Optimal and Resilient Control with Applications in Smart Distribution Grids

KAVEH PARIDARI

Licentiate Thesis
Stockholm, Sweden 2016

TRITA-EE 2016:128
ISSN 1653-5146
ISBN 978-91-7729-082-7

KTH Royal Institute of Technology
School of Electrical Engineering
Department of Automatic Control
SE-100 44 Stockholm
SWEDEN

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie licentiatesexamen i elektro och systemteknik torsdagen den 16 september 2016 klockan 14.00 i sal K1, Kungliga Tekniska högskolan, Teknikringen 56, Kemi, våningsplan 3, Stockholm.

Tryck: Universitetsservice US AB

Abstract

The power industry and society are facing the challenges and opportunities of transforming the present power grid into a smart grid. To meet these challenges, new types of control systems are connected over IT infrastructures. While this is done to meet highly set economical and environmental goals, it also introduces new sources of uncertainty in the control loops. In this thesis, we consider control design taking some of these uncertainties into account.

In Part I of the thesis, some economical and environmental concerns in smart grids are taken into account, and a scheduling framework for static loads (e.g., smart appliances in residential areas) and dynamic loads (e.g., energy storage systems) in the distribution level is investigated. This framework aims to reduce both the electricity bill and the CO_2 emissions in residential areas. A robust formulation is proposed taking the user behavior uncertainty into account, so that the optimal scheduling cost is less sensitive to unpredictable changes in user preferences. In addition, a novel distributed algorithm for the studied scheduling framework is proposed, which aims at minimizing the aggregated electricity cost of a network of apartments sharing an energy storage system. The proposed approach guarantees cooperation among consumers, and fairness in the use of the shared resources. We point out that the proposed scheduling framework is applicable to various uncertainty sources, storage technologies, and programmable electrical loads.

In Part II of the thesis, we study smart grid uncertainty resulting from possible security threats. Smart grids are one of the most complex cyber-physical systems considered, and are vulnerable to various cyber and physical attacks. These threats can affect the smart grid in different aspects such as efficiency, safety, reliability and robustness. We identify potential vulnerabilities in the interface between the physical and the IT infrastructures of the power system. These vulnerabilities may lead to an abnormal operation of the distribution network. In particular, relevant attack scenarios are introduced, together with their threat models, based on which impact analysis is being performed. The attack scenarios consider cyber adversaries that may corrupt a few measurements and reference signals, which may degrade the system's reliability and even destabilize the voltage magnitudes. In addition, a practical attack-resilient framework for networked control systems is proposed. This framework includes security information analytics to detect attacks and a resiliency policy to improve the performance of the system running under the attack. Stability and optimal performance of the networked control system under attack and by applying the proposed framework, is proved here. The framework has been applied to an energy management system and its efficiency is demonstrated on a critical attack scenario.

Acknowledgements

I would like to express my sincere appreciation towards my supervisor Henrik Sandberg, whose constructive support and guidance throughout the last years have lead to this work. I am also grateful to my co-supervisor Karl Henrik Johansson to whom I owe a substantial part of the knowledge of this thesis.

Special thanks to Alessandra Parisio, André Teixeira, and Tomonori Sadamoto for the helpful discussions and collaborations we had so far. I am also immensely grateful to my current and former colleagues at the department of Automatic Control. The time I spent with you and the fun moments we had so far make the department a place much more enjoyable to work. I would like to thank Hanna, Anneli, Silvia, Gerd, Karin, and Margreth for their excellent administrative support and help.

This work has been financially supported by the Swedish Research Council and the Knut and Alice Wallenberg Foundation, the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 608224, and the Swedish Civil Contingencies Agency. Their support is greatly acknowledged.

Finally, I would like to express my appreciation to my parents Mohsen and Minoo and my sister Kiana for their love and unconditional support throughout my life and my studies.

Contents

Chapter 1

Introduction

The world is facing an increasing energy demand. Simultaneously economical considerations and environmental concerns of promoting lower-carbon and high efficiency generation technology are becoming more and more important. Thus, the power industry and society are dealing with the challenges and opportunities of transforming the present power grid into a smart grid [13]. Development of the power grid helps the power industry to manage generation-demand balance, optimizing asset utilization, improving grid reliability, reducing environmental impact, etc. [19].

The smart grid is an electrical grid which is composed of a variety of operational and computational components including smart meters, smart appliances, renewable energy resources, and energy efficiency resources [35]. To monitor and control smart grids, industrial control systems (ICSs) play an important role [93]. ICS is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

In the electric power grid, residential areas are responsible for nearly 40% of the energy consumption in developed countries and are important consumers in the low voltage distribution level. Residential areas are known to have significant potential for energy and CO_2 emission saving, as well as for load shifting, compared to industry and transportation [90]. Thus, automatic control of electrical/thermal components in residential areal and buildings has become a necessary task for ICSs in order to achieve optimal performance. An ICS is called an energy management system (EMS) when it comes to the automatic control of electrical/thermal components in buildings. The aim of a modern EMS is to enhance the functionality of interactive control strategies leading towards energy efficiency and a more user friendly environment. In addition, penetration of distributed energy resources (DER) units that are connected to the distribution grid, can help consumers to decrease their CO_2 emission and electricity bill. DERs use renewable energy sources, including solar power, wind power, geothermal power, etc., and are located close to the load they serve. Most of the DERs are small-scale and inverter-based, which are connected at the low voltage distribution level. One way to take advantage of small-scale inverter-based DER units (which have uncertainty in terms of producing electricity), and also make them more flexible and efficient for consumers to manage their energy use, is to consider them to be collocated with energy storage systems (ESSs). Local integration of DERs and ESSs, has led to the concept of microgrids (MGs) [27, 71]. MGs can be defined as a cluster of loads, ESS and DER units that are operated in coordination and perceived as a single element by the main grid [51], which can operate in both grid-connected and islanded modes. EMS of MGs are connected to the building communication network.

These developments introduce new types of uncertainties that we need to handle in the smart grid, by making the control policies to be resilient against the emerged uncertainties. In this chapter we will give some motivating examples and introduce these uncertainties.

1.1 Motivating Applications

A few illustrative examples related to the smart distribution grid are presented here, to motivate the problems considered in this thesis.

Example 1.1.1 (Active apartments)**.**
Active *apartments are apartments where effective demand response policies are enabled through the integration of smart appliances, ESSs, scheduling algorithms, home automation systems, and information exchange over communication technologies. As an example, within the Stockholm Royal Seaport project [1], which is a new and environmentally sustainable city district being built in Stockholm, some active apartment buildings are available and occupied by families. Figure 1.1 depicts a schematic of an active apartment in the Royal Seaport project. It is of interest to investigate the potential of active apartments for saving electricity bill and reducing CO_2 emission by using an automation system for scheduling of smart appliances and ESS.*

Example 1.1.2 (HVAC system in a MG)**.**
An energy management system optimally controls all energy sources in a MG in order to minimise thermal and electrical energy consumption, while maximising users' comfort. Recently, a MG infrastructure [60] has been introduced to support both types of loads, where some equipment such as Combined Heat and Power (CHP) can be an energy source for both electrical and thermal demand. In this context, an energy management system would consider an HVAC (heating, ventilating, and air conditioning) system as an important contributor to the energy consumption. HVAC is the technology of indoor and vehicular environmental, which provides thermal comfort and acceptable indoor air quality. Figure 1.2 shows the HVAC system at the demo-site at Cork Institute of Technology. Here, the energy management system controls two main heating sources, the boiler and the CHP, which heat up the water

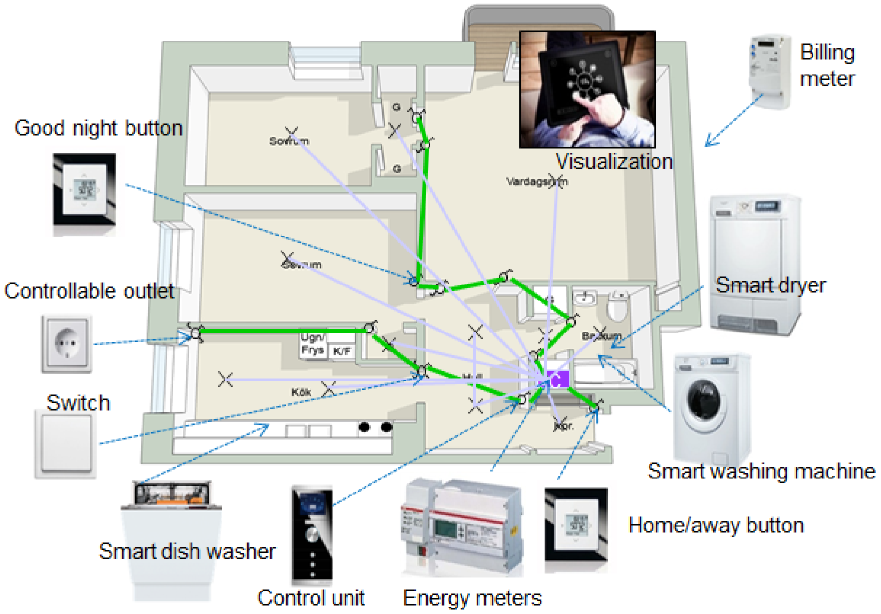

Figure 1.1: Schematic of an active apartment in the Royal Seaport project in Stockholm [1].

to a temperature set-point. The header flow delivers the heated water to each floor of the buildings (Nimbus and Rubicon), where a mixing valve is used to regulate each floor flow temperature. At the end, supplied water to each of the floors is distributed over several radiators in each building's floor, where radiator is controlled using an on/off controller to reach a predefined room temperature set-point. Since an energy management system considers an HVAC system as an important contributor to energy consumption, an HVAC system is a possible target for attacks with financial impact and to damage the heating sources (e.g. CHP and boilers). It is of interest to investigate a practical resilient policies to cope with possible adversarial actions to the HVAC system.

Example 1.1.3 (Large DER penetration to the distribution grid)**.**
High penetration levels of DER creates a different set of challenges at the distribution grid, than at transmission grid level. Given that distribution grid is generally designed to be operated in a radial fashion with one way flow of power to customers, and DER (including photovoltaic and wind technologies) interconnection violates this fundamental assumption. Impacts caused by high penetration levels of DER can be complex and severe and may include voltage increase, voltage fluctuation, reverse power flows, power quality and protection concerns, and current and voltage unbalance, among others. These impacts can become even more severe when the system is under adversarial actions. As shown in Figure 1.3, the power

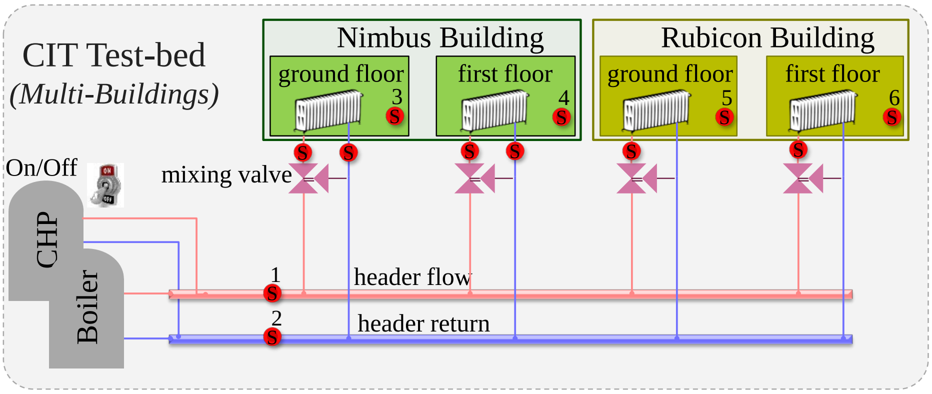

Figure 1.2: Typical BMS for HVAC system

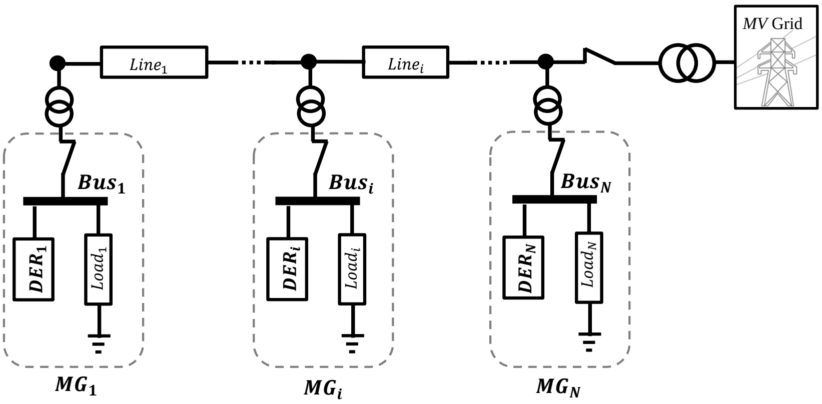

Figure 1.3: A power distribution system comprised of interconnected MGs with inverter-based DERs.

distribution grid is composed of a set of interconnected MGs that may be connected to the main grid. In this figure, the i^{th} MG (MG_i) is represented by the bus_i to which inverter-based DER_i and $Load_i$ are connected. It is of interest to investigate the stability and power sharing analysis of the controlled MGs under adversarial actions.

1.2 Objectives

The main objectives of this thesis are motivated by the examples discussed earlier. As it is mentioned, ICSs play an important role in order to achieve optimal perfor-

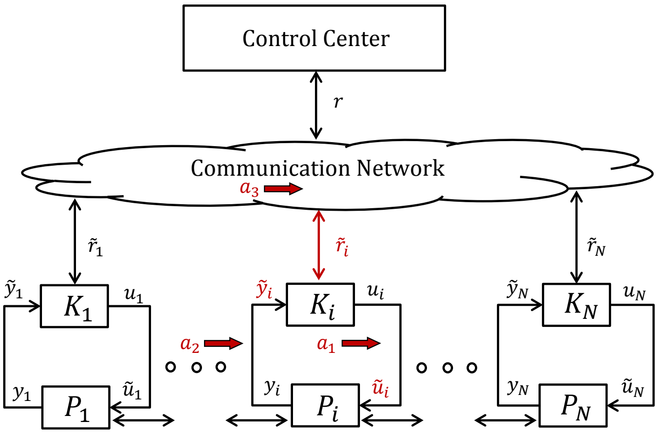

Figure 1.4: Generic block diagram of an ICS which is vulnerable to the uncertainties.

mance in smart grids. A general hierarchical structure of ICSs is considered here, which is composed of lower layer and supervisory layer (see Figure 1.4). The lower layer consists of physical interconnected infrastructure and local controllers. As it is shown in this figure, $P_1, ..., P_N$ are the interconnected plants which are controlled by the local controllers $K_1, ..., K_N$. Note that in different applications, P_i and K_i model different types of plants and controllers. For example, in the active apartment application, P_i refers to the aggregation of smart appliances in the i^{th} apartment, and K_i refers to the automation system in the i^{th} apartment. On the other hand, in the HVAC system in a MG application, P_i refers to different components of the HVAC system in Figure 1.2 (e.g., the boiler), and K_i refers to the local controller of that component (e.g., boiler's on/off controller). The supervisory layer, which is called control center here, can be viewed as the brain of the system. The control center sends set-point r_i to each controller K_i through the communication network and receives the status of the local controllers and measurement signals.

Here, we consider that the control signals (e.g., u_i), the measurement signals (e.g., y_i) and the reference signals (e.g., r_i) could be modified by a_1, a_2, and a_3, based on existing uncertainties. For example, user behavior uncertainties may modifies the control signal u_i, or adversarial actions on y_i or r_i may corrupt the measurement signal or the reference signal. These uncertainties may lead to a poor system performance, or can even cause instability. Thus it is crucial to make the ICS to be resilient against these uncertainties. To address these problems, the objectives of this thesis are divided into Part I and Part II. The main objectives in Part I are:

- Robust optimal control of residential loads, with the aim of minimizing electricity cost and CO$_2$ emission, under user behavior uncertainties (e.g., control signal u_i is modified by a_1).

- Distributed scheduling of loads in residential areas sharing an ESS, guaranteeing cooperation among consumers and fairness in the use of the shared resources among consumers.

The main objectives in Part II are:

- Voltage stability analysis of power distribution grids with high penetration levels of DERs, under adversarial actions (e.g., reference signal r_i is modified by a_3).
- Resilient optimal control of an HVAC system in a MG, in the sense of optimal state estimation, stability satisfaction, and performance improvement, under adversarial actions (e.g., measurement signal y_i is modified by a_2).

1.3 Thesis Outline

The contributions in each part of the thesis and the connection with the related publications are presented below.

Part I - This part has been motivated by the problem of reducing electricity bill and CO_2 emissions related to the energy consumption in active apartments equipped with automation system, smart appliances, and ESSs. A well studied scheduling framework for static loads (e.g., smart appliances in residential areas) and dynamic loads (e.g., energy storage systems) in residential areas, is presented here. Then a robust formulation of the studied scheduling framework is proposed. This robust scheduling framework takes the user behavior uncertainty into account so that the optimal scheduling cost is less sensitive to unpredictable changes in user preferences. In addition, a novel distributed algorithm for the studied scheduling framework is proposed in this part. The proposed distributed scheduling framework aims at minimizing the aggregated electricity costs of a network of apartments sharing an energy storage system. The proposed approach guarantees cooperation among consumers, and fairness in the use of the shared resources among consumers. These contributions have been published in the following articles.

K. Paridari, A. Parisio, H. Sandberg and K. H. Johansson. Robust scheduling of smart appliances in active apartments with user behavior uncertainty. *IEEE Transactions on Automation Science and Engineering, 13(1):247-259, 2016.*

K. Paridari, A. Parisio, H. Sandberg and K. H. Johansson. Demand response for aggregated residential consumers with energy storage sharing. In Proceedings of the *IEEE 54th Conference on Decision and Control (CDC), 2015.*

K. Paridari, A. Parisio, H. Sandberg and K. H. Johansson. Energy and CO_2 efficient scheduling of smart appliances in active houses equipped with batteries. In Proceedings of the *IEEE 10th International Conference on Automation Science and Engineering (CASE), 2014.* **Best student paper award finalist**.

Part II - In this part, we investigate security of cyber-physical networked control systems. To this end, we first identify potential vulnerabilities in the interface between the physical and the IT infrastructures of the power system. We show that these vulnerabilities may lead to an abnormal operation of the distribution network, which may degrade the system's reliability and even destabilize the voltage magnitudes. In addition, a practical cyber-secure framework for networked control systems is proposed in this part. This framework includes security information analytics to detect attacks, and a resilient policy to improve the performance of the system running under the attack. These contributions have been published in the following articles.

K. Paridari, et al. Attack-resilient industrial control systems: attack diagnosis and controller reconfiguration for energy management systems. In preparation, *2016.*

K. Paridari, A. E. Mady, S. La Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg and M. Boubekeur. Cyber-physical-security framework for building energy management system. In Proceedings of the *ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), 2016.*

A. Teixeira, **K. Paridari**, H. Sandberg and K. H. Johansson. Voltage control for interconnected microgrids under adversarial actions. In Proceedings of the *IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), 2015.*

Part I

Robust Optimal Demand Response in Residential Areas

Chapter 1

Introduction

The world is challenged by an increasing energy demand, economical consideration (reducing electricity cost), and environmental concerns of promoting lower-carbon and high efficiency generation technology. Thus, the power industry is facing the challenges and opportunities of transforming the present power grid into a smart grid. A smart grid is an electrical grid, composed of smart meters, smart appliances, renewable energy resources, computing elements and energy efficiency resources, which are integrated over a communication network.

1.1 Main Contributions

The main contributions of Part I are threefold. The first contribution presents a well studied scheduling framework for static loads (e.g., smart appliances in residential areas) and dynamic loads (e.g., ESSs), by considering the state of health of the dynamic loads. In addition, a case study is performed to assess the performance of the proposed scheduling framework to reduce both the electricity bill and the CO_2 emissions in residential areas. The above results have been published in [57].

As the second contribution, a robust formulation of the studied scheduling framework is proposed. This robust scheduling framework, takes the user behavior uncertainty into account so that the optimal scheduling cost is less sensitive to unpredictable changes in user preferences. In order to reduce the level of conservativeness of the robust solution, we introduce a parameter allowing to achieve a trade-off between the price of robustness and the protection against uncertainty. Mathematical insights into the robust formulation are illustrated and the sensitivity of the optimum cost in the presence of uncertainties is investigated. Although active apartments equipped with smart home appliances and EESs are considered as the case study here, we point out that the proposed scheduling framework is generally applicable to many use cases, e.g., charging and discharging of electrical vehicles in an effective way. In addition, it is applicable to various scenarios considering different uncertainty sources, different storage technologies and generic programmable electrical loads, as well as different optimization criteria. This contribution has been published in [59].

The third contribution in this part of the thesis, proposes a novel distributed algorithm for the studied scheduling framework. As the case study, a network of consumers coupled by energy resource sharing constraints is considered. The proposed distributed scheduling framework aims at minimizing the aggregated electricity costs. Each consumers is equipped with an energy management system that schedules the shiftable loads accounting for user preferences, while an aggregator entity coordinates the consumers demand and manages the interaction with the grid and the shared ESS via a distributed strategy. The proposed approach guarantees constraints satisfaction, cooperation among consumers, and fairness in the use of the shared resources among consumers. Performance of the proposed distributed algorithm in comparison with a centralized one is illustrated using numerical experiments. The above results have been published in [58].

1.2 Outline

The rest of Part I of this thesis is structured as follows. Chapter 2 presents some background in demand response, power consumption of an active apartment, and scheduling methods for scheduling of static and dynamic loads. A well studied scheduling framework for static and dynamic loads, by considering the state of health of the dynamic loads, is presented in Chapter 3. In Chapter 4, a robust formulation of the studied scheduling framework is proposed, which takes the user behavior uncertainty into account. Chapter 5 proposes a novel distributed algorithm for the scheduling framework. Finally, Chapter 6 provides conclusions and suggestions for future studies.

Chapter 2

Background

In this chapter, we present the background in demand response, power consumption of an active apartment, and scheduling methods for scheduling of static and dynamic loads.

2.1 Demand Response

Residential areas are responsible for nearly 40% of the energy consumption and CO_2 emission in developed countries. These areas are known to have significant potential for energy and cost savings, as well as load shifting (loads are classified as controllable (interruptible and non-interruptible) and uncontrollable), compared to industry and transportation [90]. Therefore, automation systems can be used to assist residents to take advantage of these potentials [44]. Demand Response (DR) is considered as the most cost-effective and reliable solution for the smoothing of the demand curve, when the system is under stress [86]. Thus, it has received increased attention in recent years since it can efficiently support load balancing and economical/environmental cost reduction [52], [72]. DR is commonly defined as changes in electricity use by consumers in response to changes in the electricity price over time [52], and help power markets set efficient energy prices, mitigate market power, improve economic efficiency, and increase safety [17]. Several studies have investigated the potential changes in residential electricity use under time-varying price rates by rescheduling smart (possible to control remotely) appliances [45, 25, 7]. The electricity use can also be sensitive to dynamic CO_2 intensity that is included in the demand response [80]. Thus, several works have focused on CO_2 emission factors and its potential impacts on the changes in household load profile, e.g., see [91], and also proposed load management strategies accounting for both price and CO_2 information (e.g., see [57, 76, 79, 77] and the Stockholm Royal Seaport project [1]). To achieve energy and cost savings and have effective DR policies, home appliances are required to be smart and have the ability of being switched on or off remotely and in response to price and CO_2 signals.

2.2 Load Scheduling Methods

Load scheduling problem is being formulated as an optimization problem in the literature. The optimization task is to minimize the single or multi-objective function. For example, in [77], a multi-objective optimization problem deal with a tradeoff between electricity costs and CO_2 emission, for which a dynamic programming solution is provided. Note that this tradeoff exists in certain countries including Sweden. To deal with this possible trade-off, different methods have been proposed. Weighted sum and ε-constrained approaches are two of these methods that have mostly been used in the literature [79, 77, 28]. In [28] a discrete time formulation is proposed for the scheduling problem and solves it by a minimum cut algorithm. In addition, to solve the multi-objective optimization problem, different conditions and constraints on the load operation and user time preferences should be considered.

2.3 Robust Load Scheduling

In the optimization problem for scheduling of smart appliances and ESSs, different sources of uncertainties may cause considerable deterioration in the expected outcomes (electricity bill and CO_2 emission savings), and should be taken into account. In the uncertainties which are related to the DR signals, electricity tariff and CO_2 foot-print are subject to real-time amendment or forecasting errors. These sources of uncertainties are well addressed and studied in the literature [17, 38, 37, 8].

There exist also uncertainties related to the energy consumption of smart appliances. For example, an optimization-based real-time residential load management algorithm has been proposed in [66], which takes into account uncertainties related to the power consumption and starting time of uncontrollable loads, in order to minimize the energy payment for each user. In addition, the authors of [16] propose an energy efficient scheduling algorithm taking into account the uncertainty in appliances energy consumption. The novelty in that work is the introduced energy consumption adaptation variable, which is used to model the stochastic energy consumption patterns for various household appliances.

It is known that the uncertainty can be handled by stochastic programming and robust approach, and stochastic programming generally requires higher computational burden (e.g., see numerical evaluations in [17], which indicates that the scenario based stochastic approach introduces higher computational burden than the robust approach). However a robust approach is more computationally appealing, it can lead to a conservative and potentially more expensive scheduling of appliances. In order to prevent too conservative solutions, the exist some approaches in the literature (see [9, 17, 22]).

2.4 Distributed Scheduling

Since ESS devices are still expensive, a reasonable solution to afford their expenses and benefit from the use of them would be to share it among several consumers. In addition, when the number of appliance in the residential areas increases, the computational burden for scheduling in a centralized fashion is remarkable. Therefore, the households should be coordinated by an aggregator/coordinator to share the benefits of shared ESS and also break down the computational burden. Aggregators are new entities in the electricity market that act as mediators between users and the utility operator, and possess the technology to perform DR signals and communicate with both users and utilities [24]. In [65], an algorithm is built on the alternating directions method of multipliers (ADMM), focusing on decentralized algorithms for Electric Vehicles charging. In addition, a coordination framework based on ADMM is proposed in [87] to negotiate among the households and a coordinator, with the main goal being to minimize the imbalance among communities, while including objectives and constraints for each community and taking into account each user's quality of life/activities. Based on our knowledge, the proposed frameworks in the literature are based on some assumptions (e.g., convexity of the problem) which may not be realistic, and thus their algorithm may not be directly implementable.

Chapter 3

Scheduling Framework for Constrained Power Consumption

Based on our knowledge, the mixed integer linear programming (MILP) framework that was proposed in [79] is more extendable (e.g. for including ESSs as dynamical loads) than the other methods proposed in the literature. Therefore, we base our study on the MILP framework proposed in [79] in Part I of this thesis.

