Against Distributed Denial of Service (DDoS) attacks using Software-Define Network (SDN): A Survey

Zhihao Cao
Department of Computer and Information Science
Purdue University - Indianapolis
Indianapolis, IN 46202, USA
Email: cao104@purdue.edu

***Abstract*—Software-Define Network (SDN) has emerged as a very promising network architecture in recent years. It largely simplifies the network logic and makes the network traffic more controllable by decoupling data plane and control plane out of the traditional network architecture, and having centralized controllers to control network switches. The significant difference from the traditional network architecture is that the network traffic routing is centralized into controllers such that network switches are only need to perform forwarding, instead of complicated routing protocols. The centralized controlling scheme of SDN has many novel and important capabilities such as global view of the network, software-based traffic analysis, and dynamic reconfiguring of network forwarding rules. The SDN has attracted the interests of many attackers due to the use of centralized controlling architecture and many security flaws are remained to be addressed yet. Distributed Denial of Service (DDoS) attack is one of the most frequent network attack that no effective countermeasure is acknowledged in traditional network. Fortunately, the characteristics of SDN bring us new chances to effectively against DDoS attacks. In this paper, we are going to discuss the classifications and characteristics of DDoS, analyze the advantaged capabilities of SDN architecture, and present a survey of the methods to detect and prevent DDoS attacks using SDN, and review the studies of SDN as a victim of DDoS attack.**

I. Introduction

Software-Define Network (SDN) is a new networking paradigm that is expected to replace the existing network architectures. By separating the control plane from data plane, this architecture has introduced a novel way to manage the network which allowing the network become more scalable and manageable. The centralized control architecture fundamentally changed the traditional distributed network management architecture. In SDN architecture, infrastructure layer devices become simpler and cheaper, due to the new architecture that these devices only need to support basic forwarding protocols, instead of complicated and distributed routing protocols [22].

The centralized controlling scheme of SDN has many novel and significant capabilities such as global view of the network, software-based traffic analysis, central controlling, and dynamic reconfiguring of network forwarding rules. With these capabilities, the SDN is believed to be reliability, effectiveness, simplicity, flexibility, and with lower cost [2].

Although more and more scholars and researchers are attracted to discover the potential capabilities of SDN, in the meanwhile, security vulnerabilities are also exposed. The separation of control plane from the data plane opens opportunities for security problems. Attackers can take advantages of the characteristics of SDN to launch attack focusing on control layer, infrastructure layer and application layer of SDN .

DDoS attacks are known to be the most harmful cyber-attacks. It attempt to disrupt the network services of intended users. The attackers initiate attack by sending flood requests from botnet which are great number of compromised devices that been injected malware code. Since availability is the most important requirement for an architecture of networking, to enable SDN replace the traditional network architecture, scholars and researchers must address the SDN security vulnerabilities to DDoS attacks.

The relationship between SDN and DDoS is contradictory. The capabilities of SDN can be employed to detect and react to DDoS Attacks. In contrary, the architecture of SDN exposes some security problems that are vulnerable to DDoS attacks. For the time being, the contradictory relationship between SDN and DDoS is still remained to be addressed. This survey is to help understand the capabilities and potential vulnerabilities of SDN, and how SDN can be the victim of DDoS attacks.

In this survey, we are going to review the characteristics of DDoS attacks in traditional network architecture. Next, we are going to analyze the advantaged capabilities of SDN architecture. And then provide a survey of detecting and reacting methods against DDoS attacks in SDN. In addition, we are going to review the studies of SDN as a victim of DDoS attack.

