Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

A Research Paper of Security Enforcement Policy for (SDN) (WLAN) Software Defined Network

Faridullah Amarkhil[1], Prashansa Taneja [2]
[1]Student,
[1] Computer Science Department,
[1]Alakh Prakash Goyal Shimla University, Shimla, India.

Abstract: **The considerable development in the numbers of Wi-Fi, activated devices, as well as the enhancement the network security, of wireless local area networks (WLAN), and SDN in new year's we have seen a rapid alteration, in the networking security industry leading by the SDN Software Defined Networking. the coming new generation of wireless network (WLAN), will be operating in an extremely condenses networks, and dynamics scenario. The lowness will be in the performance, caused by the disordered extension and due to the higher, level of interposition. SDN Software-Defined network architecture, will provide (WLAN), with a new experiment of performance. and ability, and security to deal with users necessitate, and services while providing, a big level of efficiency in a complexity scenario. I need a new Wi-Fi, network management, system which not only facilitates client, access operations but also provides a high-level authentication, procedure. In this paper, I introduce, a Security, Enhancement control system for Wi-Fi, devices, based on software-defined networking, in a wireless environment. In our work we demonstrate high security, of SDN (WLAN) software defined network wireless local area network for small, business environment of network. and also my work is to design and develop and demonstrate, efficient and unified network Handling, with better client's mobility, and security, for a SDN-WLAN infrastructure. and also I consider security, parameter for better management, of (SDN-WLAN). And network handling, of internal network security. And also Companies, to protect, their property and ensure the safety of its employees, they must attach great importance to the security, branch of the company build a computer system with a high level of security.**

Index Terms - SDN, WLAN, Wi-Fi, Security, Wi-Fi Protocol, Security, Blackmail.

I.INTRODUCTION

SDN Software-Defined, Networking, is a network architecture that empower the network to be intelligent, and centrally controlled or programmed using software applications. this should help to operate control the entire networks always and irrespective of the underlie network technology.

The software-defined networking (SDN) market is expected, to grow by Double-Number, among (2020), and (2023), driven by the increasing mainstream adoption, of this technology. And for good reason SDN gives IT the ability, to make changes through software code alternative of configuring of each device to control data traffic from a center console to move it in any direction. all department can now defeat tradition, network [2] agreeable, such as execution, impasse and improve a more responsive network strategy. On the security front, SDN allows an IT department to divide a network connection among an end users and the network data center. to provide various security, arrangement for the various types of network traffic, Having the capability, to more security policies for specify work. crowds are a key benefited of SDN when wireless communication problems happen, how end users and managers answer belong on different factors. Wireless networking is take more complex behind the perspective, Wireless communication trouble can be unbelievable frustrate, particularly when they occur at the wrong conceivable time, like when you want to send an email to meet a deadline and are working on the street with no access to tech support. Change off the wireless function's and straight communicate our computer to the routers, with an Ethernet, cables and wireless is also in a business services Wi-Fi, is a vitally segment of your IT infrastructures. unfit sketching, and wrong setup of your systems can make execution and security trouble. If any common wireless network matters happen, and you are leave off without suitable Wi-Fi development, you are and your worker are required, cutting off from the rest of the world. There are a number of the original, fundamentals that a person or companies needs to be informed of when provide a wireless network. Only a small number of work have particularly, looked to apply SDN to (WLAN) wireless local area networks The most prominent application to WLAN has been the SDN framework, named Odin, provides SDN-level programmability, to enterprise (WLAN) which typically support more flexibility, and richer services than normal WLANs As with other wireless networks enterprise .
needs to offer including, (SDN) implementation into wireless networks is one promising solution. We have seen how SDN has transformed campus networks data centers and the cloud to date so how can SDN help with Wi-Fi, or SDN. Wi-Fi is the best solution in delivering consistent high performance Wi-Fi to the growing number of Wi-Fi connected devices, Because of the SDN architecture, wireless networks are enabled to become more agile and scale based on the networks. Here four benefits for SDN-enabled Wi-Fi, Software Defined Networking is a paradigm that decouples the control plane from the data plane.

