This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

SDN, A Research on SDN Assets and Tools to Defense DDoS Attack in Cloud Computing Environment

Tasnim Tamanna,[1] Tasmiah Fatema,[2] and Reepa Saha[3]
[1]Data Network NovoCom Limited, Dhaka-1212, Bangladesh
[2]Dept. of EEE, University of Information Technology & Sciences, Dhaka-1212, Bangladesh
[3]Rahimafrooz, Energy Services Limited, Dhaka, Bangladesh

***Abstract*—Software Defined Networking has become a drone word to service and cloud providers since when they feel the need to make the network programmable. As the devices in data center and applications continue to rise in number, the need for bandwidth, storage and computing power grows substantially. This infrastructure needs to be managed, maintained, updated, powered and cooled. As a result, the traditional data center model is becoming too costly and complex to sustain. Also, security threats are growing significantly, Distributed Denial Service of Attacks (DDoS) is one of those vital security threats. With the advancement of Software Defined Networking (SDN), defense mechanisms against DDoS attack has opened a new door to cloud computing environment. Based over SDN, new infrastructure of cloud computing has brought novel possibilities to defense against DDoS attacks. In this paper, we are going to discuss on some of the valuable features of SDN and show we can make full use of SDN's assets and advantages to make cloud highly competent and secured against all threats. The research results in this paper can be expanded to prepare a new architecture of SDN enabled secured *IoT based cloud* environment.**

***Index Terms*—cloud computing, Software Defined networking, cloud security, DDoS, control plane centralization.**

I. Introduction

With the substantial flow of emerging technologies, cloud computing and virtualization are taking leading roles in IT market and these are gradually moving computing from desktop to the whole world wide web. As the number of devices and applications continues to rise, the need for bandwidth, storage, and computing power grows exponentially. This network infrastructure needs to be dynamic and flexible. As a result, the traditional data center model is becoming too costly and complex to sustain. Many IT experts believe that to maintain the quality of service, the future of IT market is cloud computing and software-defined networking (SDN), as a better network drives a better cloud [1].

There are three cloud computing models: A public cloud uses the shared infrastructure of a third-party service provider, who is responsible for managing, maintaining, securing and updating that technology. With a private cloud, government agencies can take advantage of cloud benefits in a private, secure setting while retaining ownership of the infrastructure. A hybrid cloud uses both a public and private cloud, which provides the flexibility to control certain applications and sensitive data and base cloud usage on specific needs and workloads [1], [2].

In the new era of advanced cloud computing, security issues are being regarded as major barriers. Requirements of security in cloud computing include: interface & APIs hacking, system vulnerability, confidentiality, availability, data loss and cloud service abuses [3]. Among all of these, the most important issue is availability, as the core responsibility of cloud computing is to provide on-demand delivery of service. In order to ruin the place of cloud computing, one of the major methods are Denial of Service (DoS) and Distributed Denial of Service (DDOS). Though many solutions have been suggested so far to defense and fight against DDoS attacks but they have met with few favorable outcome [3], [4]. But with the gradual progressing of SDN, SDN-based cloud brings us new scopes to defense and fight against DDoS attacks in cloud computing environment.

We have organized the whole paper as follows: Section II illustrates SDN and it's basic architecture. Section III elaborates current scenario and types of DDoS attacks in cloud environment, whereas Section IV discusses SDN assets and good features of SDN to prevent DDoS. Section V deals with advantages and tools of SDN for defending against DDoS. The final section concludes and summarizes the whole paper, as well as shows the way to extend this work in future.

II. What is SDN and It's Basic Architecture

The crystal clear and well-defined definition of SDN provided by ONF is as follows: "In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications" [5]. In SDN, software is allowed to run independently from the underlying hardware, which we called virtualization and this is the basis of SDN. [5] Cloud computing is now possible because of virtualization and datacenters are now allowed to vigorously supply IT resources to make the cloud computing a success. However, the idea of virtualization can now be implemented in the network as well, which means separation the function of controlling traffic from network hardware, resulting in SDN.

