

Accurate and Efficient Cyber Attack Detection in Water Filtration Systems using Machine Learning

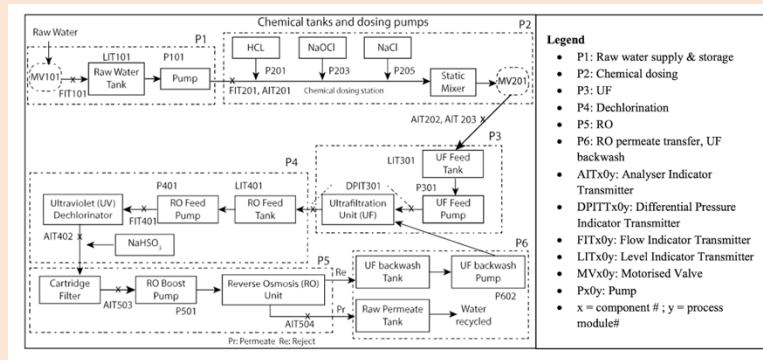
Clemson University, Department of Industrial Engineering, Clemson, SC 29634

Chloe Crozier, Janhavi Deshpande, Sumanth Pandiri, Mathew Werner, and Dr. Dan Li



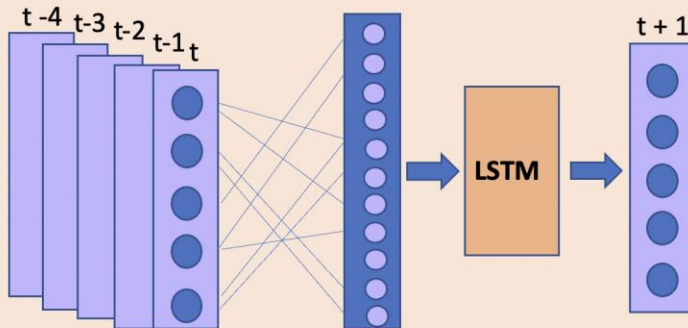
Introduction

- Industrial CPSs are prone to cyber attacks.
- Focus is on water filtration systems.
- Train LSTM models to detect attacks.



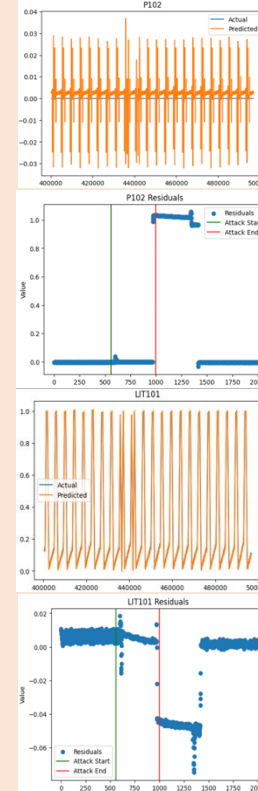
Methods: LSTM

- Two different models.
- First model uses 5 stages from a singular stage.
- Second model implements a total of 12 sensors from each of the 6 stages

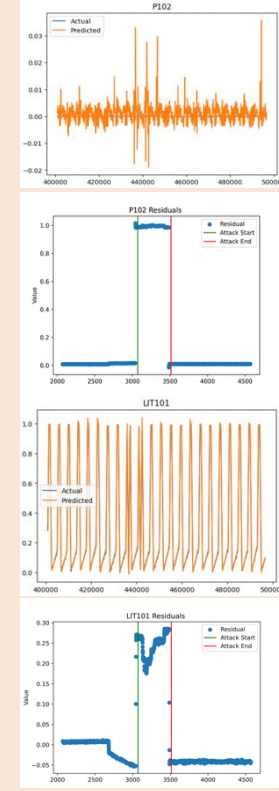


Results

Single-Stage



Multi-stage



Future Steps

- Decrease the sensitivity of the current model when sensor is not under attack.
- Create a LSTM model where one stage predicts itself and the next stage.

References

- Goh, J., Adepu, S., Tan, M., & Shan, L. Z. (2017). Anomaly detection in cyber physical systems using recurrent neural networks. Retrieved March 27, 2023, from <https://ieeexplore.ieee.org/abstract/document/7911887>
- Al-Abassi, A., Kaimpour, H., Dehghanianha, A., & Patel, R. M. (2020, May 4). An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. Retrieved March 27, 2023, from <https://ieeexplore.ieee.org/document/9086038>