International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 376-386

A Survey on Implementing Security in Software Defined Network

Sivarajan. E
Department of CSE, Anna University, Chennai.

Dr. Jeyalakshmi. V
Department of ECE, Anna University, Chennai

Abstract

Wireless Networks were widely established for simple communications between the peoples. Now a day majorly used for the making electronic online fund transfers, online bill payments, e-transport booking like a ticket booking, online healthcare services and electronic mail. The entire world is moving towards e-business and need to focus the importance of reliability and security of the wireless dynamic networks. So strong security mechanisms are needed to end users to do the tasks in secure manner. A study has been carried out on this domain, and to identify the security algorithm different stages.

Keywords--SDN, SDSWN, Wireless Networks, Security and Issues.

I. INTRODUCTION

The wireless network was introduced in the 19th century. It is one of the most important mediums of transmission of information from one device to other devices in dynamically. In this technology, the information can be transmitted through the air without requiring any cable or wires or other electronic conductors, by using electromagnetic waves like IR, RF, satellite, etc.

In the present days, wireless network has become an essential part of wireless communication devices, that permits user to communicate even from remote operated areas. There are many devices used for wireless communication like Cordless telephones, Zigbee wireless technology, GPS, Wi-Fi, satellite television and mobiles include 3G and 4G networks, Bluetooth and Wi-Fi technologies.

Types of wireless networks include wireless PAN, wireless LAN, wireless MAN, wireless WAN, MANET, cell phone networks, wireless sensor networks, satellite communication networks and terrestrial microwave networks.

The applications of wireless network is involve security systems, television remote control, wireless power transfer, Banking transaction, e-business, e-transport booking, Android based smart phone used for induction motor control, Smart phone controlled traffic signal override with density sensing system, Arduino based home automation, Robotic vehicle movement by mobile, Remotely controlled android based Electronic Notice Board, Remote operated domestic appliances control by android application, Remote password operated security control by android applications, Inventory control, Healthcare services, Real estate management, Utility industry process and Vending services.

ISSN: 2233-7857 IJFGCN

The uses of wireless network, it is any data or information can be transmitted faster and with a high speed, maintenance and installation is less cost, it can be accessed from anywhere, it is very helpful for workers, doctors working in remote areas as they can be in touch with medical centers.

The demerits of Wireless Network, it can require extra costs and equipment to set up, although increasingly routers have built-in wireless capability, as do devices such as laptops, handheld devices, modern DVD players, and TVs., File-sharing transfer speeds are normally slower with wireless networks than they are with cabled. The speeds can also vary considerably according to location in relation to the network. The general speed of a wireless connection is also usually much slower than a wired one. The connection also gets worse from the router, which can be a problem in a large building or space. Wireless connections can be obstructed by everyday household items and structures such as walls, ceilings, and furniture. Wireless networks are generally less secure. There can also be problems with neighbors stealing bandwidth, if the network hasn't been set up to be password protected. Information is also less secure too and can be easier to hack into.

The networks have been growing a lot in size and in necessities moving around hardware switches has become a burden. And since today business is so fast paced need to alter these policies from time to time again, individually, usually and manually on each device. So the network become so rigid and need to add more and more policies, this is where SDN is defined in early 2010s. This Software Defined Network is an architecture to computer networking that allows network administrators to programmatically initialize, control, change and manage network behavior dynamically via open interfaces and abstraction of lower level functionality. This SDN algorithms are utilized the controller's global view of the network to take more informed decisions for efficient resource management with secure and analyzed the performance of the algorithms under realistic load, sharing with secure condition. SDN brings exactly that it physically divides data plane from control plane of the machine. SDN is trendy topic in computer networks, and it became as a solution to all network infrastructure problems. SDN puts all control planes on to a single plane. The controller till does the same job as that of an individual control plane. Only that it has to do on large number of devices rather than just one device. It creates forwarding table and pushes them on to the data planes. The network engineer's job has now become much easier to do. He only has to deal with controller now, not every device individually. The data plane refers to forwarding of the packet from one port to the other port with the help of the forwarding tables provided by control plane. Control plane deals all the functions and processes that determine which path to use protocols.

