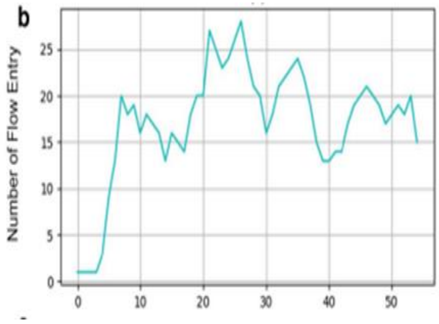

Fig 5. Result of flow entry parameter

4.1. Experiment on ICMP flood attack

An ICMP flooding incident generates a large number of packets all with the same destination IP address. In most cases, the information entropy difference between the destination IP and the source IP is less than 0.2

The destination IP's entropy differential rises as soon as the DDoS attack begins at 20 seconds. Thus, the attack has no discernible effect on the quantity of fowl entering. Figure 6c shows the outcome as predicted by the edge switch's pre-detection method. An irregularity in the edge switch alerts the controller at 22 seconds [14].

As a comparison to a standard centralized system, which has a preliminary detection module installed in the edge switch for demonstration purposes, we use our cooperative detection approach on the control plane even though our system does not. Two of the most notable distinctions between the two are the availability of real-time traffic statistics and the ability to detect unusual attacks. [18].

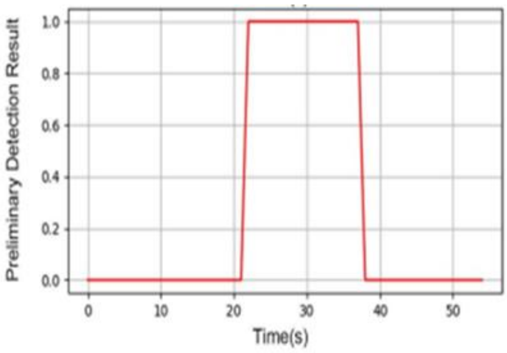

Fig 6. Preliminary detection result

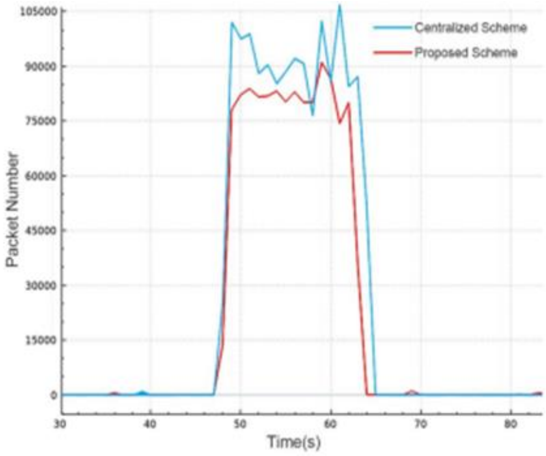

Fig 7. Flow comparison of attacked port

5. Results

5.1. Result Evaluation

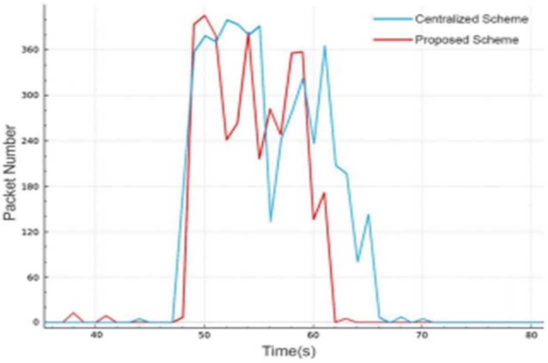

Fig 8. Centralized and Proposed scheme with respect to packet number

The proposed strategy's controller CPU use is compared to that of a centralized scheme in order to evaluate the improvement in controller overhead brought about by the proposed method.

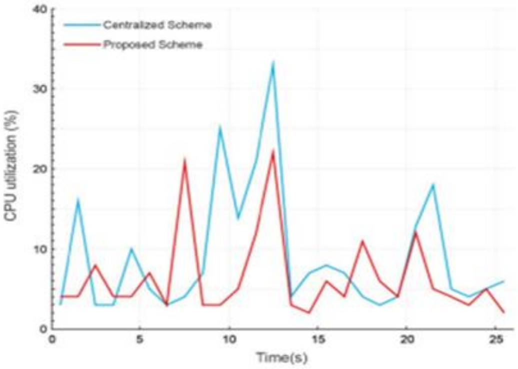

Fig 9. CPU utilization (ICMP)

