A proposal of a real-time OpenFlow DDoS detection tool

Laboratory for Software Design & Analysis
established in 2005

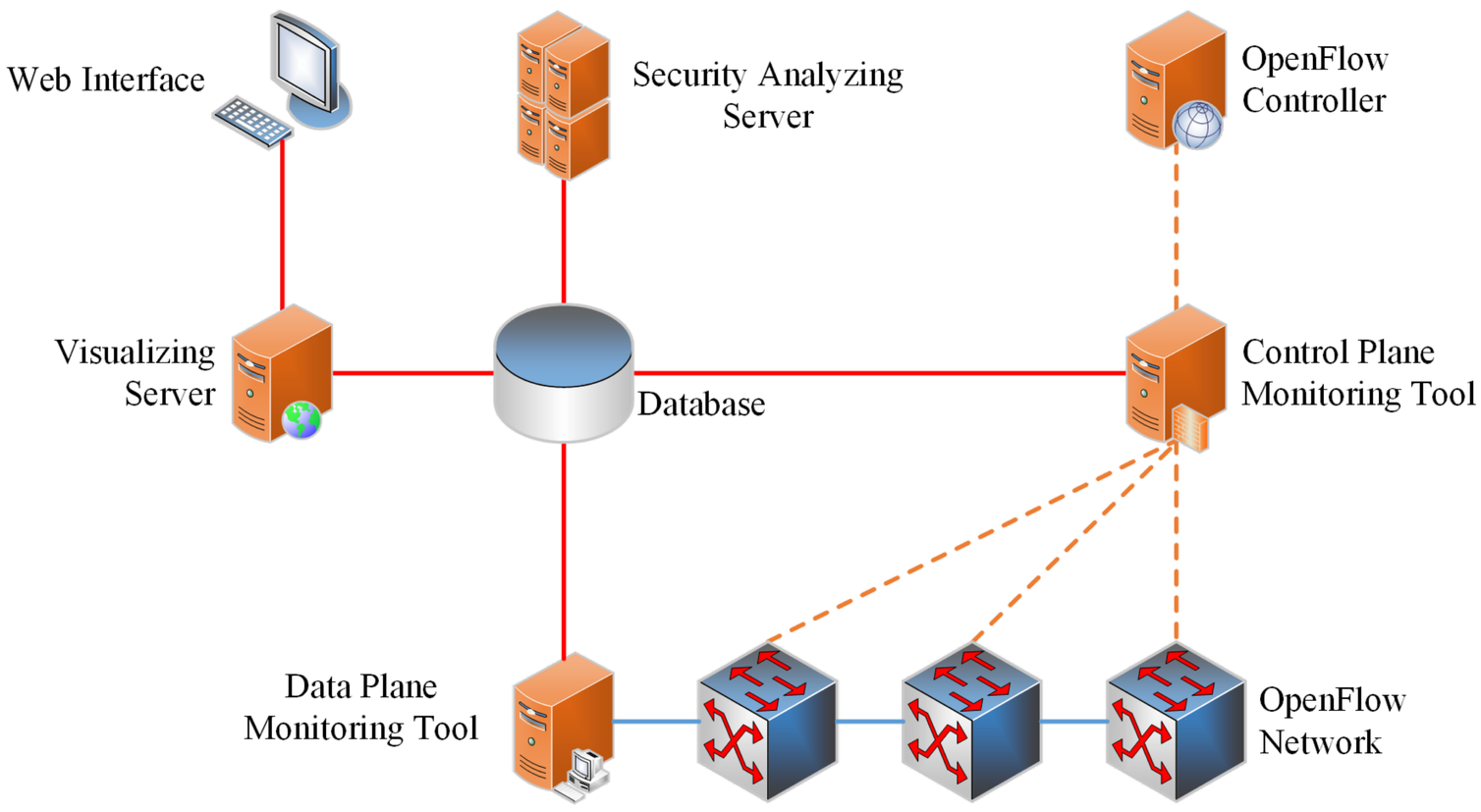
Wassapon Watanakeesuntorn, Kohei Ichikawa, Hajimu Iida, Putchong Uthayopas

Introduction

Distributed Denial of Service (DDoS) is one of the cyber attacks on the computer network. The attacker floods a huge network traffic from many sources to a target server for interrupting the service. This study aims to improve DDoS detection in Software-defined network technology. In the traditional network, it has only data plane dataset to recognize the cyber attacks. However, In SDN, control plane dataset is available in addition to the data plane dataset. Control plane is used to communicate between a centralized network controller and network switches. OpenFlow protocol is most widely adopted for the communication. DDoS detection on the SDN can use the data plane dataset together with the control plane dataset. We aim to apply deep learning techniques to detect DDoS attacks in the OpenFlow network. For the purpose, we plan to apply machine learning mechanism to a monitoring tool, Opimon, which we have developed previously.