SDN architectures fundamental principle is the segregation of control and data plane, a logically centralized controller to

978-1-5090-4442-9/17/$31.00 ©2017 IEEE

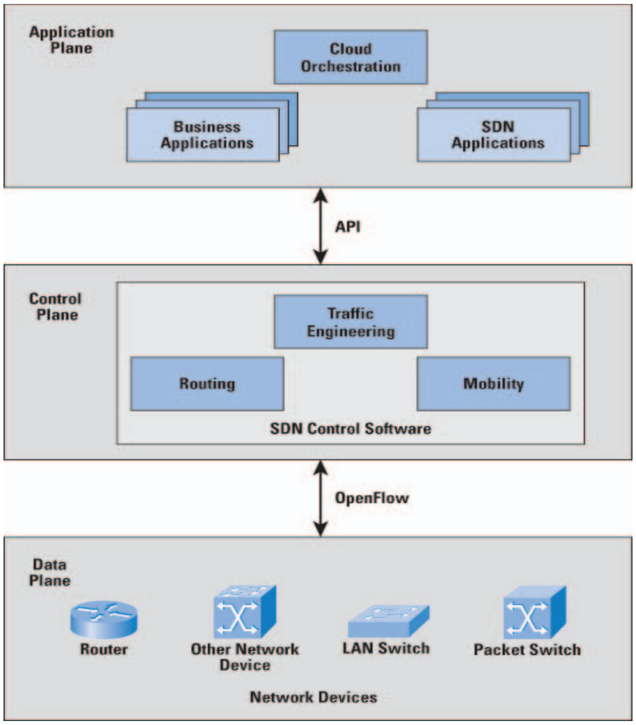

Fig. 1. SDN logical architecture [source: software-defined networks and openflow - The Internet Protocol Journal, volume 16, no. 1].

make all forwarding decisions and programmable interfaces at multiple levels. The typical architecture of SDNs according to the Internet Protocol Journal is shown in Fig. 1. As shown in the figure, this architecture involves three separate functionality planes:

1. *Data plane*—The data plane's responsibility mainly consists of forwarding functionality. All network devices, i.e.: routers, LAN switches, packet switches etc. are the elements of data plane.
2. *Control plane*—The control plane's responsibility mainly consists of control functionality of the whole network. A set of controllers makes the decision of traffic engineering and monitoring and tell the data plane devices to do so. The controllers communicate among themselves using SDNi interfaces, when there are bunch of controllers and each controller is responsible to make all network decisions for a certain zone of the network.
3. *Application plane*—The application plane is responsible for generic network management auditing, and reporting functionalities (e.g., SDN management, monitoring and security). The functionality of this plane is realized through different network management applications (e.g. Network visualization).

The SDN architecture defines also the key interfaces between the different components in it. These interfaces are stated a below:

1. *East/West bound API*—This interface is implemented by the different controllers of the SDN and is used to facilitate communications between them.
2. *Southbound API*—This interface is implemented by the different forwarding devices in the SDN to enable the communication between these devices and the controllers of the network.

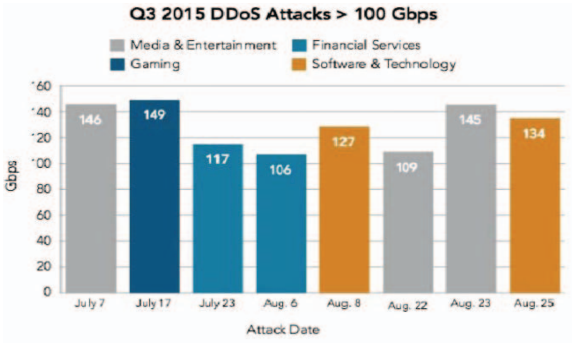

Fig. 2. Eight DDoS attacks registered more than 100 Gbps in Q3 2015 [image source: Akamai report].

