Applying NFV/SDN in Mitigating DDoS Attacks

Luying Zhou and Huaqun Guo
Institute for Infocomm Research, A*STAR, Singapore
{lzhou, guohq}@i2r.a-star.edu.sg

Abstract– **Distributed Denial of Service (DDoS) is a widely employed attacking scheme over network that interrupts services by creating network congestion, draining server resources, or disabling normal functions of network components. An attacker launches the DDoS attack from a large number of compromised while geographically distributed devices by sending low rate seemly legitimate traffic that disturbs server's service, or high rate large volume traffic that overwhelms victim's processing capacity. DDoS attack mitigating approaches that apply pre-established defending strategy, functionality or capacity, and guard at fixed locations are costly and not effective either. Network Function Virtualization (NFV) supports the flexibility in on-demand function instantiation and allocation, and recently finds its applications in handling DDoS attacks. This paper proposes a NFV and Software-Defined Networking (SDN) enabled DDoS mitigation framework. In the framework, network traffic is monitored and analyzed utilizing the SDN features of central control and global network view, and the detection of anomaly traffic will trigger the actions of corresponding countermeasure computation, defending resources virtualization, instantiation, deployment and interconnection. The paper presents an application example of the proposed framework in protecting an industrial control system, and shows its effectiveness in mitigating DDoS attacks in the control system.**

Keywords—DDoS; Network Function Virtualization; Software-Defined Networking; Anomaly Detection; Attack Mitigation; Industry Control System

I. INTRODUCTION

Distributed denial of service (DDoS) attack is one of a variety of attacks launched over the networks. Different from the cyber attacks which target information confidentiality and integrity, or access authority to steal or manipulate information, DDoS attack targets specifically the service availability by exhausting target machine's resource to render its service unavailable to legitimate users. Many DDoS attacks have targeted government news media, financial online services, and company network systems, resulting severe damages politically, socially or economically, surveyed in, e.g., papers [1, 2] .

DDoS attack typically engages a number of computers or intelligent electronic devices in the attack that seriously blocks or suspends legitimate users' access to the network services. In a botnet DDoS attack, the victim is flooded with high volume of attack packets simultaneously from a large number of distributed and coordinated hosts (bots), leading to the exhaustion of server's processing resources, or saturation of server's connecting bandwidth. Besides the flooding attack, another type of DDoS attack is to exploit the design defects of the network or system, by sending malicious packets to disrupt the protocol or an application running on the victim, resulting in malfunction or shutdown of the service.

DDoS attack defense mechanisms that are fixed in the sense of functionality, processing capacity and deploying location, could not provide effective protections as they are not flexible to meet the changes in different attack types, scales or locations.

DDoS attack detection and prevention mechanisms that consider the functional flexibility by applying Network Function Virtualization (NFV) have been recently proposed [3-7]. NFV decouples the software implementation of network functions from the underlying hardware, and supports flexible network function instantiation and capability increment. The challenges of applying NFV to mitigate DDoS attacks are the needs of a distributed and coordinated approach, flexible resource allocation and deployment, cost-effective, and not resource over provisioning. There were also works in exploiting Software-Defined Networking (SDN) capabilities such as global network views, traffic analysis, and dynamic packet forwarding rule configuration, to address the DDoS attack challenges [8, 9].

This paper proposes a DDoS mitigation framework that employs both NFV and SDN technologies in detecting and blocking DDoS attacks, and applies the developed scheme to defend critical industry systems against DDoS attacks. To our best knowledge, our scheme is among the first that apply the NFV/SDN technology into the industry control systems against the DDoS attacks.

The rest of this paper is organized as follows: We present the DDoS attack classification and mitigation methods in Section II, where we group DDoS attacks based on packet communicating connection requirements, i.e., connectionless and connection oriented. Section III discusses the problems and challenges faced in developing an efficient DDoS attack mitigation solution. In Section IV, we propose a DDoS attack mitigation framework in which the functionalities of NFV, SDN and anomaly detection are employed and arranged in a control plane and data plane separated architecture. We present the application of the proposed framework in handling a DDoS attack in an industrial control system in Section V. Section VI concludes the paper.

