Received: 12 November 2018 | Revised: 6 March 2019 | Accepted: 21 March 2019
DOI: 10.1002/cpe.5300

WILEY

SPECIAL ISSUE PAPER

A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers

Tao Han[1] | Syed Rooh Ullah Jan[2] | Zhiyuan Tan[3] | Muhammad Usman[4] | Mian Ahmad Jan[2] | Rahim Khan[2] | Yongzhao Xu[1]

[1]DGUT-CNAM Institute, Dongguan University of Technology, Dongguan, Guangdong, China
[2]Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, Pakistan
[3]School of Computing, Edinburgh Napier University, Scotland, UK
[4]Department of Computer Science and Software Engineering, Swinburne University of Technology, Hawthorn, Australia

Correspondence
Mian Ahmad Jan, Department of Computer Science, Abdul Wali Khan University Mardan, Mardan-23200, Pakistan.
Email: mianjan@awkum.edu.pk

Funding information
International Scientific and Technological Cooperation Project of Dongguan, Grant/Award Number: 2016508102011; Science and Technology Planning Project of Guangdong Province, Grant/Award Number: 2016A020210142

Summary

Software Defined Network (SDN) and Network Virtualization (NV) are emerged paradigms that simplified the control and management of the next generation networks, most importantly, Internet of Things (IoT), Cloud Computing, and Cyber-Physical Systems. The Internet of Things (IoT) includes a diverse range of a vast collection of heterogeneous devices that require inter-operable communication, scalable platforms, and security provisioning. Security provisioning to an SDN-based IoT network poses a real security challenge leading to various serious security threats due to the connection of various heterogeneous devices having a wide range of access protocols. Furthermore, the logical centralized controlled intelligence of the SDN architecture represents a plethora of security challenges due to its single point of failure. It may throw the entire network into chaos and thus expose it to various known and unknown security threats and attacks. Security of SDN controlled IoT environment is still in infancy and thus remains the prime research agenda for both the industry and academia. This paper comprehensively reviews the current state-of-the-art security threats, vulnerabilities, and issues at the control plane. Moreover, this paper contributes by presenting a detailed classification of various security attacks on the control layer. A comprehensive state-of-the-art review of the latest mitigation techniques for various security breaches is also presented. Finally, this paper presents future research directions and challenges for further investigation down the line.

KEYWORDS

controller, denial of service attacks, link flooding attacks, malicious injection attacks, software defined networks, spoofing attacks

1 | INTRODUCTION

By 2020, it is expected that the Internet of Things (IoT) will incorporate nearly 50 billion real-world physical devices. Numerous solutions have been proposed and implemented to deal with an increased number of connected devices; however, they were not designed while keeping in mind the evolution of IoT-enabled devices.[1] The projected growth in the number of connected devices means that the existing wired/wireless and mobile networks need to evolve to become more intelligent, secured, scalable, and resource-efficient to incorporate them. The scalability of these networks is essential to manage the diverse nature of data generated by these devices. Software Defined Network (SDN) and Network Virtualization (NV) are the two promising technologies to serve as key enablers for the IoT of the near future.[2] Network virtualization allows the service providers to form separate and isolated virtual networks by enabling them to share physical resources. It offers a reduced cost by sharing the network infrastructure and improved time to market for novel applications. For future IoT networks, NV will be a crucial feature that will enable differentiated Quality-of-Service (QoS) for the diverse usage scenario and quick introduction of new applications and services.

The SDN, on the other hand, is a novel programmable architecture that simplifies the control and management of next-generation networks. It has changed the way a network operates by decoupling the data plane from the control plane and manages the whole network through a centralized control intelligence,[3-5] also known as SDN controller. An SDN controller is the backbone of an SDN architecture because it performs the essential operations related to the control and management of the underlying networks.[6-10] It is responsible for the establishment and

termination of data flows at the data plane, based on various data handling policies. It implies that the network elements at the data plane are simple forwarding devices, managed and controlled by the controller. The SDN controller can assign the required resources by configuring the network policies as per requirements of an application and network hardware at the data layer. Moreover, it provides an up-to-date view of the network and topology by collecting various statistical data using open APIs. This allows network managers to apply different network-wide policies such as redirection of traffic and blocking certain packets, at the packet level without actually touching the underlying network. These attributes brought substantial managerial benefits. Although SDN has brought significant changes to the way a network operates, the single-point dependency remains a prime and challenging security issue. Compromising the security of the controller means that the safety of the whole network is at stake.

Despite all the benefits offered by the SDN, there are numerous challenging issues that need to be tackled prior to its widespread adoption. Some of these challenging issues include but are not limited to scalability, fault tolerance, communication overhead, security provisioning, and single point dependency. The centralized nature and a single point dependency of the SDN controller is its strength. However, at the same time, it is its weakness from a security point of view. For instance, if the security of the controller is compromised, protection of the whole network is compromised, and the controller becomes vulnerable to a wide range of attacks. According to the work of Hinden,[11] "why take over the hosts when you can take over the whole network?" It is, therefore, crucial to secure not only the controller but also all the layers and interfaces while designing an SDN architecture. Security needs to be delivered as a service to protect the network resources from unauthorized access and attacks. This is because the security was not initially considered while designing an SDN architecture.[12,13] Thus, an SDN design requires a simple, scalable, cost-effective, and in particular, an efficient and secure architecture. In an SDN architecture, the control plane is particularly vulnerable to a wide range of security attacks due to its strategic and centralized nature.[14-16] These attacks include but are not limited to DoS, DDoS, spoofing, and malicious injection attacks,[12,17-20] as depicted in Figure 1. Besides these attacks, an attacker may exploit various vulnerabilities in the Open Flow Protocol, the most commonly used protocol at the southbound interface that facilitate communication between the control and data layers of an SDN architecture.[21,22] Securing the controller remains a key challenging area due to it single point failure for the research community in the years to come.

Based on the literature, various SDN-related survey papers are available exploring various dimensions of SDN security. For instance, SDN and its evolution,[23-27] while only a few surveys focus on the security of SDN.[19,24,27-36] Among them, the work of Scott-Hayward et al[33] in 2013 first discussed several security challenges in SDN without an analysis model. Additionally, they did not provide a discussion of the potential countermeasures. Furthermore, the work of Alsmadi and Xu[37] conducted a survey on SDN security by means of STRODE threats model, which discuss various security issues to the overall SDN architecture. Furthermore, in the work of Ahmad et al,[28] the authors studied various security challenges experienced by the protocols and architecture of an SDN architecture. This work further explored the existing solutions for mitigating various attacks and, at the same time, classified these solutions in term of scalability, reliability, security, and performance. Another valuable work in this regards was presented in the work of Yan et al.[36] The authors surveyed various DDoS attacks targeting an SDN-based cloud architecture. An in-depth analysis of emerging trends, features, and mitigating techniques for these attacks were also explained. In the work of Scott-Hayward et al,[19] the authors provided an overview of various security challenges, introduced at each layer of an SDN paradigm. They suggested various security enhancement techniques to address the aforementioned challenges. In other works,[27,38,39] the authors investigated numerous security challenges faced by the southbound interface, ie, OpenFlow. Moreover, various solutions were proposed to overcome such challenges. A layered taxonomy of various vulnerabilities that target each layer of an SDN architecture was also discussed. Moreover, the works of Bawany et al[29] and Xiao et al[35] considered only one type of attack, ie, DDoS attack, data plane security, and challenges[30,34] or discussed security challenges of the whole SDN architecture where only a section is dedicate to the security of the SDN controller and are thus limited in their scope and completeness as they are not controller exclusive.[19,23,24,27,40] Unlike these surveys, this paper is first of its kind that provide an in-depth analysis of various security issues related to SDN controller along with their countermeasures. A systematic taxonomy of control plane agnostic attacks, ie, Denial of Service (DoS), Distributed DoS, Spoofing attack, and Malicious Injection attacks is also presented. Furthermore, this survey provides an insight into various solutions for the detection and mitigation of the aforementioned attacks along with their strength and weaknesses with regard to an SDN controller. Because a secure controller implies a secure SDN network controller, failure of the controller is

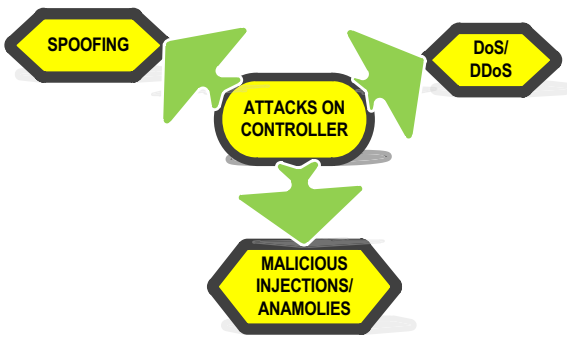

FIGURE 1 Security attacks on an SDN controller

failure of the whole SDN architecture. Due to this dependency, it is mandatory to know various controller agnostic attacks, so as to protect it as well as for its widespread adoption.

This survey paper will help us to answer questions like when, why, and which solutions are the most appropriate to tackle a particular type of attack on the controller, due to unlimited number of mitigation techniques available in the literature. It thus helps the researchers in choosing the most appropriate technique for the future on one hand, while suitable choice for practitioner on the other hand in order to fully benefit from this technology along with making SDN a promising, trustable, dependable, and secure architecture for the years to come. The main contributions of this paper are as follows.

1. This paper comprehensively reviews the existing state-of-the-art security threats, vulnerabilities, and issues at the control plane.
2. This paper presents an up-to-date thematic taxonometric classification of various security attacks on the control layer of an SDN architecture.
3. A detailed analysis of these attacks along with their mitigating techniques is also provided. Moreover, design trade-off of these mitigation techniques is also provided. These mitigation techniques are summarized in a table at the end of each subsection, highlighting their main attributes, strength, and weaknesses.
4. Finally, various research gaps are identified that open the gates for further exploration.

The rest of this paper is organized as follows. In Section 2, we provide an overview of an SDN architecture. In Section 3, we provide a detailed description of attacks and their countermeasures on an SDN controller. In this section, we provide a brief taxonomy of these attacks as well. Open security issues, challenges, and future research directions, in the context of SDN controller, are provided in Section 4. Finally, this paper is concluded in Section 5.

2 | OVERVIEW OF SDN ARCHITECTURE

According to Open Networking Foundation (ONF), the control and data planes in an SDN architecture are decoupled. Furthermore, the network intelligence and states are logically centralized, and the underlying network infrastructure is abstracted from the applications.[41] The architecture is vertically divided into three layers, ie, an application layer, a control layer, and a data layer.[42] These layers are separated from each other using northbound and southbound programming interfaces (APIs),[7,43] as depicted in Figure 2. The northbound interface facilitates the communication between the application layer and control layer. Although there exists no standardized interface, the most commonly used interface for application-to-control communication is Rest API. On the other hand, the southbound interface facilitates the communication between the control layer and data layer of an SDN architecture. OpenFlow is the most widely used API for the southbound interface. A detail discussion on these interfaces along with the aforementioned three layers are provided in this section.

2.1 | Application layer

Application layer, also known as an application plane, provides a set of services for various applications, such as security provisioning, QoS, routing, and deep packet inspection (DPI), are few to mention here. Each application consists of an SDN Application Logic and one or more

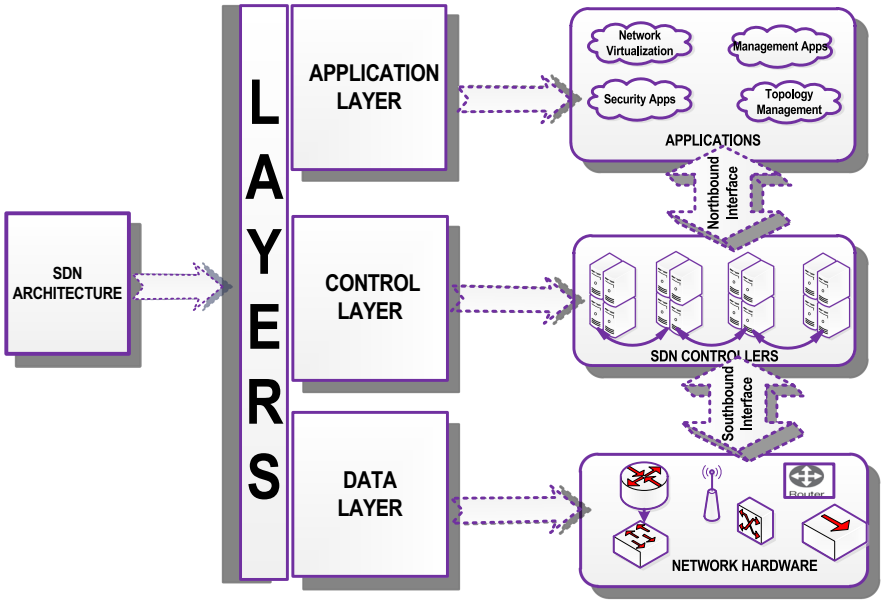

FIGURE 2 An SDN architecture

Northbound Interface (NBI) drivers. Each application supported at this layer programmatically states its requirements and desired network behavior to the controller via the northbound interface.

