PURDUE UNIVERSITY

A Cybersecurity Framework for Wireless- Controlled Smart Buildings

Research Assistant(s): Feng Wu

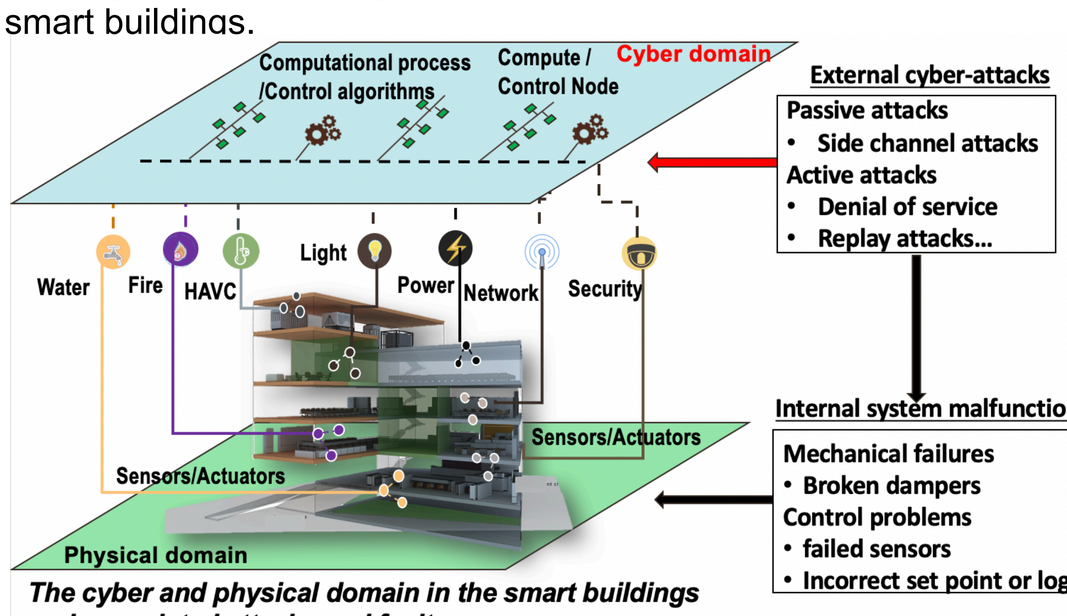
Principal Investigator(s): Ming Qu

Sponsor: Discovery Park

Contact email: *wu1239@purdue.edu*

Research Objectives

This research aimed to address the challenges of cyber attacks on buildings by developing an integrated cyber-security framework for smart buildings.

