Grenze International Journal of Engineering and Technology, January Issue

A Review of Software Defined Network Security

Shruti Patil[1] and Ameya Naik[2]
[1-2]K.J. Somaiya School of Engineering / Department of Electronics and Telecommunications, Mumbai, India
Email: shruti.patil4@somaiya.edu, ameyanaik@somaiya.edu

***Abstract*—Software Defined Networking (SDN) provides flexible, programmable networks with automation. It provides efficient network management with controller as it separates control and forwarding logic in control and data planes. SDN offers many advantages for enhanced network administration but it suffers from security issues like topology spoofing, bandwidth exhaustion and Distributed Denial of Service (DDoS) attacks etc. There is enhancement of network security as the SDN architecture provides centralized control and programmability to networks. These same attributes pose various network security challenges also. Solutions to these problems can be controller replication schemes or use of authentication mechanisms. This paper discusses security analysis of SDN.**

***Index Terms*— SDN, network security, IDS, DDoS attacks.**

I. INTRODUCTION

Technology upgrades in ICT domains like 5G, IoT, Big Data, Cloud Computing, Network Function Virtualization (NFV) demand for dynamic management of networks with the increase in bandwidth requirement and accessibility from any corner of the world. In the traditional network architectures, the network operating system and data plane are coupled together making it inefficient to provide flexibility and automation needed by these technologies. In traditional network devices, interfaces are vender specific making the management of these devices more difficult, maintenance costly and time consuming. SDN Technology offers better solution to all these problems as it separates the control logic and the forwarding hardware in two different planes, control and data plane [1]. This paper discusses the need for SDN, SDN architecture and its components, advantages, disadvantages and security issues of SDN.

A. Software Defined Network

Networks are expanding exponentially in size, increasing complexity. Due to mobility of hosts, network virtualization, cloud computing networks are becoming more dynamic. SDN framework has a control plane which acts as a centralized SDN controller. The control plane maintains a forwarding table by exchanging the topology information and decides where to forward the incoming data packet. The switch forwards or drops the packet based on this flow entry. The data and control plane communicate through OpenFlow which is the standard protocol. SDN provides several benefits [1] like Network automation, increased reliability and security of the network, Centralized network management, Standard protocol for configuring the devices from multiple vendors.

Grenze ID: 01.GIJET.12.1.577
© Grenze Scientific Society, 2026

B. SDN Architecture

Software-Defined Networking (SDN) [2],[8] uses software-based controllers or application programming interfaces (APIs) for communicating with underlying hardware infrastructure and directing the traffic on a network.

SDN architecture as shown in figure 1 includes three layers: Application layer, Control Layer, Infrastructure layer.

- Application layer: This layer contains applications which have control programs for implementation of network control logic. The application plane and control plane interact via an open Northbound API for communicating the network requirements of application [2] to the SDN controller. Some of the examples of common SDN applications are Load balancing, Firewalls, Traffic Engineering, Routing etc.
- Control layer: This layer has SDN controller which translates the requirements of the application layer through Southbound API with the data plane. It generates flow rules for data plane devices for forwarding packets[2]. The SDN control layer also referred as the Network Operating System (NOS), provides the application layer with an abstracted view of the global network. The control plane is a logically centralized controller with a physically distributed implementation for improving reliability and increasing scalability.
- Infrastructure or Data layer: This data plane consists of a set of forwarding network devices like switches. In SDN [2], the control and data plane communicate through open Southbound Interface.

