*Literature Review Draft No 1*

***Introduction –***

***Software-Defined Networking (SDN)*** *is a developing system design which improves network management and optimization with fine-grained and centralized control. By decoupling the control plane and the data plane, it has empowered uncommon programmability, computerization, and advancements in PC systems. In this manner, the run of the mill SDN foundation comprises of three noteworthy segments: the control plane, the data plane and a control channel where the two planes can impart through standard conventions.*

*As the accepted standard SDN convention, OpenFlow presents a receptive packet processing instrument with the match-action paradigm: an OpenFlow switch forms packets dependent on stream tables and when no stream sections in the neighbourhood stream table match a specific packet (known as a table-miss), the switch exemplifies this packet in a packet-in message and advances it to the controller for further processing. (M. Zhang, J. Bi, J. Bai and G. Li, 2018)[[1]](#footnote-1)*

***OpenFlow*** *- OpenFlow (OF) is viewed as one of the primary software-defined networking (SDN) models. It initially characterized the correspondence convention in SDN environments that empower the SDN Controller to straightforwardly communicate with the forwarding plane of network devices, for example, switches and routers, both physical and virtual (hypervisor-based), so it can more readily adjust to changing business prerequisites.* *(SDxCentral, 2019)[[2]](#footnote-2)*

*OpenFlow protocol in an SDN network gives the correspondence between the data plane and controller through a safe channel, (for example, SSh and IPsec). One of the DoS assaults done in SDN is the packets that are sent to OpenFlow switches utilizing fake addresses. The protected divert utilized in the OpenFlow convention can't avert this sort of attack. For this situation, every single sent packet from the switch could reach a controller. As the quantity of the packets sent to the controller expands, its resources (bandwidth, CPU) starts to deteriorate. The controller whose resources are devalued winds up clogged. The outcome is that the controller as a brain of the network when is blocked, the entire network collapses.*

*In any case, SDN's primary advantages – control logical centralization and network programmability – present new fault and attack planes. As it were, SDN makes new dangers that did not exist previously or were more diligently to abuse. For example, appropriated control rationale in customary systems offers normal safeguards against Denial-of-Service (DoS) attacks, avoiding them from influencing the entire system. Then again, an effective DoS attack on the SDN controller may injure the whole system. New attacks focusing on SDN vulnerabilities are being grown, for example, (I) Link fabrication attack and (ii) Host location hijacking [17]. These attacks focus on the network disclosure capacities of SDN exploiting the pool of authentication in reporting topology changes. (D. Ibdah, M. Kanani, N. Lachtar, N. Allan and B. Al-Duwairi, 2017)[[3]](#footnote-3)*

*We will be considering two types of DoS attacks that will affect an SDN network. In the main attack, the attacker means to debilitate the control plane data transfer capacity by flooding the system with painstakingly created packets that the switch has to send to the controller. To the extent the authors know, this attack has not been completely analyzed before. The second attack plans to fill up the switch's memory to store packet forwarding rules. This attack has been recently examined by Kloti et al. However, ¨ while Kloti et al. test the attack with OpenFlow 1.0 and POX ¨ controller.*

*We emulate these attacks on the Mininet framework and dissect the impacts of the attacks.*

***DoS Attack to SDN Controller.***

*In SDN, DoS attack is an attempt to make network devices like controllers, PCs, routers, switches, servers or network resources inaccessible to its intended clients. An attack in SDN controller works for making it difficult for the controller to handle every one of the solicitations. It additionally goes for introducing fake flow tables, which are pointless to the data plane devices hence making it inconceivable for the data plane devices to store flow table for genuine packets.*

*Ordinarily, in SDN, each packet got in the port of a switch is coordinated with the current flow table. In the event that a flow table exists for a packet when a packet is sent to an outgoing port, a packet is put away in a buffer and a packet header is sent to the controller utilizing OFPT\_PACKET\_IN. Whenever a controller is recently known to be on the outgoing port, a flow table is introduced to the switch by utilizing OFPT\_FLOW\_MOD generally flooding a packet to all switch ports with the exception of an incoming port of a switch to become familiar with the destination.*

*The packet with an alternate source IP address implies that the vast majority of the packets will prompt packet miss in the switch flows tables as a result of the packets being sent to the controller. For this situation, a controller will be overflowed with numerous packets to the process and composing a flow table back to the switch. In any case, the switch buffers may come up short on memory in light of over-burdening with useless flow table. Accordingly, no more flow table will be introduced in the switch. This bottleneck to the controller may result in numerous packets being dropped consequently low throughput and a longer delay in the network.[[4]](#footnote-4)*

