International Journal of
Applied Mathematics,
Electronics and Computers
ISSN: 2147-8228 http://ijamec.atscience.org

Advanced Technology and Science

Original Research Paper

A Preliminary Survey on the Security of Software-Defined Networks

Muhammet Fatih Akbaş *[1], Enis Karaarslan [2], Cengiz Güngör [3]

Accepted 3rd September 2016

Abstract: The number of devices connected to the Internet is increasing, data centers are growing continuously and computer networks are getting more complex. Traditional network management approach is becoming more difficult and insufficient. Software-Defined Networks (SDN) is a new generation networking approach which is expected to take place of the traditional computer networks. SDN architecture provides effective management of the large and complex networks. Although SDN have benefits from the network security perspective, it also brings new attack vectors. We believe that the network security problems in SDN architecture need more advanced solutions. In this work, a survey on the SDN security problems is presented, challenges are discussed. In this context, security threats and attack surfaces in SDN are described, the significant SDN security solution examples in the literature are given.

Keywords: *Software-Defined Networks, SDN, SDN Security*

1. Introduction

There are many network devices in computer networks such as router, switch, firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Complex and different protocols are running on these devices. Every day, new technologies such as Internet of Things (IoT), smart cities and smart management are emerging, data centers are growing and the number of devices in computer networks is increasing. Computer networks are getting more complex and heterogeneous and management of the network is becoming more difficult. Traditional network management approach is insufficient in large-scale computer networks. There is a need for a better network management approach and new methods. Software-Defined Networks (SDN) is an emerging concept that bring a new generation network management approach which is expected to take place of the traditional computer networks. SDN promise administrative convenience, hardware-independent, dynamic, scalable and flexible networking architecture. SDN provide a centralized network management and a global perspective on the network. So, this enables effective management of the large and complex networks.

With the rising of popularity of the IoT concept recently, the number of devices connected to the internet increases every day. IoT offers an environment that interact the objects we use in daily life with the other objects. All of devices that support networking technology such as computers, smart phones, tablets, air conditioners, refrigerators, cars etc. continuously produce data and this data is growing each day. As a result, big data concept emerges that represents high-volume, complex and irregular data. Big data can not be processed, stored and managed by traditional methods. Big data which becomes more valuable requires meaningful results. So, big data should be processed. Big data needs more bandwidth for processing. Nowadays, smart cities and smart management concepts come to the fore more and SDN management, security and optimization topics will need more advanced mechanisms.

In the second section of this study, the basic concepts of SDN, the benefits of SDN architecture are explained. In the third section, security threats and attack surfaces in SDN are described. In the fourth section, significant SDN security solution examples in the literature are given. In the last section, this study is summarized and future works are presented.

2. SDN & Benefits

There are three planes/layers including application, control and data and two interfaces including application-control and control-data. Control plane decides where frames/packets will be forwarded/routed. The data plane forwards the traffic to the destination. Routers and switches that we used in today, includes control plane and data plane are integrated on the same hardware. SDN concept is based on the idea of the separation of these planes. Control plane in other words network intelligence is moved to a high performance server and network management is performed with centralized controller software. The data plane is left on OpenFlow-enabled router or switch and is responsible for forwarding of packets only. SDN architecture is shown in Fig. 1. This architecture provides ability to directly programming the network and enables underlying infrastructure layer to be abstracted for network services and applications [1]. So this provides more dynamic, flexible, scalable platform and easy management of the network compared to traditional network infrastructures.

The control plane is also known as a network operating system that enables the communication between network applications and data plane. The communication between control plane and the data plane is provided with an open source network protocol OpenFlow [2]. OpenFlow is considered as a standard for SDN.

SDN architecture brings some benefits from the security perspective. SDN provides programmability and centralized controller has a global view on the network. These characteristics of SDN have an advantage against security threats. For example, when an anomaly is detected on the network, related traffic can be sent to the controller for analyzing. After the analysis process,

[1] *Information Technologies Department, İzmir Kâtip Çelebi University, İzmir/Turkey*
[2] *Computer Engineering Department, Muğla Sıtkı Koçman University, Muğla/Turkey*
[3] *International Computer Institute, Ege University, İzmir/Turkey*
** Corresponding Author: Email: mfatih.akbas@ikc.edu.tr*
Note: This paper has been presented at the 3rd International Conference on Advanced Technology & Sciences (ICAT'16) held in Konya (Turkey), September 01-03, 2016.

existing rules can be updated or new rules can be created for preventing attacks.

