Ingeniería Solidaria

Security in SDN networks and their applications

La seguridad en redes SDN y sus aplicaciones

Segurança em redes SDN e suas aplicações

Robin Estid Tapiero Tapiero[1]
Edward Alejandro Cerquera González[2]
Norberto Novoa Torres[3]

Received: January 15 th, 2020
Accepted: March 10th, 2020
Available: May 5th, 2021

How to cite this article:
R.E. Tapiero Tapiero, E.A. Cerquera González, N. Novoa Torres. "Security in SDN networks and their applications" *Revista Ingeniería Solidaria,* vol. 17, no. 2, 2021.
doi: https://doi.org/10.16925/2357-6014.2021.02.09

Research article. https://doi.org/10.16925/2357-6014.2021.02.09

[1] Telematic engineering student. Technological faculty. Francisco Jose de Caldas Distrital University. Bogotá Colombia.

Email: retapierot@correo.udistrital.edu.co

ORCID: https://orcid.org/0000-0002-9489-699X

CvLAC: 0001791732202061493

[2] Telematic engineering student. Technological faculty. Francisco Jose de Caldas Distrital University. Bogotá Colombia.

Email: edgonzalezc@correo.udistrital.edu.co

ORCID: https://orcid.org/0000-0002-7909-7815

CvLAC: 0001791731202061493

[3] Professor. Technological faculty. Francisco Jose de Caldas Distrital University. Bogotá Colombia.

Email: nnovoat@udistrital.edu.co

ORCID: https://orcid.org/0000-0003-3374-7760

Abstract

Introduction: The review article is the product of the research on Security in SDN networks and their applications, developed at the District University in 2020, presenting the latest advances, that have been made in security.

Problem: The security weaknesses that SDN networks have had, due to being a new architecture. This has not allowed traditional networks to be replaced.

Objective: To carry out a review of the state of the art of SDN networks, focusing research on the security of the control layer and its advances**.**

Methodology: The descriptive method is implemented, consulting databases such as Scopus, IEEE and ScienceDirect, using the following search criteria: SDN networks, security in SDN networks, applications with SDN networks and OpenFlow protocol. It is shown as a research sample: the Asian, European and American continents with years of research from 2014 to 2020.

Results: Great advances have been made in terms of security for SDN networks, which allows us to see an early solution to the weaknesses that it currently faces.

Conclusion: SDN networks will solve all the challenges they face and will be consolidated as a solid and reliable architecture.

Originality: an important focus is taken on the security of SDN networks and the great development that has occurred in this regard is evident.

Limitations: SDN networks are a new architecture, so their development has been very little and advances in security have been significantly affected.

Keywords: Software Defined Networks (SDN), Internet of Things (IoT), Network Function Virtualization (NFV), Open Flow protocol, Security.

Resumen

Introducción: Este artículo de revisión es resultado de una investigación sobre redes SDN y sus aplicaciones, desarrollado en la Universidad Distrital durante 2020. Presenta los últimos avances hechos en seguridad.

Objetivo: Realizar una revisión del estado del arte de las redes SDN, centrando la investigación en la seguridad del plano de control y sus avances.

Metodología: Se implementa el método descriptivo, consultando bases de datos como Scopus, IEEE y ScienceDirect, usando los siguientes criterios: redes SDN, seguridad en redes SDN, aplicaciones de las redes SDN y protocolo OpenFlow. La muestra de la investigación estuvo conformada por artículos publicados en el continente asiático, europeo y americano entre 2015 y 2020.

Resultados: Se han hecho grandes avances en términos de seguridad para las redes SDN, lo que permite vislumbrar soluciones a sus falencias actuales.

Conclusión: Las redes SDN resolverán los retos a los que se enfrentan y se consolidarán como arquitecturas sólidas y confiables.

Originalidad: Se le da un enfoque importante en la seguridad de las redes SDN y se evidencia el gran desarrollo que se ha dado en este sentido.

Limitaciones: Las redes SDN son una nueva arquitectura, así que su desarrollo es reciente y los avances en seguridad han sido seriamente afectados.

Palabras clave: Redes Definidas por Software (SDN), Internet de las cosas (IoT), virtualización de las funciones de red (NFV), protocolo OpenFlow.

Resumo

Introdução: Este artigo de revisão é resultado de uma pesquisa sobre redes SDN e suas aplicações, desenvolvida na District University durante o ano de 2020. Apresenta os últimos avanços em segurança.

Alvo: Realizar uma revisão do estado da arte das redes SDN, focando pesquisas em segurança de plano de controle e seus avanços.

Metodologia: O método descritivo é implementado, consultando bases de dados como Scopus, IEEE e ScienceDirect, utilizando os seguintes critérios: redes SDN, segurança em redes SDN, aplicações de redes SDN e protocolo OpenFlow. A amostra da pesquisa foi composta por artigos publicados nos continentes asiático, europeu e americano entre 2015 e 2020.

Resultados: Grandes avanços foram feitos em termos de segurança para redes SDN, o que nos permite vislumbrar soluções para suas deficiências atuais.

Conclusão: As redes SDN resolverão os desafios que enfrentam e serão consolidadas como arquiteturas sólidas e confiáveis.

Originalidade: Um foco importante é dado à segurança das redes SDN e é evidente o grande desenvolvimento que ocorreu nesse sentido.

Limitações: As redes SDN são uma arquitetura nova, portanto seu desenvolvimento é recente e os avanços em segurança foram seriamente afetados.

Palavras-chave: Redes Definidas por Software (SDN), Internet das Coisas (IoT), Virtualização de Funções de Rede (NFV), protocolo OpenFlow.

1. INTRODUCTION

Since organizations have increased their demand for infrastructure, network administrators have had to face the challenge of keeping the entire network operating optimally [1], a task that is not easy due to the continuous scaling requests, interoperability, and high availability, among other aspects, that has been given thanks to the multiple users requests in business applications; saturating the operation of the network and lagging behind the growth needs that organizations demand [2].

What makes the arrival of SDN networks necessary as a solution to this problem. Thanks to the infrastructure offered [3], where the data plane is disaggregated from the control plane, centralizing all administration in a node that is responsible for managing the flow of information that circulates through the control layer [4], by means of flow charts and network security guidelines, across the OpenFlow protocol that allows managing the network as a whole [5], not as a number of individual devices to be managed, with the server itself managing the switches that should send the packets. Concentrating package delivery orders in the control plane. The security problems that SDN networks still face and how the applications that articulate them, have dealt with these drawbacks [6]. Besides the development that they have presented in recent years for technologies such as IoT, Data centers and 5G, which has been evolving the work of SDN networks and projecting the disappearance of traditional networks to make way for the network of the future [7].

1.1 Literature review or research history

To develop the topics of this review article, the descriptive method [8] is used, which seeks through the exact description, to know the architecture and processes that make up the SDN networks as a focus of study [9], specifying the most relevant properties through an analysis, without altering the study factor. For this purpose some items will be proposed, which will be developed in depth and related to one another.

