Title: Attack-resilient State Estimation and Testbed-based experimental evaluation of coordinated attacks on Wide-Area Protection and Control

Abstract:

In the last decade, the power grid and several other critical infrastructures have been increasingly targeted by advanced, sophisticated adversaries as they are critical to national security and societal well-being. There is a compelling need to develop a multi-layered defense strategy that leverages a combination of infrastructure and application layer security measures when dealing with a resourceful and sophisticated adversary. One of the key motivations of this research work is to go beyond traditional infrastructure security solutions to develop attack-resilient application layer security approaches for critical monitoring, protection and control applications, which leverage both cyber and physical aspects of the grid. This research work, rests on two major components. The first component, Attack-resilient State Estimation, addresses the vulnerability of state estimation to stealthy cyber attacks, and discusses two complementary approaches to enhance its resilience. A topology-based attack vector that bypassed bad data detection methods and causes loss of system observability was identified. To mitigate the stealthy attacks on measurements and topology, an offline attack-resilient measurement design methodology was developed. In addition, an online attack-resilient anomaly detection method that utilized load forecasts, generation schedules, and synchrophasor data to detect measurement anomalies was developed. The second component, Testbed-based experimentation and performance evaluation of coordinated attacks on Wide-area Protection and Control, addresses the need to architect, develop, and leverage cyber-physical security testbed environments specifically for performing realistic attack-defense experimentation for WAMPAC use cases. An overview of testbed design objectives and design tradeoffs were discussed for different types of testbeds. Then, a methodology for CPS security testbed development based on specific WAMPAC use cases was detailed. A three-layered WAMPAC specific testbed architecture to address critical research challenges was identified. Finally, three experimental case studies that involved realistic coordinated cyber attacks on critical WAMPAC applications such as AGC, RAS were described in detail. As a part of the case studies, a novel coordinated attack vector for RAS that involved a combination of data integrity and DoS attacks was identified. Further, the hypothesis that timing of attack actions also plays a critical role in the attack impact severity was experimentally validated using the PowerCyber testbed.