International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Survey Paper on SDN and its Security Flaws

Nirsen Amal. A[1], Mr. Kuldeep Baban Vayadande[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Jain Deemed to be University, Bangalore, Karnataka, India

ABSTRACT
The Internet has prompted the production of an advanced society, where everything is associated and is open from anyplace. The conventional IP networks are brimming with intricacy and extremely difficult to oversee. It is both hard to design the organization as indicated by predefined strategies, and to reconfigure it to react to stack, blames and changes. To make things more troublesome current organizations are likewise vertically incorporated: the control and information planes are packaged together. Programming characterized organizing is an arising worldview that vows to change this situation, by breaking vertical coordination, isolating the organization's control rationale from the switches a lot, advancing centralization of the organization control, and presenting programmability of the organization. The worries, presented between the meaning of organization approaches, their execution in exchanging equipment, and the sending of traffic, is vital to the adaptability: by breaking the organization control issue into manageable pieces, SDN makes it simpler to make and present new deliberations in systems administration, streamlining network the board and empowering network advancement. In this paper, we present an overview on SDN and its security imperfections.

KEYWORDS: _SDN, Cyber security, SDN Vulnerabilities, SDN-WAN_

How to cite this paper: Nirsen Amal. A | Mr. Kuldeep Baban Vayadande "Survey Paper on SDN and its Security Flaws" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.634-639, URL: www.ijtsrd.com/papers/ijtsrd38029.pdf

IJTSRD38029

1. INTRODUCTION

Programming Defined Networking (SDN) and an assorted arrangement of SDN-based security applications will quickly pick up footing in the battle against cybercrime. SDN makes it simpler to gather network utilization data, which supports improved calculation configuration used to recognize assaults. The new age of uses will exploit better-educated SDN specialists to improve strategy requirement and traffic peculiarity discovery and moderation. These applications could hinder malevolent interlopers before they enter the basic areas of the network. The greatest advantage of SDN-empowered security is that it presents an open door for keen reaction on a granular premise by selectively blocking noxious traffic while as yet permitting ordinary traffic streams. Furthermore, SDN security applications are equipped for following up on any peculiarities by redirecting explicit organization streams to extraordinary authorization focuses or security administrations, for example, firewalls and interruption location/avoidance frameworks. When executed, SDN has an incredible potential to accomplish more noteworthy organization security perceivability and quickening the movement of actualizing new security benefits viably. Hackers are a steady danger to associations, energetically looking to abuse shortcomings in PC frameworks to benefit from the undermined information. Add to this the way that organization traffic is expanding in big business and distributed computing server farms. Subsequently, security activities groups are getting overpowered by the need to filter through security cautions and tune security motors for the most recent threats. And security needs will just develop as the IOT continues to advance.

One approach to connect this developing security hole is through canny occurrence location and mechanized response. Recently, the requirement for programmable organizations has drawn the interest of industrialists and academicians to build up a programmable systems administration model called programming characterized network (SDN). It is an exertion that will isolate network knowledge (control plane) from sending equipment (information plane). This paper will give an away from on the working of SDN and an open interface convention called Open Flow (OF). We give a wide knowledge into the working of SDN and different difficulties confronted while executing it, for example, versatility, regulator bottleneck, load adjusting in circulated regulator climate, directing and security just as its defects in detail. We examine about the various situations at which SDN is defenseless against assaults and the answers for such assaults and the conceivable security assaults in the information plane, control plane and the interface between them are expounded.

2. ARCHITECTURE

SDN can be characterized as the decoupling of control and bundle sending planes in the organization. It permits organizations to legitimately associate with applications through application programming interfaces (APIs), reinforcing application execution and security, making an adaptable, unique organization engineering that can be changed when required.

The most much of the time utilized methods for application arrangement, SDN is utilized by endeavors to send their applications quicker while additionally cutting the general organization and working expenses. IT heads utilizing SDN can oversee and arrangement their organization administrations from an incorporated point.