II.LITERATURE REVIEW

M. Gilani, (2017), SDN, introduces as future technology, paradigm to [1] enhance programmability, flexibility, scalability, interoperability and centralized control within the network. In that work, they examined the implications of SDN to enhance the mobility management in enterprise WLAN. they have proposed an efficient approach to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

incorporate the AP load security with position awareness into handover procedure. they build a simulation environment to analyze the performance of handover optimization model of SDN.
Surbhi, Sara, swat, Vishal, Agarwal, (2019) based upon the SDN challenges, [5] issues, and research directions, the study focuses on network design of SDN, its implementation, performance evaluation and _ally its variation. The network design emphasis- on the scalability of SDN, its fault-tolerance, ex- ability, and elasticity. On the other hand, network implementation focuses on integration with traditional net-work, resource management in SDN and its virtualization. The limited resources in SDN are the bandwidth between.

Deepak, Singh, (2019) survey of Software Defined Networking (SDN) Challenges State of the art research challenges: In state of the art research challenges are given the aim of the research is to describe the benefits of using SDN in a multitude of environments such as in data centers, networks, the comprehensive survey of SDN clearly edentates the several research possibilities in SDN, although several works had been done in the area of SDN but still a lot more things to be uncovered. The work done in this area is still in its initial stage. The future work in the SDN leads to increase acceptance and decrement in the cost of setting the network. switches and controller and the memory which must be efficiently utilized.
Kostal K, Bencel R, Ries, M, Kotuliak, (2018) according to SDN principles, they proposed the enhanced architecture [8] what resulted to merged control channels for SDN-WLAN wireless and wired part of the network to one control channel. He proposed the extension of Open Flow protocol for ensuring the wireless functionality and also changes in AP and SDN Controller Components for Network management.
M. Lee, Hwi Young, (2016) SDN controller based HA WLAN solution for WLANs. [3] Unlike previous research works where only theoretical concepts of SDN are discussed we developed a real-time ONOS controller based WLAN test environment. Furthermore, we also implemented and evaluated the performance of our proposed HA WLAN solution.

III.RESEARCH METHODOLOGY

For all organization, to protect its employees and good, the need is to make a strongly security system and also sensitize employees about how to use Information and Communication technology in good way. We cannot avoid technology, but we can prevent attacks by means of technology. And this way Software-defined networking SDN-WLAN aims is to make networks quick and secure The main goal of SDN-WLAN to improve network security and to improve network management and controlling. I also focus on the higher performance, for high-speed Monitoring of WLAN SDN. This consists first in identifying new key attributes brought by such technologies, for monitoring networks in particular from a security perspective. Security of SDN-WLAN networks Introducing a new protocol and interfaces as Open Flow does increases the exposition of devices, routers, switches, to attacks. SDN provides very high speed of data transfer. SDN provides better and Pretty good security and management of data. SDN provides controlling of wireless router and Wi-Fi, device, network control and management. SDN main goal is to provide high level of security of WLAN. this research paper is to provide a brief overview of SDN WLAN based Environments with a focus on their enabling technologies, application areas, structures and architectures. I have used the software tool Ns3 and network simulation and our basic work is to achieve the efficient security of SDN. So by using the above described software tools we have implemented the security algorithm. We have used the shortest coding to implement. we have used C++ language. (SDN) Software-defined Networking promises to improve the security and dexterity of networks, service providers to speedily respond to customer request for new services. These promises need to be put to the test. In addition, the problem posed by SDN networks on maintaining reliability, improved and security need to be analyzed and put to rest. One of the most common network setups Right now, router, interfaces with a focal system gadget like a center point switch or PC. The most common problem of SDN WLAN is security, problem because the traffic encryption, is also weak so attackers are able to recover transmissions from our network and also authentication, of wireless network user is not strong. For solution of this problem I consider deference security protocol to secure wireless network. and also for better security I must change the network SSID, name and I used strong encryption and then we encrypted the entire network. and for best security we consider 801.11i standard and also we can use 802.11x for authentication, and also the designing of star wireless topology. I consider C++ programing language by this language we write coding for star topology. and programing ns3 I used for connecting deference nodes. I considering one node as a central node. and we designed network for small business network and for private home network. SDN is focused on the internal network, be it the LAN or the kernel services provider networks. SDN is overall programmability, by the client, or user, and permit for effective conversion and configurational handling.