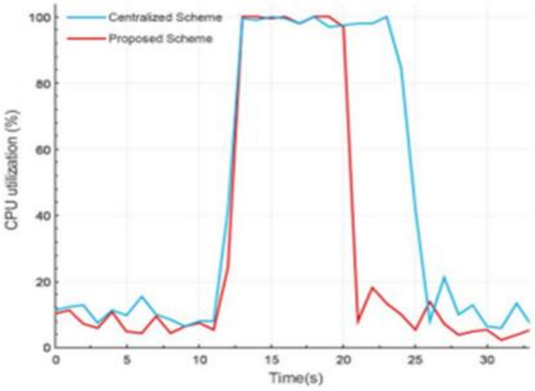

Fig 10. CPU utilization (SYN)

When comparing our proposed system with the centralized one, we utilize a controller that continuously runs the same accurate detection algorithm in a polling way on the control plane, and the edge switch on the data plane does not perform any additional processing of its own

When the app is opened, the controller's CPU use jumps considerably, up to 100%. Due to the way the suggested technique only begins the detection module when the controller receives an anomalous report from the edge switch, the CPU occupancy rate is substantially lower than in the traditional centralized system when an attack does not occur. Additionally, there are: In comparison to the current centralized method, the proposed one has a 5 s lower peak CPU occupancy rate. Because controller overhead decreases as network capacity increases, we use the topology represented in Fig. 1 to demonstrate this fact. We were only able to test with a network twice the size because of the restrictions of the test platform. The network has a tree topology with a depth of four and contains 15 switches and 30 hosts. Only standard traffic is injected into the network. The two ways are then tabulated separately in terms of CPU consumption. [18].

Every five minutes during the 65-minute statistical period, an average CPU utilization is taken for comparison. It demonstrates that the proposed technique can reduce the controller's burden even further as the network grows in size. As the network expands in size, our framework's advantages in controller overhead will become more important.

6. Conclusion

SDN-based cooperative detection of DDoS attacks using entropy and ensemble learning is proposed in this study. The preliminary inspection module is put on the edge switch in the data plane to collect real-time information on network traffic, using the rapid detection technique. In the event of an anomaly, the controller will be notified. The control plane's attack detection module uses a random forest method and a five-element feature group to identify unusual communications. If attack traffic is detected, the controller immediately sends a dropping packet command to the edge switch through a flow table update, stopping the attack in its tracks

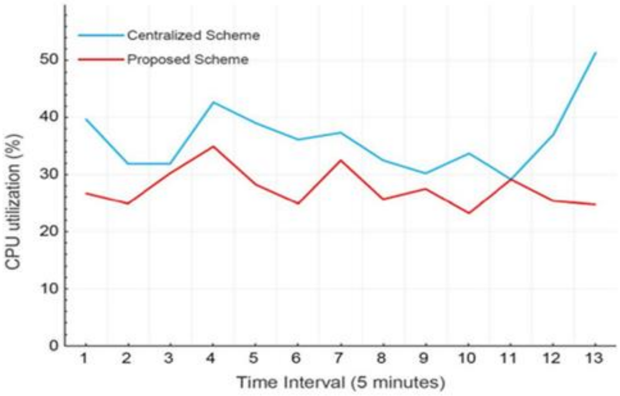

Fig 11. CPU utilization of the controller in the larger scale network

completely. During this new cooperative arrangement, some of the detection tasks were transferred from the control plane to the data plane. DDoS assaults can be detected using our method's simulations of ICMP and SYN food attacks, according to the results. When a network grows in size, the controller's CPU use can be reduced and the period of peak CPU utilization can be shortened simultaneously.

Author contributions

Laxmi Poonia: Methodology, Software, Field study, Validation, Investigation,

Seema Tinker: Conceptualization, Data curation, Writing-Original draft preparation, Field study, Visualization, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Mohammed, S.S., Hussain, R., Senko, O., Bimaganbetov, B., Lee, J., Hussain, F., Kerrache, C.A., Barka, E. and Bhuiyan, M.Z.A., 2018, October. A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network. In *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 1-8). IEEE.

[2] Giri, N., Jaisinghani, R., Kriplani, R., Ramrakhyani, T. and Bhatia, V., 2019, December. Distributed denial of service (DDoS) mitigation in software defined network using blockchain. In *2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 673-678). IEEE.

[3] Bhushan, K. and Gupta, B.B., 2019. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), pp.1985-1997.

[4] Bhushan, K. and Gupta, B.B., 2018, February. Detecting DDoS attack using software defined network (SDN) in cloud computing environment. In *2018 5th international conference on signal processing and integrated networks (SPIN)* (pp. 872-877). IEEE.

[5] Tayfour, O.E. and Marsono, M.N., 2020. Collaborative detection and mitigation of distributed denial-of-service attacks on software-defined network. *Mobile Networks and Applications*, *25*(4), pp.1338-1347.