Based on this study methodology, it is evident that in recent years the growth and importance of SDN networks as a research topic has increased. Therefore, aspects such as architecture and security [10] are issues that have evolved through various studies, which allows offering a better service with respect to traditional networks and their current disadvantages [11]. Consequently, subtopics will be developed that will contain the following: in *SDN Architecture*: data layer, control layer and application layer; in *security*, the work of the SDN control layer, its different advances through the Open Flow protocol and its projection [12] will be highlighted; in *articulated applications by SDN*, the different advances that technologies such as IoT, data centers and 5G have developed through SDN networks and their emphasis on the security part, will be mentioned [13].

The search for study material is made up of various research sources such as Scopus, IEEE and ScienceDirect databases. Basing this search on keywords such as: SDN Networks, SDN Network Architecture, Security in SDN Networks and Applications with SDN Networks. As a study sample and analysis of research material, the search for material was geographically limited to the European, Asian and American continents. In addition, this is valid as a valid temporary source of information, for articles and study material valid no less than 2015 for a valid and reliable source of information for SDN networks and their continuous development since the last decade.

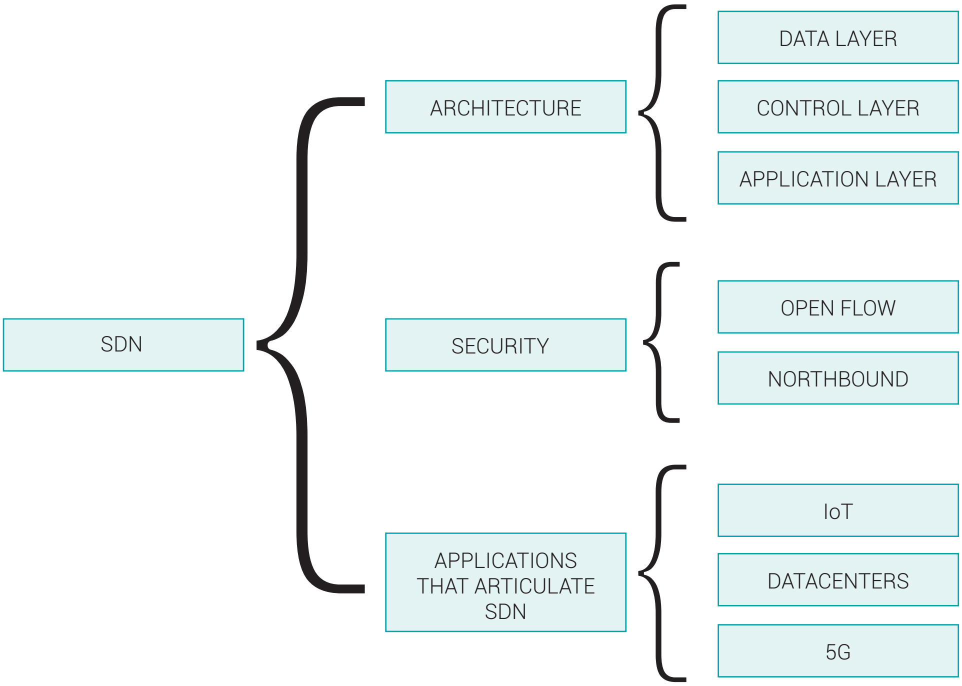

Figure 1. Research model for the state of the art developed.
Source: self made.

In 2019, Pillutla Harikrishna from India, presented an investigation that showed that the incorporation of SDN networks would help in the mitigation of DDoS attacks, allowing to investigate the flow of data traffic through the reactive process of updating the forwarding rules in the control layer; analyzing the network with a global vision and centralized control in monitoring for a better application of DDoS mitigation. This author proposed a recursively improved self-organizing map and a software-defined network-based mitigation scheme (CRESOM-SDNMS) to ensure the best detection rate during the cloud DDoS attack prevention process [14].

On one hand, Ihsan H Abdulqadder together with his research colleagues from China, in 2019, declared that the security problems faced by SDN, NFV, cloud computing and 5G, focused on the Intrusion Detection and Prevention Systems (IDPS). These researchers exposed, in turn, that the existing IDPS solutions were inadequate, which could cause a great waste of resources and various security threats. To alleviate security concerns or the early detection of an attacker, they proposed an innovative approach known as Multi-Layer Intrusion Detection and Prevention (ML-IDP) in an SDN / NFV enabled 5G network cloud. The proposed approach defends against security attacks using artificial intelligence (AI) [15].

On the other hand, Marcos V.O Assis along with his colleagues from Brazil also in 2019, presented a research related to IoT and SDN networks, exposing the security flaws that still exist. They proposed a near real-time SDN security system, which prevents DDoS attacks on the source network and protects the source SDN controller against deterioration of traffic. For this, a Convolutional Neural Network (CNN) is applied and tested for DDoS detection, describing how the system could mitigate the detected attacks. The performance results were performed in two test scenarios, indicating that the proposed SDN security system holds promise against next-generation DDoS attacks [16].

Alejandro Molina Zarca together with his colleagues from Spain in the present year, 2020; propose a contactless, policy-based security orchestration framework for an autonomous and conflict-free security orchestration in IoT scenarios with SDN / NFV; while ensuring the optimal allocation and chaining of VSF service functions (SFCs). The framework is based on semantic technologies, and considers security policies and the evolving IoT system model to dynamically and formally detect any semantic conflict during orchestration [17].

Fahad N. Nife from Poland and Zbigniew Kotulski from Iraq in 2020 propose an application firewall mechanism for SDN, which can be implemented as an extension of the network controller. To provide greater control and visibility into applications running on the network, the system can detect network applications that may affect network performance at some point, while being able to dynamically impose restriction rules on applications. The firewall architecture is designed as four cooperating modules: the Main Module, the Filtering Module, the Application Identification Module and the Security Compliance Module. The proposed mechanism verifies network traffic at the network, transport, and application levels, and installs appropriate security instructions on the network [18].

Amritpal Singh from India with his colleagues in 2020 propose a dynamic scheme called BloomStore, which manages the space by means of secure rules applying a bloom filter in SDN, with this data traffic is handled dynamically to the administrator network resources. A double security check is used for the secure data transfer by means of double hashing, that is, two independent hash functions are used to generate k hash functions. Furthermore, it is proposed that the participating hashing has insertion and query in a flowering set cube [19].

Nagarathna Ravi together with her colleague from India in 2020 propose an SDN based security scheme to mitigate DDoS on IoT servers, establishing a mechanism called learning based detection mitigation (LEDEM) that detects DDoS using a learning algorithm automatic semi-supervised and mitigates DDoS. They tested

LEDEM on the test bench and the emulated topology, and compared the results with leading-edge solutions. An improved accuracy rate of 96.28% was achieved in detecting DDoS attacks [20].

Pragati Shrivastava and her colleague from India in 2020 propose the implementation of EvilScout that seeks to prevent spoofing of a WiFi access point (AP) on a real SDN WiFi testbed with an Evil twin. They verify successful detection of the Evil Twin with high precision and low processing cost on the WiFi SDN. Carrying out a rigorous analysis of the Evil Twin in different WiFi configurations, it is possible to discover for the first time a new attack of "AP service blocking" by the Evil Twin adversary in the protected WiFi WPA2. The information that is available in the SDN driver enables simplified and more accurate detection of Evil Twins [21].

