UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Defence

Tuesday December 21, 2021 at 10:30am via Zoom

Harsh Mandali

Transfer Learning based Intrusion Detection System

Chair: Dr. Fei Song
Advisor: Dr. Charlie Obimbo
Advisory: Dr. Xiaodong Lin
Non-Advisory: Dr. Deborah Stacey

Abstract:

In recent times, organizations have faced many cyberattacks daily. The Internet is the main means of these attacks. Between the time an attack occurs, is detected, and a remedy is found and implemented, a lot of damage might have been done. Thus, there is a great need to get much faster detection and remedial times.

In networks, an Intrusion Detection System (IDS) is a major component in alleviating these attacks and securing organizations from these attacks. For this reason, much research is being done to develop IDSs that can evolve rapidly to detect these attacks, and especially day-zero attacks. The traditional approach has been that once new attack vectors are detected, the models are re-trained to determine these specific attacks and to determine their threat level.

This thesis proposes the use of Transfer Learning in the aspect of Deep Learning for Intrusion Detection. Transfer Learning allows learning from existing models. This research focuses on how developing Inductive Transfer Learning based on fine-tuning can affect the overall results of an IDS. A total of four source models are developed for detecting target Heartbleed and DoS attacks as below:

- DNN Model for Port Scan Attack
- DNN Model for Botnet, DDoS, and Port Scan Attacks
- CNN Model for Botnet, DDoS, and PortScan Attacks
- LSTM Model for Botnet, DDoS, and PortScan Attacks

Each model is transferred to learn about the target domain. Proposed methodology is evaluated for different training sizes of target domain. Out of the proposed 4 base models, the best result is acquired using PortScan based DNN model. Experimental results show that with 15% training data, the transfer learning based deep learning model achieves the best F1-score of 96.8% that is at least 10% more than the normal deep learning model as well as machine learning algorithms. The detection time of these models is observed to be approx. 0.5 seconds inferior to normal deep learning models.