Exploring Attack vectors and Security Challenges in SDN

Pradeepa.R , Pushpalatha.M

Abstract: ***Software Defined Networking (SDN) is a modern emerging technology in networking. SDN desires to furnish with composite and exclusive networking sources, it needs to decouple of carrier plane and the control plane, and also provides centralized control. The benefits of network programmability, dynamic computing, cost effective, high bandwidth, of SDN applications are discussed, but security has become an important concern. While centralized controller controlling multiple devices, this change in traditional network will be the main impact on network security. In this paper, we discuss about security issues and challenges in SDN architecture planes.***

Keywords: Software Defined Networking, Southbound API's, Northbound API's, Network attacks, Security services.

I. INTRODUCTION

Security problems were occurring and behave in different ways where the computers are networked. Malicious events occur and damage the network we call these events as attacks. Categories these attacks into four primary types such as access, modification, denial of service and repudiation attacks [2]. The variety of attacks are identified and detected in the network [1].

(i) Eavesdropping: It's a biggest security problem, to gain unauthorized access of information. Listen secretly to the private conversation of the network. A strong encryption service is needed.

(ii) Identity Spoofing: This attacker can modify, reroute or delete the data by special program to construct IP packets that appear to originate from original address.

(iii) Denial of service: Block traffic by flooding invalid data to the entire network until shutdown the application or network due to overload.

(iv) Password based attacks: Modify network and server configuration, reroute or delete data through finds a valid user account.

Dedicated encryptionsonly may not be the solution for those attacks anymore. Some of the security services to be used with suitable threat assessment and security planning. It is significant to know how exactly security services are used to counter specific type of attacks [2].

Manuscript published on 30 September 2019.
***Correspondence Author(s)**

Pradeepa R, Department of Computer Science and engineering, SRM Institute of Science and technology, Chennai, India. Email: pradimca@gmail.com
Pushpalatha M, Department of Computer Science and engineering, SRM Institute of Science and technology, Chennai, India. Email: pushpalatha.m@ktr.srmuniv.ac.in

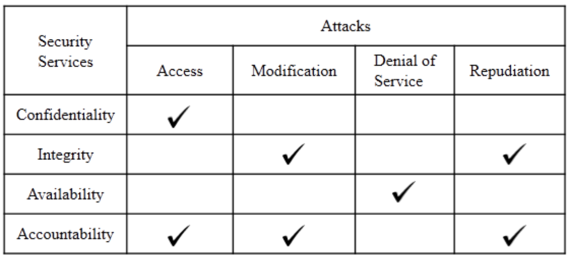
(a).Confidentiality: It is designed to prevent reaching the sensitive information to wrong people. Confidentiality is ability to hide data from unauthorized user to view. Some of the cryptographic methods are used to ensure confidentiality [3]. Access attacks can be preventing by confidentiality.

(b). Integrity: Integrity is designed to provide correctness to the information [4]. It has confidence that the data is correct and has not been modified by the unauthorized users. This service protects against the modification attack.

(c). Availability: It ensures that the data to be useful. Backups are the simplest form of availability. Some of the attackers attempt to deny access to the authorized users, such as denial of service type of attacks. These type of attacks can be prevented by availability.

(d). Accountability: Accountability does not protect against attacks by itself. But without accountability confidentiality and integrity would fail. Each of the security services hostilities specific attacks in Table.I

Table.1 Security Services hostilities attacks



Security Services	Attacks			
	Access	Modification	Denial of Service	Repudiation
Confidentiality	✓			
Integrity		✓		✓
Availability			✓	
Accountability	✓	✓		✓

We would like to adopt SDN, before that we have to mind the top issues for the concern of security. How SDN products will assure them their applications? And how infrastructure will not be in danger? And how those attacks can be avoided by the security services and additional futures in SDN? The SDN structural design can be changed to improve network security by providing highresponsive security monitoring, investigation and response system [5]. Monitoring and logging applications are run in the controller is used to explore the entire network.

An analysis of SDN Security attack vectors and securing from those attacks are presented in this paper. Security issues are classified accordingly to SDN planes affected. The prerequisite for upcoming work to launch the secure SDN is identified from its issues and foregoing research.

II. ATTACK VECTORS IN SDN

SDN is an approach of new standards for virtualization with the support of splitting the forwarding layer and the control layer. Three layer model architecture of SDN [7] consist of bottom level of network devices (Data plane layer), middle level of controllers (Controller layer) and the top level which includes applications and its services (Application layer).The widely deployed and technology matures are the goal of attackers.