II. NEED FOR SECURITY IN WIRELESS NETWORKS

Wireless security is the way of ensuring security on a wireless networks. It is a replacement of network security that provides security to a wireless computer network. It is also called as wireless security. Wireless networks are quite easy to break into. As a result, it's very important that all wireless networks safeguard against unauthorized access to their networks. To provide efficient, automatic wireless risk security need to implement a complete secure manner of wireless network security solutions. These solutions should enable the evaluation of security threats and prevent the network from the attacks.

III. LITERATURE REVIEW

Software Defined Networking architecture and role of OpenFlow SDN broadly consists of three layers: i) Application Layer, ii) Control Layer iii) Infrastructure or Data Plane Layer.

ISSN: 2233-7857 IJFGCN

a. Security in Application Layer

Network congestion during disasters and big events is a major issue, especially in metropolitan areas. Although different network operators have their own strategies to address such types of incidents, a smarter and more efficient way to address such situations is needed for Smart Cities.

The Author propose SPArTaCuS, a framework to prioritize network traffic adaptively for such situations for smart cities using a software-defined network (SDN) approach, where services that require priority are placed in virtualized networks and the mechanism is accomplished through a priority management layer in SDN architecture [1].

b. Security in Control Layer

The different approach of network management is Software Defined Network (SDN) architecture. The incoming packets in the SDN network are waiting for incoming packets in the forwarding table to match instead of routed by the switches, if there is no such matching it will be forwarded to the controller for the further processing. In SDN the major security issue is Distributed Denial of Service (DDoS) attack .The application layer or network layer which are connected to this network are faced DDoS attack. The author has discussed the DDoS attacks occur due to the traffic flow. The author used different algorithms to categorize whether the traffic is average and a typical. Using exposure ratio and accuracy parameters the algorithms are measured. Then to apply signature IDS, the algorithm that shown better accuracy is taken and then results treated by Advanced IDS which notices atypical behavior and gives the host which attacked by DDoS as a result.

An energetic, convenient and flexible rising architecture of Software Defined Network is initiative for elevated bandwidth and active nature of today's applications. To allow engineers to immediate responding to rapid changes of business needs is the main objective of SDN. The author discussed safety measures to controller of Software Defined Network. Further, by using different algorithms how to detect the attacks of DDos by categorizing receiving requirements is discussed. Good outcome has shown by the accomplishment of IDS in SDN. The author has implemented the proposed mechanism using MiniEdit controller. The completeness of the solution is done by applying SDN on unrelated topologies [2].

The Management of wireless networks as well as wired networks by using software-defined networking (SDN) has been highlighted continually. However, control features of a wireless network differ from those of a wired network in several aspects.

The author Identify the various inefficient points when controlling and managing wireless networks by using SDN and propose SDN-based control architecture called Proxcon to resolve these problems. Proxcon introduces the concept of a proxy SDN controller (PSC) for the wireless network control, and the PSC entrusted with the role of a main controller performs control operations and provides the latest network state for a network administrator. To address the control inefficiency, proxcon supports offloaded SDN operations for controlling wireless networks by utilizing the PSC, such as local control by each PSC, hybrid control utilizing the PSC and the main controller, and locally cooperative control utilizing the PSCs. The proposed architecture and the newly supported control operations can enhance scalability and response time when the logically centralized control plane responds to the various wireless network events [3].

In Wireless Local Area Networks (WLAN) with more than one access point (AP), the handoff process plays a crucial role to guarantee the user service continuity. Usually initiated by the client's equipment, it

ISSN: 2233-7857 IJFGCN

occurs smoothly on the order of seconds. However, despite being functional and well-established, this process can be inadequate in scenarios where users are executing multimedia applications, such as real-time video streaming or VoIP. For these applications, those few seconds may cause loss of packets, resulting in loss of essential information.

The Author proposes a Software Defined Wireless Networking (SDWN) approach, in which a controller decides when to initiate the handoff process and chooses the AP the client's device must connect. This approach was implemented in a test bed scenario and the results have shown its efficiency by decreasing the handoff delay and providing more stability to the process [4].