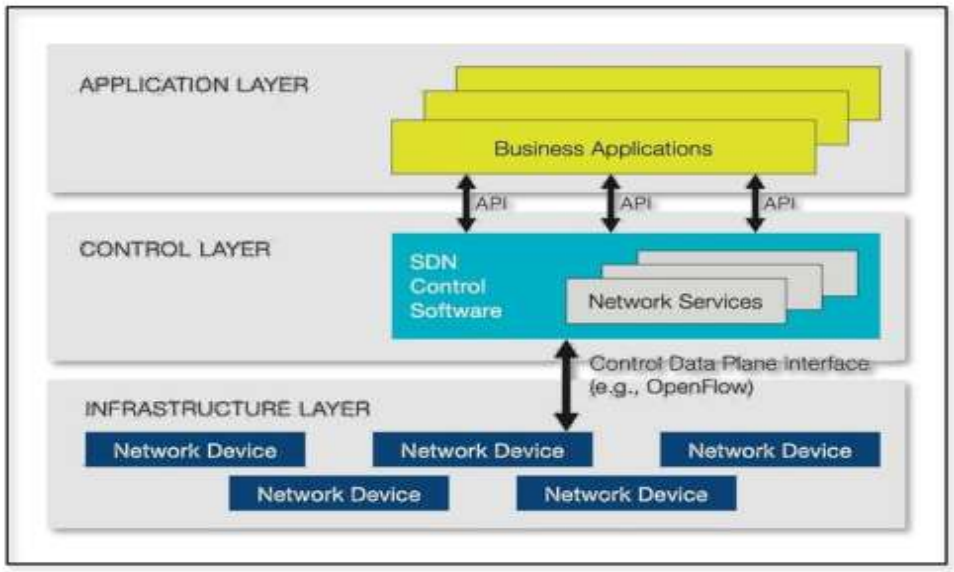

Figure 1: Basic Reference architecture for Software Defined Network [8]

C. Advantages and Disadvantages of SDN

SDN provides Network programmability in controller at control plane, abstraction of hardware giving vendor independent and cheap switches having only data plane. It provides better security. For example, if any suspicious activity in network traffic is detected by the controller then packets can be dropped or rerouted. However it can become a single point of failure for network, i.e. in case of compromised controller, the entire network gets affected. The switches in SDN lack in intelligence. They depend on control plane for decision of forwarding packets which increases the overhead of data control communication.

II. Security Analysis of SDN

In SDN, the controller monitors and maintains data generated through traffic analysis. Security policy can be updated or new policy can be generated based on this analysis. The flow rules containing this security policy can then be propagated across network. This approach [18] controls and limits the network security threats thereby enhancing the network security. These same attributes of SDN pose various network security challenges also like DoS attacks. Open programmability creates issue of trust in the network at both the interfaces. Solutions to these problems can be controller replication schemes or use of authentication mechanisms.

A. Security Enhancement Using SDN

From a security point of view, SDN can be differentiated from traditional networks on the basis of three core characteristics[18] i.e. global network view, Self-Healing Mechanisms and increased control capabilities.
SDN provides a Global Network view as it has a centralized controller which maintains traffic analysis data. This helps to detect malicious traffic and create an Intrusion Detection System(IDS) for entire network. If a routing device is dropping all or some of the packets, thus creating a black hole, then such a device can be identified easily as compared to traditional networks. Forensic analysis can be performed by tracing the logged traffic for the development of defence mechanisms against such attacks. Another important characteristic of SDN is Self-Healing Mechanisms. The control plane installs conditional flow rules in the switches which decide forwarding strategy or response of the switch when certain conditions are met. These reactions help in providing automated resiliency against attacks. The centralized controller provides more control capabilities to SDN networks [19].

B. Security challenges with SDN

SDN provides network programmability, logically centralized control and feasibility. These advantages of SDN framework help in enhancing security of networks. At the same time they may also lead to security vulnerabilities. This section categorises them as per which plane they affect [19] i. e. forwarding plane, control plane or the links connecting the two planes.

Forwarding Plane Attacks

With the limited storage the switches cannot store all the rules which are produced by the controller. SDN implementation has adopted reactive caching mechanism where whenever an incoming packet does not find a matching rule, the switch temporarily buffers the packet and sends a query to the controller for missing rule. The controller responds with new rule which gets cached in the forwarding table of the switch and packet is processed accordingly. This functionality is used by a malicious user for flooding the switch with large payload packets with different flows. As a consequence, the switch may buffer some of those large packets and large number of queries may be sent to the control plane asking for rules to process these packets. The buffer can get full and switch may keep waiting for control response causing legitimate packets to be dropped. Thus the switch becomes vulnerable to a DoS attack [19]. This flow based scheme does not specify processing of encrypted packets as it hides some of the packet's header fields from the network switches. Malicious users can skip their network border and bypass access control policy of the network by using tunnel bypassing and encryption of packets [19].

Control Plane Attacks

The SDN centralized control plane is susceptible to Distributed Denial of Service (DDoS) attacks. Flooding of network switches by many compromised hosts with packets may generate many queries to the controller ad utilize the controller's processing power. This causes the queries from legitimate hosts to be dropped or delayed [19]. In Compromised Controller Attacks, when the attacker gains access to the controller, it can control all the switches, program them to drop all incoming traffic, or use them as a platform to launch serious attacks against other targets, such as directing all received packets to a victim so as to deplete its resources [19].

Control Data Link Attacks

The link connecting the control and data planes becomes susceptible to a man-in-the-middle attack when packets sent are not encrypted. Even if they are encrypted to prevent replay attacks, the encrypted messages should include a timestamp [19].

