International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 476-482

A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)

Andry Putra Fajar[1] and Tito Waluyo Purboyo[2]

[1]College Student, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia.
[1]Orcid ID: 0000-0002-0741-6434
[2]Lecturer, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia.
[2]Orcid ID: 0000-0001-9817-3185

Abstract

Distributed Denial of Services (DDoS) attacks is one of well-known and dangerous threats to the current network which always exists and evolves in line with the development of the network itself. Current network development has entered the Software Defined Networking (SDN) era which offers centralized control and programmability network by decoupling the network control and data plane that bring on us a dynamic, cost-effective, manageable and agile platform. On the down-side, this centralized platform can bring new security challenges such as DDoS attacks on the central controller which could compromise the entire network. This paper presents security challenge on SDN and provides several approaches to mitigate the DDoS attack from various source.

Keywords: Mitigation, Distributed Denial of Services, Software Defined Network

INTRODUCTION

Currently, SDN research is growing fast significantly, and many companies plan to use it for future network. SDN architecture can strengthen the network security with its basic functions such as centralized network monitoring and provisioning and centralization of security and policy control [1] which is not exist in the current network. These features make SDN become one of a most impactful platform for network security innovations [2].

The development of the network must be followed by the development of network attacks, there is no truly safe network from attacks even for future networks such as SDN. Therefore, the development of network security should be one step ahead of the development of attacks. Although the features of SDN offers a great impact on security, it is exposed new threats that are central controller attack which might impact to all of the system availability. Availability is related to the accessibility of information when needed. Unavailability of system or information can make an organization/corporation lost their business revenue and user's satisfaction. Availability is one of CIA (Confidentiality, Integrity, and Availability) Triad pillar [3] which is the model to guide policies for network security. While confidentiality refers to privacy, integrity is equivalent to the trustworthiness of data. These two aspects are very common safety aspect for security, meanwhile, availability is not priority one.

Make an online service/server become unavailable by sending an overwhelming number and size of fake packets from multiple sources is characteristic of DDoS attacks. This kind of attacks is easy to deploy but hard to deny and very effective to exhaust the network. This paper aim is to survey the literature about security in SDN especially to mitigate the DDoS attacks.

Feature of Software Defined Networks

This section will be discussed the advantages of SDN feature that can strengthen the network security.

A. Dynamic Flow Control

Decoupling the network control and data plane enables us to design and perform network flow control algorithm easily, so we could control networks flows more efficient and effective. With this feature, we can separate malicious network flows from benign ones dynamically without installing an independent middlebox (e.g., firewall) like on the current network. As an example, FlowNAC [4] which is based on an extension of the IEEE 802.1X standard (EAPoL-in-EAPoL). This Flow-Based Network Access Control evaluate and categorize the incoming frames from the user.

B. Centralized Controller and global view of the network

These features enable us to receive all of network status information for the purpose of monitoring and provisioning network form any threats (network-wide monitoring) [5]. CloudWatcher [6] is one of the frameworks that utilize this feature for security monitoring on the cloud on SDN environment.

C. Programmable Network

SDN provides control plane programmability through application programming interfaces (APIs) [7]. With this feature, a network administrator could make a simple program or algorithm for security application easily. There is several APIs to empower this feature (OpenFlow [8], OF-Config [9], OVSDB [10], NETCONF [11]). FRESCO [12] is one example that used its own scripting language for security application on SDN.

D. Simplified Data Plane

This concept simplified the control plane modules that can drive suitable for security usage modified data plane. Data plane extension that consist connection migration and actuating triggers were introduced by AVANT-GUARD [13] for scalable and robust SDN security services.