Adaptive streaming over HTTP(DASH) is a popular method to deliver best possible quality media using available network resources. The Author propose QoS routing algorithm design for providing high quality and continuous stream of media streaming in SDN(Software Defined Network). To provide seamless DASH service over SDN is a challenge because traditional DASH service manner mismatches with SDN per-flow centralized management architecture. Therefore, it is necessary to have some interactions between communication layers for making routing decision.

Firstly, propose server driven bit rate estimation approach to computes video bit rate and inform the application QoS requirement to the control layer. The media server estimates the resources available and dynamically adapts the video bit rate in order to reduce additional software stacks on end-user devices and also present a Kalman Filter based rate adaptation mechanism that predicts the next bit rate of the media in a seamless manner.

Secondary, propose a QoS routing design for adaptive stream, it allows SDN controller evaluates all passable paths based on whole network topology by taking the bit rate of the segments in to account. And perform an experiment and presented the server driven bandwidth estimation mechanism to compute the appropriate bit rate and rate switching in smooth manner. And also construct a SDN test bed for QoS routing algorithm for adaptive streaming , it shows additional reroute step to find path that satisfy the bit rate before downgrade the video quality [5].

The Single controller implementation of SDN has many problems related to single points of failure, computational complexity growth, reliability and scalability. To solve these problems, multi-controller implementation of Software Defined Network has been introduced. Multiple controller implementation of the SDN control plane for large networks environment solves the scalability and reliability issues introduced by the centralized controller of the SDN. However, there are still open research topics related to controllers placement.

The Author discussed in placement of controllers and making solution to earlier problem like single point of failure and computational complexity growth. Distributed hierarchical control plane architecture of SDN using multiple controllers of large-scale networks is presented. Simulation result shows that hierarchical architecture solved many problems those were arising earlier in single controller architecture. Distributed hierarchical architecture does not have single point failure problems. Proposed architecture effectively reduces the computational complexity growth of SDN control plane from super linear to linear [6].

The Author discussed for the purpose of load balancing for SDN-based datacenters. Mininet emulator was utilized for the purpose of emulating the proposed system, the suggested algorithm was added to the

ISSN: 2233-7857 IJFGCN

POX controller. To evaluate our algorithm, simulated a datacenter with a Fat-Tree topology (k=4). The algorithm was proposed to dynamically balance the load by means of re-routing utilizing the information at the SDN controller. The network performance was tested in term of throughput, loss, and received data size with and without applying the proposed algorithm.

Results showed that the proposed algorithm outperforms the traditional load balancing scheme as follows; improves the throughput by a minimum of 21.9%, reduce the loss by 88.2%, increase the received data size by 20.8 %. In addition, the proposed algorithm acts as a congestion control algorithm and a new load balancing algorithm [7].

c. Security in Data Plane Layer

SDN is chancing as a new technique for running and scheming the function of networks starting from the middle, project, business and residence. This article addresses stimulating challenges and opportunities to increase security in those areas, by adding new ways to identify the threats and respond to those threats as the same way it presents the modern security services and applications which builds on SDN. The author undertakes wide-ranging survey on present work which provides security to SDN.

Research on SDN is still at starting stage, and consider it as strong indication that there is an important work have been done to put up modern security solutions and applications for these networks. The author has taken a complete analysis of security based research in SDN. The author has classified recent work into two main streams: i) threat discovery and recovery and ii) network appropriateness which simplify and improve security of networks. Further, the author has addressed feasible challenges and upcoming directions for secure SDN. The author examined security policies across heterogeneous networks to afford safe environments, and extending the OpenFlow standard with custom-made hardware and Network Function Virtualization (NFV) while building a more affluent set of features. [8]

The concept of SDN is extended to be applied to wireless networks. Traditionally, in a wired SDN environment, the OpenFlow protocol is the communication protocol used to configure the flow table of forwarding elements (i.e., switches and Access Points). However, although in IEEE 802.11 networks there is no concept of forwarding, the SDN paradigm could also be applied to set up the wireless network dynamically, in order to improve the performance. In this case, not only the network elements, that is the Access Points, but also the mobile elements should configure their link and physical layers parameters following the guidelines of a centralized SDN controller.

