Grenze International Journal of Engineering and Technology, June Issue

DDOS Attacks Detection and Mitigation in SDN using Machine Learning

Samuel Kennedy[1], R. Chitra[2], E. Vinodh Ewards[3], T. Jemima Jabaseeli[4] and M. Sandhia[5]
[1-3, 5]Division of CSE, Karunya Institute of Technology and Sciences,Coimbatore, India.
Email: samuelkennedy@karunya.edu.in, chitrar@karunya.edu, ewards@karunya.edu, sandhiam@karunya.edu.in
[4]Division of AIML, Karunya Institute of Technology and Sciences, Coimbatore, India
Email: jemima_jeba@karunya.edu

***Abstract*—A new networking paradigm called software-defined networking, or SDN, gives a controller and its applications the capacity to see the whole network and to design it in a flexible way. This allows for new developments in network protocols and applications. Many SDN applications depend on the logically centralized control plane of SDN to offer the complete network visibility, which is one of its main benefits. The literature offers a novel attack vector peculiar to SDN that substantially undermine this basis. Our novel attacks have some spirit in common with spoofing attacks in legacy networks (like the ARP poisoning attack), but they vary greatly in that they take use of certain vulnerabilities that arise from the way contemporary SDN functions differently from legacy networks. The knowledge about virtual machines, which is a crucial building piece for both topology-aware SDN applications and core SDN components, may be effectively poisoned by successful assaults.**

***Index Terms*— SDN, DDOS, Attacks, Machine Learning, networks.**

I. INTRODUCTION

Within the domain of Software-Defined Networking (SDN), networks are becoming more vulnerable to a range of cyber threats due to their increased complexity and connectedness. One such threat is Distributed Denial of Service (DDoS) assaults [1]. The goal of these assaults is to overload a network's capacity and interfere with the delivery of services. Proactive and flexible approaches are needed to address this issue in order to recognize and mitigate problems early [2]. SDN offers a viable way to improve network security through the use of machine learning and it is shown in Figure 1.

II. RELATED WORKS

The advantages that Software Defined Networking (SDN) offers, including scalability, flexibility, monitoring, and simplicity of invention, have made it very popular [3]. It must, nonetheless, be adequately shielded from security risks. The distributed denial-of-service (DDoS) assault is one of the main threats to the SDN network. In an SDN network, there are several ways to stop a DDoS assault [4]. In order to identify and stop the DDoS assault in an SDN network have assessed a number of Machine Learning approaches, including J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN) [5-8]. During the assessment phase, the best model for the suggested network was trained, chosen, and then used in a mitigation and

Grenze ID: 01.GIJET.10.2.659

Figure 1. Network Security

prevention script to identify and lessen assaults [9]. The results shown that J48 outperforms the other algorithms under evaluation, particularly when it comes to training and testing time [10].

III. METHODOLOGY

The proposed modal is look into potential defensive tactics called Topo Guard (Topology Guard) in an effort to lessen these assaults. As shown in Figure 2, the proposed system observe that it is challenging to solve the issue with static configuration alone (much like with static ARP entry for hosts or the port security feature for switches to address ARP poisoning attacks). This is because static configuration necessitates laborious, prone to error manual labor and is not appropriate for managing network dynamics, which is a valuable SDN innovation. The proposed Topo Guard modal offers a new security enhancement to the current VM Open Flow controllers that provides automated and real-time detection of Virtual Machine exploitation, in order to better balance security and usability. Topo Guard prevents host location hijacking attacks and link fabrication attacks by using SDN-specific capabilities to examine precondition and post condition to validate the validity of host migration and switch port property.

A. Allocation of Traffic Across Multiple Routing Paths

This module is designed to solve the lossy network flow optimization issue of distributing traffic across many routing channels when poisoning is present. The portfolio selection theory is to link the optimization issue to the asset allocation problem, enabling individual network nodes to assess the pollution effect locally and aggregate this data for the source nodes. SDN/Open Flow Topology Management Service's first security study. Specifically a new vulnerabilities in eight popular SDN/VM Open Flow controllers that are now in the Device Tracking Service and Link Discovery Service.

B. Characterizing The Impact of Poisioning

This module allows a source node to allocate traffic based on estimations of the influence of position, which are collected and characterized by the network nodes. To include the poision impact in the traffic allocation issue, a source node has to estimate the poision effect on transmissions across each connection. However, the local estimations must be updated continuously in order to represent the jammer movement and the dynamic impacts of the poison assault. The proposed approach suggests using Virtual Machine Poisoning Attacks to take advantage of the weaknesses is identified. It shows that such assaults are feasible both on a hardware SDN testbed and in the NetBeans emulation environment.