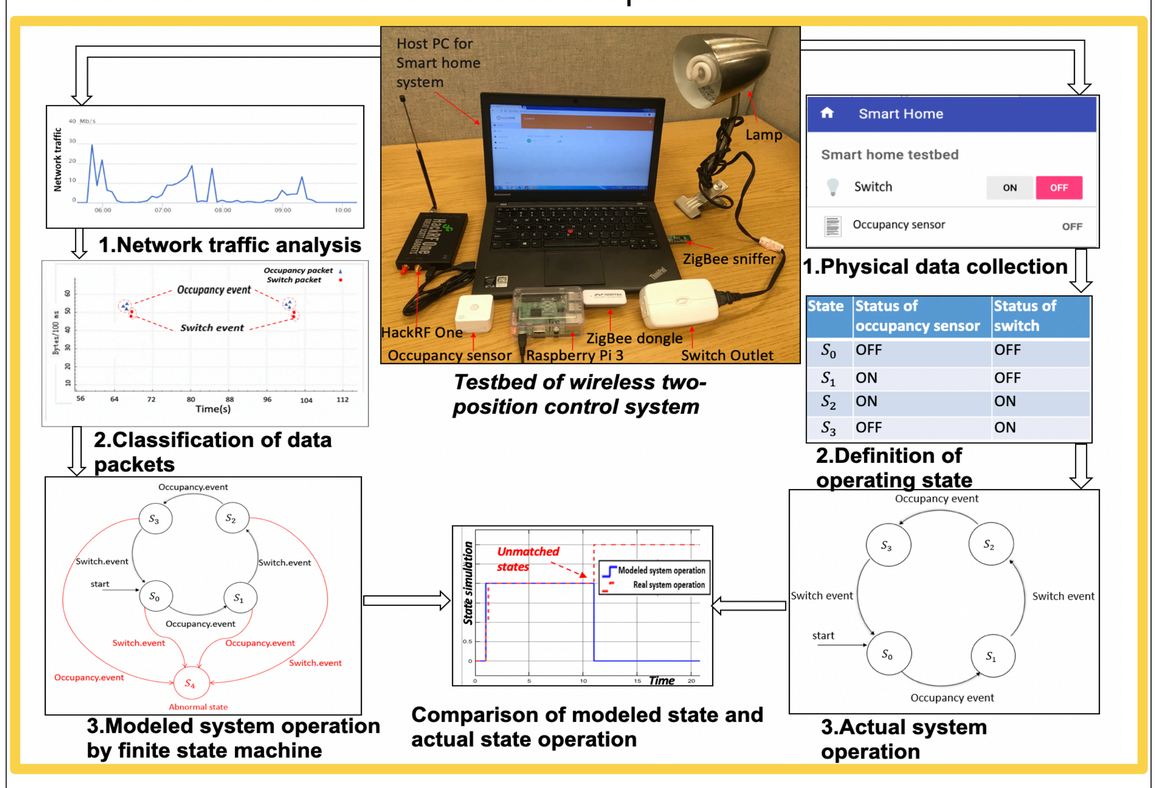


The cyber and physical domain in the smart buildings and associated attacks and faults

Methodology

Wireless-based systems are used as case studies to demonstrate the approach of the framework.

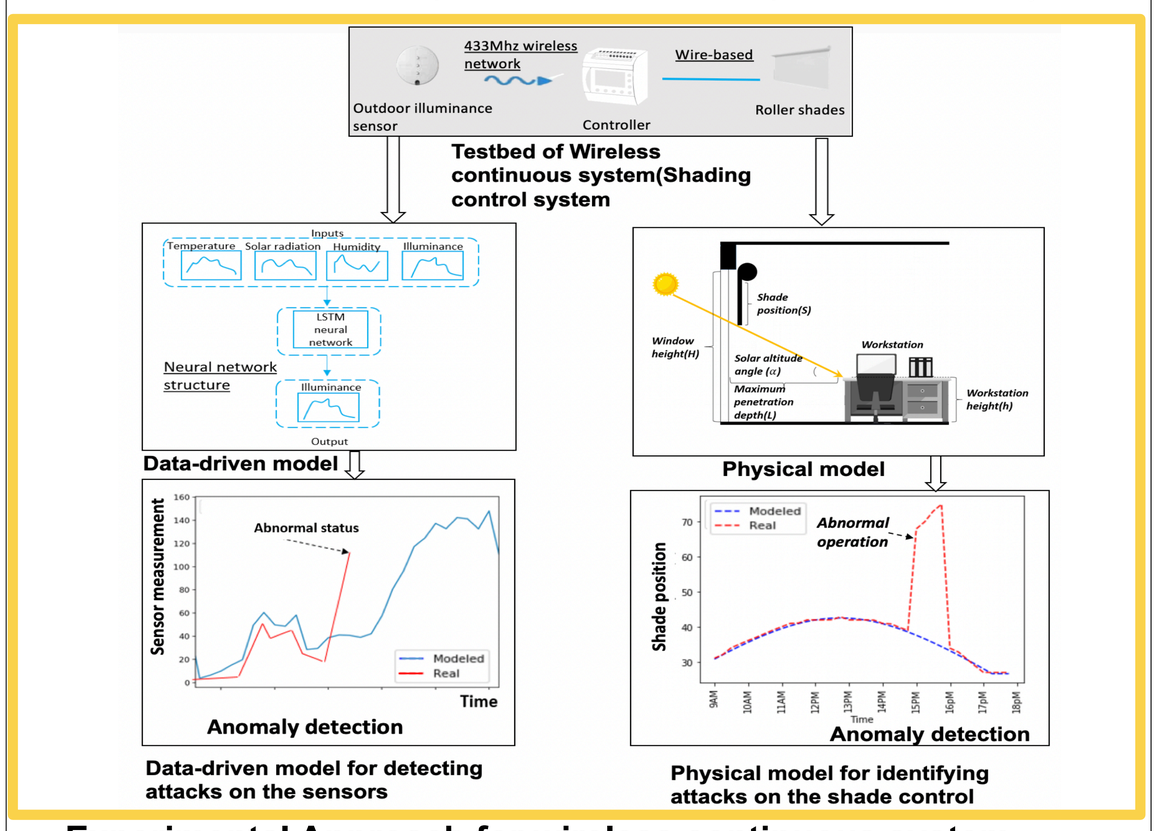
Currently, wireless-based smart building systems are operated and controlled by either a two-position or continuous-control approach. The corresponding applications are smart home and commercial building. Two different frameworks were developed.