Table. II Security Services hostilities attacks

Attack	Targeted SDN Layer				
	Application Layer	Northbound API	Control Layer	Southbound API	Data Layer
Unauthorized Access	Yes	Yes	Yes	Yes	Yes
Data Leakage					Yes
Flow Rule modification			Yes	Yes	Yes
Malicious Applications	Yes	Yes	Yes	Yes	Yes
DoS			Yes	Yes	Yes

The core security concern comprises attacks at the various layers of the SDN architecture. Let's investigate the expected attacks that could arisein its different layers. The following fig.1 is to demonstrate the SDN architecture and the attacks in various directions in each layer.

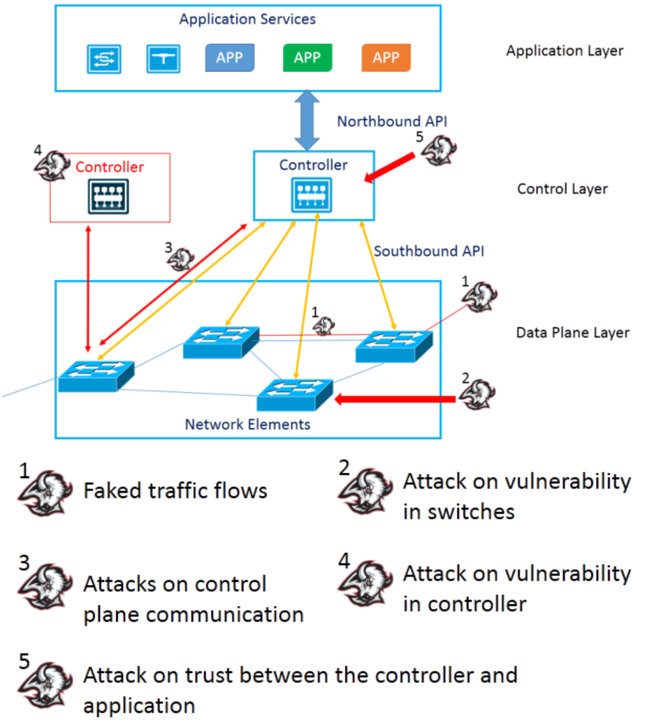

Application Services
APP
APP
APP
Application Layer
Northbound API
5
4
Controller
Controller
Control Layer
3
Southbound API
1
1
Data Plane Layer
2
Network Elements
1 Faked traffic flows
2 Attack on vulnerability in switches
3 Attacks on control plane communication
4 Attack on vulnerability in controller
5 Attack on trust between the controller and application

Figure 1: Attack vectors

A. Attacks in Data plane layer:

Target the elements and the traffic flow within the Data plane. Attackers try to access or compromise the host which is already connected with the application by physically or virtually to the network. Some of the southbound API's and protocols [8] like OpenFlow, BGP, CLI, SNMP (Simple Network Management Protocol), OpFlex, NETCONF etc… [9] Each of these protocols has their own methods for securing the communication within the network elements. But many of the protocols not have to set them up in the most secure way.

a. Faked Traffic flows

Faked traffic flow attacks involve sending a large number of fake data packets to the nodes [10]. The fake packets try to change the operational behavior of the network process.The attack deeds weaknesses in the router packet processing. Attack can be used to launch fake traffic flow in the core of thenetwork which makes the out of source availability situation. The following fig.2 shows the fake traffic flows in network.

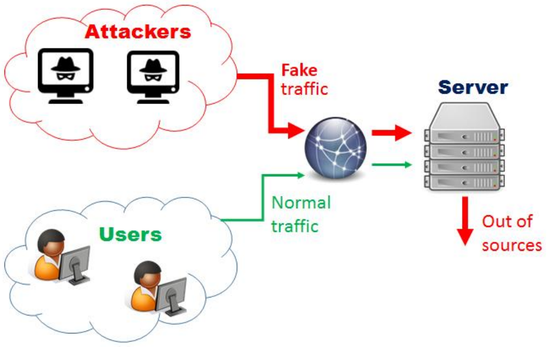


Figure 2: Faked traffic flow

The massive commonsecurity issues in networking are linked to end user systems and protocols. One example is large scalefaked traffic attacks, which are created by attackers [11]. Protected protocols are required to offer basic data security, includingvalidation and confidentiality.

b. IP Spoofing

The attacker obtains the IP address of an appropriate host and modifies packet headersso that the appropriate host appears to be the source.IP spoofing is used to hijack web browser, user who types web address of an appropriate site is taken to a dishonestWeb page created by the attacker. The following fig.3 describes the process of IP Spoofing to hijack the web site.