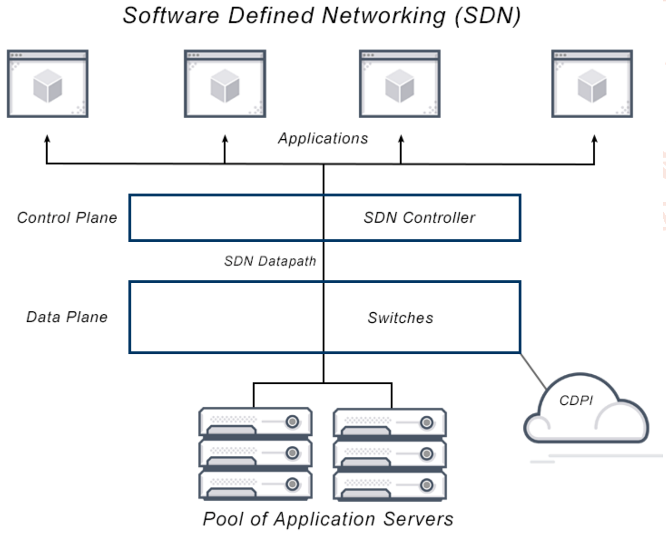
An organization worldview that gives automatic administration and control, and organization asset improvement, SDN applies open APIs to help keep up network control. The organization control is made when SDN decouples the organization design and traffic designing, isolating them from their essential equipment framework.

This splitting permits the utilization of Open Flow and other open conventions. These open conventions can get to organize switches and switches that regularly utilize restrictive and in any case shut firmware by applying around the world mindful programming control at the organization's edge.

With regards to making their own organizations, each association needs to comprehend the upsides and downsides of the diverse organization types. With expanded requests for execution and adaptability, a few cons immediately become more hard to handle than others.

Alongside the developing necessities of present day organizations, the greatest cons of keeping up customary organizations have reinforced the power of SDN.

SDN arrangements and other virtualized arrangements are thriving. The Globe Newswire contends that the SDN market will arrive at USD 59 billion by 2023.



SDN helps clients virtualize their equipment and attempts to make a PC network by separating the organization into the accompanying separate planes:

1. The control plane offers the presentation and flaw the board of Net Flow and, similar to conventions, is much of the time utilized for overseeing gadget arrangements that are distantly associated with a product characterized network.
2. The information plane advances traffic to its ideal objective. Before traffic arrives at the information plane, the control plane directs what way streams it will take by utilizing the stream convention—when an organization manager works with the product characterized networks and deals with the organization.

At the point when it was first sent by enormous endeavors, for example, Google and Amazon, SDN helped them make versatile server farms, encourage network assets and new worker extension, and decrease the outstanding task at hand for IT managers. SDN upgraded the proficiency of the up scaling cycle for these enormous organizations and immediately drew the consideration of other huge organizations who quickly embraced SDN to improve their up scaling effectiveness.

Conventional systems administration is established in fixed-work network gadgets, for example, a switch or switch. These gadgets each have certain capacities that work well together and backing the organization. On the off chance that the organization's capacities are executed as equipment builds, at that point its speed is typically reinforced.

Adaptability is a common obstacle for customary organizations. Not many APIs are uncovered for provisioning and most exchanging equipment and programming is restrictive. Customary organizations regularly function admirably with restrictive provisioning programming, yet this product can't be immediately altered varying.

Conventional systems administration comprises of the accompanying characteristics:

1. The elements of customary systems administration are essentially executed from committed gadgets utilizing at least one switches, just as switches and application conveyance regulators.
2. The usefulness of customary systems administration is generally actualized in devoted equipment, for example, application-explicit coordinated circuits (ASIC). One of the negative parts of this conventional equipment driven systems administration is its constraints.

The most outstanding contrast among SDN and conventional systems administration is that SDN is programming based while customary systems administration is generally equipment based. Since it's product based, SDN is more adaptable, permitting clients more noteworthy control and straightforwardness for overseeing assets practically all through the control plane.

Contrarily, conventional organizations use switches, switches and other actual foundation to make associations and run the organization.

SDN regulators include a northward interface that speaks with APIs. As a result of this correspondence, application engineers can legitimately program the organization, instead of utilizing the conventions needed by customary systems administration.

SDN lets clients use programming to arrangement new gadgets as opposed to utilizing actual framework, so IT chairmen can coordinate organization ways and proactively orchestrate network administrations. In contrast to customary switches, SDN likewise can more readily speak with gadgets utilizing the organization.

Virtualization typifies the essential distinction among SDN and conventional systems administration. At the point when SDN virtualizes your whole organization, it produces a theoretical duplicate of your actual organization, and lets you arrangement assets from an incorporated area.

Opposingly, with a customary organization the actual area of the control plane blocks an IT director's capacity to control the traffic stream.

