UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MsC.CS Seminar

Wednesday January 27, 2021 at 10:00AM on Zoom

Real-time Network Intrusion Detection System

Harsh Mandali

Advisor: Dr. Charlie Obimbo
Advisory Committee: Dr. Xiaodong Lin

ABSTRACT:

Nowadays, organizations face many cyberattacks almost every day. An Intrusion Detection System (IDS) is a system that can help organizations detect these attacks. In the past two decades, there is a great amount of research going on in this area due to its significance. This progress has helped to improve the classification methods to detect various kinds of attacks, such as Denial of Service, Man in The Middle, and Phishing, etc. However, many of the proposed techniques are not feasible to work in real-time. Because the execution time of detecting the network is more, this can provide access to intruders. Recent statistics also show that attacks are on the rise.

Our main objective is to research and build methods of improving the detection of malicious network payloads. This will entail:

1. Finding a faster way of detecting malicious payloads.
2. Using a dataset like CICIDS2017 (Made in Canadian Institute for Cybersecurity at University of New-Brunswick) that can provide an actual-time environment for our models.
3. Designing models with combinations of algorithms that reduce the number of false positives and false negatives.
4. Validating models in a certain time frame ‘t’ and comparing them against their performance concerning speed, accuracy, and false-positives.

In our study, we are aiming to use Self-Organizing Map, Auto Encoder, Generative Adversarial Networks, Multilayer Perceptron, and Learning Vector Quantization. The proposed system will be designed in a way that can detect intrusions in real-time as well as reduce the number of False Positives and False Negatives.