Attack on SDN Infrastructure and Security Measures

Hisham Al-Saghier *
Department of Information Technology,College of Computer & Information Sciences,
Majmaah University, Majmaah-11952, Saudi Arabia, h.alsaghier@mu.edu.sa

Abstract
Software Defined Networking (SDN) decouples the network control and network forwarding elements. The centralized controller manages the network and controls the data flow in the network elements. It has received significant attention from industry and researchers, and it has been deploying in different scenarios and environments. A centralized network plane supports programmable network management and flexibility. However, it introduces a single point of failure and scalability issues. SDN security has become a concern and many security challenges are introduced. The control plane still suffers from the number of threats such as a distributed denial of service (DDoS), man in the middle (MITM), and information modification attacks. To address these limitations, we propose a robust, secure, collaborative agent-based SDN infrastructure to detect and mitigate the attacks. We simulate and evaluate the performance of the proposed system when SDN control plan is compromised at build and run time. Simulation results show that security solutions are effective to mitigate the attacks.

Keywords:
Software Defined Networking(SDN);SDN Security; Distributed Denial of Service (DDoS) Attacks

1. Introduction

SDN network devices are divided into two layer's control plane and data plane [1]. While the data plane is just a fast packet processing layer the control plane deals with various routing protocols and maintains forwarding states [2]. So the control plan has become very complicated and it has led networks to be unstable and difficult to manage. And also these devices are closed and proprietary and it has been a barrier to innovation.

In traditional Networks Control plane is implemented with complicated software and ASIC, it was unstable and increased complexity in management. The platform is closed means vendor-specific and it was hard to modify, hard to add new functionalities, so software defined networking (SDN) comes into existence with separate control plane from the data plane. Advantage of SDN over Traditional Network, SDN provides solutions to current network infrastructure issues such as scalability, reliability, and security [3].

In SDN, the control plane is decoupled from the network devices and the controller manages the entire network in a centralized manner [4]. A centralized network plane supports programmable network management and flexibility. In this way the controllers can easily provide and maintain the global network view and controllers implement northbound API [5]. SDN is a Programmable network i.e. it provides fixed and dynamic network control [6].

However, it introduces a single point of failure and scalability issues. Researchers proposed multiple SDN controllers' architectures to address the challenges with a single point of failure [18].

The Control plane remains the main component in the networks, and attacking the control will compromise the entire network. The control plane still suffers from several threats such as a denial of service (DoS), man in the middle (MITM), and information modification attacks.

Another advantage of SDN is that it is possible to build a network with commodity servers and switches so the cost can be significantly reduced. A lot of challenges arise in SDN due to SDN application and controller have complete control of the network; controller and SDN Applications are built on the general-purpose computing platform. If the controller or application is compromised the whole network is compromised. So it is very hard to prevent all attacks. Many researchers have investigated the attack and vulnerabilities in SDN [7-9] suggested countermeasures [10-12] with different aims. Also, researchers have investigated the detection of network anomalies using the machine learning approach [13-14].

In this paper, attacks are characterized as misconfiguration, malware and insider attack. Detection and countermeasures are the main theme of this paper and proposing an agent-based security framework to collect network traffic from the forwarding plane, apply classification algorithms to detect network anomalies.

This paper is organized as follows. Section 1 includes the introduction, purpose, and significance of this research. Section 2 discussed the related work-study in the domain of SDN Security, Section 3 discussed current SDN infrastructure & security issues, Section 4 discussed the proposed framework, Section 5 discussed the implementation, identification of vulnerabilities, testing method, analysis of computed results, and countermeasures for vulnerabilities. Finally, the main findings and results discussed in the conclusion.

2. Related Work

This section highlights the work done in the domain of SDN security, we classify the relevant research work as SDN overview, security issues & challenges, threats, attack, performance issues of current SDN controllers and countermeasure.

In [1], the authors have discussed SDN network architecture, network services, security and privacy, operating systems security including distributed control plane and SDN security. Reference [5] proposed a distributed controller's architecture for SDN to address scalability and reliability. Relationship between SDN (programmable network) and network virtualization discussed in [6]. In [15] authors proposed a hybrid hierarchical control plane to improve the scalability of an SDN based large-scale networks and fast rerouting algorithm. In [16] authors proposed multiple-controller architecture based on a distributed rule store. In the distributed rule, the application layer calculated the flow rules and distributed it to multiple controllers to resolves the security and performance issues.

Classification of SDN hypervisors and proposed framework for SDN hypervisors are discussed in [17]. In SDN challenges are network's scalability, reliability, and availability, to resolve the issues authors in [18] proposed multiple controller architectures. In [19] authors discuss SDN issues and challenges and proposed mitigation techniques to address security, reliability, scalability, availability, resiliency, and performance. Reference [20] proposed Control path management framework for multi-lateral SDN network to address reliability, control path reliability algorithms also enhance the system performance. In [21] authors discussed software defined networking architecture, challenges, security attacks, countermeasures, and research trends.