II. DDOS ATTACK CLASSIFICATION AND MITIGATION METHODS

To launch a DDoS attack, the attackers usually establish a network of compromised devices, and the compromised devices (bots) are used to generate the huge volume of traffic needed to deny the victim's services to legitimate users. DDoS

attacks could be launched in various ways, in direct or indirect attack manners [2]. In a direct attack, a large number of attacking packets are sent from attacking devices to the victim directly, and the attacking packets may come from a group of devices which themselves were compromised by the attacker. The source IP addresses in the packets can be spoofed ones or real ones of the compromised devices, as the responses will not go to the actual attacker. In an indirect attack, intermediate nodes known as reflectors are used to generate the attack, in which these nodes reflect the attacking packets sent by the hidden attacker or compromised devices to the victim by sending response packets to spoofed source address (victim's IP address).

Existing works classify DDoS attacks into, e.g., two basic types of DDoS attacks, i.e., network/transport layer DDoS attacks and application layer DDoS attacks [1]. To understand better the characteristics of the DDoS attack traffic of its demands on link bandwidth, and its effects on consuming victims' computation and storage resources, we classify DDoS attacks into connectionless and connection oriented types. A connectionless attack is characterized as one way high volume traffic which floods the victim's resources, while a connection oriented attack is characterized as two-way low volume traffic which tactically deprives the victim's services to others. In the following, DDoS attack types and mitigation approaches are briefly described.

A. DDoS Attack Classification

1) *Connectionless Attacks*

The purpose of the connectionless DDoS attacks is to flood the network infrastructure consisting of routers, switches and servers by sending a large volume of attack traffic. These attacks can be launched through overwhelming bandwidth resources or exploiting protocol weaknesses, and the execution of the attacks does not solicit responses from the victims.

Protocol and configuration weakness attacks: Attackers exploit specific features of protocols or network configuration by sending large volume of unidirectional traffic to consume the victim's resources or depriving its services (e.g., TCP SYN flood [10], TCP SYN-ACK flood [11]).

Reflection-based attacks: Attackers send forged requests (e.g., DNS (Domain Name Service) or ICMP (Internet Control Message Protocol) requests) to intermediate hosts (reflectors) instead of victim, and the hosts reflect their replies to the victim so as to consume or occupy victim's resources (e.g., Smurf attack).

Jamming attacks: In the wireless network, attackers send continuous radio signals or random noise onto the wireless channel to disrupt the communication channel. In IEEE 802.11 based MAC protocols, attackers selectively send disrupting frames to collide with the RTS/CTS (Request to Send/Clear to Send) control frames or DATA frames to cause the channel bandwidth unavailable for legitimate users.

2) *Connection Oriented Attacks*

The traffic flows of the connection oriented attacks are bidirectional, happening over TCP connections, and the attacks aim to deprive victim's services (e.g., HTTP, DNS or SIP (Session Initiation Protocol) attacks). Such attacks generally consume less bandwidth and attacking traffic looks similar to normal benign one. The attacks typically operate at the application layer, and specially manipulate connection procedures of the HTTP protocol to exhaust the servers' resources. One such attack is to exploit protocol vulnerabilities to affect the listening daemon, and thus to saturate all the connections available on the listening demon on the victim host. For example, HTTP fragmentation attack is to make a server unavailable by maintaining HTTP connections for a long time. The attacker establishes a valid HTTP connection with a server, and then breaks HTTP packets into small packets (fragments) and sends the packets at a low rate as long as the server time out allows. When multiple such connections are maintained, any further request would not be satisfied due to occupied service connections in the daemon. Slowreq is another example of application layer DDoS attack that sends a large amount of slow requests to the server. In such attack, the buffer resources of the server are occupied while the server is waiting for the completion of the requests [1]. Other protocols, such as SMTP (Simple Mail Transfer Protocol), and FTP (File Transfer Protocol), are also prone to this type of DDoS attack.

