Security Analysis of Software Defined Networking

[1]Sukhmanpreet Singh, [2]Er. Amreen Kaur

[1]Department of Computer Science and Engineering, BGIET, Sangrur, Punjab, India.

Abstract : Software Defined Networking is a network paradigm shift and is changing the network industry by revolutionizing the control plane and data plane architecture. SDN centralizes all the control plane work brining heaps of benefits as compared with traditional networks. Some challenges are also under review in this paper like SDN Security. Security is a vital part of the network and as controller is centralized in SDN, any vulnerability in the controller can results in exploitation of whole network. Security Issues like DDoS attacks on controller, malware attacks, spoofing etc. can create a havoc in the network. This paper reviews security issues of Software Defined Networking with major focus on DDoS or Malware.

Keywords – Software Defined Networking, Openflow, Control Plane, Data Plane, DDoS, Malware, Spoofing.

INTRODUCTION

SDN is the emerging networking technology which has changed almost all the sectors of networking like Enterprise, Data Center and Service Provider Networks with the plethora of advantages that it brings with its deployment. Traditional Networks technologies were in use for a long time and a Stanford University student started a project named "Clean Slate Project", with an objective that how would internet be like if we start it again from the scratch. So he redesigned the traditional network architecture by decoupling the control plane and data plane[21]. SDN got the nod from large number of network giant companies like Cisco, Juniper, Huawei, Google, Microsoft etc. SDN takes the centralization[14] approach by having a centralized controller and all other devices acting as data plane devices follows the controller instructions to get the path related information. Controller and data plane switches communicates with each other using Openflow protocol. Controller is the brain of the network, just like in traditional network technologies, routing protocols builds the control plane, controller is used to build the control plane and is the major part of the SDN architecture. Control Clustering is also used in critical networks as it saves the network if there is any problem occurred in Controller, then the primary controller can also be used. SDN Controllers can be implemented in DC as a Virtual Machine or directly on a hardware server over Linux platform. Below is the figure that shows the comparison of architecture of traditional and Software Defined Networking:

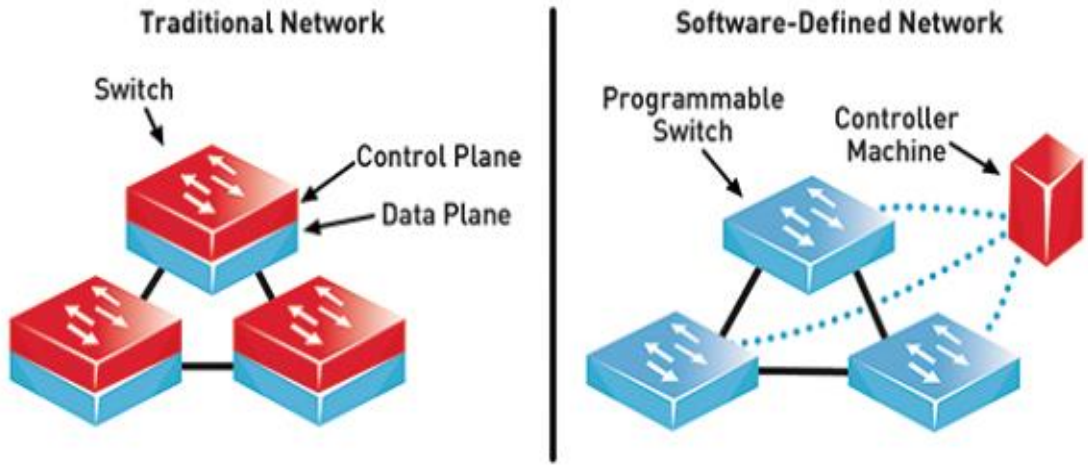

Figure 1.1 – Traditional Network vs SDN[22]

SDN ARCHITECTURE

SDN Architecture comprises of three different layers[17-19] i.e. Application, Control and Infrastructure Layer as shown in figure 1.2 below:

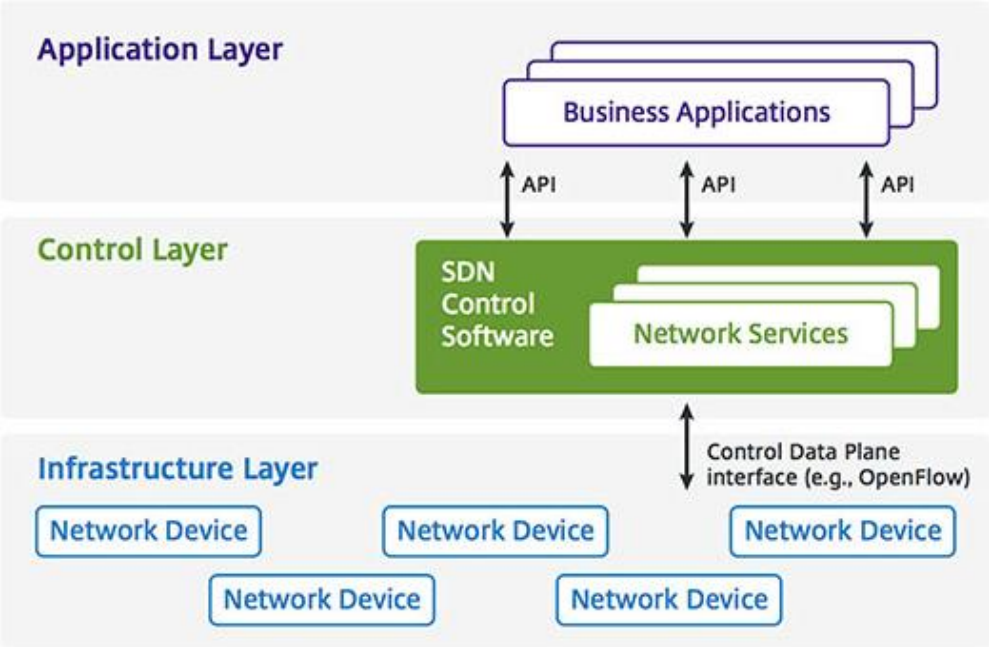

Figure 1.2 – SDN Architecture[23]

Application Layer – This layer holds the programs that communicate with the controller via Application Programming Interfaces(APIs).These applications can be of network management, analytics or they can be business related applications that runs in large scale data centers.

Control Layer – This layer is the intermediate layer of SDN Architecture. They get the instructions from Application Layer and then relays them to network components in the infrastructure layer. Controller also gets the information from the hardware devices and provide this information to the application layer.

Infrastructure Layer – This layer holds the devices that have data lane capabilities and they forwards the data as per the instructions provided to them by controller.

SDN BENEFITS

Enhancing Configuration – Configuring networks is one of the most complex and critical tasks, as a single mistake and make whole network vulnerable. In traditional networks adding a new network device like router needs configuration on that device in a tested manner, so that any changes would not affect the current network. Manual Configuration has to be performed on the new addition on devices so that they can be in working condition. With SDN, controller is the brain of the network and all the flows are controlled by the controller and it automatically reduces the configuration[6] time.

Programmable and Customizable – SDN brings the power of programming into the network where new applications and features related with network can be deployed easily. Traditional network technologies are mostly proprietary, for example, if we buy one vendor router, then it comes with a base Operating System, and in case we need to have some specific feature, then we have to buy the license for that and we do not have any customization or programmable option available on that device to add some new feature. Also, experimentation can be a big issue in traditional networks. With SDN, new features can be added[7] by using the programmable interfaces and it makes it much more flexible than using traditional networks. This is one of the reason why data center giant companies like Google and Facebook have shifted their networks to SDN from traditional networks.

Lesser Network Infrastructure Costs – Traditional networks are costly and SDN makes a very cost efficient solution for the network infrastructure industry and has reduced the network hardware and software costs by large margin. With no proprietary hardware and software needed, no control plane feature required in every device, costs have significantly reduced. Companies use single or multiple controllers in large environments and all other data plane devices are cheap in cost.

Granular Security – With large number of devices connecting with internet and cloud ,new challenges related with scalability and security have also arised in the network security industry. Controller can provide security[6] in centralized manner making security related policies easier to implement.

Better Visibility into the Network – Centralized controller means better visibility and view of the network. Finding bugs and monitoring become easy as there is no need to monitor all the devices like in traditional network, and we can get full network view from centralized controller.