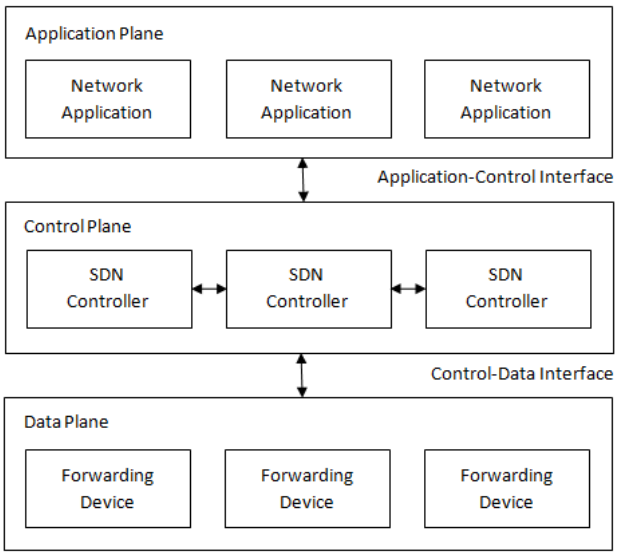

Figure 1. Software-Defined Networks (SDN) Architecture

SDN benefits are obvious. It is expected that SDN will replace the traditional computer networks in the near future. SDN also have some security threats which will be discussed in the next section.

3. SDN Security Threats & Attacks

SDN architecture has network programmability and centralized control advantages but these advantages can lead to new security threats and increase of the attack surfaces. There are variety of security threats targeted to the plane and interface of the SDN. Security threats and attack surfaces in SDN are shown in Fig. 2.

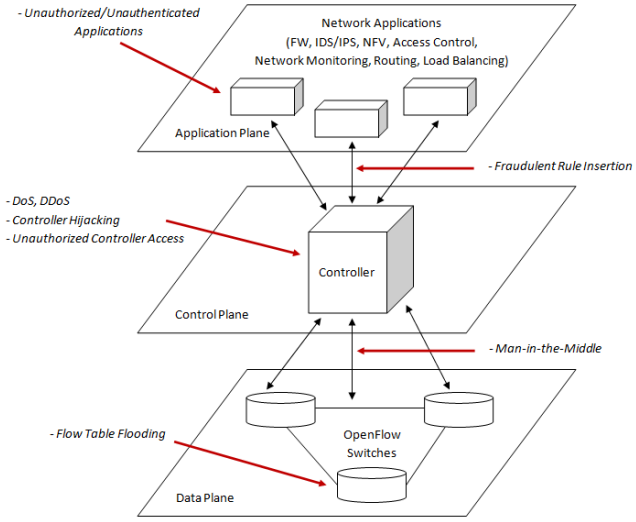

Figure 2. SDN Security Threats & Attack Surfaces

Security threats in SDN can be classified as seven different threat vectors, three of which are SDN-specific [3]. The security threats such as Denial of Service (DoS), unauthorized access, data leakage, data modification, malicious applications which are seen in all other network architectures is also seen in SDN [4]. The SDN specific ones are the attacks which target the controller software, communication between the control plane and the data plane (control-data interface) and the communication between the control plane and the application plane (controller-application interface). All those threat vectors have a potential effect on the operation of the entire network. Attacks against SDN planes and interfaces and the targeted security services are given in Table 1.

DoS and Distributed Denial of Service (DDoS) attacks against the controller and flow table flooding attacks against the switches in the data plane target the availability principle or service of the security. The logically centralized controller is one of the main features of the SDN. Although this feature provides a global perspective on the network, it emerges as one of the major weaknesses in terms of security of the SDN architecture. In [3], it is shown that the faked traffic flows can be used to make DoS attacks to OpenFlow switches and controller sources. The attacker may expose DoS attacks to the controller by sending too many packets to the controller. Similarly, more than one attacker or botnets may send large amount of packets to the switches in a systematic way. As not all of the rules are included in the flow tables of switches, this will cause a large number of queries to be sent to the controller. In this case, the controller will be exposed to DDoS attack and will become unable to respond to legitimate requests. DoS and DDoS attacks on the controller have a potential affect the functioning of the entire network in a negative way. Similarly, DoS attack may be possible also for the switches in the data plane. The flow tables of the switches which have limited cache will be vulnerable to flooding attacks when the attackers send large packets which belong to different flows. As previously stated, some of the flow rules are not available in the flow table so the queries are sent to the controller. While waiting the answer to these queries, the cache of the switches will fill up quickly. This type of attack is also called as DoS Switch [5].

