Dedicated

To

My Beloved Parents

CERTIFICATE

It is certified that the work contained in the thesis titled **Resilient Scheduling of Smart Buildings under False Data Injection Attack** by **Basant Kumar Sethi** has been carried out under my/our supervision and that this work has not been submitted elsewhere for a degree.
It is further certified that the student has fulfilled all the requirements of Comprehensive Examination, Candidacy and SOTA for the award of Ph.D. Degree.

Supervisor

Prof. Devender Singh

Deptt. of Electrical Engg.

IIT(BHU), Varanasi

Varanasi, India - 221005

Co- Supervisor

Prof. Rakesh Kumar Misra

Deptt. of Electrical Engg.

IIT(BHU), Varanasi

Varanasi, India - 221005

DECLARATION

I, **Basant Kumar Sethi**, certify that the work embodied in this thesis is my own bonafide work and carried out by me under the supervision of **Prof. Devender Singh** and **Prof. Rakesh Kumar Misra** from July-2017 to June-2022, at the Departement of Electrical Engineering, Indian Institute of Technology (BHU), Varanasi. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, etc., reported in journals, books, magazines, reports dissertations, theses, etc., or available at websites and have not included them in this thesis and have not cited as my own work.

Date: 27/06/2022
Place: Varanasi

Basant Kumar Sethi
(Basant Kumar Sethi)

CERTIFICATE BY THE SUPERVISOR

It is certified that the above statement made by the student is correct to the best of my/our knowledge.

Supervisor
Prof. Devender Singh
IIT(BHU), Varanasi

Co-Supervisor
Prof. Rakesk Kumar Misra
IIT(BHU), Varanasi

28.06.2022

Signature of Head of Department/Coordinator of School

आचार्य व विभागाध्यक्ष / PROFESSOR & HEAD
विद्युतीय अभियांत्रिकी विभाग / Department of Electrical Engineering
भारतीय प्रौद्योगिकी संस्थान / Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय) / (Banaras Hindu University)
Varanasi, U.P. (INDIA)

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: **Resilient Scheduling of Smart Buildings under False Data Injection Attack**
Name of Student: **Basant Kumar Sethi**

Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the Doctor of Philosophy.

Date: 27/06/2022
Place: Varanasi

Basant Kumar Sethi
(Basant Kumar Sethi)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute's copyright notice are indicated.

Acknowledgments

First of all, we are grateful for the opportunity to write this thesis, which will be the end of a five year journey towards a degree.

Though, only my name appears on the cover of this dissertation, so many great people have contributed to its production. I owe my gratitude to all those people who have made this thesis possible and because of whom my post graduate experience has been one that I will cherish forever.

I take this opportunity to express my profound gratitude and deep regards to my supervisors **Prof. Devender Singh** and **Prof. Rakesh Kumar Misra**, Electrical Engineering Department, IIT(BHU), Varanasi for their exemplary guidance, monitoring and constant encouragement throughout the course of this dissertation.

I want to express my deepest gratitude to **Dr. Soumya Ranjan Mohanty**, Electrical Engineering Department, IIT(BHU), Varanasi who supported me throughout my thesis work. I am grateful to **Mr. Amit Singh**, who provided me technical, moral and emotional support during my research program.

I want to express my deepest gratitude to **all staff of department of Electrical Engineering** especially **Mr. Satish Kumar Singh**, Junior technical superintendent, Electrical Engineering Department, IIT(BHU), Varanasi who supported me throughout my PhD work.

A very special gratitude goes out to my colleagues and friends with special mention to **Mr. Bables Jha, Mr. Abhishek Kumar, Mrs. Arpita Roy, Mr. Debottom Mukherjee, and Mr. Sachin Kumar**.

Finally, I would like to thank my father **Sanatan sethi**, my elder brother **Laxman Sethi** for always standing by me through both the good times and the bad.

Basant Kumar Sethi

Date: 27/06/2022 Basant Kumar Sethi

Abstract

Modern Smart Home Energy Management Systems (SHEMSs) are inherently prone to cyber-attacks due to their high exposure to the Information and Communication Technology (ICT), thereby requirement of scheduling schemes resilient to cyber-attacks is important. Further, current scenario of SHEMS may result in increased charging and discharging cycles deteriorating the battery life. Therefore, demand scheduling formulations also need to cater the effect of battery degradation cost along with user comfort. The present work attempts to formulate a comprehensive scheduling problem in terms of energy cost minimization considering the battery degradation cost. Further, a cyber-attack resilient scheduling model is proposed in the present study. This work investigates the effect of demand scheduling on the life span of battery as well as the energy cost. Further, False Data Injection (FDI) attack has been modelled using machine learning techniques, and its effects on the scheduling has been incorporated in the objective function. Scenario tree based stochastic bill generation has also been formulated to develop an FDI attack resilient scheduling. Optimisation results of the study have established that the resulting formulation is robust against FDI attacks.