Better Uptime and more reliable network – SDN and its centralization makes implementation and troubleshooting much faster than before. In traditional networks, in case of any bugs or issues, first the devices or link which creates the issues has to be found to rectify the problem and in case of a large network, it can be very difficult. But with SDN, it easy to troubleshoot the network as the only device which has to be troubleshoot is the SDN controller.

SDN CHALLENGES

Tackling Fast On-Demand Growth – Technologies like IoT, Cloud Computing, Machine Learning etc are making big changes in the industry and with that the need for network, compute resources have also increased. Tackling the growth, where billions of bytes of data is produced in data centers has to be make sure so that no performance related issues should arise.

Addressing automatic real-time changes – Network and Server automation is one of the big things happened with SDN in data center industry. APIs are used by SDN based controllers in application layer which are used to add functionality related with different services. Monitoring should be based on OpenAPIs so that any changes or updation related with SDN controllers or topology should be directly monitored and bring better visibility of the network.

Security – One of the major concerns related with SDN is the security of the controller. Protecting[3-5] controller against unauthorized access and other attacks like malware and DDOS is very important. As SDN Controller applications are mainly open source, third party applications can also be added and customized which can also become threats as there can be chances that the application added to the controller is not tested and verified and may introduce some vulnerabilities in the SDN controller and its working. Various types of attacks are explained below:

- Third party applications can be integrated with the SDN controller using its application layer and these applications are not verified and can also be malware infected which can result in malware attacks on the SDN controller.
- DDoS attacks are implemented by hacking groups in order to disrupt the application, network and service availability. This attack can be used on the controller to disrupt the controller from doing its work. Large amount of ICMP, TCP SYN, UDP, HTTP traffic bursts can be sent using the botnets which disrupts the controller services.
- Man-in-the-Middle attack is used in order to break confidentiality. Controller connects with data plane switches using Openflow protocol for the path selection process. Hackers can use the MiTM attack to steal the data over the communication channel in case strong encryption standard is not in place.
- Controller Spoofing can also be done to make the data plane switches in the network think that rogue controller is the real one.

SDN CONTROLLERS

Controller is the brain and heart of the SDN Architecture and it plays the intermediary role in connecting first and third layer of SDN model. Controller controls the whole network paths with the help of flow tables and other information shared with the data plane switches over the network. Most used and popular SDN Controllers are listed in below table:

Table 1 – SDN Controllers

Controller	Company	Open Source
POX Controller	Nicira	Yes
Beacon Controller	Stanford University	Yes
Floodlight Controller	Big Switch Networks	Yes
Floodlight-Plus Controller	Big Switch Networks	Yes
Ryu Controller	NTT Labs	Yes
OpenDaylight Controller	Linux Foundation	Yes
ONOS Controller	Linux Foundation	Yes
Open Contrail Controller	Open Contrail	Yes

DDOS

Distributed Denial of Service attack is implemented by the hackers in order to disrupt the availability of their network and application services. These attacks takes websites or servers down by bombarding large number of requests which in actual looks valid but they aren't. Most of the DDoS attacks these days are on Cloud based applications, Network Applications and websites. Hackers also used DDoS attacks in order to make target organizations focus away from some other security breach or to steal data. Companies in financial sector, ecommerce etc are susceptible to these types of attacks. Hackers launch the phishing attacks to the IT administrators of the bank and if they are successful in getting the login credentials, they launch the DDoS attack straight away so that bank become busy in dealing with the DDoS attack and hackers steal data and money via backdoor attack. Hackers also use Home routes, IoT devices, android devices with malicious apps etc can also be used to launch the attack and they become part of the botnet network. Bots are the infected devices used by cyber criminals or hackers in order to launch the attack while botnet is the network of bots used to attack the target. SDN Controllers are also susceptible to DDoS attacks

DDOS TYPES

We can perform DDoS attacks in different forms. These types are explained below:

- **Volume Based –** This attack involves gigantic amount of requests to the target. System thinks these requests of either valid or invalid. These attacks are used to choke the network bandwidth capacity. One way hacker uses for these sort of attacks are UDP amplification attack, where hackers requests for data from some third-party server and while doing this, they spoofed your target server address. Then the third party server sends the massive amount of data on the target server.
- **Application Based** – In this type of attack, hackers use vulnerabilities in the web based applications or websites which further leads to crash of web server. Hackers keep on sending application connection requests to make the database pool busy in the manner that it starts to block the legitimate requests.
- **Protocol Based** – This type of attacks are mainly on the servers or the load balancers by exploiting the method systems used for communication. In this type of attacks, packets are designed to make servers wait for response which does not exist for example with three way handshake process with TCP SYN Flood.

