Security Issues in Software Defined Networks

Mushtaque Ahmed[1], Syeda Sadaf Fatima[1], Arsal Ahmed Khan[1] , Syed Ali Sheeraz Jafri[1]

Abstract— Software defined networks (SDN) has consider to be a new network architecture for managing the network dynamics via software-enabling control. SDN promotes a large number of network applications where security is an important factor. For security, SDN is a new paradigm emergent stage in the realm of production scale networks. Centralization of network control introduces a new level of flexibility for network administrators and programmers. Security is a significant factor for contributing the consumer resistance for implementation of SDN architecture. Without addressing the issues inherent from SDNs centralized nature, the benefits in performance and network configurative flexibility cannot be harnessed. This research presents security issues in SDN and specific review of SDN architecture along with the challenges faced. Furthermore, this paper explicitly discusses working mechanics of SDN and also analyzes its security issues and countermeasures. In a nutshell, it provides the SDN security features of uniqueness and openness. Moreover, this manuscript illustrates the SDN security issues from three aspects: data layer, control layer and application layer. Some countermeasures are also explained to .address the security threats at each layer

Keywords—SDN, Security Issues, Networks, Privacy, Data Link Layer

INTRODUCTION

Software defined networking (SDN) is one of the key network architectures to simplify management of network and enable communication network modernization. A basic feature of SDN architecture is the physical separation of the control layer from the data layer. The centralized control function logically maintains network status and keeps the network state and provides the forwarding plane with instructions. New control functions can be implemented in SDN by writing to the control plane software based logic, which uses standard interfaces to implement the decision logic in the data layer. In the control layer, a network operating system (NOS) maps the whole network to various services and applications at the top of the control layer [1, 2]. SDN is promising to clarify the deployment and operation of the network, as well as reducing the total business and carrier network management costs through the provision of programmable network services. Some basic challenges of SDN are reliability, scalability, interoperability, and security.

The SDN is ground-breaking field in computer networks and virtualization. There are fewer forums and industries that are gradually working on identifying and ad dressing a number of issues. Some of the key areas of concern for safety professionals in SDN purists are highlighted below. SDN controller is responsible for most network -related functions collection of network information, configuration and selection of routes. However, it is potential attacker target due to its programmable nature. In addition, cloud computing platforms/ applications allow attackers to easily compromise and seize the SDN controller functionally, resulting in the entire network being paralyzed. SDN is also vulnerable to several threats due to the open programmable interfaces. Open interfaces can also lead to the interface being exploited in such a way that an opponent can embed malicious code that could cause an interface to behave abnormally. Therefore, the open programmable interfaces need to be scrutinized carefully [3, 4].

The main objectives of this paper is given below”

- Comprehensive review and software defined network (SDN), its constraints and challenges.
- Comparative analysis some of the mechanisms proposed as mitigations against security threats.
- Provide countermeasures by which security of SDN can be enhanced.

The remainder of the paper is organized as follows. Section 2 explains the Software defined network Architecture. In, Section 3 the challenges are discussed. The security issues in SDN are demonstrated in the section 4. Section 5 presents open research directions. At last, the conclusion and future directions are given in section 6.

Software-Defined Networks Architecture

The Open Networking Foundation (ONF) has provided definition of SDN that is most obvious and well received. “In the SDN architecture, the control and data plane are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the application” [5]. The SDN architecture is dividing into three layers, known as data forwarding or infrastructure layer, the control layer and the application layer, as shown in Figure.1.

[1] ILMA University Karachi, Pakistan
Email: engrmushtaque@hotmail.com

Data Layer

The data layer consist of numerous SDN switches that are connected physically via wired or wireless media. Every switch is responsible for transmitting network packets and has a flow table, which accommodate tens of thousands of rules for formulating decisions on transmission [6]. The data plane's main function is to forward the packets as per rules/ policy assigned.

Control Layer

The core portion of SDN architecture is the control layer. It composed of SDN controllers which provide furnished centralized control. The SDN controller connects to the switch by default south-bound API, for example Open Flow, and have a global view of it infrastructure layer of the whole network topology, i.e. switches and connections [7,8].