A game-theory based optimal and cyber-attack resilient energy scheduling in multiple smart buildings framework considering FDI attack has been proposed in this work. The proposed resilient scheduling is based on the consumers' past behaviour, and import and export power between the smart buildings and grids. An optimal resilient energy scheduling framework is designed considering Renewable Energy Sources (RESs), Combined Heat and Power (CHP) generators, Battery Storage Systems (BSSs), various Smart Home (SH) appliances and FDI attack. An iterative algorithm is used to solve a game-theory based Mixed Integer Quadratic Constrained Program (MIQCP) problem in General Algebraic Model System (GAMS) environment with a CPLEX solver. For identifying the FDI attack and making a resilient scheduling against possible attacks, the proposed technique

uses the difference between the actual and forecasted bills as well as maximum change in demand. The impacts of FDI attack which can be detrimental can be avoided, however, there may be a small difference between energy cost without considering attack and energy cost with considering resilient scheduling.

Further, the proposed resilient scheduling also been formulated for interconnected multiple smart buildings having power exchange capability among themselves. It is considered that each smart building is equipped with different types of Distributed Energy Resources (DERs), BSSs, CHP generators, Thermal Storage Systems (TSSs) and smart appliances.

Thus, in this work, a comprehensive optimal and robust scheduling is formulated to mitigate the effects of FDI attacks. The proposed method uses the information of anomaly between the actual and forecasted bills for detecting the cyber attack and making a resilient scheduling against possible attacks.

Contents

Abstract **v**

List of Tables **xi**

List of Figures **xiii**

Nomenclature **xv**

1 Introduction **1**

1.1 Background and Motivation 1

1.1.1 Energy Management System (EMS) for Smart Buildings 1

1.1.2 Distributed Energy Resources (DERs) in Smart Buildings 4

1.1.3 Cyber-attacks on Smart Building EMS 4

1.2 Literature Review 6

1.2.1 Smart Building Energy Management System 6

1.2.2 Cyber-Attack 11

1.3 Research Gaps 15

1.4 Objectives of the Thesis 17

1.5 Organisation of the Thesis 17

2 Modeling of Components of Smart Home **21**

2.1 Introduction 21

2.2 Modeling of Distributed Energy Resources 21

2.2.1 Solar PV 22

2.2.2 Wind Turbine 23

2.2.3 CHP Generator 24

2.3 Modeling of Energy Storage Systems 26

2.3.1 Battery Storage Systems 26
2.3.2 Thermal Storage Systems 28
2.4 Modeling of Loads 29
2.4.1 Unschedulable and Noninterruptible Loads (UNLs) 30
2.4.2 Temperature Dependent Loads (TDLs) 30
2.4.3 Schedulable Loads (SLs) 32
2.5 Cyber-attack 32
2.6 Summary 33

3 Smart Home Energy Management System (SHEMS) under False Data Injection (FDI) Attack 35

3.1 Introduction 35
3.2 System Architecture 36
3.3 Problem Formulation 38
3.3.1 Energy Cost and Battery Degradation Cost Minimization 38
3.3.2 Price and Bill Prediction 40
3.3.3 FDI Attack Resilient Scheduling 41
3.4 Results and Discussion 42
3.4.1 Energy Scheduling Considering Battery Degradation Cost 45
3.4.2 Energy Scheduling under FDI Attack 50
3.4.3 FDI Attack Resilient Scheduling 51
3.5 Summary 54

4 Energy Management System for Smart Buildings under FDI Attack - Decentralized Approach 55

4.1 Introduction 55
4.2 System Architecture 56
4.3 Problem Formulation 58
4.3.1 Objective Function 58
4.3.2 Game-theory model 62
4.3.3 Price and Bill Prediction 62
4.3.4 Strategy of FDI Attack 64
4.4 Results and Discussion 64

4.4.1 Electricity Bill Minimization 67
4.4.2 FDI Attack analysis 69
4.5 Summary 73

5 Energy Management System for Smart Buildings under FDI Attack-Centralized Approach 75
5.1 Introduction 75
5.2 System Architecture 76
5.3 Problem Formulation 78
5.3.1 Energy Cost Minimization 78
5.3.2 Price and Bill Prediction 83
5.3.3 FDI Attack Detection and Defense Strategy 84
5.4 Results and Discussion 86
5.4.1 Energy Cost Minimization with and without Power Exchange among Smart Buildings 88
5.4.2 Analysis of FDI Attack Detection and Defense Strategy 93
5.5 A comparison of centralized/decentralized approaches 99
5.6 Summary 100