COMMON DDOS ATTACKS

- **SYN Flood –** TCP SYN Flood uses the TCP 3-way handshake process and it exploits the server by sending hundreds of thousands of TCP SYN messages and in response Server sends TCP-SYN-ACK messages to which Attacker do not respond with TCP ACK message making the server stuck in the waiting state resulting in shutting down the service.
- **UDP Flood –** UDP is a connectionless protocol. UDP Flood uses random ports on a machine using UDP packets. Hosts then looks for the application on that port number, but unable to find any.
- **HTTP Flood –** This message sends the HTTP GET and PUT requests on the server with an advantage that it uses lesser bandwidth than other attacks, but it has the ability to make web server to use maximum resources.
- **Ping of Death –** It attacks the servers by sending malicious pings. It is not as effective as other DDoS attacks.

DDOS TOOLS

- **LOIC –** This tool is one of the most popular and used tool for DOS[24] attacks. Anonymous, one of the largest hacking groups uses this tool for DDOS. This tool is very simple to use with its GUI Interface. LOIC can be used to attack the victim using TCP, UDP, or HTTP requests. With this tool, we just need to know either URL or IP Address of the target machine.
- **PyLoris –** This tools is used for DOS attack testing for servers. It performs DOS attack on a service. PyLoris uses SOCKS proxies along with the SSL connection in order to attack a server. Different protocols which can be targeted using PyLoris[26] are HTTP, FTP, SMTP, IMAP and Telnet.
- **Hping –** This package is a command line based TCP/IP packet analyzer. Hping3[27] is used for security testing. This package supports TCP, UDP, ICMP and IP protocol based attacks. It is a powerful DDOS attack tool with the customization is brings in testing DDOS vulnerabilities.
- **Xerxes –** This DOS tool[25] is one of the most powerful tools available freely on the internet. Xerxes is written in C language. This tool is used for HTTP based attacks.
- **GoldenEye HTTP DOS Tool –** One of the simplest tools used for DOS[24] attacks. This tool was developed in Python for testing DOS vulnerabilities. It attacks using HTTP Flood method.

MALWARE

Malwares is always a big security threat to the computing system and SDN is like no other. SDN brings customization possible in the network industry and applications can be integrated with the controller at the application layer level. Third party applications which are not verified are also used by large number of companies, which can also be vulnerable to different security threats and can be malware

infected. Various types of malware including Virus, Worms. Spywares, Trojan Horses etc. can be used by attacker to attack the controller.

SPOOFING

The attacker can spoof the controller by using the spoofing attack. If spoofing attack is conducted successfully, then the attacker can easily create new flow entries and updates the flow table. Attacker by having the full privileged access of controller have full control over the network. Once entered, attacker can steal the data, or disrupt the network functioning.

CONCLUSION

Software Defined Networking is changing the network industry by bringing programmable networks and it has opened the road for application integration with the network devices by breaking the traditional proprietary device architectures. SDN made the customization possible and network programmers can add their code to bring new functionality in the networks which was not possible with the traditional networks. SDN brings a heap of benefits to the network industry, be it data centers, service providers or enterprise networks. SDN also has some challenges, out of which, security is the biggest challenge that SDN face at the moment. Attacks like DDoS, Malware, Spoofing etc. disrupts the control plane of the network resulting in disruption of all the network services.

REFERENCES

[1] Prajakta M. Ombase, Nayana P. Kulkarni, Sudhir T. Bagade and Amrapaliv V. Mhaisgawali (2017), "Survey on DoS Attack Challenges in Software Defined Networking" International Journal of Computer Applications (0975 – 8887) Volume 173 – No.2, September 2017.

[2] Huseyin POLAT, Onur POLAT (2017), "The Effects of DoS Attacks on ODL and POX SDN Controllers" 2017, 8th International Conference on Information Technology (ICIT).