C. DDoS attacks in SDN

As discussed flooding based DDoS attacks can be launched at all the layers i.e. switch, controller and data to control link. The attacker floods the victim with large number of false packets exhausting its system resources like bandwidth, memory, CPU. As a result they are not available for legitimate users and their requests cannot be handled [20]. Due to reactive caching mechanism, the throughput of the switch gets reduced as the switch gets overloaded and flow table gets overflow. The flow rule requests sent to the controller require lot of bandwidth causing channel congestion for normal flow requests [20]. They consume controller's resources causing Controller Resource Saturation. Legitimate requests may be dropped causing a single point of failure in the entire SDN[20].
The literature survey shows many Attack Detection Methods for SDN. One of the simplest methods is to determine a threshold and when the number of the messages exceed this threshold identify it as a flooding based

DDoS attack. According to the detection algorithm used, detection methods can be classified into machine learning based, the entropy based and the graphic based[20].

TABLE I. SUMMARY OF DDOS ATTACKS

Type	Reason	Resources Affected/Required	Detection Methods	Mitigation Techniques
Switch Overload & Flow Table Overflow	Reactive Caching	Throughput	1. Machine Learning based 2. Entropy Based 3. Graphic Based	4. Proactive Caching 5. IP filtering 6. Rate Limiting 7. Setting Timeout values for flow rules 8. Queue Management Methods with flow prioritisation 9. Controller Replication 10. Encryption and Time stamp Inclusion
Data to Control Channel Congestion	Flooding Flow Requests	High Bandwidth and Large buffer required		
Controller Resource Saturation	Flooding Flow Requests	CPU, Memory, Network Bandwidth		

ML based detection techniques for DDoS attacks has gain much attention in the research groups. To detect DDoS attack, the ML uses algorithms that can be trained with normal and attack patterns. The entropy based detection mechanism calculates entropy by measuring the random change of the incoming flows during a given time period. The graphic model based detection methods use a graphic model which is based on an attack detection method and deals with a dataset shift problem. Relational graphs are saved for known traffic patterns. For new traffic generated, the graphs are compared to determine malicious traffic [20].

After the detection of DDoS attack, an effective defence mechanism is required for timely restoration of the network function. Various defence mechanisms and mitigation techniques can be used as discussed in table I. The IP filtering technique suggests use of Rate Limiting for preventing the attack on bandwidth of the control layer. Another strategy is to prevent the switch's flow table overflow at the data plane by setting timeout values for flow rules [22].

For Controller Resource Saturation, queue management methods with flow prioritizing algorithm is used for enhancing the Quality of Service (QoS) of legitimate users. For Switch DoS attack due to reactive caching, proactive caching is used. The switches cache maximum number of rules which can fit in the table beforehand only. To process buffered packets quickly, a low delay is desired on the links connecting switches and control plane which makes this attack harder to take place. To address Packet encryption and tunnel bypassing, models can be constructed which analyse traffic statistics and identify the type of payload of the encrypted packets. Controller replication (logical centralization) Encryption and time stamp inclusion are some of the other strategies.

DDoS attack system is classified as per planes affected, SDN environment vulnerabilities, Attack strength, Attack goals. Table II summarises various phases of DDoS attack as recruit, exploit, infect or use, categorises launching methods as per technique, tools and protocol level used and resource affected. Table III describes DDoS Attack system. Various SDN architectural components such as controller, planes various interfaces which can be attacked are listed. It categorizes various detection mechanisms as statistical methods, Signature based or Anomaly based mechanisms. Various Mitigation mechanisms are classified based on location of detection engine. SDN sandbox comprising of various tools , controllers and switches, used for simulation and different architectures of SDN based on type of controller are listed.

TABLE II. SUMMARY OF LAUNCHING DDOS ATTACK

Summary of Launching DDoS Attack			
Four Phases	Launching Method	Category	Affects
1.Recruit-Scan for security holes	1.User friendly Tools Low Orbit Ion Cannon(LOIC), hping3, Stacheldraht	1.Transport / Network level attacks- Use ICMP, UDP, TCP, DNS protocol packets	Buffer Overflow, Congestion, Bandwidth, Server Resources- CPU, Memory
2.Exploit- Break into vulnerable machines exploiting loopholes	2.Employment Techniques- i.IPSpoofing, ii.Flooding- Direct, Reflection, iii.TCP SYN Flood, UDP Flood, ICMP Flood, HTTP Flood	2.Application level attacks- Use flooding	
3.Infect- Infect these machines with attack code			
4.Use- Compromised machines used to lauch attack			