3.1 Load Modeling and Problem Formulation

In this section, we formulate the smart home appliances and ESS scheduling problem in a MILP framework [79]. This framework considers the minimum electricity cost and CO_2 emission, and satisfies technical operation constraints of smart appliances and ESS, and consumer preferences. Electricity tariff and CO_2 footprint signals are assumed to be piecewise constant. Here, for scheduling of smart appliances, the appliances execution period is discretized into m uniform time slots Δt (e.g. Δt=10 minutes per slot). The number of appliances considered for scheduling is denoted by N, and n_i for $i = 1, 2, ..., N$, denotes the number of un-interruptible energy phases for each appliance. The energy assigned to energy phase j of appliance i during the whole period of time slot k is denoted by p_{ij}^k. In addition, auxiliary binary decision variables (x_{ij}^k) are required to indicate whether a particular energy phase is being processed or not. Moreover, two other sets of binary decision variables are needed to model the decision problem. One is denoted as s_{ij}^k, with a value of one indicating that, in appliance i, energy phase j is already finished by time slot k. The other set is denoted as t_{ij}^k. These decision variables are used to indicate whether at time slot k, appliance i is making a transition between running phase $j - 1$ to j. To minimize the electricity bill and CO_2 emission, a multi-objective optimization problem is proposed subject to the following constraints.

The constraint that is enforced to make sure that the energy phases fulfill their energy requirement is as

$$\sum_{k=1}^{m} p_{ij}^{k} = ER_{ij}, \quad \forall i, j, \tag{3.1}$$

where ER_{ij} is the energy requirements for energy phase j in appliance i. To determine that the lower and upper power limitation being assignment to the phase are satisfied, during time slot k, the constraint

$$\underline{p}_{ij}^{k} x_{ij}^{k} \leq p_{ij}^{k} \leq \overline{p}_{ij}^{k} x_{ij}^{k}, \quad \forall i, j, k, \tag{3.2}$$

is enforced, and the $\underline{p}_{ij}^{k}$ and $\overline{p}_{ij}^{k}$ are the lower and upper limits. Also, the power safety constraint can be imposed as

$$\sum_{i=1}^{N} \sum_{j=1}^{n_i} p_{ij}^{k} \leq \overline{P}^{k}, \quad \forall k. \tag{3.3}$$

$\overline{P}^{k}$ is the upper limit of the total energy assigned at time slot k. The limits on energy phases process time are imposed as

$$\underline{T}_{ij} \leq \sum_{k=1}^{m} x_{ij}^{k} \leq \overline{T}_{ij}, \quad \forall i, j, \tag{3.4}$$

where the $\underline{T}_{ij}$ and $\overline{T}_{ij}$ are the lower and upper limits of the number of time slots for energy phase j in appliance i to be processed. To satisfy the sequential processing of the energy phases of an appliance and also sequential operation between appliances, the following constraints are imposed respectively

$$\begin{array}{rcll} x_{ij}^{k} & \leq & s_{i(j-1)}^{k}, & \forall i, k, \forall j = 2, \ldots, n_i, \\ x_{ij}^{k} & \leq & s_{\tilde{i} n_{\tilde{i}}}^{k}, & \forall k, \end{array} \tag{3.5}$$

with the $\tilde{i}$ being the index of the appliance which must be finished before the appliance with i index can start running. To make sure that the energy phases are un-interruptible the following constraint is imposed.

$$\begin{array}{rcll} x_{ij}^{k} & \leq & 1 - s_{ij}^{k}, & \forall i, j, k, \\ x_{ij}^{k-1} - x_{ij}^{k} & \leq & s_{ij}^{k}, & \forall i, j, \forall k = 2, \ldots, m, \\ s_{ij}^{k-1} & \leq & s_{ij}^{k}, & \forall i, j, \forall k = 2, \ldots, m. \end{array} \tag{3.6}$$

To increase the benefits from DR signals, delays between energy phases are considered to be flexible in the smart appliances. This gives the smart appliances the capability of flexible electricity consumption to help the consumers to reduce electricity bill and CO_2 emission. To count the number of time slots spent between the energy phases in an appliance and impose lower and upper limits (which are technical specifications of each appliance and are provided by companies) on these numbers, the constraints

$$t_{ij}^k = s_{i(j-1)}^k - (x_{ij}^k + s_{ij}^k), \quad \forall i, j, \, \forall k = 2, \ldots, n_i, \tag{3.7}$$

$$\underline{D}_{ij} \leq \sum_{k=1}^{m} t_{ij}^k \leq \overline{D}_{ij}, \quad \forall i, \, \forall j = 2, \ldots, n_i, \tag{3.8}$$

are considered, where $\underline{D}_{ij}$ and $\overline{D}_{ij}$ are between-phase delay lower and upper bounds, respectively. Finally, to meet the household preferences and finishing a particular appliance within a specified time interval, the constraint

$$x_{ij}^k \leq TP_i^k, \quad \forall i, j, k, \tag{3.9}$$

is enforced, and TP_i^k is the time preference interval. To include an ESS in this framework, the following set of constraints is defined. The level of energy stored in the ESS at time slot k, should always satisfy the lower ($\underline{b}_s$) and upper ($\bar{b}_s$) limitations

$$\underline{b}_s \leq b_s^k \leq \bar{b}_s, \quad \forall k, \tag{3.10}$$

where b_s^k is the state of charge (SOC) of the ESS in time slot k. Moreover, to meet the lower and upper limitations on power exchanged with the ESS when it is charging or discharging during time slot k, the two constraints

$$0 \leq b_c^k \leq \bar{b}_c^k x_c^k \,, \quad 0 \leq b_d^k \leq \bar{b}_d^k x_d^k, \quad \forall k, \tag{3.11}$$

are enforced, in which the auxiliary binary decision variables x_c^k and x_d^k indicate whether the ESS is charging or discharging in time slot k, respectively. The power exchanged with the ESS during time slot k is denoted by b_c^k (or b_d^k) when the ESS is charging (or discharging). In addition, the constraint

$$x_c^k + x_d^k \leq 1, \quad \forall k, \tag{3.12}$$

should be satisfied to make sure that the ESS is not charging and discharging at the same time slot. To take the state of health of ESSs into account, the total number of charging and discharging cycles during a day should be limited to a determined number N_c, and the constraints

$$\begin{array}{rcl} x_c^k - x_c^{k-1} & \leq & c_t^k, \quad \forall k = 2, \ldots, m, \\ x_d^k - x_d^{k-1} & \leq & d_t^k, \quad \forall k = 2, \ldots, m, \\ \sum\limits_{k=1}^{m} c_t^k + d_t^k & \leq & N_c \,, \end{array} \tag{3.13}$$

should be satisfied, where the binary decision variables c_t^k and d_t^k determine the transition time slots to start charging and discharging, respectively. The dynamic system constraint

$$b_s^k = \alpha b_s^{k-1} + \eta_c b_c^{k-1} - \eta_d b_d^{k-1}, \quad \forall k = 2, \ldots, m, \tag{3.14}$$

describes the evolution of energy stored in the ESS, in which the α is a constant stored energy degradation in each sampling interval, and η_c and η_d are efficiencies accounting for the losses during charging and discharging. To satisfy the power balance in the system, the constraint

$$\sum_{i=1}^{N}\sum_{j=1}^{n_i} p_{ij}^k + b_c^k - b_d^k = p_G^k, \quad \forall k, \tag{3.15}$$

is enforced, where the exchanged power with the grid is denoted by p_G^k, and it should satisfy lower and upper limitations.

$$\underline{p}_G^k \leq p_G^k \leq \overline{p}_G^k, \quad \forall k, \tag{3.16}$$

where the lower limit is negative to allow energy selling to the grid. Finally, it is reasonable to assume that the initial and the final energy levels (b_s^0 and b_s^T respectively) in the ESS are the same, since the final energy level is also the initial condition for the next day scheduling. Hence, the following equality constraint on the initial and final SOC is enforced

$$b_s^0 = b_s^T. \tag{3.17}$$

Moreover, the initial level should be high enough to allow a flexible use of the ESS: in this study, we assume $b_s^0 = \underline{b}_s + \frac{\overline{b}_s - \underline{b}_s}{2}$. One can also consider b_s^0 as a variable, corresponding to the measured energy level of the ESS at the beginning of the day. Now the proposed multi-objective optimization problem of jointly scheduling smart appliances and ESS could be written as

$$\begin{array}{ll}
\underset{\substack{p,x,s,t,b_s,\\ b_c,b_d,x_c,x_d,\\ c_t,d_t,p_G}}{\text{minimize}} & \sum_{k=1}^{m} C_\lambda^k \, p_G^k \\
\text{subject to} & \text{constraints (3.1), (3.2), (3.4)} - \text{(3.9), (3.10)} - \text{(3.17)} \\
& \lambda \in [0,1], \\
& p_{ij}^k \in \mathbb{R}, \quad \forall i,j,k, \\
& x_{ij}^k, s_{ij}^k \in 0,1, \quad \forall i,j,k, \\
& t_{ij}^k \in 0,1, \quad \forall i,k, \quad \forall j = 2,\ldots,n_i, \\
& b_s^k, b_c^k, b_d^k, p_G^k \in \mathbb{R}, \quad \forall k, \\
& x_c^k, x_d^k, c_t^k, d_t^k \in 0,1, \quad \forall k,
\end{array} \tag{3.18}$$

which is called nominal problem (NOM). In the objective function, the weighted sum of electricity tariff and CO$_2$ footprint ($(1-\lambda)E^k + \lambda C^k$) is denoted by C_λ^k, and p_G^k is the total energy exchanged by the grid at time slot k. Note that the cost function is parameterized by the weighting parameter $\lambda \in [0,1]$ (that would be chosen by end-users), in which $\lambda = 0$ implies end-users only care about the electricity bill, while for $\lambda = 1$ they only take CO$_2$ emission into account. Thus, by changing the parameter λ from 0 to 1,and solving the minimization problem in (3.18), the convex hull for the Pareto curve ([14]) of our multi-objective minimization problem would be generated. The following normalizations are applied in (3.18)

$$E^k = \frac{e^k}{\max(e^1, e^2, ..., e^m)}, \quad C^k = \frac{c^k}{\max(c^1, c^2, ..., c^m)}, \tag{3.19}$$

where e^k and c^k denote the electricity bill and CO_2 foot-print for time slot k respectively and based on given 24-hour ahead tariff curves (which are piecewise constant).

Remark 3.1.1. The formulation discussed in this section can be applicable for electrical vehicles with a slight modification considering that an electrical vehicle may drive during some periods in a day. Thus, to integrate electrical vehicles in the automation systems, time preferences for electrical vehicle batteries are to be modeled in the problem formulation (similar to the time preferences introduced for smart appliances in (3.9)). Hence, the constraints

$$x_c^k \leq T_{Ec}^k, \quad x_d^k \leq T_{Ed}^k, \quad \forall k, \tag{3.20}$$

have to be added to the constraints defined from (3.10) to (3.14). Here, T_{Ec}^k and T_{Ed}^k characterize time preference intervals for charging and discharging of electrical vehicle's battery, respectively.

Remark 3.1.2. The proposed framework can provide useful insights into more effective carbon pricing, which accounts for the CO_2 emissions. Consider, for instance, that the carbon price is set as e_{CO_2} Euro per kg of CO_2 emitted; hence, the emission cost per kWh of exchanged power at each time slot k is $e_c^k = e_{CO_2} e^k$ Euro. The objective function of (3.18) can be slightly modified to include the environmental taxes as $\big((1-\lambda)E_c^k + \lambda C^k\big)p_G^k$, where E_c^k and C^k are obtained by normalizing respectively $e_c^k + e^k$ and c^k with respect to the total electricity price per kWh for the consumers at time slot k. By doing so, lambda can be interpreted as the percentage of the total cost associated to the carbon content of the electricity consumed; thus, our framework can give indications of how to incentivize a desired user behavior.

3.2 Use Cases

Here we describe how the proposed scheduling framework can be applied to relevant practical use cases, and capture relevant real world scenarios.

Power Consumption of an Active Apartment

To investigate the potential of active apartments (described in Example 1.1.1) for saving electricity bill and reducing CO_2 emission, it is necessary to have the information related to hourly energy consumption in these apartments. Within the Stockholm Royal Seaport project [1], which is a new, environmentally sustainable city district being built in Stockholm, some active apartment buildings are available and occupied by families. In the Stockholm Royal Seaport project, hourly power consumption of two active apartments which are occupied by families is available. The data has been kindly provided by Fortum Corporation, which is actively involved in this project. To assess the potential of automated active apartments for saving electricity bill and reducing CO_2 emission, it is necessary to have the information related to hourly energy consumption in apartments without automation system, and the portion of household appliances in their energy consumption. Thus, to determine the hourly power consumption of household appliances vs other consumptions, a comparison with previous works is done. In [94], apartments average hourly power consumption is a result of the empirical measuring of a total of 199 apartments between the years 2005-2008 in Sweden, which is done by the Swedish Energy Agency. In that study, five types of apartments (singles 26-64 years old and above the age of 64, couples 26-64 years old and above the age of 64 and families 26-64 years old) are taken into account. Among all these 199 apartments, 125 of them were occupied by families 26-64 years old (more than 60%) and here the data related to them is being used for comparison with the available data from Stockholm Royal Seaport project. Figure. 3.1 shows average hourly power consumption of apartments occupied with families who are 26-64 years old, in which 4% of the consumption is devoted to run washing-machine and dryer and 4% for dish-washer, and the remaining consumption is used for the other appliances. Based on these information and considering Figure. 3.1, estimated average hourly power consumption of appliances vs other consumptions for the two active apartments is shown in Figure. 3.2. As it is obvious in these two figures, the average hourly load curve profile of the studied active apartments is very similar to that of the apartments monitored in [94]. The only thing to be noticed, is that the total amount of energy being used in one day in the active apartments is approximately 9.9 kWh on average, and in comparison with the apartments that were studied in [94] (consuming 12,6 kWh on average) has decreased more than 20%. This reduction in power consumption is reasonable based on the modern home appliances that are used in the active apartments. For the simulation purposes in the next chapters of part I, 10000 active apartments with smart appliances and ESS, for the evaluation of DR programs, have been considered.

Power Consumption of Electric Vehicles

Transportation is another application area of our mathematical framework, which is the other major contributor to energy use. Transportation increases green house gas in the atmosphere and is one of the largest fossil fuel users in the world [33]. Thus, electrical vehicles have the potential of reducing fuel consumption and CO_2 emission, and optimal scheduling for charging and discharging the batteries in the electrical vehicles is a key to integrate large numbers of them in the smart grid. By optimal scheduling, electrical vehicles could function as distributed generation and energy storage, supply loads, and smooth the unpredictable renewable generation (e.g. wind and solar energy).

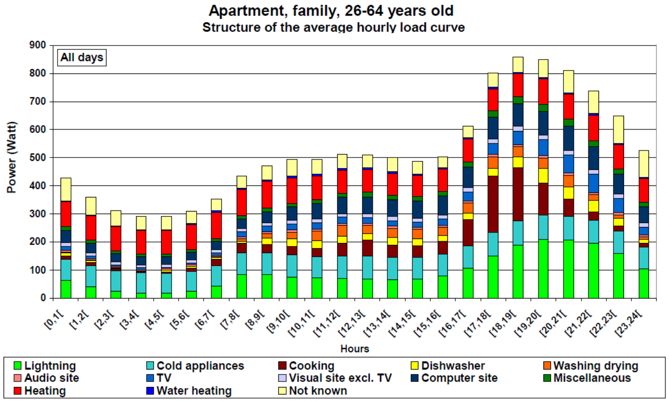

Figure 3.1: Average hourly power consumption for years 2005-2008 [94].

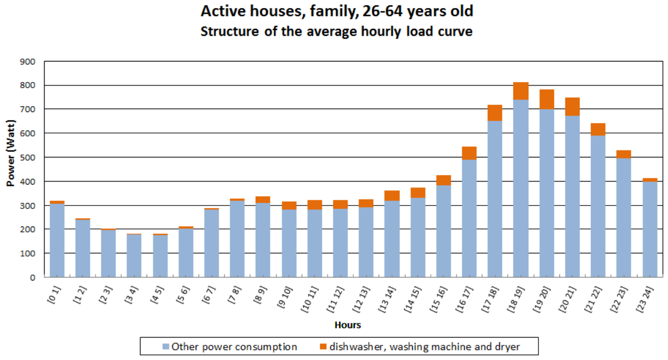

Figure 3.2: Estimated average hourly power consumption of appliances vs other consumptions (for March 2013 - January 2014) of two active apartments.

Carbon Pricing

The other relevant application area concerns environmental-related taxes and carbon pricing. The global increase in emissions raises the need of designing an effective set of environmental-related taxes that effectively reduce the global energy-related CO_2 emissions, which should be based on the carbon content of fossil fuels that are purchased and consumed. In this context, carbon pricing is a central issue. Current prices put on carbon by means of taxes or emissions trading systems in developed countries, including Sweden, are generally much lower than those needed to limit the global average temperature increase. Governments should therefore take measures to reduce the entire carbon footprint rather than their territorial emissions; namely, an optimal policy for global pollutants like CO_2 must consider the implications of international trade [53, 32]. Further, since households have generally a relevant impact on the carbon footprint, changing household consumption patterns is central to achieving sustainable development and incentivize substantial behavioural adjustments to be successful in the climate change challenge. Considering Sweden for instance, the majority of the impact on the carbon footprint is caused through households (76%) [49]. In the current institutional Swedish setting, a low carbon lifestyle is not sufficiently rewarded. Besides, the biggest portion, 43%, of the total costs for electricity currently paid by the Swedish consumer are environmental taxes (i.e., an energy tax and a quota obligation assigned to the electricity end-users for renewable electricity) and a value added tax; however, these environmental taxes for households account for other external effects than CO_2 emissions, such as noise, congestion and road wear from traffic [40].

3.3 Numerical Studies

To illustrate the efficiency of the proposed scheduling framework and also the potential future benefits of automation systems in active houses, which are provided by DR signals, 10000 apartments are considered as a case study. For this case study, three different scenarios including reference apartments (without automation system), test apartment (equipped with automation system), and test apartment with ESS (equipped with automation system and ESS) have been taken into account and compared with each other. Throughout the comparison, average hourly power consumption data from the mentioned two real active apartments (Figure. 3.2) is used, and is considered as the average hourly power consumption of the reference apartment. The technical specifications of the smart appliances (dishwasher, washing machine, and dryer) in the simulations have been extracted from [79]. For each scenario, the number and types of the smart appliances that are running in one day in those 10000 apartments, can be calculated from these technical specification, average hourly power consumption data from the two real active apartments in the day, and considering the fact that 4% of energy consumption is devoted to the washing-machine and dryer and 4% for dish-washer. Thus, by having the number and types of smart appliances, solving the multi-objective optimization (3.18) for scheduling of appliances yield to average hourly power consumption for the 10000 test apartments. To include ESS in the automation system, one should consider some limitations (e.g. charging rate and capacity), inefficiencies, and nonlinear relationships between life cycles and depth of discharge. An ESS with the following specifications is considered for the apartments with ESS

- Storage capacity: 1700 Wh
- Maximum power exchange: 1000 W
- Maximum depth of discharge: 30%
- Stored energy degradation (α): negligible
- Charging and discharging efficiency: 90%
- Maximum charging and discharging cycles: 5 (per day).

Table 3.1: Bill and CO_2 saving in 10000 active apartments (June 2013).

λ	0	0.25	0.5	0.75	1
Saving without using ESS					
CO_2 (%)	-2.88	-0.23	1.05	1.79	1.98
CO_2 (kg)	-2330	-183	849	1447	1602
bill (%)	2.41	2.16	1.56	0.68	-0.22
bill (SEK)	19013	17032	12305	5336	-1751
Saving by using ESS					
CO_2 (%)	-5.01	0.37	5.56	7.66	8.02
CO_2 (kg)	-4057	297	4501	6200	6491
bill (%)	4.94	4.10	2.46	0.70	-1.10
bill (SEK)	38948	32304	19371	5502	-8669

Solving the multi-objective optimization (3.18) for scheduling of appliances and ESS (with the mentioned specifications), yields the average hourly power consumption for the 10000 test apartments with ESS. In Figure. 3.3 average hourly power consumption curves related to smart appliances and ESS, for these three scenarios of apartments for June 2013, is shown. Note that, to show the differences more clearly, only the consumption related to the smart appliances and ESSs has beed illustrated. In addition, the total bill and CO_2 savings in these 10000 apartments for the test apartment and test apartment with ESS are compared in Table 3.1, in terms of percent and amount of saving. In all the simulations, hourly price tariffs for June 2013 are downloaded from Nordpool website [2]. In addition, the SVK website [3] provide us with electricity generation by fuel type data, electricity import, and electricity export for 2013 and hourly CO_2 foot print curves can be computed based on these data [80]. Average hourly electricity generation by fuel type data, import and export for June 2013 is shown in Figure. 3.4.

Simulations are all done on a 64bit Windows system with an Intel Core i7-3770, 3.40GHz and 16.0 GB of RAM, in Matlab R2014b. Note that the optimization problem here is posed as a MILP and solved by CPLEX (using the YALMIP MATLAB interface), which is a commercial implementation of a branch-and-bound algorithm.

Environmental and Economic Benefits

As it is mentioned in [80], in certain countries like Sweden there sometimes exists a trade-off between environmental and economic consideration, and for some electricity generation mixes, price and CO_2 intensity are negatively correlated. Moreover, it is shown in [80] that the Swedish CO_2 intensity is very sensitive to import of high carbon intensity power generation. Thus, considering only economic incentives for shifting load could result in an increased CO_2 emission, and this is obvious in the case under study. Figure 3.3 shows the comparison between the average hourly energy profiles of smart home appliances and ESS for the reference apartment, test

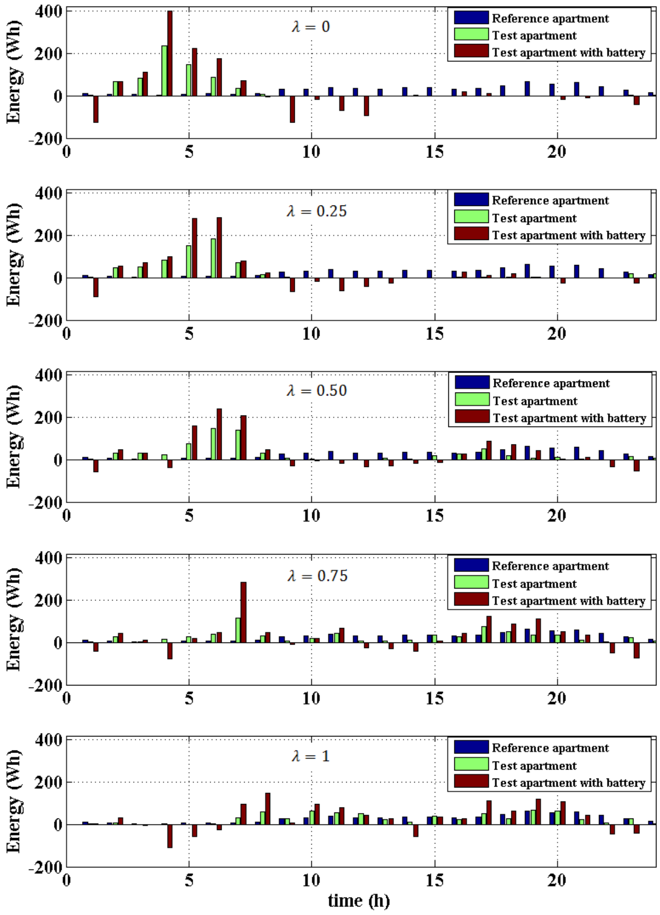

Figure 3.3: Average hourly load curves of three type of active apartments in June 2013 for different values of the weight parameter (λ).

apartment, and test apartment with ESS under different attitude of users toward the electricity bill and CO_2 emission (different λ). Comparing Figures 3.3 and 3.4 we may notice that for $\lambda = 0$ (considering economic profits only), the load tends to be shifted to the hours when the ratio of import energy to energy sources such as hydropower and nuclear power is higher (between 03:00 and 06:00), because Sweden imports are relatively inexpensive [77]. This leads to 4.94% bill saving for test apartments with ESS (Table 3.1) that is more than twice the saving in test apartment without ESS (2.41%). This scenario yields CO_2 emission to be increased with 2.88% and 5.01% for test apartments without and with ESS, respectively, which is

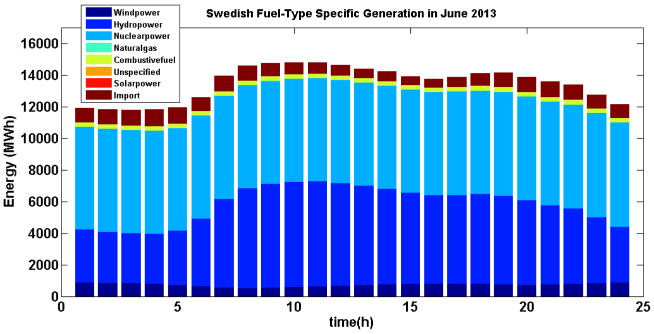

Figure 3.4: Average hourly Swedish Fuel-Type Specific Generation in June 2013.

not environmentally desired. This is due to the use of energy imported during night from Denmark, Germany and Poland whose primary energy source is combustive fuel power plants and is CO_2 intense (303, 430, and 640 gCO_2/kWh respectively), while clean energy sources such as hydropower and nuclear power have negligible CO_2 intensity (4 and 16 gCO_2/kWh respectively) [80].

On the opposite, for $\lambda = 1$ (caring about environmental impact only), the load tends to be distributed within the hours when the ratio of import energy to clean energy sources such as hydropower and nuclear power is lower (between 07:00 and 22:00). As it is illustrated in Table 3.1, scheduling in test apartment with ESS yields 8.02% CO_2 saving (more than four times of the saving in the test apartment without ESS), while increasing the electricity expenses by 1.1%, which is not desired economically. Therefore, for most customers it is most convenient to care both environmental and economic benefits. Consider, for instance, $\lambda = 0.5$ and the test apartments with ESS: in this case, we can have 5.56% and 2.46% CO_2 and bill saving, respectively, which is desirable both environmentally and economically.

ESS Profitability

To take the cost of ESS into account, and to investigate whether the ESS usage in the proposed method is profitable or not, life cycles of the deployed ESS is calculated. In the literature, lead-acid ESS for smart houses are commonly utilized [50]. In the manufacturers ESS specification data sheet for the lead-acid ESS, the number of life cycles versus different depth of discharge is given. Further, charging and discharging efficiencies for lead-acid ESS are generally 85-95%. If we consider the schedule of smart appliances and ESS in the test apartments in June 2013 (for example for $\lambda = 0.25$), simulation results show that for 10000 apartment in 30 days, ESS will be used 475513 times in total, and the depth of discharge is 21% on average. Based on the mentioned data sheet, for this percent of depth of discharge, the number of life cycles is 2600 for an ESS. We can conclude that an ESS would be economically viable if it costs less than 2500 SEK. However, we remark that the use of ESS is environmentally beneficial.

Table 3.2: Bill and CO_2 saving in 10000 active apartments, affected by time preferences (June 2013).

λ	0	0.25	0.5	0.75	1
Saving without using ESS					
CO_2 (%)	-1.31	0.71	1.59	1.80	1.84
bill (%)	0.62	0.42	0.14	-0.09	-0.41
Saving by using ESS					
CO_2 (%)	-3.44	1.31	6.10	7.67	8.02
bill (%)	3.15	2.36	1.04	-0.07	-1.39

Chapter 4

Robust Optimal Scheduling of Smart Appliances and Energy Storage Systems

In this chapter, we propose a robust approach for scheduling of smart appliances and ESS in active apartments with the aim of reducing both the electricity bill and the CO_2 emissions.