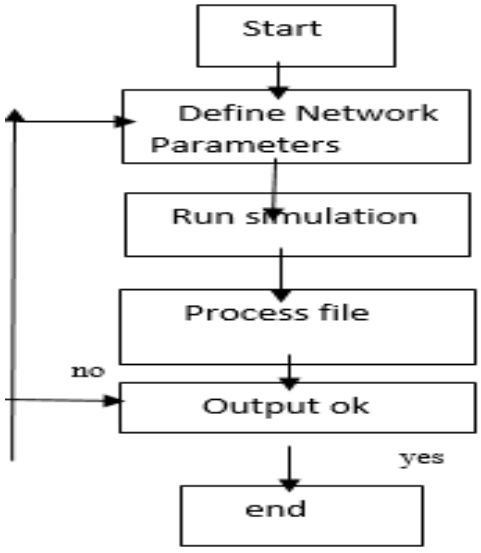

Figure 1 SDN Security process flowchart

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

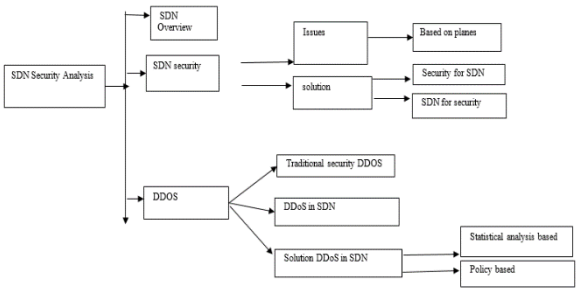

Figure 2 SDN Security survey block diagram

Upgrade Wireless Network Security Protocol:
In the event that you are utilizing a WLAN that depends just on these fundamental security highlights. it is urgent that they are accurately set up and working. Ideally, you should move up to increasingly present day security techniques, for example, Wi-Fi ensured get to (WPA) and WPA2.

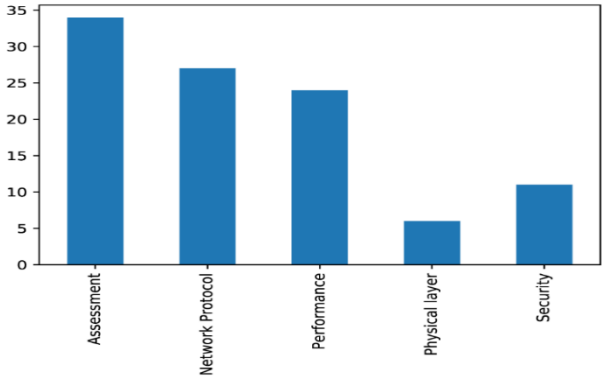

Figure 3 Analysis of security performance and data transfer

Wireless Network Security Issues and Blackmail:

- Configuration Problems
- Passive Capturing
- Rogue Access
- Denial of Service

Configuration Problems: Simple configuration, problems are mostly the cause of more vulnerability, this is because many consumer grade access points ship with no security configuration. a beginner user can set up one of these devices, rapidly and gain access everywhere, they also open up their network to external, use without other configuration.

Passive capturing: Passive capturing is accomplishing, by simply taking within domain of a targeted a wireless LAN and then listening and take information. This data can be used for a number of things including trying to break available, security settings and analyze, non-secured [4] traffics. It is approximately impossible to actually prevention this type of attacks because the nature of a wireless network what can be done is to implemented high level security standards using complexes' parameters wishful the data within this articles will be your begging point in securing, our wireless networks.

Rogue Access Points: One strategy, that is frequently utilized by assailants focusing on remote LAN is to arrangement a maverick passageway that is inside the scope of the current remote LAN. The thought is to fool some of the legal devices into the connection to the access point over the lawful access points. to real be effective, this type of attack requires some amount of physical access; this is required because if a user associates with a rogue access point then is can't to execute any of their normal duties the vulnerability, will be short lived and not that effective.

Denial of Service Attacks: where the intruder floods the network with messages affecting the availability, of the network resources Anybody familiar with network security is aware of the concept of denial of service (Do's) It is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This should be possible by essentially, sending a lot of traffic at a particular objective Obviously, the measure of traffic required to influence an objective gadget can be a lot higher than the abilities of a solitary machine However, [6] the flooding of traffic is not the only way to limit access to services; for wireless networks it can be much easier as the signal can be interfered with through a number of different techniques.

spoofing and session hijacking: where the attackers avail access to networks information and resources by assuming's the identification of a correct user.

eavesdropping: where unauthorized, third-parties intercept the data being transmitted over the secure network. and counters these threats we must create every attempt to configure our WLAN correctly. We must also enable a domain of security features such as standards authenticity, and encryption besides others access control mechanism.

