International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 06, June-2019

DDoS Detection and Denial on SDN: A Review

Dipali S. Garge[1], Dinesh G. Harkut [2]

[1]*Computer Science And Engineering, SGBAU,*
[2]*Computer Science And Engineering, SGBAU,*

Abstract— The main aim of DDoS attack is to absorb the bandwidth of a site's of network and system and so block any other access. Software Defined Networking (SDN) is a developing area where network managers can manage the network behaviour programmatically such as modify, control etc. Using this feature we can empower, facilitate or e network related security applications due to the its capacity to reprogram the data plane at any time. A DDoS attacker could produce enormous flooding traffic in a short time to a server so that the services provided by the server get degraded. This will lose of customer support, brand trust etc. To detect this DDoS attack we use a proxy based method.

Keywords— Decision tree, identity key, proxy based request and response, DDoS prevention, user management.

I. INTRODUCTION

Distributed denial-of-service (DDoS) attacks have been a real threat for network, digital, and cyber infrastructure. These attacks are capable to cause massive disruption in any information communication technology (ICT) infrastructure. There could be numerous reasons for launching DDoS attacks. These include financial gains, political gains, and disruption.
attack is the simple and a robust technique to attack Internet and system resources. The side effect seriously affects real networks together with insect viruses. Many researches for detection mechanism have performed, because of the DDoS attack increases. The existing protection mechanisms have defense capability is exclusively limited to set of DDoS attacks. Many applications where data mining procedures can be situated in the detection of DDoS attacks.

II. LITERATURE REVIEW

This chapter reviews the literature on DDoS attack detection techniques. The review focuses on studies that have attempted to provide insight into the following questions: What is the role of techniques and how it will affect on another attack? The literature review outlines explains us the overview of our project.
During the study of existing SDN-based solutions, we observed that there are many approaches for SDN-based DDoS attack detection. Based on this study, we categorized the existing approaches according to their methods of anomaly detection.

The growing prevalence of DDoS attacks show that legacy defense mechanisms are only partially effective. List of recent DDoS attacks on various recognized organizations is provided in Table 1. These attacks are targeting almost every organization. Even leading financial institutions and government organizations, having huge IT infrastructure and resources, are unable to encounter such attacks It seems necessary to explore new paradigms that can successfully respond to DDoS attacks.

Fig.1 Phases of review protocol

Literature resource:
The inclusion in this study is as the criteria below:

- Papers that apply DDoS detection technique to detect and predict DDoS attacks in a new construction or an extension of existing techniques.
- Papers that implement the existing detection and prediction techniques or Frameworks in order to present the results and personal experience.
- The papers in networking domain.

Quality assessment:
QA1. Are the aims of the research clearly articulated?

QA2. Are the proposed techniques clearly described?
QA3. Is the literature search likely to have covered all relevant studies?
QA4. Does the research add value to the academia or industry community?

Data synthesis:
The questions were answered as follows:
[1] *Fachkha et al*. said yes, the aims of the research are clearly articulated in the study, partly; the aims of the research are partially described.

[2] *Perakovic et al*. explicitly defined a technique and extracted them from each primary study; partly only summary information about the technique is presented.

[3] *Xiao et al.* identified and referenced all journals which stated or search five or more of digital libraries including additional search strategy, partly with no additional search strategy, the author only manage to get four or five digital libraries or search is stated but only involved restricted set of journal paper and conference proceedings.

[4] *Xylogiannopoulos et al.* the paper was cited by other study and referred in the industry; P the paper was cited or referred in industry; N the paper is neither cited nor referred inindustry.

[5] *Adrian Lara et al.* we present an extensive survey of SDN-based DDoS attack detection techniques. We classify these techniques according to detection mechanisms. Classification allows better understanding and improved comprehension of the existing approaches.

[6] We identify pros and cons of each technique and elaborate key requirements of an effective DDoS attack prevention mechanism.

[7] *Nabajyoti Medhi et al*. we propose a novel SDN-based proactive DDoS Defense Framework (ProDefense) for smart city data center. ProDefense allows implementation of application-specific requirements for DDoS attack detection and mitigation. ProDefense also has distributed controllers, thereby allowing effective mechanisms for distributing load and improving reliability.

[8] *Chaitanya Buragohain et al*. we present a case study showing how Pro-Defense capabilities can be utilized to secure applications built for smart cities. Our work is significant with multiple benefits. For researchers, it provides a comprehensive analysis of the existing work and identifies challenges, whereas for academicians, it offers a thorough study of the subject. Our work is also useful for the developer community in understanding strengths and weaknesses of different solutions. The industrial community could also find our work useful in understanding the requirements and assessing capabilities of these solutions.

[9] *Hwang,Wei-Shinn Ku et al*. we present a brief overview of DDoS attacks and SDN. We categorize the existing SDN-based DDoS attack detection techniques and present a survey of these techniques

[10] *Ankur Rai et al*. we describe ProDefense which is our proposed framework for detection and mitigation of DDoS attack in a smart city.