Design and Development

Opimon is a monitoring tool which we developed in previous work. It monitors OpenFlow messages between OpenFlow controller and OpenFlow switches with a proxy monitoring tool and visualizes the monitored information on the web interface. In this study, we purpose to implement a security analyzing module for Opimon to introduce security mechanism in the OpenFlow monitoring. We aim to use deep learning techniques to analyze the traffic and detect DDoS attacks in the network.

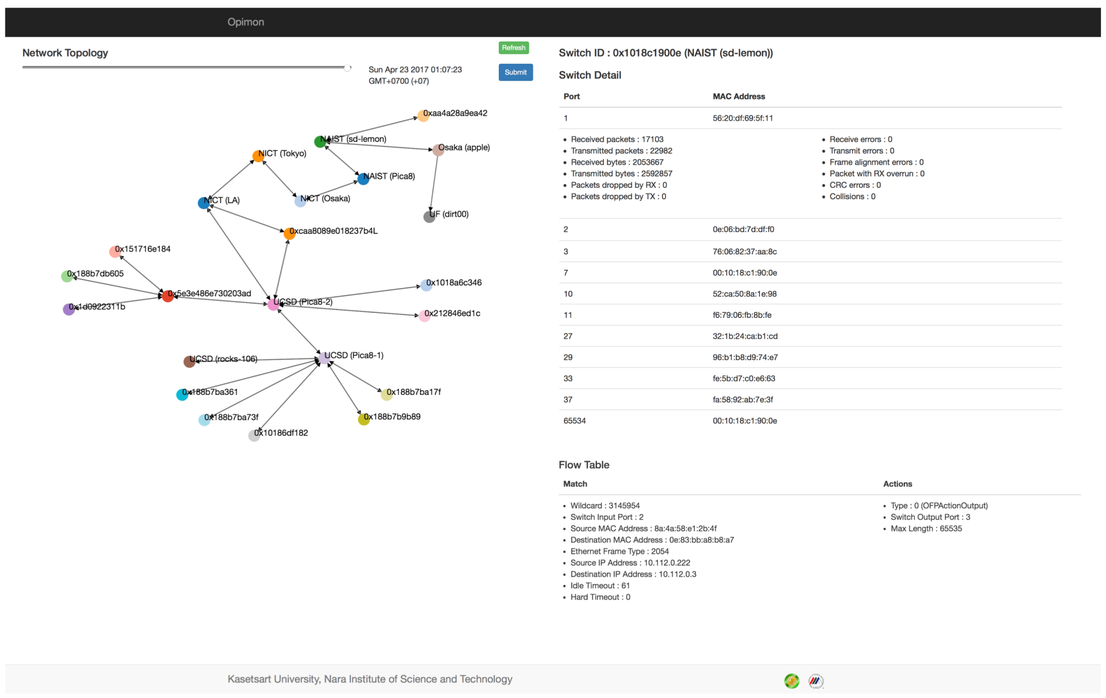


The security analyzing module is a server for analyzing traffic with data plane and control plane dataset with deep learning techniques. On the development, we use DARPA dataset, which is a DDoS dataset in the data plane. We also generate the control plane dataset by simulating an OpenFlow network using DARPA dataset. We use the both datasets of control plane and data plane to train the learning model in the security analyzing module.

The results are evaluated by the detection accuracy in case of using data plane dataset only, using control plane dataset only, and using the both plane datasets. We also aim to optimize this method to be a real-time DDoS detection with unsupervised learning.

Progress and Expected Result

Currently, we try to generate a control plane dataset by simulating an OpenFlow network with the DARPA dataset on an OpenFlow network. An Open vSwitch is used to simulate the network. We collect multiple control plane datasets by using different controllers for comparing the model and evaluating the accuracy of the detection. We generate control plane datasets by replaying DARPA dataset using tcpreplay. Opimon is used to monitor and collect the OpenFlow messages on the control plane.



We aim to develop a deep learning model which is an unsupervised learning machine for DDoS detection in the OpenFlow network. The deep learning model is integrated into the Opimon to detect and alert DDoS attacks on the web interface. We try to optimize this detection to be a real-time detection to help the developer and administrator for detecting DDoS attacks in the OpenFlow network.