2.2 | Northbound interface

The Northbound Interface (NBI) facilitates application-to-control plane communication using vendor neutral open APIs. This interface is responsible for providing an abstraction of the underlying network. Furthermore, it empowers the applications by expressing the required network behavior to the controller. However, the NBI lacks a standardized interface and, as such, is used on an ad-hoc basis as per SDN administrator choice.

2.3 | Control layer

Control layer, also known as control plane, is responsible for the management and control of the overall network. This layer contains an important network component, known as the SDN controller. This component is logically centralized; however, in principle, it is physically distributed.[6,7,9] It is responsible for establishing and terminating data flows on various network components at the data layer, based on data handling policies. Its prime responsibility is to fine-tune the forwarding tables, which reside in the forwarding plane. This tuning is based on the network topology or external service requests.[44] This layer abstracts the network complexity by maintaining an up-to-date network holistic view. There are various components of an SDN controller such as single or multiple NBI Agents, SDN Control Logic, and the Control-Data-Plane Interface (CDPI) agent. In addition, the logically centralized controller can be applied to a wide variety of physical media. For instance, guided media such as Ethernet, and unguided media such as Wi-Fi, LTE, and WSN. Some of the most widely used controllers are highlighted in Figure 3.

2.4 | Southbound interface

Southbound interface provides communication between the control and data layers of an SDN architecture. This interface provides event notification and statistical reports using southbound APIs. This interface is also known as a controller-switch communication interface because it facilitates communication between the controller and a switch at the data plane. This interface enables the network managers to implement the controller decisions on the network components of a data plane. OpenFlow is the most popular and widely used protocol at the southbound interface. Other such protocols are Cisco's Open Network Environment Platform Kit (onePK), Junipers contrail,[45] and Forwarding and Control Element Separation (ForCES) framework,[46] and protocol oblivious forwarding (POF).[45,47]

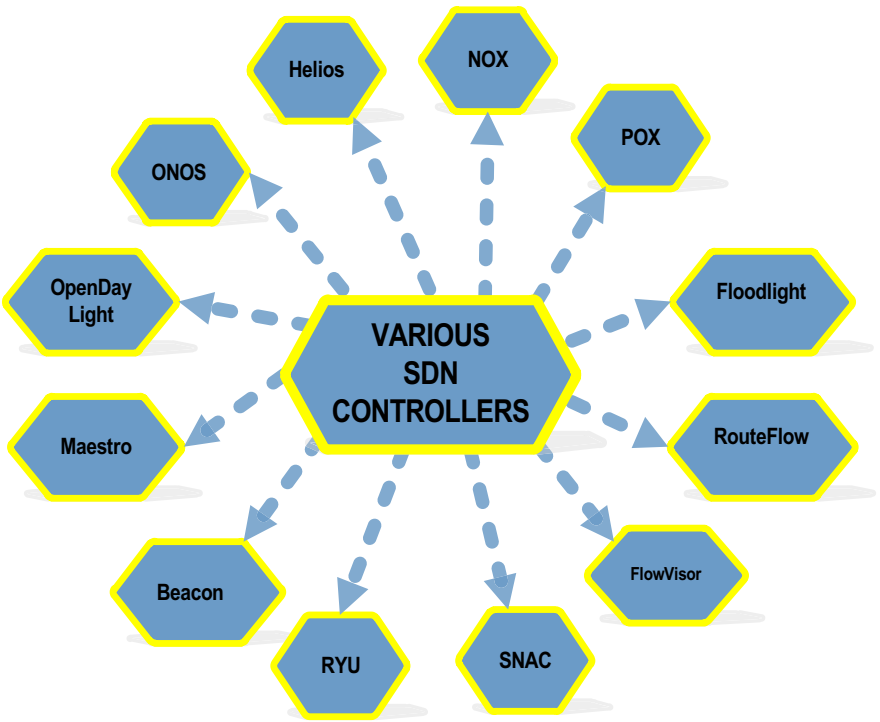

FIGURE 3 SDN controllers

2.5 | Data layer

The lowest layer in the SDN architecture is known as data layer/plane. This layer consists of forwarding network components such as, routers, physical and virtual switches, and access point. As a result, this layer is also known as infrastructure layer.[48] The data layer is responsible for the implementation of management functionalities such as forwarding data, fragmentation, and reassembly, as instructed by the controller to the SDN-enabled switches. Furthermore, the information collected by these OpenFlow switches are forwarded to the controller, using a southbound interface.[49]

3 | CONTROLLER-RELATED THREATS AND ATTACKS

In SDN, all network-related functionalities are managed, controlled and secured from a centralized controller. The single-point dependency and programmable nature of an SDN controller make it a potential choice for the attackers. If security of the controller is compromised, the whole network is vulnerable to various attacks.[14-16] An adversary can launch various attacks by exploiting vulnerabilities of a controller. These vulnerabilities can lead to castrotrophic situations, particularly in the absence of a robust and secured policy.[12,50] For instance, an attacker can spoof the address of a controller or insert a fake controller to hijack the whole network. As a result, it is essential to design a secure mechanism to protect the network in general, and the controller in particular, from a wide range of attacks.

The southbound interface needs to be protected and secured against communication overhead. Therefore, unnecessary communication that results in congestion at this interface needs to be avoided for the smooth functioning of the network. In addition, the availability and confidentiality of the controller need to be ensured. Therefore, it is essential to secure both the controller and the southbound interface against attacks and is attracting the attention of the researchers in recent years.[19,51,52] Securing the controller and southbound interface (Figure 4) may include the following:

1. Ensuring availability of the controller by protecting it against flooding attacks such as DoS and DDoS attacks.
2. The controller must be guaranteed with security policy enforcement, high availability and the minimum possible delay experienced during incoming packets.[41]
3. Being a programmable architecture, the operating system installed on a controller must be guarded against various vulnerabilities such as exploitable patches, back and open door accounts, and open ports.
4. The controller should be protected against external and physical threats.
5. The controller needs to have an automatic alert system that needs to control the data-to-control plane communication to a minimum level, during an attack, as well as informing the administrator in case of an attack.

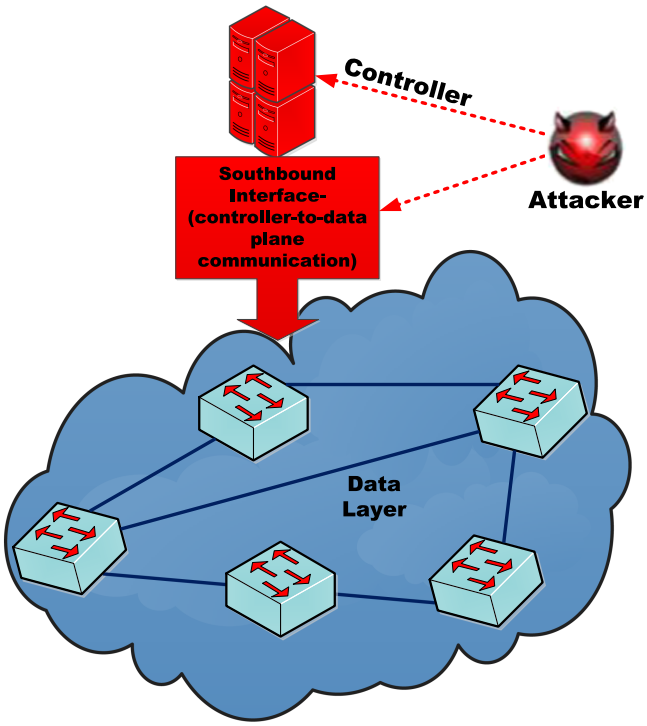

FIGURE 4 Security attacks on the SDN controllers and southbound interface

In this section, we provide a detailed discussion of the most common attacks, such as DoS/DDoS, spoofing, and malicious injection, in the context of SDN controller.

3.1 | DoS/DDoS attacks

The denial-of-service (DoS) and distributed DoS (DDoS) are the most common attacks launched by cyber criminals, cyber extortionists, and hackers. These attacks flood the controller with spoofed packets that result in serious disruption of the provided services. These attacks compromise the controller, and as such, it is unable to respond to legitimate requests and fail to offer services due to the flooding of illicit traffic by an attacker, as shown in Figure 5. Such a situation results in the exhaustion of network resources. Moreover, the controller is unable to differentiate between a genuine request and an attacker's request, due to the changes in the packet header that look somewhat identical for both these requests. During these attacks, it is a challenging task to analyze the huge traffic flow. Thus, the accuracy of the services provided by the controller is compromised along with lower response time. There are various reasons for launching DoS/DDoS attacks, such as financial gains, political gains, competitive edge, and disruption of services.[53]

Keeping in view the importance of a controller in an SDN environment, there is a need for sufficient research to detect, mitigate, and design preventive techniques, for the ever-increasing, novel, and highly sophisticated DoS and DDoS attacks. In the work of Yan et al, there exist few works that study the unique relationship between DoS/DDoS attacks and an SDN controller.[36] Moreover, the available literature is not up to date. It is mainly due to the unique relationships between an SDN and DDoS attacks that are yet to be discovered. In this section, we present the latest DoS and DDoS mitigation techniques based on Entropy, Machine learning, and Traffic pattern analysis from other works.[15,18,22,54-63] Moreover, a summary of these mitigation techniques is provided in Table 1.

3.1.1 | DoS and DDoS mitigation techniques

In the work of Boite et al,[54] the authors proposed StateSec, that employs a stateful method to utilize in-switch processing capabilities for accurate detection and efficient mitigation of DDoS attacks in an SDN architecture. StateSec mechanism offloads the controller by reducing the communication overhead at the southbound interface. The security management of StateSec consists of three main phases, ie, traffic/flow monitoring, anomaly detection, and mitigation/countermeasures. Traffic monitoring is performed within the switch, while anomaly detection and mitigation are usually implemented at the control layer. During traffic monitoring, the proposed method monitors and matches packets against four configurable traffic features, ie, IP addresses of source and destination and port addresses of source and destination inside a switch, using stateful programming. During the anomaly detection, an entropy-based algorithm is used at the controller for the detection of anomalies and various types of attacks, such as port scan, DoS, and DDoS.[64] Finally, during mitigation, the controller alleviates these attacks by taking appropriate action, such as filtering, rate limiting, and re-routing malicious traffic toward a black hole or fake server, ie, honey pot. Extensive simulation results show that StateSec is an effective and efficient technique against DDoS attacks, which incurs a lower overhead at the controller

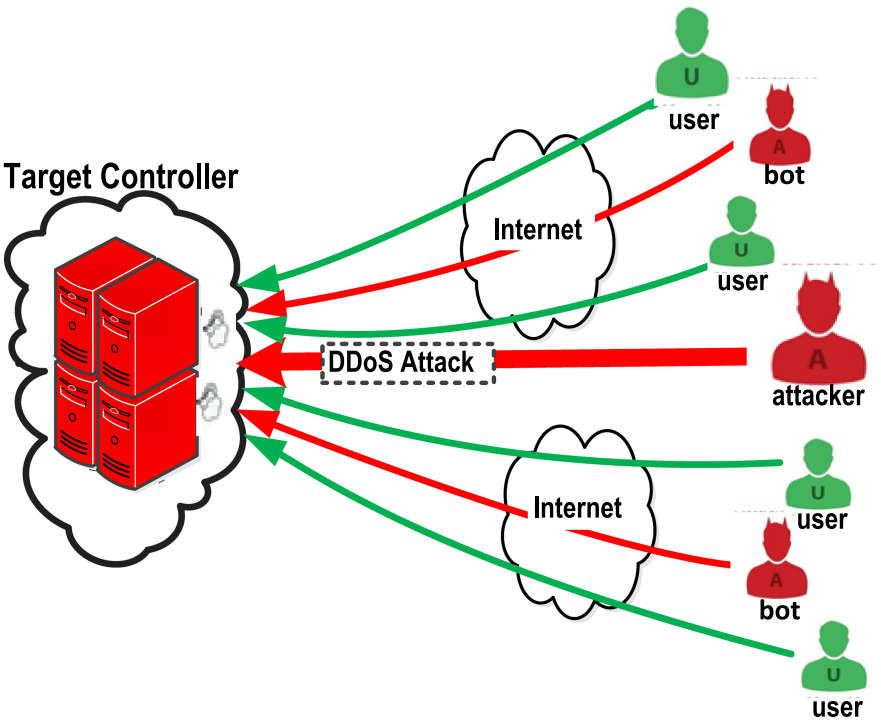

FIGURE 5 DoS attacks on an SDN controller

TABLE 1 A summary of mitigation techniques for DoS/DDoS attack on the SDN controller

Mitigation Techniques	Issues Addressed	Strengths	Weaknesses
StateSec[54]	DDoS and anomalies detection	Efficient against attacks, lower communication overhead	Not tested on complex networks, masking anomalies, and also unable to detect anomalies disturbing randomness
OpenFlow switch[57]	DoS	efficient and effective, Average of both false positive and false negative are less than 2%	Low accuracy, needs to be evaluated using formal methods
AVANT-GUARD[15]	DoS	Reduce data-to-control plane communication overhead, quick response to the changing flow dynamics at the data layer	Need to be installed at each network component, otherwise, unable to secure the network
Entropy-based DDoS detection and mitigation[61]	DDoS	computationally lightweight, generates fine-grained patterns, lower communication overhead at the southbound interface	Need to be integrated with others techniques to accomplish threshold determination and multi-element weight assignment
SGuard[22]	DoS	scalable, effective and easily integrates with OpenFlow	Controller exclusive, needs to be evaluated in complex scenarios to obtain better results
FL-GUARD[18]	DoS, DDoS	effective against spoofing attacks	Generic detection algorithm
Fuzzy-based DoS Detection[56]	DoS	lightweight, efficient and effective	Needs to be evaluated in complex environments with different topologies
Early detection of DDoS attacks against SDN controllers[59]	DDoS	lightweight, detect attacks within the first 500 packets	Unable to detect attack that generate varying traffic flows

and southbound interface. However, StateSec is unable to detect attacks with unknown patterns. Furthermore, the accuracy of the detection rate needs to be improved significantly.