In the year 2019, Zhiyuan Li along with his colleagues from China, demonstrated through their work, that normal and abnormal traffic flows through the OpenFlow communication channel have different statistical properties. Specifically, normal OpenFlow traffic, which has a low degree of self-similarity, while the occurrence of saturation attacks generally implies a higher degree of self-similarity. Therefore, SA-Detector exploits the statistical results and degrees of self-similarity of OpenFlow traffic, measured by exponents of Hurst, for the detection of anomalies. They evaluate their focus on both physical and simulation SDN environments with various time slots, network and application topologies, Internet protocols, and traffic generation tools. For the SDN physical environment, the average detection accuracy is 97.68% and the average accuracy is 94.67%. For the simulation environment, the average precision is 96.54% and the average precision is 92.06%. Additionally, SA-Detector was compared to existing saturation attack detection methods in terms of the performance metrics mentioned above and the CPU utilization of the controller. The results of the experiment indicate that SA-Detector is effective for the detection of saturation attacks in SDN [22].

2. SDN Architecture

Since 2013, the concepts of SDN (Software-Defined Networks) and NFV (Network Functions Virtualization) were introduced, which sought to simplify the network architecture and its operation, facilitating scaling, deployment of modifications, insertion of new services, shorten response times and centralize its administration [23], resulting in a more efficient network with a higher economic return. This as a response method to the continuous difficulties that OTTs (over the top media service), high data traffic, the Internet of Things and cloud services have had; those which are destroying traditional networks due to their continuous growth. and infrastructure demand, reflecting the poor architecture provided by traditional networks [24].

Software-Defined Networks (SDN) are made up of three layers: data plane, control plane, and application plane. These three layers allow the automation of the network and a better administration of the resources that are integrated within its architecture, centralizing its management, automating and guaranteeing its scalability [25]. Situation that does not appear in traditional networks that, due to its design, is neither scalable nor profitable. Through this architecture it is possible to disaggregate the control and data planes of network devices such as switches and routers [26]. The control plane has the functionality to make decisions regarding the traffic that interacts with any network device, the data plane carries the transport of data packages in the network [27] and the application plane is made up of business applications of the end user.

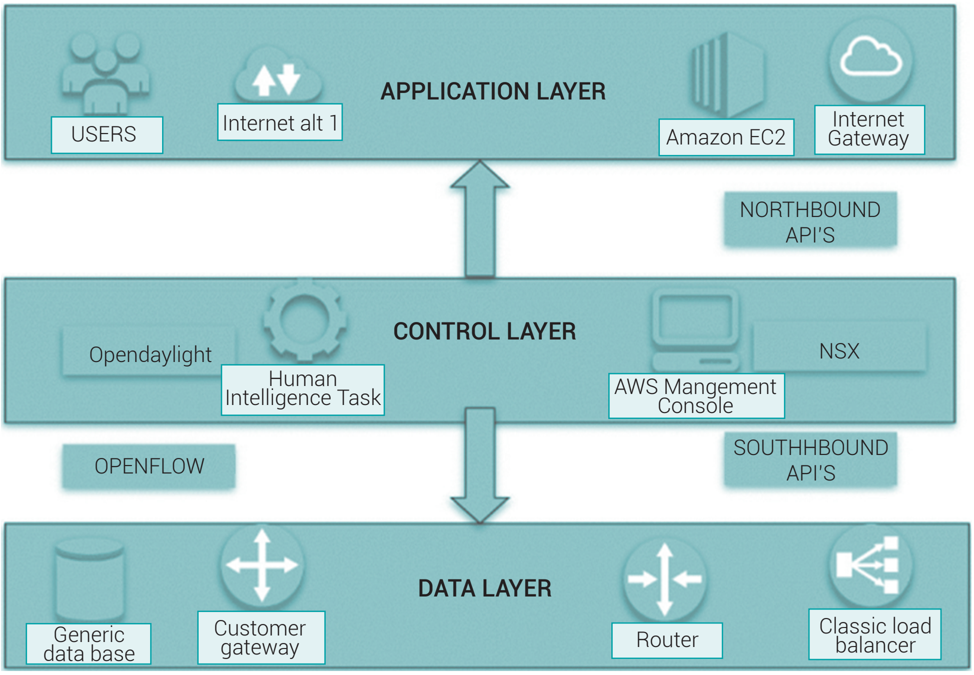

Figure 2. Elements of the Architecture of SDN networks.
Source: Self made.

2.1 Data layer

Also known as the infrastructure layer, it is made up of nodes that are in charge of packet switching and routing, replacing network devices such as switches, routers and access points that were in charge of the information that travels over the network [28]. This layer can be reprogrammable by the control layer, which through a set of instructions and rules can configure the functionality of the data layer in router or firewall mode as required through the OpenFlow API.

2.2 Control layer

This ability has the function of centralizing all the information flow that circulates through the control layer, this thanks to the fact that it configures and manages the nodes, correctly directing the traffic flow, through policies that control the flow tables in the network, forwarding or data diversion, having a broad overview of the entire network [29]. These policies are established through the OpenFlow protocol, which allows controls such as Opendaylight or NSX to send the policies and configurations that are designated for the data plane, there are also APIs such as Restful or Northbound that discriminate global application policies and policies. internal to the network, allowsing the application board to communicate with the control capability [30].

2.3 Application layer

This layer contains all end-user business applications and communicates via API north (up) with controllability. It simplifies and automates configuration tasks, services and provides the user with differentiated income according to the profile they have and the service they are going to consume, obtaining statistics that reflect their behavior on the network, and then make decisions about this information [31]; guaranteeing its security and portability since it is functional in any operating system.

3. ARTICULATED APPLICATIONS WITH SDN

3.1 IoT (Internet of Things)

IoT has taken a great boom in its development thanks to the promising solutions it has offered in technological diversity, integrating SDN networks capable of efficiently intercommunicating from one node to another at a geographical level, and in turn centralizing everything to the same point of administration. This being a great temptation for the technology industry, which want to implement this novel solution, without forgetting the changes at the infrastructure level that the IoT needs to implement and the security breaches that pose a threat to its execution [32]. Due to this, IoT technology with SDN networks is still an immature domain that has not managed to establish itself as a reliable technological solution. This, in turn, has prevented investors from sponsoring this type of research, where the biggest challenge is to offer reliable security of SDN networks to the user. Different from the type of security that traditional networks offer today, since, when an attack is made on the main node, this can compromise the architecture of the entire SDN network [33], being affected with aspects such as:

Protection of limited resources and neglected resources: The majority of IoT nodes are geographically dispersed and neglected, this being a threat, to be victims of a physical attack from which they do not possess any possibility of being saved [34]. In addition to this, the fact of having a physical node at a long distance, incurs the physical architecture that implements might be of great quality and capacity so that it can be self-sustaining. A clear example is the energy regulation of the battery with which the node is powered and an interface that allows continuous monitoring of the node, which guarantees its correct operation. What it leaves as evidence, the little security that this type of nodes has during its activity time due to the resources that are required to support its activity.