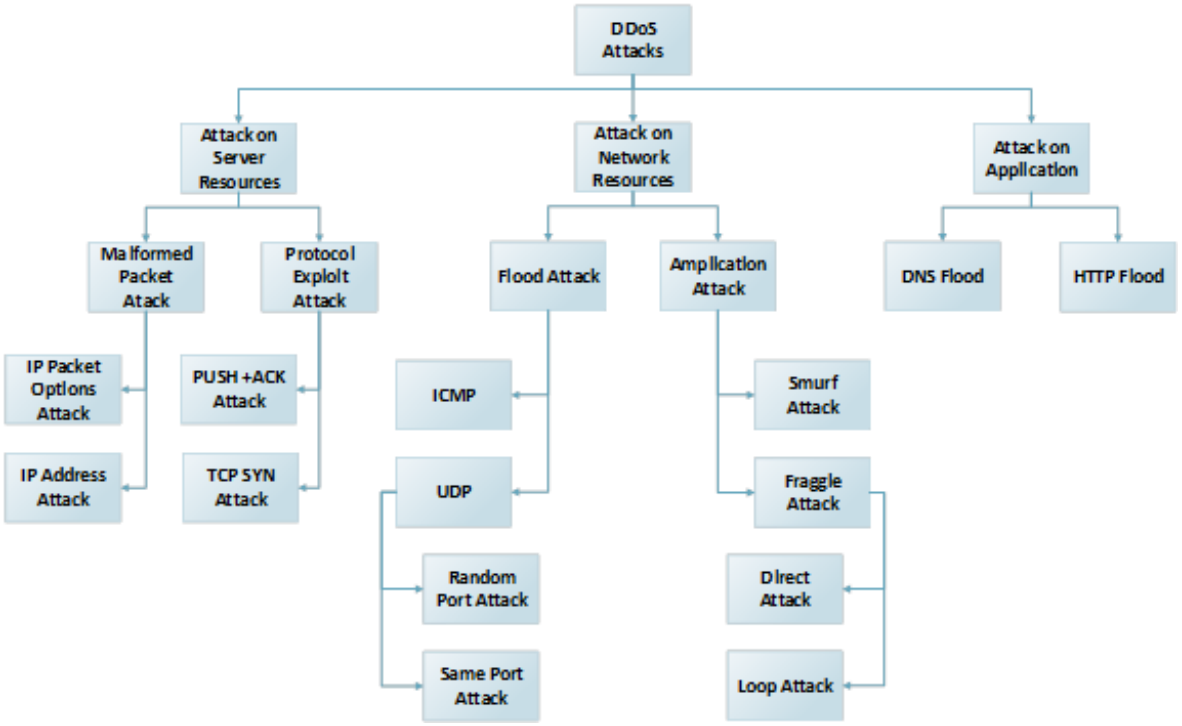

Figure 1: Taxonomy of DDoS Attacks [34]

DDoS Attacks Overview

As discussed above, make an online service/server become unavailable by sending an overwhelming number and size of fake packets from multiple sources is one of characteristic of DDoS attacks [14]. Early DoS attack aimed at the single victim with only one source attacker. Over time, it evolved to single or multiple victims against single or multiple sources (distributed) [15]. Even now the DDoS attack is easy to execute even can be launched with a limited resource against a large network which called "asymmetric attack". The taxonomy of DDoS attack can be seen in Figure 1.

What makes DDoS attacks possible?

Security is not the main focus in the design and development of the internet/network today. Most current research focuses on the way to sending data from source to destination effectively even though the protocol lack of security built to separate the malicious intent. For example, TCP protocol will not step in and stop the source to send a malicious intent that can harm the destination host hence the police traffic does not exist for this protocol [16]. This security gaps can be exploited for DDoS attacks.

The possibility of users that can be exploited due the vulnerabilities is tremendous hence there are almost 4 billion internet users per June 2017 [17]. How matter how secure the victim network, it might be attacked by DDoS if there is other user/host on world-wide can be used to launch this attack seeing that in many cases this attack launched from external victim's network and also not from the attacker's own system.

All of networks infrastructure even the biggest one has limited resources. Bandwidth, storage capacity, and processing power are natural targets for DDoS attacks. This attack aims to disrupt the victim networks through deplete victim's available resources. In a wider scope, DDoS Attacks commonly target the network, server and application resource.

A. DDoS Attacks on Network Resources

This DDoS attack aims to deplete the victim's network resource such as network bandwidth by flooding it using User Datagram Protocol (UDP) Flood or Internet Control Message Protocol (ICMP) Flood until the victim can no longer receive the legitimate traffic (see Fig. 2).

