ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol. 2, Issue 8, August 2016

Distributed Denial of Service Attacks in Network Propagation Model with Web Service

N. Angel[1], Dr. A. ChandraSekar[2]
[1]Associate Professor, Dept. of MCA, St. Joseph's College of Engineering, Chennai
[2]Professor, Dept. of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai

Abstract: - Web Services has become the real trend of enterprise IT service model that offers cost-effective and scalable processing. Meanwhile, Software-Defined Networking (SDN) is gaining popularity in enterprise networks for flexibility in network management service and reduced operational cost. There seems a trend for the two technologies to go hand-in-hand in providing an enterprise's IT services. However, the new challenges brought by the combination of Web Service and Software Defined Networking(SDN), particularly the implications on enterprise network security, have not been well understood. This paper sets to address this important problem. We start by examining the security impact, in particular, the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted. We find that Network Propagation Model (NPM) technology can actually help enterprises to defend against DDoS attacks if the defense architecture is designed properly. To that end, we propose a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to enable attack detection and a flexible control structure to allow fast and specific attack reaction. The simulation results show that our architecture can effectively and efficiently address the security challenges brought by the new network paradigm. The system show that NPM brings us a new chance to defeat DDoS attacks Web Service, and we summarize good features of SDN in defeating DDoS attacks.

Keywords: Denial of Service, web service, attack count, attack filter

I. INTRODUCTION

Networking principles have remained mostly unchanged over the past decade. Networks are built using more or less sophisticated switches and routers. These devices are being developed by tens of vendors usually using proprietary operating system and interfaces. Building heterogeneous networks on devices from different vendor's means that organization have to employ a specialist on every router brand. Configuration of different systems also increases the probability of configuration mistakes. This issue coupled with incompatibility of different versions of systems from one vendor make heterogeneous networks difficult or very expensive to manage. There is a need for a new technology to make networks more scalable, dynamic and to allow easier management of network devices from different vendors. These needs could be fulfilled by programmable networks, i. e., by Software Defined Networking (SDN). SDN could replace traditional networking. It is based on the abstraction of a control and a data plane. The main idea is to produce less sophisticated data plane devices, e. g., switches, which only forward the traffic according to a set of rules defined by the software in the control plane. This should remove the differences in proprietary interfaces of devices and makes the network administration independent of data plane devices vendors [3]. SDN also enables applications and network services to treat the network as one logical entity and grants unified access to all devices through the SDN control plane. This opens the upper layer of the network to software that can manage how a traffic in the network is forwarded.

A DDoS attack is an attempt to make a network or server resource unavailable to its intended users. This attack is relatively easy to perform, hard to defend against, and the attacker is rarely traced back. This attack was performed manually by users refreshing their browsers. Since the first attack, there have been many other more or less sophisticated DDoS attacks. Average DDoS attack bandwidth increased from 2.88 Gbps in Q3 2013 to 13.93 Gbps in Q3 2014. There were 17 attacks with bandwidth higher than 100 Gbps. Even though there are many proposed detection methods and mitigation techniques, we cannot say that the DDoS attacks are a solved problem or do not present an immense threat to the current Internet. The research in the field of SDN and general security in SDN is still in its early phase. The SDN will not erase the DDoS attacks from the Internet. Moreover, every new technology and level of abstraction opens new attack vectors. However, we believe that the attributes of SDN can help to detect and mitigate the attacks. Currently, there are several papers analyzing DDoS attack vectors and proposing new solutions of mitigation of DDoS attacks in SDN environment. Our research will be dedicated to an analysis of security challenges in SDN from the point of view of DDoS attacks and development of a new DDoS attacks mitigation technique. We believe that SDN gives us a new powerful tool against DDoS attacks. The higher flexibility and easier management of networks could be a powerful tool for detection and mitigation of DDoS attacks. However, one should be aware of upcoming security threats accompanied with the deployment of SDN. The research focused on the security in SDN is still in its early phase. The research groups are focused on the security of the data plane, security of the control plane, security of the communication between these planes and on enhancing the network security using SDN, which is also our goal. The result of our research is going to be a novel method for mitigation of DDoS attacks using the benefits of Software Defined Networking, which enhance the network security. Combination of the existing detection methods and management of SDN forms a new way of DDoS mitigation in future networks.