4.1 Uncertainty Modeling

By running the optimization scheduling algorithm, the automation system will achieve optimal points of running appliances, but there exists uncertainty in the user behavior, and they might run the appliances earlier or later. Thus, in the optimization problem (3.18) that is formulated as a MILP, there exist uncertainties on the decision variables. Note that in the literature, usually the uncertainties are assumed to be on coefficients of the inequality constraints [41, 9, 10]. Thus, the idea here is to map the uncertainty on the decision variable to an equivalent uncertainty in the weighted sum tariff, which is illustrated in Figure. 4.1. As should be clear from this figure, deviating from starting times x_1 and x_2 by at most M time slots ($M\Delta t$), turn into a variability of the tariff by at most Δy_1 and Δy_2, respectively. The parameter M can be defined based on the empirical model of the users, by having the historical data related to the uncertainties in their behaviors. This means deviating from the optimal start time of appliances, would affect the cost function, and could be equivalently considered as variability of the tariff curve that depends on the behavior of the curve in the neighbourhood of starting time. Thus, the variability in the tariff curve is mapped to the uncertainty in weighted sum tariff C_λ^k, and similar to what is done in [41], the uncertain tariff $\widetilde{C}_\lambda^k$, range in the interval:

$$|\widetilde{C}_\lambda^k - C_\lambda^k| \leq \epsilon^k |C_\lambda^k|, \quad \forall k. \tag{4.1}$$

Here, the parameter $\epsilon^k \geq 0$ is an uncertainty level at time k. As it was mentioned, deviating from the optimal start time of appliances, would affect the cost function

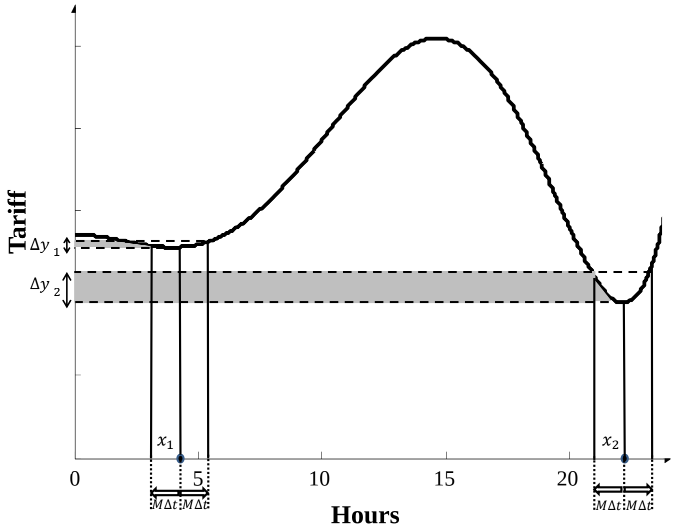

Figure 4.1: Mapping the user behavior uncertainty to tariff uncertainty.

in accordance to the behavior of the tariff curve in the neighbourhood of starting time. To apply the robust method, ϵ^k is defined as

$$\epsilon^k = \frac{\max(C_\lambda^k, \sum\limits_{i=k-M}^{k+M} \frac{C_\lambda^i}{2M+1}) - C_\lambda^k}{\max(C_\lambda^k, \sum\limits_{i=k-M}^{k+M} \frac{C_\lambda^i}{2M+1})}, \quad \forall k, \tag{4.2}$$

which is a function of the tariff curve within an interval of $\pm M\Delta t$ minutes in the neighbourhood of time slot k. Figure. 4.2 shows that the more variation we have in the tariff curve in the neighborhood of a time slot, the larger the ϵ^k we have for that time slot. The uncertain tariff $\widetilde{C}_\lambda^k$ in (4.1) appears as linear coefficient in the above inequality constraint and the robust optimization technique which is described in the following can be applied for that. Here, it is assumed that the scheduling of the EES is done by the automation system in the active apartments and only scheduling of the smart appliances is faced with uncertainty. The reason is that, the automation system recommends users when to run the appliances, but they can choose to ignore the recommendation and run the appliances earlier or later, but the EES would be scheduled by the automation system.

Remark 4.1.1. When the exchanged power limitation in (3.16) is low, then customer scheduling will also affect the ESS scheduling, as they are dependent regarding the equation (3.15). This is not the case for Sweden, and as the upper limitation in (3.16) is high enough, the EES will charge when the weighted sum tariff is low, and discharge when it is high, and is independent of appliances scheduling.

4.2 Robust Optimal Scheduling

Based on the uncertainty modeling and by defining the uncertain tariff $\widetilde{C}_{\lambda}^{k}$, the N$OM$ problem in (3.18) can be expressed in a generalized way as

$$\begin{array}{ll} \underset{\substack{p,x,s,t,b_s,\\ b_c,b_d,x_c,x_d,\\ c_t,d_t,p_G}}{\text{minimize}} & \sum_{k=1}^{m}\left(\widetilde{C}_{\lambda}^{k}\sum_{i=1}^{N}\sum_{j=1}^{n_i}p_{ij}^{k}+C_{\lambda}^{k}(b_c^k-b_d^k)\right) \\ \text{subject to} & \text{the constraints in (3.18).} \end{array} \tag{4.3}$$

By using the worst-case values of the uncertain parameter $\widetilde{C}_{\lambda}^{k}$, the problem in (4.3) can be written equivalently (e.g., see [41])as

$$\begin{array}{ll} \underset{\substack{p,x,s,t,b_s,\\ b_c,b_d,x_c,x_d,\\ c_t,d_t,p_G}}{\text{minimize}} & \sum_{k=1}^{m}C_{\lambda}^{k}\,p_G^k+\sum_{k=1}^{m}\epsilon^k\,C_{\lambda}^{k}\left(\sum_{i=1}^{N}\sum_{j=1}^{n_i}p_{ij}^{k}\right) \\ \text{subject to} & \text{the constraints in (3.18),} \end{array} \tag{4.4}$$

which is called robust optimization problem (ROB) here. A concern with this approach is that it might be conservative, and produces solutions whose objective function value is much worse than the nominal one. Effectively, by considering uncertain parameters we provide a robust solution that is feasible in all scenarios that uncertain parameters variations could be defined. For example, all the possible tariff curves being located in the gray area in Figure. 4.2are possible scenarios. However this comes at the cost of a degradation of the objective value, which could be excessive as some of the uncertain scenarios rarely occur. This increase in cost over the nominal solution is the so called *price of robustness* [10]. We then formulate an optimization problem where the degree of uncertainty can be regulated by a parameter denoted by Γ. The aim of the proposed approach is to compute schedules that are insensitive against the variation of at most Γ time slots. By varying Γ, the level of conservatism of the solution, can be controlled. The authors in [9, 10] prove that, even when more than Γ elements vary, the robust solution will be feasible with high probability.

Problem ROB is then modified such that the weighted sum tariff can be uncertain in at most Γ time slots as follow

$$\begin{array}{ll} \underset{\substack{p,x,s,t,b_s,\\ b_c,b_d,x_c,x_d,\\ c_t,d_t,p_G,q,z}}{\text{minimize}} & \sum_{k=1}^{m}C_{\lambda}^{k}\,p_G^k+z\,\Gamma+\sum_{k=1}^{m}q^k \\ \text{subject to} & \text{the constraints in (3.18),} \\ & \epsilon^k\,C_{\lambda}^{k}\left(\sum_{i=1}^{N}\sum_{j=1}^{n_i}p_{ij}^{k}\right)\le z+q^k, \quad \forall k, \\ & 0\le q^k, \quad \forall k, \\ & 0\le z, \end{array} \tag{4.5}$$

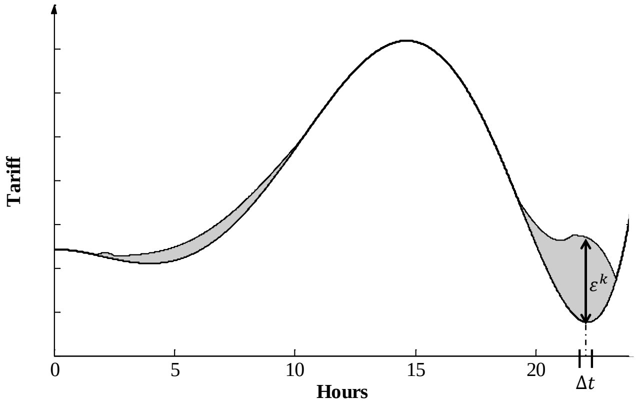

Figure 4.2: ϵ^k behavior for different time slot.

which is called flexible robust problem (R$OB-\Gamma$). The parameter Γ is also defined as *protection level* of the schedule cost against uncertainty in the user behavior. This parameter can be defined based on the empirical model of the users, by having the historical data related to the uncertainties in their behaviors.

Remark 4.2.1. In the MILP problem R$OB-\Gamma$, by having $\Gamma = 0$ the problem turns to the NOM problem and represents the most optimistic case, and the influence of user behavior uncertainty on the cost variations is completely ignored. On the other hand, by having $\Gamma = m$, user behavior uncertainty at all time slots will be considered for possible cost variations, which is the most conservative case (see [9] and [10]) and the problem is equivalent to the ROB problem.

Remark 4.2.2. The proposed framework can be generally applied to other scenarios where different sources of uncertainty and different optimization criteria must be considered. For instance, ϵ^k can represent the variation from the day-ahead price at time slot k in the real-time energy market, while different optimization criteria can account for the user comfort or the demand peak reduction.

Mathematical Insights into the Robust Formulation

Here we will provide some insights into the robust formulation in (4.5). In particular, we aim at investigating the effect of the protection level Γ on the robust schedule.

Model of Cost Uncertainty: As described in [9], we assume that each entry $\widetilde{C}^k_\lambda$, $k = 1, \dots, m$ takes values in $\left[C^k_\lambda, C^k_\lambda + d^k\right]$, where $d^k = \varepsilon^k C^k_\lambda$ represents the variation from the nominal cost coefficient, C^k_λ. We allow the possibility to have $d^k = 0$, since ε^k can be zero for some $k = 1, \dots, m$. We remind that, in this study, cost variations model the uncertainty in the user behavior.

As in [9], the parameter Γ controls the protection level for the objective function against cost variations.

Let $K = \{k|\varepsilon_k > 0\}$; Γ is assumed to be integer and takes values in $[0, |K|]$, where 0 indicates the nominal solution and $|K|$ the most conservative solution. Generally, Γ represents a tradeoff between the level of conservativeness and the cost of the robust solution: the higher is Γ, the less sensitive is the solution to cost variations at the cost of a higher nominal cost.

In the next section, we will investigate more into detail the robust counterpart of problem (4.4) in order to understand the effect on the robust schedule of increasing or decreasing the protection level Γ.

In the following, vectors are denoted by bold letters.

Interpreting the Robust Counterpart of the Scheduling Problem: In the robust approach, the best solution which is feasible for any realization of the data uncertainty in the given set is computed through the solution of the robust counterpart optimization problem. In our study, the robust counterpart of the scheduling problem (3.18) can be written as

$$\begin{aligned} \underset{\substack{p,x,s,t,b_s,\\ b_c,b_d,x_c,x_d,\\ c_t,d_t,p_G}}{\text{minimize}} \quad & \sum_{k=1}^{m} C_\lambda^k p_G^k + \beta(\boldsymbol{p}, \Gamma) \\ \text{subject to} \quad & \text{the constraints in (3.18)}, \end{aligned} \tag{4.6}$$

where $\beta(\boldsymbol{p}, \Gamma)$ is the protection function of the objective, $\rho^k := \sum\limits_{i=1}^{N} \sum\limits_{j=1}^{n_i} p_{ij}^k$ and $\boldsymbol{p} := \left[\rho^1, \ldots, \rho^m\right]^{'}$. To solve the robust counterpart optimization problem, we will show how to convert the objective function of the problem (4.6) to a linear one by following the approach in [9] and resorting to the duality.

The protection function equals the objective function of the following linear optimization problem

$$\begin{aligned} \beta(\boldsymbol{p}, \Gamma) = & \underset{\boldsymbol{z}^0}{\text{maximize}} \quad \sum_{k \in K} d^k |\rho^k| z^{0k} \\ & \text{subject to} \quad \sum_{k \in K} z^{0k} \leq \Gamma, \\ & \qquad\qquad\quad 0 \leq z^{0k} \leq 1, \quad \forall k \in K. \end{aligned} \tag{4.7}$$

Notice that ρ^k is nonnegative in our study, hence $|\rho^k| = \rho^k$; in the following we will drop the absolute value. Subsequently, we consider the dual problem of (4.7), which is then the primal.

We recall that in a dual problem a variable is introduced for each constraint in the primal so that the number of variables in the dual is equal to the number of constraints in the primal. Then the variable z is associated to the first constraint of (4.7), which involve the protection level Γ as right-hand side, and a variables q^k is associated to each constraint defining the upper bound on z^{0k}. Notice that the dual variables z and q^k are the ones introduced in problem R$OB - \Gamma$.

Consider then the dual of the problem (4.7)

$$\begin{aligned} \underset{z,\boldsymbol{q}}{\text{minimize}} \quad & \sum_{k \in K} q^k + \Gamma z \\ \text{subject to} \quad & z + q^k \geq d^k \rho^k, \\ & 0 \leq z, \ 0 \leq q^k, \forall k \in K. \end{aligned} \tag{4.8}$$

Substituting to problem (4.6), we obtain that problem (4.6) is equivalent to problem (4.5). We refer the reader to [9] for further details.

We now aim at gaining some insights into the optimal value of the protection function and how increasing the protection level Γ affects the robust solution. We start with some definitions and assumptions. Given a vector $\boldsymbol{p}_*$, let $\boldsymbol{z}_*^0$ be the optimal primal solution and $(z_*, \boldsymbol{q}_*)$ the optimal dual solution for problems (4.7) and (4.8) respectively (under non-degeneracy, the primal and dual optimal solutions are unique. In case of multiple optima, an unique optimal point can be selected by the help of appropriate tie-break rules, e.g., the lexicographic order [68]).

Without loss of generality, we assume that the indices are ordered in such that $d^1\rho_*^1 \geq d^2\rho_*^2 \geq \cdots \geq d^{|K|}\rho_*^{|K|}$. Further, assume that there are $n \geq 0$ time slots corresponding to the same value of the cost variation due to the uncertainty level, which we denote by $\bar{d\rho}$. Define the following sets of indices for time steps $k \in K$

$$\begin{aligned} \mathrm{I}_i \quad & := \quad \{i, i+1, \ldots, i+n\}, \\ \mathrm{I}_1 \quad & := \quad \{1, 2, \ldots, i-1\}, \\ \mathrm{I}_{|K|} \quad & := \quad \{i+n+1, \ldots, |K|\}, \end{aligned}$$

with $|\mathrm{I}_1| \leq \Gamma$. Notice that the set I_1 contains the time steps k with the highest values of $d^k\rho_*^k$, while the set I_i is the set of time steps with the same value of the cost variation, defined above as $\bar{d\rho}$.

We will now compute the optimal values of the primal variables in $\boldsymbol{z}_*^0$ and the dual variables in $(z_*, \boldsymbol{q}_*)$.

Notice that the dual variable z measures how the primal objective function will change if the Γ increases. If increasing Γ the value of the objective function changes, the corresponding dual, z, is positive. On the other hand, if when the primal problem is solved, the constraint with Γ is not active, this means that increasing Γ is not going to improve the objective function; hence $z = 0$. If $z > 0$, increasing Γ would be beneficial; this means that the corresponding constraint should be active at optimality. This relationship between dual variables and constraints in the primal must satisfy the complementary conditions, which mathematically state what has been explained above. At optimality, the complementary conditions must hold $\forall k \in K$

1. $z_*^{0k}\ (z_* + q_*^k - d^k\rho_*^k) = 0$
2. $z_*\ (\Gamma - \sum_{k \in K} z_*^{0k}) = 0$
3. $q_*^k\ (1 - z_*^{0k}) = 0.$

Consider the case when $n > 1$. From the complementary conditions we can derive the optimal solution of the primal and dual problems (4.7) and (4.8)

$$\begin{array}{ll} q_*^k \geq 0,\ z_* = d^k\rho_*^k - q_*^k, & \forall k \in \mathrm{I}_1, \\ q_*^k = 0,\ z_* = \bar{d}\bar{\rho}, & \forall k \in \mathrm{I}_i, \\ q_*^k = 0,\ z_* \geq d^k\rho_*^k, & \forall k \in \mathrm{I}_{|K|}, \\ z_*^{0k} = 1, & \forall k \in \mathrm{I}_1, \\ z_*^{0k} \in (0,1), & \forall k \in \mathrm{I}_i, \\ z_*^{0k} = 0, & \forall k \in \mathrm{I}_{|K|}. \end{array}$$

Notice that, if $n = |\mathrm{I}_i| > 0$ there will be multiple optimal solutions, since any combination such that $\sum_{k\in\mathrm{I}_i} z^{0k} = \Gamma - |\mathrm{I}_1|$ is an optimal solution of problem (4.6), corresponding to the same value of the objective function.

The optimal values of z_* and q_*^k are then

$$\begin{array}{l} z_* = \bar{d}\bar{p}, \\ q_*^k = d^k\rho_*^k - z_*, \quad \forall k \in I_1. \end{array}$$

If $n \leq 1$, at optimality there are clearly not time steps such that $z_*^{0k} \in (0,1)$. This means that we need only two sets of indices: *i)* $\mathrm{I}_1 := \{1, 2, \ldots, \Gamma\}$, containing Γ time steps k with the highest values of $d^k\rho_*^k$; *ii)* $\mathrm{I}_{|K|} := \{\Gamma+1, \ldots, |K|\}$. In this case, $z_* = \max_{k\in\mathrm{I}_{|K|}} d^k\rho_*^k$. Summarizing, at optimality, given the optimal appliances power assignment $\boldsymbol{p}_*$, the optimal value of the protection function in (4.4) is

$$\beta(\boldsymbol{p}_*, \Gamma) = (\Gamma - |\mathrm{I}_1|)z_* + \sum_{k\in\mathrm{I}_1} d^k\rho_*^k, \tag{4.9}$$

where $z_* = \max_{k\in\mathrm{I}_{|K|}\cup\mathrm{I}_i} d^k\rho_*^k$ and $|\mathrm{I}_1|$ being the cardinality of set I_1. From the discussion above and, in particular from (4.9), we can draw some conclusions about the effect of changing the protection level Γ on the robust solution

- as Γ grows, z_* decreases and $\sum_{k\in\mathrm{I}_1} q_*^k$ increases, since the number of time steps with $q_*^k > 0$, i.e. $|\mathrm{I}_1|$, become larger. This means that the robust optimal solution is affected more and more by the uncertain cost profile $\widetilde{C}_\lambda^k$ and less by the nominal cost profile C_λ^k, $\forall k \in K$. Then, the power assignment is generally shifted from time steps k with the lowest values of C_λ^k to time steps with lower values of $\widetilde{C}_\lambda^k$, mainly where variations are small or zero, despite the nominal tariff C_λ^k is higher;
- when the protection level Γ is small, the solution is less robust against cost variations. This entails that the optimal value of z is strictly positive and it can be used to assign power to time steps with low nominal tariffs and still high values of cost variations. When Γ increases, the optimal solution of problem (4.8) is required to be less and less sensitive to cost variations: hence, a larger number of q_*^k are to be strictly positive and a larger amount of power is assigned to time steps with small or zero variations. It can be interesting

to notice that, in cases when $\widetilde{C}_\lambda^k$ and C_λ^k have similar profiles $\forall k \in K$, the nominal and the robust schedules get closer as Γ grows. In this cases, having a high protection level does not bring any benefit;

- if Γ is larger than the number of time steps k when $d^k \rho_*^k > 0$, $z_* = 0$ and the set I_1 collects all the time steps k such that $d^k \rho_*^k > 0$. In this case, the robust solution of problem (4.5) does not depend on Γ and stays constant as Γ grows;

- for a certain value of Γ, the constraint with Γ in (4.7) is not active and then $z = 0$. This occurs when a protection is required for a number of time slots larger than the number of time slots when it is convenient to have a positive cost variation, which entails that it is convenient to buy or sell energy from/to the grid despite a positive uncertainty level. Since the constraints on the overall energy requirements, the power limits and the process times do not depend on Γ and stay the same both in the nominal and in the robust formulations, the number of time slots with a positive cost variation associated to the optimal nominal power schedule can provide a rough estimation of this value of Γ. Increasing Γ further will not change the solution of the robust optimization problem $\mathrm{R}OB - \Gamma$.

4.3 Numerical Studies

In this section, effectiveness of the proposed robust approach, in the presence of user behavior uncertainty, is shown by the simulation. In the simulations, user time preferences are considered to be uncertain, which means for each appliance the starting time, and consequently finishing time, are supposed to vary within an interval of $\pm M\Delta t = \pm 120$ minutes from their nominal value. Then we apply both the nominal and the robust approaches and we compare the computed schedules in terms of costs and sensitivity to variations of the time preferences from their nominal values. The nominal schedule is computed by solving the problem $\mathrm{R}OB-\Gamma$ with $\Gamma = 0$. The robust scheduling problem is solved with different choices of the parameter Γ in order to find the best schedule accounting for an uncertain user behavior with a reasonably small increase in cost compared to the nominal schedule.

In the simulations, the technical specifications of the smart appliances (dishwasher, washing machine, and dryer), hourly price tariffs and CO_2 foot print for June 2013, and ESS specifications are the same as the ones in Section 3.3.

To generate scenarios for simulating user behavior uncertainties in the proposed robust approach, a sampling method can be used, in which the starting time of the first energy phase of each appliance (t_{i1}^k) is considered as a variable or control input, that is allowed to vary within an interval of $t_{i1}^* \pm M\Delta t$. Here, the t_{i1}^* is the optimum starting time for the first energy phase of i^{th} appliance scheduled by $\mathrm{R}OB - \Gamma$ approach. The most common sampling method is indisputably the pure Monte Carlo, mainly because of its simplicity [23]. However, as the number of samples are limited because of the computational time, this method is known to have poor space filling properties, and leaving large un-sampled regions. Here, the Latin hypercube sampling (LHS) method [48] which is an extension of stratified sampling is utilized to generate the scenarios. The LHS method ensures that each of the input variables has all of its range represented, and partition it into the equally probable intervals. In this method, a LHS of size Y (number of partitions for each input, which is the number of time slots within the interval of $t^*_{i1} \pm M\Delta t$, that is equal to $2M + 1$) with W number of inputs (each input is the start time of one of the appliances in this work, and by having three appliances, the number of inputs is three here), is obtained from a random selection of Y values (one per stratum) for each input. Thus we achieve W Y-tuples that form the W columns of the YxW matrix of scenarios generated by LHS, that means the ith row of this matrix contains one of the partition for each input variable and will correspond to the ith scenario [29].

Sensitivity Analysis of Robust Approach

By solving the problem R$OB - \Gamma$, the sensitivity of the solution (e.g., minimum electricity bill) with respect to the user behavior uncertainty (different $M\Delta t$) and degree of robustness Γ is investigated here. The simulation results for the optimal electricity bill (here $\lambda = 0$) on 14th of June 2013 in Sweden is depicted in Figure. 4.3. The figure shows that the robust schedules outperform the nominal schedule, i.e. the one corresponding to $\Gamma = 0$ in terms of costs in the presence of user uncertainty. In particular, the best uncertain cost could be achieved when $\Gamma = 18$ and having a value of $\Gamma > 18$ does not bring any benefit in terms of costs; this is because the variable z in (4.5) is zero when $\Gamma = 18$, which implies that increasing the protection level does not change the solution. In the simulations, time slot interval $\Delta t = 10$ minutes has been considered.

Remark 4.3.1. Here, for the sensitivity analysis, different values of M have been discussed. One should notice that in the future, and by having historical data related to the user behavior uncertainties, it would be possible to determine the related M for each user and subsequently defining uncertainty level ϵ^k more precisely.

In the other simulation, effect of degree of robustness Γ on shifting the loads has been studied. In Figure. 4.4, scheduling of appliances by applying R$OB - \Gamma$ approach with $\Gamma = 0$ and $\Gamma = 18$, for $M = 12$, is depicted in Figure. 4.4. In addition, day-ahead tariff, uncertain tariff and also uncertainty level ϵ^k are shown in that figure. As it is shown in this figure, by changing the degree of robustness from $\Gamma = 0$ to $\Gamma = 18$, the scheduled dryer has been shifted from the evening to the morning to avoid the possible occurrence (in the presence of user behavior uncertainty) with the high price of electricity between 22:00 and 23:00. The number of binary variables, continuous variables and constraints (which are the most important indicators in MILP problem), in the R$OB - \Gamma$ ($\Gamma = 18$) problem, are 6624, 3027, and 22461, respectively. It takes 1.57 seconds to solve this problem by CPLEX in Matlab R2014b.

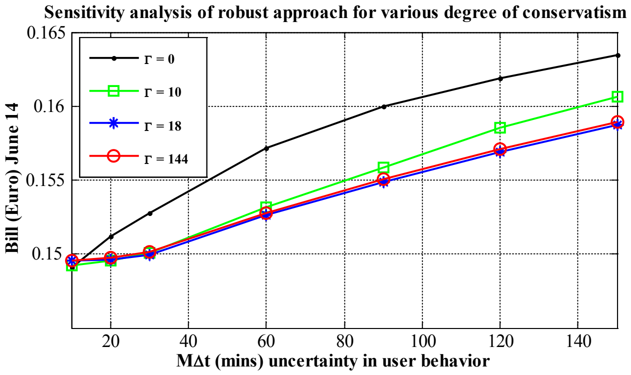

Figure 4.3: Sensitivity analysis of $ROB - \Gamma$ approach for various degree of conservatism Γ. By having $\Gamma = 0$, the problem turns to the NOM problem and represents the most optimistic case in which user behavior uncertainty is completely ignored (high sensitivity to uncertainty), and $\Gamma = 144$ is related to the the most conservative approach and the problem is equivalent to the ROB problem.

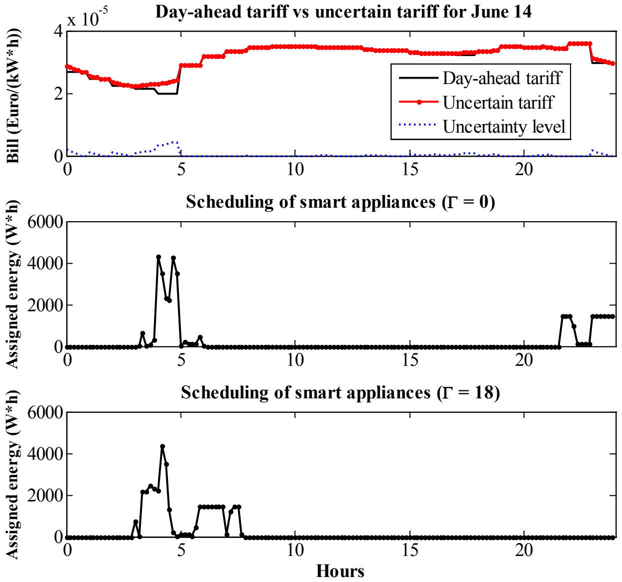

Figure 4.4: Scheduling of appliances by applying $ROB - \Gamma$ approach with $\Gamma = 0$ (turns to NOM problem, and user behavior uncertainty is completely ignored) and $\Gamma = 18$ (in which dryer has been shifted from the evening to the morning to avoid the possible occurrence with the high price of electricity between 22:00 and 23:00, in the presence of user behavior uncertainty).

