

Project Proposal

by Daniel James

Submission date: 20-Oct-2024 08:45PM (UTC+0100)

Submission ID: 240718143

File name: 40166_Daniel_James_Project_Proposal_586419_824408616.docx (136.38K)

Word count: 1602

Character count: 9260

Securing Software-Defined Networks: DDoS Detection and Mitigation Using OpenFlow

Research Proposal
Nitheesh Kaliyamurthy

Daniel James (2218766)
2218766@student.uwtsd.ac.uk

Table of Contents

1.0 - Introduction	2
2.0 – Background to Proposed Research.....	2
3.0 – Research Problem Statement	3
4.0 – Research Aims and Objectives	4
5.0 – Methodology.....	4
5.1 – Methods.....	4
5.2 – Materials	5
6.0 – Project Plan.....	6
7.0 – References.....	7

1.0 - Introduction

Software-Defined Networking (SDN) is a modern and revolutionary architecture for networks by separating the control plane from the data plane, allowing the network to become more flexible, scalable, and programmable. The SDN controller manages all other devices and traffic within the network, making it a target to attackers. Attacks on the controller could result in the entire network becoming unusable, primarily Distributed Denial of Service (DDoS) attacks. [1]

Traditional DDoS mitigation strategies are often inadequate in SDN environments due to the dynamic nature of the networks and flow of traffic. This project aims to utilise the OpenFlow protocol to detect and mitigate DDoS attacks, this will be done through designing and testing different algorithms and strategies to identify and mitigate the effects of malicious traffic, as well as evaluating the results to verify the implementations are beneficial to the overall network performance. The importance of this project lies in its potential to improve the security of Software-Defined Networks, which are becoming much more prevalent in data centres and cloud computing environments. [2] [3]

2.0 – Background to Proposed Research

SDNs work through parting the control plane from the data plane, allowing for more centralised control of the network's traffic, programmability and configurations. This separation of control and data planes is one of the largest features of SDNs which allows for more flexibility of the network as well as greater control of traffic in comparison to more traditional networks. [4]

The split of control and data planes results in the SDN controller becoming a single point of failure for the entire network. This makes the SDN controller a target to common attacks such as Distributed Denial of Service (DDoS) attacks. The DDoS attacks will aim to overwhelm the network the network using malicious traffic, such as IP packets, which can cause congestion on the network for legitimate users or even network collapse. [1]

The centralised nature of SDNs provide great flexibility and programmability but also provide a large attack surface, paired with newer and more advanced DDoS attacks, has made implementing a real-time solution challenging. These attacks can involve overloading the network using a high volume of traffic, alternatively another strategy used by attackers involves using a lower volume of traffic which uses far less resources and, in many cases, looks like genuine traffic. This low volume tactic is much harder to detect and mitigate but can still cause performance issues on the network. More

traditional methods to mitigate these attacks, such as static thresholds, are ineffective and stopping these attacks on SDNs. [1] [5]

There are existing methods available to attempt to detect and mitigate DDoS attacks, such as SnortFlow which attempt to utilise the extensive programmability and traffic analysis to detect and mitigate attacks. These methods are effective at mitigating traditional scenarios but more complex attacks that focus on overflowing the flow tables of the OpenFlow switches which lead to denial of service. Furthermore, these methods operate through the SDN controller, which would become unusable in the event of a DDoS attack, preventing any chance of mitigation if the attack is not detected soon enough. [6]

The limitations of SDN controllers, such as single points of failure, scalability issues, and bottlenecks has been researched and a possible solution of utilising a distributed control has been discussed as a possible solution. Distributed control spreads the control pane across multiple controllers, which will work together by managing each part of their network while also communicating with the other controllers to maintain the benefits of SDN, such as programmability and flexibility. The biggest benefits of this setup are redundancy and load balancing; if one of the controllers fails during an attack, another controller can take over, increasing the resilience of the network. [7]

The OpenFlow protocol plays a major role in mitigating the effects from DDoS attacks. OpenFlow allows for the configuration and modification of rules that can be dynamically changed to forward, drop or modify traffic flow. OpenFlow also gathers real-time statistics that can be used to identify attacks before it is too late to mitigate the impact. Furthermore, OpenFlow enables certain actions during an attack such as rate limiting, blocking ports, dropping packets, and isolation to protect the most crucial services within the network while the malicious traffic is being handled. [8]

According to Dong, et al. [3] the number of Distributed Denial of Service (DDoS) attacks are rising against SDNs due to the controller being a singular point of failure for the entire network. Furthermore, Dong, et al. [3] identifies a gap in research regarding the identification and alleviation of DDoS attacks on SDNs, a gap that this project hopes to investigate.