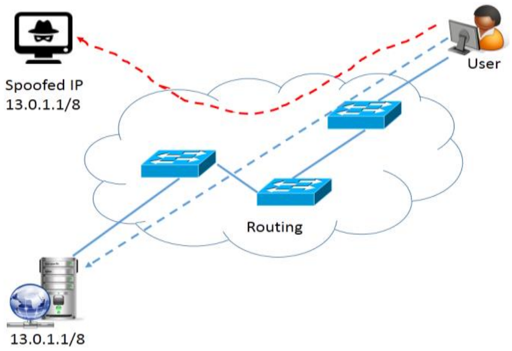


Figure 3: IP Spoofing

The attacker obtains the IP address and created a fake link between the user and the source system of a network. The fake link inoculation is also distracting the process of Shortest Path Routing facility [12]. At the end, all the traffic negotiating over the fake route will collapse into the deception of the hijacker.

B. Attacks in Control layer:

That SDN controller is a target to attack. Attackers want to create new control flows by spoofing Northbound API messages or the southbound API messages by the devices. Attacker may be tried to perform a DoS attack or any other methods to causes the controller to fail. Attackers will create fake entries in the flow tables of the network elements and the SDN engineers are not able to view those flows from the viewpoint of the controller.

Some of the proposed projects like SDNShield [13], are defense system against attacks on SDN control plane. But many of the protocols are failed to defense the control plane from attackers.

a. Denial of Service in Control plane

The SDN control plane unsuccessful to offer enough throughput. This susceptibility could be initiated by the (DDoS) distribute denial-of-service attacks [14].Attacker's attacks the controller and make changes in flow table to attacks the target machine via some of the host which are connected to the controller. The fig.4 describes control plane attack.

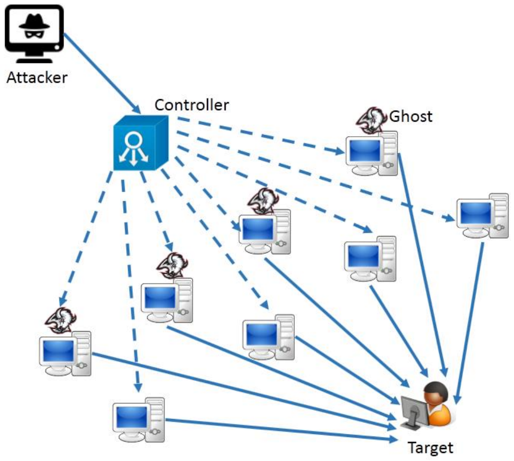


Figure 4: DDoS in Controller

Traditional DDoS security methods emphasis on protecting the data plane, and they are hopeless in the cases of SDN control plane attacks [15]. The proposed methods are only give the partial solutions to the problems by scaling the control planes using software defined switches, but it's not ultimately solve the problems caused by the DDoS attacks in SDN Control planes.

C. Attacks in Application layer:

If the controller is lacked to provide security for the northbound API, then the attackers are able to create their own control polices and achieve the full control of the SDN environment. Some of the applications are not authenticated properly so that attackers can easily create the new own configurations [16].

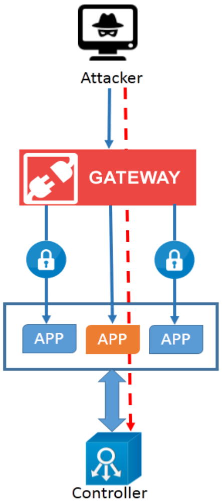


Figure 4: API Attack

Fig.4 explains the attack in application plane. Some of the API like REST use default password, there is no proper authentication so that attacker easily attacks that application plane.

III. SECURING THE LAYERS:

. We have to look at how secure an SDN system based on strengthening the three layers shown in fig.1 attack vector architecture. Most of the implementers are not follow the traditional IP networks techniques [16]. Some of the DCI protocols may not have an option for security, if they follow the same for the security, then they will be baring their network to attacks. Setting password or shared secrets may give an option. There may be configurable options to authenticate tunnel endpoints and secure the network traffic.