Impact of DR Signals on the Electricity Bill and CO_2 Saving in the Robust Approach

Here, by considering the both CO_2 intensity and electricity tariff signals, the effect of robust scheduling on bill and CO_2 emission savings in the automated apartment equipped with ESS is investigated. Taking into account the impact of user time preferences on the load shift, the scheduling of appliances have been computed for time preferences between 08:00 and 24:00 hours. Note that this time interval has been chosen based on Figure. 3.2, which shows that families in active apartments are more interested to run their household appliances within this period. In Figure. 4.5, impact of R$OB-\Gamma$ approach on bill and CO_2 savings for 10000 apartments (with user behavior uncertainty consideration) in June 2013 is investigated. In this figure, savings for three different scenarios have been studied: 1) the scenario with the non-robust approach, in which there exists uncertainty and the NOM approach has been applied, 2) the scenario with the robust approach, in which there exists uncertainty and the R$OB-\Gamma$ approach has been applied, and 3) the performance bound scenario, in which there is no uncertainty on user behavior and the NOM approach has been applied. Despite of having relatively small variability in the electricity tariff and CO_2 foot-print signals (low uncertainty level) in June 2013, the simulation results show, that the proposed robust scheduling algorithm increases the savings on CO_2 emissions and the electricity bill in the presence of user behavior uncertainty.

As it is shown in this figure, there exists a tradeoff between electricity costs and CO_2 emission in certain countries including Sweden. This means, the more caring about the electricity price, the more CO_2 emission is produced. Thus, the automation system will provide the users with the cost of electricity and CO_2 emission for different choice of λ (e.g., for $\lambda = 0, 0.25, 0.5, 0.75, 1$), and they can decide which one is of their interest. For example, by choosing λ in the middle range (e.g., for $\lambda = 0.25, 0.5$ in Figure. 4.5) for the case under study, users will have both bill and CO_2 emission savings. By choosing $\lambda \geq 0.75$ (or $\lambda \leq 0.25$), despite the CO_2 (or bill) saving, electricity cost (or CO_2 emission) increases.

Simulations are all done on a 64bit Windows system with an Intel Core i7-3770, 3.40GHz and 16.0 GB of RAM, in Matlab R2014b. The computation times for different simulation show that the computational time difference for solving the NOM problem and R$OB-\Gamma$ problem (for the same number of appliances with the same characteristics, and same user input) is negligible.

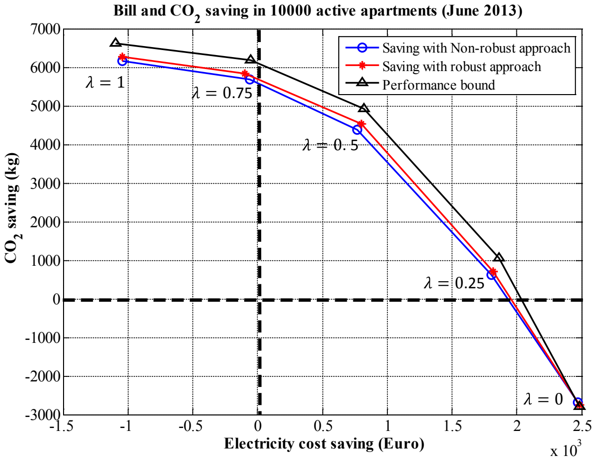

Figure 4.5: Impact of robust approach on bill and CO_2 savings in 10000 active apartments with user behavior uncertainty (convex hull for the Pareto curve ([14]) of the multi-objective minimization problem).

Chapter 5

Distributed Scheduling of Smart Appliances and Energy Storage Systems

In this chapter, a novel distributed optimization algorithm is proposed for scheduling of smart appliances in residential areas sharing an ESS. Here, the detailed modeling of loads and ESS is done and the state of health of the ESS is taken into account. In addition, there is no unrealistic assumption in the algorithm and it is directly implementable in the real world.

5.1 System Layout

As depicted in Figure 5.1, we consider a small-scale community here, which can range from the apartments in one building to a small district of a city. Each apartment is equipped with a Home Energy Management System (HEMS), which is responsible for locally operating end-user smart appliances. Each HEMS is connected to the aggregator entity via a communication network, which aims at coordinating the apartments, scheduling the ESS and managing the interaction with the distribution grid. The overall system has one single point of common coupling (PCC) with the distribution grid. The apartments are independent from each other and coupled only through the shared ESS and the PCC's power limits. In this structure, the aggregator coordinates the apartments through energy shift request signals. In this negotiation, the aggregator provides economical incentives to home users to modify their energy pattern.

5.2 Distributed Scheduling Algorithm

Here we describe the distributed algorithm for the energy management of the system under consideration. The algorithm comprises an initialization step, and the definition of MILP problems at the apartment and aggregator levels.

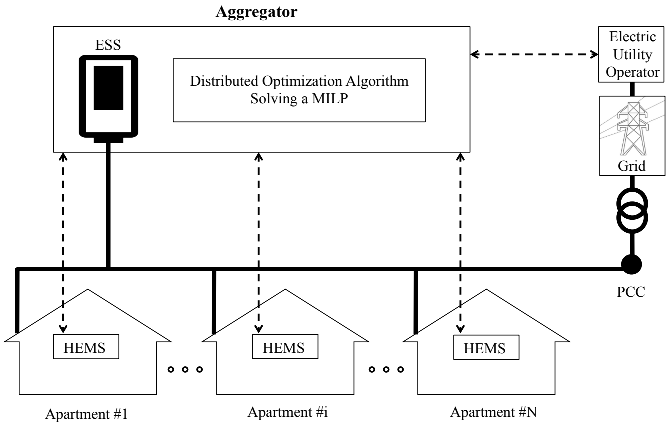

Figure 5.1: Schematic of interconnected apartments and aggregator.

Parameters and Variables: Table 5.1 reports all the other parameters and variables defined in the algorithm.

Table 5.1: Parameters and variables involved in the algorithm

l	iteration number within current time step
N	number of apartments/single-family houses
N_a	number of appliances of apartment a
$p_{G,l}$	total exchanged power with the grid at iteration l
$p_{ija,l}$	power feeding into the apartment a (for appliance i and energy phase j) at iteration l
β	penalty on the unsatisfied share of energy shift required by the Aggregator
γ	reward on the redistributed part of unsatisfied energy shift
$\underline{p}_G$, $\overline{p}_G$	lower and upper bounds on the power exchanged with the grid
$p_{T,l}$	profile of aggregated energy demand at iteration l by all the apartments
E_T	total energy requirements by all the apartments during whole the day
$G_{T,l}$	total profit due to the ESS at iteration l at the end of the horizon
$G_{\mathrm{a},l}$	profit per apartment at iteration l
Δp_l	energy shift required by the Aggregator at iteration l
$\delta p_{\mathrm{a},l}$	accepted energy shift by apartment a at iteration l
$\tilde{p}_{\mathrm{a},l}$	unsatisfied share of energy shift by apartment a at iteration l
$\delta p_{+a,l}$, $\delta p_{-a,l}$	redistributed energy shift by apartment a at iteration l ("+" for energy increase and "-" for energy decrease)

Assumption 5.2.1. *In this chapter the main focus is on the distributed algorithm and we do not consider uncertainties in the optimization problem.*

Remark 5.2.1. The proposed framework here can be generally applied to the scenarios where different sources of uncertainty and different optimization criteria must be considered. For instance, by adding the augmented term (see the robust optimization problem ROB in (4.4)) to the cost function of optimization problems at the apartment level, we can simply generalize the distributed algorithm to a robust distributed algorithm.

Algorithm Initialization

For the initial iteration of the algorithm, the following problem is solved for each apartment ($\forall a = 1, \ldots, N$):

$$\begin{array}{ll} \min & \sum\limits_{k=1}^{T} c^k \left(\sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p_{ija,0}^k \right) \\ \text{s.t.} & \text{constraints } (3.1) - (3.9). \end{array} \tag{5.1}$$

The aggregated demand profile, resulting from solving the optimization problem (5.1) for each apartment, represents the solution of the centralized problem (3.18) without including ESS. This means, without considering shared ESS, the problem of scheduling smart appliances for aggregated apartments is fully separable.

Remark 5.2.2. Sum of the optimal costs for all the apartment, without considering ESS, is an upper bound on the optimal solution of the centralized problem (3.18) with a shared ESS for all the apartments. This sum is computed as $G_{T,0} = \sum\limits_{k=1}^{T} C_\lambda^k \left(\sum\limits_{a=1}^{N} \sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p_{ija,0}^k \right)$.

To initialize the aggregator, the following problem is solved:

$$\begin{array}{ll} \min & \sum_k C_\lambda^k p_{G,0}^k \\ \text{s.t.} & \text{constraints } (3.14) - (3.17) \\ & p_{G,0}^k + b_c^k - b_d^k = p_{G,0}^k \\ & \underline{p}_G^k \leq p_{G,0}^k \leq \overline{p}_G^k \\ & \sum\limits_{k=1}^{T} p_{G,0}^k = E_T. \end{array} \tag{5.2}$$

Note that the aggregated energy profile computed through Problem (5.2) is the best possible profile since it accounts only the total energy E_T required to run all the appliances in the network of apartments, without considering user preferences and technical constraints on the energy assignment.

Remark 5.2.3. The optimal cost of Problem (5.2) is a lower bound on the optimal cost of the problem (3.18) with a shared ESS and by considering user preferences and technical constraints on the energy assignment.

Once all the apartment solve the corresponding Problem (5.1), they send the computed optimal energy profile to the aggregator, which calculates the difference between the aggregated energy profiles obtained at the apartment and desired profile at the aggregator level ($p_{G,0}^k$) as follows:

$$\Delta p_0^k = p_{G,0}^k - \left(\sum_{a=1}^{N} \sum_{i=1}^{N_a} \sum_{j=1}^{n_i} p_{ija,0}^k \right).$$

This difference is sent to the apartments as shift request signal Δp_0^k and the algorithm proceeds according the steps described in Algorithm 5.1.

Before describing the iterations of the proposed distributed algorithm, we formulate the problems to be solved at apartment and aggregator levels, to be done after initialization.

Problem at Apartment Level

The problem at apartment level a at iteration l is formulated as follows:

$$\begin{array}{ll} \min & \sum\limits_{k=1}^{T} C_\lambda^k \left(\sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p_{ija,l}^k + \beta \tilde{p}_{\mathrm{a},l}^k \right) \\ \text{s.t.} & \text{constraints } (3.1) - (3.9) \\ & \sum\limits_{j=1}^{n_i} p_{ij,l}^k = \sum\limits_{j=1}^{n_i} p_{ij,l-1}^k + \delta p_{\mathrm{a},l}^k \\ & |\frac{\Delta p_l^k}{N}| - \tilde{p}_{\mathrm{a},l}^k \leq |\delta p_{\mathrm{a},l}^k| \leq |\frac{\Delta p_l^k}{N}| \end{array} \tag{5.3}$$

where the decision variable $\delta p_{\mathrm{a},l}^k$ models the differences in the energy profile between two consecutive iterations. The variable $\delta p_{\mathrm{a},l}^k$ has the same sign of Δp_l^k, which is the energy shift request signal sent by the aggregator at iteration l. Notice that the unmet share of the energy shift $\tilde{p}_{\mathrm{a},l}^k$, which is requested by the aggregator at time slot k, is penalized in the objective function with a factor greater than energy prices by at least 2 order of magnitude. Unmet energy shift can be needed mainly to avoid constraint violation in Problem (5.3).

Problem at Aggregator Level

The problem at aggregator level at iteration l is formulated as follows:

$$\begin{array}{ll} \min & \sum_k C_\lambda^k p_{G,l}^k \\ \text{s.t.} & \text{constraints } (3.14) - (3.17) \\ & p_{T,l}^k + b_c^k - b_d^k = p_{G,l}^k \\ & p_{T,l}^k = \sum\limits_{a=1}^{N} \sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p_{ija,l}^k \\ & \underline{p}_G^k \leq p_{G,l}^k \leq \overline{p}_G^k. \end{array} \tag{5.4}$$

The shift request signal at iteration l is computed as follows:

$$\Delta p_l^k = p_{G,0}^k - \left(\sum_{a=1}^{N} \sum_{i=1}^{N_a} \sum_{j=1}^{n_i} p_{ija,l}^k \right)$$

Computation of Cost Benefits Due to ESS: The overall profit at the end of the scheduling horizon at each iteration l is: $G_{T,l} = G_{T,0} - \sum_k C_\lambda^k p_{G,l}^k$. The cost benefits are equally shared among the apartments, however a penalty is assigned to the unmet energy shift requested by the aggregator. The profit at apartment level a at iteration l is then computed as: $G_{\mathrm{a},l} = \max(\frac{G_{T,l}}{N} - \sum_k C_\lambda^k \tilde{p}_{\mathrm{a},l}^k, 0)$.

Steps of the Distributed Algorithm The steps of the proposed algorithm are detailed in 5.1.

Algorithm 5.1 Distributed algorithm

```
Initialization and computation of $\Delta p_0^k$, $\forall k$
for $l = 1, 2, \ldots, \mathrm{M}axIteration$ do
    each apartment solves Problem (5.3)
    each apartment sends to aggregator the computed power profiles
    aggregator solves Problem (5.4)
    aggregator computes $G_{T,l}$
    each apartment $a$ computes $G_{\mathrm{a},l}$
    if $G_{\mathrm{a},l} < G_{\mathrm{a},l-1}$, apartment $a$ accepts the energy profile, otherwise $p_{ija,l}^k = p_{ija,l-1}^k$, $\forall i, j, k$
    if all apartments accept, stop, otherwise compute $\Delta p_l^k$ and repeat
end for
```

Redistribution Strategy

An improvement in the solution obtained by Algorithm 5.1 at each iteration can be achieved by trying to redistribute the unmet energy shift request from the Aggregator among the apartments. Hence, the profiles of the total positive and negative unmet energy per time slot are computed respectively as $\tilde{p}_{+,l}^k = \sum\limits_{a=1}^{N} \tilde{p}_{+a,l}^k$ and $\tilde{p}_{-,l}^k = \sum\limits_{a=1}^{N} \tilde{p}_{-a,l}^k$. An additional step is to be included in Algorithm 5.1 between step 3 and 4. The redistribution is achieved by solving the following problem starting from the apartment level 1:

$$\begin{array}{ll} \min & \sum\limits_{k=1}^{T} C_\lambda^k \left(\sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p_{ija,l}^k - \gamma(\delta p_{+a,l}^k + \delta p_{-a,l}^k) \right) \\ \text{s.t.} & \text{constraints } (3.1) - (3.9) \\ & \sum\limits_{j=1}^{n_i} p_{ija,l}^k = \sum\limits_{j=1}^{n_i} \bar{p}_{ija,l}^k + \delta p_{+a,l}^k - \delta p_{-a,l}^k \\ & 0 \leq \delta p_{+a,l}^k \leq \tilde{p}_{+,l}^k \\ & 0 \leq \delta p_{-a,l}^k \leq \tilde{p}_{-,l}^k . \end{array} \tag{5.5}$$

where $\sum\limits_{j=1}^{n_i} \bar{p}_{ija,l}^k$ is the energy per time slot computed at iteration l at step 3. The total unmet energy per time slot is then updated by subtracting $\delta p_{+a,l}^k$ and $\delta p_{-a,l}^k$ from $\tilde{p}_{+,l}^k$ and $\tilde{p}_{-,l}^k$ respectively. Problem (5.5) is solved then for the next apartments until either there is still unmet energy shift or all the apartments have been asked for redistribution.

Properties of Distributed Algorithm

Algorithm 5.1 has the following desirable properties:

- **Feasibility of the solution**: at the initialization step, bounds on the optimal value of Problem (3.18) are computed. Clearly, the optimal schedules computed at the initialization step are not feasible solutions of the centralized problem. After the initialization, during each iteration of Algorithm 5.1, feasible solutions are obtained: this is guaranteed by the procedure defined by the algorithm. Effectively, during a generic iteration, the energy profiles sent by the apartments and included in (5.4) as given aggregated load satisfying all the appliances constraints and user preferences, as defined by Problem (5.3); on the other hand, the ESS schedule computed by solving (5.4) fulfills all the technical and operational constraints concerning the ESS and the interaction with the distribution grid. Every time the energy profiles at apartment level are computed based on energy shift requests from the aggregator, an updated ESS schedule is computed based on the resulting aggregated energy profile. By doing so, the solution computed at each iteration satisfies all the constraints formulated in the centralized problem (3.18);

- **Suboptimality of the solution**: as mentioned above, at the initialization step a lower and an upper bound on the optimal value of Problem (3.18) are computed. Subsequently, at each iteration of Algorithm 5.1, the solution steps towards the optimal solution of the centralized problem. This is ensured by two aspects of the procedure: *i)* an apartment accepts an update on it energy use profile only if its local objective function, which includes also ESS-related benefits, decreases; *ii)* the ESS schedule has to account for the energy profiles computed at the apartment level, which certainly leads to a value of the objective function at the aggregator level greater than the one computed at the initialization step. However, the algorithm provides a suboptimal solution since there are no guarantees that the optimal solution is reached when the algorithm terminates;

- **Fair allocation of profits**: the ESS-related profits at the end of the scheduling horizon are equally divided among the apartments, so are the energy shift requests. Further, an incentive mechanism is considered: users are penalized for the unmet energy shift request and rewarded for taking on a share of the total unmet energy shift requested by the aggregator. We will include a mathematical proof of this third property in an extended version of this study.

Remark 5.2.4. Infeasibility can occur at aggregator level during a generic iteration. This can be prevented by modifying Problem (5.4) and replacing the constraint on $p^k_{T,l}$ with the following constraint:

$$p^k_{\mathrm{a},l} - \Delta p^k_l \leq p^k_{T,l} \leq p^k_{\mathrm{a},l} + \Delta p^k_l,$$

where $p^k_{\mathrm{a},l} = \sum\limits_{a=1}^{N} \sum\limits_{i=1}^{N_a} \sum\limits_{j=1}^{n_i} p^k_{ija,l}$ and Δp^k_l is opportunely weighted in the objective function.

5.3 Motivational Example and Preliminary Results

The centralized scheduling problem for a network of apartments, which are sharing an ESS, is formulated in the (3.18). From (3.18), one may notice that p^k_G is simply the power consumption of the apartments plus power exchange (charging/discharging) whit the ESS. The point is that, the p^k_G is often tightly limited within upper and lower limits, to protect the network from overload. In this problem, aggregators goal is to minimize the electricity consumption cost for whole the system, and in the most optimistic case the smart appliances in the apartments will be scheduled (while satisfying their constraints) when the price of electricity is minimum. Also, ESS will charge when the price is low and discharge when the price is high, to make the most possible profit out of the grid. This optimistic case will result in the optimal solution for the problem as far as the p^k_G is within the power limitation bound for all the times during the day, and in this case we can say that scheduling of appliances in the apartments is decoupled from the ESS scheduling. This is not always the case, and by scheduling of the smart appliances and charging of the ESS to be happened at the same time (when the price of electricity is low), the p^k_G violates the power limitations at some points during the day. In this case, the overload should be shifted to the other times by the aggregator, in which either users should change their desired scheduling or the ESS scheduling should change. In this sense, smart appliances and ESS scheduling are coupled with each other and the optimization algorithm in the aggregator level should find an optimal solution, by joint scheduling of smart appliances and ESS.

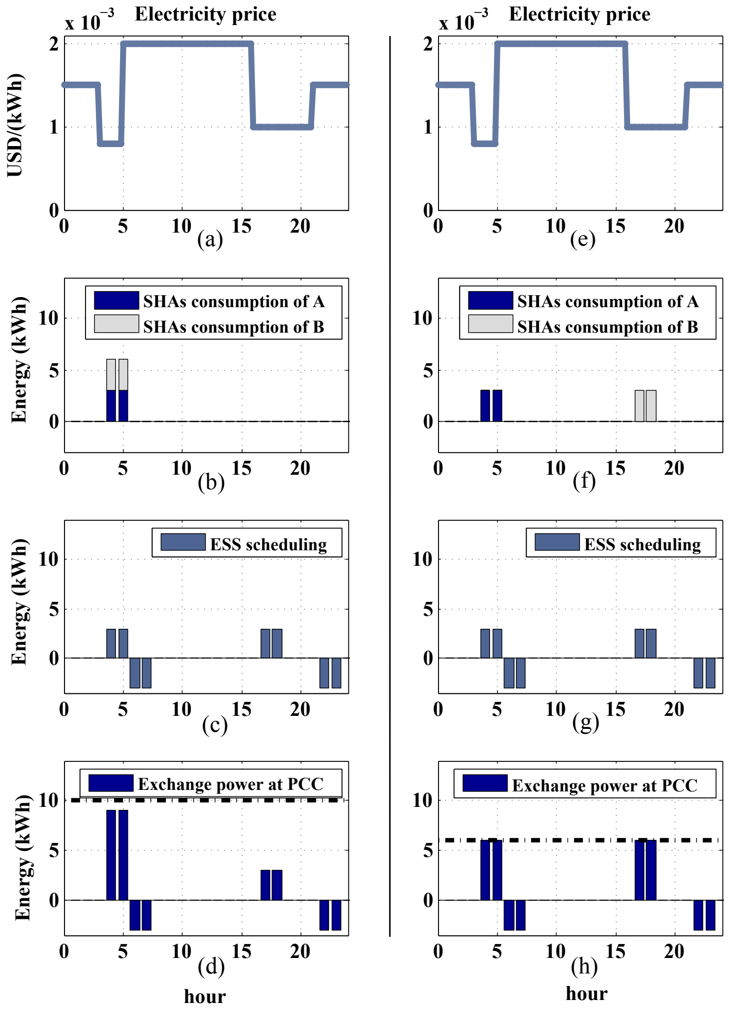

Figure 5.2: Scheduling of appliances (in the apartments A and B) and the shared ESS in two different cases, i) the boundaries on power exchange with the grid at PCC are not limiting (in the left side), and ii) the power exchange at PCC is more limited (in the right side).

Motivational Example In this example, apartments A and B (number of apatments in Figure 5.1 is two) share an ESS, and whole the system is connected to the grid at PCC. The scheduling of the shared storage, and also appliances in these apartments are shown in Figure 5.2, for two different cases,i) the boundaries on power exchange with the grid at PCC are not limiting (in the left side of the figure), and ii) the power exchange at PCC is limited in a narrow bound (in the right side).

As it is shown in the left side of this figure, by having an upper limitation on the p_G^k to be high enough (in this case 10kW), the scheduling of smart appliances in the both apartments A and B and also ESS charging will be scheduled when the electricity price has the lowest value (between 3:00 and 5:00 am). Therefore, in this case the ESS charging and the smart appliances can be scheduled in a decoupled fashion, and the maximum total power exchange (9kW between 3:00 and 5:00 am) will not violate the power limitation. smart appliances and ESS scheduling, and the total power consumption are illustrated in the parts (b), (c), and (d),respectively.

On the other hand, in the case that the power exchange limitation (6kW) is lower enough, aggregator cannot keep the same scheduling for smart appliance and ESS, otherwise a deviation from power limitation will happen at PCC (between 3:00 and 5:00 am). In this case, aggregator should manage for overload shifting from 3:00-5:00 am to another times of the day, either through negotiation with the apartments to shift their smart appliances and incentivise them with monetary profit, or by re-scheduling the ESS charging/discharging. In the first solution scenario, shifting the smart appliances consumption from the lowest price time period (3:00-5:00 am) to the other low price period (16:00-21:00), will cause a small increase in electricity bill. This is because of the small difference between the electricity price in these two period. In the second solution scenario, if the ESS-charging happens to shift from 3:00-5:00 am time duration, it will not be able to discharge in 5:00-7:00 am, and will cause a big effect on profit making. Thats because of the difference between the electricity price in these two period, which is noticeable. Thus, the first solution scenario for this coupled case is more money affordable, and parts (f) and (g) of the figure show the proper scheduling of the smart appliances and ESS. This scenario causes no violation from the power limitation (see parts (h)). Therefore, it is necessary for aggregator to apply an optimal operation strategy, through coordinating with apartments, to schedule the smart appliances and the ESS, and deal with the coupling cases. In addition, by applying a centralized approach, the calculation time would not be reasonable when the number of apartments increases. Therefore, essence of having a distributed scheduling approach is obvious.

Preliminary RSesults In order to evaluate the proposed distributed framework, we present preliminary results obtained by applying the Algorithm 5.1 to coordinate four active apartments, each of them equipped with 3 smart appliances: a dishwasher, a washing machine and a dryer. In the simulations, the technical specifications of the smart appliances (dishwasher, washing machine, and dryer) are the same as the ones in Section 3.3. We consider a piecewise constant electricity tariff signal extracted from Nordpool website. The shared ESS has the following technical features:

- Storage capacity: 20000Wh
- Maximum power exchange: 8000W

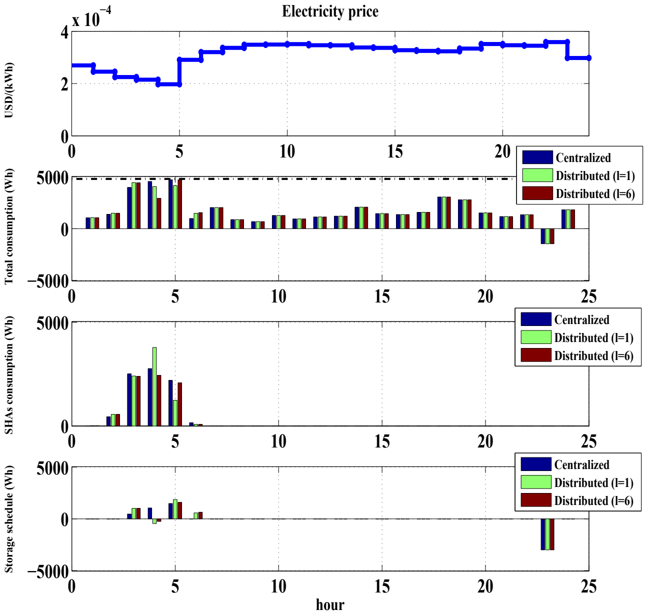

Figure 5.3: Comparison between the optimal solution of the centralized problem (3.18) and the solution computed by Algorithm 5.1 at iterations 1 and 6 (the last iteration).

- Maximum depth of discharge: 30%
- Stored energy degradation (α): negligible
- Charging and discharging efficiency: 90%
- Maximum charging and discharging cycles: 5 (per day).

We then do a comparison between the centralized scheduling of smart appliances and ESS by solving Problem (3.18) with the distributed scheduling by applying Algorithm 5.1. Figure 5.3 depicts the comparison between the solution computed by solving the centralized problem and the solutions obtained by the proposed distributed algorithm at iteration 1 and 6, which is the last iteration in this particular case study. We can notice that, as Algorithm 5.1 (the distributed approach) is iterated, the solutions get closer to the optimal one (the solution resulting from solving the centralized problem). The total electricity cost of the optimal solution is 1.200 USD while the electricity cost resulting from the final iteration of Algorithm 5.1 is 1.215 USD, hence only 1.3% higher. On the other hand, the computational time of the centralized problem (3.18) was 745 sec while the proposed distributed algorithm computes the solution in 7.29 sec, hence the computational time has decreased by two orders of magnitude.

