



Electrical and Computer Engineering Department
University of Massachusetts Dartmouth

Masters of Science
Thesis Proposal

MITIGATION TECHNIQUES AGAINST DDOS ATTACKS ON SOFTWARE DEFINED NETWORKS

By: Cameron S. Whittle

Cam Whittle _____
Cameron S. Whittle
Electrical and Computer Engineering Department
M.S. Computer Engineering Graduate Student


_____07/20/2020_____
Date

Hong Liu _____
Dr. Hong Liu
Electrical and Computer Engineering Department
Graduate Advisor

_____07/18/2020_____
Date

Hernan Ulloa _____
Mr. Hernan Ulloa
Software Engineer Technical Staff
General Dynamics Mission Systems
Graduate Committee

_____07/21/2020_____
Date

 _____
Dr. Liudong Xing
Electrical and Computer Engineering Department
Graduate Committee

_____07/27/2020_____
Date

Table of Contents

Background	3
Problem Statement	4
Technical Discussion	4
Approach	5
Bibliography	6
Schedule and Milestones	7

Background

One paragraph (1/3 page) to orient the reader to the area of research.

Network Security remains one of the largest threats to National Security that Americans face every day. From threats abroad to threats at home, cyber criminals look to electronically access our personal data and hurt the citizens or companies involved. In recent years, many methods have been used to attack businesses over the internet. A prevalent one in today's society that shows no signs of going away anytime soon is DoS attacks, specifically DDoS (Distributed Denial of Service) attacks. This method of attack has become popular among a large plethora of hackers over the years, for a variety of business and/or criminal reasons. Attackers plan on overwhelming bandwidth resources, effectively freezing a system or network (Blazek 1). They create a digital traffic jam by rapidly sending more data than a system was designed to handle. This will prevent legitimate users from accessing this site and/or service when they need to, causing the company to lose money and resources.

This freezing of communication pathways also may open the system up to new vulnerabilities that were protected prior to the DDoS attack. These attacks can sometimes last days if not weeks, creating massive economic issues for affected businesses. Additionally, DDoS attacks are used quite often in the grand scheme of things. Adversaries use this technology for a wide range of reasons, from online harassing, government leverage, ransoms, or even just a “hired-gun” of sorts who does this for a living. On average, 51% of all companies, regardless of their size, have been the target of at least one denial of service-based attack. Most companies face roughly two successful cyber-attacks per week. (Mathews, Tim, “The Anatomy of a DDoS Attack”, Imperva, Jan 12 2016, www.imperva.com/blog/anatomy-of-ddos-attack/).

Botnets are the backbone to DDoS attacks, and for good reason, effectiveness. A Botnet functions like a dormant virus in nature. Usually injected into an unsuspecting front, similar to a Trojan horse, the malware can slip past the defensive of the average computer user. Once on a PC or other Internet-of-Things (IoT) device, the malware can lay dormant for as long as the botmaster chooses. The botmaster is the attacker who operates and commands the leading offensive computer (Dhayal 1). The effectiveness of this method, similarly to other methods such as phishing, relies on basic probability. The attacker is not simply targeting one person. They are targeting as many people as possible, exponentially raising the chances of infecting the highest number of personal devices. After this preparation is complete, the botmaster can decide to awaken the viruses that lay dormant. Doing so will turn all unsuspecting and infected systems into Bots, fully controllable by the botmaster. If desired, the attacker can now turn all bots onto a DDoS attack from the comfort of their own computer. These attacks are common in today's electronic age, and attackers find new techniques every year to bypass implemented defenses. The best way to mitigate future attacks is to implement scalable mitigation systems in order to stabilize the ever-changing battlefield.

Due to the ever-increasing production of household items that connect to the internet, it is nearly impossible to add sufficient protections in place localized to each device. Smaller and simpler systems may have an un-editable default password or none at all, making them a perfect

target for these IoT botnet formations. As this is an unrealistic front to attack the problem, other possible implementations must be considered to help strengthen the overall network defense.

A software-defined network (SDN) is a programmable approach to creating a dynamic and efficient cloud computing based network configuration. These SDNs use programs to simulate the hardware and firmware capabilities of traditional routers and switches in a network. Full software integration leads to many positives in the technological age, however it also means that a bandwidth attack could be even more detrimental than against the decentralized hardware counterparts. This is why SDN-specific defenses must be tested and improved upon in order to repel new DDoS techniques (Hadiano 1).