In the work of Huang et al,[57] the authors proposed a scheme to protect the SDN controller against DDoS attacks. During the first stage, the proposed method predicts the large volumes of incoming packets. These packets are associated with every new request for each OpenFlow switch. If the amount of incoming packets is higher than a specific threshold value, the rest of the requests are forwarded to a secured gateway to determine a DDoS attack. An algorithm is employed at the gateway by designing rules that filter out those requests that cause a dramatic decrease of entropy. Finally, the controller forwards these rules to each OpenFlow switch that inspects the incoming packets. The switch requests for irregularities, in case of irregular requests. Simulation results prove that the average of false positive and false negative is less than 2%. However, the comparison needs to be made with similar algorithms, proposed in the literature.

Security analysis and monitoring are the two core elements that are required for ensuring the security of a controller. In the work of Shin et al,[15] the authors proposed AVANT-GUARD, a secured framework to protect the network against DoS attacks. AVANT-GUARD addresses the two primary security challenges, i.e, reducing communication overhead at the OpenFlow protocol (southbound interface) and providing a quick response to the changing flow dynamics at the data plane. To overcome the first challenge, AVANT-GUARD adds connection migration to the data plane that avoids any further communication. To overcome the second challenge, the authors introduced a statistic collection service on the data plane. Simulation results show that the AVANT-GUARD protects the SDN network against TCP sync-flooding attacks and network scanning attacks. However, it does not preserve the SDN against DoS attack on the application layer as well as on the Internet Control Message Protocol (ICMP) and UDP (User Datagram Protocol) layers.

In the work of Wang et al,[61] the authors proposed an approach to protect SDN controllers from DDoS attacks and anomalies. The proposed method employs a distributed and lightweight entropy-based DDoS attack detection module on every edge switch at the data plane. It results in a lower communication overhead at the controller as well as at the southbound interface. The higher value of entropy indicates an increased variation in the probability distribution, whereas a lower value indicates a decreased variation. The proposed approach uses the destination IP address at each switch for a probability distribution. As soon as a DDoS attack is detected, the alert information is forwarded to the controller for further necessary actions. The supremacy of the proposed system is that it generates fine-grained patterns with low calculation overhead in comparison to the traditional volume-based traffic analysis scheme.[29] The proposed approach has its own shortcomings. For example, the relevant information about the distribution of the analyzed feature is lost that leads to masking of anomaly effects.[65] Similarly, the different distributions with the same amount of uncertainty cannot be distinguished by entropy values. Therefore, the proposed method is unable to detect anomalies that do not disturb randomness.[66]

In the work of Wang and Chen,[22] SGuard, a lightweight and efficient security application on top of the NOX controller, for the detection of DoS attacks was proposed. The proposed architecture consists of two modules, ie, access control and classification. The access control module uses authorization information for tracing the genuine source of a packet by taking preventive measures, using such information. As

soon as a new entity enters the network, this module gathers information related to this entity such as medium access control address (MAC), logical address, port address, and switch ID. Based on this information, SGuard compares the source address, ie, MAC/IP, against the hash table entries. This module allows normal traffic into the network while denies packets from a spoofed source. Classification module, on the other hand, employs a Self Organizing Map (SOM),[67] based on the artificial neural network to classify network traffic as normal or abnormal, using a feature vector. The classification includes three sub-parts, ie, data collector, feature extractor, and a classifier. The data collector gathers the flow entries from the flow tables of OpenFlow switches, at a particular time interval. Once the data is gathered, features are extracted and are then classified using the most relevant data as feature vector from the data flow entries. This feature vector is used for the classification between normal and malicious traffic. Moreover, the classification is enhanced further by feature ranking and selection algorithms to obtain high accuracy and efficiency. All modules of SGuard cooperate in an SDN controller to guard against DoS attacks. SGuard can easily be integrated with the OpenFlow, without making any changes to its underlying architecture. Based on extensive experimental work, it was concluded that the proposed approach is lightweight, scalable, and effective against these attacks. However, the overall data training time needs to be minimized to improve the classification performance. Furthermore, SGuard needs to be evaluated for large and complex scenarios.

In the work of Liu et al,[18] the authors proposed a novel DDoS detection and prevention system, known as Floodlight-based Guard system (FL-GUARD). The architecture of FL-GUARD is based on three components, ie, anti-spoofing module, sFlow-RT collector, and a blocking module at the application plane of an SDN architecture. Initially, FL-GUARD uses the concept of dynamic IP address binding for the identification of anti-source of spoofed IP address. Next, FL-GUARD employs an improved network monitoring component, known as sFlow-RT collector, that monitors the traffic in real-time with lower delay and enhanced accuracy. Finally, DoS and DDoS attacks are detected at the source port using C-SVM, an improved version of the Support Vector Machine Algorithm (SVM). The modular design of an FL-GUARD is convenient for further modification and extension. The simulation results conclude that FL-GUARD is an efficient solution against DDoS attacks. Nonetheless, accuracy and performance of the proposed method can be enhanced further using various other machine learning approaches such a random forest and decision tree. The FL-GUARD needs to be evaluated using performance metrics such as specificity, accuracy, precession, sensitivity, and F-Measure. Finally, execution time needs to be taken into account to understand and evaluate the behaviour of the proposed architecture fully.

In the work of Dotcenko et al,[56] the authors proposed a fuzzy-based security mechanism to guard an SDN controller against DoS attacks. The proposed approach uses a Tree-reweighted message passing (TRW) algorithm[68] along with rate limiting and fuzzy inference.[69] The inference approach is the most realistic one for resolving fuzzy inference problems as it is lightweight in terms of computation and resource utilization. Simulation results reveal that the proposed method effectively detects DoS attacks in comparison to other security mechanisms. However, the proposed scheme needs to be evaluated, using complex scenarios having large volumes of traffic. Furthermore, the proposed approach does not have provisioning for mitigating strategies against attacks. In the work of Dillon and Berkelaar,[55] the authors proposed an anomaly detection technique for the mitigation of DDoS attacks on the controller in an SDN environment. The proposed method calculates a standard deviation of packet rate, collected for certain time intervals. The controller gathers these statistics from the OpenFlow switches at the data plane. A comparison is made between the previously calculated deviations against a real deviated value in the data set to detect anomalies. The proposed approach employs a three-stage solution for the detection and mitigation of DDoS attack using an RYU controller. During the first stage, irregularities are identified in the network flow. Next, the source is traced back using packet analysis of the samples. Finally, the incoming packets from malicious sources are dropped. Although the proposed approach is efficient for the detection and mitigation of DoS attacks, its performance is dependent on the underlying dataset that are used for training purposes. Thus, its performance needs to be tested using more than one dataset.

In the work of Mousavi and St Hillaire,[59] the authors proposed an entropy-based solution that detects DDoS attacks at the controller, using randomness of the incoming packets. The proposed method measures the probability of the occurrence of an event concerning the total number of events for early detection of an attack. The implementation of the proposed solution is based on a threshold value of entropy for the efficient detection of a DDoS attack. It implies that, if the entropy value is lower than this threshold value, it needs to be considered an attack. The proposed approach is lightweight in terms of the resources used and is capable of detecting DDoS within the first 500 packets of the traffic. However, this approach is not reliable since the threshold value varies in different scenarios. Due to the programmable nature of an SDN, the network configuration may change while the network is still performing real-time monitoring. Furthermore, the proposed approach lacks any mitigation strategy.

3.2 | Spoofing attacks on the SDN controller

The controller is the backbone of an SDN network as it manages and controls the whole network. Due to its centralized nature, it is vulnerable to many types of security attacks. One such attack is spoofing attack. In spoofing attacks, an adversary launches attacks on a legal entity (server/system) by mimicking a legitimate user. The adversary forges the network information, ie, IP address, MAC address, and ARP, intentionally by hiding its original identity, as shown in Figure 6.[70] These attacks violate the authentication security property of an SDN controller. Some studies show that SDN controllers, such as Floodlight, Open Daylight, Beacon, and POX are adversely affected by spoofing attacks.[21] In SDN, spoofing occurs in many forms such as IP spoofing, ARP spoofing and controller spoofing. In IP spoofing, IP address other than the attacker real IP address is used to hijack the whole network.

On the contrary to IP spoofing attacks, in Address Resolution Protocol (ARP) spoofing attacks, an association is made between the MAC address of an attacker with the IP address of a legitimate host.[27] These attacks result in the hijacking of traffic from the intended genuine users

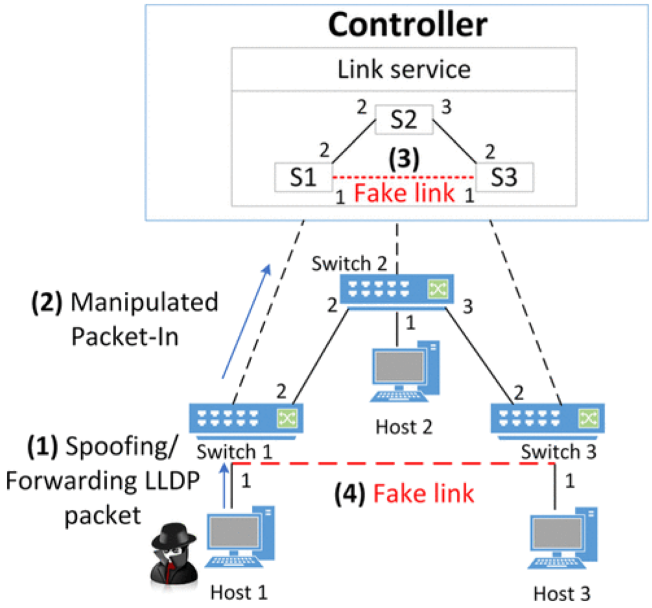

FIGURE 6 IP spoofing attack on an SDN controller[70]

and as such these users are taken out of the network. In controller spoofing attacks, a fake controller is inserted into the network that pretends to be a legitimate controller by tricking the users. In this work, we aim to refer to all these attacks as spoofing attacks collectively. A detailed discussion on spoofing attacks can be found in other works.[37,71,72]

The most challenging aspect of these attacks is tracing back the origin of an attack. This is because of poisoning network visibility, infecting topology information, misconfiguration, and hijacking of services and application provided by an SDN controller. Due to these complications, sophisticated attacks such as DoS attacks, network hijacking attacks, blackhole attacks by manipulating the routing services inside the controller, man-in-the-middle attack, and sometimes complete failure of the entire network takes place.[19,39,73] Looking at the severity of these attacks, in this section, we will discuss various solutions proposed in the literature for the detection and mitigation of an entire range of spoofing attacks that exclusively target the controller. A substantial amount of work is previously carried out in the literature to examine these attacks along with their mitigation techniques.[74-81] This work is an effort to combine the previous and latest related research work. Moreover, this section also highlights strength and weaknesses as well as possible future extensions in the aforementioned research work. It will help the research community to better understand this domain and the research efforts carried out for possible future exploration. Furthermore, it is crucial for the widespread adoption of SDN-based networks. All these attacks are summarized in Table 2.

3.2.1 | Spoofing mitigation techniques

In the work of Al-Ayyoub et al,[76] the authors have proposed Software Defined Security controller (SDSec), based on the Open vSwitch Controller, for the detection and mitigation of MAC and IP spoofing attacks.[21] SDSec uses an improved version of the OFDP protocol, known as Link Layer Discovery Protocol (LLDP), to identify an active link in the network. This is because the older version of LLDP is vulnerable to spoofing attacks.[85] The operation of SDSec is based on two tables, ie, switch table and host table, that is added to the controller using the SQLite in-memory database. The host table holds information such as hostname, IP addresses, MAC addresses, concerned switch, and its connected interfaces, authentication status, and action on traffic, relevant to the hosts in the network. The switch table, on the other hand, holds information such as names, IP addresses, MAC addresses, and available interfaces about trusted switches of the network. Every time, a new switch or host joins the network, it is authenticated before its communication with the SDSec controller. The latter either permits or denies the former to communicate on the network. The information of a new entity is checked and is authenticated by inspecting their data against the information contained in both of those tables. In case of a match in either of these tables, a false value is assigned to the AUTH field that indicates IP/MAC spoofing attacks. This means that the new host is using the same information similar to the one used by the genuine host in the network. Once a device leaves the network, its related information is removed from those tables to facilitate re-joining the network in the future. The proposed controller is extensively simulated in Mininet simulator using customized topology. Simulation results show that SDSec can efficiently detect and prevent IP and MAC spoofing attacks. The performance of SDSec may be enhanced further by adding more tables to the controller to cater for other types of attacks. Furthermore, the effectiveness of the proposed controller should be evaluated using other performance metrics and using various topologies and complex scenarios.