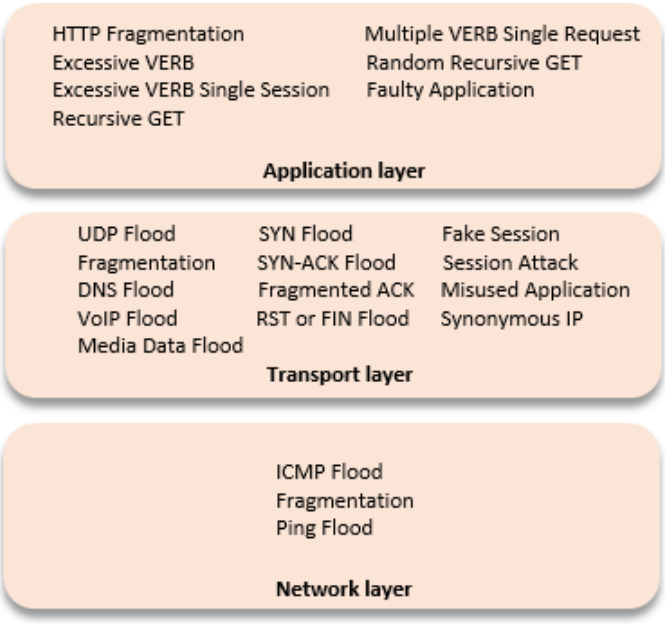

Fig. 1. Taxonomy of DDoS attacks.

II. DDoS

DDoS is a special kind of attack that easy to launch attack, but difficult to defense against. To launch an attack, attacker usually get the control on a network of computers, that we usually call it botnet. There are many break points can be utilized by attackers to launch DDoS attacks, especially the sophisticated network architecture we are applying in nowadays. Based on targeted protocol, DDoS attacks are categorized into two types in this paper:

1) Application level: By applying the DDoS flooding attacks on specific protocols which are vulnerable to DDoS attacks, the attackers are able to consume and even exhaust the target hosts resources, such as memory, and CPU. Such that make the service unavailable to intended users.

2) Transport/Network level: the attack can be launched by flooding the request of TCP, UDP, or DNS, etc. to exhaust the bandwidth of the target host. Such that the targeted hosts connectivity is severely disrupted.

The detailed summary of taxonomy of DDoS attacks is shown in Figure 1 [23].

According to the survey paper on defense methods against network/transport- level DDoS flooding attack, there are three categories are summarized [23]:

Source-based: The source-based methods are the most effective locations to defend against DDoS attacks, since by preventing the flooding packets enter into the network, the network resources (bandwidth, routers memory, routers CPU resources, etc.) can be saved. To prevent the DDoS attack from the very first place, source-based methods utilize ingress/egress filtering and Source Address Validity Enforcement protocol (SAVE) to detect the abnormal packets at the routers which near the compromised hosts. For ingress/egress filtering, it is the most widely applied method to filter the spoofed IP source address at the source ends edge routers. The filter is to limit the packets IP address range. Once an unexpected packet source IP address is detected, the router will drop the packet directly. For SAVE protocol, it can dynamically update the valid/expected source IP addresses and propagate them from the source location to all destinations routers. Such that the expected source IP addresses rule can be known promptly by wide area of routers once the new setting has been applied.

Network-based: The defending methods in this category are happened when the packet passes through the edge router of source and enters Autonomous Systems (AS) routers. In AS routers, there are two main types of DDoS detection methods: DDoS attack specific detection and anomaly based detection. [12] The DDoS attack specific detection is achieved by specifically detecting the features of target DDoS attack. For instance, in transport layer, SYN flood attack is one of the most frequent DDoS attacks. By the DDoS attack specific detection, the SYN cookie is used to against SYN flood attacks. Usually, SYN flood is achieved by a target host that keep receiving SYN requests with fake IP source addresses. Such that the target host keep sending back and waiting acknowledge from source host, and finally target host resources are exhausted by SYN requests. This will result in the degradation of target hosts performance and may even causing the server out of service. By using SYN cookie, the router can prevent such attacks happen during the initial TCP set up phase. When the SYN queues full, the SYN cookie can help the router to keep the SYN queues and keep active to receiving new TCP connection set up. Another type of DDoS detection method: Anomaly-based detection is achieved by setting up the relative behavior models and detect the anomaly by fitting the packets onto the behavior models. For instance, the threshold metric model will lock a user after several failed attempts. For Markov model, it detects the behavior of a packet based on the probability of states transition. If the sequence of states transition out of the probability, then the abnormal behavior is detected.

