Comprehensive Exam - Question #1

Rob Gillen

Question

Select one of these 2 papers (*Anomaly detection in cyber physical systems using recurrent neural networks*[1] or *Checking is believing: Event-aware program anomaly detection in cyber-physical systems*[2]), and critique it and the work described in it. Then describe how the potential methods and measurements you want to investigate would aide in evaluating the sceptibility of their proposed approach. Then, in one of the real-world domains you want to explore, discuss how the author's proposed approach compares and contrasts to what you are proposing to do.

Answer

Anomaly detection in cyber physical systems using recurrent neural networks

In this paper, the authors present an approach to detecting anomalous traffic in a cyber-physical system.

- unsupervised
- RNN as a time-series predictor
- cumulative sum method to identify anomalies
- "majority" of attacks
- "low" false-positive rate
- Utilize Long Term Short Term Memory RNN (LSTM-RNN) to correlate time series data

Contributions

- Modelling normal behavior in CPS using an unsuperivsed, deep learning approach
- identify the sensors that exhibit the anomalous behavior
- validation of the approach on the Secure Water Treatement Testbed (SWaT)

Novelty

- Work is in water critical infrastructure, specifically SWaT
- This environment reflects the complexity normally found in a real-world plant
- approach uses time-based neural networks to consider sequence of information
- not only detects anomalies, but also the source (sensor in question)

Review

asdf

how would my work measure/evaluate the suseptibility of their approach

Using a real-world domain I'm going to explore, how does the author's proposed approach compare/contrast to my work

Checking is believing: Event-aware program anomaly detection in cyber-physical systems

Review

asdf

References

[1] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *2017 ieee 18th international symposium on high assurance systems engineering (hase)*, 2017, pp. 140–145.

[2] L. Cheng, K. Tian, D. Yao, L. Sha, and R. A. Beyah, "Checking is believing: Event-aware program anomaly detection in cyber-physical systems," *CoRR*, vol. abs/1805.00074, 2018.