AbdelSalam et al[74] proposed a technique that mitigates Address resolution protocol (ARP) request as well as reply spoofing attacks on the controller of Software Defined Networks. The notable features of this technique are that it protects the network against the said attacks with increased reliability, minimum latency, and minimum communication overhead. The proposed method performs port-level ARP packet monitoring

TABLE 2 A summary of various mitigation techniques for spoofing attack on the SDN controller

Mitigation Techniques	Issues Addressed	Strengths	Weaknesses
SDSec[76]	IP and MAC spoofing prevention	efficiently detects and prevents IP and MAC spoofing attacks	does not integrated fully in SDN, and unable to offer the acceptable level of QoS as well as privacy
ARP Spoofing Mitigation[74]	ARP Reply and Request spoofing attacks	Attack detection with minimum latency and increased reliability, Performs port-level ARP packet monitoring	Lacks of an all-element threat model
Anomaly traceback[78]	Spoofing and traceback	Can easily be implemented at the SDN controller without developing dedicated routers	lacks evaluation on a benchmark data set, lack of trace route mechanism for an anomaly, and does not devise any flow statistics procedures to weighted anomalies
SDNsecured[77]	DDoS attack using IP spoofing, reply, ARP spoofing and man-in-the-middle	Employ AES for encryption and decryption while TLS for secured key exchange among the switches	lacks scalability evaluation of the controller, and cross layer controller security
Hybrid SDN[82]	ARP spoofing	A separate server is used for the collection and analysis of ARP request along with topological information of the whole network	does not study the frequency of traffic rule updates on the network performance, and non-scalable
Security-awareness SDN[83]	Network scanning, OpenFlow flooding, Switch compromise and ARP attack prevention	Security situation awareness based on features extraction with low overhead	lacks a balance between resources utilization and performance
Mitigation of DNS Amplification[79]	DNS Amplification attacks	Stores history of DNS queries as an evidence to differentiate normal packets from malicious packets	high communication overhead due to memory lookup
User Flow Validation Approach[80]	Flow table overloading, DDoS attacks and link spoofing attacks	Uses multiple Discrete-Time Finite-State Markov Chain (DTMC) model for users flow validation, unsupervised hashing for link spoofing and L1-ELM for classification	does not ensure accuracy of anomaly detection
Software-dened Mobile Networks[84]	IP-related source spoofing, DoS and DDoS	Multi-tier component-based security architecture for threats detection	non-scalable

by adding an ARP module to the controller for the successful detection and mitigation of spoofing attacks on the controller. Furthermore, it can also guard a controller against communication overloading during DoS and other such attacks under various scenarios. Simulation results reveal that the proposed approach can effectively mitigate these attacks with lower overhead. However, The proposed technique is studied in a LAN network with a single controller; thus, its effectiveness should be studied in a complex environment with multiple controllers.

In SDN, tracing back the sources of an anomaly is a real challenge. Anomaly refers to an attack using a spoofed packet or misbehavior by an attacker. Francois and Festor[78] proposed a method that passively identifies switches that are on the network path of an anomaly. Because SDN technologies tend to be deployed in the next generation networks including data centers, the proposed method can easily be implemented without developing dedicated routers like usual IP traceback techniques. The concept of the proposed method is based on forwarding rules with different parameters. The two most crucial forwarding rules are *matching* and *instruction*. The matching rule works like a filter where each packet's header is checked and matched with that of the switch tables entry to confirm whether it belongs to the flow or not. As a result, the actions such as forwarding/ modification are taken for each packet. On the other hand, instruction refers to a set of actions. OUTPUT is the primary instruction that forwards the packet to a particular port of a switch. Other such actions are *modification* of the header of a packet, ie, MAC address, TTL, and various counters for monitoring purposes, ie, number of bytes, number of packets, and duration. The proposed method is evaluated using various topologies and various attacks such as distributed attacks with many hosts to study its effectiveness. It is concluded that the proposed approach fulfill its design objectives. However, this method may be enhanced further by using stochastic analysis to find out the route that has been taken by an anomaly.

IP spoofing, reply attacks, ARP spoofing, and DDoS along with man-in-the-middle attack are series of threats to an SDN architecture in general and the controller in particular. In the work of Ertaul and Venkatachalam,[77] the authors proposed a solution that guards the SDN controller against the aforementioned attacks. The authors have employed Advanced Encryption Standard (AES)[86] along with Transport Layer Security (TLS).[87] AES was used for encryption and decryption purposes, while TLS was employed for secured key exchange among the switches. Moreover, IPsec is employed for tunneling between the hosts and gateways. Thus, IPsec preserves confidentiality and authenticity of data packets. Simulation

results show that the proposed approach can effectively mitigate DDoS attack using IP spoofing, reply, ARP spoofing, and man-in-the-middle attack. However, the proposed methods should be evaluated and tested in a real-time environment to study its effectiveness.

An automatic ARP spoofing detection and mitigation mechanism for hybrid SDN was proposed.[82] Hybrid SDN refers to the partial installation of SDN-enabled devices in a traditional network. The key benefits of such architecture are to achieve all the benefits of SDN from a traditional environment with lower deployment cost. The proposed method achieved this by installing a separate server that collects all the ARP requests. Furthermore, the controller and southbound interface are protected from the unnecessary processing of malicious data from the attackers by diverting them towards that particular server. In addition to that, topological information of the whole network is also gathered at the aforementioned server. The authors have employed a graph-based traversal mechanism that represents the network topology in the form of a graph. It can aid in the accurate detection of the attacker's location by verifying legitimate users. Next, the flow rules related to forwarding of ARP packets from the source to that particular server are installed on the switches for further analysis and accurate detection of ARP spoofing attacks. Simulation results demonstrate that the proposed method can effectively detect and mitigate threats and attacks related to ARP spoofing but lacks real-time evaluation and results.

Another beneficial work that focuses on the detection of four types of attacks, ie, network scanning attacks, OpenFlow flooding attacks, switch compromised attacks, and ARP attacks, targeting both the data plane and control plane of the SDN controller was presented in the work of Fan et al.[83] The authors proposed a security situation-awareness approach based on flow features extraction. The authors considered a total of 12 features for these four different types of attacks. Furthermore, multiple observations-based hidden Markov model (HMM)[88] was employed for the situation assessment purposes and building a quantification model in the assessor. The quantification model calculates the situation value and predicts the SDN situation status. Higher the situation status value, higher is the risk of attack. Moreover, the Baum-Welch algorithm[89] was employed to calculate probabilities and model training, while Viterbi algorithm[90] was employed for predicting the status of the network. As an initial step toward security situation awareness in SDN, simulation results show its effectiveness. However, the proposed approach may be further extended to consider other type of attacks. Furthermore, accuracy and efficiency of the proposed method may be further enhanced to adapt it for a real-time environment.

Another significant contribution in this area was presented in the work of Kim et al[79] that proposed a novel security framework to protect the network against DNS amplification attacks. The proposed framework stores the history of DNS queries and uses it as an evidence to differentiate between normal and malicious packets. The proposed framework consists of two main components, ie, a switch and an SDN controller. The responsibilities of the switch are that it stores mapping (strict one-to-one mapping), and validate query records related to DNS request, eg, the source IP addresses and destination IP addresses contained in a DNS request message. Initially, a switch checks whether the received packet is a DNS request. If true, the information is stored locally at the memory of the switch or forwarded to the controller in case of unavailability of memory in the switch. Next, the switch checks the validity of the request with the DNS response available in its memory. Upon matching, the request is then forwarded and becomes part of the DNS requests, which is later on used for validation purposes. Simulation results show that the proposed system can effectively tackle these attacks by removing the possibility of false positive packets. However, communication delay that occurs when a switch communicates with a controller due to unavailability of memory space and for the DNS request validation should be minimized. Moreover, further experiments need to be carried out in a real-world environment to study its effectiveness.

Another security architecture that protects the SDN controller from three types of security attacks, ie, flow table overloading, DDoS attacks and link spoofing attacks, was presented in the work of Liyanage et al.[80] The proposed architecture uses multiple controllers in a star topology, instead of a single controller used in previous studies, to validate the user flows. A star topology is mainly chosen to mitigate the effects of flow table overloading attacks that occur due to anomalies. For validation of users flow and flow table occupancy, the proposed architecture employs Discrete-Time Finite-State Markov Chain (DTMC) model[91] at all switches in the network. This model provides updated information from time to time on the state, ie, idle and busy/transmitting, of these switches. Moreover, the proposed architecture tackles the issue of link spoofing attack that occurs between the switches at the data layer by verifying these links using an unsupervised hashing method at the controller.[92] Finally, a hybrid classifier is employed at the controller by combining fuzzy logic classifier with extreme learning machine (L1-ELM) running on a neural network. This hybrid approach is used because it proved to be an efficient classifier that classifies malicious packets from regular data packets. The proposed approach initially blocks and detects anomalies at the switches, while the remaining anomalies that escape those switches are identified and mitigated by the controller. Moreover, switches are informed by the controller about those escaped anomalies. Results from the simulation reveal that the proposed approach can effectively defend SDN networks against the aforementioned attacks. However, the network flow should be validated in large-scale networks.

Another vital contribution for SDN controller was presented in the work of OpenHIP.[84] The author has proposed a novel multi-tier component-based security architecture. The proposed architecture aims to protect Software-defined Mobile Networks (SDMNs) against IP-related attacks such as DoS, DDoS, and IP spoofing attacks. The proposed architecture consists of five components, ie, secure communication, policy-based communication, security information and event management, security-defined monitoring, and deep packet inspection component. The role of the secure communication component is to protect the data-to-control plane channel using Host Identity Protocol (HIP) with IPSec tunneling. The policy-based communication component protects the network, associated channels, and devices against DoS and source address spoofing based on pre-defined policy. In the security management and monitoring component, Deep Packet Inspection (DPI) is carried out for the detection of vulnerabilities and security threats as well as checking the security mechanisms used in the underlying network.[80] The responsibility of security-defined monitoring is to coordinate the monitoring activities. Finally, Deep Packet Inspection (DPI) is used to improve security threat

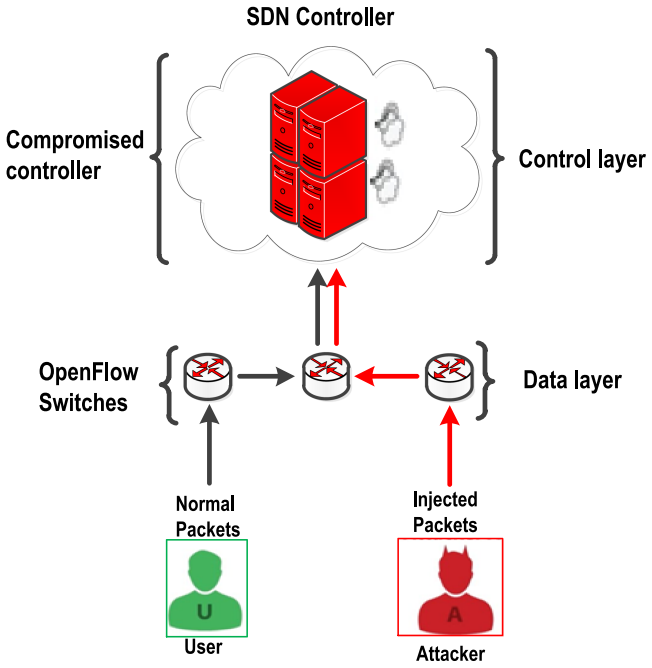

FIGURE 7 Malicious injection attacks on the SDN controller

detection. Simulation results prove that the proposed architecture can protect the network against IP-related attacks on SDMNs. However, its feasibility needs to be studied in real-world settings. Furthermore, the requirements and guidelines are not clear on how to integrate it with the current system.

3.3 | Anomalies and malicious injection attacks on the SDN controller

Malicious injection attack is yet another type of attacks and remains an intruder's preferred choice to exploit various vulnerabilities in SDN-based networks, as shown in Figure 7.[93] During malicious injection attacks, an adversary seizes a single or multiple hosts for launching malicious packets. The only thing that an attacker requires is the same privileges as a normal user. On the other hand, during SQL injection attacks, a perpetrator modifies the anticipated effect of an SQL query by injecting new SQL keywords or operators into the query. A detailed discussion on SQL injection attacks and their countermeasures can be found in the work of Halfond et al.[94] Recently, some research works have been carried out on the detection of anomalies as well as malicious injection attacks on an SDN controller.[17,95-101] However, numerous challenges remain unaddressed due to the unique characteristics of SDN controller along with the varying nature of SDN traffic. In the following section, we present the aforementioned mitigation techniques and provide an overview of them in Table 3.