With SDN, the control plane becomes programming based, permitting it to be gotten to through an associated gadget. This entrance lets IT executives oversee traffic stream with more noteworthy detail from a unified (UI). This unified area awards clients more noteworthy power over how their organizations work and how their organizations are arranged. The capacity to rapidly deal with various organization setups from an incorporated UI is particularly helpful for network division.

SDN turned into a mainstream option in contrast to conventional systems administration since it lets IT executives arrangement assets and transmission capacities varying without requiring a speculation of extra actual framework. Customary systems administration requires new equipment to expand its organization limit. The worldview for SDN versus conventional systems administration could be refined to the speculation: one requires greater hardware for development and the different requires just keystrokes.

2.1. ADVANTAGES OF SDN

SDN has the benefit of creating a structure that supports information escalated applications, for example, huge information and virtualization. Large information and virtual machines are fairly interlaced. Ingram Micro contends that "Virtualization reception is being driven by large information and SDN gives the way to oversee virtual machines and huge information network traffic."

Notwithstanding incorporating and streamlining the control of big business network the board, SDN offers the accompanying brief preferences:

- ➢ Traffic programmability
- ➢ Greater spryness
- ➢ Capacity to produce strategy driven organization oversight
- ➢ Ability to execute network mechanization

1. Incorporated organization provisioning. SDN brings together undertaking the board and provisioning by offering a bound together point of view in general organization. SDN can likewise accelerate administration conveyance and lift deftness in provisioning virtual and actual organization gadgets in a focal area.
2. All encompassing undertaking the board. Organizations must satisfy the rising need for preparing demands. SDN enables your IT division to change your organization setup with no effect on your organization. Likewise, dissimilar to Simple Network Management Protocol (SNMP), SND reinforces the administration of physical and virtual switches and organization gadgets that are from a focal regulator.
3. More granular security. Virtual machines represent a test for firewalls and substance separating, a test that is additionally compounded by close to home gadgets. By setting up a focal control point for directing security and strategy data for your endeavor, the SDN regulator rapidly turns into a help for your IT division.
4. Lower working expenses. A few advantages to SDN, for example, having a proficient organization, worker usage upgrades, and improved virtualization control, can dually help cut working expenses. Since numerous customary organization issues can be robotized and incorporated, SDN can likewise help diminish working expenses and develop regulatory reserve funds.
5. Equipment investment funds and decreased capital consumptions. SDN selection resuscitates more seasoned organization gadgets and rearranges the way toward streamlining commoditized equipment. By adhering to the directions from the SDN regulator, more seasoned equipment can be repurposed while less expensive equipment can be sent to ideal impact. This cycle permits new gadgets to become genuine "white box" switches that have insight centered at the SDN regulator.
6. Cloud deliberation. Utilizing SDN to extract cloud assets disentangles the way toward bringing together cloud assets. SDN regulators can deal with all the systems administration parts that include the enormous server farm stages.
7. Steady and opportune substance conveyance. One major advantage of SDN is the capacity to control information traffic. It's simpler to have nature of administration for Voice over Internet Protocol (VoIP) and mixed media transmissions on the off chance that you can coordinate and computerize information traffic. SDN additionally assists with steaming greater recordings since SDN reinforces network responsiveness and, accordingly, makes an improved client experience (UX).

1. The present clients request the untethered admittance to framework, applications and IT assets. This interest comes because of the expansion of cloud administrations, which requires extra stockpiling, processing and transmission capacity.
2. The coming of acquire your-own-gadget the work environment requires dynamic and adaptable organizations. These organizations should likewise be security rich and equipped for ensuring information and resources, and fulfilling consistence guidelines and guidelines. Since it holds fast to item cycles and merchant explicit climate restrictive interfaces, conventional systems administration can't fulfill these needs. Conventional systems administration will in general be inflexible, making it hard for network administrators and heads to alter the programming of their organizations. The way toward adding gadgets or expanding network limit is unwieldy and tedious, requiring involved admittance for each comfort and gadget.
3. SDN lets network administrators and managers change their assets and transmission capacities varying, giving server farms helped effectiveness, pliability and strength. Likewise, SDN doesn't need putting resources into actual framework and isn't generally equipped for being robotized, which further reinforces the odds of undertakings to reduce expenses and improve network execution.

