A Survey Paper on SDN Security in Controller and data plane

Nishant S. Pawar Mtech student, GTU,Ahmedabad
Arunvel A., Project Engineer CDAC, PUNE
Aditya kumar Shinha, Join Director CDAC, PUNE

Abstract

Software Defined Networking Technology is way to computer networking that permit to network administrators to programmatically manage, control, change and initialize network behaviour dynamically through open interface and provide data forwarding functionality in data plane. SDN have three plane: Application Plane, control plane, data plane. SDN controller is centralized server to control the incoming traffic and forwarded it on data plane. In networking area, Attacker can be do some malicious attack to harm our networking system so that providing some security functionality to protecting SDN architecture is become research topic. In this paper we discuss about network security attack and mitigation attacks for SDN. Also discuss about enhance security on software defined attack (SDN).

Keywords
Software Defined networking, OVS, network attack, openFlow, controller, Data plane, control plane.

INTRODUCTION

Software defined networking (SDN) is an example of network infrastructure which is overcome the limitation of the traditional networking infrastructure. The era of network infrastructure SDN is use for communicate to organization network, data centre infrastructure, etc. In traditional network, network device have control plane which provide information used to build a forwarding table and data plane use forwarding table for routing decision for network traffic. When SDN is different concept for networking infrastructure like abstract concept. SDN is use control plane function which is control the networking device using SDN Controller. Controller communicates with physical or virtual network through openflow protocol.[9]

SDN has benefit to decoupling of control plane and data plane, network infrastructure is abstracted from application, so that whole network is manage in logically centralized way. Three plane of SDN is application plane, control plane and data plane. This planes is communicate with interfaces known as northbound interface and southbound interface. A Northbound interface is use API (application programming interface) between application plane and control plane. Typically Ryu, REST API, etc. use for northbound and second is southbound interface which is use standard protocol openFlow to allow networking device for controller. openFlow is use as protocol between Control plane and Data Plane. Here single controller is control the several devices. Traditional network have network device which is use forwarding table and control traffic using forwarding table which is manage traffic by routing table. Network functionality is mainly implement on Network devices as software or hardware in Traditional network. In SDN, SDN software as Controller is mange the all network device using centralized configuration control.

SDN creates dynamic and flexible network architecture that can improve as business requirement changes. The purpose of SDN is reduce cost and enhance user experiment by automating whole network services, from end users to network elements and decoupling of control from network traffic processing and forwarding, centralized control and mobility of customer and application to interact with network control. Software defined networking architecture is describe as three plane show in Fig 1:

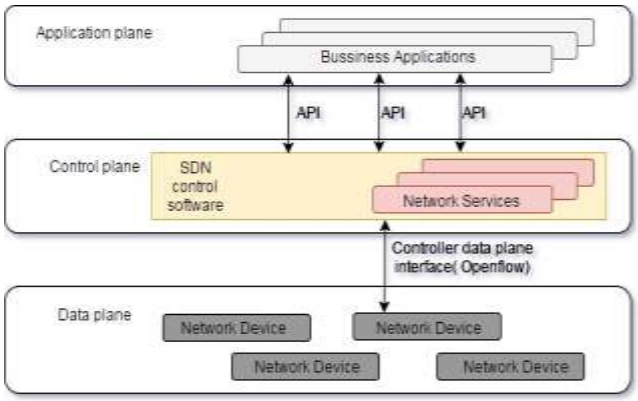

Fig 1: SDN architecture[9]

1) **Application Plane:** This layer is contains application like business application, controlling application, networking management, analytics, datacentre man-agement, etc. In application plane, application collect information and data from control layer. This applications is build abstracted view of network for decision making purposes. Interface between control plane and application plane is referred as northbound interfaces.
2) **Control plane:** This layer is useful for programming and managing data plane. It gives information from data plane and also give command or instruction to data plane. One or more software controller is communicate with data plane and it use standardized interface known as southbound interface. In controller plane, network controllers configure the network element with forwarding rules based on request from the application and security policy. Control plane contain the forwarding logic and additional routing logic.
3) **Data Plane:** This plane is responsible for forwarding data, observing local data or information and gathering statistics. Data layer is build up by using network element and providing connectivity. The data plane provided the resources that deal directly with external traffic, along with the necessary supporting resources to ensure proper virtualization, connectivity, security, availability, and quality.

The contents of the paper are present as follows. Section II Deals with SDN security and various kind of attack on network element and how to mitigate different kind of attack using different approach and security frameworks in section III. The paper is concluded in section IV.

SECURITY ISSUES AND RELATED WORK

As per survey work, SDN is network architecture that provide unparalleled programming, automation and network control. Also provide centralized control and monitoring in network.