III. Current Scenario and Types of DDoS Attack in Cloud Environment

According to the latest marker research, DDoS attack is becoming most popular and powerful type of attack day by day. This is rapidly increasing in volume and number in recent time. The recent trend is huge packet-per-second volume but time duration is small. Also, the overall number and types of attacks have been grown notably [9]. According to statistic published in the VeriSign Distributed Denial of Service Trends Report, DDoS activity is the highest it's ever been, with the final quarter of 2015 seeing an 85% rise in instances-almost double the number of attacks-when compared with the same period in 2014 [10]. The figures for Q4 2015 also represent a 15% rise on the previous quarter. On the other hand, Akamai's latest State of the Internet Security Report publishes that, internet and web attacks are enlarging in figure, volume and continuation. There has been a 125 percent grow in distributed denial of service (DDoS) attacks over year, which is another findings of the content delivery network (CDN) provider Akamai [10].

On recent records, BangStresser is the biggest DDoS attack [11]. This attack happened over the New Year's weekend against BBC's website and current US president Donal Trump's campaign site and the New World Hacking Group declared it's responsibility. This attack had been launched up to 602 Gbps and take down the site for several hours (see Fig. 2).

It is important to note that while most common DDoS attacks broadly fall into these three categories, some attacks can also be a combination. For example, the recent attack on Dyn's DNS infrastructure was a combination of an application and protocol attack on DNS services that expanded into a volumetric attack. It is also noteworthy to mention that while some attacks target the DNS infrastructure directly, others can use DNS as a means to trigger an attack. Based over these analyses, there are two types of DDoS attacks:

A. Network-Centric DDoS Attack:

Network-centric attack mainly attacks network layers 3 & 4 and try to flood the bandwidth capacity and routing infrastructure by sending very large number of bogus requests [13]. Mainly, there are four categories of network-centric attacks:

1. *Flooding/Volumetric attacks*: In flooding/volumetric attacks, huge amount of traffic is used to saturate the bandwidth of the target. It comes in a variety of forms including- TCP flood, UDP flood or ICMP flood.
2. *Protocol attacks*: Protocol attacks consume all the processing capacity of the attacked-target or intermediate critical resources like a firewall causing service interruption. SYN flood, Ping of Death are some it's examples.
3. *Reflected attacks*: In reflected attacks, the culprit sends a huge number of UDP packets to a DNS or NTP server using a spoofed source IP address. After that, the server, which is taking a medium role in this attack, sends back information back to the victimized or spoofed IP address.
4. *Amplification-based attacks*: In amplification-based attack, culprits make big or multiple response for each of the messages they receive to amplify the traffic towards the victim. Thus they attempt to harness the services of the provider.

- Application-layer DDoS attack:

In application-layer attacks, attackers target a service or database by attacking application layer of OSI model [13]. Typical application layer attacks include:

1. *HTTP flood*: The attack constantly requests a specific HTTP URL or all of the URLs in a web application. This can have a great performance impact on the targeted server.
2. *POST flood*: This attack generates HTTP POST requests, which are generally handled directly by the targeted Real Server causing a significant performance impact.
3. *Attack on DNS services*: In this attack scenario, small DNS queries are made with fake source IP addresses which in return, produce a huge amount of network traffic because DNS response messages are multiple times larger than DNS query messages. After that, this huge volume of traffic is passed to the victimized system to immobilize it.

We have also analyzed and surveyed over the type of attackers in context SDN. Attackers can be categorized into below types:

1. *External attacker*: These type of attacker does not have any authorized access to the SDN network. They have own network infrastructure and tools to interfere with other SDN operation.
2. *Internal attackers*: Internal attackers are those who reside inside the SDN network, they can be some dishonest network/telecom operators or dishonest customers. The dishonest operators always try to ruin other provider's business and dishonest customers try to gain access of SDN network and do mischievous tasks.