2.2. SDN VERSUS CONVENTIONAL ORGANIZATIONAL NETWORK

The ascent of distributed computing and the expanded interest for versatility and far off cooperation is squeezing customary venture organizations to perform like cloud organizations. For endeavors with these customary organizations, this circumstance frequently results in more slow advancement, improvement and production. In the IBM white paper, Software-characterized organizing in the new business wilderness, the creator contends that "Conventional organization structures that are excessively old, unbending and costly proportional are crooked with today's hybrid cloud (a combination of traditional, public and private cloud infrastructure) and IT as a service (ITaaS) deployments."(4) Networks that are automated and optimized within a virtualized and hybrid IT environment are more likely to help enterprises produce greater innovations and reductions in cost and complexity.

For traditional network infrastructure, each switch determines where traffic goes and then directs the traffic based off of these determinations. With SDN infrastructure, the process of determination and direction has been decoupled. Switches still direct the traffic, however the process of determining where the traffic goes is performed by an automated programmable interface. Also known as an SDN controller, this centralized control point automates network management and control and has oversight into all of the SDN's nodes.

Performed from a concentrated control point that incorporates the data and meshes the organization switches together into a solitary bound together stage. This stage permits network directors to change network-wide settings with a brought together support. While customary organization framework may warrant conveying network changes in a piecemeal manner for singular gadgets, the concentrated reassure of the SDN's foundation smoothes out the way toward performing network changes. With the concentrated comfort, the product can send fundamental organization changes firmly and consistently to every single essential gadget. Multivendor exchanging gear can likewise send any essential changes utilizing a solitary interface.

The IBM white paper expresses that "[SDN answers] the requirement for deftness, versatility and perceivability by changing equipment concentrated inheritance networks into completely programmable, virtualized [SDN] that smooth out tasks and the conveyance of new services"4. SDN framework gives network chairmen the adaptability to change network traffic and empowers network asset sending that scales at a similar speed as worker and capacity, diverting it varying. Furthermore, the SDN regulator diminishes unpredictability and empowers the organization to scale varying. The advantages of SDN are that it can assist ventures with advancing advancement and improvement and quicken time to advertise for applications and administrations.

In light of their likenesses, SDN is frequently contrasted and programming characterized wide territory organizations (SD-WANs). By utilizing broadband and Multiprotocol Label Switching (MPLS).SDN-WAN lets endeavors associate various areas. SDN is intended to work on neighborhood (LANs) and is utilized for making networks that can be rapidly changed varying. SD-WAN is intended to deliver a wide zone organization (WAN) that connects a few destinations together and uphold a WAN for a wide geological spread.

Like SDN, a SDN-WAN disposes of the requirement for keeping up loads of organization equipment. Furthermore, a SD-WAN can be utilized from a product characterized network where it offers the topographical capacities of a SD-WAN alongside the adaptable ability of SDN to be designed varying.

Likewise, SDN is arranged by the IT executive or the client, while sellers control a SD-WAN help. Since clients aren't answerable for offering the administration, a SD-WAN will in general be simpler to convey.

SDN regulator is the center of organization control. The programmable of organization and organization application are acknowledged through normalization. Specialized engineering of SDN is appeared in this design, network characterized by programming. Organization head execute more adaptable organization controls without physically changing the setup of each organization gadget.

3. VULNERABILITIES

SDN's weakness issue is chiefly gathered in charge plane and application plane.

3.1. CONTROL PLANE

Weakness of the Control Plane Centralized control plane is the foundation of organization administration, which is legitimately identified with the accessibility, dependability and information security of organization administrations. Contrasted and customary organization, SDN regulator is a significant weak point, which is the principal issue to be illuminated in SDN security. In control plane, the dangers confronting the control plane are as per the following.

1. Network observing Network aggressor gets the regulator's cut-in point from the organization, and afterward manufactures and changes control signal.
2. IP address parodying Network aggressor produces IP address to ridicule IP address through organization checking to get trust of the switch or switch. Organization hardware can be controlled to do whatever network assailant needs to do.
3. DDoS assault The assailant sends numerous assistance solicitations to the regulator, and all the mentioned return addresses are produced, which can over-burden the regulator and deny assistance.
4. Virus, worm and Trojan assault The assailant oversees the regulator and implanted pernicious code through escape clauses existing in the regulator.

