# Thesis Abstract

Monitoring a physical process and estimating its state variables is an important function needed for the proper working of a smart grid. As such, performing the aforementioned function reliably and securely is of utmost importance. State estimation in a smart grid can be properly operated with wireless sensor networks (WSN) that provide low-cost and robust monitoring solutions. However, the broadcast nature of any wireless medium makes the WSNs prone to cyber-attacks. Jamming is one such jamming attack that severely deteriorates the communication network's performance so that the measurements do not reach the destination. By congesting the communication network, jamming introduces a delay in the network. In this work, we model the delay experienced by time-critical operations in a smart grid network due to jamming and investigate its mitigation technique. False data injection (FDI) attacks are launched by an adversary to modify the measurements of a physical system that could manipulate the state variables' estimated values which can mislead the system operator and jeopardize the physical process. In this dissertation, we have investigated the issue of detecting FDI attacks on state estimation in WSN enabled smart grid, where inactive sensor nodes (SNs) of the network is compromised by the adversary to launch the attack over wireless channels. Both jamming and FDI attacks require the attacker to possess knowledge about some parameters of the physical process. In this regard, WSNs are also vulnerable to eavesdropping and signal interception that can disclose internal parameters of the physical process. Among other physical layer security techniques, allocating optimal power to transmit data over wireless channels is an important technique to secure wireless networks against cyber-attacks. Another major challenge in using WSNs for monitoring tasks and securing it against cyber-attacks is the limited capacity of the batteries powering the SNs. In this regard, wireless powered sensor networks (WPSNs) where the individual SNs follows harvest-then-transmit approach is being explored, extending the lifetime of the SNs used in monitoring critical functions. The threats from a sensor node, capable of harvesting energy from RF signal, are investigated in this thesis by studying its effects on the operation of a wireless network. Further, the SNs are operated by third parties and have the onboard processing power. Therefore, distributed resource allocation techniques are best-suited for WSNs. In this regard, game theory is used extensively as a tool for distributed resource allocation where there exists competition among the various nodes of the network. In this dissertation, the problem of physical layer security for WPSNs for smart grid communication is addressed by proposing various game-theory based distributed resource allocation. For complex games, the solution is obtained with Q-learning based algorithms. Different from existing learning techniques, we have proposed Q-learning methods that converge in environments with multiple decision-makers.