● Software Defined Networking and Security

Syeda Narmeen Bukhari
FAST NUCES

Islamabad
syedanarmeennaqvi47@gmail.com

Abdullah Khan
FAST NUCES

Islamabad
abdullahbaloch070@gmail.com

Waleed Mukhtar
FAST NUCES

Islamabad
waleed.mukhtar1999@gmail.com

Abstract— **The new layered networking architecture that Software Defined Networking brings with it, despite having many enhancements and more flexibility, causes some new problems as well. The aim of this paper is to explain the need for SDN, go into its difference with the traditional networking approach, and then explore the various cyber security issues that arise with SDN. After carrying out an in-depth research to some of the solutions to these security issues, the most significant issue- DDOS Attacks, and its most optimum solution is put forward, taking perhaps one more step toward the idealized secure future that SDN presents the possibility of.**

Keywords—software defined networking, cyber security, DDOS attacks, and architecture

I. Introduction

With the rapid progress made in networking and complexity of the ensuing requirements, manipulating traffic between end hosts occurring on a network is getting harder. This gave rise to software defined networking (SDN) which is a networking architecture that uses a software program for controlling the traffic between end hosts, so the traffic on a network is directed on its route by software. The whole paradigm of networking has shifted with networking devices now being programmable. Networks are now more centralized and can be monitored and controlled expeditiously, increasing the flexibility of the underlying architecture, and providing many new benefits along with some rising issues that need to be catered to [1].

II. Difference between Software Defined Networking and Current Networking Architecture

The SDN architecture differs from the current networking framework on quite a few points, what with progress demanding centralizations of architecture.

A. Traditional Approach

The traditional approach is hardware-based so traffic control is the responsibility of hardware devices; routers, switches, hubs and other network architecture. In this architecture, the paradigm is more or less distributed, with different protocols for all the networking devices, like OSPF, ARP, EIGRP and so on operating independently. Although these devices are connected at the heart, there is no central mechanism present to direct them [1].

B. Software Defined Networking Approach

SDN takes a more centralized approach with the SDN switch consisting of only the data plane and the control plane taking on a completely spate form in the shape of a remote controller which is the brain of the network. This gives more versatility to the whole operation and increased ease of control and accessibility. The SDN controller has the final say as it is the network-wide entity whose decisions all the switches in the network abide by. Ryu, Nox, OpenDayLight, and FloodLight are just some examples of SDN controllers. In the control, a northbound interface is employed for communicating the Application Programming Interfaces (API). Navigating traffic, as well as balancing traffic load therefore is easier, as it is not all mounted on to one physical entity, but is efficiently separated. Open Source framework and an architecture that is more layered, provides much of the isolation and flexibility that the traditional approach failed to facilitate [5].

III. Software defined networking and cyber security

With improvements come many new complexities as well, making progress and tracing not just forward but back on the path to security too. SDN, along with SDN-based cyber security applications are gaining a lot of significance in the fight against cybercrime.

With Software Defined Networking, collecting usage information of the network gets simpler, thereby enabling an improvement in attack detection algorithms. This also means that SDN agents are then better informed, and allows an improvement in enforcing policies and increased efficiency of detecting, and therefore blocking malicious network traffic before it gets a chance to enter any critical regions of the network and carry out any significant damage.

IV. SDN and cyber security attacks

Although separation of the layers in the architecture means enhanced security, and also ensures that since the layers are now independent, an attack on one layer, and any ensuing damage would only affect that particular layer, and all other layers would be left undamaged; but that is not to say that SDN has lesser security vulnerabilities. With addition of layers comes addition of opportunities to attack each layer, and new possibilities of subverting the network to carry out malicious intent.

SDN essentially has three layers; the infrastructure layer, the control layer, and the application layer, and there are also communication links between these layers. Attacks can be carried out at any layer and in different forms [2].