TABLE III. SUMMARY OF DDOS ATTACK SYSTEM

SDN components	DDos attack Defense Mechanism		SDN Sandbox			SDN Architecture
	Detection Mechanism	Mitigation Mechanism	Tools	Controller	Switches	
Controller	Statistical Methods	Based on Location of Detection Engine	Mininet	POX	Hardware switches-Openflow, CISCO	Centralized (Single Controller)
Switches	Information Theory	Source based-Attacking Host	NS3	Ryu	Software Switches-OpenVswitch (ovs), BMv2	Distributed (MultiController)
Northbound Interface	Entropy	Destination based-Victim Host	OpenNet	OpenDaylight		Hybrid (Distributed Controller)
Southbound Interface	Cluster Analysis	Network based-Network intermediate hosts(Switch/ Router		FloodLight		
EastWest Interface	Covariance Analysis	Rate Limiting				
Network Operating System	Signature based- Use Network Behavior	Filtering				
Planes	Anomaly based-Use ML, DL Techniques	TCP Proxies				
Application						
Control						
Data						
Communication Channel		Controller plane Bandwidth				
Hosts						

III. CONCLUSIONS

Security of the network is a challenge and essential for any organisation irrespective of its size. SDN enhances security policy and detection of attacks through the unified control plane. A survey of SDN and its security is provided here. The literature survey examines the transition of SDN along with applications and challenges. This paper discusses security attacks at all 3 layers of SDN and how different mitigation strategies can be used to enhance the performance of SDN in various applications.

REFERENCES

[1] Sukhveer Kaur, Krishan Kumar, Naveen Aggarwal, ”A review on P4-Programmable data planes: Architecture, research efforts, and future directions”, Elsevier, Computer Communications, Volume 170, 15 March 2021, Pages 109-129, https://doi.org/10.1016/j.comcom.2021.01.027.

[2] Fetia Bannour, Sami Souihi, Abdelhamid Mellouk, “Distributed SDN Control: Survey, Taxonomy and Challenges”, Article in IEEE Communications Surveys & Tutorials ,December 2017, DOI: 10.1109/COMST.2017.2782482,, pp. 1-26.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Chenqing Tsai, Kai Song,“Discussion on Network Security under SDN Architecture”,2023 26th ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter) | 979-8-3503-4586-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SNPD-WINTER57765.2023.10223982,pp.53-57.

[4] M. Rahouti et al.,“SDN Security Review: Threat Taxonomy, Implications, and Open Challenges”, IEEE ACCESS, VOLUME 10, 2022, DOI: 10.1109/ACCESS.2022.3168972, pp. 45820-45854.

[5] Behrooz Daneshmand, Tu Anh Le,“Software-Defined Networking: A New Approach to Fifth Generation Networks – Security Issues and Challenges Ahead”,2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN) | 978-1-6654-8550-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICUFN55119.2022.9829621,pp. 307-313.

[6] Najmun Nisa , Adnan Shahid Khan , Zeeshan Ahmad , Sehrish Aqeel ,”Conceptual Review of DoS Attacks in Software Defined Networks”, 2022 Applied Informatics International Conference (AiIC) | 978-1-7281-8428-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/AiIC54368.2022.9914598, pp.154-158.

[7] Diego Kreutz, Fernando M. V. Ramos, Paulo Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig, “Software-Defined Networking:A Comprehensive Survey”, Proceedings of the IEEE • June, DOI: 10.1109/JPROC.2014.2371999 • Source: arXiv