Controller hijacking or unauthorized controller access attacks target the confidentiality principle of the security. Vulnerabilities in the controller may have consequences which can put the entire network at danger [3]. The attacker can take over the management of misconfigured, vulnerable controller and also the management of the network. Then, the attacker can programme switches in the data plane to drop the traffic coming to the controller can use to launch attacks on other targets [5].

In the absence of mechanisms to ensure security in the communication between the control plane and the application plane, malicious applications can insert fraudulent rules into the flow table of switches. This will cause the conflict rules in the network. Therefore, reliable connection must be established by creating authorization and authentication mechanisms between controllers and applications [4].

Man-in-the-middle (MITM) attack, which occurs between control plane and the data plane communication targets confidentiality and integrity principle of security. Both the control plane and data plane will be affected by this attack type. The data modification between the control plane and the data plane is one of the most important problems in SDN. SDN architecture brings discrete planes and using unencrypted protocols in the communication between these discrete planes can cause serious consequences. MITM attack, which performs in the second layer of the OSI reference model, allows eavesdropping or modifying the traffic flow between network resources such as server, router or switch and endpoint on the network. In this case, the attacker may modify flows on the switches or be able to add new flow rules [4]. Communication channel can be made more secure by the use of TLS which is a cryptographic protocol [6]. OpenFlow protocol supports TLS connection by default. Mutual authentication can be done by exchanging certificates between controllers and switches which are responsible for the transmission of network

packets. The attacker cannot view or modify the contents of messages when encrypted protocols are used.

Table 1. Summary of Attacks against SDN

Attack Surface	Attack Type	Attack Definition	Attack against Security Service
Application Plane	Interception, Modification	Unauthorized/Unauthenticated Applications	Confidentiality, Integrity
Application-Control Interface	Fabrication	Fraudulent Rule Insertion	Integrity
Control Plane	Interruption	DoS, DDoS	Availability
	Interception	Controller Hijacking, Unauthorized Controller Access	Confidentiality
Control-Data Interface	Interception, Modification	Man-in-the-Middle	Confidentiality, Integrity
Data Plane	Interruption	Flow Table Flooding	Availability

However, TLS/SSL and Public Key Infrastructure (PKI) has some weaknesses and these vulnerabilities could be exploited [7]. If an attacker can access control plane by benefiting the protocol vulnerabilities in communication, switches under its control can be used to launch DDoS attacks [3].

Unauthorized and unauthenticated applications target confidentiality and integrity principle of the security. There are many third-party applications which run at the application layer. Controller provides abstraction for the SDN applications and this enables the applications to read and write network state [4]. This situation poses a problem for the control of the network. The attacker can use the applications that cause unauthorized access to hide himself and access network resources and manipulate the operation of the network [4].

Administrative computers that are directly connected to the controller can cause an entry point into the network. If these computers have some vulnerability the attacker can use these vulnerabilities to get control of the computers to access the controller easily.

Other threat vectors can be classified as follows [3]:

- Failure to detect an error in time,
- Failure to obtain a reliable recovery point of the network during the network problems.

4. SDN Security Solutions

There are some comprehensive surveys [4], [8]-[11] on SDN and SDN security. In these papers, concept, architecture, core components, advantages, current challenges of SDN and SDN specific security threats and solutions are discussed in detail.

Despite the advantages provided by SDN architecture, it is necessary to review network security issues. In this section, some of the SDN security studies in the literature will be analyzed. These studies include:

- Prevention and mitigation of DoS and DDoS attacks,
- Authentication and authorization mechanisms,
- Development of network security applications such as IDS/IPS and firewall.

Some security measures are offered in [3] where also SDN-specific threat vectors are discussed. In case if only one controller is used and the controller is collapsed, there will not be a fault tolerance of the network and whole network may have collapsed which is called Single Point of Failure (SPOF). To avoid this situation creation of replication of controllers and applications is proposed. Usage of diversity of controllers is recommended against software bugs. Furthermore, it is stated that the switches in data plane must be able to keep in touch with another controller in case the controller is collapsed. In such a case, dynamic device association mechanism which provides the connection of switches with multiple controllers dynamically would tolerate the faults in the network.

