A Survey of Potential Security Threats and Counter-Measures in SDN: An IoT Enabling Technology

Trupti Lotlikar, Deven Shah
trupslotlikar@gmail.com, sir.deven@gmail.com
Mumbai University

Abstract: *The exponential growth of new applications and services in both mobile devices and fixed terminals has made the communication networks a crucial point at homes and enterprises. This results in the development of new IoT applications connecting heterogeneous devices to the internet. Internet of Things (IoT) and Software defined network (SDN) can be integrated together to eliminate the use of traditional point to point connection between heterogeneous devices. Securing such complex heterogeneous networks is however a real challenge in network security. This paper focuses on various potential security challenges in SDN such as saturation attacks, denial of service (DoS) attack and its countermeasures. This paper is a step to further initiate research in SDN security as it is crucial enabler technology for IoT*

Index Terms: *Internet of Things, Software defined network, SDN security*

I. Introduction

With the spread of the Internet of Things (IoT), new complexities in both networking and internetworking in current and future networks are been imposed. Hence, networks must adapt to heterogeneity, in networking behaviour and underlying protocols. Each IoT object or entire environment has been defined in isolation and designed to solve a specific problem or attain specific objectives. IoT indicates the interconnection of several heterogeneous networks, the objects that compose them, the environments they are running, the protocols they use and the different objectives they have. This challenge could be solved using a common protocol. However different objects and protocols as mentioned, have a different requirements and objectives and hence a common protocol would not be a good option[3].Lack of standard, limits the network operators to design the networks according to their individual environment dynamically and also to neither improve their hardware nor the software.SDN would come as an rescue here. Software defined networking is a network technology where the control plane logic is decoupled from the forwarding plane and has the ability to control, change and manage network behaviour dynamically through software via open interfaces.SDN plays a role to retain the heterogeneity in networks and objects by integrating into them a control solution that interacts with the SDN controllers. Hence there is a need for the integration of SDN and IoT, since it is a crucial enabler of IoT. The rest of the paper is organized as follows. Section II describes the need for integration of IoT with SDN. Section III discusses the proposed integration of IoT with SDN. Section IV discusses SDN and its security loopholes and analysis the potential attacks on the layered structure of SDN. Section V discusses the crucial attacks and its countermeasures. Section VI concludes the paper with research conclusions

II .Why IoT Based SDN?

There would be various reasons why SDN needs to be integrated with IoT

A) Traditional routers and switches have both control (makes decision related to traffic management) and data plane (actual mechanism for routing traffic to destinations) in one device. So, these devices become slow, expensive, inflexible and non-scalable. Operators employ external tools to dynamically reconfigure these network devices. This leads to miss-configuration errors. Software Defined Networking SDN was proposed to solve these problems faced by conventional network.[11]

B) The traditional switches and routers have inbuilt protocols that the device will be using. If there is a need to change the protocol then the switch/router is to be changed. Thus changing of the protocol is very hard and costly as all the hardware is needed to be replaced accordingly.

C) Each IoT object has been configured to accomplish specific objectives and protocols so fitting them with a common and singular protocol will not suit the object designers.

D) If a researcher wants to test his design or protocol, possibility of changes is very less, since the protocols and network design for are provided by the vendor, SDN can solve this problem wherein the various users of network can utilize their slice of network by allocation of resources and when the job gets over the resources can be de-allocated.

III. Proposed Integration of SDN and IOT

3.1 IOT Controller working summarized as below:

1) Receives communication request from requestor through IOT Module. (IoT Modules are installed in the objects and are registered in the IoT Controller and provides address, protocol and underlying network)[3]
2)Finds Responder (address) in network graph.
3)Calculates path using some routing algorithm.
4)Build forwarding rules, depending on the protocols used by the objects.
5)Communicate the rules to SDN Controller.

3.2 SDN working summarized as:

Key features: a) Separation of the control plane from the data plane
b)A centralized controller and centralised view of the network
c) Open interfaces between the devices in the control plane (controllers) and those in the data plane.
The SDN allows objects relying on different or heterogeneous protocols to communicate with each other.
1)SDN establishes a forwarding path that connects both the devices in communication.
2)SDN receives the forwarding rules and sets them into the forwarders.
3)Hence a path can be built and the devices may begin the conversation.

