National Institute of Technology Rourkela

Synopsis 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	: Prof. Ashok Kumar Turuk
Venue	: Conference Hall - II (CS 323), Department of CSE
Date and Time	: 12 Dec 2024 (04.00PM)
Abstract	: The integration of the cyber and physical worlds has been driven by progress in communication, computing, and control technologies. This has also increased the incidence of malicious attacks in Cyber-Physical Systems (CPSs), of which false data injection (FDI) attacks are critical. An FDI attacker can launch an FDI attack at any chosen place in a CPS. An attacker can modify the cyber and physical system&rsquos data, which causes errors in the system&rsquos proper functioning. It is important to analyze a CPS due to FDI attacks at possible vulnerable locations. There must be defense schemes to secure a CPS from FDI attacks. Only an attack detection scheme cannot defend a CPS from FDI attacks. It is required to reduce the attacker&rsquos effect on the system. Therefore, a combined detection and mitigation mechanism is required to defend the CPSs against FDI attacks. In this thesis, a CPS is represented as a linear time-invariant system. The system is equipped with a Kalman filter as a state estimator. An LQG controller is considered to control the physical processes. First, strategies for designing, detecting, and mitigating FDI attacks are proposed with consideration for a steady-state Kalman filter gain. The effectiveness of this approach is evaluated within a CPS framework that includes a single sensor and actuator. Second, strategies for designing, detecting, and mitigating FDI attacks are proposed considering a time-varying Kalman filter and evaluating the proposed work through a CPS considering multiple sensors and actuators framework. Considering a steady-state Kalman filter gain, FDI attacks are designed and analyzed, where the attacker can modify the sensor measurements, actuator inputs, and physical system&rsquos state. It is assumed that the attacker can guess the system parameters and remain undetectable by carefully designing the attack sequences, which can disrupt the system&rsquos operation. Seven kinds of FDI attacks, in which the expected value of each attack sequence is non-zero, are identified, designed, and analyzed for their effects on the system. Seven similar types of FDI attacks are designed and analyzed, in which each attack sequence follows a zero-mean Gaussian distribution based on Kullback-Leibler (KL) divergence. Among the seven FDI attack types, the seventh type generates maximum error, in which the attacker simultaneously modifies the sensor measurements, actuator inputs, and physical system&rsquos state. The defense strategies for detecting and mitigating the seventh type&rsquos non-zero mean and zero-mean Gaussian FDI attacks for simultaneously compromising the physical system, sensor measurements, and actuator inputs are proposed. A watermarking scheme is used for attack detection. An attack mitigation scheme is proposed using control input synthesis and operating region concept. Considering the time-varying Kalman filter gain, two FDI attack types are designed, where the expected value of each attack sequence in the first FDI attack type is non-zero, and each attack sequence of the second FDI attack type follows a zero-mean Gaussian distribution. The attacker simultaneously compromises the physical system, sensor measurements, and actuator inputs. A two-stage defense strategy against such FDI attacks is proposed. In the first stage of the defense strategy, the watermarking technique is used to aid a Chi-square detector in 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. 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 also utilized to mitigate the attacker&rsquos effect. Simulation of the proposed FDI attacks and detection and mitigation strategies are evaluated using multiple numerical examples to illustrate their effectiveness. The proposed defender can detect the FDI attacks and reduce the attacker&rsquos effect.