B. DDoS Attack Detection and Mitigation Methods

As the DDoS attacks are launched over the network in a distributed manner, the attack could be detected at multiple locations, and countermeasures could be deployed in different places as well [1].

1) Detection based on Location

Source-end: Detect the DDoS attack at the source-end can facilitate the blocking of attack traffic from reaching its target, and thus effectively protect the network resources. The solutions include applying ingress routers to verify the packets from its administered network based on legitimate source IP addresses, and filtering out packets that have source IP addresses outside its subscribed range. However, the drawback of a source-end defense mechanism is the difficult to distinguish attack traffic from legitimate traffic due to low attack packet rate.

Victim-end: In contrast, a victim-end defense approach can easily detect connectionless DDoS attacks, as the attack traffic has already been built up, but cannot provide efficient protection. For the connection oriented low traffic rate attack, once detected, the end host machine would be able to handle the attack. The types of defense mechanisms used by the end host machine include, for example, firewalls and intrusion detection system (IDS), to filter out the attack packets.

Intermediate: One of the advantages of the intermediate defense mechanism is that the edge or core routers can filter out attack traffic before the attack traffic is transmitted to the target. This mechanism features the collaboration among the intermediate routers and information sharing among them. This mechanism has advantages of detecting and tracing back the attack traffic because of the collaborative operation.

2) DDoS attack mitigation methods

There are four main kinds of mitigation tools [1, 12]:

Source Identification: It provides an attacked end machine with information about the identity of the attacking sources. This information is useful for the countermeasure to block the attack traffic. Source identification mechanisms include a variety of traceback techniques to identify the attacking source.

Rate Limiting: It imposes a rate limit on the packets that have been identified as suspicious by the detection mechanism. It is usually applied when the detection cannot precisely identify the attack stream and try to avoid high false positive alarms, so this approach may not block all attack traffic.

Signature filtering: It relies on recognizing signatures generated for typical attack packets, and can be efficient to the known attacks and not effective to zero-day attacks. Packet filtering mechanisms filter out the attack packets based on the characterization provided by detection methods.

Moving target: It involves reallocating the victim and associating a new IP address in the event of attack. In this case, to continue the attack, the attacker has to find the target's new IP address, reorganize its attacking agents to launch the DDoS attack.

III. PROBLEM STATEMENT

To effectively mitigate the DDoS attack a coordinated multiple locations and elastic processing functionality approach is needed, as there are drawbacks of location based defense mechanisms in terms of attack traffic detection and blocking. The current DDoS attack mitigation mechanisms are implemented using specialized hardware equipment, and with pre-designed functionality and capacity of handling a specific type of DDoS attack. Such a defense mechanism is unable to meet the needs of handling different types of attacks, and aggregated large traffic volume which exceeds the processing capacity. An ideal defense mechanism will be capable of flexibly placing defense mechanisms on the locations where they are needed, and elastically mitigating different types or scales of the attacks.

Network Function Virtualization (NFV) was recently proposed to enhance the flexibility of network service provisioning and reduce the time to market of new services, by leveraging virtualization technologies [13–15]**.** NFV has the features as 1) *Decoupling software from hardware* - allows separate development and maintenance of software and hardware; 2) *Flexible network function deployment* –functions can be instantiated at NFV enabled device in the network and be connected in a flexible way; and 3) *Dynamic scaling* – functions can be flexibly instantiated to meet the needed processing capacity. The NFV technology enables the flexible and elastic resource allocation and deployment, and introduces new opportunities for effectively mitigating DDoS attack.

There are recent works in applying NFV technology in mitigating DDoS attacks. Dynamically deploying virtual functions at victim-end point, such as firewall or gateway, to filter, divert, or prioritize traffic are discussed in [3-5], and in [16], the virtual firewall functions are outsourced in the cloud. The application of NFV is further supported by SDN technology to connect the deployed virtual functions [6, 7].