C. Effect of Jammer Mobility on Network

This module's capacity indicates the highest number of links that may be sent over a wireless connection when using min max scheduling. Data generated by the source should always be delivered during the moment when the poisoning is happening, with a high packet delivery rate. This will result in a lower throughput rate. The traffic allocation may be altered to recover the poisoned route if the source node recognizes this impact and changes the low delivery ratio on each way.

D. Estimating End-To-End Packet Success Rates

In order to ascertain the best traffic allocation, the source must estimate the effective end-to-end packet success rate for each connection in a routing route. assuming that the update relay duration is much less than the entire time needed to transfer packets from each source to the appropriate destination. Our study delves into the

defense space and suggests automated strategies to counteract Virtual Machine Poisoning Attacks. Additionally, it provides a prototype defensive system called Topo Guard, which is now operational in Floodlight but can be readily expanded to include additional controllers. According to our analysis, Topo Guard barely slightly reduces performance.

The main system is called "SDN/Open Flow Network". The modules "Traffic Allocation across Paths," "Poison Impact Characterization," "Jammer Mobility Impact," and "Estimating End-to-End Packet Success Rates" are coupled to each other. The module "SDN/Open Flow Topology Management Service Analysis" is dedicated to the examination of security flaws in certain services.

In order to protect against virtual machine poisoning attacks, the "Automatic Mitigation & Defense System" was developed. "Evaluation & Performance Tests" is the last block, which evaluates the impact and efficacy of the suggested defensive mechanisms and modules on performance.

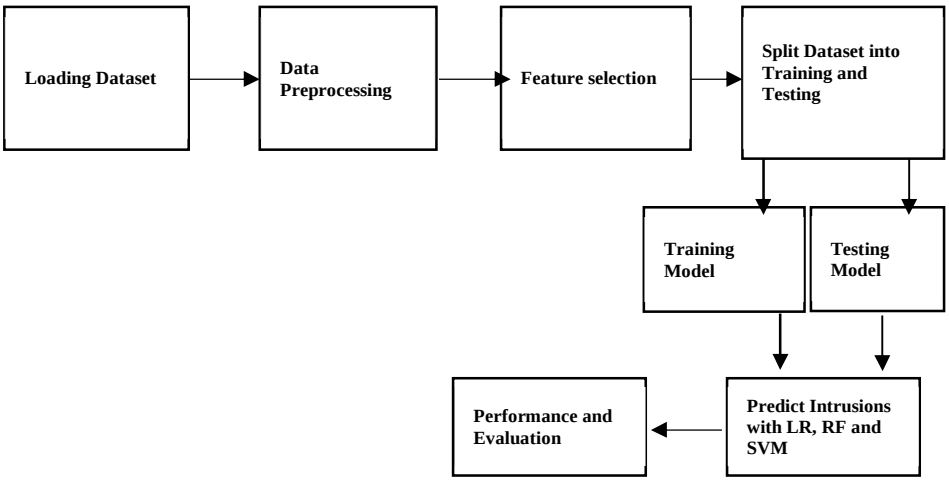

Figure 2. Block diagram of the proposed modal

E. SDN

Through the separation of the control plane from the data plane, Software-Defined Networking (SDN) introduces a more programmable and flexible method of network administration, hence revolutionizing conventional network topologies. Dynamic, centralized control over network resources is made possible by SDN's centralized control plane, which is conceptually isolated from the underlying network devices. With the help of software programs, network managers may now dynamically modify the behavior of the network, improving scalability and agility.

SDN eventually opens the door for innovation in the creation and use of cutting-edge networking services by facilitating effective resource utilization, smooth adaptation to shifting traffic patterns, and streamlined network administration. It is shown in Figure 3. This revolutionary technology creates the groundwork for the next generation of intelligent, adaptable, and responsive networks while enabling enterprises to react quickly to changing business needs.