Software Defined Networking (SDN) allows organizations to add applications more easily, streamline processes, reduce complexity, improve efficiency and provide a better user experience. In addition to security, SDN’s rapid adoption is driven by the desire to reduce capital expenditure (CAPEX) and operating expenditure (OPEX).

Previously, deploying network security solutions required networking changes in order to assure proper inspection of relevant traffic. Organizations needing multiple security gateways had to develop a highly complex routing and switching mechanism to forward various network streams to different inspection elements. When using a network switch, that switch’s proprietary firmware worked to guide packet forwarding—essentially treating all packets alike.

Web Services are composed fundamentally of computing, storage, and networking resources. In regards to network, Software-Defined Networking (SDN) has become one of the most important architectures for the management of networks that require frequent re-policing or re-configurations [13]

II. MOTIVATED

In existing system, the Web Service -based DDoS attacks or outside DDoS attacks can make ostensibly legitimate requests for a service to generate an economic Distributed Denial of Service (eDDoS)

Software-Defined Networking (SDN) is considered promising to simplify network management and enable research innovations based on the decomposition of the control and data planes. In this paper, we review SDN-related technologies. In particular, we try to cover three main parts of SDN: applications, the control plane, and the data plane anticipating that our efforts will help researchers set appropriate and meaningful directions for future SDN research.

Disadvantages:

- Using TLS/SSL does not per se guarantee secure communications.
- The security of those communications is as strong as its weakest link, which could be a self-signed certificate, a compromised certificate authority, or vulnerable applications and libraries.
- The TLS/SSL model is not enough to establish and assure trust between controllers and switches.

III. PROPOSED SYSTEM

In proposed system, first we discuss the new trends and characteristics of DDoS attacks in cloud computing environments. We show that SDN brings us a new chance to defeat DDoS attacks in cloud computing environments, and we summarize good features of SDN in defeating DDoS attacks. Software Defined Networks (SDN) is a new network architecture that provides central control over the network. This control works as if it is an operating system that can send instructions and apply changes through its interface. This operating system is called the controller. Although central control is the major advantage of SDN, it is also a single point of failure if it is made unreachable by a Distributed Denial of Service Attack (DDoS). Two main objectives of this study are utilizing the central control of SDN for attack detection and, proposing a solution that is effective and lightweight in terms of the resources that it uses. This research shows how DDoS attacks can exhaust controller resources and provides a solution to detect such attacks based on entropy variation of destination IP address. This method is able to detect DDoS within the first five hundred packets of the attack traffic.

SDN architecture can be a network of several controllers each of which is connected to a network of switches. Each of these networks and its controller can be seen as slice of the network. We are focusing on each of these slices to protect it against DDoS. If the connection between the switches and the controller is lost, the network will lose its processing plane. That means packet processing is no longer done in the controller and by losing the controller, the SDN architecture is lost. One of the possibilities that can cause the controller to be unreachable is a DDoS attack. In DDoS attacks, a large number of packets are sent to a host or a group of hosts in a network. If the source addresses of the incoming packets are spoofed, which theory usually are, the switch will not find a match and has to forward the packet to the controller. The collection of legitimate and the DDoS spoofed packets can bind the resources of the controller into continuous processing that exhausts them. This will make the controller unreachable for the newly arrived legitimate packets and may bring the controller down causing the loss of the SDN architecture. Even if there is a backup controller, it has to face the same challenge. The main goal of this research is detecting a DDoS attack in its early stages. The term early depends on the network itself. Since the controller software can be run on a laptop or a powerful desktop, the term early would depend on the tolerance of the device and traffic properties. However, if the detection happens in the first few hundred packets, the mitigation is applied before the controller is completely swamped with the large number of malicious packets [11].

