Resilient Cyber-Physical System against False Data Injection Attacks

Yu Zheng
Florida State University
yz19b@fsu.edu

Abstract: The rapid development and mass application of cyber-physical systems (CPSs) benefit from the tight conjoining and coordination among computing, communication networks, and physical processes. However, the dependency on networks and computing components provides an opportunity for malicious agents to inject undesired effects. False data injection attacks (FDIAs) are one of the malicious attacks with the capability of bypassing the bad data detection (BDD) while triggering erroneous state estimation, thereby resulting in biased operation in physical processes. Traditional resilient estimation designs for CPSs assume half of the measurements are clean, such as L1 decoder, event-trigger Luenberger observer and more. By utilizing the CPS's advanced structure, a resilient CPS framework is proposed to survive in a worse adversarial environment: concurrent attack detection and identification (CADI) and resilient estimation (RE). CADI is processing in the cyber layers and producing uncertain conclusions concurrently while RE is processing in physical layers. Several challenges are supposed to be solved systemically: 1) how to design CADI with high precision? 2) how to bridge the learning-based algorithm and the model-based estimation scheme?

Generally, to detect attacks, the CADI algorithm should be trained to understand either system nominal features or all possible attack features. In this poster, I will present a Gaussian procession regression (GPR) approach to learn system features, and a multi-layer perceptron (MLP) approach to learn attack features. For the latter, our previous work shows more diverse adversarial training data could build a more precise MLP-based detector. Thus, we will also present two different approaches of attack generation: model-based moving-horizon FDIA design against L2 decoders and data-driven generative adversary network (GAN) attack generation scheme.

Due to the inherent precision uncertainty of the learning-based CADI's conclusions, it is challenging to use it in a dynamical estimation scheme. We proposed a pruning algorithm to bridge this gap. The pruning algorithm is a statistics-based algorithm to improve the precision of CADI's result without training by observing the Bernoulli distributed feature of its precision uncertainty. Based on the result of the pruning algorithm, a weighted L1 observer design is proposed to estimate system states even if more than half of the measurements are being attacked.

In this talk, a numerical simulation and an application simulation on a power system are also presented. The numerical simulation uses abundant samples of linear systems to validate the improved resiliency of our proposed observer design with CADI and pruning algorithm. And the application simulation compares the performance of the proposed method with other typical resilient observer designs in the literature.

Acknowledgement: This work was partly supported by Department of Energy Grant no. DE-CR0000005.