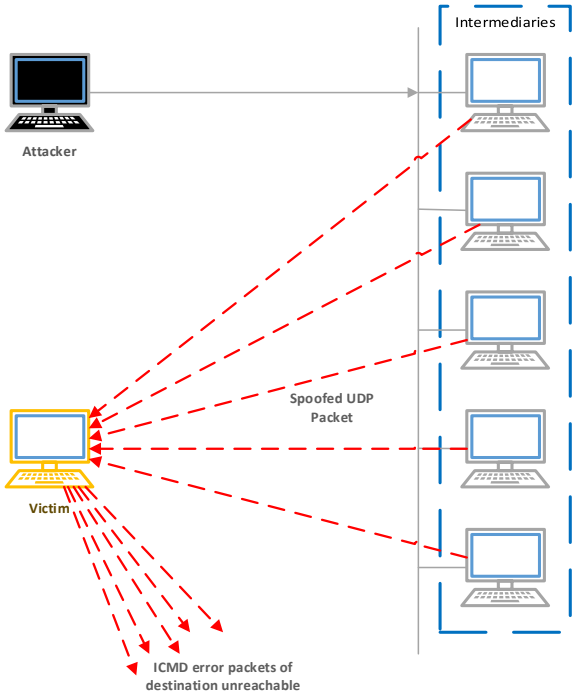

Figure 2: UDP Flood Attack

While UDP Flood [18] attack is an attack that used a huge number of UDP packets (random or same port) to overwhelming the victim (Figure 2), ICMP Flood uses the ICMP [19] (Ping) echo request packets for disrupt the legitimate traffic reach the victim (see Figure 3).

Amplifying the volume of attack traffic is characteristic of Amplification DDoS Attack. The attacker used other "trigger" machines to maximize the volume of attack traffic with only minimum traffic that sent to the triggered machine. This method can be seen in Figure 4. Attack traffic volume from UDP based attack can be amplified, this attack is known as Smurf attacks (see Figure 5) and Fraggle attacks [20].

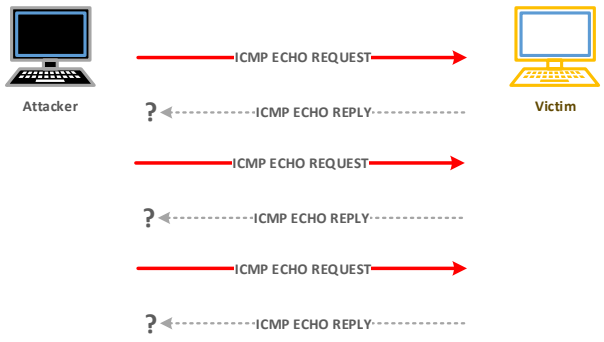

Figure 3: ICMP Flood Attack [19]

B. Every server has limited resource, both the processing capabilities and memory. This limited resource can be exploited by the DDoS attack to bring down the server. There are two types of this attack, protocol exploits attack which depletes the server resource from exploiting the specific feature of the protocol and malformed packet attack which is sending forged packets that will overload the victim with no use packet but must be processed consuming the resources. One of the common attacks that exploit the protocol is TCP SYN attack (Figure 7).

C. Vulnerable on application protocol like HTTP, HTTPS, DNS, SMTP, FTP and other application protocol can be exploited with malicious intent like a DDoS attack.