The high configurability of SDN offers clear separation among virtual networks, permitting experimentation in a real environment. Progressive deployment of new ideas can be per-formed through a seamless transition from an experimental phase to an operational phase. This feature of SDN offers great convenience in putting forward new thoughts and methods for DDoS attack mitigation. In this paper, we first analyze the impact of the combination of cloud computing and SDN on DDoS attack defense. We discuss the potential issues under this new paradigm as well as opportunities of defending DDoS attacks. Based on our analysis, we claim that if designed properly, SDN can actually be exploited to address the security challenges brought by cloud computing and the DDoS attack defense can be made more effective and efficient in the era of cloud computing and SDN. We then propose a new DDoS attack mitigation architecture using software-defined networking to demonstrate and substantiate our findings. Implementing SDN affects the DDoS attack defense greatly in both directions. On the bright side, SDN makes advanced detection logic and rich subsequent processes easier to implement. On the down-side, the devices or middle-boxes originally distributed within the network now need to be located above NOS. Compared with hardware-based packet processing, software processes packets is much slower. The network delay and traffic overhead caused by the communications between the control programs.

Based on our analysis, Web service introduces new DDoS challenges, i.e., extended defense perimeter and dynamic network topology due to its new operation model. To effectively address these challenges, the cloud provider must be able to 1) easily delegate the control of its network to cloud users; 2) fast re-configure the control according to the network topology changes caused by dynamic allocations and migrations. On one side, we could benefit from the centralized network controller and the network virtualization of SDN. The negative impact of SDN mainly comes from the efficiency of processing packets using software, which may generate new attack surface and lead to single-point failure. When designing a DDoS attack defense solution in SDN, one must take the computation and communication overhead into the consideration so that no new security vulnerability is introduced.

Advantages:

- It is the first to bring the attention of the impact on DDoS attack defense of the new network paradigm, which is a combination of Web Service and SDN.
- This scheme works well under the new network paradigm and incurs limited computation and communication over-head, which is a crucial requirement of DDoS protection in cloud computing and SDN.
- The system find that the combination of SDN and Web Service provides a unique opportunity to enhance the DDoS attack defense in an enterprise network environment.

PROPOSED ARCHITECTURE

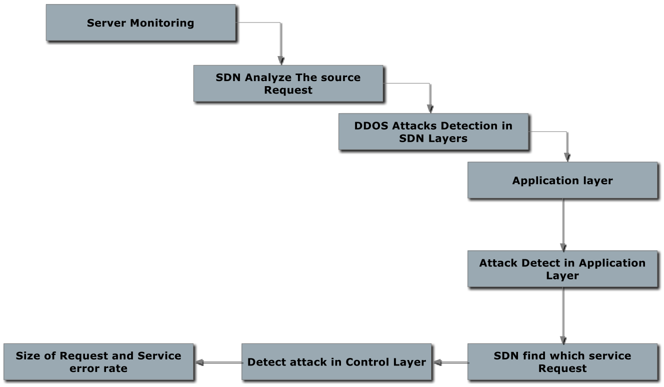
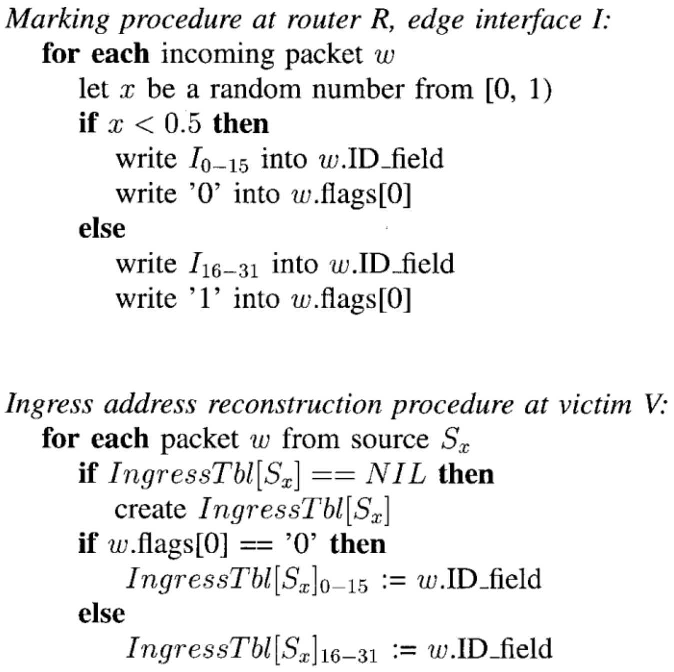