Security status monitoring: IoT was designed with the notion of being a large interconnection system that houses a huge distributed system that in turn contains subsystems, where the node that is responsible for data collection and content aggregation is the node administrator who manages the resources of each node of the network [35]. The cloud would play a role of great importance in this design, since, being dispersed nodes, the authentication of the nodes for security updates and validations must be done by certifications that would be carried out by means of cryptography methods and the computers do not count with enough architecture to support that high processing due to the significant complexity that these methods require.

Availability of services: IoT projects seek to target smart cities, smart grids, healthcare, transportation and industry; where the availability of the service plays an extremely important role. A simple reboot cannot be seen as a solution to any eventuality. Therefore, when IoT solves its security problems, it will be conceived as a great technological solution that will promote a high impact on society [36].

3.2 5G SDN mobile technology

The Software-Defined Network (SDN) is determined by 5G mobile technology, as the future of all its infrastructure by the promising solutions it aims to offer. despite the fact that its progress has not been very noticeable so far, due to security problems that it has not managed to overcome in software-defined mobile networks (SDMN). Although the security challenges it faces are great, its infrastructure potential is strong enough to overcome all these obstacles, consolidating itself as a powerful and secure network [37]. Work has been done and progress has been made on a security controller that is related to the SDN network controller [38]. Security services that could work correctly for end users of mobile networks [39].

Advances in the development of a demo workflow application are of high impact to solve the security problems presented by the SDN network in 5G technology [40]. Since it can offer parameterized service chains according to the need of the application, taking into account relevant aspects such as: network load, user demand and operator needs [41]. These services are sent through a chain optimizer through a GUI [42], when the request is successful, a response is sent to the GUI with the solution, minimizing end-to-end latency times, controlling traffic by means of flow rules [43]. This application also guarantees the integrity of the services, making possible to modify the service chains without altering the others, thanks to the identifier or ID, which allows recognizing the chain of services to be updated, by generating a display of a service chain request. A subset of switches in the WAN SD domain (software-defined red WAN), triggering dynamic adaptive capacity, redirecting traffic through other available switches [44].

SDN seeks to centralize the administration of the network through a controller, allowing the generation of better security implementation benefits to the mobile network. Thanks to the attributes that SDN offers in security, such as: logically centralized intelligence, programmability and abstraction [45]. Improving the architecture that SDN offers, it seeks to implement a fourth layer, which would be in charge of network security, incorporating an agent on the wireless edge, to prevent attacks by this means; besides it allows greater scalability in the network. However, coupling to the fourth layer is not so easy, as a failure in this security layer could paralyze the entire network, leaving it exposed to attacks by the medium [46].

3.3 Data centers

Data centers came to solve the problems of technologies such as: cloud applications, virtual machine migration or backups [47]; as they process high data traffic on geographically distributed nodes and provide 24/7 service [48]. For this reason, aspects such as the architecture being implemented, costs, consumption and reliability; have great relevance in its execution [49]. DCs (Data Centers) need intelligent intra-DC and inter-DC traffic control techniques. Therefore, the control plane, which is in charge of managing policies and the data plane, must take great care with aspects such as: availability, maturity, operator preference and functional requirements; which in turn can be: intra-DC traffic that must be flexible to control, adaptive to forwarded entries and dynamic context policies [50]. Studies have focused on control plane options that are tailored to data center requirements, such as a flexible Open Flow protocol for network and open interface control, a generalized multiprotocol label change (GMPLS) with optional Route Calculation (PCE) [51], as it offers maturity, operator-grade, and multi-domain support to control optical networks, slow migrations, and economic return; through the heterogeneous control plane that integrates GMPLS, PCE and SDN. Automated coordination, configuration and management is provided, this blueprint allows network simplification and better integration with operating systems [52].

While the administration of the control plane is based on a central node that administers the services, resources and security policies [53]; the nodes must be segmented or divided into multiple subdomains to guarantee the scalability of the network [54]. In this regard, there are two interconnection models that are the border links and the border nodes. Where the border links represent the model of two network nodes, residing in different domains that are interconnected by a shared link [55], moreover no entity in the subdomain, must have visibility to the network topology, due to security policies. And the link of border nodes where more than one node that belongs to a different domain, are reported for interconnection fines [56].

An SDN controller as a centralized entity and with full visibility of the Open Flow and GMPLS subdomains, operates the entire network as a single domain (as shown in Figure. 3), in this model the centralized SDN controller locally separates the domains to allow provisioning through dedicated interfaces at given demarcation points, scheduling cross-connections through OpenFlow, requiring the establishment of segments to the GMPLS boundary nodes, via the provisioning interface, or sending the provisioning task to ASPCE [57].

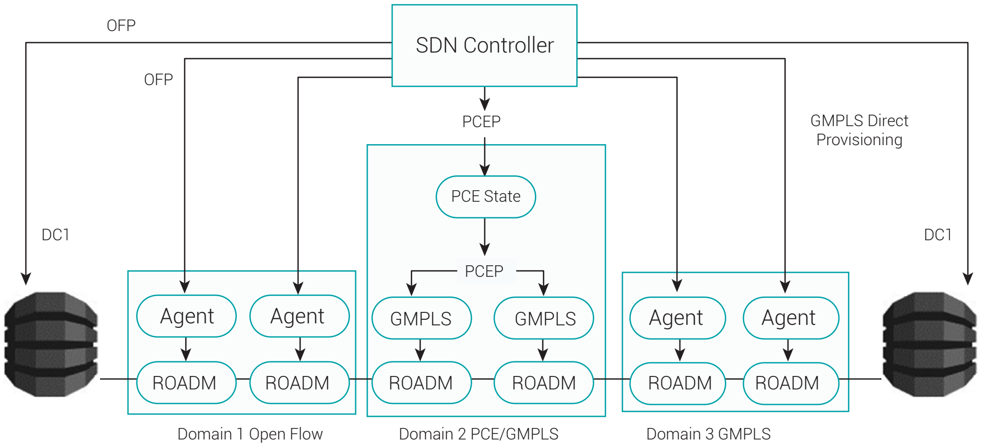

Figure 3. SDN controller model for heterogeneous domains OpenFlow / GMPLS with OpenFlow protocol, PCEP and GMPLS provisioning.
Source: self made.

4. SECURITY

Response mechanisms from the threats that compromise the functionality of the SDN network such as: brute force attacks, Phishing, DDos, Advanced Persistent Threat (APT) or Ransomware; they are ineffective [58], since many times the user performs a simple restart to return the system to a safe state [59]. These types of solutions in a Data Center, a medical center or an industry are deficient, due to their critical functionality, since the availability of the service must be guaranteed at all times and in each subsystem that integrates the SDN network [60], because the administration is centralized in a main node that when attacked would leave the entire system in a critical state [61]. Therefore, the control plane that is in charge of assigning the security policies that will be implemented in the network, must consider the response actions to the threats to which the system is exposed [62].

