Preventing Network Attacks through Deep Learning and SDN Integration

Abstract:

The continued growth of connected devices and increasing reliance on digital infrastructure will lead to an increasing number of cyber-attacks on networks. Traditional security solutions such as firewalls and intrusion detection systems will become less effective in defending against these attacks. In this project, we will use a deep learning model-based solution for detecting and preventing network attacks in a software-defined networking (SDN) environment. We will use a popular deep learning framework, to train a deep learning model based on a DDOS attack network security dataset collected from Kaggle. The model we will use is a Convolutional Neural Network (CNN). The trained model will be integrated into the SDN environment, and using Mininet we build a network and we perform attack generation on the network and the data is tested with the trained model to predict the attack. This will be used to control the behavior of one or more SDN controllers to prevent attacks. The performance of the proposed solution will be evaluated using a simulated network environment and real-world network security datasets. The results will demonstrate that our solution is effective in detecting and preventing network attacks, and has the potential to significantly enhance network security.

Keywords: SDN Environment, DDOS attack, CNN Model, and RYU Controller.

<table>
<tr><td>Student Names Numbers and Signatures</td><td><table><tr><th>Roll Number</th><th>Student name</th><th>Student Signature</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Research Group</td><td></td></tr>
<tr><td>Application Area</td><td></td></tr>
<tr><td>Name or the Signature of the Guide</td><td></td></tr>
<tr><td>Name or the Signature of the Mentor</td><td></td></tr>
</table>