A. Securing Data Plane:

There are many options to secure this communication based on the southbound protocols. Some protocols like SNMPv3 [17] offer more security and SSH is better than Telnet.

Multi domain IBC Methodology [18]: Securing the distributed SDN data plane with a multi domain capable Identity-Based Cryptography (IBC) protocol, mainly for the southbound and data plane. This IBC system, we can derive shared session key from various sub domains also. Not only this session key exchange increases the network scalability, but migration of switch in southbound and inter domain data plane communications. This leads to low power and higher network performance.

SDNSPIN Methodology [19]:SDNSPIN protocol reaches energy efficiency, based on neighbor nodes distance the power setting up for sending nodes. Security is also succeeded in host level nodes by controller with negotiation protocol SPIN, the nodes will not communicate each other without the knowledge of controller. Fig 5 shows the SDNSPIN for a secured Data plane.

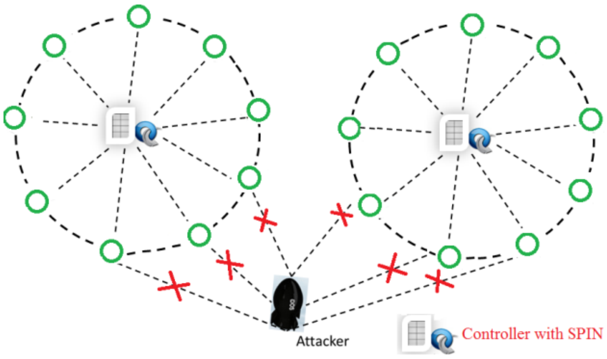


Figure 5: SDNSPIN

We need some intelligent solutions to detect and protect network devices [20]. Need some scanning methodology to locate attackers and intelligent system to react for those attacks. This is the most reliable methodology to ensure secured data plane for dynamic SDN topology.

B. Securing Control Plane:

The controller is the crucial goal of the attackers so it must be important for network operators to identify the security threats and to design their network. Controller administrators need to use some policies like role based access control (RBAC) [21].Protect the network by authorization and high availability [22] of controller architecture will help us to prevent from DoS attack in controller. An active area of research and attack mitigation have several way of solutions are discussed. Log, detect and prevent attacks by suitable actions to limit the impact of attacks. Some of solutions are not based on the detection just by improved configuration parameters they mitigate the attacks [14]. Few solutions are discussed in the following section to prevent DoS attack in controller.

AVANT-GUARD [23]: The goal of this proposal is to make secured SDN with more scalable and approachable from the dynamic network attacks. They introduce automatic insert of flow rules by starting triggers while the network under threads. Such saturation attacks are controlled by enabling the connection migration between data plane and control plane. This framework advances the security of controller with greater contribution from the data-plane layer.

OF-GUARD [24]: This proposal has two functional objectives. Packet migration is introduced to prevent from saturation attacks from data to control plane is a first objective. Fake packets make a table-miss, data plane cache is used to discard it by differentiate the fake packets and normal packets is the another objective of this proposal. The advantages of this design is attack-driven, no need to change controller applications and end hosts and just add ignorable overhead and latency.

Security-Enforcement Kernel (SEK) [25]: In this proposal they introduce specific permission model to exchange messages from application to data plane. The flow rule conflict detection algorithm is used to identify destruction in recursive flow rules. Authenticated message service is used in northbound API and the conflict is resolved by introducing a role-based hierarchical approach. And they describe the mapping of events and audit attributes by applying application –layer audit subsystem in Control layer for security audit requirements. But some limitations also there in this proposal, may some malicious application can bypass or corrupt this SEK.

SDN sEcure COntrol and Data Plane (SECOD) [26]: New triggers are used in this proposal to detect and prevent DDoS attacks in both controller and Data plane. SECOD keeps network 99.72% secured with its performance. Dynamic threshold approach used to progress the system flexibility in controller and data plane as well as utilized resources efficiently. These methods are partially control the attacks in a network, more proposals and methods are need to be implement for a fully secured network.

C. Securing Application Plane:

Secure the application plane by secure coding practices, authentication and encryption methods. Control network traffic by less cost and easier construct by using OOB [27] (Out Of Band) network. Using OOB in Northbound and Southbound communications will help us to secure the protocols. TLS [28] or SSH [29] or IPsec [30] or any other methods are used to secure the application plane and secure the controller management. Some of the possibilities will secure communication in application layer. The following authentication mechanisms are describing their secure network.