Handling the connectionless type of DDoS attacks, the schemes such as using capacity or rate limitation, or source identification will be inefficient, since the attackers launch the attacks with single independent packet, not forming traffic flows. On the location of placing defense mechanism, mitigating the attack at victim's server may be too late as the attack traffic already built up, and system resource would be exhausted for sorting out the traffic. For such attack, managing to drop attack packets far uplink from the victim's server will be more effective. While handling connection based DDoS attacks, the source identification approach may be effective at the victim end, as the traffic volume may not be high.

An effective DDoS mitigation solution should be able to detect the attack via monitoring network traffic, collecting and analyzing state information to identity anomaly with a whole network view, and have the features of dynamically allocating, deploying and coordinating the required defending resources for different attack types and scales on the network on demand.

We propose and develop a solution that integrates NFV, SDN, traffic monitoring and other technologies, and seamlessly employs them for mitigating the DDoS attacks in a distributed and coordinated manner.

IV. DDOS ATTACK MITIGATION FRAMEWORK

In the NFV environment, SDN could simplify the implementation of the virtualized network functions via flexibly allocating pooled computing resources to accomplish intended operations. SDN technology decouples the network control plane from the data plane, and centrally programs the network routing rules through open interfaces [17]. The control plane consists of a centralized controller, which maintains a global network view, and controls the network devices via standard protocols. The data plane includes data forwarding equipment, e.g., physical or virtual switches and routers. SDN enables directly program and control network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner. Combined usage of SDN with NFV facilitates the elastic deployment and management of these virtualized resource allocations responding to dynamic situations and demands.

A. SDN Usage in NFV Architectural Framework

ETSI proposed a SDN usage in NFV architectural framework [18], shown in Fig. 1. This ETSI document describes the integration of SDN and NFV technologies and the framework of SDN usage in NFV architecture which shows where SDN controller could be placed in the NFV architecture. In NFV architecture framework, there are three main functional blocks: NFV orchestrator, VNF (Virtual Network Function) manager(s), and virtual infrastructure manager (VIM). The NFV orchestrator manages and coordinates the software resources and the virtualized hardware infrastructure to ensure an optimized allocation of the necessary resources and connectivity to provide the

requested virtual network functionality. The VNF managers are responsible for the instantiation, modification, and termination during the life cycle of a VNF. The VIM is responsible for virtualizing and managing the computing, storing, and networking resources in the NFV Infrastructure (NFVI), and controlling the interaction with VNFs. In this SDN usage in NFV architecture framework, SDN controller could be deployed in various locations merged with NFV functionalities: 1) SDN controller functionality is merged with the VIM functionality; 2) SDN controller itself is virtualised as a VNF; 3) SDN controller is located in NFVI as a classic case controller for the network connectivity; 4) SDN controller is part of the operation and business support system (OBSS); and 5) SDN controller is as a physical network function (PNF), but not studied in [18].

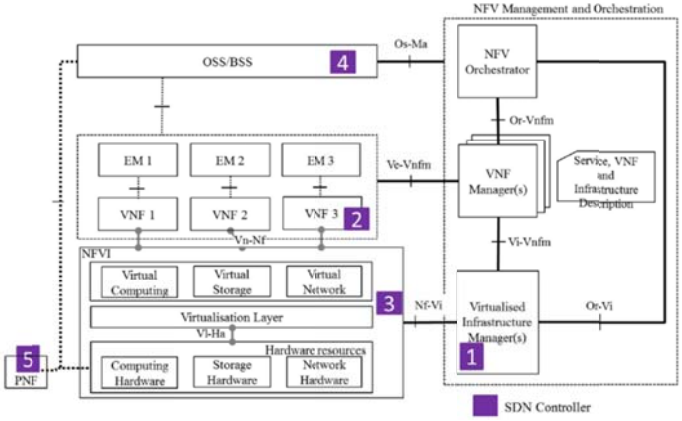

Fig. 1. Possible SDN Controller Locations in the NFV Architectural Framework [18]

B. NFV/SDN Enabled DDoS Attack Mitigation Framework

We study the application of NFV and SDN technologies in mitigating DDoS attacks, and develop a scheme that fully utilizes the flexibility and elasticity of virtual function instantiation, allocation, and deployment with NFV and SDN for the purpose of mitigating DDoS attacks.