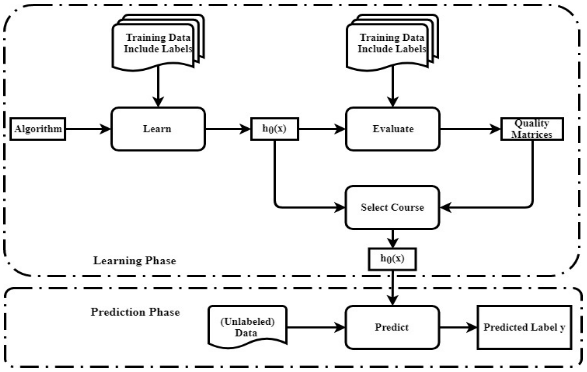

Figure 1. Proposed model of Machine learning

Application Layer

The application layer enables network operator's rapid reaction to the various company needs. To work in addition to the SDN controllers, unconventional application software has been developed to meet different applications, such as virtualization of network, detection of topology, traffic surveillance, load equilibrium, improvement of security, mobility management and so on. The application layer converse with the control layer via north-bound APIs [9].

SDN CHALLENGES

SDN promises network deployment services that are flexible, cost-effective and managed. However, many challenges still must be addressed. Some of the most important challenges are discussed below:

Reliability

The failure of the SDN controller could lead to one-point failure, which is why network topology must be smartly configured and validate to preventing failure and increasing accessibility. Currently network devices or routers fails in current networks, without interruption, traffic can pass via other devices the progression of flow. With centralized architecture of SDN controller, however, the controller breakdown can collapse the entire network without standby controller [10].

Scalability

In SDN networks, a control plane plays a vital role. A complete SDN network is divided into various logical layers. An application layer exists at the top of the stack. Application layer supports SDN applications like Open Flow to program the SDN controller in the control plane. Scalability implies two different aspects. One is to increase the number of SDN controllers and the other is to increase the number of network nodes [11].

Security

The extensive network spreading to research centers everywhere, including industries, makes it hard to make sure adequate security. Different domain has various security requirements that needed to be ensured for proper network deployment. SDN controller is responsible for most network-related functions, like network information gathering, configuration and selection of routes. However, it is potential target for attackers due to its openness. Because everything in the network can be programmed centrally, hackers only need access to the network controller to modify the data. Consequently, SDN must ensure secure communication through the incorporation of security technique [12, 13].

Interoperability

In paradigm shift from conventional networks to SDN networks, interoperability is one of the major challenges. It is necessary to synchronize the migration from one system to another to make the existing network compatible with the newly adopted system. SDN enabled capabilities should be the components used for the SDN network. However, many organizations have developed mature SDN networks despite this fact [14, 15].

SECURITY ISSUES IN SOFTWARE DEFINED NETWORKS

Some separating the layers and aggregating the functionality of the control layer to a centralized system may be critical for future networks; however, new security challenges are also created. With the progressive deployment of SDN technologies, the list of security issues in SDN is expected to grow. These issues need to be highlighted in order to take full advantage of SDN, so that appropriate security measure can be taken proactively. From a fundamental point of view, SDN security vulnerabilities are concentrated around the main areas of data layer, control layer and application layer. Hence security issues existing in the three SDN layers are described below.

Data Layer Security Issues

The routers and switches are dump forwarding devices. These forwarding data planes forwarding entities are the basis for controller decisions. SDNs architecture and operating principles comply with Open Flow specifications. In Open Flow networks, the Open Flow controller install the flow rules in the flow tables of the Open Flow switch. These flow rules can be installed before sending packets from a new host (proactive rule installation) or from a new host on the first packet (reactive rule installation). A switch has a limited number of flow tables that install the flow rules based on controller's network view. Since the decision-making capacity has been removed from the switches, the first and basic security challenge is to recognize and differentiate genuine flow rules from false and malicious rules. The second challenge is based on a switch's number of flow entries. In Open Flow, until the controller issues flow rules, a switch has to buffer unsolicited (TCP/UDP) flows, this makes the data layer prone to saturation attacks. In SDN, the security of the control plane affects the data layer directly. If a controller is compromised, it will compromise the entire network of a variety of data layer nodes. In split architecture like SDN, the data layer becomes practically offline if a switch does not receive forwarding instructions from the control because the control plane has failed or the control plane has been disconnected. The switch controller connection can be a favorable choice to attack. Separation of control and data layer can allow an attacker to stealthily change flows by manipulating Open Flow rules, leading to various active attacks, like man-in-the-middle and black-hole attacks. Complexity in setting up and using TLS as an option can vulnerability of the control channel to different types of attacks. In addition, SDN can enable the routing of network traffic via a centralized firewall to secure the data layer. However, it can take long enough to monitor messages between a switch and a controller to exhaust the switch resources with false flows leading to flooding or a compromise Dos attack [16, 17].