The Author discussed a mechanism called DEDCA (Dynamic Enhanced Distributed Channel Access) to manage the channel access in wireless networks, and a framework that enables its implementation in 802.11-based wireless networks using SDN technology. The key aspect of this alternative solution is the control over the contention window size of the wireless terminals. Thus, an adequate response to dynamic and short-term Quality of Service (QoS) requirements can be offered to services running on these networks. DEDCA mechanism relies upon the use of a scalar parameter called gain [9].

Software Defined Network (SDN) provides a new fine-grained interface enables the routing algorithm to have an a global view of the network throughputs, connectivity and flows at the data-path. The Author aims to provide a novel approach for dynamic routing algorithm for Software Defined Network in Wide Area Network (SDN-WAN); based on using a modified shortest-widest path algorithm with a fine-grained statistical method from the OpenFlow interface, called Shortest-Feasible OpenFlow Path (SFOP).

ISSN: 2233-7857 IJFGCN

This algorithm is designed to identify the optimal route from source to destination, providing efficient utilization of the SDN-WAN resources. It achieves this aim by considering both the flow requirements and the current state of the network. SFOP computes the optimal path which provides the feasible bandwidth with the lowest hop count (delay). That will present better stability in SDN communication, QoS, and usage of available resources. Moreover, this algorithm will be the base for an SDN controller because it extracts the widest available bandwidth from source to destination for a single path. It enables the controller to decide whether it is enough to use this simple algorithm only, or if a more complicated algorithm that provides larger bandwidth such as multiple-path algorithms is needed.

Finally, a test bed has been implemented using MATLAB Simulator, Pox controller, and Mininet emulator will be discussed. The latency comparison of SFOP algorithm with three other algorithm's latencies shows that this algorithm finds better latency for an optimal path. Evidence will be shown that demonstrates that SFOP has good stability in dynamic changes of SDN-WAN[10].

The proliferation of cloud-enabled services has caused an exponential growth in the traffic volume of modern data centres (DCs). An important aspect for the optimal operation of DCs related to the real-time detection of anomalies within the measured traffic volume in order to identify possible threats or challenges that are caused by either malicious or legitimate intent.

The Author present SDN-PANDA; a 'pluggable' software platform that aims to provide centralized administration and experimentation for anomaly detection techniques in Software Defined Data Centres (SDDCs) and present the overall design of the proposed scheme, and illustrate some initial results related to the performance of the current prototype with respect to scalability and basic traffic visualization. And argue that the introduced platform may facilitate the underlying functional basis for a number of real-time anomaly detection applications and provide the necessary foundations for such algorithms to be easily deployed [11].

d. Security in Control and Data Plane Layer

The author has discussed that SDWN is a modern technique in the field of wireless networks which can be used to handle the control and data independently. On one side, SDWN enables new security mechanisms. On another side new threats are identified due to the partition of the control plane and data plane. Similar to SDN, SDWN is exposed to new attacks due to physical separation of the control plane and data plane. Here the author discussed its security risk vectors as well as design issues in making it safe and sound. The authors have analyzed the security requirements of SDWN, then summarized the security attacks and counter measures in this region and suggest some future research guidelines.

SDWN, resulting from the extension of the SDN into wireless networks, will enjoy the benefits of cost-effective communications upgrading, release of new services, and development of user experience to existing infrastructure. Similar to SDN, SDWN is exposed to new attacks because of partition of the control plane and data plane physically. Research work to these types of issues has just commenced. The author hoped that, this article stimulates development of effective security solutions to make SDWN attack-flexible [12].