6 Conclusions and Future Scope 103
6.1 Conclusions 103
6.2 Future scope 104

List of Publications 123

List of Tables

1.1 Summary Types of Cyber-attack and Target System 16

3.1 Power Ratings of Unschedulable and Noninterruptible Loads (UNLs) . . . 42

3.2 Power Ratings of Schedulable Loads (SLs) 43

3.3 Power ratings of Temperature Dependant Loads (TDLs) 43

3.4 Battery Specifications. 43

3.5 Number of Components in the residential test system 43

3.6 Electricity Bill 52

4.1 Forecatsed Price 63

4.2 Specification of Components in Smart Home 66

4.3 Name plate of CHP Generator 66

4.4 Specification. 66

4.5 Maximum Change in Demand 71

4.6 Electricity Bill Comparison 71

4.7 Bill with Attack on Demand data and Attack on Price and Demand data (Coordinated) 72

5.1 Performance table on different training and testing data 84

5.3 Appliances Specification 87

5.2 Forecasted and Received Price 87

5.4 CHP Generator specification. 88

5.5 Renewable Energy Resources Specification. 88

5.6 Energy Cost 92

5.7 Energy cost under FDI attack and resilient scheduling against FDI attack . 93

5.8 Sensitivity Analysis 96

5.9 Comparison Between Anomaly Method and Proposed Method 97
5.10 Estimated β values 98
5.11 Bills of attack on demand data and both (price and demand) data 99

List of Figures

1.1 Sectorial Energy Consumption 2

1.2 Number of SH Growth Statistic 2

1.3 Residential electricity consumption 3

1.4 Renewable Energy Growth Capacity 5

1.5 Renewable Energy Source 5

2.1 Fuel Cell Based CHP Generator 25

2.2 Flowchart of Attack Vector Modelling 34

3.1 System Architecture 37

3.2 Scenario Tree for Bill Prediction 41

3.3 RES Generation [1] 44

3.4 Real Time Price (RTP) [1] 44

3.5 Expected load Variations During 24 Hours 45

3.6 Unscheduled and Scheduled Demand 46

3.7 RES Generation, Import and Export Power 46

3.8 Scheduled Demand with and without Battery Degradation Cost 47

3.9 Power Import 48

3.10 Power Export 48

3.11 SOC with and without Battery Degradation Cost 49

3.12 Charging and Discharging Cycles with and without Battery Degradation Cost 49

3.13 Utility Price with Attack 50

3.14 Power Demand without and with Attack 51

3.15 Scheduled Demand with and without FDI Attack Resilient 53

3.16 Power Import from Grid with and without Resilient 53

4.1 Architecture of SBEMS 57

4.2 Flowchart showing Prediction of Electricity Price 63

4.3 Detection Strategy Flowchart 65

4.4 RES Generation 67

4.5 Demand with and without Attack, and Resilient Scheduling 68

4.6 Import and Export Power with, and without Attack, and Resilient Scheduling 70

4.7 PDF of Electricity bill 72

5.1 Architecture of MSBEMS 77

5.2 flowchart depicting method of price forecasting 85

5.3 Flowchart Depicting the Detection Strategy 86

5.4 RES Generation 88

5.5 Scheduled demand with and without power exchange 89

5.6 Inter-Smart Building Power Exchange 90

5.7 Grid Exchange Power 91

5.8 Demand without attack, with attack and with resilient 94

5.9 Grid import and export power without attack, with attack and with resilient 95

Nomenclature

Abbreviations

2PE	Two-Point Estimation method
AC	Air Conditioner
BEMS	Building Energy Management System
BS	Battery Storage
BSS	Battery Storage System
CHP	Combined Heat and Power
CVaR	Conditional Value at Risk
DERs	Distributed Energy Resources
SLs	Schedulable Loads
DOD	Depth of Discharge
DR	Demand Response
DSM	Demand-Side Management
EMU	Energy Management Unit
EV	Electric Vehicle
EWH	Electric Water Heater
FDI	False Data Injection

UNLs	Unschedulable and Noniterruptible Loads
GA	Genetic Algorithm
GPR	Gaussian Process Regression
GWO	Grey wolf optimizer
HAN	Home Area Network
HEMS	Home Energy Management System
ICT	Information and Communication Technology
IT	Information Technology
LMU	Load Management Unit
LP	Linear Programming
MILP	Mixed-Integer Linear Programming
MINLP	Mixed-Integer Nonlinear Programming
MIQCP	Mixed-Integer Quadratic Programming
MSB	Multi Smart Building
MSBEMS	Multi Smart Building Energy Management System
MULP	Multiple-Users and Load Priority
PAR	Peak-to-Average Ratio
MDL	Maximum Demand Limit
PE	Point Estimation
PEL	Power Export Limit
PHEV	Plug-in Hybrid Electric Vehicle
PR	Power Ratio

