ABSTRACT

Author: Wu, Feng. MSCE
Institution: Purdue University
Degree Received: August 2019
Title: A Cybersecurity Framework for Wireless-Controlled Smart Buildings
Committee Chair: Ming Qu

Due to the rapid development of wireless communication and network technology, more and more wireless devices (e.g., Siemens, Lutron,etc.) are used in residential and commercial buildings. The wireless system has many advantages that traditional wired-based system do not have, such as time-saving deployment and easy maintenance. However, the wireless system is also vulnerable to cyber-attacks since the data packets are transmitted by radio waves rather than by physical medium. The current cyber detection system(e.g., Intrusion detection system) monitors the data traffic to identify the anomalies in the network. However, it is unable to detect the attacks that tamper with the control logic or operating parameters, which results in the malfunction of the system. This thesis developed an integrated, cyber-security framework for cyber-attack detection in smart buildings.

The objective of this research is to develop an integrated cyber-security framework for wireless-based smart building systems to protect buildings from the cyber-attacks. The wireless-based smart building systems are operated and controlled by either a two-position or continuous controlled approach. This study developed two different cyber-security frameworks to deal with two-position control and continuous control. For the two-position controlled smart buildings, the developed cyber-security framework integrates the data and models of both cyber and physical domains of building systems to detect faults, abnormal operations, even attacks. The cyber-security framework developed for the continuous controlled system is a hybrid model that combines two physical models for different functions: a data-driven model for detecting the faults of sensor measurements and a physical model based on engineering principle(e.g., laws of thermodynamics) or control logic to detect the anomaly of system operation.

To develop the cyber-security frameworks, two corresponding testbeds for the two-position and continuous wireless systems were utilized. The wireless-based lighting system in a smart home was the testbed for the study of the two-position control. It has a wireless occupancy sensor, an actuator for the light switch, and an open-source operating platform (OpenHAB) for system control and monitor. The smart home platform uses the ZigBee protocol to communicate wireless devices. An indoor shading system at a living lab in new Herrick building of Purdue University was utilized as the testbed for the study of the continuous controlled system. The indoor shading system exploits roller shades to block the excess daylighting to provide an acceptable illuminance condition for occupants. The shading system uses the wireless illuminance sensor, weather condition, and wire-based controller to automatically operate the shades for the acceptable illuminance.

The study implemented designed cyber-attacks to validate the effectiveness of the developed frameworks. The final results show that the developed two models were able to detect the attacks

effectively. For two-position control, an abnormal operation was identified when an abnormal state was triggered, or the modelled state and real state did not match. For continuous control, the abnormal operation was detected when there a significant deviation between the modelled measurement and the actual measurement. The cybersecurity frameworks developed in this thesis demonstrate an effective approach for detecting system faults caused by attacks. The frameworks developed could be widely used for other different building systems and beyond buildings, such as transportation or industrial manufacturing systems.