The effective defense mechanisms against DDoS attacks, as described in earlier Section II, should be able to monitor network traffic in distributed locations, analyze the traffic in respect to specified behaviours, and react to anomaly in a dynamic and coordinated manner. SDN technology has the features of having a global view of the network, and a logically centralized control of the network, which could be fully employed, combined with NFV's flexible resource deployment features, in developing effective Dodos attack defence mechanisms.

We propose a NFV/SDN enabled DDos attack mitigation framework that adopts the similar SDN control plane and data plane separation approach, enables flexible resource allocation and deployment, and incorporates event monitoring and information collecting and data analysis capabilities to facilitate anomaly activity detection. The framework is illustrated in Fig. 2, composing Application Plane, Control Plane, Data Plane, and main interfaces between controller and applications, and between controller and the physical or virtual resources. This framework achieves the integration, coordination and interoperation among the NFV, SDN and DDos mitigation technologies.

The control plane unifies the functions of control, management, monitoring, and configuration of the network. The SDN controller is located with NFV management and orchestration functions in the control plane, where functions for network monitoring, operation state collection, anomaly detection, as well as function virtualization and management are deployed. With the SDN controller, the Anomaly Detection module consists of traffic monitoring, data collection and analysis functionalities, and is responsible for data collection and analysis, and triggering the appropriate DDoS attack mitigation mechanisms from the application plane. The NFV module, by given the requirements from specific applications, virtualizes, allocates, instantiates needed functions, and manages the virtual machines. This module consists of the NFV orchestrator, VNF manager and VIM functionalities, performing the functions specified in the ETSI NFV architecture framework document [18]. The SDN module includes the SDN controller, which implements and enables the allocated virtual or physical resources. The operations of these modules are interrelated, and a module gets input information supported by another.

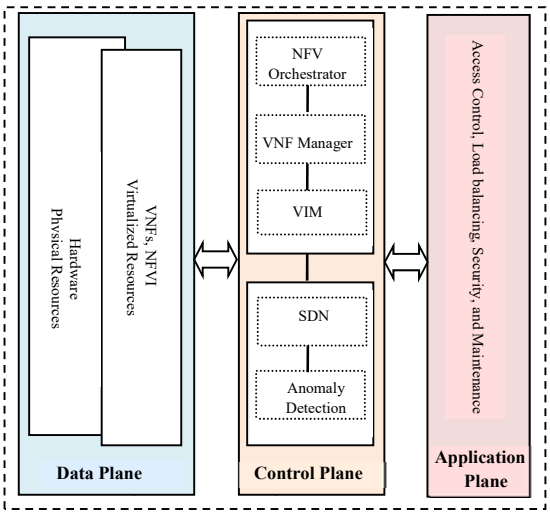

Fig. 2. NFV and SDN enabled DDoS attack mitigation framework

The design of the data plane architecture enables the integration of virtualized and physical network resources with backward compatibility. The physical hardware resources include network, computing and storage that provide connectivity, processing and storage to the VNFs through a virtualization layer, e.g., hypervisor. The virtualized functions will be appropriately instantiated, connected, and combined with un-virtualized functions over the network via the NFV and SDN modules in the control plane.

The application plane may include applications such as load balancing, access control, maintenance, network security and routing. The applications can programmatically implement strategies to control the physical networks.

With this framework, the control modules in the control plane will have the capability to monitor and analyze network events, virtualize and instantiate network functions, allocate and deploy the virtual or physical functions, and thus effectively conduct the DDoS mitigation schemes in a distributed and coordinated way.

V. Defending Critical Gateway against DDoS Attack

In this section, we describe how the NFV/SDN enabled DDoS attack mitigation framework is applied specifically in defending a critical gateway in an industrial control system against DDoS attack.