In [22], [23] authors proposed Integrated Network Functions Virtualization (NFV) and SDN architectures, NFV virtualize the network and deploy into hardware, while SDN makes networks programmable, to address reliability, performance, and scalability problems. In [24] authors proposed a cross-domain SDN architecture that supports dynamically provision of various applications and services like configuration management and decision

making to address challenges and open issues of SDN based network. In [25] authors proposed and implemented a machine learning (ML) based (DDoS) attack detection system, with very well more than ninety percent detection accuracy with a low false-positive rate.

Evolution of SDN and security attacks on SDN i.e. spoofing, tampering, repudiation, information disclosure, denial of service, as well as controls/countermeasures i.e. firewalls, IDS/IPS, access control, auditing, and policy management are discussed in [26]. Security development lifecycle to address threats, risks, and vulnerabilities are discussed in [27]. In [28] authors discussed challenges due to attacks in SDN and proposed a holistic security architecture approach. Reference [29] proposed a programmable data plane to address the configuration attack. In [30] authors proposed Data-Plane extensions to secure the switches and router against Configuration attack. Address resolution protocol poisoning attack i.e. man in the middle attack (MITM) attacks are discussed in [31] and suggested a technique from the ARP Poisoning attack to protect data center networks on SDN. In [32] Due to IoT, cyber-resilient SDN based smart grid is needed, the possible security attacks on the network such as IP spoofing and (DDoS) attacks are discussed and proposed framework to assess security risks.

Distributed Denial of Service (DDoS) attacks or misconfiguration attacks in SDN infrastructure are discussed in [33-35]. Distributed denial-of-service (DDoS) attacks, detection, and protection mechanism in large scale Network are discussed in [33] DNS amplification attack under the threat of Denial of Service affect the DNS server discussed in [34]. DDoS flooding attack problems and countermeasures are discussed in [35]. Defense mechanisms against DDoS Attacks in SDN are discussed in [36]. In [3] authors discuss the advantage of SDN over the traditional network. SDN vulnerabilities caused (DDoS) attack, proposed Advanced Support Vector Machine (ASVM) algorithm to detect DDoS attacks.

Malware attacks, detection and countermeasures on SDN Infrastructure are discussed in [7-11], [14], [37-46]. In [37] authors discussed Open issues in SDN security and proposed security framework for empirical evaluation of classifier security based on attack pattern. In [10] authors discussed possible solutions against DDoS attacks in SDN. Reference [38], [39] discussed how ML help in malware detection and suggested some countermeasures. In [40] authors discussed and implemented Malware hybrid detection using the static and dynamic approach. In [14] authors proposed a method using a machine learning approach to detect unknown malware from executable files based on micro-patterns. In [41] authors proposed ML behavior-based malware detection model. Reference [42], [43] proposed a linear, central and mesh-based approach to mitigate the DDoS attacks in real-time large SDN based Networks. In [9] authors proposed a framework to detect and mitigate Application-specific DDoS attacks. In [44] authors proposed a secure autonomous response network (SARNET) based on SDN and NFV.

In [8] authors proposed a flow-table sharing approach to protect the SDN-based cloud from flow table overloading DDoS attacks by using idle flow-table of other Open Flow. In [11] authors proposed a framework to countermeasure table-miss striking attacks that degrade the performance of the controller.

In [45] authors proposed a secure framework against DDoS attacks to secure application servers as well as other network resources. In [46] authors discussed issues in SDN security, present a comparison of IDS approaches based on machine learning and deep learning approach. Reference [7] discussed DDoS attacks and DDoS detection algorithm to find the attack path using minimum network resources and in minimum time. In [47], [48] au-

thors discussed security threats including masquerading and encrypted attack.

3.SDN & Security Issues

SDN architecture is shown below in Fig. 1. It separates control and data planes to optimize the network workload which provides high speed and intelligence of using the network resources. Also, the control plane provides practical and easy network management via network services. The control plane consists of a controller with Northbound and East/Westbound API. Northbound API enables applications to communicate with the control layer. East/westbound interfaces also allow multiple controllers to interact in distributed SDN [6], [49-50].

SDN controllers i.e. Network operating system (NOS) are external logical entities that enable the network operator to program and manage the forwarding devices based on a logically centralized network view. SDN control plane manages the data plane elements by translating the application layer policies to the underlying data plane devices and provide the network information about the network to the management plane. The basic design of the control plane is using one controller to manage the whole network. However, in the case of large scale networks, multiple controllers are used. Data plane (infrastructure layer), comprises of connected network devices that forward the network data flows based on the assigned flow rules.

The control plane implements these rules through the southbound. The southbound interface allows the control plane to communicate and control the forwarding devices. Open Flow is the main SDN protocol that is used for communication between the data plane and the controller through a secure channel that is usually a TLS/SSL. A centralized network plane supports programmable network management and flexibility. However, it introduces a single point of failure and scalability issues. Fig. 1 shows the SDN threats are attacks on data-control and control-application interfaces, attacks, and vulnerabilities in controllers and application layers.