Destination-based: The defending methods in this category are to detect and react to abnormal packets when the packets arrive the destination. At this stage, the DDoS attacks almost achieve their goal, since they already consume the bandwidth of the link to victim host and the resources of the victim host. However, by applying some DDoS detection methods, effective DDoS attacks mitigation can still be achieved. There are three methods are summarized from [12] First, input debugging, it is a retracing method that can retrace back to the original attacks link from the targeted victims

near routers. The retracing is done by repeatedly testing the upstream links. When the attackers address is retrieved, filters will be applied to filter out the abnormal packets from this address. The second method is probabilistic packet marking. Under this method, the packets will be probabilistic marked (some id of routers) by the intermediate routers. Such that the destination router can collect the id information from marked routers and reconstruct the path from the source of the packets. Another method in destination-based category is Hash-based IP trace back. This method is implemented by using a Bloom filter in each intermediate router along the path from attacks address to destination router to keep the hashed recorded of each packet that has gone through. The hash function enable the router to record such amount information of packets. Having these hashed recorded in the routers along the path, destination router can retrace the packet back to its source address easily.

Also, based on the features of application-level DDoS attacks, the defense methods are summarized into two types[23]:

Destination-based: DDoS Shield is a destination-based method that detect the features of HTTP sessions statistically and using rate-limiting to against flooding attacks.

Distributed : CAPTCHA is an effective distributed method to against DDoS attacks. CAPTCHA prevents the incoming requests/packets flooding by challenge the user with pre-generated challenges which have to be solved by real person. Although this is a simple and effective defending method, the usability is limited by the nature of this method that has to interact with real person. In the internet, most of the communication between hosts and servers are actuated by hidden applications and protocols, therefore CAPTCHA cannot be used in many circumstances.

III. SDN

SDN architecture is dynamic, manageable, cost-effective, and adaptable. These features of SDN make it easier to detect and react DDoS attacks. In this section, many features which are beneficial to against DDoS attacks are summarized. In addition, the currently available methods against DDoS attacks using SDN are provided.

A. Features of SDN

As mentioned that the features of SDN make the network more manageable, SDN has provided new chances to completely mitigate the DDoS attack. The beneficial features of DNS to against DDoS attack are summarized as follows [17]:

1) Three planes architecture: application plane, control plane, and data plane: With the central controller managing the SDN, researchers are capable to launch attack or defense experiments in manageable real world environment. The transition period of mechanisms, methods, and protocols deployment are simplified and expedited comparing to traditional distributed architecture. This also encourage the innovation of the network by the programmable network platform. In addition, the DDoS attacks become feasible and simple to be recognized due to the separation of the control plane.

2) Logical centralized controller: Due to the centralized architecture, the controllers have the knowledge of whole network and global view of the network. With these capabilities, SDN can set up consistent security police, monitor anomalous activities to predict potential threats. In addition, compromised hosts could be dynamically quarantined by the controller.

3) Programmability: External sophisticated and smart algorithms are allowed to be flexibly applied in SDN to work as defense methods against different DDoS attacks. The existing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are examples that be implemented in SDN programmable environment to enhance the consistency and security of SDN.

4) Traffic analysis: The traffic analysis improve the capabilities of switches by allowing switches using any application-based algorithms. Database, machine learning, and many other specific designed application can be implemented in real time to analyze the network traffic patterns. For the detection of abnormal traffic, Deep Packet Inspection (DPI) from IPS will be perform if critical traffic interests are found.