Control Layer Security Issues

In SDN, a centralized entity to take decisions is the control layer i.e. Open Flow controller. Therefore, because of its pivotal role, can be highly targeted at the controller is responsible for compromising the network or carrying out malicious network activities [18]. The control layer (i.e. Open Flow controllers), and their security have a direct influence on the data layer in the SDN architecture. If a controller is compromised, the entire network may be affected, including a potentially a lot of switches. This is because if a switch is unable to receive forwarding rule from the controller, it will not be able to transmit packets. The controller can thus become a main target for attackers because of its important role [19].

Application Layer Security Issues

Attacker can manipulate network configuration in the application layer, seize network resources, and steal network information and spyware or malware programs are inserted in the application, this may interfere with the normal operation of the control layer and influence the network's reliability and availability [20]. While Open Flow may use algorithms for security detection applications, they are not required. The various applications created by many companies use various programming languages could result in conflicts of interoperability or security policy [21].

Data Layer Security Threats

Security threats existing in infrastructure layer as described below. The short description of these threats are presented in Table 1.

Table 1: Security Attacks at Data Layer

Type of Threats	Caused/Possible Reason
Fake Flows	Malicious applications produce false flow rules
Table and Buffer Overflows	Storage constraints, attacking traffic saturates table and buffers
Unauthorized Access	The "data layer" only depends on the "control layer" making the security of the "data plane" dependent on the security of the controller
Flow Rule Discovery	Due to slow forwarding policy of the network
TCP-Attacks at level	TLS is available to TCP attack at a level
Flow Rule Modification	Malicious switch change the data or flow rule to some other node
Attacks by flooding	Flow tables and OpenFlow switches store a lean flow rules

Fake Flows

Flawed devices or clients can attack switches and controllers. Components of the network are used for Dos propagation. For each client, number of inserting points are stored, which can be attacked by fake data flow [22].

Table and Buffer Overflows

SDN switches that are restricted in terms of storage capacity maintain the flow table and flow buffer. If an attacker node generates an enormous amount of irregular traffic with unknown destinations, new rules will be inserted into the flow table, thus compromising, the flow table storage capacity is saturated by irregular traffic, legitimate traffic is not properly transmitted since there would not be any more ability to insert new rule [23]. Flow buffer attack is another target. Before searching for the rule or inserting new rule, the forwarded packets must be buffered in flow buffer. An attack can flood large quantities of packets to be switched to buffer, resulting in buffer over flow that leaves no space for legitimate packets to result in packet drop [24].

Table and Buffer Overflows

SDN switches that are restricted in terms of storage capacity maintain the flow table and flow buffer. If an attacker node generates an enormous amount of irregular traffic with unknown destinations, new rules will be inserted into the flow table, thus compromising, the flow table storage capacity is saturated by irregular traffic, legitimate traffic is not properly transmitted since there would not be any more ability to insert new rule [24]. Flow buffer attack is another target. Before searching for the rule or inserting new rule, the forwarded packets must be buffered in flow buffer. An attack can flood large quantities of packets to be switched to buffer, resulting in buffer over flow that leaves no space for legitimate packets to result in packet drop [25].

Unauthorized Access

One of the distinctive feature is logically centralized network control. Multiple vendor network applications can communicate with controller pool. However, if an attacker compromised a controller or an application, the network resources could be accessed and the network controlled [25].

Flow Rule of Discovery (Side Channel Attack)

Side-channel attacks use a control plane's processing time to learn network setups. In these attack, particularly an attacker creates various types of timing probes and sends the Open flow networks a stream test and some familiar effects baseline packet [25].

TCP-Level Attacks

Complexity in configuration and using TLS as an option that make the channel vulnerable to different types of attack. Any downstream switches can be seized and fine-grained eavesdropping attacks executed by the attacker immediately. In addition, the use of TLS does not deliver TCP-level protection and is therefore appropriate to TCP-level attacks [26].