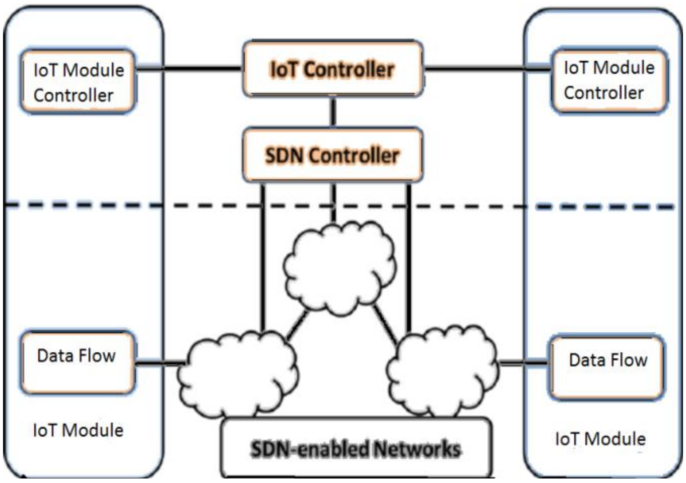

Figure 3.1: Proposed Integration of SDN and IoT

IV. SDN and security loopholes

Software defined networks provides a centralized view of the entire network, making it easier to centralize management by actively monitoring the traffic and diagnose threats in the network. However, the decoupling of control and data plane gives rise to a number of security challenges like DOS, Saturation attacks and other vulnerabilities.

The two properties of Software-defined networks that can be escape route for malicious users and a source of crucial security threat for less prepared network operators.

■ Software bugs could serve as a point of attack as software could control the network

■ The “network intelligence” is centralised in the controller, hence hacker with access to the servers that host the control software can potentially control the entire network.

There are number of security threats that can be scrutinised and their possible solutions found and categorised.

4.1 Analysis of Potential Attacks on SDN based on layered architecture.

Most SDN architecture models have three layers: a lower layer of SDN-capable network devices termed as data plane, middle layer of SDN controller(s) known as control plane and a higher layer that includes the applications and services that configure the SDN, termed as application layer. This section, describes the main security threats at each layer. The threats and corresponding countermeasures are divided into three categories based on which layer of the SDN architecture contains the corresponding attack target, i.e. the forwarding layer, the control layer and the application layer.

The fig 4.1 depicts the potential points of attack in the layered SDN architecture which would be the controller itself, the switch, the application, control and data plane along with the application-control interface and control-data interface.

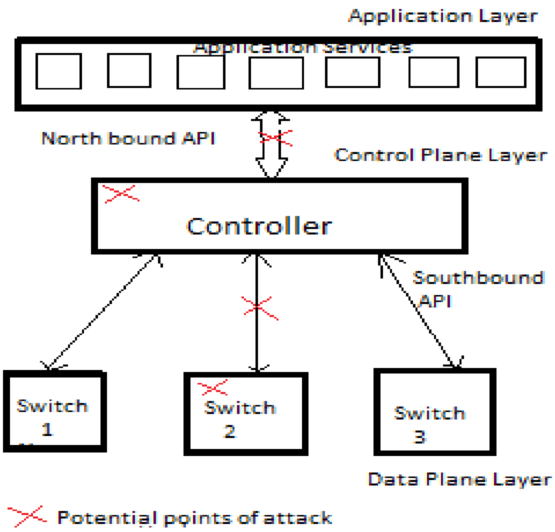

Fig 4.1 Different potential attack points in the layered SDN architecture

4.1.1 Potential Attacks on Data plane

The Data plane consists of only the forwarding devices such as routers, switches and access points which are programmed and controlled by the controller. An example of such devices is Open flow switches. The controller installs flow rules in the OpenFlow switch's flow tables.

Firstly, A switch however has a limited number of flow tables where flow rules are installed according to the controller's view of the network .Since,the switch is a dumb terminal with no decisionmaking capability,the most crucial security challenge will be to recognize if flow rules are genuine and differentiate them from malicious rules. The second challenge is Saturation attack which is caused due to the limited number of flow entries a switch can maintain. In OpenFlow, all the flow rules issued by the controller is buffered by the switch. Since buffering capacity is limited, the data plane can be proned to saturation attacks.

The third security challenge is caused due to dependency i.e. if a controller is compromised; the data plane nodes in the network will be comprised. Also if a switch does not receive forwarding instructions from the control plane, because of control plane failure ,the data plane will cease from working. This would cause the switch-controller interface to be a potential point of attack through the man-in-the- middle attack and black-hole attacks. [18].