Server Monitoring
SDN Analyze The source Request
DDOS Attacks Detection in SDN Layers
Application layer
Attack Detect in Application Layer
SDN find which service Request
Detect attack in Control Layer
Size of Request and Service error rate

Fig. 1 Architecture Diagram

The Fig 1, shows how the Distributed denial of service attacks has been detected and avoided in the application layer. If the attack propagate to control layer it can calculate the service error rate.

IV. TRACE BACK MODEL

Here The Layer detect the attacks in North bound application level, that's mean SDN find which service Request has virus signature, that indicate in Logging level. If the Logged is '1' that service are not in virus Signature and which is Logged level is '0'that request has attached a virus or malware or botnet Signature. These attacks are filter in this layer and remaining services has forward to Control Layer.



```
Marking procedure at router R, edge interface I:
  for each incoming packet $w$
    let $x$ be a random number from [0, 1)
    if $x < 0.5$ then
      write $I_{0-15}$ into $w$.ID_field
      write '0' into $w$.flags[0]
    else
      write $I_{16-31}$ into $w$.ID_field
      write '1' into $w$.flags[0]
```

```
Ingress address reconstruction procedure at victim V:
  for each packet $w$ from source $S_x$
    if $IngressTbl[S_x] == NIL$ then
      create $IngressTbl[S_x]$
    if $w$.flags[0] == '0' then
      $IngressTbl[S_x]_{0-15}$ := $w$.ID_field
    else
      $IngressTbl[S_x]_{16-31}$ := $w$.ID_field
```

Network Propagation Model

V. ATTACK DETECTION FROM SOURCE USING TCB

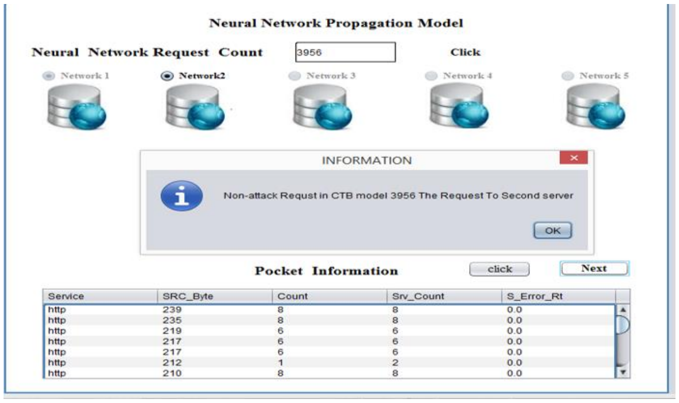
This Layer receive the request from Application layer and control the Request services forward to the server machine for Get the Required Result or Required Cloud service. This Source Request has to forwarding to each control server machine depending upon The Size of Request and Service error rate. If which is have maximum error rate that type of services are denied in this layer. And minimum error rate services only forward to the Destination server machine.

VI. NETWORK PROPAGATION MODEL

The Infrastructure layer is a Southbound of Network. It Receive the Services Request From Control Layer server Machine .It Generate The Result to each request or Provide The Services To The request IP, but before provide service…it analyze the Destination error rate.. because some of DDoS, malware or botnet attack couldn't find out above layers, that's filter maximum level of attack signature request, but still some of malwares no filter proper, so the Server indicate that service request using destination error rate, So maximum level of error request file has denied and finally the cloud service provide for non-attack request IP. The NPM server Calculate No of attack come from which IP and The time duration, Analyze the performance of Each Layer, how much attacks detect and filter in each level. And we have calculate the average level of DDOs Attacks in cloud Service

.