To allow engineers to immediate responding to rapid changes of business needs is the main objective of SDN. Another objective of SDN is making network as flexible, dynamic. SDN brings exactly that it physically divides data plane from control plane of the machine. Control plane deals all the functions and

ISSN: 2233-7857 IJFGCN

processes that determine e which path to use protocols. So SDN allow network engineers to control large data transmission from the control plane irrespective of switches and routers, so that the required services can be provided anywhere in the network.

The author highlighted a number of safety threats of computer network models layers like Data, Control and Application layers. The attackers target can predict from the architecture of SDN. An energetic, convenient and flexible rising architecture of Software Defined Network is initiative for elevated bandwidth and active nature of today's applications [13].

As communication technology and smart manufacturing have developed, the industrial internet of things (IIoT) has gained considerable attention from academia and industry. Wireless sensor networks (WSNs) have many advantages with broad applications in many areas including environmental monitoring, which makes it a very important part of IIoT. However, energy depletion and hardware malfunctions can lead to node failures in WSNs. The industrial environment can also impact the wireless channel transmission, leading to network reliability problems, even with tightly coupled control and data planes in traditional networks, which obviously also enhances network management cost and complexity.

The Author introduce a new software defined network (SDN), and modify this network to propose a framework called the improved software defined wireless sensor network (improved SD-WSN). This proposed framework can address the following issues. 1) For a large scale heterogeneous network, it solves the problem of network management and smooth merging of a WSN into IIoT. 2) The network coverage problem is solved which improves the network reliability. 3) The framework addresses node failure due to various problems, particularly related to energy consumption. Therefore, it is necessary to improve the reliability of wireless sensor networks, by developing certain schemes to reduce energy consumption and the delay time of network nodes under IIoT conditions. Experiments have shown that the improved approach significantly reduces the energy consumption of nodes and the delay time, thus improving the reliability of WSN [14].

e. Security in SDN

The sensor technology has gained awareness on WSN from research area and genuine user in many areas. The energy utilization continues to be a controlled source and remains a critical issue of Wireless Sensor Networks (WSN). Since the transmission of data in the network and communication between the networks also obsessive a lot of energy in WSN, the movement of the nodes of a sensor should be changed to extend the lifetime of the network. Finally, the author done the survey on how the energy consumption in WSN with the use of SDN. The readers understand in a better way, how SDN works and the usefulness of using SDN to manage the problems in WSN.

In this analysis, the author discussed several involvements to energy utilization in WSN, the structural design of SDN, implementation of various types of SDN on managing the energy utilization and the energy efficiency based on the latest work. The comparisons on how SDN helped to various domain networks to neutralize the energy shortage in WSN are shown in a tabular form. The complete survey has been done on the four networks (WSN, SDN, SDWN, and SDWSN) to prepare a total understanding of this pattern. Mainly the survey done on issues that needs solution to obtain its success [15].

The emergence of Internet of Things (IoT), there is now growing interest to simplify wireless network controls. This is a very challenging task, comprising information acquisition, information analysis,

ISSN: 2233-7857 IJFGCN

decision making and action implementation on large scale IoT networks. Resulting in research to explore the integration of Software Defined Networking (SDN) and IoT for a simpler, easier, and strain less network control. SDN is a promising novel paradigm shift which has the capability to enable a simplified and robust programmable wireless network serving an array of physical objects and applications.

This review article starts with the emergence of SDN and then highlights recent significant developments in the wireless and optical domains with the aim of integrating SDN and IoT. Challenges in SDN and IoT integration are also discussed from both security and scalability perspectives [16].

The SDN technology is broadly accepted by mobile engineering since fast development of Software Defined Networks (SDN). Author believes that SDN can add security in wireless mobile networks (WMN) through novel design by the benefits of SDN such as cost-effective, time saving, generalization, and directness. Depends on available solutions, author highlighted the key essentials and outline of the project. The author believes that this survey can help the way the SDN can use to improve the network security as part of continuing function [17].

The proposition of increased innovation in network applications and reduced cost for network operators has won over the networking world to the vision of Software-Defined Networking (SDN). With the excitement of holistic visibility across the network and the ability to program network devices, developers have rushed to present a range of new SDN-compliant hardware, software and services. However, amidst this frenzy of activity, one key element has only recently entered the debate: Network Security.