WLAN Security Trait:

- Service Set Identifier (SSID), these prevention connections to access points but a device uses a given identifier rightly.
- Media Access Control (MAC) this including using address related to every device to limit communication to access points.
- Wired Equivalent Privacy (WEP), WEP uses encryption keys so that only devices with the correctly key can communicate with access points.
- WEP yet be in more devices as users have found compatibilist problems when introducing new equipment's. anyway, WEP has been prevention ineffective against hacker. [7] We must consider high level any devices based on this technology.

Even out with all these security measure combines, original WLAN features cannot guaranty that our network will stay secure. What is many WLAN equipped often comes with the security measures switches off totally. If we don't switch these on, then we have absolute no security at all.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Wireless Network Device Security Protection Tip:

- Make a complex router password
- modify the routers admin accredits
- alter the network name
- reinforce Wi-Fi encryption
- Turn off Plug 'n Play.
- Turn off Remote Management

Wireless Network Security for Star Topology:

a star network has a switch or passage in the center that associates with all the terminals or hubs. The benefit of star topology is that all the unpredictability, in the network is driven to a centric node and the other nodes only need to communication in their time or frequencies slot. And also A star network is a local area network (LAN) in where all nodes workstations or other devices are directly connected to a common central computer. Each PC is in straight connected to every other via the central device. In some star networks, the central computer can also operation as a computer. The image shows a star network with nine workstations or ten if the central computer acts as a workstation.

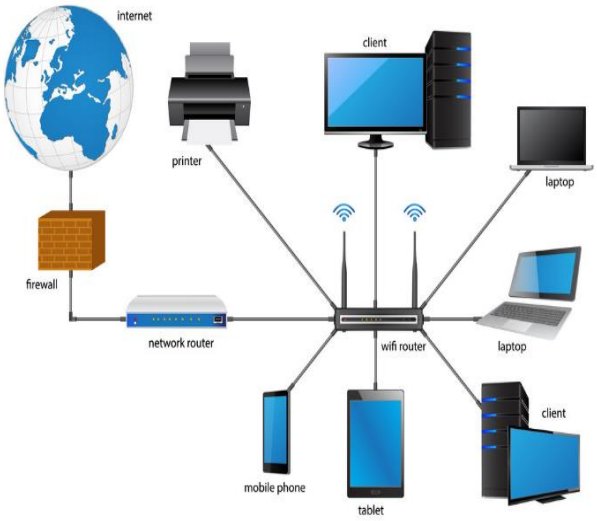

Figure 4 Architecture of star topology

Characteristics of Wireless Star Topology:

- ✓ High Speed
- ✓ Very Flexible
- ✓ High Reliability
- ✓ High Maintainability
- ✓ Has a high level of security

Table: 1

Hardware Requirements	Software requirement
Wireless, Routers	Tool: MATLAB 2016
Repeaters	Ns3 network, simulation
Antennae	Packet tracer
SDN ,APIS	Number of nodes
Access, Points	Connection to backbone LAN
4-Core 2.66 GHz CPU 32 GB of RAM 300 GB Disk Space 1 Gb/sor faster physical network adapter	Transmission, robustness and security.

RESULTS AND DISCUSSION:

implementations were implemented in NS-3 to support these new order to get accurate results and test them under different conditions. ns-3, an open source network simulator with features supporting 802.11i was used to perform the simulation. Results obtained indicate in my work. Programing NS3 is used for connecting and analysis of nine nodes. I considered one node as a central node. And I also analyzed a Security, Enhancement control system for Wi-Fi, devices, based on software-defined networking, in a wireless environment by ns3 software. We propose a smart SDN based solution for analysis of SDN-WLAN. The most common work of this scope is on security policy because the traffic encryption was so weak so attackers are able to recover our network transmissions and also authentication of wireless network user was not strong. For solution of this problem I consider deference security protocol to secure wireless network and also for better security I changed the network SSID name and I used strong encryption and then I encrypted the entire network and for best security I consider 801.11i standard and also I can use 802.11x for authentication. The 802.11x standards provide some basic security, but are becoming less adequate as use of wireless networking spreads. And for designing of star wireless topology I consider C++ programing language by this language I write coding for star topology. and programing ns3 I used for connecting deference nodes. I considered one node as a central node. and I designed for small business network and for private home network. I focused on the internal network, be it the LAN or the kernel services provider networks. SDN is overall programmability by the client or user, and permit for effective conversion and configurational handling.

