UNIVERSITI PUTRA MALAYSIA

EARLY DETECTION AND MITIGATION OF DDOS ATTACKS IN SOFTWARE DEFINED NETWORKS

MUSTAFA YAHYA ZAKARIYA AL-SAADI

FSKTM 2018 26

UPM

UNIVERSITI PUTRA MALAYSIA

BERILMU BERBAKTI

EARLY DETECTION AND MITIGATION OF DDOS ATTACKS IN SOFTWARE DEFINED NETWORKS

By

MUSTAFA YAHYA ZAKARIYA AL-SAADI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Information Security

JANUARY 2018

ABSTRACT

One of the security challenges in Software Defined networking (SDN) is Distributed denial of service (DDoS) attacks that overwhelm the controller and consume its resources making it unreachable effecting the connectivity throughout the entire network. To detect and mitigate this attack at its early stages, an entropy-based DDoS attack detection and mitigation algorithm was proposed. The algorithm was written in Python programming language to be implementing on a POX controller.

To find the proper detection threshold a series of tests on different scenarios of normal and attack traffic were conducted. If the entropy of the destination IP address falls below the threshold and continue for five consecutive times it is declared as an attack. Then the algorithm was tested with attack on one host and a subnet of six hosts with attack rates of 25%, 50% and 75% for the first case and 50%, 75% attack rate for the subnet case. The attack was detected successfully without false negative alarms since the threshold was carefully chosen. Then the next step was to test the mitigation algorithm, the same above scenarios of attack were repeated and the entropy change after the mitigation was observed. The entropy increased and came close to the normal traffic entropy.

The proposed method in this project was able to detect and mitigate the attack effectively in its early stages before the intensity escalate to a degree that exhausts the controller. This algorithm was minimal in line code to make it lightweight and made use of the controller's functionality without adding extra computational burden on the controller.

ACKNOWLEDGEMENTS

All praise is due to Almighty Allah for blessing me with faith, health and patience to finish this research.

I would like to take this opportunity to express my gratitude towards the great people who have supported me throughout the phases of this research. My supervisor, Pn. Hjh Zaiton Muda for her guidance, advise and the effort she put with me over the period of this research. I would like to acknowledge all Professors and Doctors for pushing me to a greater understanding of my research topic through the courses during the preparation of the Master study. Additionally, I would like to extend my sincere thanks to the Faculty of Computer Science and Information Technology, the university library and the University Putra Malaysia.

I would like to express my heartfelt gratitude to my parents, to whom without I wouldn't be here today, thanks for your continuous and unlimited support, my family members and all my friends.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	Application Programming Interface
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
GAU	Gaussian Classifier
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IP	Internet Protocol
MLP	Multilayer Perception
NIDS	Network Intrusion Detection System
OVS	Open Virtual Switch
SDN	Software Defined Networks
sFlow	Sampled Flow
SOM	Self-Organizing Maps
SYN	Synchronization Message
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine

CHAPTER I

INTRODUCTION

This chapter provides an overview of the Software Defined Networking (SDN) architecture and the Distributed Denial of Service Attack (DDoS) in that environment which is explained in the research background section 1.1. In section 1.2 the problem being solved is stated, followed by the research objectives in section 1.3 and the research scope in section 1.4. Finally, Section 1.5 outlines the organization of the thesis.

1.1 Research Background

The rapid development of the computing technologies such as cloud services, big data and the Internet of Things (IoT) raises new challenges such as developing and implementing new network strategies to cope with the increased demand on transmission speed and higher utilization of the network resources. Software Defined Networking (SDN) being a dynamic, adaptable and cost-efficient is considered as a prospect solution for the network demands of the next-generation. SDN network architecture separates the control plane from data plane, making the network management more efficient and easier to program since a set of controllers will be dedicated to a number of packet forwarding switches (Wang et al. 2017). The mechanism of the separation of the control and data plan is as follow, the decision of whether to forward or drop the packet is the responsibility of the SDN controller while the switches instead of processing the packets themselves they look for a match in their forwarding table, each flow entry in the forwarding table has a matching rule and the action to be taken. If they couldn't find any, the contents of the packet header will be sent to the controller for decision making regarding the received packet.

The SDN controller being the core of the SDN architecture brings the benefits of the easy monitoring through the statistics collection through the whole network, the instant implementation and configuration of rules, centralized structure in a cost effective and efficient way, yet raises many security challenges (Dayal & Srivastava 2017). Distributed denial of service attacks (DDoS) is one of the highest impact threats on the SDN networks, since when the controller is compromised with a DDoS attack, it becomes unreachable to the network switches, especially with the use of botnets to launch the DDoS attack, in which a large number of packets with spoofed IP addresses are sent to a host on the network. When those packets are received by the switch and there is no match for their header in the switch flow table, they will be forwarded to the SDN controller, which will overwhelm the controller and exhaust it trying to process them to a point where the controller becomes unresponsive. Thus, the control plane is lost and the network losses its ability to process new packets (Hoque et al. 2015). Nevertheless, SDN possesses the capabilities that can cope with the DDoS threat like the global network views that the centralized control provides, the dynamic packet forwarding rule configuration and traffic analysis if utilized through a good defense mechanism.