Fig. 1. Software Defined Networking Architecture

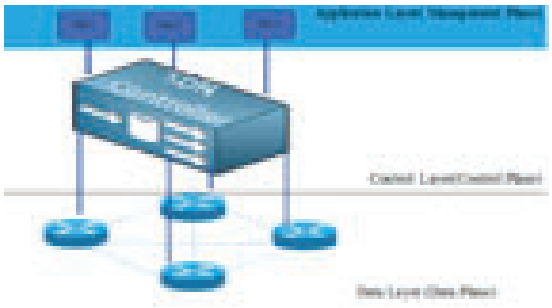


Table 1. Summary of the Literature Review

Reference-Work	SDN Overview	Security, Challenges and performance issues of current SDN controllers	Threats & Attack vulnerabilities	Security Framework	Countermeasures & Solution	Remarks: Work/Strength
[1]	✓	✓				Abstractions for software-defined networks in terms of Network services, Security and privacy
[5]	✓	✓				Proposed switch migration protocol for load balancing with the OpenFlow standard.
[6]	✓	✓				How SDN Evolve, trace the history of programmable networks
[7-11],[14]			✓	✓	✓	Detection of DDoS attacks(Malware)
[15]	✓	✓				Proposed Control plane named Orion, reduce the computational complexity of an SDN control plane
[16]	✓	✓		✓	✓	Proposed Controller performance is better than ONOS and Floodlight
[17]	✓	✓				Propose the outline for the development of a performance

						evaluation framework for SDN hypervisors.
[18]	✓	✓				Multiple controller architectures design, communication process and performance results.
[19]	✓	✓				SDN related issues and Challenges: protocol and architecture perspectives
[20]	✓	✓				Proposed and develop a control path management framework to address Reliability issues
[21]	✓	✓	✓		✓	SDN architecture, security issues, attacks and countermeasures
[22]	✓	✓	✓	✓	✓	Proposed Integrated NFV/SDN architectures
[25]		✓	✓	✓	✓	ML-based (DDoS) attack detection system, Implemented in a virtual SDN environment
[26]		✓	✓			Survey on SDN security
[28]		✓	✓	✓		Security architecture for SDN.

[29]		✓	✓	✓	✓	Proposed Programmable data plane (PD) Concept
[30]		✓	✓	✓	✓	SDN-based data plane architecture called DPX that supports security services.
[31]		✓	✓	✓	✓	Suggesting a technique to protect the data center networks from the ARP Poisoning attack using SDN
[32],[33],[34]		✓	✓	✓	✓	A framework to assess security risks within an SDN-enabled smart grid communication
[35],[36]			✓	✓		Identification and counter measure of Misconfiguration Attacks on SDN Infrastructure
[37],[38],[39] [40] ,[41], [42] ,[44], [45]			✓	✓	✓	Identification and countermeasure Malware Attack on SDN Infrastructure
[47],[48]			✓	✓	✓	Identification and countermeasure of an insider attack on SDN Infrastructure

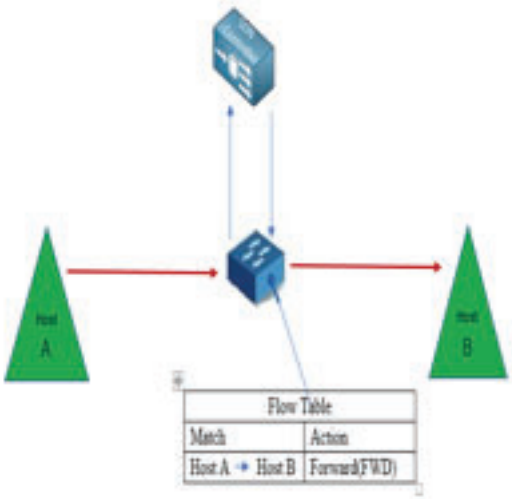
An attacker can exploit the weakness of the TLS/SSL communication channel between the SDN devices and the controller to launch attacks. Malicious SDN controllers and applications can be used to compromise the network. Other threats are forged traffic from data devices, malicious switches, vulnerabilities of administration station. Even though these threats are not specific to SDN networks, the impact on the SDN networks is more severe than traditional networks.

An attacker can use fake traffic to launch DoS/DDoS attacks on SDN switches and controllers. Also, an attacker can exploit switches vulnerabilities and then launch serious attacks against the network entities such as dropping or slow down network data flows and overloading controllers with request packets.

3.1 SDN Operation

Fig. 2 shows network topology with one SDN switch and two network hosts A and B. The switch is connected to an SDN controller.

Fig. 2. Basic SDN Operation



If in this network host A wants to try to talk to host B the switch doesn't know what to do with the packet received from host A, because it doesn't have its controlled plane anymore, so it queries a controller and the controller instructs the switch to forward all the packets from host A to host B by installing this flow Rule. So once this flow rule is installed host A can talk to host B. Some attack factors that could affect SDN infrastructure and particularly on data centers.

Modern data centers deal with a lot of virtual machines. The East-West traffic that travels within the data center has become dominant [51], [52] as shown in Fig. 3. The data centers have recently started employing this leaf-spine design that reduces the latency and the possible bottlenecks caused by the switch with traffic. But even with this new design, there remain other challenges to be solved. So that data center should be able to deal with frequent migrations and also a large number of links. And it is still expensive to scale and maintain the data centers. So this software defined data center(SDDC) is rapidly gaining attention as it can solve the challenges.