Nowadays SDN security is become a research topic for network security area. SDN is provide network infrastructure for data centre, organization building and business purpose. For the network security, basic

properties of a secure network communication for information are Confidentiality, Integrity and Availability. These are supported by techniques of Authorization, Authentication and Encryption.[10]

In SDN, some security issue is happened like unauthorized access, data leakage, data modification, malicious and compromised application, denial of service (DoS), configuration issues and system level SDN security. The more typical SDN security concerns include attack at the different SDN architecture plane. Attacker can be attack on SDN layer as: 1) Attack on data layer 2) Attack on Control layer [10][5]

In, 2016 authors article of [7] have presented secure SDN framework is called as S2NET framework it is network model which is use SDN architecture with IoT device. Which offering authentication and key agreement between controller and smart device in data plane. Smart device is work as IoT device. Another thing is secure openFlow message issuing protocol is used to securely exchange message between controller and data plane. This framework is provide authentication and integrity using Smart openflow device. Show in Fig 2.

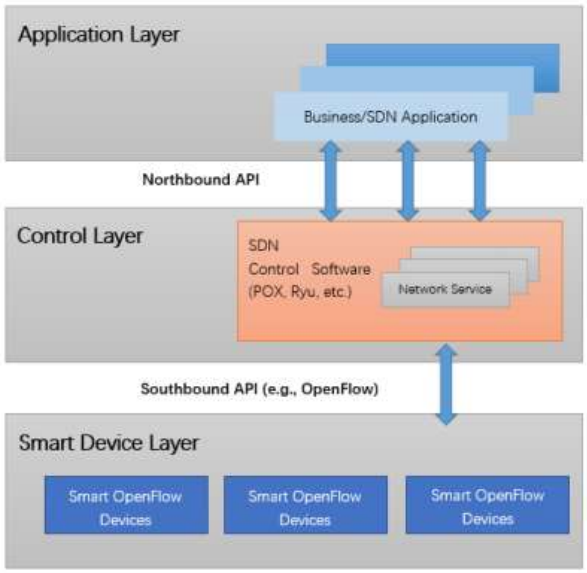

Fig 2: S2NET framework [7]

S2net is use openflow protocol and support to smart device. This framework design build a prototypical S2net as securing network platform to provide security in IB (Intelligent Building) services.[7]

Framework is use as IoT device to secure the communication channel between internal network and external network. Openflow is use as secure protocol between data plane and control plane. In Article SNET is use for controlling smart device as temperature sensor, gas sensor, fire alarm etc. S2NET is develop for achieve security property as: Integrity, Authenticity, Confidentiality, Lightweight, and Fresh key. Protocol I and protocol II is use in this framework. That become performance loss to compare with original connection setup.

In, 2016 authors article of [2] have present enhancing security in SDN base data centre. SDN feature are support to integrated network layer with security middle box like IDS and firewall. This framework is uses Syslog service. Frame-work is interconnected with SDN controller using North Bound Interface (NBI) and syslog server is gathering security log from several security middle box. Shown in Fig 3. This control unit is handle by security agent and syslog server.

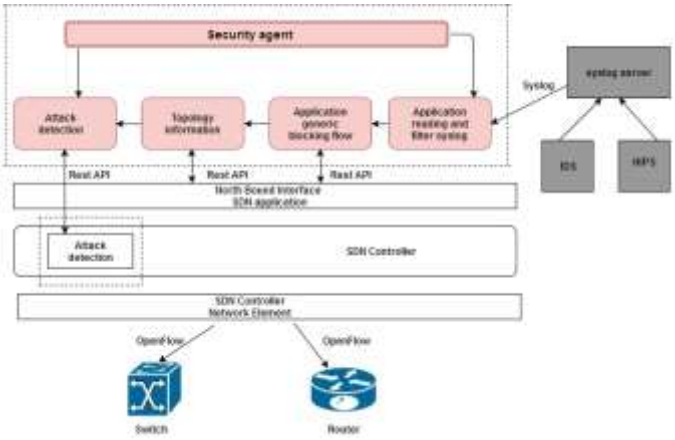

Fig 3 security framework in SDN[2]

In this [2] security layer is use in for enhancing data centre network as it will provide a new adaptive network layer as application aware. This framework is provide security for malicious traffic and unwanted request to prevent network as SDN infrastructure.

In, 2017 authors article of [1] have presented Software Defined Security (SDS) to analyse attack graph and alert for intrusion. Aim of security analysis to improve security approach for IDS using global view of attack and security state of SDN environment. Shown in Fig 4. And also achieve reducing rate of false positive attack.

Fig 4 Security analysis as SDS model[1]

In this article[2], the security state is characterized by calculated probability from environment metrics that confuse over the effect of an attack on confidentiality, integrity and availability.

In, 2016 authors article of [4] have presented security improvement using Firewall. This concept is use in SDN infrastructure to securely attached device from malicious traffics in regarded to attack and access control to updating SDN security by distributed System or devices. Proposed system model is shown in Fig 5.