State	Status of occupancy sensor	Status of switch
S_0	OFF	OFF
S_1	ON	OFF
S_2	ON	ON
S_3	OFF	ON

Experimental Approach for wireless two-position system

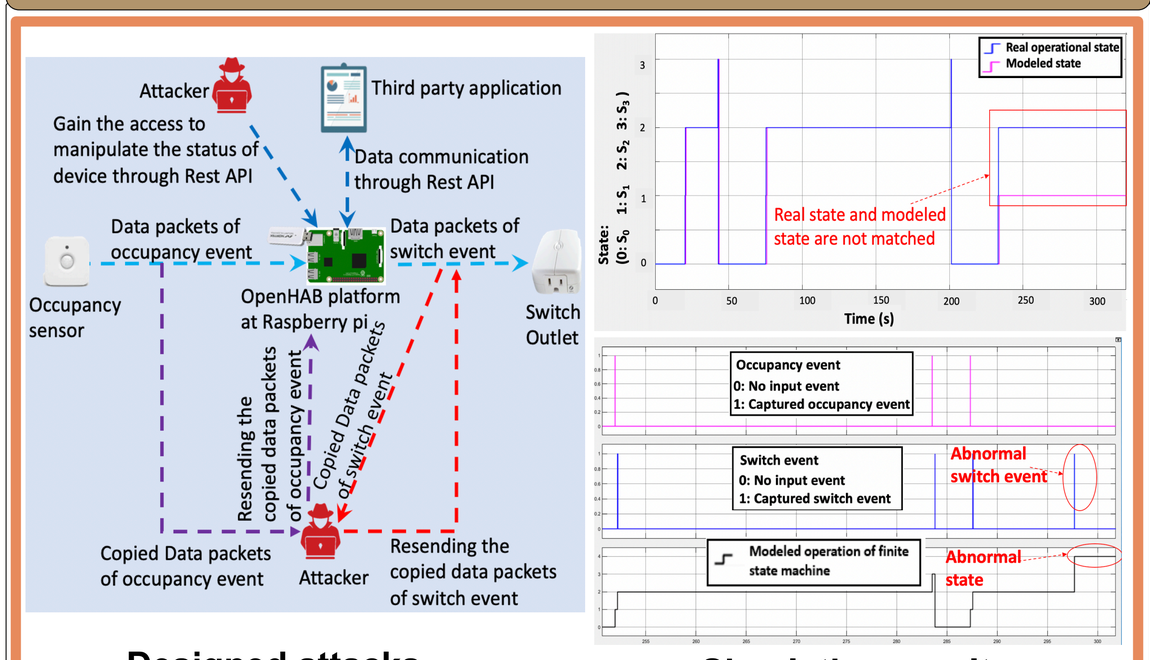
The framework for two-position control integrated the data from both cyber and physical domain to safeguard the wireless system. A finite state machine was developed to model to the operation of the system.



Experimental Approach for wireless continuous system

The framework developed for the continuous system is a hybrid model that combines two physical models for different functions: a data-driven model(Long short-term memory neural network) for detecting the faults of sensor measurements and a physical model based on engineering principle or control logic to detect the anomaly of system operation.