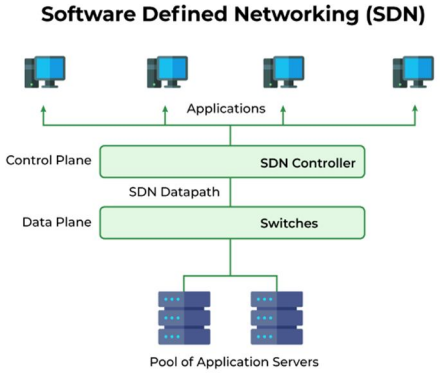

Figure 3. SDN

F. DDoS Attacks

Attacks known as Distributed Denial of Service (DDoS) pose a serious risk to networks and online services because they are designed to interfere with their regular operations. In these assaults, a number of hacked computers work together to create a botnet, or network of devices, that is designed to overload a target system with traffic and prevent normal users from accessing it. The main goal is to deplete the target's resources, including network connections, computing power, and bandwidth, in order to induce a brief or extended denial of service. DDoS assaults may take many different forms, such as protocol attacks, application-layer attacks, and volumetric attacks. It is shown in Figure 4. As these attacks become more sophisticated, they represent a serious threat to the dependability of online platforms. In order to identify, mitigate, and protect against the potentially catastrophic effect on digital services and infrastructure, it is essential to implement strong security measures and proactive techniques in order to address the intricacies of DDoS attacks.

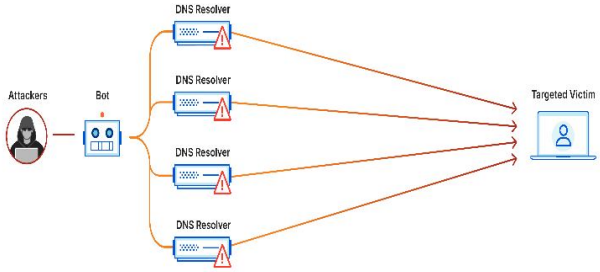

Figure 4. DDOS Attacks

G. Machine Learning

At the forefront of contemporary artificial intelligence is machine learning (ML), which is a paradigm change in the way computers learn from and make judgments based on data.

Fundamentally, machine learning (ML) uses algorithms that can identify patterns and extract insights from large datasets to enable computer systems to automatically enhance and grow their performance without explicit programming. Machine learning algorithms become skilled at making predictions, classifications, and optimizations by utilizing statistical techniques and iterative learning. This leads to advancements in a variety of fields, including natural language processing, recommendation systems, image and speech recognition, and more. By allowing systems to adapt, learn from experiences, and change in response to the dynamic problems of varied domains, from healthcare and finance to cybersecurity and beyond, machine learning (ML) is a breakthrough technology that not only boosts automation but also fosters creativity.

In this research, Muhammad Imran [1] et al. argue that Software Defined Networking (SDN) turns the switch into a dumb device by separating the controller's decision-making abilities from data transmission. Because of its essential properties, which include scalability, flexibility, and monitoring, SDNs are becoming more and more significant. SDN is susceptible to several assaults, including Denial of Service (DoS), Flooding, and Spoofing, due to its centralized management. By overloading the controller, switch, and control channel, among other components of the SDN, these assaults have the potential to reduce its overall performance. The various mitigation techniques are thoroughly reviewed in this publication, which also divides them into three groups according to how they handle malicious traffic. Furthermore, it identifies potential shortcomings in these mitigation strategies and suggest potential characteristics of an ideal defense against denial-of-service assaults. To the best of our knowledge, this study represents the first effort to categorize DoS mitigation techniques and identify their constraints in an SDN context.

In this study, Gde Dharma N [2] et al. present the Software Defined Network (SDN), a novel approach to network administration that separates the control plane from the data plane. An essential component of network management is the control plane. SDN creates the single point of failure by introducing the control plane as the network manager. The whole network will fail if the SDN controller is not available by any of the network devices. DDoS assault is one of the attack techniques that might render the SDN controller unavailable. This article presents the first phase of our study towards developing the technique for SDN controller DDoS attack detection and mitigation. In order to stop further assaults, the approach takes into account the length of time it takes to identify DDoS attacks and their temporal patterns. This article discusses how to identify and prevent DDoS attacks, as well as possible vulnerabilities in SDN controllers that may be used for such attacks. The term "software defined network," or SDN, refers to a novel approach to network administration that separates the control and data planes. The control plane is commonly termed as the controller. In SDN, the controller controls

the general behavior of the network. The network devices that function as basic packet forwarders are called data planes. Since configuration and administration are limited to the Controller, this separation has made network management simpler. It is then the controller's duty to implement the update across all networks.