A. Attack on Application Plane

The application layer consists of networking tools, devices, and applications which employ the controller in order to communicate with the control layer. SDN applications in turn use APIs to communicate with the controller the resources that are required by each application. In SDN, the functionality of these network devices is more or less the same, but the delivery is more virtual and abstract.

The attacker can use password guessing or brute force attack to gain access to an application and then use this illegal access to carry out malicious actions across the network, eavesdrop on confidential data, cause some malfunction, or enable a denial of service attack, by requesting and gaining access to a major part of the available resources, which would mean that when a legitimate application requests a resource to be allocated to it, there would be no available resources , and the service would be denied to the application.

Furthermore, confidential data could be modified as well disrupting its integrity, and configuration issues could arise too with policy enforcement and TLS adoption not being carried out properly.

B. Attack on Control Plane

The whole network topology is defined by the control plane. In network routing, the main functionality is that of the control plane, which links the routers and exchanges protocol information of connections.

An attacker can compromise the security of the vulnerable SDN controller by firstly sending false manipulated data over the network and then at the same time issuing multiple attacks on the network. Spoofed IP addresses are used to send a large number of bogus requests, thereby causing a large number of packets to be processed at the control, and causing a DDOS attack, as a legitimate user will be delayed or denied the service they request for [3].

C. Attack on the Communication Link between Planes

Sending bogus traffic on the communication link between any two planes causes a depletion of the available link bandwidth, causing legitimate users to be denied service and creating bottlenecks delaying important issues and functionalities such as vital communication, conveying of lookup tables, and enabling of route traversal due to delay in transmission of crucial information.

D. Attack on Data Plane

The Data plane is more or less the forwarding plane, which is responsible for moving the traffic along the route. The configurations enabled by the control plane are used to determine the path of entry and exit for all the packets.

Traffic diversion is one of the main attacks at this plane, where the attacker hijacks the flow of traffic, diverting it to the attacker himself for malicious use or eavesdropping, or just redirecting the traffic to incorrect locations to disrupt the flow and exploit further vulnerabilities.

The attacker may also use some network information, like timing and how long it takes to create new connections to carry out a side plane attack, having analyzed whether there are any flow rules present or not.

Packet sniffing is also a legitimate issue here causing vulnerability to the confidentiality and integrity of data. Moreover, flow-table overflow attack may also be carried out on the data plane, as the flow table maintained at the switch may be flooded.

E. Attacks that can Affect all Planes

- **DDOS Attacks**- In such attacks, the attacker creates multiple bogus packets with spoofed IP addresses so that they appear to be valid, and get introduced into the network. These packets are then sent to the controller and new flow rules are requested. More and more fake packets keep getting created and sent over the network depleting the available bandwidth, and disrupting the normal flow of the network.
- **Packet sniffing**- This is a method in which traffic is gathered from the network and analyzed in order to gauge what malicious use it may be put to. A computer or device packet sniffer is employed and the simplified SDN software encourages such an attack. Information can be collected more easily, and the packets once intercepted and used, may be redirected to their original destinations with legitimate users left completely unaware that the data has been compromised.

V. CONSIDERED SOLUTIONS TO ATTACKS

Quite a number of solutions were considered, before settling on the optimum solution to tackle the most significant issue. The more significant of these have been explored below [1][2][3][4][7][8][10].

Year	Goals Achieved	Results/ Accuracy	Technique Employed
2019	Preventing SDN against ARP Spoofing attack	Robust, easily detects and avoids ARP attacks	MiniNet

2019	Solving Switch Migration issue for Load Balancing, Robustness and Time Computation	Load balancing increased to 14 percent	MATLAB
2020	Guarantee Secure and Consistent Network	Energy Utilization, End to end Delay, Improved Throughput	MiniNet Wifi Emulator
2020	Edge Control System	High network load handled with decreased latency	Python
2020	Classification of traffic	98.8 percent accuracy	SVC-RF

VI. MOST SIGNIFICANT ATTACK – DDOS ATTACKS

It appears after much consideration that the most vulnerable and significant form of attack is the DDOS attack as it affects all the planes at varying degrees of intensity and complexity, and its solutions are therefore the most pressing.