5) Dynamic reconfigurable forwarding rules: Reconfigurable forwarding rules allow the network traffic to be allocated dynamically, so that the capabilities of switching devices are increased. In addition, the dynamic feature enables the SDN to react DDoS attacks quickly. If a security threat is detected by traffic analysis, updated security policy or new flow forwarding rules will be dynamically propagated to target network switching devices.

B. Defending DDoS attacks using SDN

The OpenFlow protocol enables SDN networking architecture to be more manageable by enforcing the centralized control. By this protocol, the new arriving packets (no matched entries in the flow table) will be directly sent to SDN controller. Then, different methods can be applied to diagonal and analyze the packets. The classifications of methods against DDoS attacks using SDN are also categorized into three types: Source-based, Network-based, and Destination based. The description of methods are as follow [23]:

1) Source-based:: As the entrance of the network, the most ideal defending method is to filter out the DDoS attacks traffic at the very starting router/switch. This can be achieved under beneficial capabilities offered by the SDN networking architecture. The source-based methods will let SDN controller to detect anomaly traffic, validate the source IP address of traffic, and filter the abnormal traffic flows.

Utilizing the programmability of SDN, a method designed by [9] can effectively protect the small business or home networks from DDoS attacks. This method uses four detection algorithms cooperating with the SDN NOX controller to detect abnormal traffic. The first algorithm is threshold random walk with credit based rate limiting. It is a classifying method to distinguish abnormal traffic by sequential hypothesis testing. The second algorithm is Rate Limiting. It limits the new connection rate by observing and capturing the characteristic of compromised hosts. The third algorithm is Maximum entropy detector. It estimates the traffic distribution by entropy and build packet types distribution by some time units. The forth algorithm is NETAD. It is a rule-based traffic filter. Based on the preset rule, NETAD filter out the un-interesting traffic and focus on the packets that are suspected to be abnormal by the detection on connection request phase. In [9] shows that by implementing these four algorithms, the abnormal traffic detection accuracy is improved significantly comparing to the traditional abnormal detection on ISP.

As the mobile traffic growing increasingly, mobile device are also possible to be compromised and be used to launch DDoS attacks. With SDN architecture, mobile traffic anomaly can be detected effectively. A method in [15] can detects mobile anomaly by real-time traffic analysis. It is achieved by having OpenFlow enabled access points to forward traffic to SDN OpenFlow controller. The access points receive and install the flow rules from controller and start to forward the mobile traffic into the network. The detection function is implemented in the controller. The detection algorithms include three algorithms. The first algorithm is Connection Success Ratio. It utilizes the observation of the connection success ratio to distinguish the good and bad hosts. Normally, a good host has the higher connection success ratio than a bad host. The second algorithm is IP Blacklist. This is literally a blacklist that keeps the record of malicious IP addresses. The records are either from the public resources or from the historic that recorded by the controller itself. If a traffic with IP address is in the blacklist, the controller will deny it directly. The third algorithm is Throttling Connection. The idea of this algorithm is to limit the rate of connections of new clients. It will distinguish normal hosts and malicious or infected hosts by the behavior. Normally, an infected host will try to establish new connections to as many other hosts as possible in order to propagate the virus. However, a normal host usually make new connections in a slow and steady rate, and the target hosts are usually correlated. With these three algorithms implementing in the controller, anomaly mobile traffic will be greatly reduced.

Since the DDoS attack is usually launched by having a control on a botnet, the routing locator spoofing problem is becoming a more and more important problem to deal with. In [20] a SDN based method called Virtual source Address Validation Edge is designed to solve this problem. By applying the global view capability of SDN architecture, this method uses OpenFlow protocol to deal with the address spoofing problem. Using OpenFlow switches to form an area that any new incoming traffic (with no matched entries in flow table) will be redirected to NOX controller. The controller will validate the source addresses of the traffic by its network-wide knowledge and preset acceptable IP address range.

