sce Tech Fest 25
Innovation Sustainability Community

Computer Sciences

Students: Michael Kaminer
Advisor: Dr. Aviad Elyashar, Prof. Shlomo Greenberg

SCE
SHAMOON COLLEGE OF ENGINEERING

Introduction

Industrial Control Systems (ICSs) are increasingly targeted by cyberattacks due to their critical role in national infrastructure.
Detecting anomalies is crucial to maintaining security.
This project investigates the potential of **Spiking Neural Networks (SNNs)** for anomaly detection in ICS environments, and whether they can outperform or complement traditional machine learning algorithms.
Experiments were conducted using several ICS datasets (SWAT, WADI, BATADAL, EPIC), and auxiliary datasets (ECG5000, TON_IoT, Tennessee, MNIST), leveraging the **SNN Torch** framework.

Results/Highlights

Working with multiple anomaly datasets was complex due to inconsistent labeling and structures.
Standalone SNNs underperformed due to lack of mature architectures and training difficulties.
Hybrid models (SNN + ML) showed improved performance and generalization.
SNNs contributed to **feature richness** when integrated with other models.

Methods.
Trained multiple models (ML, DL, SNN) on ICS and auxiliary datasets.
Used **SNN Torch** to implement biologically-inspired spiking neural models.
Benchmarked performance using metrics like **accuracy, precision, and recall**.
Evaluated **hybrid architectures** combining SNNs with ML classifiers.
Addressed challenges in dataset preprocessing and model generalization

Conclusion

This project demonstrated that while standalone SNNs are not yet mature for practical anomaly detection in ICSs, **hybrid approaches** provide promising results.
SNNs can play a valuable role in **ensemble systems** where robustness and accuracy are critical for cybersecurity in industrial environments.

Project Goals:

To assess the suitability of SNNs for anomaly detection in ICSs and evaluate whether they perform better as standalone models or in combination with traditional ML/DL models.