[8] SDxCentral. (2021, March 19). What the definition of software defined networking. https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/
[9] Bhargavi Goswami, Manasa Kulkarni, And Joy Paulose, “A Survey on P4 Challenges in Software Defined Networks: P4 Programming”, IEEE ACCESS ,22 May 2023 , VOLUME 11, 2023, DOI:10.1109/ACCESS.2023.3275756, pp-54373-54387.
[10] Ya Gao and Zhenling Wang, “A Review of P4 Programmable Data Planes for Network Security”, Hindawi, Mobile Information Systems, Volume 2021, Article ID 1257046, 24 pages, https://doi.org/10.1155/2021/1257046, pp-1-24.
[11] Michael Menth, Habib Mostafaei, Daniel Merling and Marco Häberle, “Implementation and Evaluation of Activity-Based Congestion Management Using P4 (P4-ABC)”, MDPI, Journal of Future Internet 2019, 11, 159; doi:10.3390/fi11070159, pp-1-12.
[12] Frederik Hausera, Marco Häberlea, Daniel Merlinga, Steffen Lindnera, Vladimir Gurevichb, Florian Zeigerc, Reinhard Frankc, Michael Mentha, “A Survey on Data Plane Programming with P4: Fundamentals, Advances, and Applied Research”, JNCA arXiv:2101.10632v3 [cs.NI] 4 Aug 2021, pp-1-141.
[13] Athanasios Liatifis, Panagiotis Sarigiannidis, Vasileios Argyriou, Thomas Lagkas, “Advancing SDN from OpenFlow to P4: A Survey”, ACM Computing Surveys, Vol. 55, No. 9, Article 186, January 2023, https://doi.org/10.1145/3556973,pp-186:1-186:37 .
[14] Yanling Zhao, Ye Li, Xinchang Zhang, Guanggang Geng, Wei Zhang ,Yanjie Sun, “A Survey of Networking Applications Applying the Software Defined Networking Concept Based on Machine Learning”, Volume 7, 2019, Pages 95397 – 95417, Electronic ISSN: 2169-3536, IEEE, DOI: 10.1109/ACCESS.2019.2928564.
[15] Babu R. Dawadi , Danda B. Rawat , Shashidhar R. Joshi , Pietro Manzoni, “Intelligent Approach to Network Device Migration Planning towards Software-Defined IPv6 Networks”, Sensors, MDPI, 2021 Dec 26. DOI: 10.3390/s22010143.
[16] Jie Lu , Zhen Zhang, Tao Hu , Peng Yi, And Julong Lan,” A Survey of Controller Placement Problem in Software-Defined Networking”, Volume 7, 2019, Pages: 24290 – 24307, EISSN: 2169-3536, IEEE, DOI: 10.1109/ACCESS.2019.2893283.
[17] María B. Jimenez, David Fernandez, Jorge Eduardo Rivadeneira, Luis Bellido , And Andres Cardenas , “A Survey of the Main Security Issues and Solutions for the SDN Architecture”, IEEE ACCESS,VOLUME 9, 2021, DOI-10.1109/ACCESS.2021.3109564, pp.122016-122038.
[18] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. “SDN Security: A Survey”. In 2013 IEEE SDN for Future Networks and Services (SDN4FNS) (pp. 1-7). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/SDN4FNS.2013.6702553
[19] Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. “Software-Defined Networking Security: Pros and Cons.”,(2015). IEEE Communications Magazine, 53(6), 73-79, doi:10.1109/MCOM.2015.7120048
[20] XU Xiaoqiong, YU Hongfang, and YANG Kun, “DDoS Attack in Software Defined Networks: A Survey”, ZTE COMMUNICATIONS , August 2017 Vol.15 No. 3, published online September 12, 2017, DOI:10.3969/j.issn.1673□5188.2017.03.003, http://kns.cnki.net/kcms/detail/34.1294.TN.20170912.1054.002.html,
[21] Trupti Lotlikar and Deven Shah, ” A Software Approach for Mitigation of DoS Attacks on SDN’s (Software-Defined Networks)”, Springer Nature Singapore Pte Ltd. 2019, Soft Computing in Data Analytics, Advances in Intelligent Systems and Computing 758,https://doi.org/10.1007/978-981-13-0514-6_33
[22] Prof. Trupti Lotlikar, Dr. Deven shah, “Defense Mechanism for DoS Attacks in SDN (Software Defined Network)”, 2019 International Conference on Nascent Technologies in Engineering (ICNTE 2019) 978-1-5386-9166-3/19/$31.00 ©2019 IEEE
[23] Trupti Lotlikar, Deven Shah, “A Survey of Potential Security Threats and Counter-Measures in SDN: An IoT Enabling Technology”,IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 67-74 , www.iosrjournals.org International conference on computing and virtualization (ICCCV-17) 72 | Page Thakur college of Engineering and Technology.
[24] M. Conti, A. Gangwal and M. S. Gaur, "A comprehensive and effective mechanism for DDoS detection in SDN," 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, Italy, 2017, pp. 1-8, doi: 10.1109/WiMOB.2017.8115796
[25] R. Kandoi and M. Antikainen, "Denial-of-service attacks in OpenFlow SDN networks," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 2015, pp. 1322-1326, doi: 10.1109/INM.2015.7140489.
[26] Y. Xu and Y. Liu, "DDoS attack detection under SDN context," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 2016, pp. 1-9, doi: 10.1109/INFOCOM.2016.7524500
[27] Ali T.E. Chong, Y.-W., Manickam, S., “Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. “ ,Appl. Sci. 2023, 13, 3183. https://doi.org/10.3390/app13053183
[28] Alrashede, Hamad & Eassa, Fathy & Marish, Abdullah, “Security of East-West Interface of SDN: A Review of Challenges, Solutions, and Future Directions”, June 2025 Engineering, Technology & Applied Science Research. 15. pp. 23376-23385, DOI:10.48084/etasr.10988.