2) Network-based: In [10], a lightweight DDoS flooding attacks detection method is proposed. This method uses the packets features to distinguish if traffic flows are anomaly or not. The feature extraction processes is implemented in a low overhead level. The processes includes three part. The first part is Flow Collector which will request flows from flow tables of switches periodically. The second part is Feature Extractor. After the controller receives the flows, any features which are useful to DDoS detection are extracted. The third part is the classifier which is responsible to analyze the extracted features from packets. Based on the classifying method Self-Organizing Maps (SOM), it classifies if the packet is normal packet or DDoS flooding packet. With the SDN capability that allowing traffic analysis using external application, the centralized controller, and the programmability of the network, these processes can be implemented in a low overhead level, and allowing the SOM to be used as the classifying method to find out anomaly traffic.

A content oriented networking architecture is designed in [21]. With the usage of accountability and content aware audit, this method can be employed to detect DDoS attacks promptly. When the controller receives a certain type of contents more than expected number of times, the DDoS flooding attack is detected by this situation.

In [5], the author combines OpenFlow and sFlow protocol to construct a new method to detect and mitigate DDoS attacks. By using collector, it applies the packet extraction method as [10] proposed to perform the anomaly detection. As well, it utilizes the sFlows feature, packet sampling capability, to increase the scalability and decrease the need for flow exchanges between switch/router and controller.

A low memory overhead method named Distributed and collaborative per flow monitoring (DCM) is designed in [1]. Employing a small size of memory, DCM keeps records of monitoring rules in Bloom filters. By programmability of SDN architecture, DCM installs a dynamic monitoring program into data plane switches. It also has many Bloom

filters to implement varied kinds of measurement operation. DCM also be able to send updates and reconfigurations of Bloom filters to switches.

The Network-based methods summarized in here can all be implemented as SDN applications. Based on the description of these methods, four major parts can be concluded: Collector, Feature extractor, Anomaly detection, and DDoS flooding traffic mitigation.

3) Destination-based: The destination-based methods mainly focus on retracing the received packets and performing diagnosis. By retrieving the full stories of packets during the transmission, many valuable information are useful for the diagnosis. A packet-histories reconstructing platform, NetSight, is introduced in [6]. It offers a feasible way to collect interested packets, and in this platform, interested packet histories can be easily and accurately retrieved by applications.

A SDN control plane traffic recording application is presented in [16] which supports consistent and scalable traffic replaying. Benefit from the programmable and centralized control capabilities of SDN architecture, this method is able to dynamically record traffic between controller and switches, and between switches. By replaying the recorded traffic, packets histories will be revealed by performing a traffic diagnosis on the controller.

The methods on destination-based are basically trying to retrieve the histories of traffic and perform troubleshooting. Unlike the traditional DDoS defending methods which are mainly focus on getting the original attackers IP addresses and updates its filter rules.

IV. SDN can be a victim of DDoS Attacks

Although SDN are greatly expected to defeat the DDoS attacks by exploiting many beneficial capabilities of SDN architecture to against DDoS attacks, the security problem of SDN architecture is also a big concern. In this section, we are going to discuss the security vulnerabilities of SDN by 3 logical architecture layers: Application layer, Control layer, and Infrastructure layer. Also, some existing solutions are summarized.

As shown in figure 2, the three layer architecture opens many possible break points for DDoS flooding attacks. Based on the features of these vulnerable points, the DDoS attacks targeting on SDN are classified into the following three categories:

A. Application layer

There are mainly two possible attacking strategies on application layer. The first one is to attack the software