The fourth security challenge would be of Denial of Service (DoS) attack, in which an attacker tries to attack the network devices from within the network itself. An attacker could then compromise a host that is already connected to the network and then to a flood attack on the network devices.

4.1.2 Potential Attacks on Control Plane

The SDN Controller is a central point of control and decision making. Hence, it can be highly targeted source of attack. The first security challenge is

1) Threat due to lack of scalability:

The controller needs to handle large number of flows , however if the SDN is not that scalable, then the control plane could be prone to saturation attack and DOS attack. There is a limit to the number of forwarding devices that can be managed by a single controller.There is a high probability of single point of failure if the number of flows on the controller increase,.[11].However, it is found that the multiple controller concept fails to prevent single point of failure [19].

2) Application Layer interface:

Applications implemented on top of the control plane can pose serious security threats to the control plane. The controller need to authenticate applications and authorize resources only after proper scrutiny. Every application has different operations to perform and hence have different requirements. This could be a source of attack and hence scrutiny is required before the applications could access the resource of the network..

3) Multiple Controller causing distributed Control Plane:

Multiple controllers have to be deployed to manage a huge number and variety of devices that cannot be managed by a single SDN controller,.SDN have widely utilized multiple controllers as shown in fig 4.2 where the load of a failed controller is redistributed to the other controllers. However, use of multiple controllers cannot protect SDN networks from a single point of failure ,since the load can exceed the capacity causing of cascading failures of controllers [19].

DoS and DDoS attacks are also a very crucial attacks in Control plane , which are discussed later in the paper.

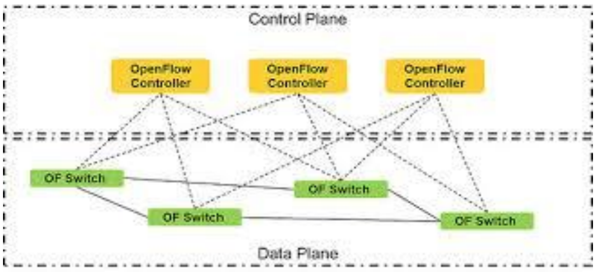

Fig 4.2 Control plane with multiple controllers.

4.1.3 Potential Attacks on Application Plane

SDN Application plane consists of programs that communicate with desired network requirements to the SDN Controller via APIs. Applications can cause crucial security challenges on network resources ,services and functions. However, there are no standard security applications, that are agreed upon to guide the security researchers.

The security threats in the application plane are:

1) Application, Authentication & Authorization:

Authenticating applications are the major issue in the SDN domains. Applications that run on the controller inherit the access rights to network resources, and network behavior manipulation mostly without proper security mechanisms for protecting network resources from malicious activities [30]. Hence, authentication of the applications running on centralized control architecture is a major security challenge. Secondly, if an application server that stores users details is compromised, credentials of legitimate users can be used to inject authorized, but, forged flows into the network. Thirdly, there are no mechanisms to certify SDN network applications .

2) Access Control and Accountability:

One of the key security issues to be handled are Access control and accountability mechanisms .Every application has different access needs like characteristics of the network eg traffic flows, header packet fields etc, hence immense care has to be taken while giving access control.

Secondly, applications which provide services for the network such as access control, firewall or intrusion detection services need to be scrutinized for vulnerabilities. Thirdly, instantiation can be another major threat , in which a malicious application can bypass access control by using an instance of the another class application. Fourthly, We also have some SDNaware applications which are capable of locating and directly communicating with the SDN controllers while the non SDN applications communicate indirectly with application datagrams in specific formats [31]. In the latter case, a legitimate, but compromised SDN application can become a gateway for unauthorized access to the control plane.

V Crucial attacks and their Countermeasures

5.1. Attack on Centralised Controller

The centralized controller serves as a "potential single point of attack and failure." and therefore the attacks and vulnerabilities in controllers are probably the most severe threats to SDN architecture..It is a central point of control that distributes security information consistently throughout the network.

If the controller is compromised, the whole network would collapse, hence termed as the single point of failure.

Counter Measures:

The single point of failure can be resolved by using Multiple controllers system as already discussed in section 4.1.2.