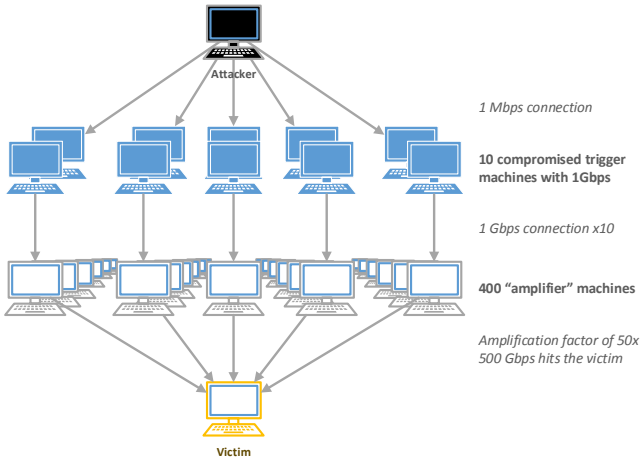

Figure 4: Amplification Attack

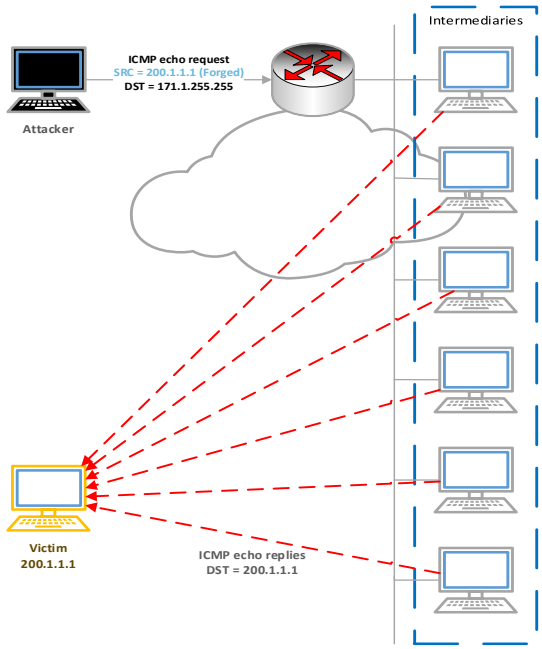

Figure 5: Smurf Attack [21]

DDoS Attacks Vector on SDN

In this section, we describe the attacks vector faced specifically by SDN architecture. SDN has a significantly different packet processing procedure compared with the current network that delivered more diverse and flexible attack [22].

DDoS attacks on SDN Controller

When compared with a computer, the SDN controller's role is a central processing unit that organizes the other component and executes the given input command, therefore, the SDN controller is the brain of the entire network that might become a single point failure that disrupts entire network if attacked by DDoS attacks [23]. This controller has three main potential threats.

The first threat attacks on control plane communications which exploit from lack of trust guarantees [24] between controller and switches. An attacker can generate DDoS attacks if the control plane was compromised.

The second threat is attacks on and vulnerabilities in controllers. Basic nature SDN that is easy to program can be both advantages and disadvantages. When an attacker can embed the malicious program to SDN controller it could potentially harm the entire network since the controller can do anything to its own network. Another type of attacks on the controller is TCP Flood attack which is sending an overwhelming number and size of malicious packets to the controller which makes the controller busy even crash. UDP flood attack also has the same effect with TCP flood that can make controller busy and malfunction.

The third threat is lack of mechanisms to guarantee the applications of the controller. This threat is similar to the first threat whereas this threat concerned the trust between applications on the controller.