PV	Photovoltaic cell
RE	Renewable Energy
RES	Renewable Energy Source
RMSE	Root Mean Suare Error
RTP	Real Time Pricing
SB	Smart Building
SH	Smart Home
SHEMS	Smart Home Energy Management System
SOC	State of Charge
TC	Thermal Capacity
TDLs	Temperature Dependent Loads
TOU	Time of Use
TSS	Thermal Storage System
TSOC	State of Charge of TSS
UN	Utility Networrk
PRL	Part Load Ratio
SM	smart meter

List of sets, parameters and variables

a_s	number of SLs
a_u	number of UNLs
a_{td}	number of TDLs
t	index of time
b	index of buildings
h	index of smart home
w	index of scenario
P^s	solar PV power in kW
DF	derating factor
P_{STC}	nominal PV array power
G_{STC}	solar radiance at STC
G_A	global solar radiation
T_{STC}	temperature under STC
C_T	PV temperature co-efficient
T_C	solar PV cell temperature
G	global solar radiation
BC	battery capacity
f	false injected data
h	actual smart meter data
y	smart meter output after attack
μ	mean

σ	standard deviation
T_a	ambient temperature
NT	normal operating cell temperature
P^w	wind power in kW
C_P	power co-efficient
V	wind speed in $meter/sec$
A	swept area in m^2
ρ	air density
σ	self discharging of battery
P^{ch}	charging power of battery
P^{ch}_{max}	maximum charging power of battery
P^{dis}	discharging power of battery
P^{dis}_{max}	maximum discharging power of battery
η^{ch}	battery charging efficiency
η^{dis}	battery discharging efficiency
Δt	time interval
P^{chp}_c	CHP rated capacity
P^{chp}	CHP output power
H^{chp}	CHP heat output
P_{TE}	CHP heat to electrical power ratio
T^{in}	internal temperature of refrigerator
ϵ	inertia constant for refrigerator

ϵ_{air}	factor of inertia of air for AC
η_{rf}	efficiency of refrigerator
K_{rf}	insulation constant of refrigerator
P_{rf}	power consumption of refrigerator
P_{rrf}	rated power of refrigerator
S_{rf}	ON/OFF status of refrigerator
T_r	room temperature for AC
P_{rac}	rated power of AC
K_{air}	thermal conductivity of AC
η_{ac}	efficiency of AC
S_{ac}	binary status of AC
P_{ac}	power consumption of AC
T_r^{min}	minimum room temperature
T_r^{max}	maximum room temperature
P_{SL}	power consumption by SL
S_{a_s}	binary status of a_s appliance
P_{a_s}	rated power of a_s appliance
C_{dis}	degradation cost due discharging cycle
C_{in}	initial investment cost of battery
n_{std}	permissible number of charging or discharging cycle
D	average DOD of battery
C_{DOD}	battery degradation cost due to DOD

C_{cyc}	battery degradation cost
B^p	predicted bill
π	probability
E	net energy of smart home
C	electricity cost
P_{UNLs}	power consumption of UNLs
P_{TDLs}	power consumption of TDLs
P^r	renewable power generation
d_{a_s}	time duration of appliance a_s to complete the task
tin_{a_s}	starting time of appliance a_s
$tout_{a_s}$	ending time of appliance a_s
P_{mdl}	maximum demand limit
T^{min}	minimum temperature
T^{max}	maximum temperature
SOC^{min}	minimum SOC
SOC^{max}	maximum SOC
B	actual bill
γ	attacked price
λ_g	natural gas price
λ_x	power export price
λ	reference/forecasted price
λ_{bmc}	battery maintenance cost

P^R	forecasted demand
τ	tolerance
P^{gimp}	grid import power
P^{gexp}	grid export power
P^{gex}	grid exchange power
P_{bim}	building import power
P_{bex}	building export power
P_{a_i}	total power consumption of ${a_i}^{th}$ appliance
P_{rated,a_i}	rated power of ${a_i}^{th}$ appliance
P_b	demand of b^{th} smart building
α_b	binary variable of grid
α_1	binary variable of battery storage system
P^{disT}	discharging power of TSS
P^{chT}	charging power of TSS
η^{disT}	discharging efficiency of TSS
η^{chT}	charging efficiency of TSS
α_2	binary variable of thermal storage system
SOC^T	SOC of TSS
SOC^T	SOC of TSS
H_h	total heat demand of h^{th} SH
H^{disT}	discharging heat of TSS
H^{chT}	charging heat of TSS