National Institute of Technology Rourkela

Defence Seminar

Seminar Title	: Design of False Data Injection Attacks and Their Detection and Mitigation in a Cyber-Physical System
Speaker	: Sushree Padhan (Rollno : 519cs1007)
Supervisor	: Ashok Kumar Turuk
Venue	: Convention Hall, CSE Department
Date and Time	: 29 Jun 2025 (5 PM)
Abstract	: Cyber-physical systems (CPSs) are susceptible to various attacks, of which false data injection (FDI) attacks are more critical. An attacker can launch an FDI attack at any chosen location in a CPS and modify the cyber and physical system&rsquos data, causing errors in the system&rsquos proper functioning. It is important to analyze FDI attacks at possible vulnerable locations and detect and mitigate them to defend the CPS. This thesis is an attempt in this direction. The thesis proposes strategies to design, detect, and mitigate FDI attacks in CPSs. A steady-state Kalman filter is used in the design of FDI attacks. Seven types of FDI attacks are proposed, in which each attack sequence follows a non-zero mean and zero-mean Gaussian distribution based on Kullback-Leibler (KL) divergence. It is observed that FDI attacks, in which the attacker simultaneously modifies the sensor measurements, actuator inputs, and physical system&rsquos state, generate maximum state estimation error. Next, a defense strategy is proposed for detecting and mitigating the non-zero mean and zero-mean Gaussian FDI attacks that simultaneously compromise the physical system, sensor measurements, and actuator inputs under a steady-state Kalman filter. A watermarking scheme is used to aid a Chi-square detector for attack detection. An attack mitigation scheme is proposed using control input synthesis and operating region concept. In this defense strategy, once an attack gets detected, the control inputs are generated from the proposed control input generation algorithm, where the system&rsquos operating regions are considered. It is observed from the simulation that the proposed defense strategy can detect and reduce the FDI attacker&rsquos effect on the system. Considering a time-varying Kalman filter, the non-zero mean and zero-mean Gaussian FDI attack types are designed, where the attacker simultaneously compromises the physical system, sensor measurements, and actuator inputs. Then, a two-stage defense strategy against FDI attacks is proposed. In the first stage of the defense strategy, the watermarking technique aids a Chi-square detector for attack detection. In the second stage of the defense strategy, a control scheme and a time-varying compensation signal are proposed to mitigate the attacker&rsquos effect. It is observed that the proposed control strategy reduces the attack effects. Finally, a reinforcement learning-based FDI attack detection strategy is proposed for better detection. The attack detection process is expressed as a partially observable Markov decision process and solved using Chi-square measurements with a sliding observation window. The reward parameters used in the training phase are designed. After an attack gets detected, a compensation-based attack mitigation strategy is initialized to mitigate the attacker&rsquos effect. It is observed that the RL-based detection strategy with the compensation-based mitigation scheme detects and reduces both non-zero mean and zero-mean Gaussian FDI attacks.