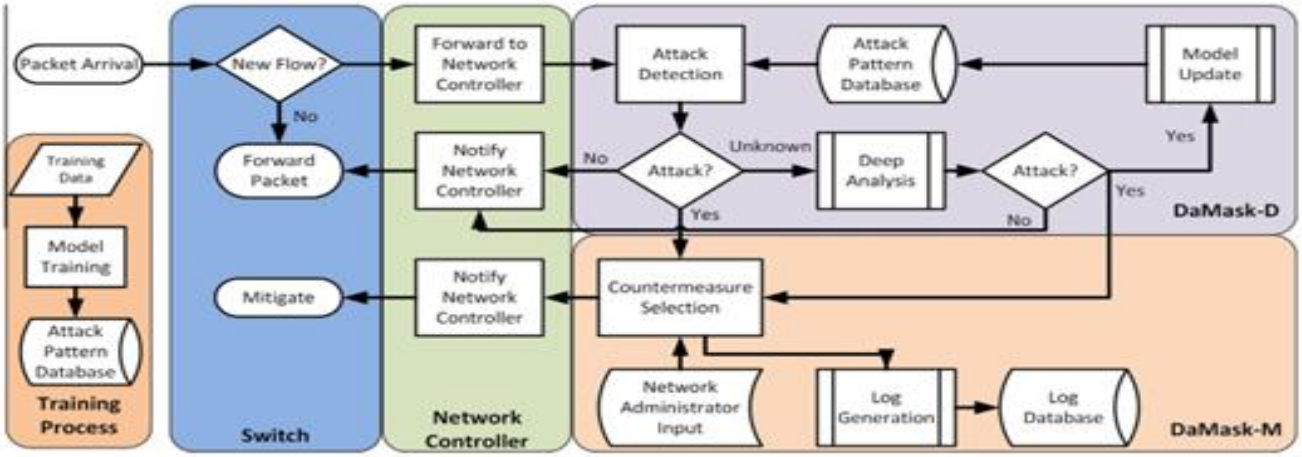

Figure 6: Workflow of DaMask [25]

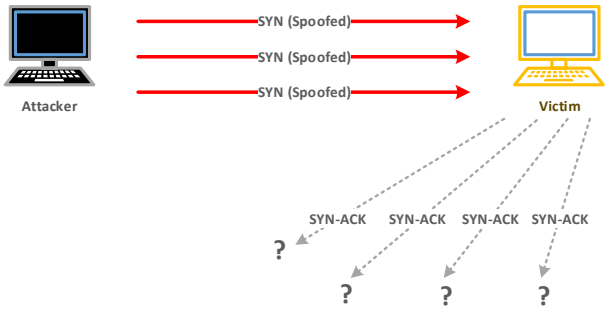

Figure 7: TCP SYN Attack

Types of DDOS Attack Mitigation

Commonly disconnect/block victim network/server from the internet or main-server is the only way to do for mitigation DDoS attack. Blocking the source is the hardest way since the attacker launch the attack from a huge amount of distributed intermediaries host (bots) through a DDoS attack, so defending against it is a challenging issue. This section, we describe various existing methods for DDoS attack detection and mitigation. The summarize of this section can be seen in Table 1.

DaMask [25] present two module: DaMask-D is detection module used anomaly-based and DaMask-M which is the mitigation module that has countermeasure selection and log generation (see Figure 6). The detection module of DaMask-D used the probabilistic interference graphical model that can address the dataset shift problem. DaMask-M matches the suitable countermeasure for different attack and registers a new countermeasure policy for the new type of attack (not recorded on log database) on the network controller when DaMask-M receives an alert from DaMask-D. A similar approach has been proposed by T Chin et al. [26] for against SYN flood attack using collaborative of *Monitors* and *Correlators*. The *Monitors* has the same role with DaMask-D whereas DaMask-M same with the *Correlators.*

Virtual source Address Validation Edge (VAVE) [27] provide an improvement of Source Address Validation Improvements (SAVI) to against the IP Spoofing which commonly used for DDoS attack. VAVE use the nature of SDN which can analyze all traffic on the network and dynamically update the policy for against IP Spoofing. Similarly, SDN-Guard present a scheme for rerouting, timeout management, and monitoring potential malicious intent.

CPRecovery [28] present primary-backup replication method for the SDN controller (especially network operating system) that can be used for smooth transition from failed primary controller to last valid state secondary (backup) controller (replication phase) and vice versa (recovery phase). This transition is flagged by inactivity probe via State Update Messages which are exchanged on both controllers (See Figure 8). This method prevents fail state controller on SDN if get attacked by the DDoS attack.

FlowTrApp [29] proposed traffic flow analytic (either legitimate traffic or attack traffic) algorithm that can block attack flow based flow rate and flow duration of a flow. An attacker will not be blocked when doing the first attempt, mitigation is done when attacker send malicious traffic frequently which is not match with any legitimate traffic pattern.