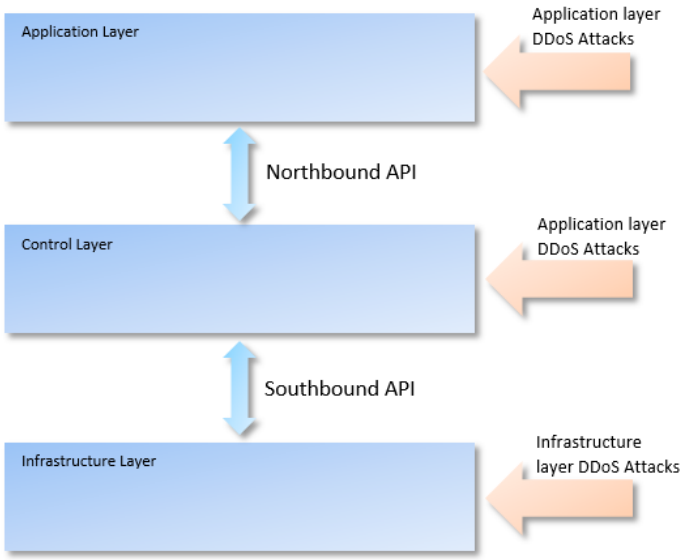

Fig. 2. Potential attacks on three layers of SDN architecture.

installed in this layer. Since some operational problems still remain to be solved under the separation of software and resources architecture, the attack of an application may implicate other applications. Another possible DDoS attacks strategy is attacking on the Northbound API.

B. Control layer

Due to the separation of the control plane from the data plane, the centralized controller architecture which can be regarded as the root of the whole network, attracts the favor of DDoS attacks, since the single point failure of the controller could cause the whole network shutdown. The break points on the control layer can be targeted by DDoS attacks are centralized controller, Northbound API, Southbound API, Westbound API or Eastbound API. The DDoS attacks can also from infrastructure layer. Due to the principle of SDN architecture that infrastructure layer (data plane) will quest the flow rules on new incoming packets which cannot find match on its flow table, it may result in the controller receiving overhead queries which causing the high occupation of switch-controller bandwidth and the exhausting of controller resources.

C. Infrestructure layer

There are mainly switches in this layer. To bright down a switch, the attackers can focus on sending DDoS flooding traffic to a single switch with spoofed source addresses. Every time when the switch receives packets with no matches on this flow table, there are two possible way to quest the controller: the first way is sending the whole packet to control. The second way is sending the header only to controller which the payload of the packet will remain in the memory of the switch. Attacks could potentially get use of

this way to keep sending source address spoofed packets and intended to overflow the switchs memory. Due to the high cost of the memory component (TCAM) , the size of the memory would not be too large. [18], [13]

V. Conclusion

In this paper, we have introduced the classifications and characteristics of DDoS attacks in traditional network architecture. After that we have analyzed the capabilities of SDN, and then we have discussed detecting and reacting methods against DDoS attacks under SDN using the beneficial capabilities of SDN. Due to the SDN may also be the victim of DDoS attacks, we have summarized the break points of SDN by three layers that DDoS attacks may launch on.

Through the comprehensive study of the relationship between DDoS attacks and SDN, we have seen that their relationships are contradiction: SDN is a good network architecture that can effectively detect and mitigate the DDoS attacks by its advantaged capabilities. However, SDN itself can be the target of DDoS attacks. Due to the SDN is still under theoretical experimental phase, many security vulnerabilities are remained to be solved yet. More researches on the security aspect of SDN are needed in order to bring this architecture into real life.

References

[1] Q. Chen, Y. Yu, and X. Li. Distributed collaborative monitoring in software defined networks. In *in Proc. HotSDN, 2014, pp. 8590*.

[2] Nhu-Ngoc Dao, Junho Park, Minho Park, and Sungrae Choi. A feasible method to combat against DDoS attack in SDN network. In *International Conference on Information Networking (ICOIN)*, 2015. DOI: 10.1109/ICOIN.2015.7057902.

[3] Ping Dong, Xiaojiang Du, Hongke Zhang, and Tong Xu. A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In *IEEE International Conference on Communications (ICC)*, 2016. DOI: 10.1109/ICC.2016.7510992.

[4] S. Sezer et al. Are we ready for SDN? Implementation challenges for software-defined networks. In *IEEE Commun. Mag., vol. 51, no. 7, pp. 3643*, Jul. 2013.