3.3.1 | Mitigation techniques for anomalies and malicious injection attacks

A novel topology discovery protocol, Secure, and Efficient OpenFlow Discovery Protocol (sOFTDP) was proposed in the work of Azzouni et al.[17] The design objectives of the sOFTDP were to overcome various operational and security limitations of the OpenFlow Discovery Protocol (OFDP).[104] The proposed protocol is lightweight, dynamic, and suggests minimal changes to the Open Flow switch design. Minimal changes to the open flow switch imply that sOFTDP shifts a part of the topology discovery procedure from the controller to a switch. As such, the switch alone detects the link events and notifies the controller, whenever necessary. A controller contains the necessary mechanism to deal with switch notifications and dynamically changes its topology map for making routing decisions without prior knowledge of the events that cause topological changes. The two main events that cause topological changes are adding new links to the network and removal of existing links from the network. The proposed protocol was implemented as a topology discovery protocol module in the floodlight controller for evaluation purposes. Simulation results showed that sOFTDP outperforms OFDP regarding security, performance, and topology discovery time, respectively. Despite all these advantages, sOFTDP is unable to protect the network against the link fabrication attacks on relay nodes. Moreover, effectiveness of the proposed protocol should be tested in large and complex scenarios.

Another significant contribution is EUNOIA,[99] a threat-aware system based on machine learning. The proposed system detects and mitigates network intrusion in four stages, ie, data processing for feature selection, predictive data modelling for machine learning and anomaly detection, decision making for intrusion detection, and response system. During the first stage, redundant data is filtered out from a large volume of

TABLE 3 A summary of mitigation techniques for malicious injection attacks on the SDN controller

Mitigation Techniques	Issues Addressed	Strengths	Weaknesses
sOFTDP[17]	Link Injection and Fabrication attacks	Secured, Improved performance and topology discovery time	Ineffective against link fabrication attacks in relay manner, and not evaluated on larger testbeds
EUNOIA[99]	IDS	Machine learning-based effective solution for intrusion detection system	Needs to be tested on multiple classifiers
RAD[102]	Anomalies detection	Enhances performance by detecting attacks with improved agility and efficiency, even during link failure and burst Traffic	Needs to be evaluated for complex traffic generation and in different attack scenarios
Synaptic[98]	Anomalies and vulnerabilities	Guard a security chain against anomalies, intrusion and vulnerabilities	Can be enhanced further using formal methods
ML-based IDS[103]	Detect and mitigate DoS, probe, U2R, and R2L attacks with an improved accuracy	A flow-based anomaly detection using machine learning techniques to overcome the limitation of signature-based IDS.	Low accuracy, i.e., high-false rate
Byzantine FL[97]	Protect data and control planes, and southbound interface against unauthorized access using multiple controllers	A cost effective controller assignment algorithm for a given set of switches	Lacks optimal controller assignment algorithm
Athena[96]	Detects well-known network anomalies in an efficient manner	Scalable anomaly detection framework requiring minimal programming effort and no specialized software	Controller exclusive, and overload the devices at the data plane during heavy traffic
Sampled-DP[95]	Anomalies detection	Cluster centers and outlier points extraction to eliminate redundancy	Low performance, and slow response towards intrusion
Dynamic Access Control system (DAC)[100]	API abuse attacks	Secured API requests with minimum latency	Limited in its scope because it is controller specific
Scalable Traffic Sampling[101]	Anomalies and malicious packet detection in large-scaled networks	Enhances monitoring and performance by selecting the most feasible switches for scalable traffic sampling	Does not consider complex topologies and attacks scenarios

data that include raw data containing both historical archival traffic and real-time incoming traffic data. This stage reduces ambiguity from voluminous traffic gathered previously for the predictive data modelling subsystem with increased reliability. In the predictive data modelling stage, an attack model for intrusion detection is developed using decision-tree machine learning algorithms.[105] The classification algorithm is used to train a classifier that can label or predict any new unknown audit data, related to either relevant or irrelevant class. Once a classification model is developed, malicious data is identified in real-time with minimal overhead. In decision making for intrusion detection stage, redundancy and uncertainty in the previous stages are further enhanced using random forest machine learning algorithm[106] along with active learning technique.[107] This stage protects the controller against network intrusion while detecting anomalies with improved accuracy. In the final stage, ie, the response system, EUNOIA employs a reactive routing and novel cost function. Simulation results show that the proposed system is lightweight and an efficient solution against the network intrusion detection. The drawback of EUONIA is that the cost function employed at the response system is straightforward and needs to be improved. Furthermore, EUNOIA exclusively considers a large volume of data. However, the effectiveness of the proposed methods should be studied and tested with varying sizes of data.

Robust and Agile Defense (RAD) system[102] is a reactive mechanism that guards the SDN controller against spoofing attacks while ensuring high availability and reliability of the underlying network. The design of RAD is based on three modules of a controller, ie, a traffic analyzer, a traffic engineer, and a rule manager. Each of these modules has its role and responsibilities. The role of the traffic analyzer is to monitor the bursty and bandwidth-starving traffic flows using sampled flow real-time (sFlowRT),[108] a real-time monitoring tool. A signature-based intrusion detection system, ie, snort IDS,[109] is used to recognize anomalies and attacks, based on attack signatures. Traffic engineering module, on the other hand, monitors network utilization and delay for each link. The link incurring high cost regarding these two metrics is excluded from the route generation. The authors aim for the creation of a suitable route for multi-dimensional and load balancing data with improved efficiency. The cost function of the traffic engineering module controls the preference weight of these two sub-modules and is responsible for the normalization of various ranges of metric values. Finally, the rule manager module creates the flow rules for the data layer and selection of the best routes for regulating traffic using both reactive and proactive approaches with increased scalability. Simulation result shows that RAD can easily be integrated with the SDN controller and enhance its performance. However, the proposed system fails to detect anomalies. Furthermore, RAD

should be evaluated using various topologies and attack scenarios using routing metrics other than the one used by the authors. The cost function used in the traffic engineering sub-module can be enhanced and evaluated for further studies.

Synaptic[98] is an automated method that performs automatic verification of security chains deployed at the control and data planes of an SDN architecture. Security chains consist of various security functions such as firewalls and intrusion detection systems and are responsible for the prevention of data leakage and any security violations. Due to the dynamic and complex nature of these security chains, it is essential to guard it against attacks, anomalies, and possible intrusion. Synaptic built formal verification models from security chains using a frenetic family of the SDN programming language, particularly using pyretic language along with an extension called Kinetic.[110-112] The role of the pyretic language is to specify network configuration in Python, which is later on compiled into low-level rules. On the other hand, the Kinetic extension is used to define policies for the control layer. All these functions are combined to generate formal models based on security chain specification before its implementation. Translation specification algorithms, eg, Satisfiability Modulo Theories (SMT)[113] are used at the data plane, while Kinetic is used at the control plane to translate specification of security chains into formal methods that can then be verified automatically. A prototype of the proposed approach is designed, and its performance is evaluated in term of response time and memory consumption with varying sizes of security chains using various validity checkers such as CVC4,[114] veriT,[113] and nuXmv.[115] Simulation results show that the proposed system can be enhanced further by using various translation algorithms that support more complex rules related to the said security functions. Furthermore, formal models that are generated by checked properties may be enhanced.

There are two types of Intrusion Detection System (IDS),[116] ie, a Host intrusion detection system (HIDS) and a network intrusion detection system (NIDS). In the work of Abubakar and Pranggono,[103] the authors proposed a two-stage Network Intrusion Detection System (NDIS). It is based on pattern recognition used for a neural network with machine learning approaches for the detection of signature and non-signature based attacks on an SDN controller. During the first stage, a virtual testbed is designed and developed to simulate the processes of a real network environment using a star topology. Hosts with the server and vice versa are connected to the OpenFlow switch for the detection of signature-based attacks. In the second stage, non-signature-based or unknown attacks are detected and are integrated with the signature-based architecture, designed for the previous stage. This hybrid approach can effectively detect both signature and non-signature-based attacks. Based on the simulation results, it was concluded that the proposed architecture achieves its objectives with 97% detection accuracy. However, this detection accuracy may be enhanced further using other neural network techniques.

The Byzantine fault-tolerant mechanism[97] is used to secure the control plane, data plane, and control-to-data plane interface against unauthorized access. The proposed mechanism manages each device at the data plane using multiple controllers.[117] Byzantine architecture ensures accurate updates of flow tables despite issuing false instructions by numerous compromised controllers. The authors have designed a cost-effective controller assignment algorithm, based on a heuristic, also known as Capacity First Allocation (CFA). The CFA ensures that an optimal number of controllers required for a given set of switches are maintained while satisfying their security requirements. The assignment algorithm serves two purposes. First, the varying number of controllers needed for each switch and, second, the number of switches served by a single controller. Thus, the proposed algorithm ensure to employ an optimal number of controllers needed for a switch, based on the minimum residual capacity of the controllers, while keeping in view the cost of deploying these controllers. Furthermore, Byzantine mechanism exchanges various messages between a set of controllers connected with a switch. Its performance is hugely dependent on the link latency among these controllers. The proposed algorithm is extensively simulated using various scenarios. Based on the simulations results, it was concluded that the proposed mechanism efficiently assigns the controllers based on the requirements for a given set of switches. The performance of the proposed architecture may be evaluated further using algorithms other than the one used in this paper. Furthermore, the proposed architecture may be studied further in more complex scenarios under different network conditions.

Another significant contribution is Athena,[96] an integrated, scalable, and distributed framework to support sophisticated anomaly detection across the control and data planes of an SDN controller. Athena's API offers the developers an abstraction from a complex data extraction service, with minimal programming effort while implementing and adding new and third party anomaly detection services to the SDN stack. This is because the proposed architecture does not require any specialized software except OpenFlow support. Compared with the previously available solutions, the proposed architecture include a variety of network features and detection algorithms for use in simplifying the design and deployment of general-purpose data plane-based anomaly detection framework in large-scale SDN networks. In terms of scalability, the network feature collection and data management of the proposed architecture uses a distributed database, a computing cluster, and a distributed controller. Network features are generated and collected above the controller instances in a distributed manner, and the same is published to the database. To speed up the runtime detection, Athena integrates a machine learning library and an anomaly detection algorithm, which is installed in the form of jobs at the computing cluster. Simulation results of the proposed architecture reveal that it can efficiently support well-known network anomaly detection services. However, the performance of the proposed method can be enhanced further using high performance distributed databases such as Cassandra, instead of MongoDB used by Athena.

Sampled-DP[95] is yet another essential anomaly detection framework. It is the combination of two algorithms, namely, density peak-based clustering algorithm with sampling adaptation and an unsupervised cluster-based feature selection mechanism. The density peak-based clustering algorithm with sampling adaptation algorithm automatically extracts the cluster centers and outlier points with increased memory and time efficiency, as opposed to the other such clustering methods in the literature. On the other hand, the second algorithm groups together attributes having maximum redundancy and remove them for feature selection purposes. The performance of sampled-DP is evaluated using KDDCup99 dataset.[118] It was concluded that the proposed framework outperforms the existing algorithms in term of runtime, adjusted mutual

information, homogeneity score, and detection accuracy. However, the sampled-DP needs to be improved further in such a way that it performs real-time packet clustering to protect the network much quicker against any possible intrusion. Furthermore, the performance of sampled-DP is dataset-dependent. Therefore, its behavior needs to be studied using complex datasets having a variety of features.

In the work of Tseng et al,[100] the authors proposed a controller-specific Dynamic Access Control system (DAC). According to the authors, the static permission does not protect the controller against API abuse. Therefore, DAC employs four dynamic permission controls, ie, read, add, update, and remove, for authorizing an Open Flow app to access an SDN controller. The DAC consists of three components, ie, a high-level policy engine, a northbound security extension between the control layer and application layer, and a controller-specific IDS. The high-level policy engine pre-defines and validates every request for each Open Flow application, according to the aforementioned permission set. The northbound security extension is responsible for authenticating and authorizing every request from Open Flow app as well as validating every request, using accounting records provided by the controller-specific IDS. This extension employs a token-based and password-based authentication. The controller-specific IDS, on the other hand, is responsible for the collection of information related to permission choices and accounting records from the database and high-level policy engine. Controller DAC is used on the top of four open source SDN controllers including OpenDaylight, ONOS, Floodlight, and Ryu. Simulation results show that the proposed methods can effectively and efficiently protect an SDN controller from API abuse vulnerabilities with a minor latency of less than 0.5%, using dynamic access control, as opposed to static control.

One of the challenging issues is how to select a set of switches for data sampling in an SDN with increased reliability and scalability. Yoon et al[101] tackled this issue by selecting switches with the relatively higher importance that improve the monitoring and performance of the IDS as well as reduces the chances of congestion in the network. The author has used a packet sampling technique by capturing only selected packets from the traffic flow at the selected set of switches for monitoring purposes. To overcome this issue, the authors employed a centrality measure, based on graph theory, as a packet sampling technique for the selection of packet sampling points among the switches in the network. It selects the sampling points based on the number of shortest paths that pass through a switch for all the node pairs.[119] Once a decision regarding data sampling points is confirmed, a decision sampling rate is made. Packets are sampled at the selected switches at a specific rate. The sampled data are then forwarded to an IDS for further analysis of malicious traffic and anomalies. Simulation results demonstrate that the proposed method enhances the performance of an IDS by efficiently capturing anomalies in a large-scale network. However, further experiments need to be carried out using sampling point techniques, other than the one employed in this paper.