The SDDC can reduce the complexity by leveraging the global network view and network program ability offered by SDN and it is also possible to reduce the capital expenditure by building and scaling the data center with commodities servers and switches and also it is possible to readjust the operational costs by centralizing and automating a lot of management tasks.

The control plane is also scalable because it is always possible to spawn more virtual machines to host more controller nodes if needed. The complexity of the network is low, with a global network view, low cost, centralized and automated management, highly available and scalable control plan, distributed SDN controller, VMs to host the controller Nodes.

4. Proposed Frame Work: SDN Security Evaluation

The purpose of the proposed framework shown below in Fig. 4, is to automatically instantiates known attacks against SDN elements across the diverse environment and assists unknown security problems within SDN Deployment. Additional components are agent manager, application agent, agent channel and agent host. Agent Manager control all the additional component, and it runs on managed code i.e. router, controller and forward notification to the application agent, agent channel and agent host. The application agent is an autonomous agent or intelligent agent work in a dynamic environment responsible for achieving goals into actionable tasks. The agent channel is responsible for online channel management, distribution channels effectively among the components. Agent hosts are managed code runs into the data plane.

5. Performance Evaluation

The attack vectors that could affect the

SDN infrastructure are misconfiguration, malware and insider attacks. We simulate and evaluate the performance of our system under these attacks

- Malware 1, Due to this SDN control plane compromises at build-time
- Malware 2- SDN control plane compromises at run-time

5.1. Simulation Set up

Steps:

1- Fetching ONOS source

2- Building ONOS with Maven

3- Creating ONOS package that is deployed in a control plane

4- Deployed this package (ConFig.d to form a three-node ONOS Cluster) to three virtual machines (VM)

5- Reverse cell connected (attacker host)-Three node ONOS cluster created (Victim ONOS)

SDN Control Plane Components: The controllers that we consider in virtual SDN infrastructure are open network operating system(ONOS), and open daylight (ODL). Distributed network operating system, provide a base design for commercial SDN controller products, for example, brocade SDN and controller is based on open daylight.

So the first attack vector is a misconfiguration, on ONOS and open daylight, both implement various interfaces for management purpose and if an attacker can gain access to any one of these interfaces the attacker can freely manipulate the entire SDC network. And regarding this attack vector ONOS and the open daylight community have relieved the security guideline and possible mitigation would be changing default credentials and properly configuring the network.

Second Attack Vector Malware, Malware infection at build time and at run time, Also ONOS is prone to malware and the infection can take place during the build and run time. The possible defense is, to download the project source from a trusted source code repository.

Fig. 3. Software Defined Data Center(SDDC) Network Design and Attack Vector

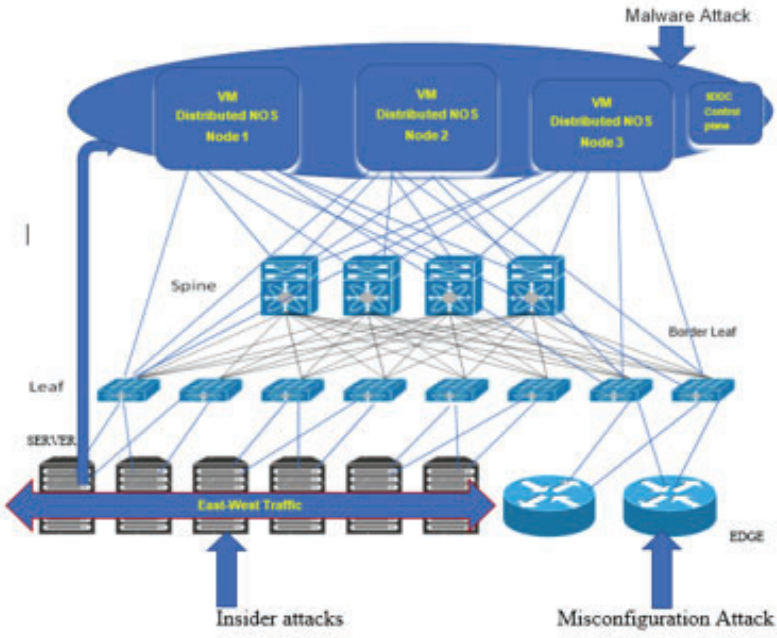
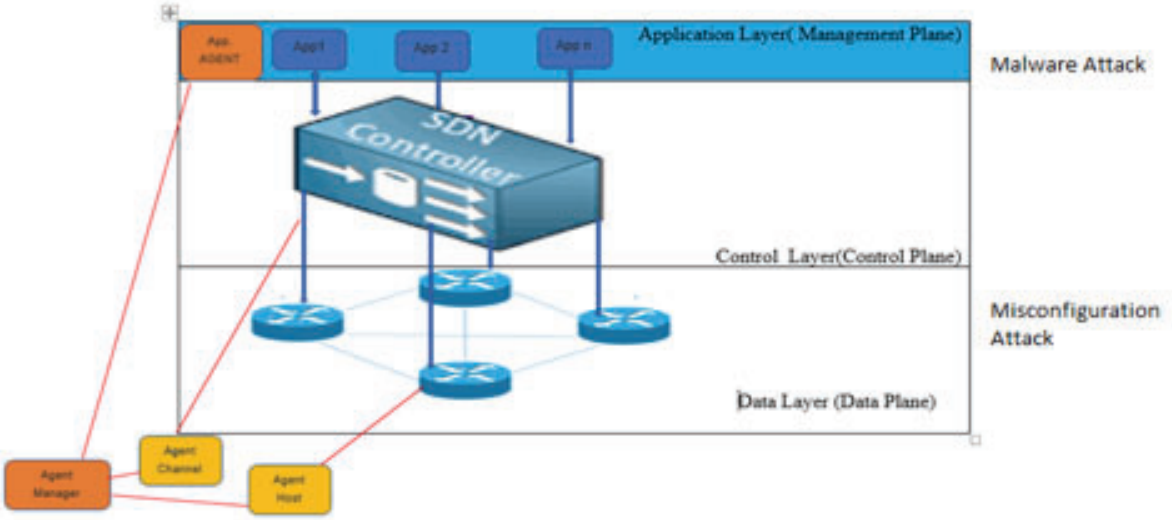