5.2. Saturation Attacks

This attack causes the attacker to flood the control plane with data packets by launching denial of service attack . This event is called the data-to-control plane saturation attack that floods SDN networks [22]. The attacker may generate a large number of fake packets, where each packet are spoofed with random value. These packets will trigger table-miss and send a lot of packet-in messages to controller. As a result, this attack could overload the buff er memory of network devices, generate amplified traffic to occupy the data-to-control plane bandwidth and shut the controller from responding.

Counter Measures:

This saturation attack is guarded by using an proposed framework called OF-GUARD[22] that prevents data-to-control plane saturation attack by using packet migration and data plane cache. This proposal causes the control plane and data plane to keep working even when suffering from the data-to control plane saturation attacks by using packet migration . Data plane cache distinguishes between fake and normal packets and also stores proactive flow rules and cache table miss. Avant-Guard[29] tries to resolve TCP based flooding attack .

5.3 DoS and DDoS Attacks:

A Denial-of-Service (DoS) and distributed DoS attacks are the most threatening security challenges for the SDN controller. DoS attack in SDN networks causes a networking resources such as a switch to unable to forward packets as expected. A successful attack involves sending a large number of packets to the switch, possibly instantiating new flows. A DoS attack as shown in fig. 5.1 .The attacker scans and collects network information, If the attacker understands that a target network is likely to use SDN, the attacker will further conduct the resource consumption attack [33] .A DoS attack on the SDN controller is shown in fig 5.4 where an attacker continuously sends packets with random headers so that the controller goes into a dormant state.

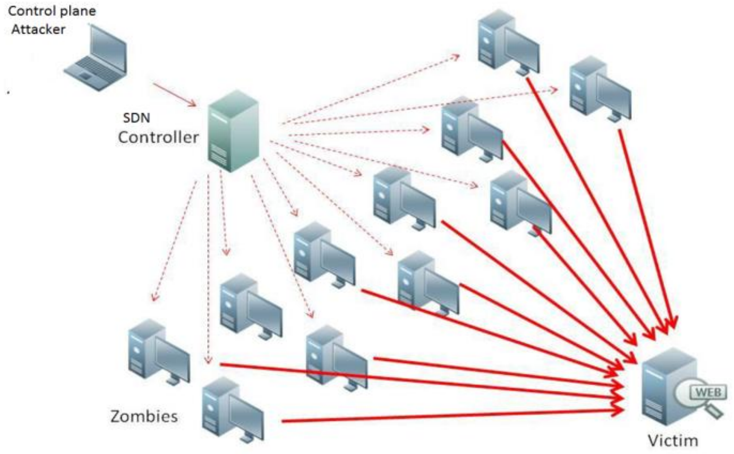

Fig 5.1 DoS and DDoSAttacks

Counter Measures:

DoS attacks can be simulated using an open source network emulator known as Mininet. A network of virtual hosts, controllers, switches and links is created using the tool to simulate the scenario [24].

A defense method against DDoS attack is proposed [30], which makes use of intrusion detection systems which recognizes abnormal traffic flows caused by DoS attack. FlowVisor[31] proposes an agent between switches and the controller; it accepts rules from controllers and rewrites them .This controller might then create a rule to drop all UDP traffic in response to a DoS attack .

5.4 Man-in –Middle Attacks

A man-in-the-middle attack is a crucial threat in SDN as it can effect both the control plane and data plane. This attack can be enforced between the controller and the switch, where the attacker inserts an agent device between the source and the destination node, and is used to intercept all the data, tamper and modify the data packets. These attack of man-in-the-middle attacks can be implemented by various methods like session hijacking, DNS spoofing, sync spoofing and other methods .A generalised view is depicted in fig.5.2.

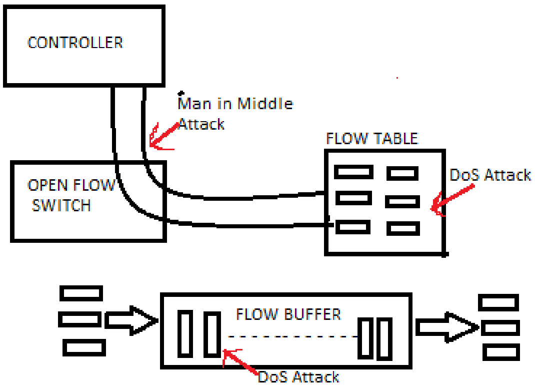

Fig 5.2 Implementation of Man in the Middle attack in SDN

Counter Measures:

To prevent the man-in-the-middle attack the approach is to create a secure channel between the controller and switches. Another alternative countermeasure is FlowChecker [21] which is a validation tool able to recognize internal configuration errors of switches. Misconfigurations can also be detected. FortNOX [27] can detect various forwarding rules collisions.