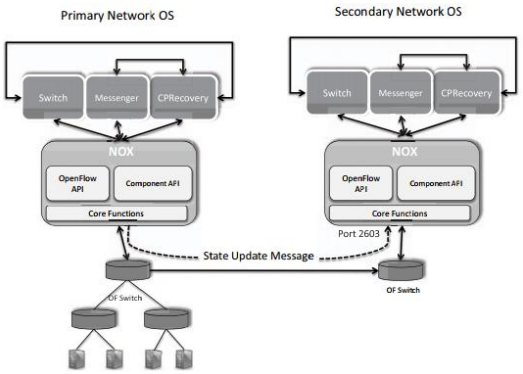

Figure 8: Communication between Primary and Secondary controllers, through CPRecovery component [28]

Hu et al. [30] introduced a Distributed Intrusion Detection System (IDS). This IDS method uses Event Processing Engine to detect the network attack. This engine consists of sub-controller, event bus, event channel, and hyper-controlled. The task of hyper-controller is coordinate the sub-controller and

Table 1: Types of DDOS Attack Mitigation

Research Work	Problem/Goal	Proposed Solution
FlowNAC [4]	Protect the network from unwanted user that can drive to DDoS attack	User's flow-based authentication mechanism
CloudWatcher [6]	Protect against malicious intent on cloud network using OpenFlow	Defense mechanism that contains monitoring and routing rule generator
FRESCO [12]	Facilitate security application development for SDN	Programming framework for enhancing security of SDN
AVANT-GUARD [13]	Protect control plane from saturation attack.	Data plane extension that consists connection migration and actuating triggers
DaMask [25]	Protect Cloud Computing based SDN from DDoS attack.	Two module defense mechanism composed detection module (DaMask-D) and mitigation module (DaMask-M)
T Chin et al. [26]	Protect SDN controller from TCP SYN Flood attack	Defense mechanism with collaborative of *Monitors* (detection) and *Correlators* (Mitigation).
VAVE [27]	Source address validation (IP Spoofing)	Validation mechanism using NOX controller
CPRecovery [28]	Protect SDN controller from failure through DDoS attack	Primary-backup replication method for smooth transition between primary and secondary controller while primary controller was compromised by DDoS attack
FlowTrApp [29]	Detecting and mitigating both high and low rate DDoS on data center based SDN	A defense architecture (FlowTrApp) based on flow traffic
Hu et al. [30]	Protect a large number of traffic flows and flow entries	Event-based IDS
Skowyra [31]	Protect embedded mobile device using OpenFlow	Learning Intrusion Detection System (L-IDS) for detect and respond relies on a mathematical or profile-based model
Belyaev et al. [32]	Extending the server survival time during the DDoS attack	Load balancing based on Bellman-Ford algorithm is used to define the shortest paths routes to the endpoint servers to spread the attack traffic.
SHDA [33]	Protect against Slow HTTP DDoS attack	defense mechanism on application layer that can detect and mitigate Slow HTTP DDoS attack relies on incomplete HTTP request analysis

detect any malicious traffic flow that sent via event bus and buffered from event channel. A Learning-IDS based on nature of SDN (programmable) was proposed by Skowyra [31], which have the flexibility to change the network state to response the malicious intent.

Belyaev et al. [32] introduce new load balancing method for extending the server survival time due to the DDoS attack. When an attack occurs on the server, the load balancing algorithm starts to override the routing table. Bellman-Ford algorithm is used to define the shortest paths routes to the endpoint servers to spread the attack traffic.

SHDA [33] proposed a defense mechanism on application layer that can detect and mitigate Slow HTTP DDoS attack which has similar traffic pattern with a legitimate user. The attack determined if incomplete HTTP request received when web server open connections threshold number exceeded.

CONCLUSION AND FUTURE WORK

The summarize of this paper explained in figure 9. SDN architecture can strengthen the network security with its natural functions such as centralized network monitoring and provisioning and centralization of security and policy control that can drive our network to the next level of dynamic, cost-effective, manageable and agile network platform. These functions delivered from control plane on SDN which is does not exist in the current network. However, the evolution of the network in line with its threats as well. SDN bring new security challenges, "how to secure the control plane from any threats?", since this is the most vital part of the SDN that can mess entire network if get compromised.

One of a reputable threat to the network is DDoS attacks. The generic characteristic of this attack drains the resources (bandwidth, memory, and others) of network, server or

application since the resources are limited. Every network even new platform like SDN avoid from this threat. Moreover, if the controller of SDN gets compromised from this attack, the impact of damage will greater than the current network which is breakdown the entire network. The previous section explained DDoS attack vector on SDN specifically for the controller. Then several approaches of defense mechanism described from the research community. They have own mechanism and relatively different each other, however their mechanism far from perfect against DDoS attack and still many innovation opportunities to patch up the SDN security by utilizing the advantages of SDN platform.