Use of OpenFlow protocol leads to some security issues with it. For example, an attacker may send too many OpenFlow request and expose the control plane to DoS attack. This case will cause a bottleneck between control plane and data plane. So, the network will be unmanageable. Therefore, the central controller must be protected from DoS and DDoS attacks which could affect the entire network. A framework which is called AVANT-GUARD [12] has been developed for the purpose of enhancing security in OpenFlow networks. This framework is located in the data plane and consists of two modules named Connection Migration and Actuating Trigger. Intelligence is added to the data plane in Connection Migration and control plane is being more resistant against DoS attacks such as TCP SYN. This is carried out by analyzing the TCP sessions opened in the data plane. Connection Migration module decreases the interaction between control plane and data plane. The Actuating Trigger module provides the installation of the necessary flow rules. It is stated that this plug-in is also effective against network scanning attacks but does not provide any protection against DoS attacks in application-level and UDP or ICMP protocol-based attacks. It is expressed that after the attack is detected, control plane should be able to respond quickly. Therefore, quick access to the statistics belonging network traffic from data plane is of great importance. Within the scope of study, the statistics are collected from data plane and sent to the control plane. Accordingly, the behaviors detected as attack are prevented.

IDS and Anomaly Detection System (ADS) are used for the purpose of detecting threats in traditional network infrastructures. These security systems are generally located in Internet Service Providers (ISP) or backbone devices. This approach changes in SDN. These systems can be brought to the endpoints with SDN.

In a study [13], ADS is proposed for home and Small Office/Home Office (SOHO) networks using OpenFlow. Accordingly, an application which runs in NOX [14] controller is developed and implementation of four anomaly detection algorithms are described. This solution offers more efficient anomaly detection in home and SOHO networks than the ISP.

In another study [15], usage of central controller is proposed for the detection of DDoS attacks. Random distribution of incoming packets to the network is calculated in this method that runs on POX [16] controller. Entropy is used in order to calculate this probability. There are two components in DDoS detection. One of them is windows size and the other one is threshold. The window size is depended on time period and number of packets. Entropy calculates random distribution of incoming packet depending on window size. If the entropy value exceeds the predefined threshold value, traffic is determined as an attack. The proposed method can detect the attack within the first 250 packets of harmful traffic by using destination IP addresses. It is stated that attack detection rate for the predefined threshold value is %96. Furthermore, such parameters as destination IP addresses, window size and threshold value can be set to the desired values in real time according to the requirements of the controller. In this respect, it offers a flexible solution. Also, tests are performed and same results are obtained for TCP and UDP packets. It is stated that detecting DDoS in its early stages depends on tolerance of the controller and traffic properties.

In a recent work [17], a simple DoS prevention system is performed in SDN. A solution is offered against DNS DoS attacks using flow information obtained from each network device. Therefore, anomaly detection can be performed on each switch in the local area network. Also, the advantage of central management which is brought by SDN architecture is discussed.

Controller acts like a firewall in OpenFlow-based networks. The traffic is passed on the controller and analyzed. According to its result, passing of packets is allowed or rejected. In [18], it is discussed that a design acts like a firewall of each switch in data plane and sending of packets to the controller is not necessary. A flow-based distributed firewall prototype is developed in this work for developing a simple packet filtering firewall in SDN. The rule set is installed on each network device as flow entries. This firewall prototype creates a firewall object for each network device connected to the controller. Firewall object is connected to the related device without any delay. Each firewall object has an index number and stored in a list in order. The functions of each firewall object can be accessed through command line by index number in the list. Firewall can control the traffic by modifying flow tables of switches in data plane.

In [19], more than one controller usage is suggested for the purpose of protecting control plane from unauthorized access in SDN. Each switch in data plane can be managed by more than one controller using byzantine fault tolerance algorithm.

A security application kernel which is called FortNOX [20] is proposed for preventing fraudulent rule insertion that may be caused by malicious applications. FortNOX provides prioritizing the flow rules by performing role-based authorization. Furthermore, it detects a new flow rule which conflicts with an existing flow rule.

Security Enhanced Floodlight (SE-Floodlight) which is an extension of OpenFlow controller Floodlight is introduced in [21]. SE-Floodlight which is an improvement of FortNOX offers a Security Enforcement Kernel (SEK). It provides role-based authorization between control plane and OpenFlow applications in application plane. SE-Floodlight has a digital signature validation for each rule insertion. OpenFlow application is digitally verified by the SEK at runtime. Operations (making query, modification on the network or creating traffic flow rule) are permitted after the application is signed and validity is verified.