Flow Rule Modification

The controller is capable programming network devices for SDN traffic flow control. If an attacker could seize the controller, then the entire system would be controlled effectively, in network devices, the attacker can put or change the flow rules from this privileged position, to the advantage of attacker, which would allow packets to be controlled over the network [26].

Flooding Attacks

Attacker can create traffic loads excessively heavy to overwhelm the whole network resources. It is easy to control these attacks using software defined networks [27].

Control Layer Security Threats

Security threats are also existing on control layer as we discussed above. The short description of control layer threats is presented in Table 2.

Table 2: Security Attacks at Control Layer

Type of Threats	Caused/Possible Reason
Threats from Application	Due to malicious applications and open programming interface of the controller
Threats based on multi – controller distributed	Difficult consolidation for multi – tenant and distribution of the access of control in consistent multi – controller configuration
Hijacked/ Rogue Controller	Full control, flow and defined policies of the SDN network
Black-hole Attack	Nodes in the network give false information on the controller route
Scalability and Availability	Intelligence centralization in one operation most likely it will have challenges in terms of scalability and availability
Man in the middle of the attack	Without TLS support, the communication channel is not secure
Controller-switch Communication Flood	Due to the limited memory resources or storage capacity

Threats from Applications

The application at the top of the control plane (in some cases third-party applications) pose SDN controller's security threats. Application in the higher APIs to obtain network information on before accessing network resources, these types of applications must be scrutinized. The various applications may have different functional requirements and require them to customize security policy. For example, application for intrusion detection need to inspect the packet header field, whereas applications for load balancing may require network statistics such as packet counter values to balance the load [27].

Threat based on Distributed Multi Controllers

Multiple physical controllers that manage the network should be transparent to the "data layer" instead of a single one, this mean that controller must emerge as a single controller throughout network. In this circumstance, the application which spread multiple control network domain will have to address many security issues during network information transmission, i.e. authorization, authentication and private issues [27].

Hijacked/ Rouge Controller

From one point, SDN control the entire network makes it up the SDN architecture's most important part. If an attacker can compromise the controller, it can control the whole network and control the action of the controller and change the flow entries, for example, stopping certain types of packets from to reach their destination, redirecting to malicious infrastructure node [28].

Black – Hole Attack

There might also be a black hole type attack where a node settles between the targeted device and the controller and directly drops any packet it receives without transmitting it to the controller. This leads to a failure of network communication and makes legitimate user's services inconvenient [28].

Man-in-the-Middle Attack

If there is a malicious node between the controller and the data path on the data layer, a man - in - the middle attack occurs. An agent node insert (man-in-the-middle) between source and destination node used to intercept and change communication data without having to be detected by any side of the communication. The man-in-the-middle node can change content instead of transmitting the messages directly to the controller (or vice versa) [29].

Controller Switch Communication Flood

The SDN architecture introduces one of SDN's core security weakness; the combining core controller and control and data plane separation, because of the controller's communication path with the network, the controller could be flooded by an attacker device with packets that require a decision on flow rules and make the controller inaccessible to legitimate users [28, 29].

APPLICATION LAYER SECURITY THREATS

Application layer short description of security threats are presented in Table 3.

Table 3: Security Attacks at Application Layer

Type of Threat	Caused/Possible Reason
Illegal Access	Software vulnerabilities of the controller and by passing of the authentication mechanism
Security Rules & Configuration Conflicts	Access control and accountability contrast for different software and application software variety
Lack of Access Control and Accountability	Difficult to implement third-party control of access and accountability
Configuration Issues	Incorrect use of security features
Insertion of fraudulent flow rules	Malicious or compromised applications can create false flow rules and can hardly check whether an application is compromised
Resource Attacks	A malicious application can execute removal of controller instance from the system command
Policy Enforcement	Incorrect use of security features

Illegal access

Controller running application are very expandable and flexible, with the privileges of accessing network resources and controlling network behavior. Most of these application is developed by third parties, not vendors of controllers. Consequently, the absence of standardized safe SDN application mechanism causes security threats [29].

Security rule and configuration conflicts

The application layer needs security applications to access the controller's security interfaces to deliver a wide range of services on the network. Conflicts may arise between security rules along with the complexity of the applications, the result is network services confusion and management complexity [28,29].

Lack of access control and accountability

Access control and accountability for nested application is a real challenge for SDN (e.g. Application using a different application instance). SDN applications can it be either SDN conscious or SDN conscious. Application with SDN awareness can find and communicate with the SDN controller directly while, ignoring SDN applications communication indirectly with application datagrams in specific formats [30].

