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. They begin by describing the problem and providing a broad overview of their approach - Long Short Term Memory based Recurrent Neural Networks (LSTM-RNN) with CUSUM for anomaly detection. They describe what they believe are their contributions and novelty: unsupervised approach based on LSTM-RNN + CUSUM, low false positive rate, techniques demonstrated in the context of a water treatment plant, and the ability to not only detect the presence of an anomaly, but also the sensor that is being tampered with. They follow this with a description of LTSM-RNN and CUSUM and the equations they chose. They describe their test dataset - The Secure Water Treament Plant (SWaT) at iTrust[3], their attack scenarios, and then their expriements and results.

There are two primary aspects of the authors' approach. First, they utilize LSTM-RNN to provide a time-series based prediction of what each sensor's subsequent value should be. This prediction value is then compared against the actual/provided value and evaluated for suitability via CUSUM[4]. They build these models and evaluate the output of each sensor in an attempt to validate each sensor's readings. For the prediction, they appear to follow the model in [5] with the primary difference being the approach used in evaluation (CUSUM vs. probablity error above a fixed threshold).

In their results they demonstrate the ability to capture the majority of their attacks. The only one they did not capture was one in which the system behaved in a normal fashion and the "attack" was assumed to be part of regular operations. Their figures (particularly 2, 3, 4) could have been re-organized to more clearly communicate their attacks and the relations between the values being displayed. Regardless of their layout choices, the attacks can be clearly identified.

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.

[3] iTrust | Signapore University of Technology and D. (SUTD), "Secure water treatment." [Online]. Available: https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/.

[4] E. S. PAGE, "CONTINUOUS inspection schemes," *Biometrika*, vol. 41, nos. 1-2, pp. 100–115, 1954.

[5] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long Short Term Memory Networks for Anomaly Detection in Time Series," *European Symposium on Artificial Neural Networks*, pp. 22–24, 2015.