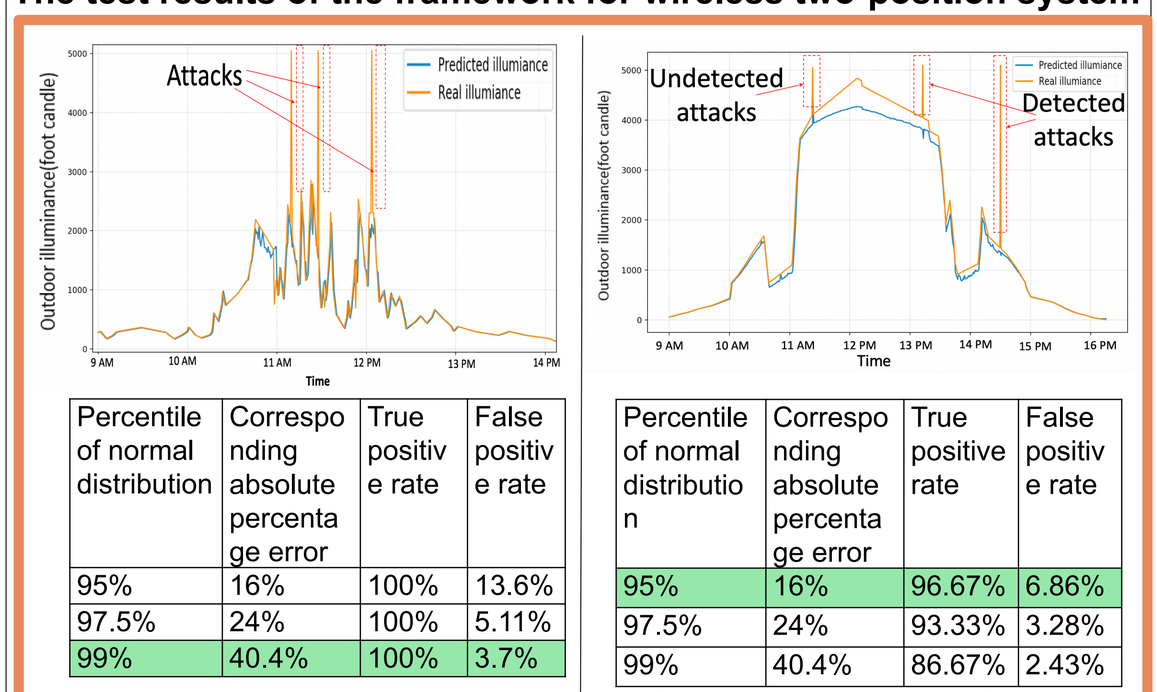
Results



Designed attacks **Simulation results**

Designed replay attacks and attack through third-party application were implemented to validate the performance of the framework. Based on the test, it can 100% capture the cyber attack through finite state machine model or the comparison between modeled state and actual state.

The test results of the framework for wireless two-position system



Percentile of normal distribution	Corresponding absolute percentage error	True positive rate	False positive rate
95%	16%	100%	13.6%
97.5%	24%	100%	5.11%
99%	40.4%	100%	3.7%

Simulated results of partly cloudy day

Percentile of normal distribution	Corresponding absolute percentage error	True positive rate	False positive rate
95%	16%	96.67%	6.86%
97.5%	24%	93.33%	3.28%
99%	40.4%	86.67%	2.43%

Simulated results of sunny day

Replay attacks were implemented on the shading control system to validate the performance of the framework. For partly cloudy condition, the developed data-driven model can 100% detect all the attacks by choosing different different thresholds. For sunny day, the model can capture 96.67% attacks when smallest threshold of APE was selected. To minimize the FPR, the different threshold should be selected based on the outdoor weather.

The test results of the framework for wireless continuous system

Future Work

- Future research should focus on the investigation of the packet feature of Wi-Fi devices since the Wi-Fi devices increasingly accepted by manufacturers.
- The testbed of the continuous controlled system is a semi-wireless based system. Further research should implement attacks on a wireless-based shade control.
- Other emerging neural network, such as Hierarchical Temporal Memory(HIM) or Gated Recurrent Unit(GRU), can be investigated in the future to improve the attack detection accuracy.

Potential Impact of Research

The cybersecurity frameworks developed in this research demonstrate an effective approach for detecting system faults caused by attacks. The methods developed could be widely used for other different building systems and beyond buildings, such as transportation or industrial manufacturing systems.

Acknowledgements

The research presented was supported by the Discovery Park at Purdue University.

PURDUE MECHANICAL ENGINEERING

RAY W. HERRICK LABORATORIES