UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Tuesday December 3, 2019 at 10:00AM in Reynolds, Room 2224

A Deep Learning-based Framework for Cyber Attack Detection in Industrial Control Systems

Sanaz Nakhodchi

Advisor: Dr. Ali Dehghantanha

Co-Advisor: Dr. Hassan Khan

Committee Member: Dr. Luiza Antonie

ABSTRACT:

Critical infrastructures such as power systems, gas pipeline, water and transportation are playing a significant role in supporting our day-to-day activities. These critical infrastructures are increasingly connected to public networks which expose them to a wide range of cyberattacks. Advanced Persistent Threat (APT) actors and state sponsored hacking groups are consistently targeting our defense, energy, transport, health and financial infrastructure. In 2015 BlackEnery3 attack against Ukraine's power grid system caused blackout for more than 230,000 homes. In 2018, vulnerabilities detected in critical infrastructure rose by 14% and about 90% of organizations handling critical infrastructure reported at least one compromised in the past two years. These critical infrastructures are heavily relying on Industrial Control Systems (ICS) for providing uninterrupted services. Connecting ICS devices to public networks in order to boost operational efficiency significantly increase the risk of cyberattacks.

In ICS, cyber attacks can be detected in Information Technology (IT) layer or in Operational Technology (OT) layer. Detection in IT layer is based on characteristics such as IP address that the device is connecting to, domain name, application calls, etc. Based on Pyramid of Pain (PoP) theory, it is relatively easy for attackers to change their attack properties at IT layer and bypass detection. However, changing OT layer properties such as voltage, power consumption, etc. is much more difficult. Moreover, considering the number and geographical distribution of ICS devices in critical infrastructure networks, the capacity for human-based cyberattack detection is very limited and we require machine learning-based solutions.

The goal of this study is to develop a deep learning-based framework for accurate detection of seen and unseen cyberattacks in industrial control systems at OT layer. Firstly, we offer a deep supervised model for accurate detection of previously seen cyberattacks. We are mixing the Convolutional Neural Network (CNN) and Bag of Feature (BoF)-based pooling to build a model for accurate detection of previously seen cyberattack. Secondly, we develop an unsupervised Deep Support Vector Data Description (Deep SVDD) model on kernel-based mode for detecting unseen attacks. Three standard datasets namely Power system, Gas Pipeline and Water Storage Tank are used to evaluate results of this research. We are reporting our models accuracy (how far the methods could detect attacks accurately), precision (ratio of predicting cyber-attack that are correctly labeled as attack), recall (ratio of cyber-attack samples that are correctly predicted) and F1 score (the harmonic of precision and recall).
The results of our research may make a significant impact on protecting critical infrastructure such as power systems, gas pipeline, oil transportation etc. against cyberattacks.