[6] Hugues-Salas, E., Ntavou, F., Ou, Y., Kennard, J.E., White, C., Gkounis, D., Nikolovgenis, K., Kanellos, G., Erven, C., Lord, A. and Nejabati, R., 2018, March. Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN). In *Optical fiber communication conference* (pp. M2A-6). Optica Publishing Group.

[7] Khairi, M.H., Ariffin, S.H., Latiff, N.A., Abdullah, A.S. and Hassan, M.K., 2018. A review of anomaly detection techniques and distributed denial of service (DDoS) on software defined network (SDN). *Engineering, Technology & Applied Science Research*, *8*(2), pp.2724-2730.

[8] Yadav, S.K., Suguna, P. and Velusamy, R.L., 2019, July. Entropy based mitigation of Distributed-Denial-of-Service (DDoS) attack on control plane in software-defined-network (SDN). In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

[9] Shah, S.Q.A., Khan, F.Z. and Ahmad, M., 2021. The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. *Computer Networks*, *187*, p.107825.

[10] Ubale, T. and Jain, A.K., 2020. Survey on DDoS attack techniques and solutions in software-defined network. In *Handbook of computer networks and cyber security* (pp. 389-419). Springer, Cham.

[11] Novaes, M.P., Carvalho, L.F., Lloret, J. and Proença, M.L., 2020. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, *8*, pp.83765-83781.

[12] Ur Rasool, R., Wang, H., Ashraf, U., Ahmed, K., Anwar, Z. and Rafique, W., 2020. A survey of link flooding attacks in software defined network ecosystems. *Journal of Network and Computer Applications*, *172*, p.102803.

[13] Zhai, P., Song, Y., Zhu, X., Cao, L., Zhang, J. and Yang, C., 2020, August. Distributed denial of service defense in software defined network using OpenFlow. In *2020 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 1274-1279). IEEE.

[14] Saba Bashir Ahmed, Yasir Abdelgadir Mohamed, "An Approach for Software-Defined Networks Security", 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), pp.1-8, 2023

[15] Kyaw, A.T., Oo, M.Z. and Khin, C.S., 2020, June. Machine-Learning Based DDOS Attack Classifier in Software Defined Network. In 2020 17th International

Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 431-434). IEEE.

[16] Lawal, B.H. and Nuray, A.T., 2018, May. Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In *2018 26th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.

[17] Guha Roy, D. and Srirama, S.N., 2021. A blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network. *Software: practice and experience*, *51*(7), pp.1540-1556.

[18] Pillutla, H. and Arjunan, A., 2019. Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, *10*(4), pp.1547-1559.

[19] Bavani, K., Ramkumar, M.P. and GSR, E.S., 2020, March. Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined Network. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 380-385). IEEE.

[20] Ali, A. and Yousaf, M.M., 2020. Novel three-tier intrusion detection and prevention system in software defined network. *IEEE Access*, *8*, pp.109662-109676.

[21] Lukaseder, T., Ghosh, S. and Kargl, F., 2018. Mitigation of flooding and slow DDoS attacks in a software-defined network. *arXiv preprint arXiv:1808.05357*.

[22] Al-Sakran, H., Alharbi, Y. and Serguievskaia, I., 2019, October. Framework architecture for securing IoT using blockchain, smart contract and software defined network technologies. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-6). IEEE.

[23] Tu, Z., Zhou, H., Li, K., Li, M. and Tian, A., 2020. An energy-efficient topology design and DDoS attacks mitigation for green software-defined satellite network. *IEEE access*, *8*, pp.211434-211450.

[24] Dharmadhikari, C., Kulkarni, S., Temkar, S., Bendale, S. and Student, B.E., 2019. A study of DDoS attacks in software defined networks. *IRJET*, *6*(12).

[25] Fenil, E. and Mohan Kumar, P., 2022. ShChain_3D-ResNet: Sharding Blockchain with 3D-Residual Network (3D-ResNet) Deep Learning Model for Classifying DDoS Attack in Software Defined Network. *Symmetry*, *14*(6), p.1254.

[26] Patil, J., Tokekar, V., Rajan, A. and Rawat, A., 2022. Discriminate, locate and mitigate DDoS traffic in presence of Flash Crowd in Software Defined Network. *The Journal of Supercomputing*, pp.1-24.

[27] Joshi, B.K., Joshi, N. and Joshi, M.C., 2018, August. Early detection of distributed denial of service attack in era of software-defined network. In *2018 Eleventh International Conference on Contemporary Computing (IC3)* (pp. 1-3). IEEE.