Fig. 4. Proposed Frame Work



Attack Vector - Malware 1, due to this SDN control plane compromises at build-time, it will manipulate host file and settings. If there was a network attack against the built environment, the malicious library could have been pulled from untrusted repositories and injected into the deployable package and causes DNS cache poisoning and ARP spoofing attack. And if this infected package is deployed this may put the entire data center at risk.

Another attack vector (Malware 2- SDN control plane compromises at run-time) is malicious SDN applications, ONOS, and open daylight both support the deployment of SDN applications. So that network administrators and operators can easily install SDN and applications using CLI, GUI or rest API. So to make them download and install malicious applications social engineering texts can be used and once this malicious application is installed. The application can manipulate the behavior of the control plane and the entire network.

And lastly, the SDDC control plane is also prone to insider attacks launched by malicious tenants. The malicious tenants may generate massive network flows to saturate the control plane and also they may send out crafted packets to manipulate the global network view maintained by the controller.

The attack scenarios

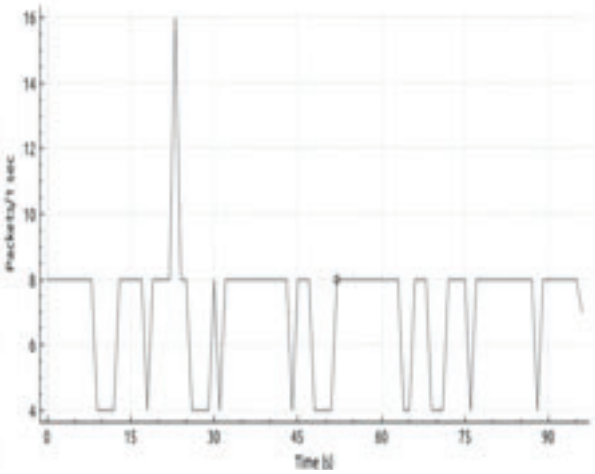
Compromising SDN control plane at build time and run time. Two attack scenario is discussed and implemented that breaks the SDDC infrastructure.

In the first attack scenario, we assume that the victim has built on us in an insecure environment and we use a maven repository to inject the malicious library into the deployment package. Once this infected package is deployed the malicious code will be executed and the attacker will get remote access to each hosted control or host machine and then will try to inject an arbitrary ONOS note to the control plane. An ONOS package that is deployable to the control plane. And deploying the package to three different virtual machines. ONOS deployed on the cluster. We have three nodes on the ONOS cluster form and the attacker host. We have a reverse shell connected back to the attacker. And the attacker host it is possible to access and modify all of the onus configurations including the credentials to access CSI

and GUI and also rest API. And also it is possible to modify the cluster configurations. So going to manipulate the cluster configurations to inject an unauthorized ONOS node to the cluster. So once the cluster restarts, it has four nodes on this cluster including one unauthorized node and the attacker can easily access the control plane and manipulate the entire SDN network with this unauthorized name.

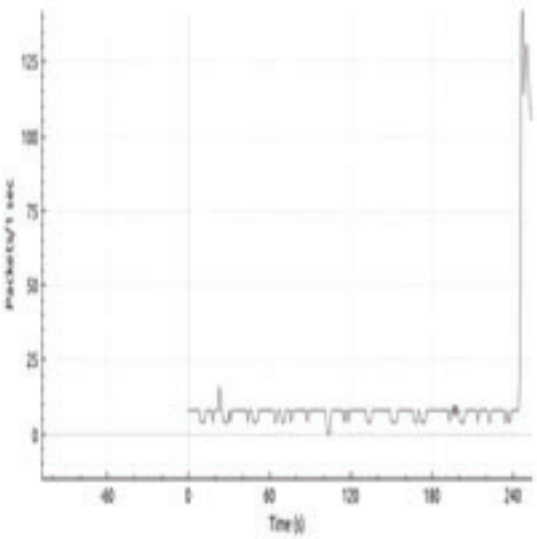
Analysis of the simulated network is also evaluated through Wireshark. Input-Output (IO) graph of Network is in under Normal Operation shown as in Fig. 5.