VII. SIMULATION RESULTS



Neural Network Propagation Model

Neural Network Request Count 3956

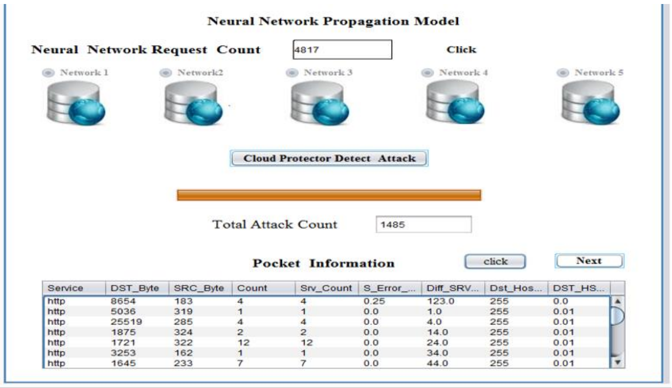
INFORMATION

Non-attack Requst in CTB model 3956 The Request To Second server

Pocket Information

Service	SRC_Byte	Count	Srv_Count	S_Error_Rt
http	239	8	8	0.0
http	235	8	8	0.0
http	219	6	6	0.0
http	217	6	6	0.0
http	217	6	6	0.0
http	212	1	2	0.0
http	210	8	8	0.0

Fig. 2 Attack Detection



Neural Network Propagation Model

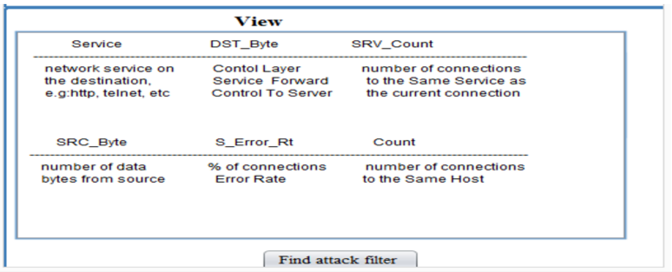
Neural Network Request Count 4817

Total Attack Count 1485

Pocket Information

Service	DST_Byte	SRC_Byte	Count	Srv_Count	S_Error_...	Diff_SRV...	Dst_Hos...	DST_HS...
http	8654	183	4	4	0.25	123.0	255	0.0
http	5036	319	1	1	0.0	1.0	255	0.01
http	25519	285	4	4	0.0	4.0	255	0.01
http	1875	324	2	2	0.0	14.0	255	0.01
http	1721	322	12	12	0.0	24.0	255	0.01
http	3253	162	1	1	0.0	34.0	255	0.01
http	1645	233	7	7	0.0	44.0	255	0.01

Fig. 3 Attack Count



View

Service	DST_Byte	SRV_Count
network service on the destination, e.g:http, telnet, etc	Contol Layer Service Forward Control To Server	number of connections to the Same Service as the current connection

SRC_Byte	S_Error_Rt	Count
number of data bytes from source	% of connections Error Rate	number of connections to the Same Host

Fig 4. Attack Filtering

Fig 2 shows that, the algorithm will detect and manage the attacks in the server. Fig 3 and 4 shows the attack count and attack rate.

VIII. PERFORMACE ANALYSIS

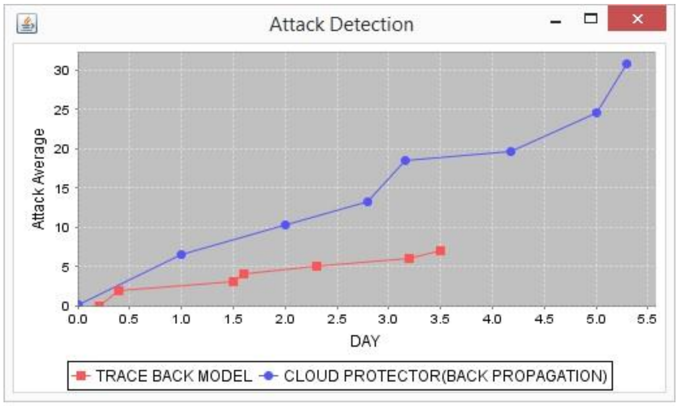


Fig. 5 Attack Detection Graph

The Fig 5 shows that, by using Network Propagation Model (NPM), the attack can be detected more than SDN