*Experts have explored the different techniques misused in various vulnerability attacks on DoS in SDN networks. K. Cabaj et al. featured the attributes of SDN networks in connection to security. So as to achieve a verified security framework in SDN networks, they recommended three basic perspectives that ought to be considered. Initial, a constrained include given by an OpenFlow protocol, which gives the correspondence between the data plane and controller. Second, global network see that ought to be observed by a solitary point, what's more, finally no help ought to be accommodated extra applications like middleboxes, NAT or firewall in the engineering structure of SDN. In actuality, SDN structures may incorporate extra applications like load balancing, routing, firewall, middleboxes and NAT through northbound API.*

*The investigation of Jeremy M. Dover attempted to exploit the vulnerability in the Open Floodlight controller. He showed that an assailant with access to the OpenFlow control network can specifically deny or crippling correspondence between an individual forwarding plane with a controller by utilizing datapath\_id or dpid. The aggressor data plane will boot utilizing the equivalent datapath\_id being utilized by a real data plane compelling the controller to end the association with the genuine one. In the event that the aggressor intentionally planned to deny the genuine data plane access, it will objectively do it in a more tightly cycle than the real data plane.*

*While Seungwon and Guofei Gu noticed that an attack on SDN network by utilization a fingerprint attack can be perceived by the diverse reaction time from the SDN network when there is no flow for a packet and when there is a flow. Realizing the objective network is utilizing SDN and the state of the flow rule, the assailant can send a packet to consume SDN resources.*

*In Kevin Benton et al. clarified the absence of help of TLS in a large portion of the kinds of switches and controllers utilized in SDN network. They showed that a controller or entire SDN network might be presented to DoS attacks with Packet-In messages when the responsive guidelines planned are not cautiously executed. They represented this by demonstrating an l2\_learning segment in POX controller which typically leaves a probability of numerous attacks like traffic flooding of a multicast address; traffic to obscure MAC address is overflowed without a standard addition or a cutoff counter and topping off a switch flow table by making packets with random source MAC addresses.*

*Then again, Kandoi, R. what's more, Markku A. examined two sorts of DoS attacks explicit to OpenFlow SDN networks; attacks on the control plane bandwidth and attack on the switch's flow table. They discovered that the timeout estimation of a flow table and the bandwidth between a switch and controller significantly affected the switch's ability. In any case, their investigation was just centred around POX controller and did exclude different measurements, for example, switch buffer. To add on, the impact of bandwidth between two imparting hosts was not clarified, if every one of the attacks were to be performed at the same time.*

***References***

Benton, Kevin, L. Jean Camp, and Chris Small. "Openflow vulnerability assessment." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013.

Cabaj K, Wytrebowicz J, Kuklinski S, Radziszewski P, Dinh KT. SDN Architecture Impact on Network Security. InFedCSIS Position Papers pp. 143-148, 2014 Sep

Dover, Jeremy M. "A denial of service attack against the Open Floodlight SDN controller." 2013

Ieeexplore.ieee.org. (2019). *FloodShield: Securing the SDN Infrastructure Against Denial-of-Service Attacks - IEEE Conference Publication*. [online] Available at: https://ieeexplore.ieee.org/document/8455969 [Accessed 14 Apr. 2019].

Ieeexplore.ieee.org. (2019). *On the security of SDN-enabled smartgrid systems - IEEE Conference Publication*. [online] Available at: https://ieeexplore.ieee.org/document/8251983 [Accessed 14 Apr. 2019].

Kandoi, Rajat, and Markku Antikainen. "Denial-of-service attacks in OpenFlow SDN networks." Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015.

SDxCentral. (2019). *What is OpenFlow? Definition and How it Relates to SDN*. [online] Available at: https://www.sdxcentral.com/networking/sdn/definitions/what-is-openflow/ [Accessed 14 Apr. 2019].

1. Reference taken from Paper - FloodShield: Securing the SDN Infrastructure Against Denial-of-Service Attacks. [↑](#footnote-ref-1)
2. Reference taken from <https://www.sdxcentral.com/networking/sdn/definitions/what-is-openflow/> [↑](#footnote-ref-2)
3. Reference taken from Paper – On the Security of SDN-Enabled Smartgrid Systems. [↑](#footnote-ref-3)
4. Reference taken from Paper – The Effects of DoS Attacks on ODL and POX SDN Controllers. [↑](#footnote-ref-4)