Note that in the simulation results here, the optimal electricity bill has been discussed and the weighting parameter $\lambda = 0$ has been considered. In addition, simulations are all done on a 64bit Windows system with an Intel Core i7-3770, 3.40GHz and 16.0 GB of RAM, in Matlab R2014b.

Chapter 6

Conclusion and Future Work

This chapter concludes Part I of this thesis in which a novel robust optimal scheduling formulation is proposed for scheduling of smart appliances and ESS in residential areas.

In Chapter 3 a multi-objective Mixed Integer Linear Programming (MILP), which aims to decrease the CO_2 emissions and the electricity bill is studied.

A robust formulation for the optimal scheduling, which consider the user behavior uncertainty, is proposed in Chapter 4. In this formulation the optimal appliances schedule is less sensitive to unpredictable changes in user preferences. The user behavior uncertainty is modeled as uncertainty in the cost function coefficients. We point out that the proposed scheduling framework is applicable to scenarios with various uncertainty sources, storage technologies, generic programmable electrical loads, as well as different optimization criteria. Due to the high cost of ESSs and computational burden for scheduling of large number of appliances, it could be convenient to consumers to deploy and share ESSs in a cooperative manner. Thus, in Chapter 5 we propose an iterative distributed approach to solve the problem of coordinating the set of smart appliances located in a network of apartments sharing an ESS, such that each household can profit from the use of the ESS while technical and operational constraints, as well as user preferences, are satisfied. The problem of coordinating the shared resources among the consumers is complicated by a fairness requirement, i.e., storage will equally benefit consumers according to their flexible loads. The novel distributed scheduling algorithm has the following properties *i)* provides a feasible solution to the centralized scheduling problem; *ii)* allocates fairly ESS-related profits among the users; *iii)* requires limited messages to be exchanged between each consumer and the aggregator, and no message passing among the consumers, to keep consumers' privacy, and (iii) is suitable for online optimization-based control scheme, such as MPC. Several numerical studies based on real energy consumption data from active apartments have been done in Part I. In some of these numerical studies, we investigate the impact of DR policies on electricity price and CO_2 savings in the presence of user behavior uncertainties. Some other numerical studies are performed to illustrate the effectiveness of the distributed algorithm. It has been shown in these studies that the computed solution by the distributed algorithm is close to the optimal one computed by a centralized problem.

Many interesting open questions remain in the area of demand response that can be considered for future works. As an example, it was discussed in Chapter 3 that only 8% of the power consumption of the active apartments is devoted to the smart appliances, while almost 50% of it is related to the lightning, heating and cold appliances. Thus, by taking these consumptions into account in automated systems, the bill and CO_2 savings could be significantly increased. Note that this study is based on a day-ahead electricity tariff, while one can investigate the problem considering real-time electricity tariff. Moreover, there are other uncertainties that could be taken into account in Chapter 4, such as real-time tariff uncertainty because of huge load shifting by using automation system in a large number of apartments. This uncertainty could be taken into account, and interpreted as the level of uncertainties (ϵ^k). In addition, in that chapter, degree of conservatism Γ has been introduced, but no systematic approach has been proposed to tune this parameter. One could find a tuning method for it, based on the user behavior historical data. In Chapter 5, some of the proposed distributed algorithm's properties such as feasibility and sub-optimality of the solution, and fair allocation of profit have been investigated. It would be interesting to study the other properties such as convergence rate of the proposed iterative distributed algorithm.

Part II

Resilient Control for Energy Management Systems

Chapter 1

Introduction

To monitor and control physical/chemical processes, industrial control systems (ICSs) play an important role in daily life. ICS is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. ICSs are commonly seen in many critical infrastructures such as electricity generation, transmission and distribution, water treatment, manufacturing, etc [93]. In electricity distribution grid, automatic control of electrical/thermal components in buildings has become a necessary task for ICSs in order to achieve optimal performance. An ICS is called an energy management system (EMS) when it comes to the automatic control of electrical/thermal components in buildings. The aim of a modern EMS is to enhance the functionality of interactive control strategies leading towards energy efficiency and a more user friendly environment. By connection of the EMS to the building communication network, the possibility of EMS cyber-attack increases. The StuxNet cyber-attack supposedly targeting a nuclear-enrichment plant (by corrupting the measurements and actuator signals) in Iran, see [20], and BlackEnergy malware targeting several electricity distribution companies in Ukraine, see [4], are concrete examples of cyber-attacks. In addiion, as discussed in [83], attacks on the measurement signals may lead to a poor system performance, or may even cause instability. Thus, it is crucial to make the control of EMS to be resilient against cyber crime.

1.1 Main Contributions

The main contributions of Part II are twofold. As the first contribution, we identify potential vulnerabilities in the interface between the physical and the IT infrastructures of distribution power system. These vulnerabilities may lead to an abnormal operation of the distribution network. In particular, relevant attack scenarios are introduced, together with their threat models, based on which impact analysis are performed. The attack scenarios consider cyber adversaries that may corrupt a few measurements and reference signals, which may degrade the system's reliability and even destabilize the voltage magnitudes. For example, we show that a cyber adversary, without having substantial model knowledge, may destabilize the power system by merely redirecting measurements communicated through the communication network. This contribution has been published in [83].

As the second contribution, a practical cyber-secure framework for networked control systems is proposed. This framework, includes security information analytics to detect attacks, and a resilient policy to improve the performance of the system running under the attack. Stability and optimal performance of the networked control system, under attack and by applying the proposed framework, is proved here. The framework has been applied to an energy management system and its efficiency is demonstrated on a real critical attack scenario. This contribution is studied in [56] and [55].

1.2 Outline

The rest of Part II of this thesis is structured as follows. Chapter 2 presents some related background. Potential vulnerabilities in the interface between the physical and the IT infrastructures of the power system has been identified, and the impact of adversarial actions has been assessed in Chapter 3. In Chapter 4, a practical cyber-secure framework for networked control systems is proposed. This framework, includes security information analytics to detect attacks, and resilient policy to improve the performance of the system running under the attack. Finally, Chapter 5 provides conclusions and suggestions for future studies.

Chapter 2

Background

2.1 Voltage Stability in Distribution Grid

Motivated by environmental, economic and technological aspects, interests in renewable energy sources is growing worldwide. Most of these sources are small-scale inverter-based distributed generation (DG) units connected at the low voltage and medium voltage levels. Thus, the power generation infrastructure is moving from purely large centralized plants at the high voltage levels to a mixed generation pool consisting of conventional large plants and smaller distributed generation units at lower voltage levels. In this new paradigm, it is more challenging to operate the electric power networks in a reliable and resilient mode. These challenges may be tackled by facilitating a local integration of renewable energy sources, which las led to the concept of microgrids (MGs) [27, 71]. An MG is a low-voltage electrical network, composed of several DGs, energy storage elements, and controllable loads, and their integration with the main grid is accomplished by using suitable power electronic devices (inverters). In addition, an MG is able to operate in the grid-connected mode (connected to the wide-area electric power system), and also in the islanded mode (disconnected from the main grid). The problem of voltage stability and power sharing analysis of MGs has been carried out in several studies in the literature. For radial lossless microgrids, and under the assumption of constant voltage amplitudes, analytic conditions for proportional power sharing and synchronization of have been derived in [73]. Conditions for voltage stability for lossless parallel MGs with one common load have been derived in [74]. In addition, [70] gives conditions on the droop gains to ensure stability of droop-controlled inverter-based lossless MGs with general meshed topology.

2.2 Smart Grids' Vulnerabilities

Electrical power networks in the new energy generation paradigm are very complex and face numerous challenges. To facilitate their safe and reliable operation, they need to be tightly coupled with the supervisory control and data acquisition

(SCADA) systems that monitor and operate the power infrastructure by collecting data from remote facilities and meters, and sending back supervisory control commands. On the other hand, the power networks coupled with the SCADA systems face new challenges, as these systems may become susceptible to malicious cyber threats through the communication infrastructure. The safe and stable operation of power networks must be ensured, not only in the normal situations, but also in the cases when the cyber security of SCADA systems is threatened by malicious attacks [5]. Black-Energy malware targeting several electricity distribution companies in Ukraine [4], is one of the recent concrete examples of cyber-attacks. Thus, it is important to analyze potential vulnerabilities of the system, by modeling and studying different threats to the controlled system, and devise resilient schemes to mitigate high-risk threats. Recently, there has been a substantial work on cyber security of power transmission networks, addressing, for instance, certain classes of undetectable false data injection attacks [42, 67, 31, 78]. In addition, the impact of these attacks on the system operation [89, 84] and possible protective and countermeasures [39, 88] have been investigated. In comparison with transmission level, as mentioned in [34], security issues at the distribution system level have not been as extensively studied. The impact of cyber attacks on centralized voltage regulation in distribution systems was considered in [34]. The vulnerabilities that may be introduced by the integrated Volt-VAR control scheme, when an adversary is able to inject false data measurements into the system, is studied in [82]. To the best of our knowledge, none of the previous works have studied cyber attacks on the inverter-based microgrids.

2.3 Attack Resilient Control Policies

Recently, there has been an increase in control systems security research. To this end, security information analytics (SIA) enables quick detection of cyber-attacks by checking the system behaviour. As discussed in [15], SIA requires the ability to handle processing of huge amounts of data, by using new analytics and visualization techniques for attack detection. Once the attack is detected, control policies which are resilient against the attacks, should be triggered. Design of control and estimation algorithms which are resilient against faults is not a new problem, but those algorithms may not be efficient against malicious cyber-attacks. For example, *virtual sensor* (VS) and *virtual actuator* concepts, have been introduced in [46] to deal with sensor and actuator failures, respectively. Attacks may be more complex than faults, and may use some information of the system to corrupt the measurements in an intelligent way, and result in worse consequences than faults. Thus, there has been a recent increase in control systems security research and design of resilient control and estimation algorithms against attacks [69, 26, 81, 21, 54, 11, 61]. In [69], the authors consider the problem of control and estimation in a networked system when the communication links are subject to disturbances (corresponding to packet losses), resulting from a denial of service attack for instance. In [26], a more intelligent jammer is considered who plans his attacks in order to maximize a certain cost, while the objective of the controller is to minimize this same cost. The results are however derived in the case of one-dimensional systems, which is the main limitation of the work. The problem of reaching consensus in the presence of malicious agents is studied in [81]. The authors characterize the number of infected nodes that can be tolerated and propose a way to overcome the effect of the malicious agents when possible. One particularity of that work is that the dynamics is part of the algorithm and can be specifically designed, rather than being given as in a physical system. The estimation and control of linear systems, when some of the sensors or actuators are corrupted by an attacker, is studied in [21]. They propose an efficient algorithm inspired from techniques in compressed sensing to estimate the state of the plant despite attacks. The authors assume that the attacked nodes does not change over time. In addition, a general framework to model and analyse impact of attacks, is proposed in [85]. In [54], a method for state estimation in presence of attacks, for systems with noise and modeling errors is proposed. It is shown that the attacker cannot destabilize the system by exploiting the difference between the model used for state estimation and the real physical dynamics of the system. In [11], a control technique is proposed which is resilient against certain sensor attacks. In that technique, a recursive filtering algorithm, to estimate the states of the system, is implemented that takes advantage of redundancy in the information received by the controller.

Chapter 3

Impact Assessment in Distribution Grid

In this chapter, after recalling some properties of certain classes of linear time-invariant (LTI) systems, we first tackle the problem of voltage stability and reactive power balancing in the droop-controlled MGs, and provide criteria for designing the controller gains in terms of the power system parameters. We then identify potential vulnerabilities in the interface between the physical and the IT infrastructures of the power system, and assess the impact of adversarial actions.

3.1 Preliminaries

In this section, we recall important properties of certain classes of linear time-invariant (LTI) systems that will be useful in the subsequent sections. Let us consider a general LTI system of the form:

$$\begin{cases} \dot{x}(t) = Ax(t) + Fu(t) \\ y(t) = Cx(t) + Du(t), \end{cases} \tag{3.1}$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^p$ are the system state, the control input, and the controlled output at time t, respectively. Denoting $a_{ij} = [A]_{i,j}$ as the entry of A in the i-th row and j-th column, the class of diagonally dominant matrices is defined as follows.

Definition 3.1.1 (Diagonally dominant matrices)**.** *The matrix A is said to be row-diagonally dominant if its entries satisfy the conditions*

$$|a_{ii}| \geq \sum_{j \neq i} |a_{ij}|, \ \forall i \in \{1, \dots, n\}. \tag{3.2}$$

Given the above definition, the system (3.1) is said to be row-diagonally dominant if the state matrix A is row-diagonally dominant.

Another relevant class of systems is that of positive systems (see [64], for instance), which play an important role here.

Definition 3.1.2 (Positive systems)**.** *The LTI system* (3.1) *is said to be positive if the following conditions hold:*

1. *The matrix A is Metzler, i.e., it has non-negative off-diagonal entries;*

2. *The matrices F, C and D are non-negative, i.e., they only have non-negative entries.*

Positive systems have several interesting properties, e.g., $x(0) \geq 0$ and $u(t) \geq 0$ result in trajectories satisfying $x(t) \geq 0$ for all t, where $x \geq 0$ for a vector x denotes the element-wise inequality. In particular, the following properties of positive systems are instrumental in our analysis.

Proposition 3.1.1 ([64])**.** *If the system* (3.1) *is positive, the following statements hold:*

1. *The matrix A is Hurwitz (every eigenvalue of A has strictly negative real part) if, and only if, there exists a $\xi \in \mathbb{R}^n$ such that $\xi > 0$ and $A\xi < 0$.*

2. *Let $m = p = 1$, define $H(s) = C(sI - A)^{-1}F + D$ as the transfer function of the system* (3.1)*, and suppose A is Hurwitz. The $\mathcal{L}_\infty$-induced norm of* (3.1) *is given by*

$$\| H \|_{\infty-ind} = \sup_{\|u\|_{\mathcal{L}_\infty} \neq 0} \frac{\| y \|_{\mathcal{L}_\infty}}{\| u \|_{\mathcal{L}_\infty}} = H(0). \tag{3.3}$$

3.2 Problem Formulation

As shown in Figure 3.1, the power distribution system is considered to be a set of interconnected MGs that may be connected to the main grid through the feeder substation (bus 0), where each MG is represented by a bus to which inverter-based DER resources and loads are connected. Although Figure 3.1 depicts a line network, we consider generic connected topologies where the network is characterized by the undirected graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the vertex set, $\mathcal{E}$ is the edge set, and $\mathcal{N}_i = \{j \in \mathcal{V} : (i, j) \in \mathcal{E}\}$ denotes the neighbor set of the i-th bus. In this system, the states are defined as V_i and θ_i, which are voltage magnitude and voltage angle of the i-th bus, respectively, and $i \in \mathcal{V}$.

Assumption 3.2.1. *In the power distribution network under study, the following assumptions are made:*

1. *The three-phase power network is balanced (so that it can be represented as an equivalent single-phase system);*

2. *All N buses are assumed to be inverter buses [71], each represented by V_i and θ_i for $i = 1, \ldots, N$.*

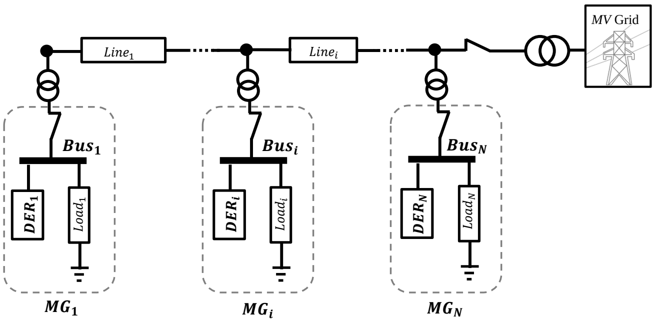

Figure 3.1: A power distribution system comprised of interconnected microgrids with inverter-based DERs.

Under the Assumption 3.2.1, the active and reactive power injections at bus i is given respectively by

$$\begin{aligned} P_i &= V_i^2 G_i - \sum_{j \in \mathcal{N}_i} V_i V_j (G_{ij} \cos(\theta_{ij}) + B_{ij} \sin(\theta_{ij})), \\ Q_i &= -V_i^2 B_i - \sum_{j \in \mathcal{N}_i} V_i V_j (G_{ij} \sin(\theta_{ij}) - B_{ij} \cos(\theta_{ij})), \end{aligned} \tag{3.4}$$

in which, $G_{ij} = R_{ij}/(R_{ij}^2 + X_{ij}^2) \geq 0$ and $B_{ij} = -X_{ij}/(R_{ij}^2 + X_{ij}^2) \leq 0$ are respectively the conductance and susceptance of the transmission line between the i-th and j-th buses, and R_{ij} and X_{ij} are resistance and reactance of the same line between the same buses, respectively. In addition, self-conductance and self-susceptance are defined as $G_i = G_{ii} + \sum_{j \in \mathcal{N}_i} G_{ij}$ and $B_i = B_{ii} + \sum_{j \in \mathcal{N}_i} B_{ij}$, respectively. Note that the angle difference between node i and j, $\theta_i - \theta_j$, is simply written as θ_{ij} in the rest of this chapter.

Assumption 3.2.2. *In the power distribution system under study, all transmission line impedances are assumed to have the uniform ratio $\rho = R_{ij}/X_{ij} = -G_{ij}/B_{ij}$ for all $(i, j) \in \mathcal{E}$.*

Controller Structure

Using the capabilities of the local inverter-based DERs, each MG is controlled by a droop controller, which remotely receives the reference signal (V_i^* as the reference voltage for the i-th bus) and measurements (V_j and θ_j, as the voltage magnitude and voltage angle of the j-th bus, respectively) through the communication network, using a suitable communication protocol such as the IEC 61850. The controller and related signals are shown in Figure 3.2. Since we are interested in the voltage dynamics of the power system, the phase-angle dynamics are neglected and we assume that all phase-angles are constant. In terms of the voltage dynamics, each

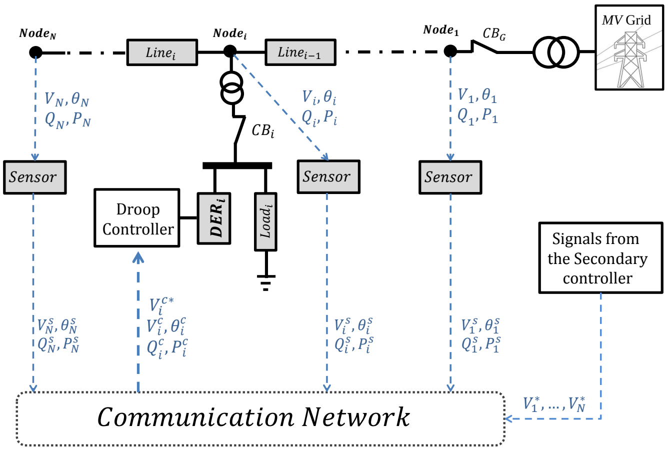

Figure 3.2: The inverter-based DERs of a MG are controlled by a droop controller. The physical quantities are measured by sensors at each node, which then transmit their measurements (denoted by the superscript s) to the droop controllers. The control signal is computed based on the measurements and reference signals received by the controller (denoted with the superscript c).

MG i is modeled as the single integrator

$$\tau_i \dot{V}_i(t) = u_{V_i}(t), \tag{3.5}$$

where $\tau_i > 0$ is the inverter's time constant and $u_{V_i}(t)$ is the control signal computed by the droop controller at time $t \geq 0$. In particular, we consider the voltage quadratic droop controller [73, see equation (7)] described by

$$u_{V_i}(t) = -K_i V_i^c(t) \left(V_i^c(t) - V_i^{c\star}(t) \right) - Q_i^c(t), \tag{3.6}$$

where $K_i > 0$ is the droop control gain and $V_i^c(t)$, $Q_i^c(t)$, and $V_i^{c\star}(t)$ are the voltage measurement, reactive injection measurement, and voltage reference signal with respect to bus i, respectively, that are received by the droop controller, as illustrated in Figure 3.2.

Under nominal operation, we have that these signals match the corresponding physical variables and reference signals, i.e., $V_i^c(t) = V_i(t)$, $Q_i^c(t) = Q_i(t)$, and $V_i^{c\star}(t) = V_i^\star(t)$ ($V_i^\star(t)$ is sent by a higher level controller which is called Secondary controller). Hence, the closed-loop dynamics of inverter node i under nominal operation are given by the differential equations

$$\begin{aligned} \tau_i \dot{V}_i &= -K_i V_i \left(V_i - V_i^\star \right) - Q_i \\ &= -V_i \left(K_i V_i - K_i V_i^\star + \sum_{j \in \mathcal{V}} l_{ij}(\theta) V_j \right), \ \forall i = 1, \ldots, N, \end{aligned} \tag{3.7}$$

where the time argument has been omitted. In addition, under the Assumption 3.2.2, the parameter l_{ij} is written as

$$l_{ij} = \begin{cases} B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ -B_i, & i = j. \end{cases} \tag{3.8}$$

Denoting $V = [V_1 \, \dots \, V_N]^\top$ and $[V]$ as the diagonal matrix with $[V]_{ii} = V_i$, the voltage dynamics under the quadratic droop control can be written in vector form as

$$[\tau]\dot{V} = [V] \left([K]V^\star - ([K] + L(\theta)) \, V \right), \tag{3.9}$$

where the matrix $L(\theta)$ is defined as $[L(\theta)]_{ij} = l_{ij}(\theta)$ and $[K]$ as the diagonal matrix with $[K]_{ii} = K_i$.

Linearization of the Voltage Dynamics

In the following sections, we consider that the power system (3.9) is linearized around an equilibrium point $(\bar{V}, \bar{V}^{c\star})$ such that $-([K] + L(\theta)) \, \bar{V} + [K]\bar{V}^\star = 0$. Additionally, the following assumptions is considered throughout the remainder of this chapter.

Assumption 3.2.3. *The phase-angle differences between any neighboring nodes, θ_{ij} for $(i, j) \in \mathcal{E}$, is assumed to be constant.*

By Assumption 3.2.3, and denoting $x(t) = V(t) - \bar{V}$ and $u(t) = V^{c\star}(t) - \bar{V}^{c\star}$ as the voltage and reference deviations, respectively, the corresponding linearized system is given by

$$\dot{x}(t) = Ax(t) + Fu(t), \tag{3.10}$$

where $A = -[\bar{V}][\tau]^{-1} ([K] + L(\theta))$ and $F = [\bar{V}][\tau]^{-1}[K]$. For simplicity, in the following we suppose that $\bar{V} = \mathbf{1}$pu, where $\mathbf{1}$ denotes a vector with all entries equal to 1.

3.3 Stability Analysis

In this section, we provide necessary and sufficient conditions on the power system parameters so that the linearized dynamics are positive and row-diagonally dominant. These properties are then used to establish the asymptotic stability of the linearized system. Moreover, they play an important role when studying the power system under the different attack scenarios in subsequent sections.

System Properties

First we derive necessary and sufficient conditions for the linearized system (3.10) to be positive, which requires the following definition.

Definition 3.3.1. *The maximum phase difference between any two neighboring nodes is defined as*

$$\Delta_\theta = \max_{(i,j)\in\mathcal{E}} |\theta_{ij}|. \tag{3.11}$$

In addition, as in any conventional power system, here we assume that $\Delta_\theta < \pi/2$ [70].

Theorem 3.3.1. *Consider the power distribution network under study, having active and reactive power injections* (3.4) *at bus i with $\Delta_\theta < \pi/2$, and applying the quadratic droop controller* (3.7) *for each MG. Then the necessary and sufficient condition to make the linearized system* (3.10) *positive is*

$$\rho \leq |\cot(\Delta_\theta)|. \tag{3.12}$$

Proof. Recall the linearized system (3.10) with $A = -[\tilde{\tau}]^{-1}([K] + L(\theta))$ and $F = [\tilde{\tau}]^{-1}[K]$. From (3.8), a_{ij} read as

$$a_{ij} = \begin{cases} -\tau_i^{-1} B_{ij}(\rho\sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ \tau_i^{-1}(-K_i + B_{ii} + \sum_{j\in\mathcal{N}_i} B_{ij}), & i = j. \end{cases} \tag{3.13}$$

Based on Definition 3.1.2, the system is positive if and only if $[F]_{i,j} \geq 0$ and $a_{ij} \geq 0$ for all i and j. Since the controller parameters τ_i and K_i are positive, we conclude that $[F]_{i,j} \geq 0$ holds. Moreover, as the susceptance B_{ij} is always negative, the inequalities $a_{ij} \geq 0$ for all i and j can be rewritten as

$$\begin{cases} \rho\sin(\theta_{ij}) + \cos(\theta_{ij}) \geq 0 \\ \rho\sin(\theta_{ji}) + \cos(\theta_{ji}) \geq 0, \end{cases} \tag{3.14}$$

for all the neighboring i and j. From these inequalities, and assuming that $\Delta_\theta < \pi/2$, we have $\rho \leq |\cot(\Delta_\theta)|$. □

Next we characterize necessary and sufficient conditions for a linearized positive system to be row-diagonally dominant.

Lemma 3.3.2. *Suppose the linearized system* (3.10) *is positive. The system* (3.10) *is row-diagonally dominant if, and only if, the following inequality holds*

$$K_i + |B_{ii}| \geq (\sqrt{\rho^2+1} - 1) \sum_{j\in\mathcal{N}_i} |B_{ij}|. \tag{3.15}$$

Proof. Given the entries of A in (3.13) and Definition 3.1.1, the system (3.10) is row-diagonally dominant if, and only if,

$$|-K_i + B_{ii} + \sum_{j\in\mathcal{N}_i} B_{ij}| \geq \sum_{j\in\mathcal{N}_i} |-B_{ij}(\rho\sin(\theta_{ij}) + \cos(\theta_{ij}))|. \tag{3.16}$$

The proof follows by considering the worst-case phase-angle differences θ_{ij} that maximize the right-hand side term, i.e.,

$$\theta_{ij} = \underset{\theta\in[-\Delta_\theta,\, \Delta_\theta]}{\arg\max} \left(\rho \sin(\theta) + \cos(\theta)\right), \tag{3.17}$$

for all $(i,j) \in \mathcal{E}$. Since the system is positive from the inequalities in (3.14), we know that

$$\frac{\partial^2}{\partial\theta^2}\left(\rho\sin(\theta) + \cos(\theta)\right) \leq 0$$

holds for all the neighboring i and j. Hence, the solution to (3.17) can be obtained by solving the following equations

$$\begin{cases} 0 = \dfrac{\partial}{\partial\theta}\left(\rho\sin(\theta) + \cos(\theta)\right) \\ 1 = \sin(\theta)^2 + \cos(\theta)^2 \end{cases} \tag{3.18}$$

and verifying that its solution belongs to the feasible set $\theta \in [-\Delta_\theta,\, \Delta_\theta]$. In fact, the system of equations (3.18) is solved for $\theta^\star$ such that $\cos(\theta^\star) = 1/\sqrt{1+\rho^2}$. Note that $\theta^\star$ yields $\rho\sin(\theta^\star) + \cos(\theta^\star) = \sqrt{1+\rho^2} > 0$, which indicates that $\theta^\star$ satisfies the positivity constraints (3.14). Hence, since the linearized system is positive, we conclude that $\theta^\star$ belongs to the set $[-\Delta_\theta,\, \Delta_\theta]$, thus solving (3.17).