When detecting a DDoS attack in SDN environment the time factor is very critical in mitigating the attack, if the detection process takes too long from the point of receiving the attack, the controller and the switches will be put through a large amount of attack packet to be handled to the degree that controller's resources are exhausted and becomes overwhelmed, as a result the controller is destroyed and becomes unreachable (Cui et al. 2016). Hence detecting the attack in its early stages is very important for successfully mitigating the attack. To achieve this a fast and efficient detection method is required that makes use of the controller capabilities and does not consumes a lot of the controller's processing resources.

Since one of the functions of the controller is the collection of statistics, the work in this thesis to implement an entropy based DDoS detection algorithm will utilize that function to collect another set of statistics to be added to the controller by modifying the controller's code. Entropy measures the probability of an event happening with respect to the total number of events. For the algorithm in this research the entropy will check the randomness of the destination IP addresses for the incoming packets to be used as a metric in detecting the attack. When a host or a number of hosts experience an increase in the number of received packet excessively this will result in a decrease in the randomness and the entropy as a result. This might indicate an attack when the entropy drops below a defined threshold. The threshold is set based on the normal traffic pattern and is easily adjusted while the controller is running due to the programmable advantage of the SDN.

1.2 Problem Statement

The centralized structure of SDN architecture makes the controller act as the operating system of the whole network. Despite the benefits of this architecture, it introduces many security challenges and could lead to a single point of failure, since when the controller becomes unreachable will render the whole network unresponsive to incoming traffic. One of these security challenges that possesses a large impact is the distributed denial of service attacks (DDoS).

When dealing with DDoS attack in real time scenario, usually the attack is originated using botnets. Botnets are a set of compromised devices that the attacker uses to target one or more devices on the victim's network. The attack traffic is generated using spoofed source IP addresses which make it extremely hard to distinguish the legitimate traffic from the attack traffic based on the source IP addresses and also make it useless to mitigate the attack by blocking those source IP addresses. In SDN architecture the challenge is even bigger since when the switches find a no match for the incoming spoofed packets in their flow tables they send them to the controller and the controller having to deal with that huge amount of traffic attack will get overwhelmed.

Although a lot of research has been done on securing the SDN controller against DDoS attack most of the proposed solution are either requires large computational resources or lacks the proper mitigation methods. Thus, finding a fast and efficient DDoS detection and mitigation method that can identify and stops the attack in its early stages before the controller becomes unreachable, while being light weight to not add an extra load to the controller, and consume less processing resources is critical for mitigating the attack in SDN environment.

1.3 Objectives of the study

This research studies the detection and mitigation of DDoS attacks on the SDN architecture using an entropy based algorithm through the following objectives:

1. To propose an algorithm that detect and mitigate the DDoS attack in SDN environment that is fast, reliable and lightweight.
2. To implement the algorithm on the SDN controller (POX controller) using the python programming language. And set the proper detection threshold for the entropy through different scenarios of normal and attack traffic.
3. To test the algorithm through different scenarios of normal and attack traffic with different attack intensity.

1.4 Scope of the study

This research is limited to study of DDoS attack effect and its early detection and mitigation in the SDN environment through network simulation and proposes an entropy based DDoS attack detection method and determines the entropy threshold for the proposed algorithm. Then mitigating the attack before it overwhelms the controller.

1.5 Thesis organization

This thesis is structured as follow:

Chapter 1 This chapter provides an introduction of the Software Defined Networking (SDN) architecture and the Distributed Denial of Service Attack (DDoS) in this environment as well as the problem being solved, the research objectives and scope.

Chapter 2 provides the literature review of SDN and OpenFlow architecture. The security issues of the SDN is also featured, the impact of the DDoS attack on the controller and the SDN network. And the DDoS detection and mitigation techniques for the SDN environment are also discussed.

Chapter 3 describes the methodology of the proposed solution for the DDoS detection and mitigation algorithm, how it is implemented on the controller.

Chapter 4 presents the result of the implementation of the proposed algorithm and analyse the experiment results of the simulation.

Chapter 5 concludes this research in the light of the results obtained, and future works are outlined.

REFERENCES

Big Switch Networks. (2014, Mar) Project Floodlight. [Online]. http://www.projectfloodlight.org/floodlight/

Braga, R., Mota, E., & Passito, A. (2010, October). Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Local Computer Networks (LCN), 2010 IEEE 35th Conference on (pp. 408-415). IEEE.

