CYBER-ATTACK RESILIENT DESIGN OF WIDE AREA MEASUREMENT SYSTEM IN SMART GRID

Abstract

Advances in information, communication, and computer technologies and their subsequent application in power system infrastructure have resulted in the emergence of new technologies such as the Wide Area Measurement System (WAMS). Fast, highly accurate, and timestamped data from the Phasor Measurement Units (PMUs) have made real-time wide area situational awareness possible. They have also solved many complex power systems problems like preventing relay maloperations. However, the IEEE C37.118 PMU data's vulnerability to cyber-attacks can paralyze the working of such applications. While denial-of-service (DoS) attacks can blind the system operator about the grid's condition, data manipulation attacks can mislead the decision-making at the control center, compromising the power system's operation. Thus, it is crucial to secure PMU data against these attacks and avoid their adverse effect on the end applications. Further, for wide area protection and control applications (WAPAC) which involve sending a decision signal from the control center (based on PDC data) to the intelligent electronic devices (IEDs) in the substation, secure communication of such critical messages is also important for overall attack resiliency of such applications.

In this regard, the work in this thesis focuses on ensuring the availability, confidentiality, and integrity of synchrophasor data (IEEE C37.188) from PMUs (in substations) to the PDC (in the control center). It also discusses ways to secure critical decision signals, which can be communicated using IEC 61850-90-5 R-GOOSE protocol from protection schemes (in the control center) to the IEDs (Relays or BCUs) in the substation. The approach used in this work is inspired by the guidelines provided by the National Institute of Standard and Technology (NIST) for the cybersecurity of critical infrastructures. In this context, a cyber-physical WAMS testbed is developed for risk assessment, and then attack resiliency of PMU data based wide area monitoring and protection application (WAMAP) applications is enhanced by redesigning the WAMS framework with attack prevention, detection and mitigation strategies as discussed below:

- Cyber-physical WAMS testbed is developed for vulnerability assessment and studying the impact of cyber-attacks. The testbed includes industry-standard hardware, software, and communication protocols (IEEE C37.118 and IEC 61850-90-5).

- DoS attack prevention strategy is developed for PMU data in the WAMS framework using concepts of redundancy and randomness. Thereafter, unique fingerprints based attack detection strategy is suggested for determining the root cause of data unavailability in terms of communication issues or DoS attacks. The detection strategy also identifies different types of DoS attacks.
- DoS attack mitigation approach is developed for PMU data using machine learning imputation techniques and deep learning networks to ensure attack resiliency of wide area monitoring and protection applications (situational awareness and adaptive relaying) during PMU data unavailability.
- A methodology for data manipulation attack detection in the WAMS framework for wide area monitoring and offline applications is suggested. The approach is based on the intrinsic properties of WAMS infrastructure and the existing strong and synchronized power grid. Further, to enhance attack resiliency of time-critical wide area applications against data manipulation attacks, a detection, and mitigation approach using deep learning networks is also developed.
- For overall attack resiliency of wide area protection applications like adaptive relaying, security of supervisory decision messages (IEC 61850-90-5 R-GOOSE messages) from the control center to the IEDs in the substation is enhanced using Cryptography technique and Blockchain concepts.

Keywords: Cyber Security**,** Wide Area Measurement Systems, Wide Area Situational Awareness, Adaptive Relaying, IEEE C37.118, IEC 61850-90-5 R-GOOSE, Denial-of-Service Attacks, Data Manipulation Attacks, Cryptography