Considering the optimal value of (3.17), $\rho\sin(\theta^\star) + \cos(\theta^\star) = \sqrt{1+\rho^2}$, and noticing that the controller parameters K_i are positive and all the susceptance B_{ij} are negative, the proof concludes by rewriting the inequalities (3.16) as

$$K_i + |B_{ii}| + \sum_{j\in\mathcal{N}_i} |B_{ij}| \geq \sum_{j\in\mathcal{N}_i} \sqrt{\rho^2+1}|B_{ij}|. \tag{3.19}$$

□

These properties play important roles in the characterization of the attack impacts, and they are also used in analyzing the stability of the linearized system.

Stability of the Power System

Next we establish the stability of the linearized system, using the positivity and row-diagonally dominance properties of the linearized system. Specifically, when the system is positive, the next result states the necessary and sufficient conditions for stability and then shows that row-diagonally dominance ensures stability.

Theorem 3.3.3. *Consider the linearized dynamics of the power system* (3.10) *and suppose the necessary and sufficient condition* (3.12) *from Theorem 3.3.1 is satisfied. Then the linearized system is positive and the following statements hold:*

1. *the system is asymptotically stable if and only if there exist positive scalars* $\xi_i > 0$ *such that the following inequality holds for all* $i = 1, \ldots, n$*:*

$$\xi_i|-K_i + B_i| > \sum_{j\in\mathcal{N}_i} \xi_j|-B_{ij}(\rho\sin(\theta_{ij}) + \cos(\theta_{ij}))|;$$

2. *the system is asymptotically stable if it is row-diagonally dominant, i.e., the following inequality holds for all* $i = 1, \ldots, n$*:*

$$|-K_i + B_i| > \sum_{j\in\mathcal{N}_i} |-B_{ij}(\rho\sin(\theta_{ij}) + \cos(\theta_{ij}))|.$$

Proof. Recalling that the entries of A are given by (3.13), the necessary and sufficient condition for stability follows directly from the positivity of the system and Proposition 3.1.1, i.e., the existence of a positive vector $\xi > 0$ such that $A\xi < 0$.

On the other hand, the sufficient condition for stability is obtained by considering $\xi_i = 1$ for all i and verifying that $A\mathbf{1} < 0$ can be rewritten as (3.16), given that τ_i and $\rho\sin(\theta_{ij}) + \cos(\theta_{ij})$ are positive and B_{ij} is negative. □

Remark 3.3.1. Note that we may not have control on self-susceptance (B_{ii}) and it belongs to the interval $[0, \bar{B}_{ii}]$, so to be more conservative, the sufficient condition in Proposition 3.3.3 can be written as:

$$K_i \geq \sum_{j\in\mathcal{N}_i} (\sqrt{\rho^2+1} - 1)|B_{ij}|. \tag{3.20}$$

Remark 3.3.2. It could be interesting to characterize conditions on (3.10) under which V satisfies $|V - \mathbf{1}| < \delta$. This problem is related to the validity of (3.10), which assumes that V is positive. It also relates to how $V^{c\star}$ should be constrained so that the system is safe.

3.4 Impact of Adversarial Actions

In this section, we consider different attack scenarios to the droop-controller and discuss preliminary results on their impact with respect to a linearized version of (3.9).

The following subsections follow a similar structure and each one considers a specific attack scenario. In particular, each subsection begins by describing the adversarial model and how it affects the droop-controller. Then, the impact of the attack is characterized based on properties of the linearized system, such as stability and input-output induced-norm. Such characterizations also aim at identifying which sets of attacked nodes yield possibly higher impacts, thus indicating which threats may pose a high risk to the system. The theoretical analysis is then complemented with numerical simulations of the attack scenarios in the nonlinear system (3.9).

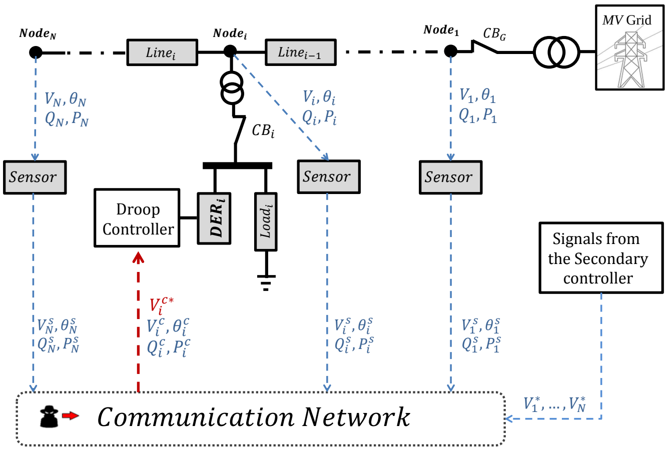

Figure 3.3: An inverter-based droop controller under a reference signal attack at bus i, where the adversary corrupts $V_i^{c\star}$.

Voltage Reference Attack

The present scenario considers an adversary that injects false-data into the communication network supporting the control system. In particular, we suppose that the reference signal of bus j is corrupted, as depicted in Figure 3.3, so that

$$V_j^{c\star}(t) = u^a(t). \tag{3.21}$$

Hence, the corresponding control signal at bus j is given by

$$u_{V_j} = -K_j V_j^c \left(V_j^c - u^a(t)\right) - Q_j^c, \tag{3.22}$$

where the $u^a(t)$ is defined by the adversary. The impact of the attack is measured in terms of the resulting changes to the voltage magnitude at another bus $i \neq j$ in the network, i.e. V_i. The resulting linearized system can be expressed as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \tau_j^{-1} K_j e_j u^a(t) \\ y_i(t) &= e_i^\top x(t) \end{aligned} \tag{3.23}$$

where $A = -[\tau]^{-1}\left([K] + L(\theta)\right)$ and $e_i \in \mathbb{R}^n$ is the i-th column of the n-dimensional identify matrix. In particular, we quantify the attack's impact as the maximum deviation of $y_i(t)$ caused by a corrupted reference $u^a(t)$ that is bounded as $|u^a(t)| \leq 1$. In fact, this metric corresponds to the $\mathcal{L}_\infty$-induced norm of (3.23). For power systems satisfying the conditions of Theorem 3.3.1 and Lemma 3.3.2, i.e., the system (3.23) is positive and stable, the following characterization of the worst-case attack naturally follows from Proposition 3.1.1.

Lemma 3.4.1. *Consider the linearized power system* (3.10)*, which is assumed to be positive and asymptotically stable, and let $H_{ij}(s)$ be the transfer function of* (3.23)*. The worst-case impact on node i of a reference attack on bus j, characterized as the $\mathcal{L}_\infty$-induced norm of* (3.23)*, is given by $H_{ij}(0) = -\tau_j^{-1}K_j e_i^\top A^{-1} e_j = \tau_j^{-1}K_j[-A^{-1}]_{i,j}$.*

Such characterization of the worst-case impact can be leveraged to compare different attacks and identify scenarios with higher impact. In particular, supposing bus j is attacked, we are interested in assessing which other bus $i \neq j$ is most affected by the attack. That is, we seek to compute

$$i^\star = \arg\max_i H_{ij}(0) = \arg\max_i [-A^{-1}]_{i,j},$$

where the common factor $\tau_j^{-1}K_j$ has been omitted.

Although solving such problem would, in general, require the computation of all entries of $-A^{-1}$, specific power system topologies admit simpler solutions. Specifically, for power systems whose topology corresponds to a line graph, the following result establishes that the $\mathcal{L}_\infty$-induced norm $[-A^{-1}]_{i,j}$ decreases as the distance between i and j increases.

Theorem 3.4.2. *Consider a power system satisfying the conditions of Theorem 3.3.1 and Lemma 3.3.2, whose topology corresponds to a line graph. Furthermore, suppose the droop-controller at bus j is under a reference signal attack, being described by* (3.22)*. Then the $\mathcal{L}_\infty$-induced norm of* (3.23) *is given by $H_{ij}(0) = \tau_j^{-1}K_j[-A^{-1}]_{i,j}$, which satisfies the monotonicity conditions*

$$\begin{aligned} &[-A^{-1}]_{i,j} > [-A^{-1}]_{i+1,j},\ \forall j \leq i \\ &[-A^{-1}]_{i,j} > [-A^{-1}]_{i-1,j},\ \forall j \geq i. \end{aligned} \tag{3.24}$$

Proof. Note that Theorem 3.3.1 and Lemma 3.3.2 imply that the power system (3.23) is positive and asymptotically stable, respectively. Hence, from Lemma 3.4.1, the $\mathcal{L}_\infty$-induced norm of (3.23) is given by $H_{ij}(0) = [-A^{-1}]_{i,j}$. Moreover, since the power system's topology is a line, the buses may be ordered so that the system matrix A is tridiagonal. Define the variables

$$\alpha_i = [-A]_{i,i}, \quad \beta_i = [-A]_{i,i+1}, \quad \varsigma_i = [-A]_{i+1,i},$$

which characterize the entries of the tridiagonal matrix $-A$. Assuming that $\beta_i \neq 0$

for all $i \leq N-1$, the inverse of A can be explicitly derived as [18, Theorem 2.1]

$$[-A^{-1}]_{i,j} = \begin{cases} (-1)^{i+j} \prod_{l=i}^{j-1} \beta_l \dfrac{\displaystyle\prod_{l=j+1}^{N} \phi_l}{\displaystyle\prod_{l=i}^{N} \delta_l} & \text{, if } j \geq i \\ (-1)^{i+j} \prod_{l=j}^{i-1} \varsigma_l \dfrac{\displaystyle\prod_{l=i+1}^{N} \phi_l}{\displaystyle\prod_{l=j}^{N} \delta_l} & \text{, if } j < i \end{cases}$$

with the convention that an empty product equals 1, where ϕ_i and δ_i are given by the recursions

$$\phi_i = \alpha_i - \frac{\beta_i \varsigma_i}{\phi_{i+1}}, \quad \phi_N = \alpha_N,$$
$$\delta_i = \alpha_i - \frac{\beta_{i-1}\varsigma_{i-1}}{\delta_{i-1}}, \quad \delta_1 = \alpha_1.$$

Hence, the conditions in (3.24) may be rewritten as

$$\begin{aligned} -\frac{\phi_{i+1}}{\varsigma_i} > 1, \ \forall j \leq i \\ -\frac{\delta_{i-1}}{\beta_{i-1}} > 1, \ \forall j \geq i. \end{aligned} \tag{3.25}$$

The proof follows through an induction argument, which makes use of the positivity and row-diagonally dominance properties of A. The induction argument for the second inequality of (3.24) is derived as follows. First we show that having $-\dfrac{\delta_{i-1}}{\beta_{i-1}} > 1$ for some $j \geq i$ implies that $-\dfrac{\delta_i}{\beta_i} > 1$ also holds. In fact, from the recursion of δ_i we have

$$\delta_i \geq -\beta_i - \varsigma_{i-1} - \frac{\beta_{i-1}\varsigma_{i-1}}{\delta_{i-1}} = -\beta_i - \varsigma_{i-1}(1 + \frac{\beta_{i-1}}{\delta_{i-1}}) \geq -\beta_i > 0,$$

where the first inequality follows from the positivity and the diagonally dominance properties of A, i.e., $\alpha_i = -[A]_{i,i} \geq [A]_{i,i+1} + [A]_{i,i-1} = -\beta_i - \varsigma_{i-1}$, while the hypothesis $-\dfrac{\delta_{i-1}}{\beta_{i-1}} > 1$ yields the second inequality. The induction argument is concluded by noting that $-\beta_i$ is positive and $-\dfrac{\delta_1}{\beta_1} = -\dfrac{\alpha_1}{\beta_1} \geq \dfrac{\beta_1}{\beta_1}$.

A similar proof holds for the first inequality of (3.24). □

Considering line graphs, using the results of Theorem 3.4.2, we conclude that the bus most affected by the attack at bus j, defined as $i^\star = \arg\max_i H_{ij}(0)$, corresponds to one of the neighboring buses of j, i.e., $i^\star = \arg \max_{i \in \{j-1,\, j+1\}} [-A^{-1}]_{i,j}$.

Numerical Example

To illustrate the impact of the attack on the reference signal, we consider a radial 4-bus power system in island mode with identical power lines, loads, and inverters. The power system is characterized by (3.4) with the parameters $\rho = 0.5$, $B_{ij} = -0.2$, and $G_{ij} = -\rho B_{ij}$ for all edges $(i, j) \in \mathcal{E}$ and $B_{ii} = -0.001$ and $G_{ii} = \rho |B_{ii}|$ for all buses. The power inverters are modeled by (3.5) and (3.6) with parameters $\tau_i = 10^{-4}$ and $K_i = 0.2$ for all buses. Additionally, the phase-angle differences are constant throughout the simulation of the voltage dynamics and are given by $\theta_{12} = -0.11$rad, $\theta_{23} = 0.045$rad, and $\theta_{34} = -0.11$rad.

The system dynamics are described by the nonlinear differential equations (3.9), with the corresponding linearized dynamics characterized by (3.10) with

$$A = 10^{-4} \cdot \begin{bmatrix} -4.01 & 1.88 & 0 & 0 \\ 2.1 & -6.01 & 2.04 & 0 \\ 0 & 1.95 & -6.01 & 1.88 \\ 0 & 0 & 2.1 & -4.01 \end{bmatrix}.$$

Clearly, the system is positive and row-diagonally dominant. Since the diagonal entries A are negative, the system is also asymptotically stable.

Now consider the reference signal attack scenario where the voltage reference transmitted to bus 3 is corrupted by an adversary, which is modeled by (3.23). Following the discussion in this section, we seek to assess which buses, other than bus 3, are most affected by such attack. From Lemma 3.4.1, the worst-case impact of such attack on a given bus i in the network corresponds to $H_{i3}(0) = -K_3 \tau_3^{-1} e_i^\top A^{-1} e_3$. In present example, the set of worst-case gains to buses 1, 2, and 4 are given by $H_{13}(0) = 0.09$, $H_{23}(0) = 0.19$, and $H_{43}(0) = 0.25$, respectively. As stated by Theorem 3.4.2, for line graphs, the largest worst-case impact takes place at one of the neighbors of bus 3, which here corresponds to bus 4.

The decrease of the impact as the distance to bus 3 increases is visible on the voltage trajectories of the nonlinear system under a reference attack on bus 3, as depicted in Figure 3.4.

Voltage Measurement Routing Attack

Here we consider an adversary that is able to redirect truthful data from its intended destination to another receiving bus in the network. In particular, we suppose that the adversary redirects the voltage measurement from bus j as if it were a measurement from bus i, which is captured by having

$$V_i^c = V_j^s = V_j.$$

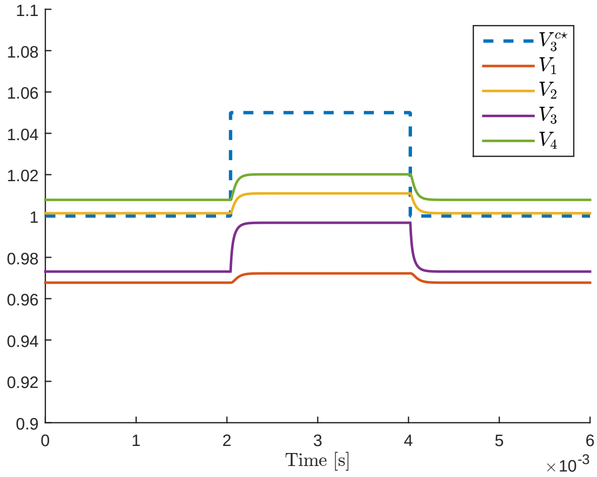

Figure 3.4: Trajectories of the voltage magnitudes under a reference signal attack at bus 3.

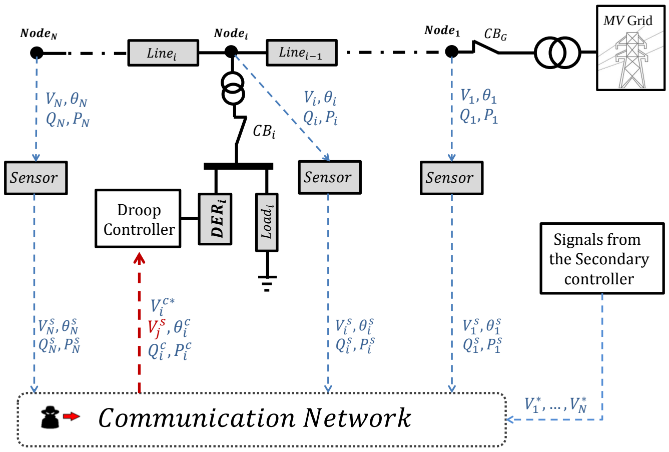

Figure 3.5: An inverter-based droop controller under a voltage measurement routing attack that feeds a measurement from bus j to bus i.

The corresponding control signal under attack is described as

$$\begin{aligned} u_{V_i} &= -K_i V_j^s \left(V_j^s - V_i^{c\star} \right) - Q_i^c \\ u_{V_k} &= -K_k V_k^c \left(V_k^c - V_k^{c\star} \right) - Q_k^c, \; \forall k \neq i. \end{aligned} \tag{3.26}$$

The resulting linearized system can be expressed as

$$\dot{x}(t) = \left(A - \tau_i^{-1} K_i e_i (e_j - e_i)^\top\right) x(t), \tag{3.27}$$

where the term $-\tau_i^{-1} K_i e_i (e_j - e_i)^\top x(t)$ can be interpreted as replacing the nominal feedback term $\tau_i^{-1} K_i V_i$ by the corrupted feedback $\tau_i^{-1} K_i V_j$ at bus i. In fact, such attack scenario can be rewritten as the following static output-feedback law

$$\begin{aligned} \dot{x}(t) &= \underbrace{(A + \tau_i^{-1} K_i e_i e_i^\top)}_{=\tilde{A}_i} x(t) + \tau_i^{-1} e_i u(t) \\ y_j(t) &= e_j^\top x(t) \\ u(t) &= -K_i y_j(t), \end{aligned} \tag{3.28}$$

where the matrix $\tilde{A}_i$ is independent of the control gain K_i.

Note that the closed-loop system under attack (3.27) is no longer positive, nor diagonally dominant, since we have $[A - \tau_i^{-1} K_i e_i (e_j - e_i)^\top]_{i,j} = -K_i < 0$ and $[A - \tau_i^{-1} K_i e_i (e_j - e_i)^\top]_{i,i} = [A]_{ii} + K_i$. As such, the results of Section 3.3 may not be used to establish the stability of (3.27). In fact, the closed-loop system (3.27) may indeed be unstable for certain values of $K_i \geq 0$, as established by the following result.

Theorem 3.4.3. *Consider the power system under routing attack described by* (3.27)*. There exists a control gain $K_i \geq 0$ for which the system is unstable if* $\operatorname{dist}(j, i) \geq 2$*, where* $\operatorname{dist}(j, i)$ *is the shortest length between buses i and j.*

Proof. The trivial case occurs when $\tilde{A}_i$ is not Hurwitz, for which $K_i = 0$ yields an unstable system. In the remaining of the proof, we suppose $\tilde{A}_i$ is Hurwitz. The proof follows from examining the root locus of the closed-loop system (3.28) with respect to the control gain $K_i > 0$. In particular, let r be the relative degree of the system, which also corresponds to the number of asymptotes of the root loci to which the closed-loop poles converge as $K_i > 0$ increases. Clearly, for $r \geq 3$ there exists at least one asymptote intersecting the complex right half-plane and we conclude that the system may become unstable for a sufficiently large gain K_i. To conclude the proof, we next argue that r is characterized as $r = \operatorname{dist}(j, i) + 1$.

Recall the definition of relative degree as the smallest integer $r \geq 1$ yielding a non-zero Markov parameter, i.e., $CA^{r-1}F \neq 0$. Given the particular structure of the feedback loop (3.28), this definition corresponds to the smallest integer for which $e_j^\top \tilde{A}_i^{r-1} e_i = [\tilde{A}_i^{r-1}]_{ji} \neq 0$ holds. Note that $\tilde{A}$ can be written as $\tilde{A}_i = -\mathcal{D}_i + \mathcal{A}$, where $\mathcal{D}_i$ is a diagonal positive definite matrix and $\mathcal{A}$ is a weighted adjacency matrix with positive edge-weights. Hence $\tilde{A}_i^k$ can be characterized as

$$\tilde{A}_i^k = \mathcal{A}^k + \sum_{l=0}^{k-1} \binom{k}{l} (-\mathcal{D}_i)^{k-l} \mathcal{A}^l. \tag{3.29}$$

Since the sparsity pattern of $\mathcal{A}^l$ is not altered by left-multiplying it with the diagonal matrix $(-\mathcal{D}_i)^{k-l}$, we conclude that $\min\{r > 0 \,|\, [\tilde{A}_i^{r-1}]_{ji} \neq 0\}$ is equal to $\min\{r >$

$0 \,|\, [\mathcal{A}^{r-1}]_{ji} \neq 0\}$. The remaining of the proof follows by using the non-negativity of $\mathcal{A}$ and Lemma 2.5 in [30], which states that there exists a path of length k between buses i and j if and only if $e_j^\top \mathcal{A}^k e_i > 0$. Since, by definition, $\mathrm{dist}(j,i)$ is the smallest integer such that $e_j^\top \mathcal{A}^{\mathrm{dist}(j,i)} e_i > 0$, we conclude that the system has relative degree $r = \mathrm{dist}(j,i) + 1$. □

Theorem 3.4.3 establishes the existence of a positive gain K_i for which the attacked system becomes unstable when $\mathrm{dist}(j,i) \geq 2$. Similar results were derived in [6] under the assumption that the open-loop system remains diagonally dominant, which does not hold for the present system.

Numerical Example

Recall the example described in Section 3.4 and consider the measurement routing attack scenario where an adversary replaces the voltage measurement at bus 1 with the voltage measurement of bus 4, which is modeled by (3.27) with $i = 1$ and $j = 4$. The resulting closed-loop state matrix is

$$\tilde{A}_1 - K_1 e_1 e_4^\top = 10^{-4} \cdot \begin{bmatrix} -2.01 & 1.88 & 0 & -2 \\ 2.1 & -6.01 & 2.04 & 0 \\ 0 & 1.95 & -6.01 & 1.88 \\ 0 & 0 & 2.1 & -4.01 \end{bmatrix},$$

which is clearly not diagonally dominant, nor positive. Despite stability, the lack of such properties leads to contradictory behaviors, as illustrated by the response to a step-change in one reference, depicted in Figure 3.6. Despite the increase in the reference signal, bus 1 further decreased its voltage.

As stated in Theorem 3.4.3, since the distance between buses 1 and 4 is greater than 1, there exists a gain $K_1 \geq 0$ for which the system under attack becomes unstable. This is illustrated through the corresponding root-locus depicted in Figure 3.7.

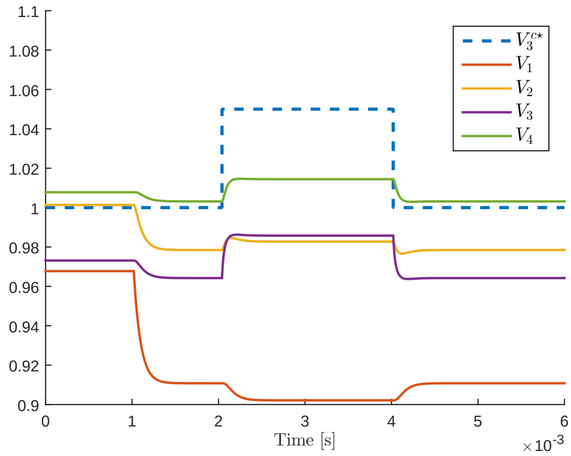

Figure 3.6: Trajectories of the voltage magnitudes under a voltage measurement routing attack that feeds a measurement from bus 4 to bus 1, followed by a reference change at bus 3.

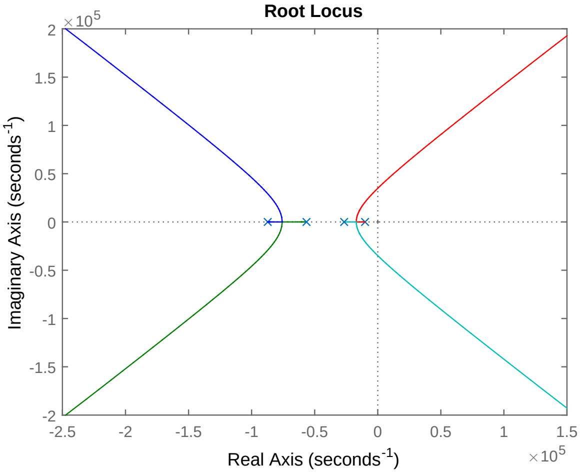

Figure 3.7: Root-locus of the system (3.28) with respect to $K_1 \geq 0$.

Chapter 4

Cyber-Physical Security Framework of Energy Management Systems

In this chapter, as a motivating application, a controlled HVAC system has been described and modeled first. We then describe a general hierarchical structure of an ICS, which is composed of lower layer and supervisory layer. A model for the attack to the measurements of the ICSs' lower layer, has been described, for which a resilience policy is proposed. We then study the stability and optimal performance of the this policy.

4.1 Application Domains

As we discussed in Example 1.1.2, an EMS optimally controls all energy sources in a building and considers an HVAC system as an important contributor to energy consumption. Connecting the EMS to the building communication network makes it a target for attacks with financial impact. In addition, attacking the EMS can lead to safety risks [36] due to damage to water transport system or to the heating sources (e.g. CHP and boilers). Thus, a resilience policy in Section 4.4 is proposed to mitigate the attack impacts. In order to evaluate the feasibility of the proposed framework, a Simulink model was developed to capture the CIT demo-site dynamics. The model was developed using *Grey Box* modelling [75], where the model structure is created based on the thermodynamic theory of each component and the model parameters are tuned using real-world data from the CIT demo-site. The model has been validated using data trend analysis against the real-world data at the CIT demo-site.

In order to evaluate the feasibility of the proposed framework, a Simulink model was developed to capture the CIT demo-site dynamics. The model was developed using *Grey Box* modelling [75], where the model structure is created based on the thermodynamic theory of each component and the model parameters are tuned

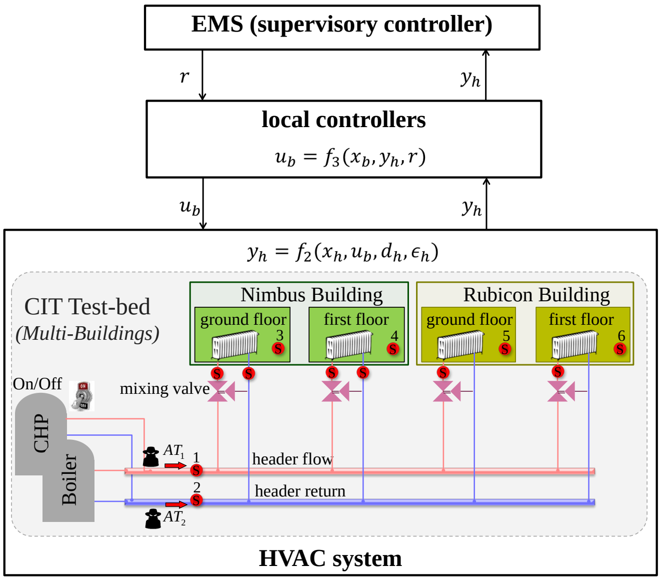

Figure 4.1: Typical BMS for HVAC system

using real-world data from the CIT demo-site. The model has been validated using data trend analysis against the real-world data at the CIT demo-site.

