National Institute of Technology Rourkela

Synopsis Seminar

Seminar Title	: Development of A Multi-Layer Protection Framework for Cyber-Physical Microgrids
Speaker	: Kunal Kumar (Rollno : 521ee1002)
Supervisor	: Susmita Kar
Venue	: EE401
Date and Time	: 15 May 2025 (11:00 AM)

Abstract : The transformation of conventional power systems into cyber physical microgrids has brought forth a range of operational advantages, such as decentralization, improved reliability, and seamless integration of renewable energy sources, while simultaneously introducing complex vulnerabilities across physical, communication, and cyber layers. Faults in the physical layer, bad data in the communication infrastructure, and sophisticated cyber-attacks like False Data Injection Attacks (FDIAs) present significant challenges to the secure and resilient operation of microgrids. Furthermore, the overlap of these anomalies in dynamic environments can lead to misclassification, resulting in false alarms or undetected threats.

This report proposes a comprehensive, multi layered anomaly detection and classification framework that ensures resilient microgrid operation. At the physical layer, a Rate of Change (ROC) based detection mechanism using Differential Positive Sequence Admittance Angle (DPSAA) is developed to accurately identify shunt and high impedance faults across grid connected and islanded modes. At the communication layer, a robust, non-iterative state estimation model leveraging &muPMU data and M estimators is introduced to detect and eliminate bad data caused by noise or sensor errors with minimal computational burden. At the cyber layer, an Iteration Free Detection of False Data (IFDFD) algorithm is formulated to detect stealthy FDIAs in static environments using nodal power injection data and statistical filtering. To extend resilience to dynamic microgrid conditions, operational disturbances such as capacitor switching, sudden load variations, generator and line outages, and various physical faults are simulated on a modified IEEE 13 bus system. A blockchain integrated detection framework using a Power Imbalance Attack Index (PIAI) and smart contracts is proposed to distinguish FDIAs from these normal but transient events. Furthermore, to address the critical issue of differentiating between physical faults and cyber-attacks, two blockchain enabled classification schemes are presented: the Bus Interconnectivity Search Algorithm (BISA) and the Blockchain Driven Event Detection Index (BEDI), utilizing residual patterns and sequence component analysis, respectively.

Bad data detection and FDIA simulation and validation are carried out on a modified IEEE 14 bus system in a static environment, while fault scenarios and dynamic operational disturbances are modelled and tested on a modified IEEE 13 bus system. Results demonstrate high detection accuracy, low latency, and scalable protection capabilities. The integration of blockchain technology ensures data immutability, transparency, and autonomous execution of detection logic, culminating in a robust and secure cyber physical microgrid framework capable of real time anomaly detection, classification, and response.