Problem Statement

One or two sentences that concisely state the problem that will be addressed by the research.

Given the prevalence and crippling effectiveness of botnets and the end DDoS attack goal, specifically on an SDN environment, an implemented dynamic solution is necessary to accurately monitor and provide security to a network of IoT devices. Implementations can be either on the host/botnet infection stage, or on the end-level target DDoS attack level.

Technical Discussion

About one page that presents some of the more important aspects of the proposed research. This should include a summary of the state-of-the-art in the particular research area.

Many personal computers have antivirus software implemented, giving them a strong defense against different types of zombie malware. However, IoT botnets similar to the “Mirai Botnet” are designed to target all kinds of internet connected systems. They can latch onto things like baby monitors, router, cameras, and more. Many devices like these do not have the same protections in place, and therefore are an easy target for creating a zombie army (Kambourakis 1). The reason for the decreased security is partially due to the devices being a lot simpler than a full personal computer system, having much less memory and hardware resources. The way in which many of these botnet systems self-propagate to new devices lies on their design. Implemented is a CnC, or command and control server. The CnC is responsible for handling and managing all of the bot devices during the infection phase. Without the attacker’s presence, the CnC effectively can store all of the bot credentials and send the bot binaries to all of the newly infected devices.

Modern DDoS attacks all perform the same end goal, however, target different aspects of a vulnerable SDN. While looking at DDoS attacks, they tend to fall into three main categories: volume-based attacks, protocol attacks, and application layer attacks. With these broad categories of course, there are some specific attacks that fall into more than one. In general, however, these are the standard categories for the DDoS attack framework. Volume-based attacks are measured in bits per second and this is where the bots attempt to overwhelm the bandwidth of the site through brute force. Protocol attacks are measured in packet per second and generally, look to consume server resources/the resources of auxiliary equipment that is essential

to the network. Lastly, the application layer attacks are measured in requests per second and target the individual application, masquerading as innocent requests (“DDoS Attacks”, Imperva, Imperva Learn, imperva.com/learn/application-security/ddos-attacks/). Within each category, there are a plethora of successful techniques that hackers use every year to freeze networks and web services.

One common example of a popular volume-based attack is the ICMP flood where a botnet sends ICMP (ping) requests as fast as possible to a network. The network will attempt to reply with echo reply packets, which only compounds the problem. At this point, both incoming and outgoing traffic is flooded, and overall performance may take a hit. An example of a protocol flood would include a TCP SYN flood. This attack exploits the three-way handshake protocol to spoof fake connections to all open ports, leaving the SDN to wait for ACK packets that are never coming. More details on examples will be delved into within the final paper.

A typical SDN operates using three layers of a computer network stack: the application layer, the control layer, and the data layer. These layers handle the actual controls of the simulated routing and switching as well as having control to monitor and validate transferring data packets (Ravindran 1). It is easy to see why these systems are becoming more and more popular in today’s world, however by design; these SDNs are particularly vulnerable to DDoS existing solely in the digital space. This is mainly due to the systems having a centralized critical failure point, the controller. Overwhelming the SDN with packets wielding spoofed IPs causes the controller to have to update the flow table faster than it has the resources to handle (Bavani 382). However, the strength of an SDN is that with control over the network through editable programs, the system admin has direct control over how they can make changes to protect the network.

Different implementations of SDNs have been designed and tested in order to help mitigate these attacks. With the ability to customize the way a network operates, the security implementations are endless. Some methods look at different network topologies while others look into active botnet monitoring and detection implementations. Entropy based solutions are an interesting idea that leads to statistical analysis on the randomness of network traffic in order to detect an attack early. Meanwhile, some defenses monitor for botnet traffic and communication of infected devices while others look to detect and mitigate the DDoS attack on the target end (Chen 1, 2). It is clear that there is no absolute solution to these types of attacks, but by critically analyzing each one, upgraded systems can be implemented to add stability and control to the environment.

Approach

One paragraph (1/3 page) that describes the methods that will be applied in conducting the research.

The first step to my master thesis will be to analyze a large array of key papers on the subject. This will be done by compiling an extensive annotated bibliography on research and implementations done by other engineers. Next, I will look into setting up an SDN in the lab space using a Linux-based virtual machine. I will be focusing on specifically implementing

common defenses for an SDN OpenFlow controller using packet filtering and attack detection approaches. While considering attacks, I will specifically be focusing on protocol attacks to look at how to protect protocol vulnerabilities in the SDN control plane. With an SDN in place, I will simulate a DDoS attack on the system to see how it behaves in an attempt to replicate the results found by others in the field.