III. PROPOSED WORK

Distributed denial-of-service (DDoS) attacks have become a weapon of choice for hackers, cyber extortionists, and cyber terrorists. These attacks can swiftly incapacitate a victim, causing huge revenue lossesWe classify solutions based on DDoS attack detection techniques and identify requirements of an effective solution. Based on our findings.
We have created different modules on which basis we can avoid DDOS types of attacks

Modules:
1) *User management*: In this module, user can able to do registration, login, Account unlocking, Get notification about account locking and uer can Send request to access application
2) *Attacks Prevention*: In this module, we proposed some preventive techniques to avoid DDOS types of attacks.
3) *Proxy based DDOS Detection:* Proxy server will be act as an intermediate server between client and server. When any user wants to send request to access application server, the request will be first transferred to proxy server. The request will be checked by the proxy server. If the request is new, the request will be transferred to Attack Detection Server. Otherwise the request will be processed and transferred to application server.
4) *DDOS prevention using Decision Tree Algorithm*- System will be trained with decision rules for different situations According to the decision tree rules, system will detect DDOS attackIf attack detected, the client machine details will be updated in database on attack detection server. Otherwise the request will be transferred to application server.

5) *Applications (Enterprise Search Engine)*- AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data.

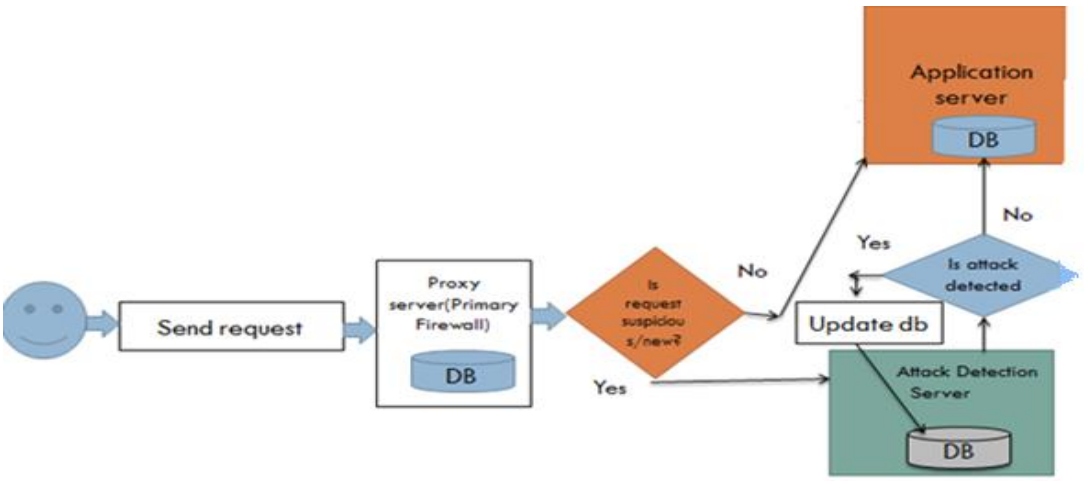

Fig.2 Flow Diagram

IV. CONCLUSIONS

In this work, we implemented a proxy based DDoS detection system for attack detection in an SDN environment. in this research we used decision tree algorithm and identity key algorithm for malicious attacks. These attacks are capable to cause massive disruption in any information communication technology (ICT) infrastructure. So here we implemented this techniques. DoS/DDoS attacks are attempt to make controller functions such as online services or web applications unavailable to clients by exhausting computing or memory resources of servers using multiple attackers In the future, we aim to reduce the controller's bottleneck and implement an NIDS that can detect different kinds of network attacks

REFERENCES

[1] Cisco Visual Networking Index Predicts Near-Tripling of IP Traffic by 2020. https:// newsroom.cisco.com/press-release-content?articleId=1771211 Accessed 14 Nov 2016
[2] DDoS Attack on BBC May Have Been Biggest in History. http://www.csoonline.com/ article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-beenbiggest-in-history.html Accessed 14 Nov. 2016
[3] Hping3. http://wiki.hping.org Accessed 14 Nov. 2016
[4] KDD Cup 99. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html Accessed 14 Nov. 2016
[5] Open vSwitch. http://www.openvswitch.org Accessed 14 Nov. 2016
[6] POX Wiki: Open Networking Lab. https://openflow.stanford.edu/display/ONL/POX+Wiki Accessed 14 Nov. 2016
[7] Tcpdump. http://www.tcpdump.org Accessed 14 Nov. 2016
[8] Tcpreplay. http://tcpreplay.synfin.net Accessed 14 Nov. 2016
[9] The Recent DDoS Attacks on Banks: 7 Key Lessons. https://www.neustar.biz/resources/ whitepapers/recent-ddos-attacks-on-banks Accessed 14 Nov. 2016
[10] Verisign Q2 2016 DDoS Trends: Layer 7 DDoS Attacks a Grwoing Trend. https: //blog.verisign.com/security/verisign-q2-2016-ddos-trends-layer-7-ddosattacks-a-growing-trend/ Accessed 14 Nov. 2016
[11] Ankur Rai, Rama Krishna Challa, "Survey on Recent DDoS Mitigation Techniques and comparitive techniques" , Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100214, August 2016.
[12] Chaitanya Buragohain, Nabajyoti Medhi, "FlowTrApp: An SDN Based Architecture for DDoS Attack Detection and Mitigation in Data Centers" ,2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN).
[13] Adrian Lara, Byrav Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking, IEEE Transactions on Network and Service Management", Vol. 13, No. 1, March 2016.
[14] Yu Chen,Kai Hwang,Wei-Shinn Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains", IEEE Transactions on parallel and distributed systems, Vol. 18,No. 12,December 2007.