IV. SDN Assets and Good Features of SDN to Prevent DDoS

In this part valuable assets of an SDN network infrastructure are presented that are commonly found in the literature in a hierarchical manner. Based on a single first top layer classification these SDN assets are distinguished into:

- **Data plane assets:** This asset group includes all physical instances of the network such as switching devices (Switches/Routers) and the communication medium (wired or wireless). Data plane assets include both hardware and software (e.g. Firmware, or a more or less full-fledged operating system and software switch) of the so called network elements.
- **Control plane assets:** This asset group includes any SDN assets related to the control plane of the SDN. Such assets include both the hardware (e.g. controllers and Interfaces) and software used to realize SDN control (e.g. protocols for the controller communication), along with system configuration and control data.
- **Application plane assets:** This asset group includes software applications that are used to implement any network explicitly, directly. Applications can communicate their network requirements and desired network behavior to the SDN Controllers via APIs. Application plane assets include also hardware that is used to run these applications (e.g. Servers).
- **Service provider IT infrastructure assets:** This asset group includes any component of an IT infrastructure that is used by or belong to any service provider in the SDN from a billing system to stored data of an end user in a cloud.
- **Network service provider physical infrastructure assets:** This asset group includes physical assets of the network service providers including every construction (e.g. Buildings, data centers etc.), machinery as well as the power supply networks.

Major distinct features of SDN architecture includes:

1. *The control and data planes are decoupled*

Control functionality is removed from network device that will become simple forwarding elements. Control plane only works with controller that operate data plane elements.

2. *Flow-based forwarding decision*

In the SDN context, a flow is a sequence of packets between a source and a destination. Traffic engineering, monitoring, isolating bad traffic from the good etc. are implemented in SDN based over flow-based forwarding decision. OpenFlow protocol is used for this purpose by the controller to direct data plane elements.

3. *Control logic is transferred to an independent object*

The controller is a software platform that is transferred to a dedicated server and used to control and maintain whole network operation. A set of controllers for different network zones makes the decision of traffic engineering and monitoring and tell the data plane devices of that zone to do so.

4. *Programmable network*

One of the basic characteristics of SDN is, the whole network is programmable using software applications to fulfill data plane requirements on top of the controller. Mostly used programming languages for this purpose are Python in POX and Ryu, Java in OpenDaylight, Floodlight & Beacon etc.

V. Advantages and Tools of SDN to Protect Cloud from DDoS

As aforementioned, SDN has numerous well-defined features and some of the features offer many solutions for mitigating DDoS attacks:

1. *Segregation of control plane and data plane*

As SDN decouples the data plane from the control plane, it is easily possible to experiment over DDoS threats and defense mechanisms against it. SDN's high configurability offers clear partition among virtual networks and huge potential in putting forward new techniques and hypotheses for DDoS attack mitigation.

2. *Controller centralization*

As the controller has overall knowledge of whole network, it can easily build uniform security rules and monitor or observe traffic/flow patterns for possible DDoS threats. When an attacker tries to attack the network, the centralized controller can isolate compromised hosts and authenticate legitimate hosts in a fast dynamic process.

3. *Programmability of whole network by exterior applications*

SDN programmability supports a process of collecting intelligence from current intrusion detection systems and intrusion prevention system. Based over various types of DDoS attacks, a lot of smart and fast algorithms can be used to protect the network.

4. *Traffic analysis based on software*

Traffic/flow analysis is a basic requirement for a network operation system. Software based traffic analysis is performed using various software tools, smart and fast algorithms and databases, which enables innovative network operation.

5. *Forwarding rules and flow abstraction are dynamically updated*

As forwarding rules are dynamically updated in SDN so that whenever a DDOS attack occurs, they can response in prompt manner. Besides, new and updated security rules can be spread over the whole network in the form of flow rules, and thus drop the malicious traffic in a quick way.

6. *Fully automated operation*

For network security, automation has become a basic requirement. The network is expanding substantially and it will be critical and time-consuming to apply security policy in each device instead of having an automated manner. The SDN controller will enable automated security control using robust APIs and schedule the security policies. The policies will then be distributed to all associated switches of data plane. Malicious traffic comes and is directed towards the security defense pool for further processing using the suitable filtering and defense mechanisms [12].