Nowadays the industrial control systems (ICS) are vulnerable to cyber attacks due to the openness and the increased connectivity as a result of adopting common operating systems and standard communication and application protocols for the efficiency and effectiveness of production and management [19, 20]. The system could be compromised by various attacks, including the DDoS attacks, since in the distributed control networks, e.g., transport system control or industrial Internet of things (IIoT) networks, devices (e.g., servers, controllers, sensors and actuators) could be infected with malwares and manipulated by attackers to launch DDoS attack.

In these industry circumstances, the industrial control systems are managed and controlled by a single organization, and hence the resources in the system can be fully mobilized by the central controller in handling the DDoS attacks, which are the features the designed NFV/SDN defense framework prefers in order to effectively carry out the distributed and coordinated DDoS attack defense schemes.

An industrial control system can comprise multiple interconnected networks, including central and local control networks, and control field networks, and could be further connected to external networks for convenient control and management. The DDoS attack could be launched by infected devices in those networks to disrupt or damage a certain critical system or controllers, for example, the gateway, as illustrated in Fig. 3. The attack aims to consume the gateway resource by flooding connectionless attack traffic to it and makes the communication channel between the controller and control devices unavailable. The attack traffic could initiate from local and central networks and reaches the targeted gateway through the router in this DDoS attack scenario.

Applying this NFV/SDN enabled DDoS attack mitigation framework, the defense against the attack can be conducted in a systematic way. The procedures of the DDoS attack mitigation are outlined as follows:

1) Increased traffic at the gateway is monitored and analyzed at the anomaly detection module in the control plane.
2) The analysis results are reported to the network security service in the application plane;
3) Appropriate attack countermeasures are decided, required resource calculated, and converted from application plane to the control plane;
4) NFV module virtualizes, allocates and instantiates VNFs to handle the attack traffic, e.g., deploying VNF in the router to block the attack traffic, divert it to other VNFs for further processing, or tracing the source of attack traffic; or deploying VNFs in the ingress routers to detect and block the attack traffic, or limit the traffic rate, and so on.
5) SDN module sets the routing paths to connect the VNFs.

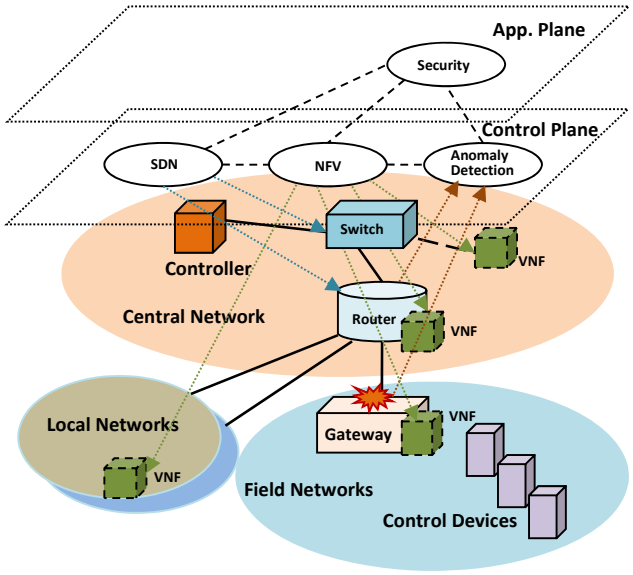

Fig.3. NFV/SDN enabled DDoS mitigation scheme for ICS against DDoS attacks scenario

The NFV module has the global view of the virtualised functions in the control network, and manages the dynamics on the network service topology. The topology dynamics information is communicated to the SDN controller through an interface between the NFV module and the SDN module for dynamically chaining various deployed processing functions. The SDN controller sends the data forwarding rules to the routing devices in the data plane, and the data packes are forwarded according to the rules received.

As the control network resources are all managed by one organization and accessible by the central controller, the required information collecting, resource allocating and deploying, and functions coordinating, are practically achievable.