5.6 Black hole Attacks

A blackhole attack as depicted in fig. 5.3 is a network condition where the flow path ends abruptly and the traffic cannot be routed to the destination. A malicious switch in the flow path may drop or spoof packets, thereby preventing the flow from reaching the destination.

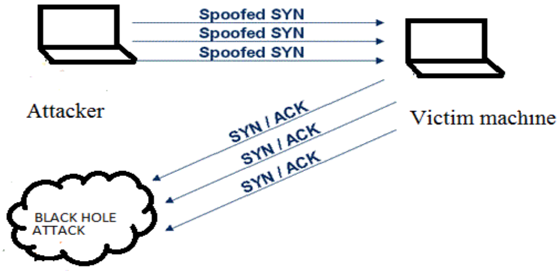

Fig 5.3 Implementation of Black Hole attack in SDN

Counter Measures:

SPHINX [18] detects the switch blackhole attack associated with switches by verifying the flow graph and captures the flow patterns of the actual network traffic along a path in the flow graph. It also monitors the byte statistics per flow at each switch in the flow path, and determines if the switches are reporting inconsistent values of bytes transmitted than expected. If the bytes reported across the switches fall below a threshold, SPHINX indicates an security threat

VII Conclusion

The flexibility offered by SDN can be effectively used to allow objects connected to heterogeneous networks to communicate to each other. This is independent of the capabilities of such objects, so it fits perfectly into IoT scenarios. Specific protocols serve specific purposes and hence does not permit the objects to easily interact. This problem can be resolved by using the mechanisms of integration of SDN with IoT objects. In this paper, we discussed the need for integration of both IoT and SDN. Then, we discussed the state of the art of SDN security and analyzed the security issues on basis of the 3 layers :the data forwarding layer, the control layer and the application layer. The countermeasures of the crucial security challenges were discussed. The future scope would be to work on security challenges pertaining to Denial of Service attacks on the control and data plane

References

[1]. John A Stankovic, Life fellow ”Research Directions for the internet of Things” IEEE 2014 internet of things journal, vol. 1, no. 1, February 2014.

[2]. Charles Gomez and Joseph Paradells, Technical University of Catalonia “Wireless Home Automation Networks: A Survey of Architectures and Technologies” by, published in IEEE Communications Magazine, June 2010

[3]. Pedro Martinez-Julia and Antonio F. Skarmeta “Empowering the Internet of things with Software Defined Networking” [white paper] in June 2015.

[4]. Diego KreutzFernando , M. V. Ramos, Paulo Verissimo, University of Lisbon, Portugal “Towards secure and dependable software defined networks” published in IEEE journal , August 2013.

[5]. M.K Shin, K.H.Nam, and H. J.Kim “Software-defined networking (SDN): A reference architecture and open APIs” published at published by IEEE Journal at ICT Convergence(ICTC) international conference in October 2012.

[6]. Roberto Minerva, senior Manager in Telecom Italia Labs, and DomenicoRotondi, IEEE Affiliate, Senior Consultant in FINCONS Spain “Defining The Internet of Things: A Work In Progress” by published in IEEE Journal , November 2015.

[7]. AkramHakiri, AniruddhaGokhale and Pascal Berthou “Software Defined Networking: Challenges and research opportunities for future Internet” published in computer networks journal Volume 75, Part A, December 2014.

[8]. SakirSezer, Sandra Scott-Hayward, and PushpinderKaurChouhan, CSIT, Queen’s University Belfast “ Implementation Challenges for Software Defined Networks” published in IEEE communications journal in July 2013.

[9]. Vandana C.P “Security improvement in IoT based on Software Defined Networking(SDN)” in international journal of science, engineering and technology research (IJSETR),Volume 5, Issue 1, January2016.

[10]. Po-Wen Chi, Chein-Ting Kuo, He-Ming Ruan, Shih-jen Chen and ChiN-Laung Lei, “An AMI Threat Detection Mechanism Based on SDN Networks” in Eight international conference on emerging security information, system and technologies, Taiwan .