Configuration Issues

Access Implementing network policies and configurations like Transport Layer Security (TLS) is important in SDN. However, all layers in SDN architecture may be affected by misconfiguration and overlooking security features [30].

Fraudulent Flow Rules Insertion

Controller-running applications have access to network resources and may control network behavior. The issue of malicious applications arises due to the SDN framework allowing third-party applications to be integrated using northbound APIs. However, the network may be controlled by a malicious or compromised application. Likewise, a poorly or buggy designed application involuntarily introduce network vulnerabilities [30].

Resource Attack

Malicious application can exhaust exorbitant and critical system resources along with memory and CPU, thus affecting the legitimate performance of application and controller itself. In addition, a malicious SDN application can execute exit and dismiss control instances [28-30].

Policy enforcement

SDN enable us to easily program the network and create dynamic flow policies. Indeed, this advantage can also lead to vulnerabilities in security. Inconsistencies need to be detected with multi-application or multi-device policies to resolve policy conflicts [29-31].

OPEN RESEARCH ISSUES

Software Defined Networks (SDN) is become apparent architecture satisfactory for today's dynamic, high applications bandwidth. It could help organizations to speed up the deployment of applications and reduce IT costs through policy allowing automation of workflow. Many research issues which are not yet well investigated and need to be addressed through research like Application-level DDos attacks using SDN, Mobile DDos attacking using SDN, Implement Multiple Locations Defensive across27-layer traffic analysis, cooperate among the key defensive point and build a DDos attacks tolerant system using SDN. Another research issue to modify the Open Flow procedure to decrease the number of controller messages and the OF switches to reduce congestion on the control channel. A lightweight and easy solution can be designed to observe and mitigate Dos attacks in SDN with the Block malicious traffic, minimum additional traffic, avoid redundant processing and keep the core function alive feature. The potential attacks that a compromised forwarding device can bring against various technologies that are carried into SDNs like Software Defined Clouds, there is a need to focus much more on the importance of security for SDN planes.

CONCLUSION AND FUTURE WORK

This research work is based on survey of Security issues in Software Defined Networks (SDN), and specific review of SDN architecture and challenges also explained how SDN works and analyzed its security issues and countermeasures, and give SDN great security features of uniqueness and openness. Moreover, presented the SDN security issues from three aspects: data forwarding layer, control layer and application layer. Some countermeasures are also presented to address the security threats at each layer.

In this survey, the evidence of the two sides of the SDN security coin has been presented; that is possible to improve network security using the characteristics of SDN architecture, and that the SDN architecture introduces security issues. The contribution in that work on enhancement to network security via SDN is more mature. In future, we aim to implement SDN standard, Open Flow, and develop a small real SDN based network. Moreover, we also aim to develop a secure data forwarding approach in order to increase the secure data dissemination. Several other attacks will be analyzed in the future and countermeasure can be provided to deal with attacks effectively.

REFERENCES

[1] Varadharajan, V., Karmakar, K., Tupakula, U., & Hitchens, M. (2019), "A Policy-Based Security Architecture for Software-Defined Networks." Transactions on Information Forensics and Security, 14(4), pp. 897-912.

[2] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016), "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: Asurvey, some research issues, and challenges." Communications Surveys & Tutorials, 18(1), pp. 602-622. Ieee

[3] Saxena, M., & Kumar, R. (2016, March), "A recent trends in software defined networking (SDN) security." In 2016 3rd International Conference on Computing for Sustainable Global Development pp. 851-855. IEEE.

[4] Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015), "A survey on software-definednetworking." Communications Surveys & Tutorials, V. 17(1), pp. 27-51.

[5] Dayal, N., Maity, P., Srivastava, S., & Khondoker, R. (2016), "Research trends in security and DDoS in SDN." Security and Communication Networks, 9(18),

pp. 6386-6411.

[6] Ahmed, A., Manzoor, A., Halepoto, I. A., Abbas, F., & Rajput, U. (2018), “Security Threats and Countermeasures in Software Defined Networks.” International Journal of Computer Science and Network Security, 18(4), pp. 69-74.

[7] Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J. & Rao, N. (2013), “Are we ready for SDN? Implementation challenges for software-defined networks.” Communications Magazine, 51(7), pp. 36-43.

