Chapter 1

Introduction

The electric power grid is a complex system subject to natural disasters and nuisance attacks, in addition to the rapid system dynamics and demand swings inherent in providing electric power across large areas. A balance between electricity generation and consumption at all times is one necessary condition for the normal operation of the power system, and large imbalances can cause power outages, leading to economic losses, physical damage, or even bodily harm. In addition, the power system is an example of a cyber-physical system (CPS), which consists of physical components such as actuators, sensors and controllers that communicate with each other over a network. Although communication networks are often protected by security measures, cyber attacks can still take place when a malicious attacker obtains unauthorized access. In a power system, cyber attacks not only compromise information, but can also cause physical damage. Therefore, it is desirable to protect the system against such cyber attacks. This thesis presents progress in the path towards finding solutions to these two problems and consists of two main parts. Chapters 2 and 3 describe first attempts at using commercial buildings to provide frequency regulation – a type of service used by electricity grid operators to balance electricity generation and demand. Chapters 4 and 5 focus on developing methods that estimate the true state of a power system when it is under cyber attack.

1.1 Frequency Regulation from Commercial Buildings

A balance of electricity generation and demand must be maintained at all times to achieve the reliable operation of the power system. Any mismatch between them is reflected through the grid frequency: if generation exactly meets demand, then the grid frequency is at its nominal value of 60 Hz (in the U.S.); if generation exceeds demand, then the frequency increases, and vice versa. Therefore, to maintain normal operation of the power grid, the grid operator uses reserves known as ancillary

services (AS) to correct any mismatch between electricity generation and demand. Amongst these reserves, frequency regulation is the highest quality AS over which the grid operator has almost real-time control and is active continuously during normal operation of the grid. Recent rapid increase in the penetration of renewable energy sources has escalated the volatility and uncertainty of electricity generation, which led to a greater demand for frequency regulation reserves. Traditionally, these reserves have been provided by fast ramping power generators. However, an alternative is to explore the flexibility on the demand side, which may have less economic and environmental cost in the long run. More specifically, loads can provide regulation by increasing (decreasing) their electricity consumption when the grid frequency increases (decreases).

In particular, commercial buildings are a tremendous untapped resource for this application. First, they account for a large fraction of the total electricity consumption (more than 35% in the U.S., 39% of which is due to heating, ventilation and air conditioning (HVAC) systems [91]). Second, the building's large thermal capacity allows the power consumption of HVAC systems be partly shifted in time without compromising occupant comfort. Third, many commercial buildings are equipped with a variable frequency drive which can be controlled to vary the power consumption of supply fans of the HVAC system quickly and continuously [38]. This greatly simplifies tracking of the reference regulation signal, as opposed to resources with on-off control. Fourth, about one third of commercial buildings in the U.S. are equipped with a building automation system (BAS) [8] which facilitates the implementation of new controllers.

On the other hand, there are a number of challenges in using commercial buildings for frequency regulation. First, obtaining a building model that is amenable to control is not straightforward, because commercial buildings are often subject to large disturbances such as occupancy, that are difficult to capture. In addition, buildings are often not sufficiently excited, as they must satisfy strict regulatory requirements during regular operation, which limit the type and duration of excitation experiments that can be conducted. Second, about one third of commercial buildings in the U.S. are equipped with variable air volume (VAV) HVAC systems [38], which are typically complex with many control variables and interdependent control loops.

This thesis proposes procedures to develop both data-driven and physics-based models for the thermodynamic behavior of commercial buildings, and provides a quantitative comparison between them using both open- and closed-loop metrics. In addition, this thesis presents an experimental demonstration of the feasibility of using a VAV HVAC system for frequency regulation, where experiments are conducted in full accordance with Pennsylvania, New Jersey, Maryland's (PJM's) requirements. To the best of our knowledge, this is the first report where an occupied commercial building equipped with a VAV HVAC system can successfully provide frequency regulation.

1.2 Secure State Estimation against Cyber Attacks

A key element in the development of smart power transmission systems over the past decade is the tremendous advancement of the synchrophasor technology. This is enabled by phasor measurement units (PMUs) which record and communicate GPS-synchronized, high sampling rate dynamic power system data, and they are currently being installed at different points in the North American grid, especially under the smart grid initiatives of the U.S. Department of Energy. Significant efforts have been made in using PMU measurements for wide area control in a smart grid. In such a system, a wide area control system (WACS) communicates with PMUs over a communication network to achieve increased efficiency and reliability of the power system. However, communication networks are often vulnerable to cyber attacks. For example, [56] describes a multi-switch attack, in which different switches in a power network attacked at different times, can lead to stealthy and wide-scale cascading failures in the power system. Therefore, in order to protect the system against cyber attacks, the WACS must estimate the system's true states before using the received data for computing control signals. However, this is a challenging task as cyber attacks can be erratic and difficult to model.

Secure estimation problems study how to estimate the true system states when measurements are corrupted and/or control inputs are compromised by attackers. There has been tremendous amount of work in developing secure state estimation algorithms, mostly for linear dynamical systems and/or by assuming the attack signal follows a certain distribution. However, the power system can only be approximated by a linear model under small perturbations in the system. Under a severe disturbance, such as a single or multi-phase short-circuit or a generator loss, the linearized model does not remain valid [51], [95]. Therefore, the existing linear estimation techniques lack performance guarantees when the system undergoes large perturbations which are typical of highly loaded practical systems. To overcome the above drawbacks, this thesis builds on previous results to first propose a secure state estimation algorithm for linear dynamical systems without any assumption on the sensor attacks or corruptions (i.e., corruptions can follow any particular model). The only assumption concerning the corrupted sensors is about the number of sensors that are corrupted due to attacks or failures. This thesis then extends the results to two classes of nonlinear systems and demonstrates through numerical simulations how the proposed estimation algorithm can be used to protect the nonlinear power system against cyber attacks.