VII. OPTIMUM SOLUTION

An optimum machine learning algorithm is proposed as the solution to the DDOS attacks. In this solution, features are first of all logged into a CSV file, and an SDN dataset is created, on which the machine learning algorithm is then trained. A model of Support Vector Classifier with Random Forest (SVC-RF) is used to classify the traffic in to benign and malicious. This hybrid model is chosen as the optimum solution as it has the lowest false-alarm rate ratio, and has an accuracy of 98.8 percent. A few steps are involved in the enforcement of this method and these are listed below.

A. Generation of SDN Data Set Through a MiniNet Emulator

A training dataset consisting of malicious traffic is provided to the mininet emulator, which builds a SDN topology of the network.

B. Classification of Traffic in to Benign and Malicious Through Machine Learning

The ML algorithm classifies the dataset to benign and malicious traffic using SVC-RF.

C. Detection of Attack

Since the labeling of the dataset has been carried out so efficiently, and the classes of benign and malicious are so distinct, detecting attacks in the form of malicious traffic is simple enough, and once this detection occurs, the malicious traffic or packets can easily be blocked and prevented from entering critical regions of the network, thus decreasing the danger of DDOS attacks, as well as other attacks enabled through malicious traffic entry on to the network.

VIII. CONCLUSION

It may be concluded that of the few vulnerabilities that Software Defined Networking has, the most vulnerable is the SDN controller. SDN and the programmable features it provides create challenges as well as improved flexibility and the most prominent among these is the DDOS attacks, which may be appropriately tackled using a number of tools and techniques, the optimum among which is the application of SVC-RF.

ACKNOWLEDGMENT

This paper was written as part of our Information Security course at FAST NUCES, Islamabad, and assigned by our instructor Mr Abdullah Abid. Thereby, we acknowledge the equipment of our capabilities to write it through the course and the education we acquired from said institution.

References

[1] Ahuja, Singal et al. “Automated DDOS Attack Detection in Software Defined Networking”. *Journal of Network and Computer Applications*. (2021)

[2] Ayush, Rejo. “Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)”. *Third International Conference on Computing and Network Communications (CoCoNet ’19)*. (2020).

[3] Eliyan, Lubna Fayez, and Roberto Di Pietro. "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges." *Future Generation Computer Systems* 122 (2021): 149-171.

[4] Ghaffar, Zeba, et al. "A topical review on machine learning, software defined networking, internet of things applications: Research limitations and challenges." *Electronics* 10.8 (2021): 880.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[5] Haji, Saad H., et al. "Comparison of software defined networking with traditional networking." *Asian Journal of Research in Computer Science* (2021): 1-18.K. Elissa, “Title of paper if known,” unpublished.

[6] Hande, Yogita, and Akkalashmi Muddana. "A survey on intrusion detection system for software defined networks (SDN)." *Research Anthology on Artificial Intelligence Applications in Security*. IGI Global, 2021. 467-489.

[7] Jafarian, Tohid, et al. "A survey and classification of the security anomaly detection mechanisms in software defined networks." *Cluster Computing* 24.2 (2021): 1235-1253.

[8] Muthukumaran, V., et al. "Improving network security based on trust-aware routing protocols using long short-term memory-queuing segment-routing algorithms." *International Journal of Information Technology Project Management (IJITPM)* 12.4 (2021): 47-60.

[9] Sudar, K. Muthamil, et al. "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques." *2021 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2021.

[10] Wang, Yuqing, et al. "A new traffic prediction algorithm to software defined networking." *Mobile Networks and Applications* 26.2 (2021): 716-725.

[11] Yurekten, Ozgur, and Mehmet Demirci. "SDN-based cyber defense: A survey." *Future Generation Computer Systems* 115 (2021): 126-149.

****