**Date: 24/06/2021**

**Project Title: Reinforcement Learning with Drift Detection for Autonomous modelling in IoT and industrial IoT environment.**

Idea: Learning from the dataset of IoT and Operational Technology(OT), this learning is useful for understanding the way industrial devices should be place, how should they communicate, and further in attack scenarios, learning the model with normal/benign and attack data will give solution to detect the abnormal behaviour in the system.

Outcome of the work: Anomaly based detection system, which detects change in system behaviour and report to the controller.

Research Questions to Answer:

1. Can we identify the attacker is remote or insider?
2. Can we identify is it a fault, failure or attack?
3. Can we inform the ICS operator in real time about the attack?
4. Does legitimate change in data flow can be distinguish with changes due to Attack?

Initial Requirement:

Looking for data contain both Benign and Attack data

To perform learning, first challenge is to get the correct dataset.

There are two sets of dataset with which we can move forward.

1. Collection of dataset like network dataset, simulation or real testbed environment variable measurements.
2. Binaries of the executable run on controllers of OT and IoT devices.

Implementation:

Cleaning of dataset: Removing unwanted features, Avoiding Null values

Pre-processing of data : Normalizing the data values, selection of useful features.

Link to clean and preprocess

<https://erainnovator.com/data-preprocessing-with-python/>

Machine Learning Model.

Reinforcement Learning:

Reinforcement learning (RL) is an area of machine learning concerned with how intelligent agents ought to take actions in an environment in order to maximize the notion of cumulative reward. Reinforcement learning is one of three basic machine learning paradigms, alongside supervised learning and unsupervised learning.

Concept Drift:

In predictive analytics and machine learning, the concept drift means that the statistical properties of the target variable, which the model is trying to predict, change over time in unforeseen ways. This causes problems because the predictions become less accurate as time passes. The term concept refers to the quantity to be predicted.

Methodology

Look to generate attack graph from the dataset(look into python for generating attack graph), that will take as input to model, reinforcement learning model will also incorporate drift detection to increase accuracy, ultimately a behaviour based detection system will be generated, there will be a controller that listens the model output and generate alarm in case of anomalous behaviour.

Training and Testing:

There are two modes of training.

1. Offline Training
2. Online Training

Results:

Compare the existing work with state of the art solutions.

Use of concept drift and online training advantages

Discussions:

Answer the stated research question before the start of research work.

Conclusions:

Future research questions:

Learning only from online dataset challenges?

Whether it is important to have in-house set up with our own dataset?