Security mechanisms have been developed to mitigate the threats faced by the SDN network, handling recognition filters that analyze the content and validity of packets as the Gateway does, which is the first line of security that is presented in the net; being responsible for certifying the source of the packets traveling on the platform [63]. Being as important this work of the gateway, the control plane must somehow confirm the assertiveness of the Gateway. This type of validation on packet content is a fairly rigorous and sensitive task for network security, which is why it has been sought to implement the Blockchain technology that performs packet verification instantaneously and has been implemented by public and private organizations, due to its potential in technology that focuses on a structural model data distributed, tamper-proof of being replicated, which is shared with network subdomains [64]. The implemented data structure generates a security Hash that is created at the moment of detecting the packet and this Hash will contain the ID of the information that this packet contains. With this if any data of the packet information is modified, the original Hash can be compared with the one generated by the modification that is made and when comparing the Hash, it will be evidenced that the detected packet was altered regarding the original information of the packet [65].

The security hash is generated in the content of the block or in its header. It contains a subset of the general registry of records made by all interconnected subdomains that have access to the system and that have a reference to the hash of the previous blocks. By means of this method, a link between blocks is generated, which is connected in the form of a chain, as shown in Figure 4.

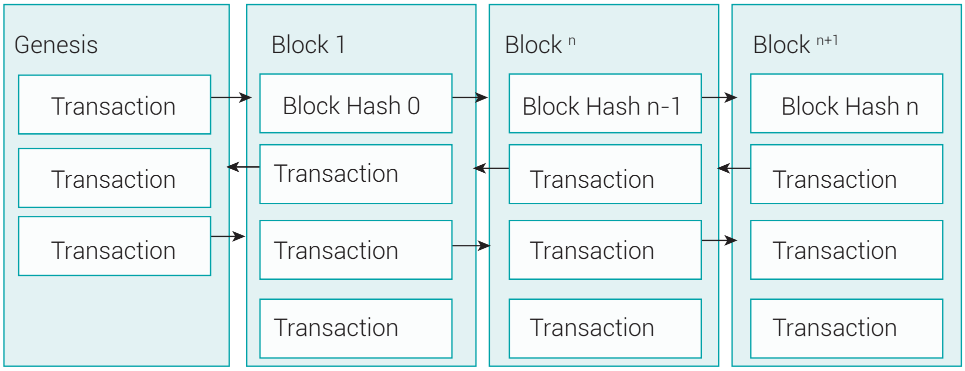

Figure 4. Blockchain.
Source: self made.

As it can be seen, the only block with a slightly different structure is the first one, which is known as Genesis and which is in charge of allowing distribution with all clients who have access to the Blockchain network. It can also be used as a key for encrypted content on the network [66]. Through this process, the network nodes are able to analyze the content stored in the data structure, allowing a real-time impression of the state of the network [67]. The data structure that Blockchain uses is distributed, which allows the nodes belonging to the network to communicate instantly. Nodes that have tracking authorization can validate the data stored in the packages that enter the system, regardless the volume of information. A fully reliable distributed and encrypted database is available as it is constantly updated due to its distributed structure [68].

Blockchains are completely reliable in terms of the integrity of their data, since the algorithms they implement are robust and do not allow them to be violated. In addition to this, Blockchains capture the modifications that are made to the packets, so the Security Hash would receive modifications and the threat would be detected immediately. The Genesis block, being the main node of the chain, is the strongest, so violating its security is quite complex [69]. These security features make Blockchain an effective method for the control plane in the SDN network [70].

4.1 OpenFlow

The most popular standard for SDN network administrators is OpenFlow, since it allows more effective control of routing tables remotely [71]. This OpenFlow protocol was found in 2007 by the academic and business sectors, with the help of the universities of Stanford and California. Currently the Open Networking Foundation (ONF) is in charge of defining the standard. OpenFlow records the packet flow using the Flow Chart that stores package data such as: source address, destination address, source port, destination port, DSCP, user ID, project ID, and number of protocol [72], [75].

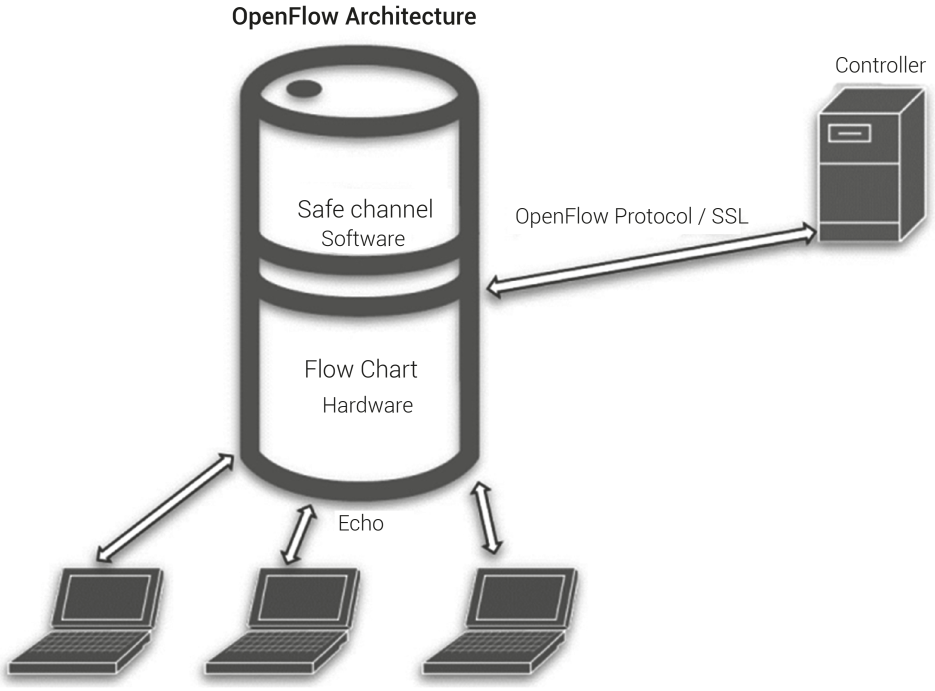

Figure 5. OpenFlow Architecture.
Source: Self made.

Backing up information for the organization has always been a topic of great importance. Through cloud orchestration, it addresses the composition of elements in the system, which support network activities, coordination and administration of services [73]. This in order to reduce the use of the network architecture, leaving the management of the system more profitable for the network administrator, which can be in charge of modifying the security of the control plane that is the main node of the network, and therefore, it would be the most considered point to attack due to threats from the organization. Considering that as this is the main point of administration and management of the network, it must have all the necessary levels of security and have plans of action against the risks that may be generated in the activity of the network.

5. DISCUSSION AND CONCLUSIONS

Security in SDN networks has taken a good course as security developments have increased in recent years. Advances can be seen from Multi-Layer Intrusion Detection and Prevention (ML-IDP) in an SDN / NFV enabled 5G network cloud to protect against security attacks using artificial intelligence; to security systems against DDoS attacks on the source network, protecting the SDN controller from sources against the deterioration of traffic through a Convolutional Neural Network.

