

# Contents

<b>Abstract</b>	<b>v</b>
<b>List of Tables</b>	<b>xi</b>
<b>List of Figures</b>	<b>xiii</b>
<b>Nomenclature</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
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
<b>2 Modeling of Components of Smart Home</b>	<b>21</b>
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
<b>3</b>	<b>Smart Home Energy Management System (SHEMS) under False Data Injection (FDI) Attack</b>	<b>35</b>
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
<b>4</b>	<b>Energy Management System for Smart Buildings under FDI Attack - Decentralized Approach</b>	<b>55</b>
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
<b>5</b>	<b>Energy Management System for Smart Buildings under FDI Attack-Centralized Approach</b>	<b>75</b>
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
<b>6</b>	<b>Conclusions and Future Scope</b>	<b>103</b>
6.1	Conclusions . . . . .	103
6.2	Future scope . . . . .	104
	<b>List of Publications</b>	<b>123</b>