Wireless star topology coding

```
#include "ns3/center-module.h"
#include "ns3/netanim-module.h"
#include "ns3/web-module.h"
#include "ns3/highlight point-module.h"
#include "ns3/applications-module.h"
#include "ns3/highlight point-format module.h"
//Network topology (default)
//
// n2 n3 n4.
// \ | / .
// \|/ .
// n1--- n0---n5.
```

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

```
// /|\ . \
// / | \ . \6
// n9 n8 n7.
utilizing namespace ns3;

NS_LOG_COMPONENT_DEFINE ("Star");

int

fundamental (int argc, singe *argv[])

/Set up some default esteems for the reproduction. //
Config::Set Default ("ns3::OnOffApplication::PacketSize",
UintegerValue (138));

??? try and stick 15kb/s into the data rate

Config::SetDefault ("ns3::OnOffApplication::DataRate",
StringValue ("14kb/s"));

// Default number of nodes in the star. Overridable by
command lineargument.

uint32_t ntalkes = 8;

CommandLine cmd;

cmd.AddValue ("ntalkes", "Number of nodes to place in
the star", ntalkes);

cmd.Parse (argc, argv);

 NS_LOG_INFO ("Build star topology.");

                  PointTo PointHelper pointToPoint;

           pointToPoint.SetDeviceAttribute ("DataRate",
StringValue ("5Mbps"));

              pointToPoint.SetChannelAttribute ("Delay",
StringValue ("2ms"));

              PointToPointStarHelper star (nSpokes,
pointToPoint);

               NS_LOG_INFO ("Install internet stack on all
nodes.");

                InternetStackHelper internet;

                star.InstallStack (internet);

                NS_LOG_INFO ("Assign IP Addresses.");

              star.AssignIpv4Addresses (Ipv4AddressHelper
("20.1.1.0",        "255.255.0.0"));

               NS_LOG_INFO ("Create applications.");

               Uint14_t port = 60000;

            Address hubLocalAddress (InetSocketAddress
(Ipv4Address::GetAny    (), port));

              PacketSinkHelper packetSinkHelper
("ns3::TcpSocketFactory",     hubLocalAddress);

   ApplicationContainer hubApp =
packetSinkHelper.Install (star.GetHub ());

   routerApp.Start (Seconds (1.0));

   routerApp.Stop (Seconds (10.0));

  Create OnOff applications to send TCP to the hub, one on
each spoke node.

    OnOffHelper onOffHelper ("ns3::TcpSocketFactory",
Address ());

    onOffHelper.SetAttribute ("OnTime", StringValue
("ns3::ConstantRandomVariable[Constant=1]"));

            onOffHelper.SetAttribute ("OffTime",
StringValue
("ns3::ConstantRandomVariable[Constant=0]"));

     ApplicationContainer spokeApps ;

      for (uint32_t i = 0; i < star.talkCount (); ++i)

     AddressValue remoteAddress (InetSocketAddress

      (star.GetHubIpv4Address (i), port));

       onOffHelper.SetAttribute ("Remote", remoteAddress);

 talkApps.Add   (onOffHelper.Install   (star.GetSpokeNode
(i)));

   talkApps.Start (Seconds (1.0));

   talkApps.Stop (Seconds (10.0));

     NS_LOG_INFO ("Enable static global routing.");

    // Turn on global static routing so we can actually be
routed    across the star.

    Ipv4GlobalRoutingHelper::PopulateRoutingTables ();

    NS_LOG_INFO ("Enable pcap tracing.");

  // Do pcap tracing on all point-to-point devices on all
nodes.

    pointToPoint.EnablePcapAll ("star");

    NS_LOG_INFO ("Run reproduction.");

    reproduction ::Run ();

    Reproduction ::Destroy ();

    NS_LOG_INFO ("Done.");

      return 0;

}
```