Lastly, I will work with my graduate advisor to upgrade current implementations and test newer/combined solutions to the problem. With new data, I will analyze what works and what does not, to provide research on the ever-growing field of SDN-DDoS defense. All acquired findings and experimental data will be documented along the way to ensure that it can be compiled into a comprehensive thesis analysis.

Bibliography

MLA Format

1. Ravindran, S., et al. "An Approach to Secure Software Defined Network against Botnet Attack." IOP Science Publishing, Journal of Physics: Conference Series, 2019, iopscience.iop.org/article/10.1088/1742-6596/1362/1/012127/pdf.
2. Kambourakis, G., et al. "The Mirai Botnet and the IoT Zombie Armies." *IEEE Xplore*, IEEE Conference Publication, 11 Dec. 2017, ieeexplore.ieee.org/document/8170867.
3. Dhayal, H., and J. Kumar. "Botnet and P2P Botnet Detection Strategies: A Review." *IEEE Xplore*, IEEE Conference Publication, 8 Nov. 2018, ieeexplore.ieee.org/document/8524529/.
4. Blazek, P., et al. "Scalable DDoS Mitigation System." *IEEE Xplore*, IEEE Conference Publication, 25 July 2019, ieeexplore.ieee.org/abstract/document/8768869.
5. Hadiano, R., and Purboyo, T. "A Simulation Study of SDN Defense Against Botnet Attack Based on Network Traffic Detection." *ARNP Journals*, *ARNP Journal of Engineering and Applied Sciences*, 10 May 2018, arnpjournals.org/jeas/research_papers/rp_2018/jeas_0518_7092.pdf.
6. Su, S-C., et al. "Detecting P2P Botnet in Software Defined Networks." *Hindawi*, *Wiley Journals*, 29 January 2018, downloads.hindawi.com/journals/scn/2018/4723862.pdf
7. Dao, N-N., et al. "A Feasible Method to Combat DDoS Attack in SDN Network." *IEEE Xplore*, IEEE Conference Publication, 12 March 2015, ieeexplore.ieee.org/document/7057902.
8. Chen, K-Y., et al. "SDNShield: Towards More Comprehensive Defense Against DDoS Attacks on SDN Control Plane." *IEEE Xplore*, IEEE Conference Publication, 23 February 2017, ieeexplore.ieee.org/document/7860467.
9. Swami, R., et al. "Defending DDoS Against Software Defined Networks Using Entropy." *IEEE Xplore*, IEEE Conference Publication, 29 July 2019, ieeexplore.ieee.org/document/8777688.
10. Taha, M., et al. "Lightweight Algorithm for Protecting SDN Controller Against DDoS Attacks." *ResearchGate*, *ResearchGate Conference Publication*, September 2017,

researchgate.net/publication/322322301_Lightweight_algorithm_for_protecting_SDN_controller_against_DDoS_attacks.

11. Saharan, S., and Gupta, V. "Prevention and Mitigation of DNS Based DDoS Attacks in SDN Environment." IEEE Xplore, IEEE Conference Publication, 13 May 2019, ieeexplore.ieee.org/abstract/document/8711258.
12. Bavani, K., et al. "Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined Network." IEEE Xplore, IEEE Conference Publication, 23 April 2020, ieeexplore.ieee.org/document/9074231.
13. Dantas Silva, F., et al. "A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technology in IoT Scenarios." MDPI, MDPI Open Access, 29 May 2020, mdpi.com/1424-8220/20/11/3078.
14. Novaes, M., et al. "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment." IEEE Xplore, IEEE Open Access Journal, 18 May 2020, ieeexplore.ieee.org/document/9085352.

Schedule and Milestones

Displays a plan for completion of the project or thesis.

Research Milestone	Month/Year
Summer 2020	
Thesis Proposal, Annotated Bibliography, & Proposed Scheme	August 2020
Fall 2020	
Setup Model/Simulation of SDN and Attack	September 2020
Analyze Model & Simulations of Previous Work and Propose Changes	October 2020
Validate & Compare Proposed Changes	November 2020
Report Progress and Obtain Committee Feedback	December 2020
Spring 2021	
Draft Thesis to Committee	January 2021
Draft a conference paper	January 2021
Revise Thesis Based on Committee Feedback	February 2021
Thesis Finalizing	March – April 2021
Defend Thesis	May 2021

Tentative Schedule (subject to change)