Author discussed, the security in SDN is surveyed presenting both the research community and industry advances in this area. The challenges to securing the network from the persistent attacker are discussed and the holistic approach to the security architecture that is required for SDN is described. Future research directions that will be key to providing network security in SDN are identified [18].

IOT has proven to be the most emerging technology where millions of devices can connect to the internet which makes the life feasible without any human intervention. This paper has analyzed the challenges associated with IOT technology. Two major issues security and privacy of data and user information has discussed in detail. In this research paper solution of major issue of security is also proposed. One of the important requirements of IOT is to have a quality of service where the data among the devices should be as high as possible without degrading the performance.

The Author proposed a software model based on Software Defined Network (SDN). Software Defined Network is a technology that increases the performance of the network and reduces the hardware usage and also provides a better security and privacy compare to the traditional networks. Lastly, the paper has discussed about the architectural design of SDN and suitable for IoT and Ad-hoc networks [19].

This article is a summary description of the Cognitive Packet Network (CPN) which is an example both of a completely software defined network (SDN) and of a self-aware computer network (SAN) which has been completely implemented and used in numerous experiments. CPN is able to observe its own internal performance as well as the interfaces of the external systems that it interacts with, in order to modify its behavior so as to adaptively achieve objectives, such as discovering services for its users, improving their Quality of Service (QoS), reduce its own energy consumption, compensate for components which fail or malfunction, detect and react to intrusions, and defend itself against attacks [20].

ISSN: 2233-7857 IJFGCN

IV. PROPOSED SYSTEM

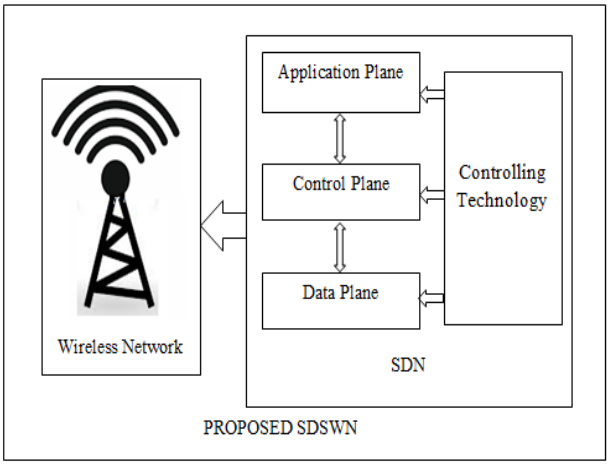

Fig. 1. Architecture of SDSWN

The Fig.1 shows the proposed Architecture of the Software Defined Secure Wireless Network (SDSWN). The SDN Comprises the three planes called Application Plane, Control Plane and Data plane which are controlled by the SDN Controlling Technology. The SDSWN module can be used to monitor the traffic, type of data packets and all other related parameters of Wireless Network. The concept of SDN enables the wireless networks to be implemented with high security so that the SDSWN is resulting. The proposed model is yet to be implemented and this model will give improved security for the wireless Networks.

V. CONCLUSION

A detailed knowledge were gained after the deep study on the various researches in the area of implementing security in wireless Network using Software defined network. The different security techniques were discussed according different phases of SDN. A Control Security technology will plan, to along with its design complexity and achievements to implement.

VI. REFERENCES

[1] Rohit Abhishek, Shuai Zhao, Deep Medhi (2016).
SPArTaCuS:Service Priority Adaptiveness for Emergency Traffic in Smart Cities using Software-Defined Networking. IEEE.

[2] Barki, L., Shidling, A., Meti, N., Narayan, D. G., &Mulla, M. M. (2016, September). Detection of distributed denial of service attacks in software defined networks. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2576-2581). IEEE.

[3] Kim, W. S., & Chung, S. H. (2016). Proxy SDN Controller for Wireless Networks. Mobile Information Systems, 2016.