[11]. YogitaHande and AishwaryaJadhav “Software defined networking with Intrusion Detection System” in International Journal of Engineering and technical Research (IJETR) Volume 2, issue-10, October 2014

[12]. Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara andSubhas Chandra Mukhopadhyay. “Towards the Implementation of IoT for Environmental Condition Monitoring in Homes” published in IEEE Sensors Journal, Vol.13,No.10, October 2013.

[13]. Ijaz Ahmad, SunethNamal, Mika Ylianttila, Senior member IEEE and Andrei Gurtov “Security in Software Defined Networks:Asurvey”IEEE communication survey and tutorials, Vol 17,No.4. Fourth quarter 2015.

[14]. Rajeev Piyare, Department of InformationElectronics Engineering“Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone”, Mokpo National University, published in International Journal of Internet of Things 2013.

[15]. Stephan Haller SAP Research Center Zurich Technical Report “The Things in the Internet of Things” presented as poster at the conference on internet of things conference in December 2010**.**

[16]. 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.

[17]. Sheungwon Shin, Guofei GU SUCESS Lab, Texas A&M University “Attacking Software Defined Networks: A Feasibility Study” in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013.

[18]. Mohan Dhawan, Rishabh Poddar,KshiteejMahajan, and Vijay Mann.“SPHINX: Detecting Security Attacks in Software-Defined Networks.” In Proceedings of the 22th Annual Network and Distributed System Security Symposium (NDSS’15), February 2015.

[19]. G.Yao, J.Bi,andL.Guo,“Onthecascading failures ofmulti-controllers in software defined networks,” in Proc. 21st IEEE ICNP, Oct. 2013,

[20]. P. Fonseca, R. Bennesby, E. Mota, and A. Passito, “A replication component for resilient OpenFlow-based networking,” inProc.IEEENOMS, Apr. 2012, pp. 933–939

[21]. E. Al-Shaer and S. Al-Haj, “FlowChecker: Configuration analysis and verification of federated openflow infrastructures,” in Proc. 3rd ACM Workshop SafeConfig, 2010.

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

[23]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow: Enabling Innovation in Campus Networks,” SIGCOMM Computer Communication. Rev., April 2008.

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

[25]. DierksT(2008) “The transport layersecurity(TLS) “ protocol version1.2[Online]. Available: https://tools.ietf.org/htmlrfc5246

[26]. K. Benton, L. J. Camp, and C. Small, “OpenFlow vulnerability assessment,” in Proc. 2nd ACM SIGCOMM WorkshopHotSDN,2013.

[27]. Yao G, Bi J, Xiao P (2011)”Source address validationsolution with OpenFlow/NOXg architecture.” In: 19th IEEE International Conference on Network Protocols (ICNP).

[28]. H. Xie, T. Tsou, D. Lopez, H. Yin, and V. Gurbani, “Use cases for ALTO with software defined networks,” Working Draft, IETF Secretariat, Internet-Draft, 2012.

[29]. S. Shin, V. Yegneswaran, P. Porras, and G. Gu. Avant-guard: Scalable and vigilant switch flow management in software-defined networks in CCS 2013.

[30]. Braga R, Mota E, Passito A (2010) " LightweightDDoS flooding attack detection using NOX/OpenFlow. In: IEEE 35th Conference on Local Computer Networks (LCN)

[31]. Sherwood R, Gibb G, Yap K K, Appenzeller G, CasadoM, McKeown N, Parulkar G (2009) "Flowvisor: a network virtualization layer."OpenFlow Switch Consortium, Tech.

[32]. Nayak A K, Reimers A, Feamster N, Clark R (2009). Resonance: dynamic access control for enterprise networks. In: Proceedings of the 1st ACM Workshop on Research on EnterpriseNetworking.

[33]. S. Shin and G. Gu, "Attacking software-defined networks: a first feasibility study," in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Software Defined Networking., 2013, pp. 165–166.

[34]. P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A replication componentforresilient OpenFlow-based networking," inProc.IEEENOMS, Apr. 2012, pp. 933–939.

[35]. http://cdn.ttgtmedia.com/searchNetworking/.../SDN_Eguide.pdf

[36]. http://search**sdn**.techtarget.com/.../SDN-and-wireless-LAN-meet-for-unified-network-management

[37]. "SDN Security Attacks" http://www.networkworld.com/article/2840273/sdn/sdn-security-attack-vectors-and-sdn-hardening.html

[38]. "Advantage of SDN", http://www.ingrammicroadvisor.com/data-center/7-advantages-of-software-defined-networking