Benton, K., Camp, L. J., & Small, C. (2013, August). Openflow vulnerability assessment. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 151-152). ACM.

Chourishi, D., Miri, A., Milić, M., & Ismaeel, S. (2015, May). Role-based multiple controllers for load balancing and security in SDN. In Humanitarian Technology Conference (IHTC2015), 2015 IEEE Canada International (pp. 1-4). IEEE.

Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., & Zheng, X. (2016). SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 68, 65-79.

D. Erickson. (2014, Jan) Openflow. [Online]. https://openflow.stanford.edu/display/Beacon/Home

David, J., & Thomas, C. (2015). DDoS attack detection using fast entropy approach on flow-based network traffic. Procedia Computer Science, 50, 30-36.

Dhawan, M., Poddar, R., Mahajan, K., & Mann, V. (2015, February). SPHINX: Detecting Security Attacks in Software-Defined Networks. In NDSS.

David, J., & Thomas, C. (2015). DDoS attack detection using fast entropy approach on flow-based network traffic. Procedia Computer Science, 50, 30-36.

Dayal, N. & Srivastava, S., 2017. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. IEEE.

Fonseca, P., Bennesby, R., Mota, E., & Passito, A. (2012, April). A replication component for resilient OpenFlow-based networking. In Network Operations and Management Symposium (NOMS), 2012 IEEE (pp. 933-939). IEEE.

Fundation, O. N. (2012). Software-defined networking: The new norm for networks. ONF White Paper, 2, 2-6.

Giseop, No & Ilkyeun, Ra. (2009, September). An efficient and reliable DDoS attack detection using a fast entropy computation method. In Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on (pp. 1223-1228). IEEE.

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2242-2270.

Hsu, S. W., Chen, T. Y., Chang, Y. C., Chen, S. H., Chao, H. C., Lin, T. Y., & Shih, W. K. (2015, September). Design a Hash-Based Control Mechanism in vSwitch for Software-Defined Networking Environment. In Cluster Computing (CLUSTER), 2015 IEEE International Conference on (pp. 498-499). IEEE.

Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and openflow: From concept to implementation. IEEE Communications Surveys & Tutorials, 16(4), 2181-2206.

Hu, Y. L., Su, W. B., Wu, L. Y., Huang, Y., & Kuo, S. Y. (2013, June). Design of event-based intrusion detection system on OpenFlow network. In Dependable Systems and Networks (DSN), 2013 43rd Annual IEEE/IFIP International Conference on (pp. 1-2). IEEE.

Hu, Z., Wang, M., Yan, X., Yin, Y., & Luo, Z. (2015, February). A comprehensive security architecture for SDN. In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on (pp. 30-37). IEEE.

Jmal, R., & Fourati, L. C. (2014, June). Implementing shortest path routing mechanism using Openflow POX controller. In Networks, Computers and Communications, The 2014 International Symposium on (pp. 1-6). IEEE.

Kalkan, K., Gur, G., & Alagoz, F. (2017). Defense Mechanisms against DDoS Attacks in SDN Environment. IEEE Communications Magazine, 55(9), 175-179.

Katta, N. P., Rexford, J., & Walker, D. (2013, August). Incremental consistent updates. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 49-54). ACM.

Keti, F., & Askar, S. (2015, February). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. In Intelligent Systems, Modelling and Simulation (ISMS), 2015 6th International Conference on (pp. 205-210). IEEE.

Kloti, R., Kotronis, V., & Smith, P. (2013, October). Openflow: A security analysis. In Network Protocols (ICNP), 2013 21st IEEE International Conference on (pp. 1-6). IEEE.

Kokila, R. T., Selvi, S. T., & Govindarajan, K. (2014, December). DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Advanced Computing (ICoAC), 2014 Sixth International Conference on (pp. 205-210). IEEE.

Kreutz, D., Ramos, F., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55-60). ACM.

Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

Lim, S., Yang, S., Kim, Y., Yang, S., & Kim, H. (2015). Controller scheduling for continued SDN operation under DDoS attacks. Electronics Letters, 51(16), 1259-1261.

Linux Foundation. (2014, Jan) Open Daylight. [Online]. http://www.opendaylight.org/

M. McCauley. (2013, Nov) NOXREPO. [Online]. http://www.noxrepo.org/

M. Team, "Mininet," Octopress, 2015. [Online]. Available: http://mininet.org/. [Accessed 07 July 2015].

Mehdi, S. A., Khalid, J., & Khayam, S. A. (2011, September). Revisiting traffic anomaly detection using software defined networking. In International Workshop on Recent Advances in Intrusion Detection (pp. 161-180). Springer, Berlin, Heidelberg.

