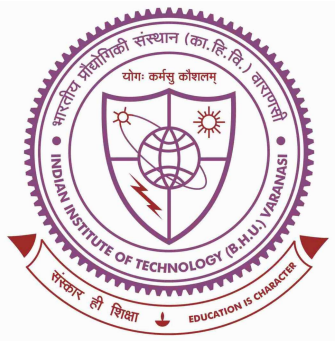
# Resilient Scheduling of Smart Buildings under False Data Injection Attack




Thesis submitted in partial fulfillment
for the award of degree

Doctor of Philosophy

by

**Basant Kumar Sethi**

**DEPARTMENT OF ELECTRICAL ENGINEERING**
**Indian Institute of Technology**
**(Banaras Hindu University)**
**Varanasi**

**Roll No: 17081010**

2022

# Chapter 6

# Conclusions and Future Scope

## 6.1 Conclusions

The aims of the work presented in this thesis is to minimize the energy cost based on the scheduling of smart home appliances and distributed energy resources under the FDI attack. Highlights of the work presented in this dissertation are as follows.

In this thesis, smart buildings energy management considering different approaches has been presented. Due to the presence of communication networks and IoT based smart appliances, the interaction of SBs and utility becomes prone to cyber-attacks. In this work, the impact of FDI attack on EMS of SBs has been investigated. The work aims towards developing a resilient energy management framework against various types of FDI-attacks, i.e. FDI in price data, FDI in demand data, and coordinated FDI in both price and demand data.

First, an EMS for a single smart home has been developed. In this study, an assessment of the impact of battery degradation cost on energy scheduling is investigated. It is observed from the investigations that the inclusion of battery degradation cost plays a significant role in reducing the frequency of battery charging/discharging. It is also observed that inclusion of battery degradation cost in scheduling process increases the energy cost. Apart from this, the impact of FDI-attack (on price signal) on energy cost has also been examined. It is observed that FDI-attack on price signal can alter the scheduling pattern and cause significant financial loss to the consumers. A resilient scheduling framework that relies on the stochastic bill prediction, has also been developed to minimise the financial losses. The numerical results show that the proposed resilience EMS is quite effective

in presence of FDI-attacks.

Then, a game-theoretic EMS framework has been developed for multiple SBs. In this framework, the strategy of one SB is influenced by the strategies of other SBs. Therefore, the equilibrium strategies of SBs are sensitive to (i) The price signal broadcasted by the utility and (ii) Power exchange requests of all the SBs. FDI-attacks on price signal and/or power exchange requests of SBs can lead to change in the strategies of SBs. Therefore, FDI-attacks on price and demand data change the scheduled demand pattern and energy costs of SBs. This change itself can be utilized to detect the FDI-attacks. By considering this fact, a detection technique has been developed and validated through numerical results. However, as FDI-attack detection is a post -facto analysis, to minimise the impact of FDI-attacks, a resilient scheduling strategy based on power exchange pattern has been proposed. The numerical results show the efficacy of proposed resilient scheduling strategy. It is observed that the proposed detection technique and resilient scheduling strategy provide effective solution against FDI-attacks on price as well as demand data.

Finally, an EMS under FDI attack considering power exchange capability of inter-connected SBs have been developed. As in this formulation, SBs are inter-connected to each other, an SB can take financial benefit from other SBs under these attack conditions. To avoid this types of activity, a robust EMS (resilience towards FDI attack) has been developed. The proposed detection technique and resilience EMS against FDI-attacks are effective solution for SBs having power exchange capability.

## 6.2 Future scope

Keeping this work in mind, the following topics can be suggested for future studies.

- In this work, we have used deterministic models of different types of smart home loads and distributed energy resources. For the future studies, these models can be improved by incorporating the stochastic behaviour of smart home loads and the DERs.

- Smart home cyber-physical system are vulnerable to various types of cyber-attacks. In this work, we have considered only FDI attack modeling and impacts. However, other types of attack modeling and impacts such as Denial-of-Service (DoS) and Man-in-the-Middle (MiTM) attacks can be considered for investigation.

- In this thesis, energy cost minimization is done based on various optimal scheduling techniques of smart home appliances. The energy cost minimization can also be performed using machine learning methods.

- Here, we have made scheduling resilient against FDI attack based on the consumer past behaviour, and import and export power constraints. In future. other bases for scheduling resilient to cyber-attacks can be investigated and formulated.