The current advances in SDN security and the benefits offered by this architecture will be the force that will prevail in the technologies of the future.

In this article, a review of the most relevant categories of the SDN network model has been developed, as well as specific developments in security, allowing a frame of reference for future research in the security area, as this is the focus of study. For this, a description of the architecture and the network layers was made, contextualizing the reader in the functionality of its components and the importance of each of these.

The technologies that articulate SDN networks such as IoT, Data centers and 5G were documented detailing how SDN is incorporated into its applications and the challenges it has to face to be consolidated in each one of them. In addition, there was an emphasis on the security problem that SDN has had, since its centralized administration model implies a great risk if an attack is received on this node, implying the fall of the entire network and the denial of services. In the same way, developments have been implemented to correct this danger, through security policies that are responsible for preventing all kinds of attacks against the core of the network, through the OpenFlow protocol that allows managing the network as a whole, making easier for the network administrator, to manage hardware and software devices. The review was limited to the latest advances that have been developed in SDN networks, their significant progress and the result of the research that showed that the obstacles faced by this security architecture will no longer be an impediment to its development in the future, [74].

6. REFERENCES

[1] P. Shome, M. Yan, S. M. Najafabad, N. Mastronarde and A. Sprintson, “CrossFlow: A cross-layer architecture for SDR using SDN principles,” 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 37-39, doi: https://doi.org/10.1109/NFV-SDN.2015.7387403.

[2] M. Aslan and A. Matrawy, “On the Impact of Network State Collection on the Performance of SDN Applications,” in IEEE Communications Letters, vol. 20, no. 1, pp. 5-8, Jan. 2016, doi: https://doi.org/10.1109/LCOMM.2015.2496955.

[3] T. Nadeau and K. Gray, An Auhoritative Review of Network Programmability Technologies. California: O’Reilly, 2013.

[4] D. Maldonado, “Diseño e implementación de una aplicación bajo una Arquitectura SDN”, Tesis de maestría, Pontificia Universidad Javeriana, Bogotá, 2014.

[5] D. F. Garzón Triana, C. E. Montenegro Marín, y P. A. Gaona García, “Lenguaje de dominio específico para configuración de dispositivos de redes”, ing. Solidar, vol. 12, n.º 20, pp. 83-94, oct. 2016.

[6] F. Meneses, D. Corujo, A. Neto and R. L. Aguiar, “SDN-based End-to-End Flow Control in Mobile Slice Environments,” 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1-5, doi: https://doi.org/10.1109/NFV-SDN.2018.8725764.

[7] Blenk, A. Basta, J. Zerwas and W. Kellerer, “Pairing SDN with network virtualization: The network hypervisor placement problem,” 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 198-204, doi: https://doi.org/10.1109/NFV-SDN.2015.7387427.

[8] R. Hernández Sampieri, C. Fernández Collado, and M. D. P. Baptista Lucio, Metodología de la investigación. 5nd. Ed. Bogotá: MC GRAW HILL. 2014. pp. 92-100.

[9] H. Rivera Linares, F. Silva Cubillos, J. Hernández Gutierrez, y D. Mosquera Palacios, “Gestión gráfica de dispositivos activos de red multivendedor”, ing. Solidar, vol. 14, n.º 24, pp. 1-11, Jan. 2018.

[10] B. Valencia Suárez, S. Santacruz Pareja, L. Becerra Sánchez, y J. Padilla Aguilar, “Mininet: una herramienta versátil para emulación y prototipado de Redes Definidas por Software”, eci, vol. 9, n.º 17, pp. 62 - 70, Jul. 2019.

[11] M. I. Hamed, B. M. ElHalawany, M. M. Fouda and A. S. T. Eldien, “A novel approach for resource utilization and management in SDN,” 2017 13th International Computer Engineering Conference (ICENCO), Cairo, 2017, pp. 337-342, doi: https://doi.org/10.1109/ICENCO.2017.8289810.

[12] B. Pandya, S. Parmar, Z. Saquib and A. Saxena, “Framework for securing SDN southbound communication,” 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2017, pp. 1-5, doi: https://doi.org/10.1109/ICIIECS.2017.8275912.

[13] Jalili, H. Nazari, S. Namvarasl and M. Keshtgari, “A comprehensive analysis on control plane deployment in SDN: In-band versus out-of-band solutions,” 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2017, pp. 1025-1031, doi: https://doi.org/10.1109/KBEI.2017.8324949.

[14] Harikrishna, P., Amuthan, A. SDN-based DDoS Attack Mitigation Scheme using Convolution Recursively Enhanced Self Organizing Maps. Sādhanā 45, 104 (2020). https://doi-org.bdigital.udistrital.edu.co/10.1007/s12046-020-01353-x.

[15] Ihsan H Abdulqadder, Shijie Zhou, Deqing Zou, Israa T. Aziz, Syed Muhammad Abrar Akber, Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms, Computer Networks, Volume 179, 2020, 107364, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2020.107364.

[16] Marcos V.O. de Assis, Luiz F. Carvalho, Joel J.P.C. Rodrigues, Jaime Lloret, Mario L. Proença Jr, Near real-time security system applied to SDN environments in IoT networks using convolutional neural network, Computers & Electrical Engineering, Volume 86, 2020, 106738, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2020.106738.

[17] Molina Zarca, A.; Bagaa, M.; Bernal Bernabe, J.; Taleb, T.; Skarmeta, A.F. Semantic-Aware Security Orchestration in SDN/NFV-Enabled IoT Systems. Sensors 2020, 20, 3622.

[18] Nife, F.N., Kotulski, Z. Application-Aware Firewall Mechanism for Software Defined Networks. J Netw Syst Manage 28, 605–626 (2020). https://doi-org.bdigital.udistrital.edu.co/10.1007/s10922-020-09518-z.

[19] A. Singh, S. Batra, G. S. Aujla, N. Kumar and L. T. Yang, "BloomStore: Dynamic Bloom-Filter-based Secure Rule-Space Management Scheme in SDN," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6252-6262, Oct. 2020, doi: https://doi.org/10.1109/TII.2020.2966708.

[20] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3559-3570, April 2020, doi: https://doi.org/10.1109/JIOT.2020.2973176.

[21] P. Shrivastava, M. S. Jamal and K. Kataoka, "EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 89-102, March 2020, doi: https://doi.org/10.1109/TNSM.2020.2972774.

[22] Z. Li, W. Xing, S. Khamaiseh and D. Xu, "Detecting Saturation Attacks Based on Self-Similarity of OpenFlow Traffic," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 607-621, March 2020, doi: https://doi.org/10.1109/TNSM.2019.2959268.

[23] L. Richarson and S. Ruby, RESTful Web Services. California: O'Reilly, 2008, pp. 94-102.

[24] K. Pentikousis, Y. Wang and W. Hu, "Mobileflow: Toward software-defined mobile networks," in IEEE Communications Magazine, vol. 51, no. 7, pp. 44-53, Jul 2013, doi: https://doi.org/10.1109/MCOM.2013.6553677.