Weakness of SDN control plane For an ordinary activity of SDN network framework, if the assailant can oversee or dispatch framework assets, (for example, trade, directing, access control, stream control, throughput control, and so forth), and make the capacity or execution of SDN framework influenced, it is said that SDN control framework is delicate, that implies SDN control plane is powerless. 255 Advances in Engineering Research (AER), volume 148 Formal as of now, Open Flow convention and SSL convention are utilized to convey between SDN regulator and general organization gadgets. Furthermore, the weaknesses of those two conventions are additionally the wellspring of SDN control plane's weakness. It is essential to plan a control transport procedure dependent on these two protocols. Controlled weakness of SDN control plane A typical activity of SDN network framework, in the event that it is an asset methodology of the administration and dispatch framework to counter assault, so the capacity and execution of SDN network framework can be played ordinarily, the weakness of the SDN control framework is controllable. That implies the organization proprietor has the system to control the weakness of SDN control plane.

3.2. APPLICATION PLANE

Weakness of the Application Plane The application layer will give an assortment of complex organization application administrations through application programming and the executives procedure, and it additionally has a similar weakness issue due to the programmability of the application level. The weakness of the application plane primarily incorporates:

1. Malicious application: Through the application layer of the utilization of worms, spyware, etc, to take network data, change network arrangement, involve network assets, etc, to meddle with the typical working cycle of the control plane, so the regulator control of the organization disarray.
2. Application of the Security rule struggle: In request to give different kinds of organization application benefits, the application layer needs to create security rules to get to a portion of the regulator's security interfaces. With the difficulty of use, there is a contention of security rules between different applications, which prompts the disarray of organization administrations and the expansion of the board intricacy. To diminish the weakness of SDN application plane, it is important to think about the sensibility of SDN application. Just SDN application is sensible, and the weakness of its application plane can be controlled.

Weakness reasonability of SDN application plane For SDN network application administration framework, if the technique of overseeing and dispatching framework assets exists, the application administration arrangement of SDN application plane will has diverse safe running execution. It is said that the weakness of SDN network application plane can be overseen by the control technique. Conversation on Reducing the Vulnerability of SDN To manufacture a protected SDN network, lessen the weakness of SDN network, it is important to successfully deal with the gear, application, security control technique, guidance transmission methodology, application administration the executives system and execution. We talk about the weakness of SDN from the control plane and the application plane. In view of the investigation in the past area, we assemble an insurance control methodology of SDN network.The first is to expand the control of the transmission technique in the control level. The regulator's transmission control and access control is delicate controllable and reasonable, and doesn't permit the regulator API programming interface to be excessively open and make it under the security rules, and control the guidance transmission. The second is to expand the application the board system in the application level. The Open help, application administration access rules and the programmable interface of utilization are overseen and controlled. 258 Advances in Engineering Research (AER), volume 148 At the control level, the security strategy control is designed and overseen by the regulator. What's more, the trade, steering and sending are brought out through the control guidelines gave by the regulator. So the control of the control plane expanded the transmission technique. The regulator has a progression of severe approval, access control, security the executives, programming interface control and different standards. So the apparent strange organization gear, anomalous conduct so as to detach, to maintain a strategic distance from enormous scope harm. Simultaneously the regulator as per the control transmission system can investigate the organization conduct capacity concurring the log, the traffic, the current help, etc. It is normally necessitated that the control level must be planned with an adequate number of control systems p and its application work g , so the regulator gets enough viable control procedure to Pc P ⊂ the quantity of ( ) A f Sc D≠ . What's more, the plan of the control technique application work g comparative with the aggressor's capacity f must be intricate enough. This limits the weakness of the SDN network control layer to guarantee the security of the control plane of the SDN network. At the application plane, utilizing the expanded application the executives procedure, the application plane has a progression of security administration access rules and application the board system, can be utilized to offer types of assistance, just as the requirement for the interface of the regulator to distinguish, the use of rules and arrangements to be permitted to turn into an authentic application in SDN. It can likewise be utilized to screen and kill security dangers with the administration control technique of programmable interface and the current innovation, and further reinforce the security insurance of the application plane regulator. Simultaneously, the application plane approaches control methodology, which can keep aggressors from utilizing the open interface to assault the organization regulator through the application administration, and utilize a few interfaces to screen the organization. As a rule for every application plane, an application the executives methodology must be discovered an I( ) to make the Se an I ( )) the biggest, with the goal that the weakness of the SDN network application plane is limited and the administration execution is best applied to guarantee the security and dependability of the SDN network application administration.

4. KNOWN VULNERABILITIES IN SDN

1 CVE-2018-1078 2018-03-16 2019-10-09 7.5 None
Remote Low Not required Partial Partial Partial Open Day Light variant Carbon SR3 and prior contain a weakness during hub compromise that can bring about traffic streams that ought to be lapsed or ought to terminate in no time being re-introduced and their clocks reset bringing about traffic being permitted that ought to be lapsed.