Fig. 5. Normal Traffic IO Graph



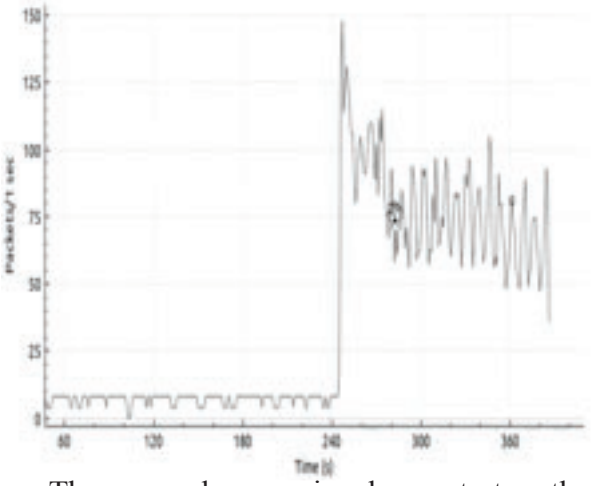
Flood traffic from host h2 to h1 (Victims) is shown in Fig. 6. A sudden higher spike represents the flood traffics.

Fig. 6. DDoS IO Graph



Mitigation of DDoS Attack is shown in Fig. 7, mitigating the malicious traffic which is flooding our victims, in this case, it will be host 1(H1). The sudden drop in the graph shows mitigation is applied

Fig. 7. Mitigation Flow IO graph



The second scenario demonstrates the threat of malicious SDN applications. In this case, we assume that the network operator has been fooled by social engineering attack and downloaded a malicious SDN application. So once the application is installed to the SDN controller Cluster. The application stealthily degrades the over network performance by abusing a weakness of a particular switch form here.

So as a proof of concept we use a simple test that consists of 1 switch device and 2 Network hosts. We have open data like controller console and on the right, we have one of the network costs for performance measurement. And manager assistant application and the other bundles running inside a controller. So when the switches are connected to the controller on the network host we perform the ping test to show our network performance.

Attacks are due to vulnerabilities in the proposed virtual SDN network, the following vulnerabilities are identified;

1- No System Integrity Protection-There is no System Integrity Protection for the NOS

component. The integrity of the CORE NOS component must be guaranteed. The first problem is that there is no system where protection for NOS in controllers. Deemed malicious libraries can be injected in the build process and the source code of the SDN controller could be manipulated before a building. But currently, since there is no mechanism to detect a loss of time integrity to the operator might directly deploy a compromise testing controller to the network. So. The code signing or other intuitive The second scenario demonstrates the threat of malicious SDN applications. In this case, we assume that the network operator has been fooled by social engineering attack and downloaded a malicious SDN application. So once the application is installed to the SDN controller Cluster. The application stealthily degrades the over network performance by abusing a weakness of a particular switch form here.

So as a proof of concept we use a simple test that consists of 1 switch device and 2 Network hosts. We have open data like controller console and on the right, we have one of the network costs for performance measurement. And manager assistant application and the other bundles running inside a controller. So when the switches are connected to the controller on the network host we perform the ping test to show our network performance.

Attacks are due to vulnerabilities in the proposed virtual SDN network, the following vulnerabilities are identified;

1- No System Integrity Protection-There is no System Integrity Protection for the NOS component. The integrity of the CORE NOS component must be guaranteed. The first problem is that there is no system where protection for NOS in controllers. Deemed malicious libraries can be injected in the build process and the source code of the SDN controller could be manipulated before a building. But currently, since there is no mechanism to detect a loss of time integrity to the operator might directly deploy a compromise testing controller to the network. So. The code signing or other intuitive protection mechanisms such as checksum could be possible solutions to this problem.

2- No authentication of SDN cluster nodes- This is a serious threat because the arbitrary on ONOS node can completely take over the control of the entire control plane into a network. public key infrastructure (PKI) based authentication could be one of the possible defenses of this threat.

3- No application access control- These applications are granted very powerful authority even though they are just applications running on an operating system. So application including even malicious one can access the core of the controller and freely manipulate the network behavior. The police based access control mechanism could be useful.

4- Switch device firmware Abuse- It degrades the network performance. In SDN, devices implement both hardware-based and software-based flow table. So if a packet is matched by looking up the software table it incurs significant overhead, so such packet matching strategies may vary, depending on the vendor and firmware version. Defense flow rule conflict detection and arbitration possible defense mechanism to mitigate such an attack could be detected and arbitrating global conflicts.