Public Key Infrastructure [31]: In this proposal they describe about the peer encryption methodology. Deploying TLS as an access and authentication protocol in the controller based architecture using public key infrastructure. For this architecture each system must have key pairs on its secure place and key exchange between different systems is provided which ensure the security of the system.

Trust of first use [31]: It's an approach of authentication using SSH protocol using automatic generated keys and trust of first use method. All systems are treated as SSH based clients and controller as a server connected with key. Two different level of security configuration is used in this proposal, one is automatic acceptance and another one is trust based system by verifying public key in first time which completely reduces the eavesdropping via SSH tunneled messages. IPsec [31]: In this analysis IPsec protocol is used in host to host architecture, creates the secure communication between the systems and allows authenticating each other. This IPsec scheme working in a network layer so that IPsec protocol protect any application traffic over the network. Other then known attacks on IPsec solutions were recommended to apply [32].

Recent days, there are many Machine Learning approaches are proposed to detect various attacks or abnormal behavior on SDN. ML based approach to detect DoS attack [33] in this proposal various ML schemes are used to detect normal and abnormal behavior of the network, various supervised classifier performance are compared and few of them found to be high accuracy rate in detection with low false alarm rate. This mechanism is run parallel in application layer without affecting the performance of other layers and no need to change anything on data or control layers. From these analysis benefits as well as drawbacks in the proposals but few attacks are not been established and appropriately researched yet.

IV. CONCLUSION:

We try to prognosticate the attackers target with SDN Layers. The organizations, protocols, controller software are new and the previous history of SDN attacks is unknown. We can envisage where an attacker can attack based on SDN architecture. If we act ourselves like an attacker's, we can influence and spot the weakness of attacker's. Then we can toughen that weakness ahead of time. Each organization should consider how to secure their system before launch SDN deployment project in early design stage itself. In this survey we provide an overview of possible attacks in SDN layers and some of the solutions to protect from those attacks but none of the solutions given full production for that attacks. Setting up it from the initial stage will save the network from many problems down the road.