In [22], assignments of full priveleges for each OpenFlow application which cause unauthorized access problems are discussed. In this context, an isolation mechanism is proposed. The system which is called PermOF provides permissions with minimum priveleges for applications. PermOF enforce to perform these permissions in Application Programming Interface (API) entry of the controller. It is stated that this solution protects the network from unauthorized controller attacks.

In [23], a solution which is called Virtual Address Validation Edge (VAVE) is proposed for IP spoofing in OpenFlow/NOX architecture. VAVE is an application that runs on the controller. It performs source address validation against IP spoofing attacks. If any incoming packet does not match a rule in the flow table of OpenFlow switch, then first packet is sent to the NOX controller for the source address validation. If an IP spoofing is detected then controller adds a rule to the switch in order to stop incoming traffic from this source address. VAVE provides protection against data plane DoS attacks such as flow table flooding.

OpenFlow and sFlow is combined for anomaly detection and mitigation in [24]. This solution consists of collector, anomaly detection and anomaly mitigation modules. Flow statistics are gathered by using OpenFlow and sFlow protocols in the collector module. The statistics are analyzed and anomalies are identified in anomaly detection module. Flow-entries are inserted in the flow table of switches in order to neutralize malicious traffic in anomaly mitigation module. Flow-entries which are inserted have higher priority than any existing flow-entry in the flow table. These modules act as a feedback control loop. This architecture supports various algorithms such as statistical anomaly detection, machine learning-based anomaly detection and data mining-based anomaly detection according to preferred design. In this study, entropy-based algorithm is used. DDoS attacks, worm propagation and port scan attacks are detected successfully.

SDN, Network Functions Virtualization (NFV) and cloud computing technologies will play important role to meet the requirements of future mobile networks. In [25], multi-tier security architecture is presented to solve the security problems in the future of Software-Defined Mobile Networks (SDMN). This architecture consists of four components. Security is provided between the control and data plane communication by using Host Identity Protocol (HIP) and IPSec tunnelling techniques. Rule-based approach is used to protect the network to unwanted access, source address spoofing and DoS attacks. Software-Defined Monitoring (SDM) is used to detect and prevent security threats on the network. SDM uses Deep Packet Inspection (DPI) and traffic monitoring techniques. Synchronizing network security with the network traffic provides real-time information and necessary flow rules are installed to the flow tables of switches in the data plane.

5. Conclusion and Future Work

SDN bring a new generation networking approach. Traditional and cumbersome network architectures transform into the dynamic network architecture with SDN. Although SDN provides an open and programmable platform there are many problems to be solved in topics such as network security, routing algorithms, virtualization and load balancing. SDN must be designed in a good manner from the security perspective.

SDN security studies in the literature are mainly on prevention and mitigation of DoS/DDoS attacks. The controller should be used effectively and the traffic statistics should be analyzed. SDN can be used to prevent DoS/DDoS attacks. However, OpenFlow protocol may be misused to make such attacks and there are framework proposals to prevent those. Attacks have to be detected in time and proposed systems should be optimized for that. Artificial Intelligence (AI) solutions which analyze TCP sessions and detect some attacks are being developed. However, application-level or UDP/ICMP protocol-based attacks are not covered in detail.

The controller is the most important point of the SDN. Security of the controller should be satisfied and the rules should be controlled against fraudulent rule insertion. There are also some other solutions like having more than one controller to provide fault tolerance.

At this stage, we believe it is too early that we can say SDN provide a secure network infrastructure. There is much work needs to be done and more effort should be spent on SDN security to reach the SDN potential.

Cognitive Networks (CN) which exhibit intelligent behaviours will probably come out in the near future, we believe AI-based solutions in SDN security would be much more useful. Studies on integration of AI techniques with SDN, 4G/5G networks, Heterogeneous Networks (HetNets) and mobile networks can play an important role in the creation of CN. Processing big data with using AI techniques such as machine learning will allow the development of CN. CN will depend on information and be learning-based, exhibiting intelligent behaviors. With CN, it may be possible to develop networks which can learn from past data and decide automatically about encountered in future events. It will be possible to give specific services to the users with this intelligent network architecture. As a future work, we plan to represent these issues and propose new solutions in the following publications.

References

[1] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks". White Paper, 2013.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner. "OpenFlow: Enabling Innovation in Campus Networks". ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.

[3] D. Kreutz, F. M. V. Ramos and P. Verissimo. "Towards Secure and Dependable Software-Defined Networks". Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 55-60, 2013.