In this study, Cheng-Hsu Lin [3] et al. recommended that software-defined networking (SDN) applications be built to serve different SDN network operations (traffic engineering, routing, security, etc.). The control plane's APIs are essential to its functioning. They could be hacked or maliciously constructed by outside parties. Even though several research has been conducted to combat fraudulent applications, these studies only impose coarse-grained constraints on the APIs that the apps utilize. In this study, is aim to demonstrate that existing defenses are unable to identify or block certain fraudulent flow entries. They might make it more difficult for control-plane services to function or for packets to be properly routed in the data plane. The proposed system is designed to handle two attacks, topology spoofing and forwarding based DoS, and study their underlying causes and damage to demonstrate their detrimental effects. Next, it is suggested to use an event-based, context-aware anomaly detection (CEAD) system to protect against harmful flow entries. It offers more precise control over the flow entries that applications define. In contrast to previous research, it finds anomalies by looking at the context association between an event, the app that records it, and the flow entries that the app sets for the event. The increase TCP connection attempt rates, our assessment findings demonstrate that the CEAD is scalable with little cost and can identify every fraudulent flow entry in the scenarios is provided. By separating the data plane from the control plane, software-defined networking, or SDN, allows for programmatic network management at a centralized controller.

The bulk of commercial activity in our interconnected and linked world occurs in networks built on cloud computing infrastructure that transcend national, regional, and jurisdictional barriers, as suggested by C. Tselios [4] et al. in this research. Software Defined Networking (SDN), an emerging networking paradigm that aims to greatly simplify policy enforcement and network reconfiguration in a dynamic way, makes such an efficient entity connectivity conceivable. When safety-critical applications are taken into account, this unique networking paradigm's enhanced attack surface in comparison to typical networking installations proven to be a difficult problem that inspires distrust, despite the evident benefits it offers. Additional security considerations arise, particularly when SDN is used to enable networking features associated to the Internet of Things (IoT). This is because such installations are more vulnerable to certain sorts of attacks, and any IoT application would need inter-cloud connection. Because there are so many linked nodes, effectively monitoring every entity is a true problem that has to be overcome to avoid service interruptions and system deterioration.

In this study, Jeanette Smith-Perrone [5] et al. advocated distributed denial-of-service (DDoS) attacks, pointing out that the cyber threat environment is changing more quickly than conventional IPS/IDS systems can keep up with using the use of attack signatures. Large corporate settings are increasingly vulnerable to assaults due to their scale, scope, and variability, which also reduces the availability of resources for e-commerce, cloud, hosting, and carrier platforms. An overview of the Distributed Denial of Service (DDoS) attack issue, the existing mitigation procedure, and suggested automation for accurate mitigation are presented in this work. In order to minimize 0-day assaults, describe in this article a workable method for stopping DDoS attacks without the need for human involvement. The DDoS issue that affects cloud, SDN, and big business networks is explained in this article. The cyber threat environment and distributed denial-of-service (DDoS) attacks are changing more quickly than standard IPS/IDS systems can keep up with using the use of attack signatures. Large corporate settings are increasingly vulnerable to assaults due to their scale, scope, and variability, which also reduces the availability of resources for e-commerce, cloud, hosting, and carrier platforms. An overview of the Distributed Denial of Service (DDoS) attack issue, the existing mitigation procedure, and suggested automation for accurate mitigation are presented in this work.

IV. Result Analysis

As shown in Table 1, throughput is unaffected by utilizing SDN in a moderate network; throughput is 0.086 Gbps for both conventional and standard SDN. By contrast, the SDN reduces the 98.384 μs latency in the conventional network to 71.817 μs. Likewise, SDN causes the jitter to decrease from 16.225 μs to 14.123 μs. In comparison to the old network, there was a 27% overall latency reduction and a 12.95% jitter reduction, suggesting that SDN may improve real-time traffic. The network throughput is increased from 0.086 Gbps to 0.100 Gbps by the eSDN, and it has much lower latency and jitter than the SDN. Furthermore, the congestion management method significantly reduces the number of collided packets, improving the quality of service (QoS) of the network as a whole.

TABLE I. RESULT ANALYSIS OF THE PROPOSED MODAL

Network type	Throughput (Gbps)	Delay	Jitter
Traditional	0.086	98.384	16.225
SDN	0.086	71.817	14.123
eSDN	0.1	58.92	10.86
dSDN	0.1	41.45	8.79

As shown in Figure 5, the network throughput in SDN and conventional networks is the same since light traffic has fewer devices and can be managed by the old network with the same network performance. Nevertheless, eSDN greatly increases throughput in networks with little traffic. Using dSDN resulted in a 0.16% boost in throughput. The latency and jitter are decreased greatly compared to eSDN. With dSDN, the total latency dropped from 58.92 µs to 41.45 µs, and the jitter dropped from 10.86 µs to 8.79 µs. The outcome demonstrates that by eliminating needless jitter and delays, dSDN may enhance network performance. However, since the scope is much smaller in a mild network, the improvement in network QoS is negligible.