3.0 – Research Problem Statement

Software-Defined Networks (SDNs) offer centralised control and flexibility of networks, this centralisation makes them highly vulnerable to Distributed Denial of Service (DDoS) attacks, especially through the targeting of the SDN controller. Traditional DDoS mitigation techniques are often ineffective in SDN environments due to dynamic traffic

patterns. This project aims to address this gap through the development and implementation of a real-time DDoS detection and mitigation strategy using OpenFlow.

4.0 – Research Aims and Objectives

The aim of this project is to enhance the security of Software-Defined Networks by developing efficient real-time DDoS detection and mitigation using OpenFlow, with a focus on protecting against attacks while maintaining integrity of legitimate traffic.

- Objective 1 – Implement an SDN environment using OpenFlow
 - Set up a simulated software-defined network using tools such as Mininet and an OpenFlow based controller, such as Ryu, to emulate real world conditions for testing.
- Objective 2 – Design and implement a DDoS detection algorithm
 - Develop a detection mechanism within the SDN controller to identify any abnormal traffic patterns.
- Objective 3 – Develop and test DDoS mitigation strategies
 - Implement mitigation strategies using OpenFlow to block or reroute malicious traffic while ensuring minimal impact on legitimate traffic.
- Objective 4 – Evaluate network performance
 - Assess the performance of the implemented detection and mitigation strategies, measuring deliverable factors such as detection accuracy, latency and network throughput.

5.0 – Methodology

5.1 – Methods

This project will use quantitative data, measuring network performance through measurable indicators such as latency packet loss, and detection accuracy during various DDoS attack scenarios. The creation of a simulated software-defined network using OpenFlow will allow for controlled and repeatable experiments that mimic real-world conditions.

The research strategy for this project will be a development. The project will involve designing and implementing DDoS detection and mitigation system in a Software-Defined Network using the OpenFlow protocol. The development process will include:

- Building the Software-Defined Network using Mininet
- Implementing DDoS detection algorithms on the SDN controller

- Creation of mitigation strategies using OpenFlow rules to block and reroute malicious traffic

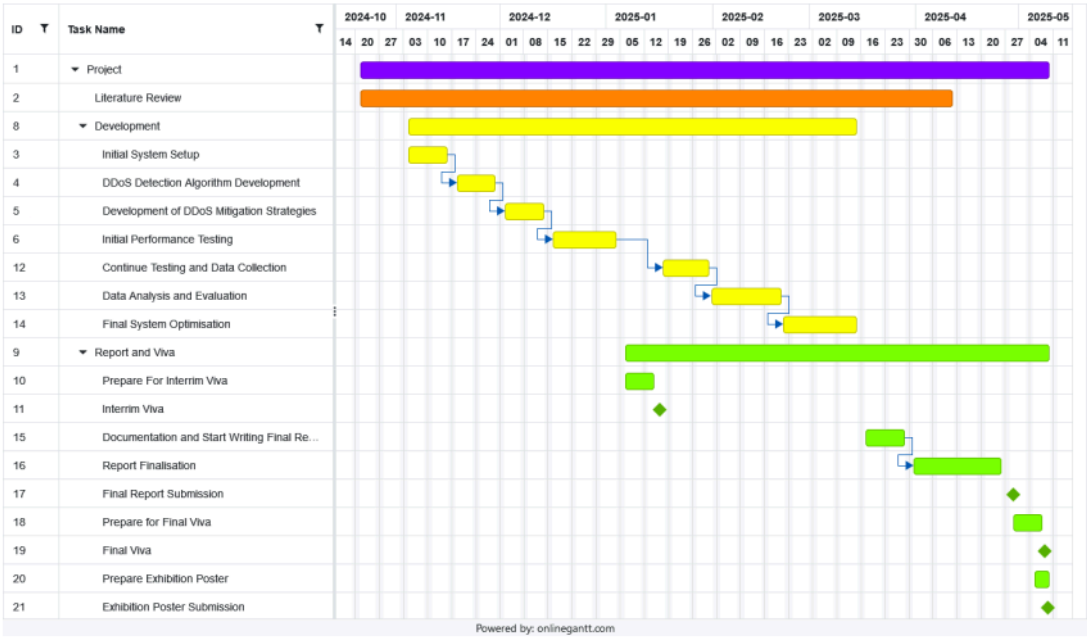
The system architecture will consist of the following:

- SDN Controller – A central controller such as Ryu to manage network flow through OpenFlow rules.
- OpenFlow Switches – Routing network traffic based on the SDN controller configurations and instructions, these will also be used for statistics and data collection.
- DDoS Detection – A element of the controller, developed using Python, to monitor and detect abnormal traffic and distinguish between legitimate traffic and DDoS attacks.
- Mitigation – Another element of the controller, to reroute or drop malicious traffic to minimise network interference.