2 CVE-2017-1000411 404 Overflow 2018-01-31 2019-10-02 5.0 None
Remote Low Not required None None Partial Open Flow Plugin and Open Day Light Controller forms Nitrogen, Carbon, Boron, Robert Varga, Anil Vishnoi contain an imperfection when various 'terminated' streams take up the memory asset of CONFIG DATASTORE which prompts CONTROLLER closure. On the off chance that various streams with 'inert break' and 'hard-break' are shipped off the Open flow Plugin REST API, the terminated streams will in the long

run crash the regulator once its asset distributions set with the JVM size are surpassed. Despite the fact that the introduced streams (with break set) are taken out from organization (and in this way from regulator's activities DS), the lapsed sections are as yet present in CONFIG DS. The assault can begin both from NORTH or SOUTH. The above portrayal is for a north bound assault. A south bound assault can start when an assailant endeavors a stream flooding assault and since streams accompany breaks, the assault isn't effective. Notwithstanding, the aggressor will currently be effective in CONTROLLER flood assault (asset utilization). In spite of the fact that, the organization (real stream tables) and operational DS are just (~)1% involved, the regulator demands for asset utilization. This happens on the grounds that the introduced streams get eliminated from the organization upon break.

3 CVE-2015-1612 20 2017-04-04 2017-04-11 5.0 None Remote Low Not required None Partial None Open Flow module for Open Day light before Helium SR3 permits far off aggressors to parody the SDN geography and influence the progression of information, identified with the reuse of LLDP parcels, otherwise known as "LLDP Relay."

4 CVE-2015-1611 20 2017-04-04 2017-04-11 5.0 None Remote Low Not required None Partial None Open Flow module for Open Day light before Helium SR3 permits distant aggressors to parody the SDN geography and influence the progression of information, identified with "fake LLDP infusion."

5. CONCLUSION

At present, the research on the security and vulnerability of SDN network is still in its initial stages. This paper first analyzed the SDN technical architecture principle and the development present situation. We researched the security characteristic and the vulnerability question in the SDN structure, analyzed its vulnerability in the control level and the application level and proposed the corresponding vulnerability question judgment model. On this basis, the architecture of the protection control architecture is constructed.

This architecture explore controllable and manageable problems of network, which is expected to promote the further research on the security and vulnerability of SDN network.

6. REFERENCE

[1] Prof. Trupti Lotlikar Department of Information Technology Terna Engineering college/ Fr. CRIT NaviMumbai, India., Dr. Deven Shah Department of Information Technology Thakur College of Engineering and Technology Kandivali, Mumbai, India "A Defense Mechanism for DoS Attacks in SDN (Software Defined Network) "

[2] Sandra Scott-Hayward, Member IEEE, SriramNatarajan and SakirSezer, Member IEEE "A Survey of Security in Software Defined Networks" IEEE communication survey and tutorials, Vol 18, No.1. First quarter 2016.

[3] Zhaogang Shu, Jaifu Wan, Di Li, J. Lin, A. Vasilakos, "Security in Software Defined Networking: Threats and Countermeasures." published in 2016.

[4] R. Kl¨oti, V. Kotronis, P. Smith, "Open Flow: A SecurityAnalysis,"2013.

[5] YogitaHande and AishwaryaJadhav "Software defined networking with Intrusion Detection System" in International Journal of Engineering and technical Research (IJETR) Volume 2, issue-10, October 2013.

[6] E. Al-Shaer and S. Al-Haj, "Flow Checker: Configuration analysis and verification of federated open flow infrastructures," in Proc. 3rd ACM Workshop SafeConfig, 2010.

[7] Haopei Wang, Lei Xu and GuofeiGu, Texas A&M University " OF-GUARD:A DoS attack prevention extension in Software –Defined Networks" published at open Networking Summit 2014, Research track, Santa Clara, CA.

[8] Charu P. P and Mary John, "A framework for design and simulation of Dos Attacks on SDN Network "international journal of innovative research in computer and communication engineering, vol.4, Issue 2, February 2016.

[9] K. Benton, L. J. Camp, and C. Small, "Open Flow vulnerability assessment," in Proc. 2nd ACM SIGCOMM WorkshopHotSDN, 2013.

[10] Zhaongang Shu, Jaifu Wan, Di Li ,Muhammad Ali Imran," Security in Software-Defined Networking: Threats and Countermeasures" Mobile Networks and applications