The configuration of the processing resources, network resources in the data plane is conducted by the SDN controller, using the available software, e.g., Openflow.

VI. Conclusion

We presented the DDoS mitigation framework that employs the NFV/SDN technology and applied it to defend critical industry systems against the DDoS attack. Our framework consists of the application plan, the control plan and the data plan. In the control plane, the Anomaly Detection module is responsible for data collection and analysis, and triggering the appropriate DDoS attack mitigation mechanisms from the application plane. The NFV module virtualizes,

allocates, instantiates and manages the virtual machines for a specific DDoS attack mitigation requirement. The SDN module with the SDN controller implements and enables the allocated virtual or physical resources. We then applied our framework into the industrial control system to show its effectiveness against the DDoS attacks. The future work will be on implementing the framework and evaluating experimentally it over our developed testbed.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate. The special thanks are also given to SMRT Trains Ltd for providing domain knowledge and technical support.

REFERENCES

[1] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense MechanismsAgainst Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013.

[2] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015.

[3] C. J. Fung and B. McCormick. "Vguard: A distributed denial of service attack mitigation method using network function virtualization". In Network and Service Management (CNSM), 2015 11th International Conference on, pages 64–70. IEEE, 2015.

[4] H. M. Jakaria, W. Yang, B. Rashidi, C. Fung, and M. A. Rahman. "Vfence: A defense against distributed denial of service attacks using network function virtualization". In 11th IEEE International Workshop on Security, Trust, and Privacy for Software Applications (STPSA 2016). IEEE, 2016.

[5] B. Rashidi, and C. Fung, "CoFence: A collaborative DDoS defence using network function virtualization", International Conference on Network and Service Management (CNSM), 2016.

[6] K. Futamura, A. Karasaridis, E. Noel, P. Reeser, A. Sridharan, C. Johnson, and P. Velardo "vDNS closed-loop control: A framework for an elastic control plane service", IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), pages 170-176, 2015.

[7] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey. "Bohatei: Flexible and elastic ddos defense". In 24th USENIX Security Symposium (USENIX Security 15), pages 817–832, Washington, D.C., 2015. USENIX Association.

[8] Q. Yan, F. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER 2016, pp602-622

[9] Y. Xu and Y. Liu, "DDoS Attack Detection under SDN Context", IEEE INFOCOM 2016

[10] Incapsula. TCP SYN Flood. DDoS Attack Glossary. Retrieved on May 5, 2017 from https://www.incapsula.com/ddos/attack-glossary/syn-flood.html

[11] Corero. SYN-ACK Flood. Retrieved on May 5, 2017 from https://www.corero.com/resources/ddos-attack-types/syn-flood-ack.html

[12] J. Mirkovic, and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Volume 34 Issue 2, April 2004, Pages 39-53.

[13] ETSI GS NFV, "Network Functions Virtualisation (NFV): Architectural Framework," 2:V1.1.1, 2013.

[14] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER 2016.

[15] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Functions Virtualization: Challenges andOpportunities for Innovations", AT&T Labs Research, 2015.

[16] F. Guenane, M. Nogueira, and A. Serhrouchni. "Ddos mitigation cloudbased service". In Trustcom/BigDataSE/ISPA, 2015 IEEE, volume 1, pages 1363–1368, Aug 2015.

[17] W. Xia, Y. Wen, C. Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 1, 2015, pp27-51

[18] ETSI GS NFV-EVE "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework", 005 V1.1.1 (2015-12).

[19] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2, May 2015, http://nvlpubs.nist.gov/nistpubs /SpecialPublications/NIST.SP.800-82r2.pdf.

[20] L. Zhou, H. Guo, D. Li, J. Wong, and J. Zhou, "Mind the Gap: Security Analysis of Metro Platform Screen Door System", Singapore Cyber Security R&D Conference (SG-CRC), February, 2017. In Cryptology and Information Security Series Ebook, Vol 15: A Systems Approach to Cyber Security, pp. 70 – 85.