6. Conclusion

The paper aims to design and evaluate the SDN Security framework, that addresses the limitation and detects and mitigates the attacks. Attacks are characterized as misconfiguration, malware, and insider attack. In this paper we discussed SDN Architecture, SDN operation, attacks on software defined Data Center(SDDC). Literature review section highlights the work done in the domain of SDN security and countermeasure. Simulation and performance

evaluation was evaluated due to misconfiguration, malware and insider attack. Attacks are due to vulnerabilities in the proposed virtual SDN network, the main vulnerabilities are identified as no system integrity protection, no application access control and switch device firmware abuse. Possible defense and countermeasures of are discussed. Future work can also involve improving in Software defined data center (SDDC) security architecture with additional resilient recovery mechanisms.

References

Casado, M.; Foster, N.; Guha, A. (SDN Abstraction, Overview) Abstractions for software-defined networks. Commun. ACM 2014, 57, 86–95.

Akyildiz IF, Lee A, Wang P, et al., 2014. A roadmap for traffic engineering in SDN-OpenFlow networks. Comput Netw, 71:1–30.

Myint Oo, Myo, Sinchai Kamolphiwong, Thossaporn Kamolphiwong, and Sangsuree Vasupongayya. "Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)." Journal of Computer Networks and Communications 2019 (2019).

Salsano S, Blefari-Melazzi N, Detti A, et al., 2013. Information-centric networking over SDN and OpenFlow: architectural aspects and experiments on the OFELIA testbed. Comput Netw, 57(16):3207–3221.

Dixit A, Hao F, Mukherjee S, et al., 2013. Towards an elastic distributed SDN controller. ACM SIGCOMM Comput Commun Rev, 43(4):7–12.]

Feamster N, Rexford J, Zegura E, 2014. The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Comput Commun Rev, 44(2):87–98].

Chen, Wen, Suchao Xiao, Leijie Liu, Xueqin Jiang, and Zhangbin Tang. "A DDoS attacks traceback scheme for SDN-based smart city." Computers & Electrical Engineering 81 (2020): 106503],

Bhushan, Kriti, and Brij B. Gupta. "Distributed denial of service (DDoS) attack mitigation in the software defined network (SDN)-based cloud computing environment." Journal of Ambient Intelligence and Humanized Computing 10, no. 5 (2019): 1985-1997.

Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. "DDoS attack detection and mitigation using SDN: methods, practices, and solutions." Arabian Journal for Science and Engineering 42, no. 2 (2017): 425-441.

Kalkan, Kubra, Gurkan Gur, and Fatih Alagoz. "Defense mechanisms against DDoS attacks in the SDN environment." IEEE Communications Magazine 55, no. 9 (2017): 175-179.

Xu, Jianfeng, Liming Wang, and Zhen Xu. "An enhanced saturation attack and its mitigation mechanism in software-defined networking." Computer Networks (2019): 107092.

Sufian Hameed ,ID and Hassan Ahmed Khan, SDN Based Collaborative Scheme for Mitigation of DDoS Attacks,2018 MDPI

Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. "Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS Attack." In Proceedings of International Joint Conference on Computational Intelligence, pp. 49-60. Springer, Singapore, 2020

Hashemi, H.; Hamzeh, A. Visual malware detection using a local malicious pattern. J. Comput. Virol. Hacking Tech. 2018, 15, 1–14. [CrossRef]]

Fu, Yonghong, Jun Bi, Ze Chen, Kai Gao, Baobao Zhang, Guangxu Chen, and Jianping Wu. "A hybrid hierarchical control plane for flow-based large-scale software-defined networks." IEEE Transactions on Network and Service Management 12, no. 2 (2015): 117-131.

Wang, Huan-zhao, Peng Zhang, Lei Xiong, Xin Liu, and Cheng-chen Hu. "A secure and high-performance multi-controller architecture for software-defined networking." Frontiers of Information Technology & Electronic Engineering 17, no. 7 (2016): 634-646.

Blenk, Andreas, Arsany Basta, Martin Reisslein, and Wolfgang Kellerer. "Survey on network virtualization hypervisors for software defined networking." IEEE Communications Surveys & Tutorials 18, no. 1 (2015): 655-685.

Blial, Othmane, Mouad Ben Mamoun, and Redouane Benaini. "An overview on SDN architectures with multiple controllers." Journal of Computer Networks and Communications 2016 (2016).

Benzekki, Kamal, Abdeslam El Fergougui, and Abdelbaki Elbelrhiti Elalaoui. "Software"defined networking (SDN): a survey." Security and communication networks 9, no. 18 (2016): 5803-5833.

Song, Sejun, Hyungbae Park, Baek-Young Choi, Taesang Choi, and Henry Zhu. "Control path management framework for enhancing software-defined network (SDN) reliability." IEEE Transactions on Network and Service Management 14, no. 2 (2017): 302-316.

Rawat, Danda B., and Swetha R. Reddy. "Software defined networking architecture, security and energy efficiency: A survey." IEEE Communications Surveys & Tutorials 19, no. 1 (2016): 325-346.

Bonfim, Michel S., Kelvin L. Dias, and Stenio FL Fernandes. "Integrated NFV/SDN architectures: A systematic literature review." ACM Computing Surveys (CSUR) 51, no. 6 (2019): 114.

