CHAPTER 1
INTRODUCTION

1.1 Background

SDN is network management technology in which enables centralized network monitoring and centralization of security and policy control to improve performance and monitoring network [1]. Even though the SDN can improve the performance of the network, there are still security threads in SDN network one of them is DDoS, DDoS is a well-known cyber-attack that make the network source or network server unavailable by disrupting the services by sending a large amount of data or pinging the server with several hosts simultaneously.

Confidentiality, Integrity, and Availability (CIA) is a security requirement in which the model guides policy in network security [2]. Confidentiality is mean that the privacy of our data must be secured from people that threaten our data security. Integrity is mean that data that we save cannot be changed or modified by an unauthorized person. Availability is mean that service that cloud computing over should be available and can be accessed anytime and anywhere. Availability is crucial among the triad pilar of security since the core function of the network is to provide on-demand service of different levels. DDoS (Distributed Denial of Service) and DoS (Denial of Service) flooding attacks are a threat for the Availability because DDoS can make the server and network resource unavailable to its intended users.

SDN has the features in Defeating the DDoS attacks [1] such as Separation of the control plane from the data plane, by separating the data plane from the data plane it enables establish easily, large scale attack and defense, logically centralized controller, this feature helps to build the consistent security policy, There are several ways to overcome the DDoS in SDN, the most effective and efficient way to overcome the DDoS attack however is to preventing the DDoS flood attacks the server (source) of the network. Source-based defense mechanism means to prevent the DDoS attack attacking the server and filtering the IP address of the network from anomaly traffic.

SVM (Support Vector Machine) on the other hand, can classify and can predict the incoming data based on the learned data. This thesis offers SVM that combined with the RYU controller and can be used to prevent the DDoS attack from attacking the server of the network by analyzing the incoming traffic and classifying the traffic

to determine whether it was normal traffic or DDoS traffic based on the learned traffic data, and the RYU controller blocking the port of the attackers based on data from SVM.

1.2 Problem Formulation

1. DDoS attack interrupting the network service between the server and the client by attacking the server.
2. Even though the SDN has a built-in firewall, the firewall can only overcome the DDoS attack with fixed IP whereas most of DDoS attack using random IP.

1.3 Purpose

The following is the purpose of this research:

1. To measure the impact of DDoS attack on the server.
2. Mitigating the DDoS attack by filtering the packet of incoming traffic in the source of the attack by using SVM that combined with RYU controller.
3. Measuring the throughput, downtime, and recovery time of the server after the SVM with RYU controller mitigated the DDoS attack.

1.4 Scope of Research

The topology used is tree topology with 1 controller, 5 switches, and 16 hosts. The traffic load that is used in the simulation is TCP protocol with 10 Mbps bandwidth and the DDoS attack that is used in the simulation is a TCP flood attack with a 100s attack time.

1.5 Research Methodology

This thesis uses methodologies :

1. Literature study, data from several networking journal get collected and selected which journal is more relevant to SDN security.
2. Simulation, Creating the topology on Mininet.

3. Examination, attacker attack the server TCP flood DDoS .
4. Prevention, preventing DDoS attack using source-based defense mechanism with SVM combined with RYU controller.
5. Analyzing, analyzing the impact of DDoS in the simulation.

1.6 Structure of Thesis

The rest of this thesis is describe as follow :

- Chapter 2 BASIC CONCEPT
  This chapter explains explain about what is SDN (Software Defined Network), what is DDoS (Distributed Denial Of Service), and what kind of defense mechanism is commonly use in the SDN
- Chapter 3 SIMULATION DESIGN
  This chapter explain how the model, workflow, architecture, and system design of the simulation.
- Bab 4 RESULT ANALYSIS
  This chapter analyze the impact of DDoS
- Bab 5 CONCLUSION AND SUGGESTION
  This chapter is Conclusion and Suggestion