4 | OPEN RESEARCH ISSUES, CHALLENGES, AND DIRECTIONS

The centralized and programmable nature of an SDN makes it a promising, innovative, and adaptable technology. It has simplified many issues related to the control and management of the next generation networks.[120,121] However, among others, security provisioning remains one of the major issue that hinder its widespread adoption.[122,123] This is particularly due to the centralized controller, which is responsible for the control and managemet of the overall network.[124] According to Hinden,[11] "why take over the hosts when you can take over the whole network?" It is therefore imperative to consider security as a service while designing an SDN network, in general, and the controller in particular.[12] To ensure security of the SDN controller, novel and innovative mechanisms need to be developed that are computationally lightweight and can efficiently and effectively identify malicious traffic.[125,126] Moreover, further studies should be carried out to study the characteristics of southbound interface (SBI), which facilitates communication between a controller and various network components at the data layer, ie, flow rules installation,[127,128] network configuration,[129] traffic statistics,[130] and optimal path selection.[131] These challenges should be addressed to protect the controller against malicious traffic that later on results in various security attacks such as DoS/DDos, spoofing, and malicious injection attacks.[122,132,133] Furthermore, such malicious traffic can disrupt various network operations required for the smooth functioning of a network. There is no built-in security mechanism at the southbound interface. This provides an ideal platform for adversaries to launch various attacks on the SDN controllers.[122,130] It is thus imperative to develop novel link scanning mechanisms, similar to the work of Mirkovic and Reiher,[134] to identify whether congestion on the southbound interface is caused by normal traffic or malicious traffic from an attacker.

The SDN controller is highly vulnerable to malicious traffic, particular during flooding attacks. These attacks disrupt various functions and services offered by the network in general and controller in particular to the legitimate users. In the literature, a threshold value is used to detect and mitigate such attacks and proved to be very effective.[135-137] Once the traffic at the network crosses that specific threshold value, flooding attack on the network is detected, and an alarm is raised. However, attacks such as flash crowd-based attacks[29] bypass these threshold-based mechanisms and are thus remain undetected. This is because the attackers craft their traffic to look legitimate and may use spoofed addresses to launch such attacks by making it very difficult to combat. Therefore, more research is needed that not only detect attacks on the basis of threshold value but also on novice IP address filtering techniques,[138,139] and deep packet inspection[140-142] that detect malicious packets with lower delay and increased accuracy.[143,144] The researchers should strive for novice and computationally lightweight traffic flow analysis techniques that analyze the characteristics of Open Flow traffic stored in switches at the data layer to identify the malicious traffic. Therefore, early detection of DDoS becomes an important area for further exploration.[133]

In SDN, real-time monitoring needs to be performed for the identification of malicious traffic with increased accuracy, primarily during large-scale DoS/DDoS attacks. Thus, accuracy is a major concern of various DDoS mitigation techniques.[145-147] It can help us to determine how accurately the system can detect the occurrence or absence of an attack. For instance, an inaccurate technique can generate a large number of

false alarms by making the traffic flow through the system unnoticed. It is thus important to quickly react to an attack by detecting it with high precision, particularly, during heavy traffic from the perpetrator in DDoS attacks. In addition, most of the existing DoS mitigation techniques incur higher communication and processing overhead during the detection stage in which the data from network components at the data layer are collected and transferred to the controller for decision making.[148-151] It is thus necessary to design novel monitoring and response mechanisms with lower computational overhead that alert the network component, detecting the attacker traffic and safeguarding the network from such attacks.[152,153] In this regard, some of the response mechanisms that need to be looked further in detail includes high enforced policy module with predefined actions,[154] identity management,[155] certification from multiple authorities,[156] threat isolation, and public key encryption of data.[122] Establishing an automatic trust management[157,158] and mutual authentication,[159] among the communicating entities, should be supported to protect the network from various known and unknown attacks.[122] Scalability is another important issue that needs to enhance in particular during the DDoS attack.[126,160,161] With the increasing rate, volume, and number of bots used in these attacks, defense mechanisms should be able to perform effectively in the presence of a large attack. In these situations, automatic network slicing is an effective technique for securing controllers against DDoS in distributed environments.[162] However, issues such as inconsistent configuration/synchronization[122,142,163] is a hidden security threat and need further research.

In addition, security of the existing mechanisms such as forensic remediation,[164,165] verification framework,[166] proactive and reactive recovery mechanisms,[122,167,168] resilient control planes,[34,168-171] SDN security framework,[40,172] state machine replication,[40,173,174] and dynamic, automated, and assured device association[175] should be enhanced to cater for the known and unknown attacks in the future. On the other hand, malicious packets can affect the network view that results in flow rule conflicts and policy violations. It is thus necessary to propose novel techniques that enforce the security by tackling the issue of policy violation in SDNs.[137,160,176] Moreover, for the effective mitigation of malware injection attacks, defense mechanisms such as N-version protection[177] should be investigated further.

5 | CONCLUSIONS

Despite the hype surrounding SDN, its security-related issues have not been explored in depth. It is because security was not considered initially, despite its core value in an SDN design. It is due to various aforementioned security issues among many other security dimensions that hinder its widespread adoption. It is thus imperative to tackle various security dimensions to make it a promising and secure technology; otherwise, its benefits might be quickly overcome by its security concerns. It is therefore utmost important to consider security as essential part while designing an SDN. In this paper, we have provided a comprehensive and critical discussion on the latest security attacks that exclusively target SDN controller along with a detailed discussion on their mitigation techniques, unlike previously related surveys that are either specific to a particular type of attack or discuss attacks on the whole SDN architecture. Furthermore, this paper provides guidance to the readers on the suitability of a particular mitigation technique for a particular scenario. Moreover, future directions and suggestions for securing SDN architecture in general and the control layer in particular are provided. From this survey, we have concluded that conducive efforts are needed to explore innovative methods for ensuring security of the SDN controller due to single point dependency. It is expected that more research efforts should be carried out to validate elements address, establish trust mechanisms between all elements, ensuring strong encryption, authentication, and access control among devices. Research should focus on designing highly accurate attack detection model and novice monitoring methods that report the sudden increase in packet-in events in advance. Unfortunately, cyber attacks may be detected, but after the damage is done. Therefore, developing a cyber system that can survive an attack is a challenge. However, our effort is to complement existing surveys and stimulate more research studies in this area in order to make SDN a secure, trustful, and dependable architecture in the years to come.

ACKNOWLEDGMENTS

The author Syed Rooh Ullah Jan is the equal first co-author of this paper. This work was supported in part by the International Scientific and Technological Cooperation Project of Dongguan (2016508102011) and in part by the Science and Technology Planning Project of Guangdong Province (2016A020210142).

ORCID

Muhammad Usman https://orcid.org/0000-0003-2165-4575
Mian Ahmad Jan https://orcid.org/0000-0002-5298-1328

REFERENCES

1. Jan MA, Usman M, He X, Rehman AU. SAMS: a seamless and authorized multimedia streaming framework for WMSN-based IoMT. *IEEE Internet Things J*. 2018.
2. Cheng X, Wu Y, Min G, Zomaya AY. Network function virtualization in dynamic networks: a stochastic perspective. *IEEE J Sel Areas Commun*. 2018;36(10):2218-2232.

3. Huang H, Yin H, Min G, Jiang H, Zhang J, Wu Y. Data-driven information plane in software-defined networking. *IEEE Commun Mag*. 2017;55(6):218-224.
4. Lara A, Kolasani A, Ramamurthy B. Network innovation using OpenFlow: a survey. *IEEE Commun Surv Tutor*. 2014;16(1):493-512.
5. Miao W, Min G, Wu Y, Wang H, Hu J. Performance modelling and analysis of software-defined networking under bursty multimedia traffic. *ACM Trans Multimed Comput Commun Appl*. 2016;12(5s):77.
6. Hu F, Hao Q, Bao K. A survey on software-defined network and OpenFlow: from concept to implementation. *IEEE Commun Surv Tutor*. 2014;16(4):2181-2206.
7. Kreutz D, Ramos FMV, Verissimo P, Rothenberg CE, Azodolmolky S, Uhlig S. Software-defined networking: a comprehensive survey. *Proc IEEE*. 2015;103(1):14-76.
8. Wang G, Zhao Y, Huang J, Wu Y. An effective approach to controller placement in software defined wide area networks. *IEEE Trans Netw Serv Manag*. 2018;15(1):344-355.
9. Xia W, Wen Y, Foh CH, Niyato D, Xie H. A survey on software-defined networking. *IEEE Commun Surv Tutor*. 2015;17(1):27-51.
10. Zuo Y, Wu Y, Min G, Cui L. Learning-based network path planning for traffic engineering. *Future Gener Comput Syst*. 2019;92:59-67.
11. Hinden RM. Why take over the hosts when you can take over the network. Paper presented at: RSA Conference; 2014; San Francisco, CA.
12. Akhunzada A, Gani A, Anuar NB, et al. Secure and dependable software defined networks. *J Netw Comput Appl*. 2016;61:199-221.
13. Hakiri A, Gokhale A, Berthou P, Schmidt DC, Gayraud T. Software-defined networking: challenges and research opportunities for future internet. *Computer Networks*. 2014;75:453-471.
14. Hong S, Xu L, Wang H, Gu G. Poisoning network visibility in software-defined networks: new attacks and countermeasures. Paper presented at: 22nd Annual Network and Distributed System Security Symposium (NDSS); 2015; San Diego, CA.
15. Shin S, Yegneswaran V, Porras P, Gu G. AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security; 2013; Berlin, Germany.
16. Wang H, Xu L, Gu G. Floodguard: a DoS attack prevention extension in software-defined networks. Paper presented at: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2015; Rio de Janeiro, Brazil.
17. Azzouni A, Boutaba R, Trang NTM, Pujolle G. sOFTDP: secure and efficient topology discovery protocol for SDN. 2017. arXiv preprint arXiv:1705.04527.
18. Liu J, Lai Y, Zhang S. FL-GUARD: a detection and defense system for DDoS attack in SDN. In: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy; 2017; Wuhan, China.
19. Scott-Hayward S, Natarajan S, Sezer S. A survey of security in software defined networks. *IEEE Commun Surv Tutor*. 2016;18(1):623-654.
20. Zaalouk A, Khondoker R, Marx R, Bayarou KM. OrchSec: an orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions. Paper presented at: 2014 IEEE Network Operations and Management Symposium (NOMS); 2014; Kraków, Poland.
21. Al-Zewairi M, Suleiman D, Almajali S. An experimental software defined security controller for software defined network. Paper presented at: 2017 Fourth International Conference on Software Defined Systems (SDS); 2017; Valencia, Spain.
22. Wang T, Chen H. SGuard: a lightweight SDN safe-guard architecture for DOS attacks. *China Communications*. 2017;14(6):113-125.
23. Bertaux L, Hakiri A, Medjiah S, Berthou P, Abdellatif S. A DDS/SDN based communication system for efficient support of dynamic distributed real-time applications. Paper presented at: 2014 IEEE/ACM 18th International Symposium on Distributed Simulation and Real Time Applications (DS-RT); 2014; Toulouse, France.
24. Farhady H, Lee HY, Nakao A. Software-defined networking: a survey. *Computer Networks*. 2015;81:79-95.
25. Hu F. *Network Innovation Through OpenFlow and SDN: Principles and Design*. Boca Raton, FL: CRC Press; 2014.
26. Jagadeesan NA, Krishnamachari B. Software-defined networking paradigms in wireless networks: a survey. *ACM Comput Surv*. 2015;47(2):27.
27. Li W, Meng W, Kwok LF. A survey on OpenFlow-based software defined networks: security challenges and countermeasures. *J Netw Comput Appl*. 2016;68:126-139.
28. Ahmad I, Namal S, Ylianttila M, Gurtov A. Security in software defined networks: a survey. *IEEE Commun Surv Tutor*. 2015;17(4):2317-2346.
29. Bawany NZ, Shamsi JA, Salah K. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arab J Sci Eng*. 2017;42(2):425-441.
30. Dargahi T, Caponi A, Ambrosin M, Bianchi G, Conti M. A survey on the security of stateful SDN data planes. *IEEE Commun Surv Tutor*. 2017;19(3):1701-1725.
31. Haque MR, Tan SC, Yusoff Z, Lee CK, Kaspin R. DDos attack monitoring using smart controller placement in software defined networking architecture. In: *Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018*. Berlin, Germany: Springer; 2019:195-203.
32. Karmakar KK, Varadharajan V, Tupakula U. Mitigating attacks in software defined network (SDN). Paper presented at: 2017 Fourth International Conference on Software Defined Systems (SDS); 2017; Valencia, Spain.
33. Scott-Hayward S, O'Callaghan G, Sezer S. SDN security: a survey. Paper presented at: 2013 IEEE SDN for Future Networks and Services (SDN4FNS); 2013; Trento, Italy.
34. Shaghaghi A, Kaafar MA, Buyya R, Jha S. Software-defined network (SDN) data plane security: issues, solutions and future directions. 2018. arXiv preprint arXiv:1804.00262.
35. Xiao R, Zhu H, Song C, Liu X, Dong J, Li H. Attacking network isolation in software-defined networks: new attacks and countermeasures. Paper presented at: 2018 27th International Conference on Computer Communication and Networks (ICCCN); 2018; Hangzhou, China.
36. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges. *IEEE Commun Surv Tutor*. 2016;18(1):602-622.
37. Alsmadi I, Xu D. Security of software defined networks: a survey. *Comput Secur*. 2015;53:79-108.
38. Banse C, Rangarajan S. A secure northbound interface for SDN applications. Paper presented at: 2015 IEEE Trustcom/BigDataSE/ISPA; 2015; Helsinki, Finland.