[25] J. Tourrilhes, P. Sharma, S. Banerjee and J. Pettit, "SDN and OpenFlow Evolution: A Standards Perspective," in Computer, vol. 47, no. 11, pp. 22-29, Nov. 2014, doi: https://doi.org/10.1109/MC.2014.326.

[26] W. Zhou, L. Li and W. Chou, "SDN Northbound REST API with Efficient Caches," 2014 IEEE International Conference on Web Services, Anchorage, AK, 2014, pp. 257-264, doi: https://doi.org/10.1109/ICWS.2014.46.

[27] W. Zhou, L. Li, M. Luo and W. Chou, "REST API Design Patterns for SDN Northbound API," 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, 2014, pp. 358-365, doi: https://doi.org/10.1109/WAINA.2014.153.

[28] Z. Yang and K. L. Yeung, “SDN Candidate Selection in Hybrid IP/SDN Networks for Single Link Failure Protection,” in IEEE/ACM Transactions on Networking, vol. 28, no. 1, pp. 312-321, Feb. 2020, doi: https://doi.org/10.1109/TNET.2019.2959588.

[29] P. Morreale and J. Anderson, Software Defined Networking, Univ. Politec. 1st Edition, Catalunya, CRC Press, 2014. pp. 1–67.

[30] B. Y. Yoon, S. Kim and J. Lee, “Transport SDN architecture for distributed cloud services,” 2014 12th International Conference on Optical Internet 2014 (COIN), Jeju, 2014, pp. 1-2, doi: https://doi.org/10.1109/COIN.2014.6950614.

[31] L. Cui, F. R. Yu and Q. Yan, “When big data meets software-defined networking: SDN for big data and big data for SDN,” in IEEE Network, vol. 30, no. 1, pp. 58-65, January-February 2016, doi: https://doi.org/10.1109/MNET.2016.7389832.

[32] H. Jang and J. Lin, “SDN based QoS aware bandwidth management framework of ISP for smart homes,” 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, 2017, pp. 1-6, doi: https://doi.org/10.1109/UIC-ATC.2017.8397480.

[33] Mckeown, H. Rashvand, T. Wilcox and P. Thomas, “Priority SDN Controlled Integrated Wireless and Powerline Wired for Smart-Home Internet of Things,” 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, 2015, pp. 1825-1830, doi: https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.331.

[34] T. Theodorou and L. Mamatas, “CORAL-SDN: A software-defined networking solution for the Internet of Things,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, 2017, pp. 1-2, doi: https://doi.org/10.1109/NFV-SDN.2017.8169870.

[35] P. Bosshart, D. Daly, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker, “Programming Protocol- Independent Packet Processors”, ACM SIGCOMM Computer Communication Review, Vol. 44, No.3, July 2014, pp. 88–95, doi: https://doi.org/10.1145/2656877.2656890.

[36] L. Sidki, Y. Ben-Shimol and A. Sadovski, “Fault tolerant mechanisms for SDN controllers,” 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, 2016, pp. 173-178, doi: https://doi.org/10.1109/NFV-SDN.2016.7919494.

[37] R. Bifulco and R. Canonico, "Analysis of the handover procedure in Follow-Me Cloud," 2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET), Paris, 2012, pp. 185-187, doi: https://doi.org/10.1109/CloudNet.2012.6483683.

[38] M. B. Al-Somaidai, "Survey of Software Components to Emulate OpenFlow Protocol as an SDN Implementation", American Journal of Software Engineering and Applications, vol. 3, no. 6, December 2014, pp. 74, doi: https://doi.org/10.11648/j.ajsea.20140306.12.

[39] S. Ali and M. Ghazal, "Real-time Heart Attack Mobile Detection Service (RHAMDS): An IoT use case for Software Defined Networks," 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, 2017, pp. 1-6, doi: https://doi.org/10.1109/CCECE.2017.7946780.

[40] P. Demestichas et al., "5G on the Horizon: Key Challenges for the Radio-Access Network," in IEEE Vehicular Technology Magazine, vol. 8, no. 3, pp. 47-53, Sept. 2013, doi: https://doi.org/10.1109/MVT.2013.2269187.

[41] D. La Oliva et al., "Xhaul: toward an integrated fronthaul/backhaul architecture in 5G networks," in IEEE Wireless Communications, vol. 22, no. 5, pp. 32-40, October 2015, doi: https://doi.org/10.1109/MWC.2015.7306535.

[42] Sutton, "5G network architecture," The Journal, vol. 12, pp. 8–15, 2018.

[43] X. Costa-Perez et al., "5G-Crosshaul: An SDN/NFV Integrated Fronthaul/Backhaul Transport Network Architecture," in IEEE Wireless Communications, vol. 24, no. 1, pp. 38-45, February 2017, doi: https://doi.org/10.1109/MWC.2017.1600181WC.

[44] R. S. Kalan, M. Sayit and A. C. Begen, "Implementation of SAND Architecture Using SDN," 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1-6, doi: https://doi.org/10.1109/NFV-SDN.2018.8725632.

[45] G. Bianchi, E. Biton, N. Blefari-Melazzi, I. Borges, L. Chiaraviglio, P. de la Cruz Ramos, P. Eardley, F. Fontes, M. J. McGrath, L. Natarianni, D. Niculescu, C. Parada, M. Popovici, V. Riccobene, S. Salsano, B. Sayadi, J. Thomson, C. Tselios, and G. Tsolis, "Superfluidity: a flexible functional architecture for 5G networks", Emerg. Telecommun, vol. 27, pp. 1178–1186, 2016, doi: https://doi.org/10.1002/ett.3082.

[46] D. Gedia and L. Perigo, "Performance Evaluation of SDN-VNF in Virtual Machine and Container," 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1-7, doi: https://doi.org/10.1109/NFV-SDN.2018.8725805.

[47] J. Teixeira, G. Antichi, D. Adami, A. Del Chiaro, S. Giordano and A. Santos, “Datacenter in a Box: Test Your SDN Cloud-Datacenter Controller at Home,” 2013 Second European Workshop on Software Defined Networks, Berlin, 2013, pp. 99-104, doi: https://doi.org/10.1109/EWSDN.2013.23.

[48] Asensio, L. Gifre, M. Ruiz and L. Velasco, “Carrier SDN for flexgrid-based inter-datacenter connectivity,” 2014 16th International Conference on Transparent Optical Networks (ICTON), Graz, 2014, pp. 1-4, doi: https://doi.org/10.1109/ICTON.2014.6876337.

[49] P. Varga et al., “Real-time security services for SDN-based datacenters,” 2017 13th International Conference on Network and Service Management (CNSM), Tokyo, 2017, pp. 1-9, doi: https://doi.org/10.23919/CNSM.2017.8256030.

[50] W. Hong, K. Wang and Y. Hsu, “Application-Aware Resource Allocation for SDN-based Cloud Datacenters,” 2013 International Conference on Cloud Computing and Big Data, Fuzhou, 2013, pp. 106-110, doi: https://doi.org/10.1109/CLOUDCOM-ASIA.2013.44.