System Model Identification

A nonlinear model of the controlled HVAC system (see Figure 4.1) can be represented by

$$\underbrace{\begin{bmatrix} x_h(k+1) \\ x_b(k+1) \end{bmatrix}}_{x_s} = f_1(x_h(k), u_b(k), d_h(k), \epsilon_h(k)) \tag{4.1a}$$

$$y_h(k) = f_2(x_h(k), u_b(k), \epsilon_h(k)) \tag{4.1b}$$

$$u_b(k) = f_3(x_b(k), y_h(k), r(k)), \tag{4.1c}$$

where, x_h, x_b, u_b and y_h are the HVAC system's state, local controllers' state, control input and measurement signal, respectively. Here, d_h and ϵ_h are disturbance and noise, respectively. Here, the dynamic equation (4.1a) accounts for the thermal dynamics of the HVAC system including heating sources, mixing valves, pipe-lines and radiators, and dynamics of local controllers. The algebraic equation (4.1b) accounts for the measurement of the system, and (4.1c) represent control input vector u_b, including the PI and on/off controllers' signals being sent to the HVAC components. In addition, the signal r is being sent by the supervisory controller to the local controllers, which is considered as a correction signal and will be discussed in Section 4.4. Here, the noise ϵ_h can arise from measurement sensors, or water circulation loop.

The proposed resilience policy in Section 4.2 estimates outputs of the system, based on a linearized model of the controlled HVAC system shown in Figure 4.1. In practice, the precise model (4.1) may not be known. In addition, having access to the system-wide states x_h and x_b, for a bulk system, is not always the case. Thus, a linear model that is able to explain the covariance of the outputs (e.g., the six measurements of the sensors S_1-S_6 in Figure 4.1), is enough to estimate the output. To arrive at a linear state-space model of the controlled HVAC system (4.1), a subspace identification followed by a prediction error method [43] is applied here. In this identification, the external temperature (which is the disturbance d_h to the system) is considered as the input, and the temperature of header flow, header return, Nimbus building ground floor, Nimbus building first floor, Rubicon building ground floor and Rubicon building first floor are considered as the outputs, respectively. The system modeling in this manner results in a simple linear third-order system, in the innovation form [62]:

$$\begin{aligned} x_s(k+1) &= A_s x_s(k) + B_s u_b(k) + K_s \epsilon(k) \\ y_h(k) &= C_s x_s(k) + D_s u_b(k) + \epsilon(k), \end{aligned} \tag{4.2}$$

where the matrices A_s, B_s, C_s, D_s and K_s are the system's matrices with appropriate dimensions, and the innovation $\epsilon(k)$ is the noise (statistics of which is also estimated in the system identification) and independent of past input and output data [62].

4.2 Industrial Control Systems' Hierarchy

In this section, we describe a general hierarchical structure of an ICS, which is composed of lower layer and supervisory layer.

Lower Layer

Lower layer, which is called *plant*, consists of physical interconnected infrastructure and local controllers. A schematic of the plant is illustrated in Figure 4.2. As it is shown in this figure, the physical interconnected infrastructure is represented by interconnected processes $(P_i, i \in \Phi)$, which are controlled by the local controllers $(K_i, i \in \Phi)$. Here, $\Phi = \{1, ..., N\}$ is the index set of processes. In this networked control system, u_i, y_i, $\tilde{u}_i$ and $\tilde{y}_i$ are the sent control signal by the controller K_i, the sent sensor measurement by the process P_i, the received control signal by the process P_i, and the received measurement signal by the controller K_i, respectively. Here, the process P_i is given by

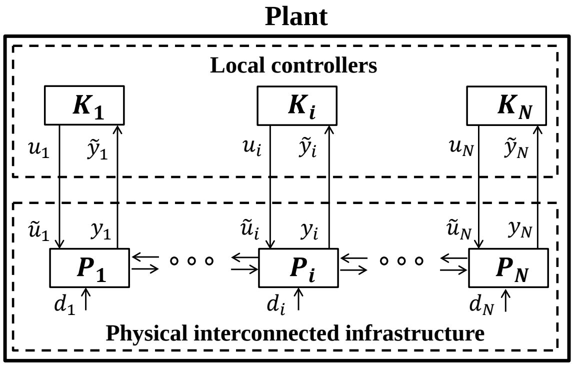

Figure 4.2: Schematic of a linear closed-loop system.

$$\begin{aligned} \xi_i(k+1) =& A_i\xi_i(k) + B_i\tilde{u}_i(k) + D_i d_i(k) + \sum_{j\neq i} J_{ij}C_j\xi_j(k) + w_i(k), \\ y_i(k) =& C_i\xi_i(k) + \nu_i(k). \end{aligned} \tag{4.3}$$

where, $\xi_i \in \mathbb{R}^{n_i}$ is the local state vector of the i^{th} process, $\tilde{u}_i \in \mathbb{R}^{s_i}$ is the received control signal vector, and $y_i \in \mathbb{R}^{p_i}$ is the local measurement vector. In (4.3), d_i is a deterministic disturbance vector, and w_i and ν_i are process and measurement zero-mean Gaussian white noise, respectively. Here, the matrices A_i, B_i, C_i, D_i and J_{ij} have dimensions conformably with the vectors, and the matrix J_{ij} captures the interaction between the processes P_i and P_j. The local control signal $u_i(k)$ is given by the controller K_i,

$$\begin{aligned} \eta_i(k+1) &= E_i\eta_i(k) + F_i\tilde{y}_i(k), \\ u_i(k) &= H_i\eta_i(k), \end{aligned} \tag{4.4}$$

where, $\eta_i \in \mathbb{R}^{q_i}$ is the local state vector of the controller, $u_i \in \mathbb{R}^{s_i}$ is the local control signal vector calculated by the controller, and $\tilde{y}_i \in \mathbb{R}^{p_i}$ is the received measurement vector. Here, the matrices E_i, H_i and F_i have dimensions conformably with the vectors. Thus, the closed-loop interconnected system evolves as

$$\begin{aligned} \begin{bmatrix} \xi(k+1) \\ \eta(k+1) \end{bmatrix} &= \underbrace{\begin{bmatrix} [A] + J[C] & [B][H] \\ [F][C] & [E] \end{bmatrix}}_{A^{cl}} \underbrace{\begin{bmatrix} \xi(k) \\ \eta(k) \end{bmatrix}}_{x(k)} + \underbrace{\begin{bmatrix} [D] \\ 0 \end{bmatrix}}_{B_1^{cl}} d(k) + \underbrace{\begin{bmatrix} I & 0 \\ 0 & [F] \end{bmatrix}}_{M} \begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix} \\ y(k) &= \underbrace{\begin{bmatrix} [C] & 0 \end{bmatrix}}_{C^{cl}} \begin{bmatrix} \xi(k) \\ \eta(k) \end{bmatrix} + \underbrace{\begin{bmatrix} 0 & I \end{bmatrix}}_{N} \begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix}, \end{aligned} \tag{4.5}$$

where, $x \in \mathbb{R}^{n_x}$ is the state vector of the plant, $[A]$ represents a block-diagonal matrix with A_i as the i-th diagonal block, and J is a matrix with J_{ij} as the (i, j)-th block (diagonal blocks are zero). Note that $\xi = [\xi_1^\top \dots \xi_N^\top]^\top$, $\eta = [\eta_1^\top \dots \eta_N^\top]^\top$, $y = [y_1^\top \dots y_N^\top]^\top$, $d = [d_1^\top \dots d_N^\top]^\top$, $u = [u_1^\top \dots u_N^\top]^\top$, $w = [w_1^\top \dots w_N^\top]^\top$ and $\nu = [\nu_1^\top \dots \nu_N^\top]^\top$. Let the expectation and the covariance of w and ν to be

$$\mathbf{E}\begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix} = 0,\ \mathbf{E}\begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix}\begin{bmatrix} w(l) \\ \nu(l) \end{bmatrix}^\top = \underbrace{\begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}}_{R}\delta_{kl}, \tag{4.6}$$

where, R_{11} and R_{22} are the covariance of w and ν, respectively, and $R_{12} = R_{21}^\top$ is the constant cross covariance between w and ν.

Note that the system described by (4.5) is under *normal condition*, and there is no anomaly in the received control and measurement signals $\tilde{u}_i$ and $\tilde{y}_i$. This means $\tilde{u}_i = u_i$ and $\tilde{y}_i = y_i$, $i \in \Phi$. Under this condition, we have the following assumption, which captures that the plant is assumed to be stable and well-configured initially.

Assumption 4.2.1. *The linear closed-loop system* (4.5) *is stable, which means the matrix A^{cl} is Schur stable (i.e., $\rho(A^{cl}) < 1$), and also the pair (A^{cl}, C^{cl}) is observable.*

Supervisory Layer

Supervisory layer, which is called *supervisory controller* here, can be viewed as the brain of the system. A schematic of the supervisory controller is illustrated in Figure 4.3, which provides us with three crucial subtasks:

1. *Attack detection*: decide whether or not an attack (see Section 4.3 for attack modeling) has occurred. This step determines the time at which some of the measurement signals are subject to attacks. When an attack is being detected we say it is in an *abnormal condition.*
2. *Attack isolation*: find in which measurements attacks have occurred. This step determines the location of the attacks (e.g., $\tilde{y}_i \neq y_i$).
3. *Controller reconfiguration*: if attack is being detected and isolated, the related control loops have to be reconfigured. Here, reconfiguration includes the selection of a new control configuration where the corrupted measurement signals are replaced by alternatives. To this end, correction signal r_i is derived and sent to the related local control loop to correct the corrupted signal $\tilde{y}_i$.

The SIA tool in the supervisory controller, which consists of a set of outlier detection algorithms and a web application, is responsible for attack detection (see Section 4.5). To perform the controller reconfiguration, the resilience policy applies estimation-based methods (see Section 4.4) to generate the correction signals r_i.

Remark 4.2.1. Here, both the SIA and the resilience policy, perform attack isolation using different methods, and the most conservative isolation is selected. This redundancy in the attack isolation, increases defense-in-depth in our proposed security framework.

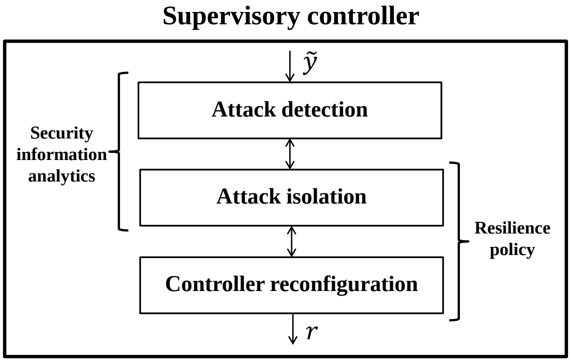

Figure 4.3: Schematic of the supervisory controller

4.3 Attack Model

Here, we consider the attacker as a man-in-the-middle, who can secretly listen to and alter the communication between the processes and controllers in the lower layer, knows the model of the plant (e.g., by applying system identification), and corrupt the measurement signals y_i. Here, the supervisory layer is assumed to not be accessible by the attacker. An example of an attack to the lower layer of an ICS is shown in the Figure 4.4, in which the measurement y_i is perturbed by adding the offset Δy_i. Thus, we define measurements' attack vector $\Delta y = [\Delta y_1^\top ... \Delta y_N^\top]^\top$, which has zero entries for the unattacked measurements, and non-zero entries for the attacked ones. Therefore, a general model for the received measurement signals by the local controllers, and subsequently supervisory controller, is given by

$$\tilde{y} = y + \Delta y. \tag{4.7}$$

Remark 4.3.1. Here, we assume that there is no attack on the control signals, $\tilde{u}_i = u_i$, $i \in \Phi$. The setup can be easily extended to include also the attacks on the control signals.

Undetectable Attack

As it is mentioned in Chapter 1, undetectable attacks are theoretically interesting, since they cannot be detected by the anomaly detectors. By assuming that $u = 0$, for an attack signal Δy to be undetectable, we need to ensure there exists an initial state x_0, which results in $\tilde{y} = 0$. Existence of such a signal can easily be checked by considering the matrix pencil (Rosenbrock system matrix)

$$\mathcal{P}(z) = \begin{bmatrix} A^{cl} - zI & B_a \\ C^{cl} & I \end{bmatrix}$$

where z is the invariant zero of the system (see [92]). Thus, an attack $\Delta y(k) = z_0^k \Delta y_0$, $\Delta y_0 \in \mathbb{C}^N$, $z_0 \in \mathbb{C}$, is undetectable iff there exists $x_0 \in \mathbb{R}^{n_x}$ such that $\mathcal{P}(z_0)$ does not have full column rank and we have

$$\mathcal{P}(z_0) \begin{bmatrix} x_0 \\ \Delta y_0 \end{bmatrix} = 0. \tag{4.8}$$

Remark 4.3.2. The proposed resilience policy in Section 4.4 guarantees that such undetectable attacks cannot be performed to the system.

4.4 Resilience Policy

A comprehensive security posture for the ICS should include mechanisms for attack diagnosis (detection and isolation) and response to attacks (controller reconfiguration). To keep the problem formulation contiguous with the previous section, and easier for the reader to follow, in this section resilience policy is discussed, and the next section is devoted to the attack diagnosis. The proposed resilience policy in this paper guarantees the ICS to meet these criteria:

1. *undetectable attack blocking*: no undetectable attack is possible to be injected to the measurement signals.

2. *stability*: system is stable under normal and abnormal conditions.

3. *performance optimality*: performance is optimal, in the measure of minimum variance error of state estimation, under abnormal condition.

Remark 4.4.1. To achieve all these criteria we need to protect some of the measurements. This protection can be done either by measurement signal encryption or by making it hard wired. Later in this section it is described which measurements should be protected.

Definition 4.4.1. *Considering that some of the measurements are protected, we define four types of measurements:*

1) Unprotected measurements*: we assume the attacker can have access to at most m number of sensor measurements y_j for $j \in \Gamma$. Here, $\Gamma \subset \Phi$ is the index set of unprotected measurements, and the cardinality of* Γ *is* $\mathbf{card}(\Gamma) = m$*.*

2) Protected measurements*: these measurement are not accessible by the attacker. Here, $\Gamma^C = \Phi \setminus \Gamma$ is the index set of protected measurements, where* $\mathbf{card}(\Gamma^C) = N - m = h$*.*

3) Attacked measurements*: since attacking all the unprotected measurements is costly for the attacker, some of them may be unattacked by the attacker. Thus, we define the set of attacked measurements y_j for $j \in \Gamma^a$. Here, $\Gamma^a \subset \Gamma$ is the index set of attacked measurements (*$0 \leq \mathbf{card}(\Gamma^a) \leq m$*), and we have $\tilde{y}_i \neq y_i$, $\forall i \in \Gamma^a$.*

4) Healthy measurements*: here, $\Gamma^h = \Phi \setminus \Gamma^a$ is the index set of healthy measurements, and we have $\tilde{y}_i = y_i$, $\forall i \in \Gamma^h$.*

Here, we consider the attacker to be able to secretly listen to, and alter the unprotected measurements. From [63] we learn that if the closed-loop transfer function from Δy_i to y_i, which is seen by the attacker, is nonzero, then the attacker can destabilize the system. To achieve this goal, the attacker derives the destabilizing feedback policy Δy_i, that violates the small-gain theorem's necessary and sufficient conditions.

Remark 4.4.2. Thus, to ensure the stability of the closed-loop system, the resilience policy should altogether eliminate the influence of the corrupted measurement from the control loop, by means of correction vector signal r. In this way the transfer function, from Δy_i to y_i becomes zero.

Control Reconfiguration

The correction vector signal r is generated and sent to the local controllers to correct the attacked signals y_j for $\forall i \in \Gamma^a$. This results to controller reconfiguration. To generate the correction vector signal r, an observer that is called *virtual sensor*, which is a Kalman filter, is implemented in the supervisory controller. Since the virtual sensor is running in the supervisory level, it has access to system-wide measurements $(y_1, ..., y_{n_y})$ and can estimate the states of the plant $(\hat{x}_i, i = 1, ..., n_x)$, based on the available model of the system and all the available healthy measurements, in all the times. By having $\hat{x}$, the correction vector signal r is calculated and sent to the plant by the supervisory controller (see Figure 4.4).

Since the attacker has access to the m number of unprotected measurements y_i, $\forall i \in \Gamma$, we can consider 2^m different attack scenarios. This means there are 2^m different modes $\sigma \in \{1, ..., 2^m\}$ for the system operation, and each mode indicates which measurements are under attack. Considering different modes of operation, the measurement attack vector and the correction vector signals are represented by Δy_σ and r_σ, respectively, at any given time k.

Here, the system mode is $\sigma = 1$ if system is under normal condition ($\Delta y_\sigma = 0$ if $\sigma = 1$), and we have $\sigma \in \{2, ..., 2^m\}$ for the all the possible abnormal conditions ($\Delta y_\sigma \neq 0$ if $\sigma \neq 1$). Note that by $\sigma = 2^m$ we mean the mode in which all the unprotected measurements are attacked. Having different modes of operation, and considering the introduced Δy_σ and r_σ, the discrete-time LTI system model (4.5) turns into a switched linear system (see [12])

$$\begin{aligned} x(k+1) =& A^{cl}x(k) + B_1^{cl}d(k) + B_2^{cl}\left(\Delta y_\sigma(k) + r_\sigma(k)\right) + M\begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix} \\ y(k) =& C^{cl}x(k) + N\begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix}, \end{aligned} \tag{4.9}$$

where, $B_2^{cl} = \begin{bmatrix} 0 & [F]^\top \end{bmatrix}^\top$. The switched linear model (4.9) is called abnormal system model. Note that $\sigma(k)$ can vary over time, and the goal of $r_\sigma(k)$ is to replace the attacked measurement $\tilde{y}$ with $\hat{y}$. Here, for simplicity of notation, we have used the subscript σ instead of $\sigma(k)$ which is dependent on the given time k.

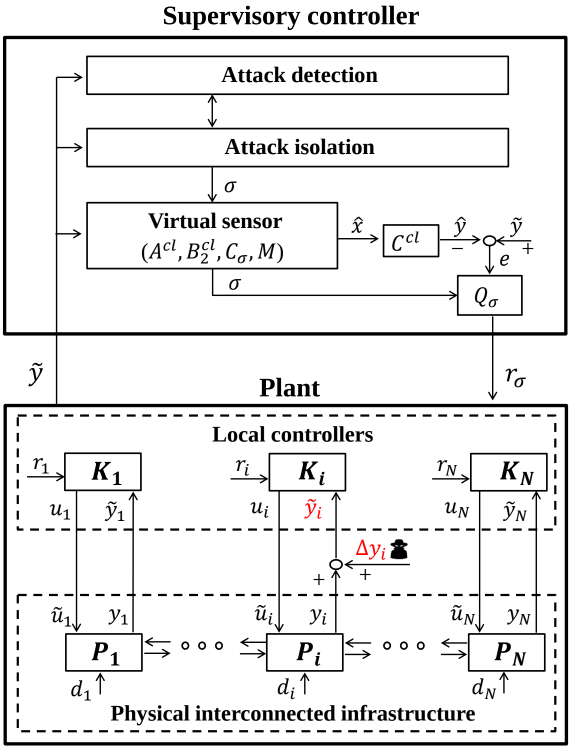

Figure 4.4: Schematic of control system, which is resilient against the adversarial actions on the measurements.

State Estimation Problem

Under the normal and abnormal conditions, and for different attack scenarios, the virtual sensor generates an estimate of the outputs $(C_i x_i(k), i \in \Phi)$, by receiving the measurement signals and based on the linear state-space model of the plant.

Remark 4.4.3. If the model of the processes P_i and the controllers K_i are not available, or the system is bulk (as discussed in Section 4.1), a linear state-space model that is able to explain the covariance of the outputs y and is being derived by applying system identification, may be used instead.

Note that the virtual sensor is an output estimator $(\hat{y}_i, i \in 1, ..., n_y)$ based on all the available healthy measurements (see [47]). Thus, the corrupted measurements are not used by the virtual sensor, and based on the mode of attack σ, it results in the switched linear systems. Under different operation modes σ, and at each given time k, a linear estimation $\hat{x}$ of the unknown system state x is determined here. At each given time k, the SIA informs the virtual sensor that the measurements

$y_j, j \in \Gamma^a$ are corrupted and should not be used for updating and predicting the states of the system. This means, the system mode σ is determined by the SIA and is being sent to the virtual sensor. To account for the fact that there can be communication delays between the plant and the supervisory controller, we make the following assumption. (The assumption can be relaxed at the expense of a slightly more complicated estimator.)

Assumption 4.4.1. *At the given time k, only the measurements until time $k-1$ are available in the supervisory controller.*

Based on Assumption 4.4.1, the virtual sensor, which is a switched Kalman filter here (see [12]), takes the prediction step for the state of the system as

$$\hat{x}(k+1|k) = A^{cl}\hat{x}(k|k-1) + K_\sigma(k)\underbrace{[y_\sigma(k) - C_\sigma\hat{x}(k|k-1)]}_{\epsilon(k)}, \tag{4.10}$$

where, $y_\sigma(k)$ is a vector of healthy measurements. Here, C_σ is constructed from the matrix C^{cl} by removing the rows related to the corrupted measurements and based on the operation mode σ. Note that by $\hat{x}(k|k-1)$ we mean an estimation of $x(k)$, given the measurements $y_\sigma(t)$ up until time $t = k-1$, and the optimal one step ahead prediction of $y(k)$ is $\hat{y}(k) = C^{cl}\hat{x}(k|k-1)$. The time-varying Kalman gain $K_\sigma(k)$ is given by

$$\begin{aligned} K_\sigma(k) &= \left(A^{cl}P_\sigma(k)C_\sigma^\top + R_{12\sigma}\right) \times (C_\sigma P_\sigma(k)C_\sigma^\top + R_{2\sigma})^{-1}, \\ P_\sigma(k) &= A^{cl}P_\sigma(k-1){A^{cl}}^\top + R_{1\sigma} - \left(A^{cl}P_\sigma(k-1)C_\sigma^\top + R_{12\sigma}\right) \\ &\quad \times \left(C_\sigma P_\sigma(k-1)C_\sigma^\top + R_{2\sigma}\right)^{-1} \times \left(A^{cl}P_\sigma(k-1)C_\sigma^\top + R_{12\sigma}\right)^\top . \end{aligned} \tag{4.11}$$

where, $P_\sigma(k)$ is the time-varying estimation error covariance matrix. In (4.11), we have $R_{1\sigma} = MRM^\top$, $R_{2\sigma} = N_\sigma RN_\sigma^\top$, and $R_{12\sigma} = MRN_\sigma^\top$. Here, N_σ is constructed from the matrix N by removing the rows related to the corrupted measurements and based on the operation mode σ.

In this assumption, the system is under the worst case attack mode $\sigma = 2^m$, in which all the m number of the unprotected sensor measurements ($y_j, \forall j \in \Gamma$) are under attack and the virtual sensor only uses the information of the protected measurements' noise. Therefore, the system is stabilizable for the all other modes σ. By having $\hat{x}(k|k-1)$, the correction signal for different mode is then given by

$$r_\sigma(k) = Q_\sigma(k)\left(\tilde{y}(k) - C^{cl}\hat{x}(k+1|k)\right). \tag{4.12}$$

Here, the matrix $Q_\sigma(k)$ is chosen to be a diagonal matrix, having -1 on diagonal entries related to the measurements under attack, and 0 on the rest. In this way, the resilience policy omits the attacked measurements (see Remark 4.4.2), and uses the estimated outputs instead.

Based on the estimated states, the supervisory controller will send the correction signal r_σ to the plant for control reconfiguration and to improve the performance of the system under attack. The local controller receives the signal $y + \Delta y_\sigma + r_\sigma$ to instead of $y + \Delta y_\sigma$. The signal $y + \Delta y_\sigma + r_\sigma$ would not be of the same quality, and may be time-delayed compared to measurements of the system y under normal condition. However, in this way we make sure that the attacker cannot destabilize the system (see Remark 4.4.2). The other advantage of this approach is that it does not require many changes in the lower-level designs. We next will prove that the proposed scheme indeed preserves performance optimality and stability.

Definition 4.4.2 (Completely switched observability [12])**.** *The deterministic part of* (4.9) *is completely switched observable over the finite time horizon [*k_0, k_1*] if and only if the observability matrix*

$$\boldsymbol{D}(k_1, k_0) := \begin{bmatrix} C_\sigma(k_0) \\ C_\sigma(k_0+1)A^{cl} \\ \vdots \\ C_\sigma(k_1)\left(A^{cl}\right)^{k_1-k_0} \end{bmatrix} \tag{4.13}$$

has full rank, $\operatorname{rank} \boldsymbol{D}(k_1, k_0) = n_x$ *for each possible switching sequence* $\sigma(k_0), ..., \sigma(k_1)$*.*

However, the switched observability of the system (4.9) is not ensured by the assumption that for each subsystem $\sigma \in \{1, ..., 2^m\}$, the pair (A^{cl}, C_σ) is observable. Therefore we need the following result.

Assumption 4.4.2. *There exists redundancy in the sensor measurements' information, and the system is observable from only the protected measurements,* $y_i, i \in \Gamma^C$*.*

Lemma 4.4.1. *Consider the switched system* (4.9) *with the finite number of switching modes* $\sigma \in \{1, ..., 2^m\}$*. This system is completely switched observable over the finite time horizon [*k_0, k_1*],* $\forall k_1 \geq k_0 + n_x - 1$ *under the Assumption 4.4.2.*

Proof. Based on the Assumption 4.4.2, at most m number of measurements could be corrupted, and there exist 2^m different modes $\sigma \in \{1, ..., 2^m\}$ for the switched system. Here, C_{2^m} relates to the worst case mode in which all the m measurements are corrupted. We know that C_{2^m} is in a subset of $C_\sigma, \forall \sigma \in \{1, ..., 2^m\}$. In addition, based on the Assumption 4.4.2, we know that A^{cl}, C_{2^m} is observable ($\mathbf{Obsv}(A^{cl}, C_{2^m}) = n_x$). Thus, $\operatorname{rank} \mathbf{Obsv}(A^{cl}, C_{2^m}) \leq \operatorname{rank} \mathbf{D}(k_1, k_0), \forall k_1 \geq k_0 + n_x - 1$, which means that $\operatorname{rank} \mathbf{D}(k_1, k_0) = n_x$. □

Lemma 4.4.2. *If for each possible switching sequence* $\sigma(k_0), ..., \sigma(k_1)$ *over the finite time horizon [*k_0, k_1*], the pair (*A^{cl}, C^{cl}_σ*) is completely switched observable and the pair (*A^{cl}, M*) is controllable, then by defining* $P_\sigma(k) = \boldsymbol{E}(e^x(k)e^x(k)^\top)$*, for an arbitrary switching sequence* $\sigma(0), ..., \sigma(k), \forall k$*, the error variance* $tr(P_\sigma(k))$ *of the switching state estimation is bounded. Note that* $e^x(k) = x(k) - \hat{x}(k)$ *is the estimation error.*

Proof. See [12], Lemma 2 for instance. □

Theorem 4.4.3. *The application of the switching Kalman filter* (4.10) *yields an unbiased linear estimate $\hat{x}(k)$ of the system state $x(k)$ with minimum error variances $\forall k \geq n_x - 1$, for an arbitrary switching sequence $\sigma(0), ..., \sigma(k)$.*

Proof. Based on the Lemma 4.4.1, the switched linear system (4.9) is completely switched observable over the finite time horizon $[0, k]$, $\forall k \geq n_x - 1$. By having completely switched observability, as it is shown in proof of Lemma 3 in [12], the switching Kalman filter (4.10) leads to the minimum error variance $\forall k \geq n_x - 1$. □

Remark 4.4.4. Considering only the protected measurement for the estimation, in all the conditions, gives a lower bound $(tr\,(P_\sigma(k))\,, \sigma = 2^m, \forall k)$ on the performance of the system in the sense of variance of the estimation error $e^x(k)$. Thus, by considering all the healthy measurements which gives us more information for the estimation, the application of the switching Kalman filter (4.10) yields an unbiased linear estimate $\hat{x}(k)$ of the system state $x(k)$ with minimum error variance $(tr\,(P_\sigma(k))\,, \sigma \in \{1, ..., 2^m\}, \forall k)$.

