**ANOMALY DETECTION FOR CYBER PHYSICAL SYSTEMS SECURITY**

**BACKGROUND MOTIVATION**

Cyber-Physical Systems (CPS) are computer-based systems that monitor and control physical processes using embedded sensors, actuators, control processing units and communication devices. They characterize many critical infrastructures sustaining our modern society. CPS are typically large scale and consist of highly interconnected hardware and software components, whose objective is to enable ease of management for sensor-based communication-enabled autonomous systems. Examples include nuclear power plants, water distribution plants, water purification plants, networks of autonomous cars, electric power distribution, oil and natural gas distribution, etc.

As such, the reliability of CPS is critical in ensuring that the lives are not threatened. Reason being as CPS become increasingly connected to the internet for remote monitoring and control, they become vulnerable to cybersecurity attacks on their communication channels, which may lead to physical consequences in the forms of service disruptions and failures. One prominent case study is the Stuxnet ***<cite>*** worm that was launched against an Iranian Nuclear Power plant which caused the centrifuge to operate in an anomalous manner. Cybersecurity attacks such as this can have potentially devastating impacts on human lives, geopolitical stability, etc.

Hence, it is essential to protect the integrity of CPS and ***anomaly detection is one of the critical cybersecurity measures in CPS.*** This is an area which we propose to investigate in the project.

**PROJECT OBJECTIVES**

We propose to explore the application of machine learning for anomaly detection in Cyber Physical Systems. The motivation to embark on this is because we would like to appreciate the real world uses of machine learning in the area of cybersecurity and explore the potential it has. We would also like to experience firsthand how machine learning algorithms should be implemented from start to finish in an applied context.

There are 2 potential CPS contexts for applying machine learning for anomaly detection. As part of our plan, the team plans to assess both contexts prior to deciding on one. The 2 contexts are described as follow:

1. Potential Context 1: The context here will be a water distribution network. We will work with data sets from the BATADAL design challenge, which is based on a fictitious water supply system of a town. This system closely resembles that of a real setting and contains multiple sensors and actuators that enable water sources to serve customers spread throughout the network. Different processes, representing distinct stages of the water supply system (extraction, treatment, delivery), will take place simultaneously. Attackers may compromise one or more components of this system and the goal of an anomaly detection algorithm is to monitor the operation of the water distribution system using time-series data collected from the sensors and actuators to raise an alarm when an attack is detected. The BATADAL dataset ***<cite>*** comprises of data of the different sensors and actuators in a fictitious Water Distribution Plant of C-Town. It contains 43 different sensors/actuators spread across the entire C-Town and it can also be broken down into its different processes, targeting different parts of C-Town.
2. Potential Context 2: SWaT is a fully operational scaled down water treatment plant that can produce 5 gallons/minute of filtered water. SWaT is a six-stage filtration process that mimics a large modern water treatment plant. The SWaT dataset consists of seven days of normal continuous operation and four days with attack. A total of thirty-six attacks were conducted during the four days, and is the most updated and complex open source dataset till date. The data consists of all the sensors and actuator values over the said duration.

**PROJECT PLAN OUTLINE**

This project will be executed in these stages:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Work Stage | | Description | Timeline | AB | Marcus | Ming Qing |
| 1 | 1.1 | Understanding nature of CPS contexts | 2 wks | Joint discussion to decide on which CPS context to use | | |
|  | 1.2 | Source for prior works on anomaly detection | Individual survey & consolidate | Individual survey & consolidate | Individual survey & consolidate |
|  | 1.3 | Explore different ML algorithms | Study 1 candidate algorithm | Study 1 candidate algorithm | Study 1 candidate algorithm |
| 2 | 2.1 | Data preprocessing & selected CPS architecture | 1 wk | Joint work to analyse data & CPS architecture.  Setup data preprocessing pipeline. | | |
| 3 | 3.1 | Implement selected ML algorithm | 3 wks | Joint work to design ML pipeline and implement the necessary algorithms within pipeline.  Collect results | | |
| 4 | 4.1 | Write report/paper | 1 wk | Draft respective sections & collate. | Draft respective sections & collate. | Draft respective sections & collate. |

**EXPECTED OUTCOMES**

At the end of this project, we aim to be able to effectively detect anomalies in our chosen dataset, by using the anomaly detection algorithm that we implemented. We envision that effectiveness would be measured by the amount of time it takes to detect the anomaly from the time it was first launched, and by the number of false positives and negatives that resulted from this algorithm. Furthermore, we would have explored the different approaches of anomaly detection in Cyber Physical Systems by studying different machine learning techniques and their associated pros and cons respectively.

**EXPECTED RISKS**

* As the CPS context is new for us, understanding the nature of CPS (e.g. C-Town, SWaT) and its infrastructure will require some time for us to contextualise the machine learning task.
* Learning may be tricky due to the high dimensionality of the dataset and may require good features selection process. Noisy data might be an issue.
* Implementation of anomaly detection machine learning algorithms may be non-trivial.