7. *Traffic tunneling*

In the recent scenario of network infrastructure, SDN involves network virtualization to run virtual network. The encapsulated traffic needs to be addressed by the security component of the network to ensure QoS and access control. For properly monitoring the traffic, security solutions of network will need to accompany the ability to de-capsulate the traffic, or rely upon switches to translate SDN encapsulation and decapsulation protocols to VLANs.

We also surveyed over existing techniques, tools and practices for DDoS mitigation:

1. *Radware's DefensePro*

DefenseFlow module keeps traffic statistics and detects attack. To mitigate DDoS, DefensePro module clears traffic and redirects clear flow to destination.

2. *Alcatel Lucent's OmniSwitch*

It detects DDoS by statistical analysis with the help of sFlow and mitigation application decides action to mitigate DDoS.

3. *Brocade's MLXe Series Router*

It detects DDoS by sFlow-enabled statistical analysis and with the help of predefined techniques, it mitigates DDoS.

4. *OpenFlow DDoS Mitigation*

It detects DDoS by using standard deviation, handler packet symmetry. It mitigates DDoS attack by blocking attack flow.

5. *Mitigating Denial of Service attacks in OpenFLow networks*

It detects DDoS by statistical analysis and mitigates by blocking the flow.

6. *Flooding DDoS Mitigation and Traffic*

It detects DDoS by clustering and cluster traffic ration of normal to attack. By providing slower rate service to possible attack requests, it mitigates DDoS.

VI. Future Works and Conclusion

By 2020, industry analysts predict the making and use of zillions of "Internet of Things" devices and these devices are going to generate a large amount of data. What is really important to note, these data need to be processed and stored in a cloud computing environment. That means, we need to think of outside the box of Internet of Things and make it expand to the cloud of things. Integrating IoT with cloud computing, makes a new paradigm and this will only be possible, when we build and maintain our network using SDN.

In this paper, we have discussed on current scenarios of security issues in Cloud Computing environment and different types of DDoS attacks in cloud environment. Also, we have discussed on present scenario of security threats, i.e. DDoS attack in this environment, SDN structure and some of the distinct features of SDN. Finally we have discussed about how to deal with security threats in cloud using SDN features. In the new era of Internet of Things integrated with cloud computing, this work may help to prepare a new architecture of SDN enabled secured *IoT based cloud*environment.

References

[1] M. Rouse, *Cloud computing*. SearchCloudComputing. TechTarget. Sept. 2015, Retrieved 20 May 2016.

[2] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Computer networks*, Elsevier, vol. 81, pp. 308–319, 2015.

[3] Fahmida Y. Rashid, "The dirty dozen: 12 cloud security threats," in *InfoWorld*, Mar. 11, 2016.

[4] N. Z. Bawany, J. A. Shamsi, and K. Salah, *DDoS attack detection and mitigation using SDN: Methods, practices, and solution*, Springer, Feb. 02, 2017.

[5] N. Dayal, P. Maity, S. Srivastava, and R Khondoker, "Research trends in security and DDoS in SDN," *Security Comm. Networks*, 2017.

[6] SDN Analytics for DDOS Mitigation, Solving Real World Enterprise Problems Today, Alcatel-Lucent.

[7] R. Sahay, G. Blanc, Z. Zhangyz, and H. Debar, "Towards autonomic DDoS mitigation using software defined networking".

[8] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," 2013

[9] "What is a DDOS attack?," K4LINUX, July 19, 2014.

[10] D. Bisson, "DDoS attacks increased by 180% compared to 2014, reveals Akamai report," The State of Security, Jan. 14, 2016.

[11] *DeMISTIfying Infosec: DDoS*, MISTI Training Institute.

[12] *SDN based cloud data center security*, Huawei, June 24, 2014.

[13] O. Alominle, *(DDOS) distributed denial of service attack*, Linkedin, February 24, 2016.

[14] W. Stalling, "Software-defined networks and openflow," *The Internet Protocol Journal*, vol. 16, no. 1, Mar. 2013.

[15] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys & Tutorials*, June 26, 2015.