Hoang, Doan B., and Sarah Farahmandian. "Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies." In Guide to Security in SDN and NFV, pp. 3-32. Springer, Cham, 2017. book

Shi, Yongpeng, Yurui Cao, Jiajia Liu, and Nei Kato. "A cross-domain SDN architecture for multi-layered space-terrestrial integrated networks." IEEE Network 33, no. 1 (2019): 29-35.

Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. "Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS

Attack." In Proceedings of International Joint Conference on Computational Intelligence, pp. 49-60. Springer, Singapore, 2020.

Alsmadi, Izzat, and Dianxiang Xu. "Security of software defined networks: A survey." computers & security 53 (2015): 79-108.

Al-Fedaghi, Sabah, and Abdulrahman Alkandari. "On Security Development Lifecycle: Conceptual Description of Vulnerabilities, Risks, and Threats." International Journal of Digital Content Technology and its Applications 5, no. 5 (2011): 296-306.

Scott-Hayward, Sandra, Sriram Natarajan, and Sakir Sezer. "A survey of security in software defined networks." IEEE Communications Surveys & Tutorials 18, no. 1 (2015): 623-654.

Feng, Wendi, Zhi-Li Zhang, Chuanchang Liu, and Junliang Chen. "Clé: Enhancing Security with Programmable Dataplane Enabled Hybrid SDN." In Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies, pp. 76-77. ACM, 2019.

Park, Taejune, Yeonkeun Kim, Vinod Yegneswaran, Phillip Porras, Zhaoyan Xu, KyoungSoo Park, and Seungwon Shin. "DPX: Data-Plane eXtensions for SDN Security Service Instantiation." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 415-437. Springer, Cham, 2019.

Ali, Ali Faiq, and Wesam S. Bhaya. "Software Defined Network (SDN) Security Against Address Resolution Protocol Poisoning Attack." Journal of Computational and Theoretical Nanoscience 16, no. 3 (2019): 956-963.

Maziku, Hellen, Sachin Shetty, and David M. Nicol. "Security risk assessment for SDN-enabled smart grids." Computer Communications 133 (2019): 1-11.

François, J.; Aib, I.; Boutaba, R. FireCol: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Netw. (TON) 2012, 20, 1828–1841.

Anagnostopoulos, M.; Kambourakis, G.; Kopanos, P.; Louloudakis, G.; Gritzalis, S. DNS amplification attack revisited. Comput. Secur. 2013, 39, 475–485.

Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. Commun. Surv. Tutor. IEEE 2013, 15, 2046–2069.

.Kalkan, K.; Gur, G.; Alagoz, F. Defense Mechanisms against DDoS Attacks in SDN Environment. IEEE Commun. Mag. 2017, 55, 175–179.

Biggio, B.; Fumera, G.; Roli, F. Security evaluation of pattern classifiers under attack. IEEE Trans. Knowl. Data Eng. 2014, 26, 984–996. [CrossRef]

Chen, L.; Ye, Y. SecMD: Make Machine Learning More Secure against Adversarial Malware Attacks; Springer International Publishing: Cham, Switzerland, 2017; Volume 10400, pp. 76–89.

Biggio, B.; Corona, I.; Maiorca, D.; Nelson, B.; Srndic, N.; Laskov, P.; Giacinto, G.; Roli, F. Evasion Attacks against Machine Learning at Test Time; Springer: Berlin/Heidelberg, Germany, 2017; pp. 387–402.

Damodaran, A.; di Troia, F.; Visaggio, C.A.; Austin, T.H.; Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. J. Comput. Virol. Hacking Tech. 2017, 13, 1–12.

Galal, H.S.; Mahdy, Y.B.; Atiea, M.A. Behavior-based features model for malware detection. J.

Hameed, Sufian, and Hassan Ahmed Khan. "SDN based collaborative scheme for mitigation of DDoS attacks." Future Internet 10, no. 3 (2018): 23.

.Kalkan, K.; Gur, G.; Alagoz, F. Defense Mechanisms against DDoS Attacks in SDN Environment. IEEE Commun. Mag. 2017, 55, 175–179.

.Koning, Ralph, Ben de Graaff, Gleb Polevoy, R. Meijer, C. de Laat, and Paola Grosso. "Measuring the efficiency of sdn mitigations against attacks on computer infrastructures." Future Generation Computer Systems 91 • 2018

Bawany, Narmeen Zakaria, and Jawwad A. Shamsi. "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks." Journal of Network and Computer Applications 145 (2019): 102381.

.Hande, Yogita, and Akkalashmi Muddana. "A Survey on Intrusion Detection System for Software Defined Networks (SDN)." International Journal of Business Data Communications and Networking (IJBDCN) 16, no. 1 (2020): 28-47.

.Neu, Charles Varlei. "Detecting encrypted attacks in software-defined networking." (2019).

Chen, Wen, Suchao Xiao, Leijie Liu, Xueqin Jiang, and Zhangbin Tang. "A DDoS attacks traceback scheme for SDN-based smart city." Computers & Electrical Engineering 81 (2020): 106503.

Retrieved from https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf

Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T.: A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Commun Surv Tutorials. 16(3), (2014)

Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/

white-paper-c11-731860.html.

Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-735863.pdf.