[51] P. Samadi, D. Calhoun, H. Wang and K. Bergman, “Accelerating cast traffic delivery in data centers leveraging physical layer optics and SDN,” 2014 International Conference on Optical Network Design and Modeling, Stockholm, 2014, pp. 73-77.

[52] Y. Han, S. Seo, J. Li, J. Hyun, J. Yoo and J. W. Hong, “Software defined networking-based traffic engineering for data center networks,” The 16th Asia-Pacific Network Operations and Management Symposium, Hsinchu, 2014, pp. 1-6, doi: https://doi.org/10.1109/APNOMS.2014.6996601.

[53] Elgendi, K. S. Munasinghe and A. Jamalipour, “A three-tier SDN architecture for DenseNets,” 2015 9th International Conference on Signal Processing and Communication Systems (ICSPCS), Cairns, QLD, 2015, pp. 1-7, doi: https://doi.org/10.1109/ICSPCS.2015.7391793.

[54] Monga, E. Pouyoul and C. Guok, “Software-Defined Networking for Big-Data Science - Architectural Models from Campus to the WAN,” 2012 SC Companion: High Performance Computing, Networking Storage and Analysis, Salt Lake City, UT, 2012, pp. 1629-1635, doi: https://doi.org/10.1109/SC.Companion.2012.341.

[55] M. Osman, J. Núñez-Martínez and J. Mangues-Bafalluy, “Hybrid SDN: Evaluation of the impact of an unreliable control channel,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, 2017, pp. 242-246, doi: https://doi.org/10.1109/NFV-SDN.2017.8169866.

[56] P. Qin, B. Dai, B. Huang and G. Xu, “Bandwidth-Aware Scheduling With SDN in Hadoop: A New Trend for Big Data,” in IEEE Systems Journal, vol. 11, no. 4, pp. 2337-2344, Dec. 2017, doi: https://doi.org/10.1109/JSYST.2015.2496368.

[57] U. Khan and B. K. Ratha, “Time series prediction QoS routing in software defined vehicular ad-hoc network,” 2015 International Conference on Man and Machine Interfacing (MAMI), Bhubaneswar, 2015, pp. 1-6, doi: https://doi.org/10.1109/MAMI.2015.7456576.

[58] P. Jayashree and F. Infant Princy, “Leveraging SDN to conserve energy in WSN-An analysis,” 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, 2015, pp. 1-6, doi: https://doi.org/10.1109/ICSCN.2015.7219904.

[59] S. Jain, M. Zhu, J. Zolla, U. Hölzle, S. Stuart, A. Vahdat, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer and J. Zhou, “B4: Experience with a Globally-Deployed Software Defined WAN”, ACM SIGCOMM Computer Communication Review, Vol.43, No.4, August 2013, pp. 3, doi: https://doi.org/10.1145/2534169.2486019.

[60] S. Lazar and C. Stefan, “Future Vehicular networks: What control technologies?,” 2016 International Conference on Communications (COMM), Bucharest, 2016, pp. 337-340, doi: https://doi.org/10.1109/ICComm.2016.7528203.

[61] E. K. Ali, M. Manel and Y. Habib, “An Efficient MPLS-Based Source Routing Scheme in Software-Defined Wide Area Networks (SD-WAN),” 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, 2017, pp. 1205-1211, doi: https://doi.org/10.1109/AICCSA.2017.165.

[62] E. Rojas, “From Software-Defined to Human-Defined Networking: Challenges and Opportunities,” in IEEE Network, vol. 32, no. 1, pp. 179-185, Jan.-Feb. 2018, doi: https://doi.org/10.1109/MNET.2017.1700070.

[63] T. Ninikrishna et al., “Software defined IoT: Issues and challenges,” 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 723-726, doi: https://doi.org/10.1109/ICCMC.2017.8282560.

[64] M. Ketel, “Enhancing BYOD Security Through SDN,” SoutheastCon 2018, St. Petersburg, FL, 2018, pp. 1-2, doi: https://doi.org/10.1109/SECON.2018.8479230.

[65] P. Amaral, P. F. Pinto, L. Bernardo and A. Mazandarani, “Application Aware SDN Architecture using Semi-supervised Traffic Classification,” 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1-6, doi: https://doi.org/10.1109/NFV-SDN.2018.8725753.

[66] Hung-Chin Jang, Chi-Wei Huang and Fu-Ku Yeh, “Design a bandwidth allocation framework for SDN based smart home,” 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-6, doi: https://doi.org/10.1109/IEMCON.2016.7746320.

[67] H S. Van Rossem et al., “Deploying elastic routing capability in an SDN/NFV-enabled environment,” 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 22-24, doi: https://doi.org/10.1109/NFV-SDN.2015.7387398.

[68] D. Tatang, F. Quinkert, J. Frank, C. Röpke and T. Holz, “SDN-Guard: Protecting SDN controllers against SDN rootkits,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, 2017, pp. 297-302, doi: https://doi.org/10.1109/NFV-SDN.2017.8169856.

[69] Aydeger, K. Akkaya and A. S. Uluagac, “SDN-based resilience for smart grid communications,” 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 31-33, doi: https://doi.org/10.1109/NFV-SDN.2015.7387401.

[70] C. J. Casey, M. Yan, C. Chojnacki and A. Sprintson, “Flowsim: Interactive SDN switch visualization,” 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 34-36, doi: https://doi.org/10.1109/NFV-SDN.2015.7387402.

[71] J. Medved, R. Varga, A. Tkacik and K. Gray, “OpenDaylight: Towards a Model-Driven SDN Controller architecture,” Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, 2014, pp. 1-6, doi: https://doi.org/10.1109/WoWMoM.2014.6918985.

[72] M. Paliwal, D. Shrimankar and O. Tembhurne, “Controllers in SDN: A Review Report,” in IEEE Access, vol. 6, pp. 36256-36270, 2018, doi: https://doi.org/10.1109/ACCESS.2018.2846236.

[73] R. Mijumbi, J. Serrat, J. Gorricho, S. Latre, M. Charalambides and D. Lopez, “Management and orchestration challenges in network functions virtualization,” in IEEE Communications Magazine, vol. 54, no. 1, pp. 98-105, January 2016, doi: https://doi.org/10.1109/MCOM.2016.7378433.

[74] M. Ángel Barrera Pérez, N. Y. Serrato Losada, E. Rojas Sánchez, y G. Mancilla Gaona, “Estado del arte en redes definidas por software (SDN)”, Vis. Electron., vol. 13, n.º 1, pp. 178-194, ene. 2019. https://doi.org/10.14483/22484728.14424

[75] J. F. Herrera-Cubides, P. A. Gaona-García, C. E. Montenegro-Marín, S. Sánchez-Alonso, y D. Martin-Moncunill, "Abstraction of linked data's world", Visión electrónica, vol. 13, no. 1, pp. 57-74, feb. 2019. https://doi.org/10.14483/22484728.14397