[3] Abimbola Sangodoyin, Tshiamo Sigwele, Prashant Pillai, Yim Fun Hu, Irfan Awan and Jules Disso (2018), "DoS Attack Impact Assessment on Software Defined Networks" ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018.

[4] Zhaogang Shu, Jiafu Wan, Di Li, Jiaxiang Lin, Athanasios V. Vasilakos, and Muhammad Imran. 2016. Security in Software-Defined Networking: Threats and Countermeasures. *Mob. Netw. Appl.* 21, 5 (October 2016), 764-776. DOI: http://dx.doi.org/10.1007/s11036-016-0676-x

[5] Diego Kreutz, Fernando M. V. Ramos and Paulo Verissimo(2013), "Towards Secure and Dependable Software-Defined Networks", HotSDN'13, ACM.

[6] D. Kreutz, F. Ramos, P. Verissimo, C. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey,"Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, January 2015.

[7] Alexander Gelberger, Niv Yemini, Ran Giladi," Performance Analysis of Software-Defined Networking (SDN)"IEEE,2013.

[8] XU Xiaoqiong, YU Hongfang, and YANG Kun(2017), "DDoS Attack in Software Defined Networks: A Survey", ZTE COMMUNICATIONS.

[9] Nick Feamster, Jennifer Rexford, Ellen Zegura(2015), "The Road to SDN: An Intellectual History of Programmable Networks", Princeton, USA.

[10] OpenDaylight project, *https://www.opendaylight.org*

[11]GitHub of OpenDaylight IntegrationProject,*https://github.com/opendaylight/integration.*

[12] Nicira. It's time to virtualize the network, 2012. *http://nicira.com/en/network-virtualization-platform*.

[13] NSF Guidelines for Planning and Managing the Major Research Equipment and Facilities Construction (MREFC) Account. *http://www.nsf.gov/bfa/docs/mrefcguidelines1206.pdf, Nov. 2005.*

[14] Open Networking Foundation. *https://www.opennetworking.org/*.

[15] Open vSwitch. *https://openvswitch.org*.

[16] Quagga routing software suite. https://www.quagga.net/

[17] Scott Shenker, Martin Casado, Teemu Koponen, Nick McKeown, et al. The future of networking, and the past of protocols. Open Networking Summit, 20:1-30, 2011.

[18] Open Networking Foundation. Software-defined networking: The new norm for networks. ONF White Paper, 2:2-6, 2012.

[19] Software defined networking, big switch networks.https://www.bigswitch.com/company/sdn-technology

[20] Software defined networking, microsoft. https://docs.microsoft.com/en-us/windows-server/networking/sdn/software-defined-networking

[21] Radia Perlman, Anoop Ghanwani, Donald Eastlake 3rd, Dinesh Dutt, and Silvano Gai. Routing bridges (rbridges): Base protocol specification. 2011.

[22]SDN Explained Article *https://commsbusiness.co.uk/features/software-defined-networking-sdn-explained/*

[23] MaxTech , " SDN Architecture" , *http://learning.maxtech4u.com/software-defined-networking/*

[24] Best DOS Attacks and Free DOS Attacking Tools., 2019. *https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref*.

[25] Xerxes DOS Tool., *https://github.com/zanyarjamal/xerxes*.

[26] PyLoris DOS Tool., *https://sourceforge.net/projects/pyloris/*.

[27]Hping3.,*https://tools.kali.org/information-gathering/hping3*.

[28] B. H. Lawal and A. T. Nuray, "Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)," *2018 26th Signal Processing and Communications Applications Conference (SIU)*, Izmir, 2018, pp. 1-4. doi: 10.1109/SIU.2018.8404674

[29] Bawany, Narmeen & Shamsi, Jawwad & Salah, Khaled. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arabian Journal for Science and Engineering. 42. 10.1007/s13369-017 -2414-5.

[30] Shang Gao, Zecheng Li, Yuan Yao, Bin Xiao, SongtaoGuo and YuanyuanYang(2018), "Software-Defined Firewall: Enabling Malware Traffic Detection and Programmable Security Control**",**ASIACCS'18, Incheon, Republic of Korea.

[31] ArashShaghaghi, Mohamed Ali Kaafar, RajkumarBuyya, Sanjay Jha(2018), "Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions",Cluster Computing Journal.