[28] Mohammadi, R., Lal, C., Conti, M. and Sharma, L., 2022. Software defined network-based HTTP flooding attack defender. *Computers and Electrical Engineering*, *101*, p.108019.

[29] Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A. and Alsubhi, K., 2022. Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network, *Intelligent Automation and Soft Computing*, 32(2):923-938.

[30] Susilo, B. and Sari, R.F., 2021, January. Intrusion Detection in Software Defined Network Using Deep Learning Approach. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0807-0812). IEEE.

[31] S. G. Rawat *et al.*, "A Survey of DDoS Attacks Detection Schemes in SDN Environment," *2023 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Genoa, Italy, 2023, pp. 01-06, doi: 10.1109/CITS58301.2023.10188707.

[32] N. Gupta, R. Agarwal, S. S. Dari, S. Malik, R. Bhatt and D. Dhabliya, "DDoS and Cyber Attacks Detection and Mitigation in SDN: A Comprehensive Research of Moving Target Defense Systems," *2023 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2023, pp. 1-8, doi: 10.1109/ICDSNS58469.2023.10245455.

[33] A. R and K. S, "Deep Learning Approach for Intrusion Detection and Mitigation in IoT Environment: A Comprehensive Study," 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2023, pp. 1-6, doi: 10.1109/RAEEUCCI57140.2023.10134161.

[34] L. N. Kamalesh, P. Kumar and N. Pradhan, "Threats to Control Plane of Software Defined Networks: An Extensive Study," *2023 4th International Conference on Computing and Communication Systems (I3CS)*, Shillong, India, 2023, pp. 1-10, doi: 10.1109/I3CS58314.2023.10127564.

[35] A. R and K. S, "Deep Learning Approach for Intrusion Detection and Mitigation in IoT Environment: A Comprehensive Study," 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), *Chennai, India, 2023, pp. 1-6, doi: 10.1109/RAEEUCCI57140.2023.10134161.*

[36] S. G. Rawat *et al*., "A Survey of DDoS Attacks Detection Schemes in SDN Environment," *2023 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Genoa, Italy, 2023, pp. 01-06, doi: 10.1109/CITS58301.2023.10188707.

[37] Rai, A., D Vyavahare, P. and Jain, A., 2019. Disatributed DoS attack detection and mitigation in software defined network (SDN). Proceedings of Recent Advances in Interdisciplinary Trends in Engineering & Applications (RAITEA).

[38] Kousar, H., Mulla, M.M., Shettar, P. and Narayan, D.G., 2021, June. Detection of DDoS Attacks in Software Defined Network using Decision Tree. In 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT) (pp. 783-788). IEEE.

[39] Matsa, L.S., Zodi-Lusilao, G.A. and Bhunu-Shava, F., 2021, November. Forward Feature Selection for DDoS Detection on Cross-Plane of Software Defined Network Using Hybrid Deep Learning. In 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1-7). IEEE.

[40] Scaranti, G.F., Carvalho, L.F., Junior, S.B., Lloret, J. and Proença Jr, M.L., 2022. Unsupervised online anomaly detection in Software Defined Network environments. Expert Systems with Applications, 191, p.116225.

[41] Harikrishna, P. and Amuthan, A., 2021. Rival-Model Penalized Self-Organizing Map enforced DDoS attack prevention mechanism for software defined network-based cloud computing environment. Journal of Parallel and Distributed Computing, 154, pp.142-152.

[42] Ahmed, Z., Afaqui, N. and Humayan, O., 2019. Detection and prevention of DDoS attacks on software defined networks controllers for smart grid. International Journal of Computer Applications, 975, p.8887.

[43] Tayfour, O.E. and Marsono, M.N., 2021. Collaborative detection and mitigation of DDoS in software-defined networks. The Journal of Supercomputing, 77(11), pp.13166-13190.

[44] Fouladi, R.F., Ermiş, O. and Anarim, E., 2022. A Novel Approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-Defined network. Computers & Security, 112, p.102524.

[45] X. Chen *et al*., "Empowering DDoS Attack Mitigation with Programmable Switches," in *IEEE Network*, vol. 37, no. 3, pp. 112-117, May/June 2023, doi: 10.1109/MNET.107.2100643.

[46] Rambabu, B. ., Vikranth, B. ., Anupkanth, S. ., Samya, B. ., & Satyanarayana, N. . (2023). Spread Spectrum based QoS aware Energy Efficient Clustering Algorithm for Wireless Sensor Networks . International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 154–160. https://doi.org/10.17762/ijritcc.v11i1.6085

[47] Juan Garcia, Guðmundsdóttir Anna, Johansson Anna, Maria Jansen, Anna Wagner. Intelligent Decision Support using Neural Networks in Decision Science. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/203