REFERENCES

1. VivekRichhariya and Praveen Kaushik, "A survey on network attacks in mobile ad hoc network", International journal of advanced research in computer science and software engineering, Volume4,Issue 5, May 2014.
2. Eric Maiwald, "Types of attacks and information security services", in book Fundamentals of Network Security Tata McGraw Hill edition 2010.
3. Alexander J. Summers "What is security analysis? " overview and introduction to this topic is in www.doc.ic.ac.uk/~ajs300/security/CIA.htm
4. ShyamNandan Kumar " Review on Network security and cryptography" International Transaction of Electrical and Computer Engineers system , 2015 3(1), pp 1-11
5. Sandra Scott-Hayward,Gemm O'Callaghan and SakirSezer "SDN Security: A Survey",Future Networks and services, Nov 2013 IEEE SDN for.
6. C.Douligeris and D.N Serpanos, "Network Security : Current status and future directions." Wiley.com 2007.
7. GagandeepGarg, RoopaliGarg, "Review on Architecture and security issues of SDN" International journal of innovative research in computer and communication engineering vol. 2, issue 11, Nov 2014.
8. What are southbound API's? in https://www.sdxcentral.com/sdn/definitions/southbound-interface-api/ from sdxcentral
9. Marc Mendonca Bruno Astuto A. Nunes, Xuan-Nam nguyen, Katia Obraczka, and Thierry Turletti"A survey of software-defined networking past present and future of programmable networks" IEEE Communications Surveys & Tutorials Volume:16 , Issue: 3 Aug 2014
10. DanaiChasaki, Tilman Wolf "Attacks and Defenses in the Data Plane of Networks" IEEE transactions on dependable and secure computing 2012.
11. Sreeja Nair M ;Harikrishnan Nair M P "A Study of DDoS Attack in Data Plane Network" IJSTE - International Journal of Science Technology & Engineering| Volume 3 | Issue 05 | November 2016
12. Sungmin Hong, Lei Xu , Haopei Wang, GuofeiGu"Poisoning network visibility in Software Defined Network: New attacks and countermeasures" NDSS'15 8-11 February 2015, San Diego, CA, USA, ISBN 1-891562-38-X
13. Xitao Wen ; Bo Yang ; Yan Chen ; Chengchen Hu ; Yi Wang ; Bin Liu ; Xiaolin Chen "SDNShield: Reconciliating Configurable Application Permissions for SDN App Markets" IEEE Xplore:03 October 2016 ,10.1109/DSN.2016.20
14. RajatKandoi ; MarkkuAntikainen"Denial-of-service attacks in OpenFlow SDN networks" Integrated Network Management (IM), 2015 IFIP/IEEEXplore on 02 July 2015, 10.1109/INM.2015.7140489
15. AbdelhadiAzzouni , Othmen Braham, Nguyen Thi Mai Trang, Guy Pujolle and RaoufBoutaba "Fingerprinting OpenFlow controllers: The first step to attack an SDN Control plane" Networking and internet Architecture(cs.NI) cite as : arXiv:1611.02370[cd.NI]
16. Sandra Scott-Hayward, Member, IEEE, Sriram Natarajan, and SakirSezer Member, IEEE, "A Survey of Security in Software Defined Networks" IEEE communications surveys and tutorials, 18(1), 623-654 DOI: 10.1109/COMST.2015.2453114
17. William Stallings "Security comes to SNMP: The new SNMPv3 proposed internet standards" The Internet Protocol Journal – Volume 1, No.3
18. JunHuy Lam, Sang-Gon Lee, Hoon-Jae Lee, and YustusEkoOktian "Securing SDN Southbound and Data Plane Communication with IBC" Mobile Information Systems Volume 2016 (2016), Article ID 1708970, http://dx.doi.org/10.1155/2016/1708970
19. PradeepaR,M.Pushpalatha "SDN enabled SPIN routing protocol for wireless sensor network" 978-1-4673-9338-6/16/$31.00 ©2016 IEEE pages: 639-643.
20. Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. "Software-defined network (sdn) data plane security: Issues, solutions and future directions." arXiv preprint arXiv:1804.00262. 2018.
21. Sylvia Osborn,Ravi Sandhu, QamarMunawer "Configuring role-based access control to enforce mandatory and discretionary access control policies" ACM Transactions on Information and System Security (TISSEC) Volume 3 Issue 2, May 2000 Pages 85-106
22. High Availability: Cisco Wireless LAN Controller Configuration Guide, Release 7.4
23. S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-defined Networks," in Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 413–424.
24. H. Wang, L. Xu, and G. Gu, "OF-GUARD: A DoS Attack Prevention Extension in Software-Defined Networks. Open Networking Summit 2014," https://www.usenix.org/sites/default/files/ons2014-poster-wang.pdf,accessed on 13.11.2014.
25. Phillip Porras, Steven Cheung, Martin Fong, Keith Skinner, and VinodYegneswaran "Securing the Software Defined Network Control Layer" NDSS'15, Feb 2015, San Diego, CA, USA Copyright 2015 Internet Society, ISBN 1-891562-38-X.
26. Wang, S., Chandrasekharan, S., Gomez, K., Kandeepan, S., Al-Hourani, A., Asghar, M. R., ... & Zanna, P. "SECOD: SDN sEcure control and data plane algorithm for detecting and defending against DoS attacks". In NOMS 2018 IEEE/IFIP Network Operations and Management Symposium pp. 1-5
27. OOB: A little-known technology with big potential By Dennis DrogsethNetwork World Oct 24, 2005
28. N. Ferguson and B. Schneier, Practical cryptography. Wiley New York, 2003, vol. 141.
29. "SSH Vuln Note," URL: http://www.kb.cert.org/vuls/id/958563.
30. J. P. Degabriele and K. G. Paterson, "Attacking the ipsec standards in encryption-only configurations." in IEEE Symposium on Security and Privacy, vol. 161, Oakland, 2007, pp. 335–349.
31. Dominik Samociuk, "Secure Communication between OpenFlow Switches and Controllers"IARIA, 2015. ISBN: 978-1-61208-428-2 32.
32. J. P. Degabriele and K. G. Paterson, "Attacking the ipsec standards in encryption-only configurations." in IEEE Symposium on Security and Privacy, vol. 161, Oakland, 2007, pp. 335–349.
33. Singh, P. K., Jha, S. K., Nandi, S. K., & Nandi, S. "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture". In TENCON 2018 IEEE Region 10 Conference pp. 0144-0149.