39. Kloti R, Kotronis V, Smith P. OpenFlow: a security analysis. Paper presented at: 2013 21st IEEE International Conference on Network Protocols (ICNP); 2013; Göttingen, Germany.
40. Zhang H, Cai Z, Liu Q, Xiao Q, Li Y, Cheang CF. A survey on security-aware measurement in SDN. *Secur Commun Netw*. 2018;2018.
41. Vissicchio S, Vanbever L, Bonaventure O. Opportunities and research challenges of hybrid software defined networks. *ACM SIGCOMM Comput Commun Rev*. 2014;44(2):70-75.
42. *Software-Defined Networking: The New Norm for Networks*. Vol 2. ONF White Paper. Menlo Park, CA: Open Networking Foundation: 2012:2-6.
43. Nunes BAA, Mendonca M, Nguyen X-N, Obraczka K, Turletti T. A survey of software-defined networking: past, present, and future of programmable networks. *IEEE Commun Surv Tutor*. 2014;16(3):1617-1634.
44. Haleplidis E, Pentikousis K, Denazis S, Salim JH, Meyer D, Koufopavlou O. Software-defined networking (SDN): layers and architecture terminology. RFC 7426. 2015.
45. Jarraya Y, Madi T, Debbabi M. A survey and a layered taxonomy of software-defined networking. *IEEE Commun Surv Tutor*. 2014;16(4):1955-1980.
46. Doria A, Salim JH, Haas R, et al. Forwarding and control element separation (forCES) protocol specification. RFC 5810. 2010.
47. Song H. Protocol-oblivious forwarding: unleash the power of SDN through a future-proof forwarding plane. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking; 2013; Hong Kong, China.
48. Jain R, Paul S. Network virtualization and software defined networking for cloud computing: a survey. *IEEE Commun Mag*. 2013;51(11):24-31.
49. Govindarajan K, Meng KC, Ong H. A literature review on software-defined networking (SDN) research topics, challenges and solutions. Paper presented at: 2013 Fifth International Conference on Advanced Computing (ICoAC); 2013; Chennai, India.
50. Metzler J. Understanding software-defined networks. InformationWeek Reports. 2012:1-25.
51. Dacier MC, Dietrich S, Kargl F, König H. Overview of talks: network monitoring & SDN. In: *Network Attack Detection and Defense-Security Challenges and Opportunities of Software-Defined Networking*. Wadern, Germany: Dagstuhl Publishing; 2017.
52. Ramos FMV, Kreutz D, Verissimo P. Software-defined networks: on the road to the softwarization of networking. *Cutter IT J*. 2015.
53. Gandhi R, Sharma A, Mahoney W, Sousan W, Zhu Q, Laplante P. Dimensions of cyber-attacks: cultural, social, economic, and political. *IEEE Technol Soc Mag*. 2011;30(1):28-38.
54. Boite J, Nardin P-A, Rebecchi F, Bouet M, Conan V. StateSec: stateful monitoring for DDoS protection in software defined networks. Paper presented at: 2017 IEEE Conference on Network Softwarization (NetSoft); 2017; Bologna, Italy.
55. Dillon C, Berkelaar M. OpenFlow (d) DoS mitigation. 2014.
56. Dotcenko S, Vladyko A, Letenko I. A fuzzy logic-based information security management for software-defined networks. Paper presented at: 2014 16th International Conference on Advanced Communication Technology (ICACT); 2014; Pyeongchang, South Korea.
57. Huang X, Du X, Song B. An effective DDoS defense scheme for SDN. Paper presented at: 2017 IEEE International Conference on Communications (ICC); 2017; Paris, France.
58. Johnson JL. Design of experiments and progressively sequenced regression are combined to achieve minimum data sample size. *Int J Hydromechatronics*. 2018;1(3):308-331.
59. Mousavi SM, St-Hilaire M. Early detection of DDoS attacks against SDN controllers. Paper presented at: 2015 International Conference on Computing, Networking and Communications (ICNC); 2015; Garden Grove, CA.
60. Shivakumara P, Tang D, Asadzadehkaljahi M, Lu T, Pal U, Anisi MH. CNN-RNN based method for license plate recognition. *CAAI Trans Intell Technol*. 2018;3(3):169-175.
61. Wang R, Jia Z, Ju L. An entropy-based distributed DDoS detection mechanism in software-defined networking. Paper presented at: 2015 IEEE Trustcom/BigDataSE/ISPA; 2015; Helsinki, Finland.
62. Zhang S, Iwashita H, Sanada K. Thermal performance difference of ideal gas model and van der Waals gas model in gas-loaded accumulator. *Int J Hydromechatronics*. 2018;1(3):293-307.
63. Zhou Y, Sun Q, Liu J. Robust optimisation algorithm for the measurement matrix in compressed sensing. *CAAI Trans Intell Technol*. 2018;3(3):133-139.
64. Lakhina A, Crovella M, Diot C. Mining anomalies using traffic feature distributions. *ACM SIGCOMM Comput Commun Rev*; 2005;35(4):217-228.
65. Fiadino P, D'Alconzo A, Schiavone M, Casas P. Challenging entropy-based anomaly detection and diagnosis in cellular networks. *ACM SIGCOMM Comput Commun Rev*. 2015;45(4):87-88.
66. Javed M, Ashfaq AB, Shafiq MZ, Khayam SA. On the inefficient use of entropy for anomaly detection. In: *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009. Proceedings*. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2009.
67. Kohonen T. The self-organizing map. *Neurocomputing*. 1998;21(1-3):1-6.
68. Schechter SE, Jung J, Berger AW. Fast detection of scanning worm infections. In: *Recent Advances in Intrusion Detection: 7th International Symposium, RAID 2004, Sophia Antipolis, France, September 15-17, 2004. Proceedings*. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2004.
69. Chai Y, Jia L, Zhang Z. Mamdani model based adaptive neural fuzzy inference system and its application. *Int J Comput Intell*. 2009;5(1):22-29.
70. Nguyen T-H, Yoo M. A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers. *Int J Distributed Sens Netw*. 2017;13(11). https://doi.org/10.1177/1550147717739157
71. De Vivo M, de Vivo GO, Isern G. Internet security attacks at the basic levels. *ACM SIGOPS Oper Syst Rev*. 1998;32(2):4-15.
72. Halili R. Network security and spoofing attacks. 2018. https://pecb.com/article/network-security-and-spoofing-attacks-
73. Akhunzada A, Ahmed E, Gani A, Khan MK, Imran M, Guizani S. Securing software defined networks: taxonomy, requirements, and open issues. *IEEE Commun Mag*. 2015;53(4):36-44.
74. AbdelSalam AM, El-Sisi AB, Reddy R. Mitigating ARP spoofing attacks in software-defined networks. Paper presented at: 2016 26th International Conference on Computer Theory and Applications (ICCTA); 2016; Alexandria, Egypt.
75. Abdulqadder IH, Zou D, Aziz IT, Yuan B. Validating user flows to protect software defined network environments. *Secur Commun Netw*. 2018;2018.

76. Al-Ayyoub M, Jararweh Y, Benkhelifa E, Vouk M, Rindos A. SDSecurity: a software defined security experimental framework. Paper presented at: 2015 IEEE International Conference on Communication Workshop (ICCW); 2015; London, UK.
77. Ertaul L, Venkatachalam K. Security of software defined networks (SDN). In: Proceedings of the 2017 International Conference on Wireless Networks (ICWN); 2017; Las Vegas, NV.
78. Francois J, Festor O. Anomaly traceback using software defined networking. Paper presented at: 2014 IEEE International Workshop on Information Forensics and Security (WIFS); 2014; Atlanta, GA.
79. Kim S, Lee S, Cho G, Ahmed ME, Jeong JP, Kim H. Preventing DNS amplification attacks using the history of DNS queries with SDN. In: *Computer Security - ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*. Cham, Switzerland: Springer International Publishing; 2017.
80. Liyanage M, Ahmed I, Okwuibe J, et al. Enhancing security of software defined mobile networks. *IEEE Access*. 2017;5:9422-9438.
81. Tang H, Xu C, Luo X, OuYang J. Traceback-based bloomfilter IPS in defending SYN flooding attack. Paper presented at: 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom); 2009; Beijing, China.
82. Ubaid F, Amin R, Ubaid FB, Iqbal MM. Mitigating address spoofing attacks in hybrid SDN. *Int J Adv Comput Sci Appl*. 2017;8(4):562-570.
83. Fan Z, Xiao Y, Nayak A, Tan C. An improved network security situation assessment approach in software defined networks. *Peer-to-Peer Netw Appl*. 2019;12(2):295-309.
84. OpenHIP. The OpenHIP project. 2018. www.openhip.org
85. Alharbi T, Portmann M, Pakzad F. The (in) security of topology discovery in software defined networks. Paper presented at: 2015 IEEE 40th Conference on Local Computer Networks (LCN); 2015; Clearwater Beach, FL.
86. Blumenthal U, Maino F, McCloghrie K. The advanced encryption standard (AES) cipher algorithm in the SNMP user-based security model. RFC 3826. 2004.
87. Dierks T, Rescorla E. The transport layer security (TLS) protocol version 1.2. RFC 5246. 2008.
88. Rabiner LR, Juang B-H. An introduction to hidden Markov models. *IEEE ASSP Mag*. 1986;3(1):4-16.
89. Welch LR. Hidden Markov models and the Baum-Welch algorithm. *IEEE Inf Theory Soc Newsl*. 2003;53(4):10-13.
90. Hendrix H. *Viterbi Decoding Techniques in the TMS320C54x Family*. Application Report. Dallas, TX: Texas Instruments; 1996.
91. Ciardo G. Discrete-time Markovian stochastic Petri nets. In: *Computations With Markov Chains: Proceedings of the 2nd International Workshop on the Numerical Solution of Markov Chains*. Berlin, Germany: Springer; 1995;339-358.
92. Nguyen T-H, Yoo M. Analysis of link discovery service attacks in SDN controller. Paper presented at: 2017 International Conference on Information Networking (ICOIN); 2017; Da Nang, Vietnam.
93. Deng S, Gao X, Lu Z, Gao X. Packet injection attack and its defense in software-defined networks. *IEEE Trans Inf Forensics Secur*. 2018;13(3):695-705.
94. Halfond WG, Viegas J, Orso A. A classification of SQL-injection attacks and countermeasures. In: Proceedings of the IEEE International Symposium on Secure Software Engineering; 2006; Arlington, VA.
95. He D, Chan S, Ni X, Guizani M. Software-defined-networking-enabled traffic anomaly detection and mitigation. *IEEE Internet Things J*. 2017;4(6):1890-1898.
96. Lee S, Kim J, Shin S, Porras P, Yegneswaran V. Athena: a framework for scalable anomaly detection in software-defined networks. Paper presented at: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2017; Denver, CO.
97. Li H, Li P, Guo S, Nayak A. Byzantine-resilient secure software-defined networks with multiple controllers in cloud. *IEEE Trans Cloud Comput*. 2014;2(4):436-447.
98. Schnepf N, Badonnel R, Lahmadi A, Merz S. Automated verification of security chains in software-defined networks with synaptic. Paper presented at: 2017 IEEE Conference on Network Softwarization (NetSoft); 2017; Bologna, Italy.
99. Song C, Park Y, Golani K, Kim Y, Bhatt K, Goswami K. Machine-learning based threat-aware system in software defined networks. Paper presented at: 2017 26th International Conference on Computer Communication and Networks (ICCCN); 2017; Vancouver, Canada.
100. Tseng Y, Pattaranantakul M, He R, Zhang Z, Naït-Abdesselam F. Controller DAC: securing SDN controller with dynamic access control. Paper presented at: 2017 IEEE International Conference on Communications (ICC); 2017; Paris, France.
101. Yoon S, Ha T, Kim S, Lim H. Scalable traffic sampling using centrality measure on software-defined networks. *IEEE Commun Mag*. 2017;55(7):43-49.
102. Kim M, Park Y, Kotalwar R. Robust and agile system against fault and anomaly traffic in software defined networks. *Applied Sciences*. 2017;7(3):266.
103. Abubakar A, Pranggono B. Machine learning based intrusion detection system for software defined networks. Paper presented at: 2017 Seventh International Conference on Emerging Security Technologies (EST); 2017; Canterbury, UK.
104. McKeown N, Anderson T, Balakrishnan H, et al. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Comput Commun Rev*. 2008;38(2):69-74.
105. Sinclair C, Pierce L, Matzner S. An application of machine learning to network intrusion detection. In: Proceedings of the 1999 15th Annual Computer Security Applications Conference (ACSAC); 1999; Phoenix, AZ.
106. Breiman L. Random forests. *Machine Learning*. 2001;45(1):5-32.
107. Cohn DA, Ghahramani Z, Jordan MI. Active learning with statistical models. *J Artif Intell Res*. 1996;4:129-145.
108. sFlow RT. A real-time monitoring tool (sampled flow real-time). 2018. www.inmon.com/products/sFlow-RT.php
109. Snort. A signature based intrusion detection system (Snort ids). 2018. www.en.wikipedia.org/wiki/Snort
110. Foster N, Guha A, Reitblatt M, et al. Languages for software-defined networks. *IEEE Commun Mag*. 2013;51(2):128-134.
111. Foster N, Harrison R, Freedman MJ, et al. Frenetic: a network programming language. *ACM SIGPLAN Notices*. 2011;46(9):279-291.
112. Kim H, Reich J, Gupta A, Shahbaz M, Feamster N, Clark R. Kinetic: verifiable dynamic network control. Paper presented at: 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI); 2015; Oakland, CA.