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

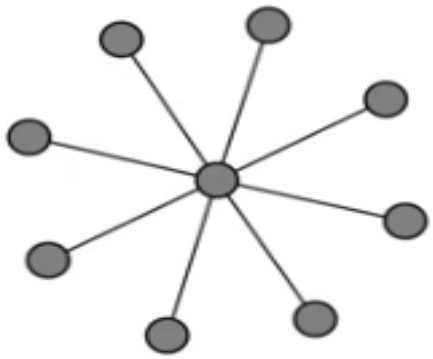

Figure 5 first step output of star topology by ns3

Figure 6 second step output of topology by ns3 result

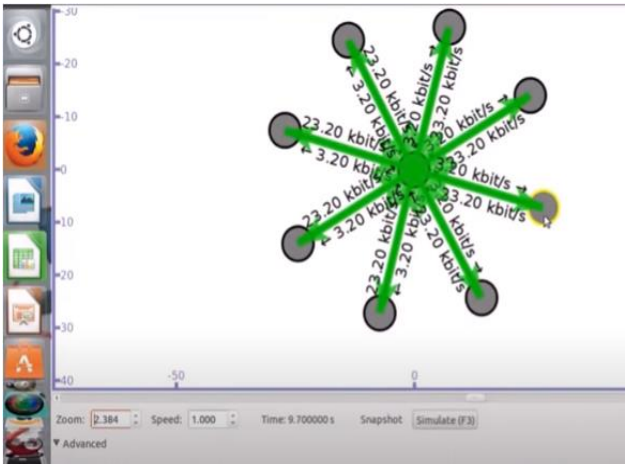

Figure 7 Third step output of topology by ns3 result

IV.CONCLUSION

We cannot live without Information and Communication technology, and current situation. In this Research paper our goal is network security, management, to improved client's mobility, and Security, for SDN-WLAN infrastructure. to integrates, enterprise, WLAN services. to unified Network management for better security. and for development the infrastructure of SDN WLAN. And also for business growth and for connect, and communicate wirelessly unlike a traditional, Wired LAN in which devices communicate, over Ethernet cable devices on a WLAN communicate Via Wi-Fi network. and SDN is focused, on the internal network be it the LAN or the core service Provider network, and we also focus the security of SDN to build into the designed as supply as a Help to ensures the availability, trueness and security of every single accompanied assets and data. and we consider star topology for current work and we designed network for small business network and for private home network. one of the most common network setups. In this configuration, every node connects to a central network device like a Router, or switch, computer Furthermore, our unified network management introduces easier performance for SDN- WLAN architecture, and security. The Future work of SDN-WLAN replaces traditional devices switches, enabling the investment customer to directly interact with different services. It allows the customer to purchase and implement new functions through a single portal, according to Pigg Clark. SDN is the Future of IT Networking. With the current mature virtualization of most infrastructure components such as servers and storage, the industry urges network virtualization to increase network seeped.

REFERENCES:

[1] Gilani, Syed Mushhad M., Tang Hong, Wenqiang Jin, Guofeng Zhao, H. Meng Heang, and Chuan Xu. "Mobility management in IEEE 802.11 WLAN using SDN/NFV technologies." EURASIP Journal on Wireless Communications and Networking (2017) no. 1 (2017): 1-14.

[2] Saraswat, Surbhi, Vishal Agarwal, Hari Prabhat Gupta, Rahul Mishra, Ashish Gupta, and Tanima Dutta. "Challenges and solutions in Software Defined Networking: 141 (2019) 23-58.

[3] Lei, T., Lu, Z., Wen, X., Zhao, X., & Wang, L. (2014, May). SWAN: An SDN based campus WLAN framework. In 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE) (pp. 1-5). IEEE.

[4] Zhao, D.; Zhu, M.; Xu, M. Supporting One Big AP illusion in enterprise WLAN an SDN-based solution. In Proceedings of the 2014 Sixth International Conference on Wireless Communications and Signal Processing (WCSP), Hefei, China, 23–25 October (2014)

[5] Saraswat, Surbhi, et al. "Challenges and solutions in Software Defined Networking: A survey." Journal of Network and Computer Applications. (2019) 23-58.

[6] Gilani, S.M.M., Hong, T., Jin, W., Zhao, G., Heang, H.M. and Xu, C., 2017. Mobility management in IEEE 802.11 WLAN using SDN/NFV on pp.1-14.

[7] Abbasi, Aaqif Afzaal, Almas Abbasi, Shahaboddin Shamshirband, Anthony Theodore Chronopoulos, Valerio Persico, and Antonio Pescapè. "Software-defined cloud computing: A systematic review on latest trends and developments." IEEE Access 7 (2019)

[8] Bencel, Rastislav, Kristián Košt'ál, Ivan Kotuliak, and Michal Ries. "Common SDN control channel for seamless handover in 802.11." In 2018 Wireless Days (WD), pp. 34-36. IEEE, (2018).