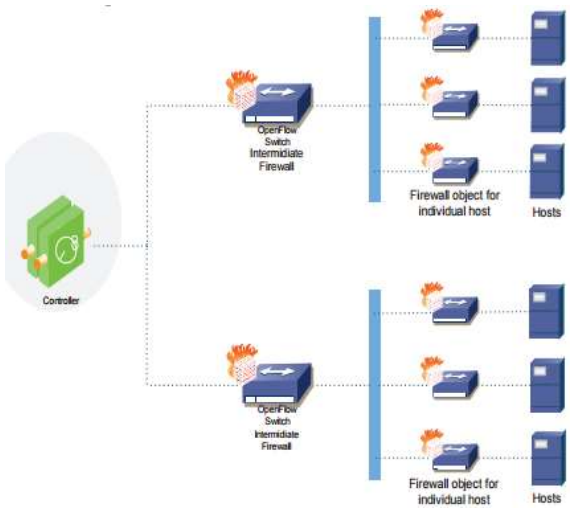

Fig 5 Propose model using Firewall[4]

Here openflow switch is act as intermediate firewall. Every host have separate firewall object in network and this is light weight and flexible implement.

This proposed model of SDN using firewall is develop to improve facilities. It gives proper protection and reduces manual work and also reduce or minimize difficulty which current system have.

In, 2017 authors articles of [3] have presented policy based approach to overcome network attack. They implement open sources SDN controller for develop policy based security application and use in real time scenarios. This approach is use to control and defend the SDN domain behaviour.

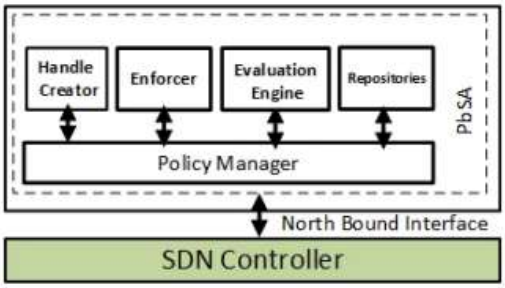

Fig 6 policy based security architecture for SDN[3]

Shown in fig 6, the policy based Architecture is use for securing the agreeability in SDN area. The Policy based Security Architecture can either shape some portion of the SDN Controller or can keep running as a Security Application over the SDN Controller. They have composed the Policy based Security Architecture as a Security Application running on top a SDN Controller for adaptability reasons. PbSA is actualized in the North Bound API interface of the Controller.

Policy based security application is capable to prevent and control the SDN domain behaviour. Using ONOS SDN controller, application and observe threat scenario is possible for this model. Some networking attack is mitigated using Policy based security architecture.

CONCLUSION AND FUTURE WORK

In this paper, we study Software defined network is emerging network-technology which provide centralized control and security is become main issue in SDN. We have study SDN security implementation with different method and focus on security Framework for different kind of attack. So here we conclude that various Security attack and also framework which is use for securing, prevention to SDN network.

Firewall , IDS, IPS, ACL this element is use for securing network in Software defined networking and we can be secure data palne and Control plane using this methodology.

Further related work could be doing by Securing data plane and Control plane for unauthorized access, ARP Poisoning and spoofing, data leakage in communication channel.

REFERENCES

[1] Nadya EL MOUSSAID, Ahmed TOUMANARI, Maryam EL AZHARI "*Security Analysis as Software-defined Security for SDN Environment*" Fourth International Conference, IEEE,2017

[2] Moustafa Ammar, Mohamed Rizk, Ayman Abdel-Hamid, Ahmed K. Aboul-Seoud "*A Framework for Security Enhancement in SDN-based Datacenters*" IEEE-2016

[3] Kallol Krishna Karmakar, Vijay Varadharajan, Udaya Tupakula "*Mitigating Attacks in Software Defined Network(SDN)*" Fourth International Conference on Software Defined Systems, IEEE,2017

[4] Dhaval satasiya, rupal raviya, hires kumar,"Enhanced SDN security using Firewall in Distributed scenario ", IEEE, 2016

[5] Marc C. Dacier, Hartmut König and Radoslaw Cwalinski, Frank Kargl, Sven Dietrich "*Security Challenges and Opportunities of Software-Defined Networking*", IEEE,2017

[6] Seungwon Shin, Lei Xu, Sungmin Hong, Guofei Gu , "*Enhancing Network Security through Software Defined Networking (SDN)*" IEEE, 2016

[7] Nian Xue, Xin Huang , Jie Zhang "*S2Net: A Security Framework for Software Defined Intelligent Building Networks*", IEEE, 2016

[8] Mudit Saxena, Dr. Rakesh Kumar, "A Recent Trends in Software Defined Networking (SDN) Security", IEEE, 2016

[9] En.wikipedia.org. (2017). Software-defined networking. [online] Available at: https://en.wikipedia.org/wiki/Software_defined_networking [Accessed 22 Sep. 2017].

[10] Hogg, S. (2017). SDN Security Attack Vectors and SDN Hardening. [online] Network World. Available at: https://www.networkworld.com/article/2840273/sdn/sdn-security-attack-vectors-and sdn hardening.html [Accessed 22 Nov. 2017].

[11] Global Config Technology Solutions, Inc. (2017). Software Defined Networking vs. Traditional Networking. [online] Available at: http://globalconfig.net/software-defined-networking-vs-traditional/ [Accessed 24 Nov. 2017].