Mousavi, S. M., & St-Hilaire, M. (2017). Early Detection of DDoS Attacks Against Software Defined Network Controllers. Journal of Network and Systems Management, 1-19.

Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.

"openflow-spec-v1.3.0," Open Networking Foundation, 2012.

Open Networking Foundation: www.opennetworking.org (2014)

Open Vswitch. (2014, Jan) [Online]. http://openvswitch.org/

Oshima, S., Nakashima, T., & Sueyoshi, T. (2010, February). Early DoS/DDoS detection method using short-term statistics. In Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on (pp. 168-173). IEEE.

Piedrahita, A. F. M., Rueda, S., Mattos, D. M., & Duarte, O. C. M. (2015, October). FlowFence: a denial of service defense system for software defined networking. In Global Information Infrastructure and Networking Symposium (GIIS), 2015 (pp. 1-6). IEEE.

POX, "Pox openflow controller," 2014, Accessed: Sept.2014. [Online]. Available: http://www.noxrepo.org/pox/about-pox.

Prete, L. R., Schweitzer, C. M., Shinoda, A. A., & de Oliveira, R. L. S. (2014, June). Simulation in an SDN network scenario using the POX Controller. In Communications and Computing (COLCOM), 2014 IEEE Colombian Conference on (pp. 1-6). IEEE.

Saxena, M., & Kumar, R. (2016, March). A recent trends in software defined networking (SDN) security. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 851-855). IEEE.

Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013, November). SDN security: A survey. In Future Networks and Services (SDN4FNS), 2013 IEEE SDN For (pp. 1-7). IEEE.

Secdev.org, "Scapy," (22 June 2015) [Online]. Available: http://www.secdev.org/projects/scapy/.

Securelist, (6 November 2017) [Online]. Available: https://securelist.com/ddos-attacks-in-q3-2017/83041/

Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., ... & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), 36-43.

Shin, S., & Gu, G. (2013, August). Attacking software-defined networks: A first feasibility study. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 165-166). ACM.

Shin, S., Porras, P. A., Yegneswaran, V., Fong, M. W., Gu, G., & Tyson, M. (2013, February). FRESCO: Modular Composable Security Services for Software-Defined Networks. In NDSS.

Shin, S., Yegneswaran, V., Porras, P., & Gu, G. (2013, November). Avant-guard: Scalable and vigilant switch flow management in software-defined networks. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 413-424). ACM.

Tamaras, G., Athanasiou, F., & Denazis, S. (2017). Efficient topology discovery algorithm for software-defined networks. IET Networks, 6(6), 157-161.

Tri, H. T. N., & Kim, K. (2015, January). Assessing the impact of resource attack in Software Defined Network. In Information Networking (ICOIN), 2015 International Conference on (pp. 420-425). IEEE.

Tselios, C., Politis, I., & Kotsopoulos, S. (2017). Enhancing SDN Security for IoT-related deployments through Blockchain. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 303-308.

Wang, A., Guo, Y., Hao, F., Lakshman, T. V., & Chen, S. (2014, December). Scotch: Elastically scaling up sdn control-plane using vswitch based overlay. In Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (pp. 403-414). ACM.

Wang, R., Jia, Z., & Ju, L. (2015, August). An entropy-based distributed DDoS detection mechanism in software-defined networking. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 310-317). IEEE.

Wang, G., Zhao, Y., Huang, J., & Wu, Y. (2017). An Effective Approach to Controller Placement in Software Defined Wide Area Networks. IEEE Transactions on Network and Service Management.

Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). A survey on software-defined networking. IEEE Communications Surveys & Tutorials, 17(1), 27-51.

Xing, T., Huang, D., Xu, L., Chung, C. J., & Khatkar, P. (2013, March). Snortflow: A openflow-based intrusion prevention system in cloud environment. In Research and Educational Experiment Workshop (GREE), 2013 Second GENI (pp. 89-92). IEEE.

Yao, G., Bi, J., & Guo, L. (2013, October). On the cascading failures of multi-controllers in software defined networks. In Network Protocols (ICNP), 2013 21st IEEE International Conference on (pp. 1-2). IEEE.

YuHunag, C., MinChi, T., YaoTing, C., YuChieh, C., & YanRen, C. (2010, November). A novel design for future on-demand service and security. In Communication Technology (ICCT), 2010 12th IEEE International Conference on (pp. 385-388). IEEE.

Zaalouk, A., Khondoker, R., Marx, R., & Bayarou, K. (2014, May). Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions. In Network Operations and Management Symposium (NOMS), 2014 IEEE (pp. 1-9). IEEE.

Zhang, J., Qin, Z., Ou, L., Jiang, P., Liu, J., & Liu, A. X. (2010, October). An advanced entropy-based DDOS detection scheme. In Information Networking and Automation (ICINA), 2010 International Conference on (Vol. 2, pp. V2-67). IEEE.