National Institute of Technology Rourkela

Departmental Seminar

Seminar Title	: Defense against False Data Injection Attack in a Cyber-Physical System
Speaker	: Sushree Padhan (519cs1007)
Supervisor	: Sumanta Pyne, PIC Seminar
Venue	: Conference Hall of CSE Department
Date and Time	: 23 Jul 2024 (17:30)

Abstract : Cyber-physical systems (CPSs) are closed-loop feedback systems that efficiently control the physical processes through cyber-systems. Security threats like false data injection (FDI) attacks are increasing in CPSs. FDI attacks disrupt the system's performance by modifying the original data. It is necessary to have mechanisms in place to defend against FDI attacks and enhance security in CPSs. This paper proposes a two-stage defense scheme against an FDI attack that can simultaneously modify the data in physical and cyber systems. The first stage is attack detection using a watermarking technique with a Chi-square detector. The second stage is attack mitigation, in which we generate a time-varying compensation signal to reduce the attacker's effect and propose a control scheme. We demonstrate the simulation results of the proposed defense scheme against the FDI attack using an unmanned aerial system (UAS) as an example.