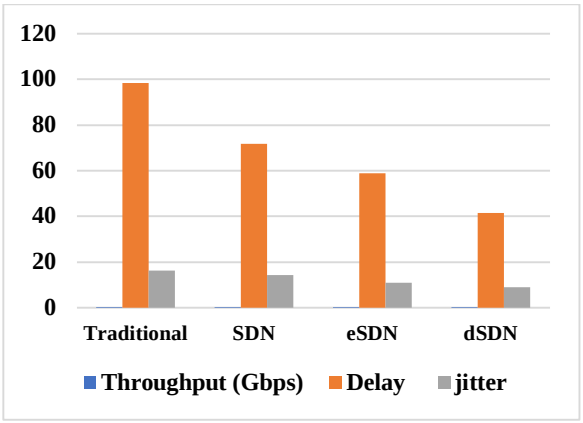

Figure 5. Comparison graph

Subsequent study in this area should concentrate on the ever-changing landscape of cybersecurity threats, which calls for constant investigation to find and fix new Software-Defined Networking (SDN) vulnerabilities. To maintain strong defense against complex attacks and accommodate new attack vectors, further research is required to expand and modify the suggested security measures. In order to improve the flexibility and autonomy of SDN security systems, research efforts might also focus on the development of machine learning algorithms for real-time threat detection and response. Retaining the efficacy and relevance of security procedures would need cooperation with industry partners and ongoing evaluation of evolving SDN technology.

V. CONCLUSION

In summary, our study has shown significant flaws in popular Software-Defined Networking (SDN) controllers, with a particular emphasis on attacks known as Virtual Machine Poisoning. The fundamental components of SDN are seriously threatened by the discovered attack vectors, which might result in major security lapses including hijacking, denial of service, and man-in-the-middle assaults. Because the Poisoning Network routing was created in such an organized way, there is less traffic growth going forward. Simplified code is used because it is more comprehensible and adaptable. By using the pollution-aware traffic allocation formulation, they assess the impact of changing network and protocol settings to track performance trends. Specifically curious in how the maximum number of routing pathways and the update relay period affect flow allocation performance. The average is taken for the simulated outcomes throughout all simulation runs to provide a single, which may be used to compare trials with varying update times or numbers of pathways. It is replicated a small-scale network similar to the one in while adjusting protocol and network settings to track performance trends and make improvements.

REFERENCES

[1] Imran, M., Durad, M. H., Khan, F. A., & Derhab, A. (2019). Toward an optimal solution against denial-of-service attacks in software defined networks. Future Generation Computer Systems, 92, 444-453.Dharma, N. G., Muthohar, M. F., Prayuda, J. A., Priagung, K., & Choi, D. (2015, August). Time-based DDoS detection and mitigation for SDN controller. In *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)* (pp. 550-553). IEEE.

[2] Lin, C. H., Li, C. Y., & Wang, K. (2018, December). Setting malicious flow entries against SDN operations: attacks and countermeasures. In *2018 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1-8). IEEE.

[3] Tselios, C., Politis, I., & Kotsopoulos, S. (2017, November). Enhancing SDN security for IoT-related deployments through blockchain. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (pp. 303-308). IEEE.

[4] Smith-perrone, J., & Sims, J. (2017, January). Securing cloud, SDN and large data network environments from emerging DDoS attacks. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 466-469). IEEE.

[5] Zhang, B., Zhang, T., & Yu, Z. (2017, December). DDoS detection and prevention based on artificial intelligence techniques. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)* (pp. 1276-1280). IEEE.

[6] Choudhury, S., & Bhowal, A. (2015, May). Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection. In *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* (pp. 89-95). IEEE.

[7] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, *12*(2), 493-501.

[8] Robinson, R. R., & Thomas, C. (2015, December). Ranking of machine learning algorithms based on the performance in classifying DDoS attacks. In *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)* (pp. 185-190). IEEE.

[9] Yang, L., & Zhao, H. (2018, October). DDoS attack identification and defense using SDN based on machine learning method. In *2018 15th international symposium on pervasive systems, algorithms and networks (I-SPAN)* (pp. 174-178). IEEE.

[10] Nazario, J. (2008). DDoS attack evolution. Network Security, 2008(7), 7-10