CURENT

curent.utk.edu/research

RESEARCH

PMU Measurement-based Cyber-Physical Security

Overview

The goal of this project is to assess the cyber capabilities and weaknesses of PMUs by creating different scenarios and performing extensive simulations and experiments. While PMUs and their measurement data are the key enabling technology for modeling and monitoring, they represent increased dependency on cyber resources, which could result in vulnerabilities to cyber attacks. Understanding the cyber capabilities and weaknesses associated with PMUs and measurement data is therefore of paramount importance to the power systems.

Technology Pathway

Complex cyber-physical systems (CPS) in combination with the power grid are more vulnerable to cyber-physical attacks than either of these alone. This is because cyber attacks and physical attacks are intrinsically interconnected. They can often be used together to create new attack surfaces, to have greater impact on the system or to make it more difficult to thwart. While much attention has been steered toward cybersecurity, physical security, as well as the interplay between the cyber and physical systems, has been largely neglected. We propose to study cyber-physical security and our main focus is to utilize the interaction between cyber and physical systems to develop closed-loop solutions that synergistically integrate sensing, control, processing, communication and actuation. Specifically, cyber-physical security for the power grid will be theoretically and systematically studied, and physical laws and realities will be applied to combat cyber and physical attacks. We consider the most sophisticated attackers who attempt to deceive the system on the physical level or the root level, not the cyber level or the surface level. It has been theoretically shown that such attacks can go undetected with current solutions, and we will create practical attack scenarios that support this theory. We will also design novel algorithms that can maintain the proper operation of power systems when the attacks take place. The simulated attacks, their impacts and attack defenses will be demonstrated using the Large Scale Test Bed (LTB) and Hardware Test Bed (HTB).

Impact

- Significantly improve the security, reliability and robustness of the power system.
- Achieve substantially better performance than traditional IT security technologies through specifically designing schemes and models for the power CPS.

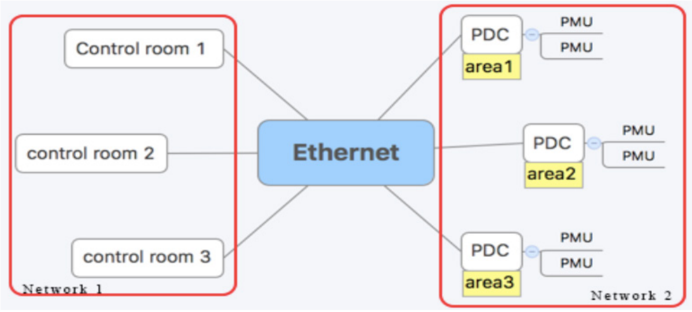
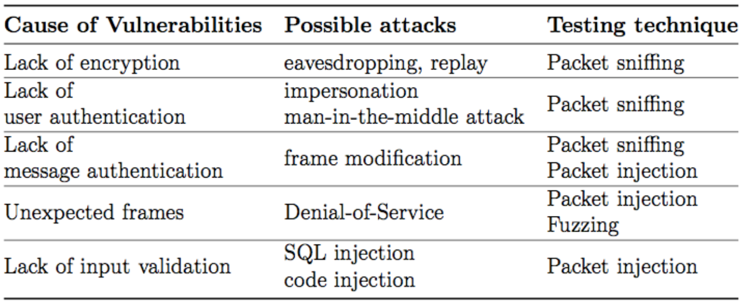


Fig. 1 - The test network



Cause of Vulnerabilities	Possible attacks	Testing technique
Lack of encryption	eavesdropping, replay	Packet sniffing
Lack of user authentication	impersonation man-in-the-middle attack	Packet sniffing
Lack of message authentication	frame modification	Packet sniffing Packet injection
Unexpected frames	Denial-of-Service	Packet injection Fuzzing
Lack of input validation	SQL injection code injection	Packet injection

Fig. 2 - Vulnerabilities validated in pentesting

POINT OF CONTACT

Jinyuan Sun
865.974.0426 (ph.)
865.974.9723 (fax)
jinyuansunstella@utk.edu
THE UNIVERSITY OF TENNESSEE KNOXVILLE

research funding provided by