IX. CONCLUSION

With Network Propagation Model (NPM) both of the technology emerging as the future enterprise IT solutions, it is worthwhile to look at the implications of the combination of the two, particularly on the enterprise network security. In this paper, we analyze the impact of web service and NPM on DDoS attack defense. Based on our analysis, we identify the challenges and the benefits raised by these new technologies. We claim that with careful design, NPM could help with DDoS attack protection. To substantiate our finding, we proposed our solution of defending DDoS attack—Damask architecture. Compared to the existing solutions, Damask requires little effort from the cloud provider which means few changes are required from the current cloud computing service architecture. The NPM-based network monitoring and control mechanism allow companies to control and configure their defense mechanisms in the cloud effectively without affecting other cloud users. We also carried out a simulation study using real network traces to evaluate the performance. The results show that our proposed Damask is successful in dealing with the new challenges raised. The NPM-based network management can rapidly adapt to the network topological changes.

REFERENCES

[1] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," IEEE Common. Surveys &Tutorials, vol.15, no. 2, 2013, pp. 843–59.

[2] S. T. Zagat, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Common. Surveys Tutorials, vol. 15, no. 4, 2013, pp. 2046–69.

[3] W. Xia et al., "A Survey on Software-Defined Networking," IEEE Common. Surveys &Tutorials, 2014, to be published.

[4] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN Security: A Survey," Proc. IEEE SDN for Future Networks and Services (SDN4FNS), 2013, pp. 1–7.

[5] R. Shea and J. Liu, "Performance of Virtual Machines under Networked Denial of Service Attacks: Experiments and Analysis," IEEE Systems J., vol. 7, no. 2, 2013, pp. 335–45.

[6] S. Sezer et al., "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," IEEE Common. Mag., vol. 51, no. 7, 2013.

[7] A. TaheriMonfared and C. Rong, “Multi-Tenant Network Monitoring Based on Software Defined Networking, “Proc. OTM Conf. Move to Meaningful Internet Systems, 2013.

[8] C.-J. Chung et al., “Nice: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems,” IEEE Trans. Dependable and Secure Computing, vol. 10, no. 4, July 2013, pp. 198–211.

[9] R. Jin and B. Wang, “Malware Detection for Mobile Devices Using Software-Defined Networking,” Proc.IEEE 2nd GENI on Research and Educational ExperimentWksp. (GREE), 2013, pp. 81–88.

[10] Y. Yu, Q. Chen, and X. Li, “Distributed Collaborative Monitoring in Software Defined Networks,” arXivpreprint arXiv: 1403.8008, 2014.17

[11] S. Shin and G. Gu, “Attacking Software-Defined Net-works: A First Feasibility Study,” Proc. 2nd ACM SIG-COMM Wksp. Hot Topics Software Defined Networking, 2013, pp. 165–66.

[12] P. Porras et al., “A Security Enforcement Kernel for Open Flow Networks,” Proc. 1st Wksp. Hot Topics in Software Defined Networks, 2012, pp. 121–126.

[13] D. Kreutz, F. Ramos, and P. Verissimo, “Towards Secure and Dependable Software-Defined Networks, “Proc. 2nd ACM SIGCOMM Wksp. Hot Topics in Soft-ware Defined Networking, 2013, pp. 55–60.

[14] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka and T. Turletti, “A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Net-works,” IEEE Common. Surveys & Tutorials, vol. 16, no.3, Third Quarter 2014, pp. 1617–34.

[15] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Avant-Guard: Scalable and Vigilant Switch Flow Management in Software-Defined Networks,” Proc. ACM SIGSACConf. Computer &Common. Security, 2013, pp.413–24.