[5] K. Giotis, G. Androulidakis, C. Argyropoulos, and D. Kalogeras. Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. In *Comput. Netw., vol. 62, pp. 122136*, 2014.

[6] B. Heller, D. Mazieres, V. Jeyakumar, N. McKeown, and N. Handigol. I know what your packet did last hop: Using packet histories to troubleshoot networks. In *in Proc. Symp. NSDI, 2014, pp. 7185*.

[7] F. Hu, Q. Hao, and K. Bao. A survey on software-defined network (SDN) and openflow: From concept to implementation. In *IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 21812206*, 2014.

[8] Y.-D. Lin, D. Pitt, D. Hausheer, E. Johnson, and Y.-B. Lin. Software Defined Networking: Standardization for cloud computings second wave. In *Computer, vol. 47, no. 11, pp. 1921*, Nov. 2014.

[9] S. A. Mehdi, J. Khalid, and S. A. Khayam. Revisiting traffic anomaly detection using software defined networking. In *Recent Adv. Intrusion Detect., 2011, pp. 161180.*

[10] E. Mota, R. Braga, and A. Passito. Lightweight DDoS flooding attack detection using nox/openflow. In *35th IEEE Conf. LCN, pp. 408415.*, 2010.

[11] S. M. Mousavi. Early detection of DDoS attacks in software defined networks controller. In *M.S. thesis, Dept. Syst. Comput. Eng., Carleton Univ., Ottawa, ON, USA*, 2014.

[12] T. Peng, C. Leckie, and K. Ramamohanarao. Survey of network-based defense mechanisms countering the DoS and DDoS problems. In *ACM Comput. Surveys, vol. 39, no. 1, pp. 142*, Apr. 2007.

[13] S. Sezer. Are we ready for SDN? Implementation challenges for software-defined networks. In *IEEE Commun. Mag, vol. 51, no. 7, pp. 3643*, Jul. 2013.

[14] Amir Shoeb and Dr T. Chithralekha. Resource Management of Switches and Controller During Saturation Time to Avoid DDoS in SDN. In *IEEE International Conference on Engineering and Technology (ICETECH)*, 2016. DOI: 10.1109/ICETECH.2016.7569231.

[15] B. Wang and R. Jin. Malware detection for mobile devices using software-defined networking. In *IEEE 2nd GREE Workshop, pp. 8188.*, 2013.

[16] A. Wundsam. OFRewind: Enabling record and replay troubleshooting for networks. In *in Proc. USENIX Annu. Tech. Conf. 2011, pp. 139*.

[17] W. Xia, Y. Wen, C. Foh, D. Niyato, and H. Xie. A survey on software defined networking. In *IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 2751*, 2015.

[18] Y. Xu and Y. Liu. DDoS Attack Detection under SDN Context. In *IEEE INFOCOM*, 2016. DOI: 10.1109/INFOCOM.2016.7524500.

[19] Q. Yan and F. R. Yu. Distributed denial of service attacks in software-defined networking with cloud computing. In *IEEE Commun. Mag., vol. 53, no. 4, pp. 5259*, Apr. 2015.

[20] G. Yao, J. Bi, and P. Xiao. Source address validation solution with openflow/nox architecture. In *19th IEEE ICNP*, 2011.

[21] T. Y. W. Yoon, H. C. J. Suh, T. Kwon, and Y. Choi. Implementation of a content-oriented networking architecture (CONA): A focus on DDoS countermeasure. In *in Prof. Eur. NetFPGA Develop. Workshop, pp. 15*, 2010.

[22] Bin Yuan, Deqing Zou, Shui Yu, Hai Jin, Weizhong Qiang, and Jinan Shen. Defending against Flow Table Overloading Attack in Software-Defined Networks. In *IEEE Transactions on Services Computing (Volume: PP, Issue: 99)*. DOI: 10.1109/TSC.2016.2602861.

[23] S. T. Zargar, J. Joshi, and D. Tipper. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. In *IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 20462069*, 2013.