[4] S. Scott-Hayward, S. Natarajan and S. Sezer. "A Survey of Security in Software Defined Networks". IEEE Communication Surveys & Tutorials, vol. 18, no. 1, pp. 623-654, 2016.

[5] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes. "Software-Defined Networking Security: Pros and Cons". IEEE Communications Magazine - Communication Standards Supplement, pp. 73-79, 2015.

[6] Open Networking Foundation, "OpenFlow Switch Specification", Version 1.5.1, 2015.

[7] R. Holz, T. Riedmaier, N. Kammenhuber and G. Carle. "X.509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-Middle". 17th European Symposium on Research in Computer Security (ESORICS 2012), pp. 217-234, 2012.

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

[9] Y. Jarraya, T. Madi and M. Debbabi. "A Survey and a Layered Taxonomy of Software-Defined Networking". IEEE Communication Surveys & Tutorials, vol. 16, no. 4, pp. 1955-1980, 2014.

[10] S. Scott-Hayward, G. O'Callaghan and S. Sezer. "SDN Security: A Survey". IEEE SDN for Future Networks and Services (SDN4FNS 2013), pp. 1-7, 2013.

[11] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov. "Security in Software Defined Networks: A Survey". IEEE Communication Surveys & Tutorials, vol. 17, no. 4, pp. 2317-2346, 2015.

[12] S. Shin, V. Yegneswaran, P. Porras and G. Gu. "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks". 20th ACM SIGSAC Conference on Computer & Communications Security (CCS 2013), pp. 413-424, 2013.

[13] S. A. Mehdi, J. Khalid and S. A. Khayam. "Revisiting Traffic Anomaly Detection using Software Defined Networking". 14th International Conference on Recent Advances in Intrusion Detection (RAID 2011), pp. 161-180, 2011.

[14] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown and S. Shenker. "NOX: Towards an Operating System for Networks". ACM SIGCOMM Computer Communication Review, vol. 38, no. 3, pp. 105-110, 2008.

[15] S. M. Mousavi and M. St-Hilaire. "Early Detection of DDoS Attacks against SDN Controllers". IEEE International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, pp. 77-81, 2015.

[16] S. Ramadona, B. A. Hidayatulloh, D. F. Siswanto and N. Syambas. "The Simulation of SDN Network Using POX Controller: Case in Politeknik Caltex Riau". 9th International Conference on Telecommunication Systems, Services and Applications (TSSA), pp. 1-6, 2015.

[17] G. Akin, E. Karaarslan, O. Buk and E. Ucar. "SDN Architecture Fundamentals & DoS Prevention Basics: A Case Study with OpenFlow". International Scientific Conference (UNITECH 2015), Gabrovo, 2015.

[18] J. G. V. Pena and W. E. Yu. "Development of a Distributed Firewall Using Software Defined Networking Technology". IEEE 4th International Conference on Information Science and Technology, pp. 449-452, 2014.

[19] H. Li, P. Li, S. Guo and S. Yu. "Byzantine-Resilient Secure Software-Defined Networks with Multiple Controllers". IEEE International Conference on Communications (ICC 2014) - Communication and Information Systems Security Symposium, pp. 695-700, 2014.

[20] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson and G. Gu. "A Security Enforcement Kernel for OpenFlow Networks". First ACM SIGCOMM Workshop on Hot Topics in Software Defined Networks, pp. 121-126, 2012.

[21] P. Porras, S. Cheung, M. Fong, K. Skinner and V. Yegneswaran. “Securing the Software-Defined Network Control Layer”. Network and Distributed System Security Symposium (NDSS), pp. 1-15, 2015.

[22] X. Wen, Y. Chen, C. Hu, C. Shi and Y. Wang. “Towards a Secure Controller Platform for OpenFlow Applications”. Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 171-172, 2013.

[23] G. Yao, J. Bi and P. Xiao. “Source Address Validation Solution with OpenFlow/NOX Architecture”. 19th IEEE International Conference on Network Protocols (ICNP), pp. 7-12, 2011.

[24] K. Giotis, C. Argyropoulos, G. Androulikadis, D. Kalogeras and V. Maglaris. “Combining OpenFlow and sFlow for an Effective and Scalable Anomaly Detection and Mitigation Mechanism on SDN Environments”. Computer Networks, vol. 62, pp. 122-136, 2014.

[25] M. Liyanage, I. Ahmad, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. de Oca, A. Valtierra and C. Jimenez. “Security for Future Software Defined Mobile Networks”. IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2015), pp. 256-264, 2015.