5.2 – Materials

- Data Source and Collection: Data will be generated using simulated DDoS attacks in Mininet, OpenFlow will be used to gather this traffic statistics, such as packet count and flow entries, to evaluate performance.
- Tools and Software: The project will use Mininet for network simulation, OpenFlow and Ryu, and Python libraries. Wireshark and other tools such as sFlow will be used to aid in traffic analysis.
- Ethical Considerations: As all data will be gathered on a simulated and controlled environment, there will be no sensitive or personal data involved resulting in little to no ethical concerns.
- Hardware: A standard computer with virtualisation software, such as Oracle VirtualBox, is sufficient; no specialised hardware is required.

6.0 – Project Plan



7.0 – References

References

- [1] M. AL-Adaileh, et al., "Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller-A Review," *Access*, vol. 8, pp.1, 2020. doi: 10.1109/ACCESS.2020.3013998.
- [2] J. Cui, et al., "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," *Future Generation Comput.Syst.*, vol. 97, pp.275–283, 2019. doi: 10.1016/j.future.2019.02.037.
- [3] S. Dong, K. Abbas and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," *Access*, vol. 7, pp.80813–80828, 2019. doi: 10.1109/ACCESS.2019.2922196.
- [4] R. Sahay, W. Meng and C. D. Jensen, "The application of Software Defined Networking on securing computer networks: A survey," *Journal of network and computer applications*, vol. 131, pp.89–108, 2019. doi: 10.1016/j.jnca.2019.01.019.
- [5] A. Banitalebi Dehkordi, M. Soltanaghaei and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J.Supercomput.*, vol. 77, no. 3, pp.2383–2415, 2021. doi: 10.1007/s11227-020-03323-w.
- [6] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *J Ambient Intell Human Comput*, vol. 10, no. 5, pp.1985–1997, 2019. doi: 10.1007/s12652-018-0800-9.
- [7] F. Bannour, S. Souihi and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," *COMST*, vol. 20, no. 1, pp.333–354, 2018. doi: 10.1109/COMST.2017.2782482.
- [8] N. Z. Bawany, J. A. Shamsi and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arab J Sci Eng*, vol. 42, no. 2, pp.425–441, 2017. doi: 10.1007/s13369-017-2414-5.

Project Proposal

GRADEMARK REPORT

FINAL GRADE

/100

GENERAL COMMENTS

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student Daniel James Mark **85**

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project		
Your project proposal is well-formulated and clearly addresses the issues in SDN security. Title aligns with the proposed challenges. Aim and Objectives set well. With some adjustments to your aim and objectives, with more adequate literature reviews and setting up appropriate methodology to implement your proposal, this project has the potential to bring out valuable insights.	20	18
Background to the Project / Literature Review (400 words)		

Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts Literature review done well. However, more adequate literatures, critical appraisals could have added value to the work. To Do: + Define Keywords and Search for Literatures ScienceDirect, ACM, and IEEE (Accessible via UWTSD Library) + Do a detailed Literature review to identify existing work that focuses on DDoS Attacks and its Mitigation in SDN Environment. + Focus to get information on the dataset used, or Packet Generation Tools, Controller, Algorithms used.	20	17
Project Design (500 words)		

Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed Design proposed well. Addressed a lot of requirements to complete the work. However, more tools, parameters need to be considered. Which Packet Generating tools is proposed? Creating an algorithm or using any existing algorithms? Is it kind of AI based security proposal? To Do: + Benchmark the existing literature and try to re-create a similar design + Creating an Algorithm to implement a DDoS attack is challenging with the Time Limit you have. + Use the existing Algorithm and test. + Maybe consider experimenting 2 or more methods from the existing literatures and analyse its performance in mitigating DDoS attacks.	30	25
--	-----------	----

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8