113. Bouton T, de Oliveira DCB, Déharbe D, Fontaine P. veriT: an open, trustable and efficient SMT-solver. In: *Automated Deduction - CADE-22: 22nd International Conference on Automated Deduction, Montreal, Canada, August 2-7, 2009. Proceedings.* Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2009.
114. Barrett C, Sebastiani R, Seshia SA, Tinelli C. Satisfiability modulo theories. In: *Handbook of Satisfiability*. Vol 185. Amsterdam, The Netherlands: IOS Press; 2009:825-885.
115. Cavada R, Cimatti A, Dorigatti M, et al. The nuXmv symbolic model checker. In: *Computer Aided Verification: 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings.* Cham, Switzerland: Springer International Publishing; 2014.
116. Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. In: Proceedings of the 2002 International Joint Conference on Neural Networks (IJCNN); 2002; Honolulu, HI.
117. Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst*. 2002;20(4):398-461.
118. KDDCup (KDDCup99 dataset). 1999. www.kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
119. Freeman LC. A set of measures of centrality based on betweenness. *Sociometry*. 1977;40(1):35-41.
120. Ali SR. Software defined networking (SDN). In: *Next Generation and Advanced Network Reliability Analysis: Using Markov Models and Software Reliability Engineering*. Cham, Switzerland: Springer; 2019;105-130.
121. Rana DS, Dhondiyal SA, Chamoli SK. Software defined networking (SDN) challenges, issues and solution. *Int J Comput Sci Eng*. 2019;7(1):884-889.
122. Benabbou J, Elbaamrani K, Idboufker N. Security in OpenFlow-based SDN, opportunities and challenges. *Photonic Netw Commun*. 2019;37(1):1-23.
123. Sahoo KS, Panda SK, Sahoo S, Sahoo B, Dash R. Toward secure software-defined networks against distributed denial of service attack. *J Supercomput*. 2019:1-46.
124. Zhu L, Karim MM, Sharif K, Li F, Du X, Guizani M. SDN controllers: benchmarking & performance evaluation. 2019. arXiv preprint arXiv:1902.04491.
125. Koning R, de Graaff B, Polevoy G, Meijer R, de Laat C, Grosso P. Measuring the efficiency of SDN mitigations against attacks on computer infrastructures. *Future Gener Comput Syst*. 2019;91:144-156.
126. Sultana N, Chilamkurti N, Peng W, Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Netw Appl*. 2019;12(2):493-501.
127. Bera S, Misra S, Jamalipour A. FlowStat: adaptive flow-rule placement for per-flow statistics in SDN. *IEEE J Sel Areas Commun*. 2019;37(3):530-539.
128. Comer D, Rastegarnia A. Towards disaggregating the SDN control plane. 2019. arXiv preprint arXiv:1902.00581.
129. Shimanaka T, Masuoka R, Hay B. Cyber deception architecture: covert attack reconnaissance using a safe SDN approach. In: Proceedings of the 52nd Hawaii International Conference on System Sciences; 2019; Maui, HI.
130. Demirpolat A, Ergenç D, Ozturk E, Ayar Y, Onur E. Software-defined network security. In: *Enabling Technologies and Architectures for Next-Generation Networking Capabilities*. Hershey, PA: IGI Global; 2019:232-253.
131. Alouache L, Nguyen N, Aliouat M, Chelouah R. Survey on IoV routing protocols: security and network architecture. *Int J Commun Syst*. 2019;32(2):e3849.
132. Alshra'a AS, Seitz J. Using inspector device to stop packet injection attack in SDN. *IEEE Commun Lett*. 2019.
133. McGrew D, Beck KS, inventors: Cisco Technology Inc, assignee. Inspection of traffic via SDN. US patent 10205641. February 12, 2019.
134. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput Commun Rev*. 2004;34(2):39-53.
135. David J, Thomas C. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. *Comput Secur*. 2019;82:284-295.
136. Bhagat Patil AR, Thakur NV. Mitigation against denial-of-service flooding and malformed packet attacks. In: *Third International Congress on Information and Communication Technology: ICICT 2018, London*. Berlin, Germany: Springer; 2019.
137. Wang Y, Hu T, Tang G, Xie J, Lu J. SGS: safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking. *IEEE Access*. 2019;7:34699-34710.
138. Dao N-N, Park J, Park M, Cho S. A feasible method to combat against DDoS attack in SDN network. Paper presented at: 2015 International Conference on Information Networking (ICOIN); 2015; Siem Reap, Cambodia.
139. Li C, Qin Z, Novak E, Li Q. Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet Things J*. 2017;4(5):1156-1164.
140. Bonfim MS, Dias KL, Fernandes SFL. Integrated NFV/SDN architectures: a systematic literature review. *ACM Comput Surv*. 2019;51(6). Article No 114.
141. Shanbhag P, Dronadula LN, Abhilash R, inventors: Fortinet Inc, assignee. Reducing multicast service traffic for matching and streaming in SDN (software defined networking enabled networks. US patent 10193763. January 29, 2019.
142. Yu C, Lan J, Guo Z, Hu Y, Baker T. An adaptive and lightweight update mechanism for SDN. *IEEE Access*. 2019;7:12914-12927.
143. D'Cruze H, Wang P, Sbeit RO, Ray A. A software-defined networking (SDN) approach to mitigating DDoS attacks. In: *Information Technology-New Generations: 14th International Conference on Information Technology*. Cham, Switzerland: Springer International Publishing; 2018;141-145.
144. Miao W, Min G, Wu Y, et al. Stochastic performance analysis of network function virtualisation in future internet. *IEEE J Sel Areas Commun*. 2019;37(3):613-626.
145. Abdulqadder I, Zou D, Aziz I, Yuan B, Dai W. Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment. *IEEE Trans Emerg Top Comput*. 2018.
146. Fawcett L, Scott-Hayward S, Broadbent M, Wright A, Race N. Tennison: a distributed SDN framework for scalable network security. *IEEE J Sel Areas Commun*. 2018;36(12):2805-2818.
147. Nguyen TN. The challenges in SDN/ML based network security: a survey. 2018. arXiv preprint arXiv:1804.03539.
148. Cabaj K, Gregorczyk M, Mazurczyk W, Nowakowski P, Żórawski P. Network threats mitigation using software-defined networking for the 5G internet of radio light system. *Secur Commun Netw*. 2019;2019.
149. Liu G, Quan W, Cheng N, Zhang H, Yu S. Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things. *J Netw Comput Appl*. 2019;130:1-13.

150. Ni J, Lin X, Shen XS. Toward edge-assisted Internet of Things: from security and efficiency perspectives. 2019. arXiv preprint arXiv:1902.07094.
151. Rebecchi F, Boite J, Nardin P-A, Bouet M, Conan V. DDos protection with stateful software-defined networking. *Int J Netw Manag*. 2019;29(1):e2042.
152. Cui J, Lu Q, Zhong H, Tian M, Liu L. A load-balancing mechanism for distributed SDN control plane using response time. *IEEE Trans Netw Serv Manag*. 2018;15(4):1197-1206.
153. Ros FJ, Ruiz PM. Five nines of southbound reliability in software-defined networks. In: Proceedings of the Third Workshop on Hot Topics in Software Defined Networking; 2014; Chicago, IL.
154. Maziku H, Shetty S, Nicol DM. Security risk assessment for SDN-enabled smart grids. *Computer Communications*. 2019;133:1-11.
155. Alsmadi I. Identity management. In: *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics*. Cham, Switzerland: Springer; 2019;313-329.
156. Reddy T, Wing D, Patil P, inventors. Short term certificate management during distributed denial of service attacks. US patent app 16/110,102. January 10, 2019.
157. Talbi S, Bouabdallah A. Interest-based trust management scheme for social Internet of Things. *J Ambient Intell Humaniz Comput*. 2019:1-12.
158. Zhong H, Sheng J, Xu Y, Cui J. SCPLBS: a smart cooperative platform for load balancing and security on SDN distributed controllers. *Peer-to-Peer Netw Appl*. 2019;12(2):440-451.
159. Umer T, Rehmani MH, Kamal AE, Mihaylova L. Information and resource management systems for Internet of Things: energy management, communication protocols and future applications. *Future Gener Comput Syst*; 2019;92:1021-1027.
160. Paladi N, Gehrmann C. SDN access control for the masses. *Comput Secur*. 2019;80:155-172.
161. Weng J-S, Weng J, Zhang Y, Luo W, Lan W. BENBI: scalable and dynamic access control on the northbound interface of SDN-based VANET. *IEEE Trans Veh Technol*. 2019;68(1):822-831.
162. Do S, Le LV, Paul Lin BS, Tung L-P. SDN/NFV based Internet of Things for multi-tenant networks. *Trans Netw Commun*. 2019;6(6):40.
163. Priya ID, Silas S. A survey on research challenges and applications in empowering the SDN-based Internet of Things. In: *Advances in Big Data and Cloud Computing: Proceedings of ICBDCC18*. Berlin, Germany: Springer; 2019.
164. Kobo HI, Abu-Mahfouz AM, Hancke GP. A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE Access*. 2017;5:1872-1899.
165. Patil P, Hash L, White J, Tekeoglu A. *Security Challenges in SDN Implementation* [master's thesis]. Utica, NY: State University of New York Polytechnic Institute; 2018.
166. Amin R, Reisslein M, Shah N. Hybrid SDN networks: a survey of existing approaches. *IEEE Commun Surv Tutor*. 2018;20(4):3259-3306.
167. Abdallah S, Elhajj IH, Chehab A, Kayssi A. A network management framework for SDN. Paper presented at: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 2018; Paris, France.
168. Machuca CM, Vizarreta P, Durner R, Santos D, de Sousa A. Design problems towards reliable SDN networks. In: Proceedings of the Photonic Networks and Devices; 2018; Zürich, Switzerland.
169. Dvir A, Haddad Y, Zilberman A. Wireless controller placement problem. Paper presented at: 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC); 2018; Las Vegas, NV.
170. Gillani F, Al-Shaer E, Duan Q. In-design resilient SDN control plane and elastic forwarding against aggressive DDoS attacks. In: Proceedings of the 5th ACM Workshop on Moving Target Defense; 2018; Toronto, Canada.
171. Vestin J. *SDN-Enabled Resiliency in Computer Networks* [PhD thesis]. Karlstad, Sweden: Karlstads Universitet; 2018.
172. Kreutz D, Yu J, Esteves-Veríssimo P, Magalhães C, Ramos FMV. The kiss principle in software-defined networking: a framework for secure communications. *IEEE Secur Priv*. 2018;16(5):60-70.
173. Nayyer A, Sharma AK, Awasthi LK. Issues in software-defined networking. In: *Proceedings of 2nd International Conference on Communication, Computing and Networking: ICCCN 2018, NITTTR Chandigarh, India*. Berlin, Germany: Springer; 2019.
174. Nguyen B, Zhang T, Radunovic B, et al. *A Reliable Distributed Cellular Core Network for Hyper-Scale Public Clouds*. Technical Report. Redmond, WA: Microsoft Corporation; 2018. https://www.microsoft.com/en-us/research/uploads/prod/2018/02/ECHO-TR.pdf
175. Zhang S, Li X, Tan Z, Peng T, Wang G. A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services. *Future Gener Comput Syst*. 2019;94:40-50.
176. Jabal AA, Davari M, Bertino E, et al. Methods and tools for policy analysis. *ACM Comput Surv*. 2019;51(6):121.
177. Zheng J, Namin AS. A survey on the moving target defense strategies: an architectural perspective. *J Comput Sci Technol*. 2019;34(1):207-233.

How to cite this article: Han T, Jan SRU, Tan Z, et al. A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. *Concurrency Computat Pract Exper*. 2020;32:e5300. https://doi.org/10.1002/cpe.5300