SDN with its features bring us to the next level of networking especially for IoT and Mesh Network and become one of a most impactful platform for network security innovations. However, its much work to do to make SDN become more secure than current network. We believe that marriage of proven security mechanism in current network and the capability of SDN drive to reliable and robust future network on the security aspect and another aspect.

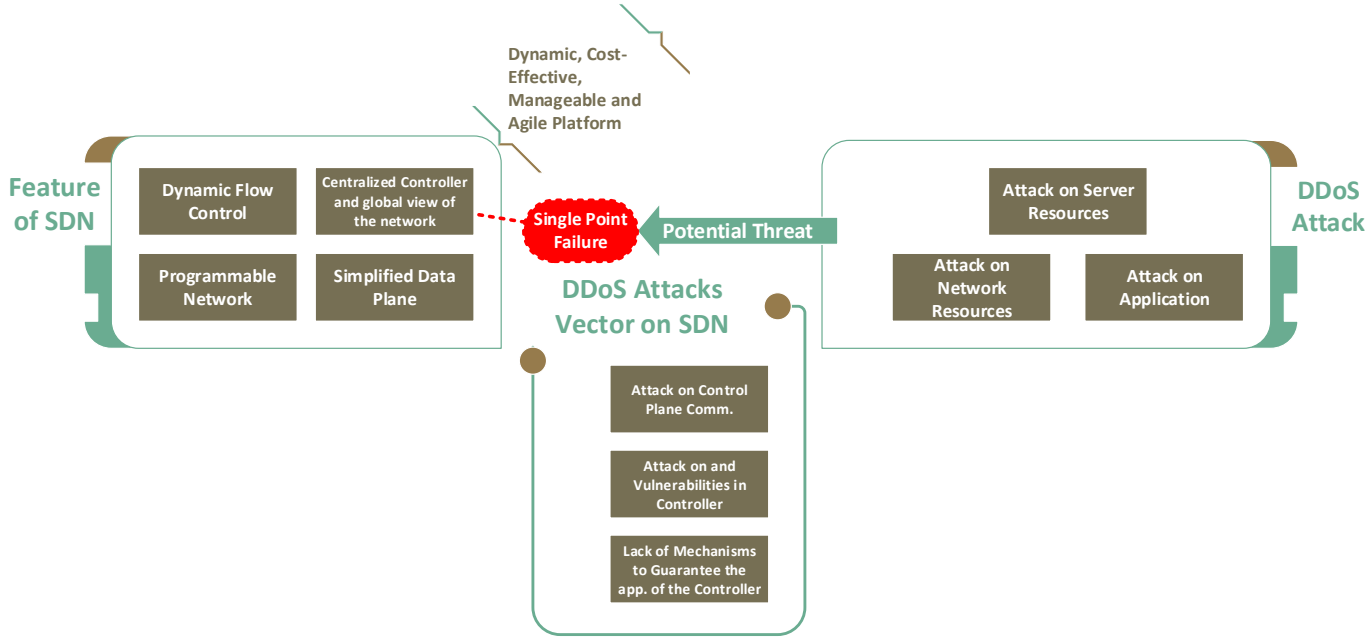

Figure 9: Summarize of A Survey Paper on Mitigation of Distributed Denial of Service on Software Defined Network

REFERENCES

[1] N. McKeown and T. Anderson, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, 2008.

[2] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A Survey of Security in Software Defined Networks," *IEEE COMMUNICATION SURVEYS & TUTORIALS*, vol. 18, 2016.

[3] S. Qadir and Quadri, "Information Availability: An Insight into the Most Important Attribute of Information Security," *Journal of Information Security*, vol. 07, no. 03, 2016.

[4] J. Matias, J. Garay, and A. Mendiola, "FlowNAC: Flow-based Network Access Control," *Third European Workshop on Software-Defined Networks*, 2014.

