Cyber risk modeling and attack-resilient control for power grid

The electric power grid is a cyber-physical system (CPS) that forms the lifeline of modern society. The advanced devices and communication infrastructure of the Supervisory Control and Data Acquisition (SCADA) system enable operators to deliver reliable and high-quality power. However, inherent cyber security vulnerabilities put system operation at risk by providing an attack surface to cyber threat actors. A smart attacker, that is, a cyber threat actor with expertise in physical power system operation could cause severe damage to the power grid infrastructure and its reliability by stealthily manipulating SCADA operation. This dissertation explores such impacts to power grid operation from cyber attacks and more importantly, introduces novel mitigation schemes to minimize or negate the impacts. It has two primary components - risk modeling of coordinated cyber attacks and attack resilient control.

Coordinated cyber attacks are attacks that target multiple power system components simultaneously. The notion of spatial and temporal coordinated cyber attacks is introduced and their impact on power system reliability is quantified. A systematic risk modeling framework is proposed as offline mitigation. The risk for a substation is modeled as the product of the vulnerability of its SCADA infrastructure and the impact from its compromise. Vulnerability is quantified by modeling the SCADA network using Stochastic Petri Nets. Impact to system reliability is quantified in terms of traditional reliability metrics. The methodology is applied to a test system and the attack vectors are ranked by risk. Results show that the methodology is useful in identifying infrastructural upgrade requirements and security enhancements. An enhancement to the contingency analysis application is proposed as mitigation for online operation. The proposed algorithm efficiently captures impactful coordinated vectors by significantly reducing the number of cases to be evaluated. Results reveal the algorithm's ability to identify almost all impactful attack vectors for a line under review without the need for a comprehensive study.

The second component of the thesis explores the impact of data integrity attacks on power system control applications. Specifically, the impact of data integrity attacks on Automatic Generation Control (AGC) is examined and Attack-Resilient Control (ARC) is proposed as mitigation. ARC for AGC proposes the use of physical system information to design algorithms for the detection and mitigation of cyber attacks. Domain-specific anomaly detection and attack mitigation algorithms were developed for AGC using short-term load forecast data. The performance of AGC was tested on a standard test system with and without ARC. The results show that ARC for AGC is able to detect data integrity attacks, maintain system within stability margins and enhance overall system security by providing defense-in-depth.

Future work includes expanding the risk analysis framework to include different types of coordinated attacks and to compare impact expressed in different power system metrics. Mitigation of temporal coordinated attacks and transient stability analysis of spatial and temporal attacks are also a part of future work. Finally, the attack resilient control framework should be enhanced to differentiate abnormal measurements due to cyber attacks from legitimate aberrations due to power system contingencies.