ISSN: 2233-7857 IJFGCN

[4] Cunha, N., Lima, R., Anjos, E., & Matos, F. (2018). Software Defined Wireless Networking Approach for Managing Handoff in IEEE 802.11 Networks. Wireless Communications and Mobile Computing, 2018.

[5] Xianshu Jin, Hwiyun Ju, Sungchol Cho, Boyeong Mun, Cheongbin Kim, Sunyoung Han*(2016). QoS Routing Design for Adaptive Streaming in Software Defined Network. IEEE.

[6] Prashant D. Bhole, Dinesh D. Puri (2015). Distributed Hierarchical Control Plane of Software Defined Networking. ICCICN.(pp. 516-522).

[7] Faaiz S. Fizi, Shavan Askar (2016). A Novel Load Balancing Algorithm for Software Defined Network Based Datacenters. (CoBCom), (pp. 1-6).

[8] Ali, S. T., Sivaraman, V., Radford, A., &Jha, S. (2015). A survey of securing networks using software defined networking. IEEE transactions on reliability, (pp.1-12).

[9] A Software-Defined Networking Framework to Provide

Dynamic QoS Management in IEEE 802.11 Network Pilar

Manzanares-Lopez, JosemariaMalgosa-Sanahuja and Juan Pedro Muñoz-Gea(Sensor 2018), (pp. 1-24).

[10] Ameer Mosa Al-Sadi, Ali Al-Sherbaz, James Xue, Scott

Turner (2016). Routing Algorithm Optimization for

Software Defined Network WAN. (AICMITCSA).

[11] Brian R. Granby, b Askwith, Angelos K. Marnerides (2015).

SDN-PANDA: Software-Defined Network Platform for Anomaly Detection Applications, IEEE (pp. 463-466).

[12] Daojing He, Sammy Chan, & Mohsen Guizani (2016).

Securing software defined Wireless networks. IEEE

Communications Magazine, (pp. 20-25).

[13] Patil, V., Patil, C., &Awale, R. N. (2017, July). Security

challenges in software defined network and their solutions. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

[14] Duan, Y., Li, W., Fu, X., Luo, Y., & Yang, L. (2017). A methodology for reliability of WSN based on software defined network in adaptive industrial environment. IEEE/CAA Journal of AutomaticaSinica, 5(1), 74-82.

[15] Ali, N. F., Said, A. M., Nisar, K., & Aziz, I. A. (2017, November). A survey on software defined network approaches for achieving energy efficiency in wireless sensor network.In 2017 IEEE Conference on Wireless Sensors (ICWiSe) (pp. 28-33). IEEE.

[16] Sood, K., Yu, S., & Xiang, Y. (2015). Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet of Things

Journal.

[17] Ding, A. Y., Crowcroft, J., Tarkoma, S., &Flinck, H. (2014). Software defined networking for security enhancement in wireless mobile networks. Computer Networks, 66, 94-101.

ISSN: 2233-7857 IJFGCN

[18] Scott-Hayward, S., Natarajan, S., &Sezer, S. (2015). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1), 623-654.

[19] Fatma AL Shuhaimi, Manju Jose, Ajay Vikram Singh (2016). Software Defined Network as Solution to Overcome Security Challenges in IOT. IEEE, 491-496.

[20] Erol Gelenbe FIEEE FACM (2013). A Software Defined Self-Aware Network: The Cognitive Packet Network. Ninth International Conference on Semantics, Knowledge and Grids, (pp. 1-5)

[21] S.Palanivel Rajan, C.Vivek, "Analysis and Design of Microstrip Patch Antenna for Radar Communication", Journal of Electrical Engineering & Technology, Online ISSN No.: 2093-7423, Print ISSN No.: 1975-0102, Vol. No.: 14, Issue : 2, DOI: 10.1007/s42835-018-00072-y, pp. 923–929, 2019.

[22] S.Palanivel Rajan, M.Paranthaman, "Characterization of Compact and Efficient Patch Antenna with single inset feeding technique for Wireless Applications", Journal of Applied Research and Technology, ISSN: 1665–6423, Vol. 17, Issue 4, pp. 297-301, 2019

ISSN: 2233-7857 IJFGCN