[5] S. Sezer, S. Scott-Hayward, and P. K. Chouhan, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Communications Magazine*, 2013.

[6] S. Shin and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," *Proceedings of the 7th Workshop on Secure Network Protocols (NPSec12), co-located with IEEE ICNP12*, 2013.

[7] V. Gupta, K. Kaur, and S. Kaur, "Network Programmability using Software," *3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2013.

[8] Open Networking Foundation, "Software-Defined Networking:" *ONF White Paper*, 2012.

[9] Open Networking Foundation, "OF-CONFIG 1.2 : OpenFlow Management and Configuration," *ONF TS-016*, 2014.

[10] VMware, "The Open vSwitch Database Management Protocol," *RFC 7047*, 2013.

[11] R. E. Ed, "Network Configuration Protocol (NETCONF)," *RFC 6241*, 2011.

[12] S. Shin, P. Porras, and V. Yegneswaran, "FRESCO: Modular Composable Security Services," *ISOC Network and Distributed System Security Symposium*, 2013.

[13] S. Shin, V. Yegneswaran, and P. Porras, "AVANT-GUARD: Scalable and Vigilant Switch Flow," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013.

[14] M. McDowell, "Understanding Denial-of-Service Attacks," 06 February 2013. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015.

[15] CERT/CC, "Trends in Denial of Service," October 2001. [Online].Available:https://resources.sei.cmu.edu/asset_files/WhitePaper/2001_019_001_52491.pdf.

[16] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*," 2004. [Online]. Available:https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf.

[17] "Internet World Stats : Usage and Population Statistics," [Online].Available:http://www.internetworldstats.com/stats.htm.

[18] S. S. Kolahi, K. Treseangrat and B. Sarrafpour, "Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13," in *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, 2015.

[19] Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," *International Journal of New Technology and Research (IJNTR)*, vol. 3, pp. 63-69, 2017.

[20] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," in *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, California, 2007.

[21] CERT/CC, "Smurf IP Denial-of-Service Attacks," 13 March 2000. [Online].

Available:https://www.cert.org/historical/advisories/CA-1998-01.cfm?.

[22] Q. Yan, Q. Gong and F.-a. Deng, "Detection of DDoS Attacks against wireless," *Ad Hoc & Sensor Wireless Networks*, 2016.

[23] D. Kreutz, F. M. V. Ramos, and P. E. Verıssimo, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, 2014.

[24] D. Kreutz, F. M. V. Ramos and P. Verissimo, "Towards Secure and Dependable Software-Defined," in *ACM SIGCOMM Conference*, Hong Kong, 2013.

[25] B. Wang, Y. Zheng and W. Lou, "DDoS attack protection in the era of cloud computing," *Computer Networks*, 2015.

[26] T. Chin, X. Mountrouidou and X. Li, "An SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment," in *IEEE Military Communications Conference*, Florida, 2015.

[27] G. Yao, J. B. Xiao, and P. Xiao, "Source Address Validation Solution with OpenFlow/NOX Architecture," *19th IEEE International Conference on Network Protocols*, 2011.

[28] P. Fonseca, R. Bennesby, E. Mota and A. Passito, "A Replication Component for Resilient OpenFlow-based Networking," in *IEEE Network Operations and Management Symposium*, 2012.

[29] C. Buragohain and N. Medhi, "FlowTrApp: An SDN Based Architecture for DDoS Attack Detection and Mitigation in Data Centers," in *3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2016.

[30] Y.-L. Hu and W.-B. Su, "Design of Event-Based Intrusion Detection System on OpenFlow Network," in *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2013.

[31] R. Skowyra, "Software-Defined IDS for Securing Embedded Mobile Devices," in *IEEE High-Performance Extreme Computing Conference (HPEC)*, 2013.

[32] M. Belyaev and S. Gaivoronski, "Towards Load Balancing in SDN-Networks During," in *International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC)*, Moscow, 2014.

[33] K. Hong and Y. Kim, "SDN-Assisted Slow HTTP DDoS Attack Defense Method," *IEEE Communications Letters*, vol. PP, no. 99, 2017.

[34] Stephen M. Specht, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," *Electrical Engineering Princeton University*.