**SDN Project Proposal**

**CS 6301 – 503**

**Members:**

Juhi Bhandari

Stephen Blystone

Taniya Riar

Ishwank Singh

**Project Summary:**

Our project has two main parts. For both parts we will setup a network using Mininet and use ONOS as the controller.

1. For the first part, we plan to integrate an open-source Firewall/IDS into the network. We will inject attacks into the network and determine if the Firewall/IDS can catch them.
2. For the second part we will remove the open-source Firewall/IDS from our network. We will instead train a Machine Learning algorithm to identify traffic that is “hostile” and should be dropped.
   1. We will create a ONOS Application in Java to communicate with the ONOS controller. Our Application will receive packet information from the controller, run the information through our Machine Learning Algorithm, and request the controller to drop/allow the traffic accordingly.

**Tools used:**

**Network:** Mininet

**Controller:** ONOS 1.12

**Intrusion Detection System (IDS):** currently investigating pfSense or Snort

**Current Progress (as of 2/11/2018)**

Tasks Currently Completed:

1. Mininet working
2. ONOS controller compiled, installed and working
3. Understand the ONOS architecture
4. Ran shell script to create a Template ONOS Application
5. Studied sample ONOS Applications from the ONOS GitHub

Tasks Currently in Progress:

1. Understanding the ONOS API and determining what we need to extract
2. Writing our Application that calls the ONOS API
3. Investigating pfSense and Snort and how to integrate into our network
4. Determining the network topology we will use to test.
5. Writing Python Code for creating the Mininet network topology

Future Tasks:

1. Determine how to get training data for our Machine Learning Algorithm. This is dependent on the information we can extract from the ONOS API.
2. Write our Machine Learning Algorithm and integrate that into our ONOS Application