[8] Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2018), “Software-defined network (sdn) data plane security: Issues, solutions and future directions.” arXiv preprint arXiv:1804.00262.

[9] Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015), “Security in software defined networks: A survey.” Communications Surveys & Tutorials, 17(4), pp. 2317-2346.

[10] Shu, Z., Wan, J., Li, D., Lin, J., Vasilakos, A. V., & Imran, M. (2016), “Security in software-defined networking: Threats and countermeasures.” Mobile Networks and Applications, 21(5), pp. 764-776.

[11] Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., & Khan, S. U. (2016), “Secure and dependable software defined networks.” Journal of Network and Computer Applications, V. 61, pp. 199-221.

[12] Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016), “A survey of security in software defined networks.” Communications Surveys & Tutorials, 18(1), pp. 623-654. Ieee

[13] Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2017, July), “Security in software-defined wireless sensor networks: Threats, challenges and potential solutions.” In 2017 IEEE 15th International Conference on Industrial Informatics (INDIN) pp. 168-173. IEEE.

[14] Kreutz, D., Ramos, F. M., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015), “Software-defined networking: A comprehensive survey.” 103(1), pp. 14-76. IEEE

[15] Spooner, J., & Zhu, S. Y. (2016), “A review of solutions for SDN-exclusive security issues.” International Journal of Advanced Computer Science and Applications (IJACSA).

[16] Scott-Hayward, S., O’Callaghan, G., & Sezer, S. (2013, November), “SDN security: A survey.”SDN for Future Networks and Services (SDN4FNS) pp. 1-7. IEEE.

[17] Gao, S., Li, Z., Xiao, B., & Wei, G. (2018), “Security threats in the data plane of software-defined networks.” IEEE network, 32(4), pp. 108-113.

[18] Li, W., Meng, W., & Kwok, L. F. (2016), “A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures.” Journal of Network and Computer Applications, V. 68, pp. 126-139.

[19] Rawat, D. B., & Reddy, S. R. (2017), “Software defined networking architecture, security and energy efficiency: A survey.” Communications Surveys & Tutorials, 19(1), pp. 325-346. Ieee

[20] Porras, P. A., Cheung, S., Fong, M. W., Skinner, K., & Yegneswaran, V. (2015, February), “Securing the Software Defined Network Control Layer.” In NDSS

[21] Yan, Q., & Yu, F. R. (2015), “Distributed denial of service attacks in software-defined networking with cloud computing.” Communications Magazine, 53(4), pp. 52-59.

[22] Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015), “Software-defined networking security: pros and cons.” Communications Magazine, 53(6), pp. 73-79. Ieee

23] Feghali, A., Kilany, R., & Chamoun, M. (2015), “SDN security problems and solutions analysis.” International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS) pp. 1-5. IEEE.

[24] Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014), “Software defined networking: State of the art and research challenges.” Computer Networks, V. 72, pp. 74-98.

[25] Shin, S., Xu, L., Hong, S., & Gu, G. (2016), “Enhancing network security through software defined networking (sdn).” 25th International Conference on Computer Communication and Networks (ICCCN) pp. 1-9. IEEE

.

[26] Prakash, A., & Priyadarshini, R. (2018), “An Intelligent Software defined Network Controller for preventing Distributed Denial of Service Attack.” Second International Conference on Inventive Communication and Computational Technologies (ICICCT) pp. 585-589. IEEE.

[27] Li, Yong, and Min Chen. “Software-defined network function virtualization: A survey.” IEEE Access 3 (2015): 2542-2553.

[28] Duan, Xiaoyu, and Xianbin Wang. “Authentication handover and privacy protection in 5G hetnets using software-defined networking.” IEEE Communications Magazine 53, no. 4 (2015): 28-35.

[29] Dotcenko, Sergei, Andrei Vladyko, and Ivan Letenko. “A fuzzy logic-based information securitymanagement for software-defined networks.” In 16th International Conference on Advanced Communication Technology, pp. 167-171. IEEE, 2014.

[30] Chen, Min, Yongfeng Qian, Shiwen Mao, Wan Tang, and Ximin Yang. “Software-defined mobile networks security.” Mobile Networks and Applications 21, no. 5 (2016): 729-743.

[31] Alsmadi, Izzat, and Dianxiang Xu. “Security of software defined networks: A survey.” Computers & security 53 (2015): 79-108.