By designing the switched observer (4.10) for the stochastic switched linear system (4.9), for different modes of operation $\sigma_k \in \{1, ..., 2^m\}, \forall k$, the closed-loop dynamics of the system is given by

$$\begin{bmatrix} x(k+1) \\ e^x(k+1) \end{bmatrix} = \underbrace{\begin{bmatrix} A^{cl} & B_2^{cl} Q_\sigma C^{cl} \\ 0 & A^{cl} + B_2^{cl} Q_\sigma C^{cl} - K_\sigma(k) C_\sigma \end{bmatrix}}_{A_\sigma^{sp}} \begin{bmatrix} x(k) \\ e^x(k) \end{bmatrix} + \begin{bmatrix} B_1^{cl} \\ B_1^{cl} \end{bmatrix} d(k)$$
$$+ B_2^{cl} \begin{bmatrix} I + Q_\sigma \\ 0 \end{bmatrix} \Delta y_\sigma(k) + \begin{bmatrix} M + B_2^{cl} Q_\sigma N_\sigma \\ M + B_2^{cl} Q_\sigma N_\sigma - K_\sigma(k) N_\sigma \end{bmatrix} \begin{bmatrix} w(k) \\ \nu(k) \end{bmatrix}. \tag{4.14}$$

Assumption 4.4.3. *The states of the system* (4.9) *are all reachable, from the protected measurements' noise. This means that the pair $(A^{cl} - R_{12\sigma} R_{2\sigma}^{-1} C_\sigma, R_{1\sigma} - R_{12\sigma} R_{2\sigma}^{-1} R_{12\sigma}^\top)$ is stabilizable for $\sigma = 2^m$.*

Theorem 4.4.4. *The closed-loop system* (4.14) *is asymptotically stable, for arbitrary switching sequence modes $\sigma \in \{1, ..., 2^m\}, \forall k$.*

Proof. Here, since $(I + Q_\sigma)$ is a diagonal matrix with diagonal zero entries for the corresponding nonzero entries of $\Delta y_\sigma(k)$, the we have $(I + Q_\sigma)\,\Delta y_\sigma(k) = 0$. In addition, $e^x(k)$ is the input for the state $x(k)$, and the matrix $A_{\sigma_1}^{sp} \times A_{\sigma_2}^{sp} \times \cdots \times A_{\sigma_l}^{sp}, \forall l$, which is an upper block triangular matrix, has bounded off diagonal block (since the matrices A^{cl} and $A^{cl} + B_2^{cl} Q_\sigma C^{cl} - K_\sigma(k) C_\sigma$ are stable matrices). In [12], proof of Lemma 4, it is shown that the deterministic part of the error $e^x(k)$ is asymptotically stable in the sense of Lyapunov and vanishes for $k \to \infty$. Thus, the closed-loop system is asymptotically stable since the effects of $e^x(k)$ on $x(k)$ vanishes, the effect of $\Delta y_\sigma(k)$ on $x(k)$ is zero, and A^{cl} is Schur stable by Assumption 4.2.1. □

4.5 Attack Diagnosis

Attack diagnosis play an important role to recover the system from attack and is composed of attack detection and isolation, which are two of the crucial subtasks in the supervisory controller (see Section 4.2).

Attack Detection

The SIA tool is responsible for detecting potential attacks and for providing information to the resilient control policy. It consists of a set of anomaly detection algorithms that allows analysts to examine the results. The SIA tool uses a combination of (i) domain-specific expert knowledge and (ii) machine learning algorithms, to understand the behavior of the system under normal, stable operating conditions, and to detect any anomalies or deviations from normal behavior. These anomalies are flagged as potential attacks and the resilient policy is triggered to maintain stability of the system, while further investigation into the anomalies is carried out. The combination of expert knowledge and data-driven machine learning approaches aims to provide a high attack detection rate, in the face of highly sophisticated attackers. The expert knowledge component exploits domain-specific physical laws and system topology, to define the explicit relationships between different variables in the system; if these relationships are not satisfied by the measured variables, it may indicate that one or more of the variables is under attack. Despite not having explicit definitions, these relationships between operating conditions and measured variables can play an important role in detecting abnormal behavior in the system. A well-designed machine learning algorithm can allow the implicit patterns and dependencies in the data to be learned, building a model that represents the normal behavior of the system. Measured data can then be compared to the model to determine if the system is operating normally or not.

Attack Isolation

Attack isolation is one of the crucial subtasks in the supervisory controller (see Section 4.2), which determines the location of the attacks (e.g., $\tilde{y}_i \neq y_i$). In other words, it determines operational modes $\sigma_k \in \{1, ..., 2^m\}$ of the system in all the times. To perform the attack isolation here, the steps of the proposed algorithm are detailed in the following algorithm.

Remark 4.5.1. In the most conservative scenario, protected measurements are determined as the set of healthy measurements and $\hat{x}(k'+1|k')$ is computed based on those measurements only.

4.6 Simulation Results

The performance of the proposed resilient control for the BMS, is evaluated in this section. In the simulation results shown in the Figure 4.5, the temperature of header flow, header return, the ground and first floor of Nimbus building, and

Algorithm 4.1 Attack isolation algorithm

```
1: Attack is detected by SIA at time $k'$
2: Resilience policy generates the residue $r_e$, by using protected measurements only at time $k'$
3: Attacked measurements are isolated based on $r_e$, and a set of healthy measurements is determined by resilience policy
4: A set of *modified measurements* including healthy measurements plus estimation of the attacked ones (being estimated by the resilience policy based on the healthy measurements) is sent to SIA to confirm the normality of the set of the modified measurements
5: If the normality of the set of the modified measurements is confirmed by SIA, determine operational mode $\sigma_k$ and compute $\hat{x}(k'+1|k')$, otherwise a more conservative residue generation policy is chosen and go to step 2
```

the ground and first floor of the Rubicon building are under consideration. These temperatures are respectively corresponding to the six measurements of the sensors S_1-S_6 in Figure 4.1. The results are shown for three different cases of healthy BMS, attacked BMS, and attack-resilient BMS. In the simulations, a multi-attack scenario (the combined attacks AT_1 and AT_2, which is shown in Figure 4.1) is considered to start at the k' =3000s. It means that after the k', the measurements of the header flow and header return temperatures are manipulated by adding 15°C to each of them, and are fed to the respective controllers. In this attack scenario, the attack is considered to be detected by the SIA immediately after k', and the corrupted measurements are replaced with their estimates that are sent by the VS. As it is illustrated in Figure 4.1, the multi-attack on the measurements leads to high safety risk due to damaging of CHP in the attacked BMS, since return temperature is below 65°C after the attack. In this attack scenario, the attack-resilient BMS is robust against the multi-attack and have the same performance as the healthy BMS.

In Figure 4.6, measurements of the header flow and header return temperatures in the healthy BMS are shown, and compared with the estimates of the outputs of the attack resilient BMS. Note that the estimates of the outputs are computed by the VS, and one can see that the VS accurately estimates the measurements of the healthy system in the presence of the attack.

Some major factors such as communication delay, large amount of data, and time-consuming security analysis algorithms, can affect the real-time attack detections. To investigate performance of the proposed resilient control in these situations, the following scenario is considered. Assume that the same attack as before, starts at time k' =3000s, and is detected at 3300s (with five minutes delay). As it is shown in Figure 4.7, the attack-resilient BMS has the same outputs as the attacked BMS until attack detection (3300s), but it can recover the system to return to the normal conditions after that. We have done other simulations with different delays for the attack detections, and in all the cases, the attack-resilient BMS has

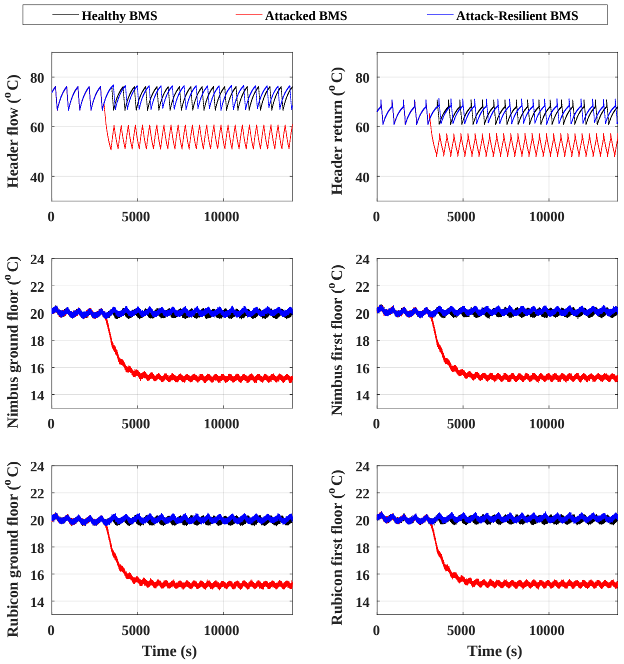

Figure 4.5: Performance comparison of the Healthy BMS, Attacked BMS and Attack-Resilient BMS, in the presence of attack on the header flow and return temperature measurements

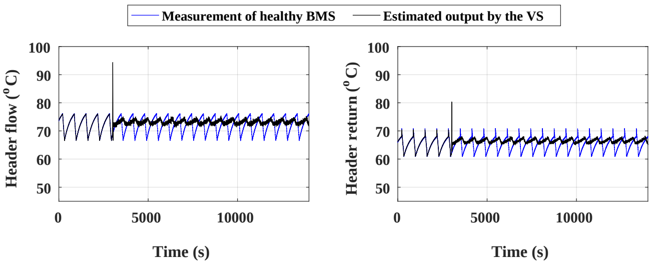

Figure 4.6: Measurements of the header flow and header return temperatures in the healthy BMS in comparison with the estimation of the outputs (which are computed by the VS) in the attack-resilient BMS.

recovered the system to return to the normal conditions after the attack detection.

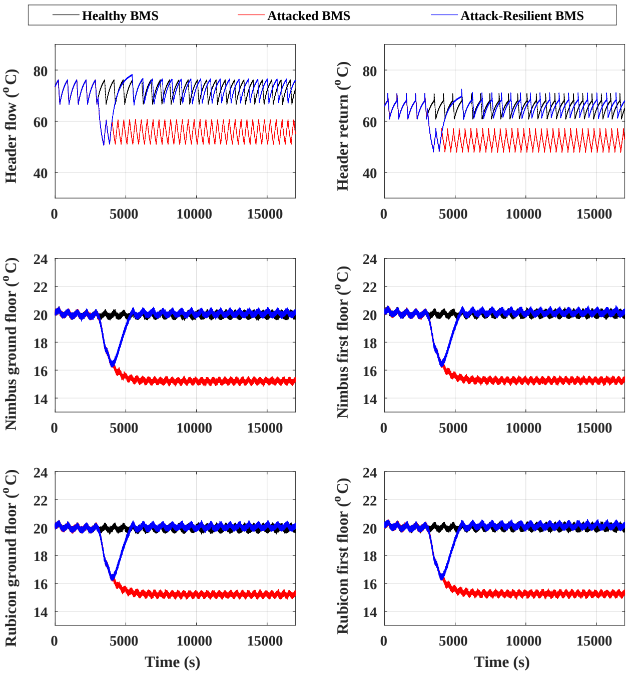

Figure 4.7: Performance comparison of the Healthy BMS, Attacked BMS and Attack-Resilient BMS, in the presence of delay in attack detection (the attack starts at time 3000s, and is detected at 3300s).

Chapter 5

Conclusion and Future Work

This chapter concludes Part II of this thesis. In Chapter 3, the properties of a voltage droop control scheme in interconnected microgrids under adversarial actions have been studied. First the power system dynamics under nominal operation were analyzed, and conditions ensuring relevant system properties, including stability, were derived. Then, two attack scenarios were discussed, where the adversary is able to manipulate the measurement data and reference signals received by the voltage droop controllers. Each attack scenario admits multiple instances, depending of which set of nodes are attacked. The potential impact of different instances of each scenario were compared using control-theoretic tools, which provides a basis to identify high-risk attack instance in each scenario. Our methodology was illustrated on a line network through numerical examples. A cyber-security framework applicable to a building Energy Management System is studied in Chapter 4. The framework uses the physics of the system to drive the security information analytics and resilient policy. System stability and framework efficiency is proved. Simulation studies are performed on a critical attack scenario, where the security information analytics algorithm triggers the resilient control to recover from the attack. Simulation results show that the proposed resilient control policy can recover the system from abnormal conditions, even when there exist delay for the attack detections.

There are several research directions to explore regarding the work presented in this part. In Chapter 3, quadratic droor controller has been applied for each MG. However there exist other types of controllers (e.g., droop and reactive current controllers), for which one can study the properties of voltage control scheme in interconnected MGs under adversarial actions. Although it is shown that the proposed resilience policy in Chapter 4 is able to cope with the attacks to the ICSs' lower layer, it would be interesting to investigate the cases where the supervisory layer is under attack at the same time. In this chapter virtual sensor generates an estimate of the outputs based on the identified linear state-space model of the plant. This model parameters are assumed to be perfect, while by considering uncertainties in them, stability and performance analysis of the system remain unclear.

Bibliography

[1] URL `http://www.stockholmroyalseaport.com/en/`.

[2] URL `http://www.nordpoolspot.com/`.

[3] URL `http://www.svk.se/`.

[4] URL `https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01`.

[5] G. Andersson, P.M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, A. Teixeira, G. Dan, H. Sandberg, and K.H. Johansson. Cyber-security of scada systems. In *Innovative Smart Grid Technologies (ISGT), IEEE PES*, pages 1–2, Jan 2012.

[6] J. A.Torres and S. Roy. Stabilization and destabilization of network processes by sparse remote feedback: Graph-theoretic approach. In *American Control Conference*, pages 3984–3989, June 2014.

[7] C. Bartusch, F. Wallin, M. Odlare, I. Vassileva, and L. Wester. Introducing a demand-based electricity distribution tariff in the residential sector: Demand response and customer perception. *Energy Policy*, 39:5008–5025, 2011.

[8] N. Bassamzadeh, R. Ghanem, S. Lu, and S. J. Kazemitabar. Robust scheduling of smart appliances with uncertain electricity prices in a heterogeneous population. *Energy and Buildings*, 84:537–547, 2014.

[9] D. Bertsimas and M. Sim. Robust discrete optimization and network flows. *Mathematical Programming*, 98:49–71, 2003.

[10] D. Bertsimas and M. Sim. The price of robustness. *Oper. Res.*, 52:35–53, 2004.

[11] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G.J. Pappas, and Insup Lee. Attack resilient state estimation for autonomous robotic systems. In *Intelligent Robots and Systems (IROS 2014), IEEE/RSJ International Conference on*, pages 3692–3698, 2014.

[12] G. Böker and J. Lunze. Stability and performance of switching kalman filters. *International Journal of Control*, 75(16-17):1269–1281, 2002.

[13] A. Bose. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid*, 1(1):11–19, 2010.

[14] S. Boyd and L. Vandenberghe. *Convex Optimization.* Cambridge University Press, 2004.

[15] A. A. Cardenas, P. K. Manadhata, and S. P. Rajan. Big data analytics for security. *IEEE Security & Privacy*, (6):7476, 2013.

[16] X. Chen, T. Wei, and S. Hu. Uncertainty-aware household appliance scheduling considering dynamic electricity pricing in smart home. *Smart Grid, IEEE Transactions on*, 4:932–941, 2013.

[17] Z. Chen, L. Wu, and Y. Fu. Real-time price-based demand response management for residential appliances via stochastic optimization and robust optimization. *Smart Grid, IEEE Transactions on*, 3:1822–1831, 2012.

[18] C. M. da Fonseca and J. Petronilho. Explicit inverses of some tridiagonal matrices. *Linear Algebra and its Applications*, 325(1–3), 2001.

[19] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - the new and improved power grid a survey. *IEEE Communications Surveys and Tutorials*, 2011.

[20] J. P. Farwell and R. Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[21] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *Automatic Control, IEEE Transactions on*, 59(6):1454–1467, 2014.

[22] M. Fischetti and M. Monaci. Light robustness. In *Robust and Online Large-Scale Optimization*, volume 5868, pages 61–84. Springer, 2009.

[23] J. E Gentle. *Random number generation and Monte Carlo methods.* Springer, 2003.

[24] L. Gkatzikis, I. Koutsopoulos, and T. Salonidis. The role of aggregators in smart grid demand response markets. *Selected Areas in Communications, IEEE Journal on*, 31:1247–1257, 2013.

[25] S. Gottwalt, W. Ketter, C. Block, J. Collins, and C. Weinhardt. Demand side management a simulation of household behavior under variable prices. *Energy Policy*, 39:8163–8174, 2011.

[26] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligent jammer with limited actions. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 1096–1101, 2010.

[27] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay. Microgrids. *Power and Energy Magazine, IEEE*, 5(4):78–94, July 2007.

[28] J. M. Hendrickx, R. M. Jungers, G. Vankeerberghen, and L. A. Wolsey. An efficient technique for solving the scheduling of appliances in smart-homes. In *American Control Conference (ACC)*, pages 4051–4058, June 2014.

[29] S. Hess, K. E Train, and J. W Polak. On the use of a modified latin hypercube sampling (MLHS) method in the estimation of a mixed logit model for vehicle choice. *Transportation Research Part B: Methodological*, 40:147–163, 2006.

[30] J. B. Hoagg and D. S. Bernstein. On the zeros, initial undershoot, and relative degree of lumped-mass structures. In *American Control Conference*, pages 394–399, June 2006.

[31] G. Hug and J.A. Giampapa. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *Smart Grid, IEEE Transactions on*, 3(3):1362–1370, Sept 2012.

[32] International Monetary Fund. Fiscal policy to address energy environmental impacts. Technical Report Ei R2014:18, IMF Survey Magazine, July 2014.

[33] A. Ipakchi and F. Albuyeh. Grid of the future. *Power and Energy Magazine, IEEE*, 7:52–62, 2009.

[34] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi. On detection of cyber attacks against voltage control in distribution power grids. In *Smart Grid Communications, IEEE International Conference on*, pages 842–847, November 2014.

[35] D. Kathan and et al. Assessment of demand response and advanced metering. *United States Federal Energy Regulatory Commission*, 2008.

[36] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1):81–85, 2010.

[37] S. Kim and G.B. Giannakis. Scalable and robust demand response with mixed-integer constraints. *Smart Grid, IEEE Transactions on*, 4:2089–2099, 2013.

[38] T.T. Kim and H.V. Poor. Scheduling power consumption with price uncertainty. *Smart Grid, IEEE Transactions on*, 2:519–527, 2011.

[39] O. Kosut, L. Jia, R. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *First IEEE International Conference on Smart Grid Communications*, 2010.

[40] E. Larsson, J. Leymann, G. Morèn, T. Alkefjärd, A. Falk, T. Björkström, C. Hjulström, J. Roupe, and K. Granath. The Swedish electricity and natural markets 2013. Technical report, The Swedish Energy Markets Inspectorate, June 2014.

[41] X. Lin, S. L. Janak, and C. A. Floudas. A new robust optimization approach for scheduling under uncertainty: I. bounded uncertainty. *Computers & Chemical Engineering*, 28:1069 – 1085, 2004.

[42] Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *16th ACM Conference on Computer and Communications Security*, 2009.

[43] L. Ljung. Prediction error estimation methods. *Circuits, Systems and Signal Processing*, 21(1):11–21, 2002.

[44] C.-H Lu, C.-L. Wu, T.-H. Yang, H.-W. Yeh, M.-Y. Weng, L.-C. Fu, and T.-Y.C. Tai. Energy-responsive aggregate context for energy saving in a multi-resident environment. *Automation Science and Engineering, IEEE Transactions on*, 11:715–729, 2014.

[45] J. M. Lujano-Rojas, C. Monteiro, R. Dufo-Lopez, and J. L. Bernal-Agustin. Optimum residential load management strategy for real time pricing (RTP) demand response programs. *Energy Policy*, 45:671–679, 2012.

[46] J. Lunze M. Staroswiecki M. Blanke, M. Kinnaert. *Diagnosis and Fault-Tolerant Control*. Springer, Berlin Heidelberg, 2006.

[47] J Lunze M Staroswiecki M Blanke, M Kinnaert. *Diagnosis and Fault-Tolerant Control*. Springer, Berlin Heidelberg, 2006.

[48] M. D. McKay, R. J. Beckman, and W. J. Conover. A comparison of three methods for selecting values of input variables in the analysis of output from a computer code. *Technometrics*, 42:55–61, 2000.

[49] J. Minx, K. Scott, G. Peters, and J. Barrett. An Analysis of Sweden Carbon Footprint. Technical report, Stockholm Environment Institute, University of York, Heslington, YO10 5DD, UK, 2008.

[50] A. Mishra, D. Irwin, P. Shenoy, J. Kurose, and Ting Zhu. Smartcharge: Cutting the electricity bill in smart homes with energy storage. pages 1–10, 2012.

[51] D.E. Olivares, C.A. Cañizares, and M. Kazerani. A centralized energy management system for isolated microgrids. *Smart Grid, IEEE Transactions on*, 5(4):1864–1875, 2014.

[52] D. O'Neill, M. Levorato, A. Goldsmith, and U. Mitra. Residential demand response using reinforcement learning. In *Smart Grid Communications (SmartGridComm), First IEEE International Conference on*, pages 409–414, 2010.

[53] Organisation for Economic Co-operation and Development (OECD). Effective carbon prices. Technical report, OECD Publishing, 2013.

[54] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, Insup Lee, and G.J. Pappas. Robustness of attack-resilient state estimators. In *Cyber-Physical Systems (ICCPS), 2014 ACM/IEEE International Conference on*, pages 163–174, 2014.

[55] K. Paridari and et al. Attack-resilient industrial control systems: attack diagnosis and controller reconfiguration for energy management systems. In preparation, 2016.

[56] K. Paridari, A. E. D. Mady, S. La Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, and M. Boubekeur. Cyber-physical-security framework for building energy management system. In *ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–9, 2016.

[57] K. Paridari, A. Parisio, H. Sandberg, and K. H. Johansson. Energy and CO_2 efficient scheduling of smart appliances in active houses equipped with batteries. In *Automation Science and Engineering (CASE), IEEE International Conference on*, 2014.

[58] K. Paridari, A. Parisio, H. Sandberg, and K. H. Johansson. Demand response for aggregated residential consumers with energy storage sharing. In *54th IEEE Conference on Decision and Control (CDC)*, pages 2024–2030, 2015.

[59] K. Paridari, A. Parisio, H. Sandberg, and K. H. Johansson. Robust scheduling of smart appliances in active apartments with user behavior uncertainty. *IEEE Transactions on Automation Science and Engineering*, 13(1):247–259, 2016.

[60] K. Park, Y. Kim, S. Kim, K. Kim, W. Lee, and H. Park. Building energy management system based on smart grid. *Telecommunications Energy Conference (INTELEC), 2011 IEEE 33rd International*, pages 1–4, October 2011.

[61] F. Pasqualetti, F. Dorfler, and F. Bullo. Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems. *Control Systems, IEEE*, 35(1):110–127, 2015.

[62] S. Joe Qin. An overview of subspace identification. *Computers and Chemical Engineering*, 30(12):1502–1513, 2006.

[63] A. Rai, D. Ward, S. Roy, and S. Warnick. Vulnerable links and secure architectures in the stabilization of networks of controlled dynamical systems. In *American Control Conference (ACC), 2012*, pages 1248–1253, 2012.

[64] A. Rantzer. Distributed control of positive systems. In *Decision and Control and European Control Conference (CDC-ECC), 50th IEEE Conference on*, pages 6608–6611, Dec 2011.

[65] J. Rivera, P. Wolfrum, S. Hirche, C. Goebel, and H.-A. Jacobsen. Alternating direction method of multipliers for decentralized electric vehicle charging control. In *Decision and Control (CDC), IEEE 52nd Annual Conference on*, pages 6960–6965, 2013.

[66] P. Samadi, H. Mohsenian-Rad, V.W.S. Wong, and R. Schober. Tackling the load uncertainty challenges for energy consumption scheduling in smart grid. *Smart Grid, IEEE Transactions on*, 4:1007–1016, 2013.

[67] H. Sandberg, A. Teixeira, and K. H. Johansson. On security indices for state estimators in power networks. In *First Workshop on Secure Control Systems, CPSWeek*, Stockholm, Sweden, April 2010.

[68] H. E. Scarf and T. Hansen. *The computation of economic equilibria.* Cowles foundation for research in economics at Yale university. Yale University Press, New Haven, 1973.

[69] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S.S. Sastry. Foundations of control and estimation over lossy networks. *Proceedings of the IEEE*, 95(1):163–187, 2007.

[70] J. Schiffer, R. Ortega, A. Astolfi, J. Raisch, and T. Sezi. Conditions for stability of droop-controlled inverter-based microgrids. *Automatica*, 50(10):2457–2469, 2014.

[71] F. Shahnia, R. P.S. Chandrasena, S. Rajakaruna, and A. Ghosh. Primary control level of parallel distributed energy resources converters in system of multiple interconnected autonomous microgrids within self-healing networks. *IET Generation, Transmission & Distribution*, 8(2):203–222, 2014.

[72] P. Siano. Demand response and smart grids-a survey. *Renewable and Sustainable Energy Reviews*, 30:461–478, 2014.

[73] J. W. Simpson-Porco, F. Dörfler, and F. Bullo. Synchronization and power sharing for droop-controlled inverters in islanded microgrids. *Automatica*, 49 (9):2603 – 2611, 2013.

[74] J.W. Simpson-Porco, F. Dorfler, and F. Bullo. Voltage stabilization in microgrids via quadratic droop control. In *Decision and Control (CDC), IEEE 52nd Conference on*, pages 7582–7589, Dec 2013.

[75] B. Sohlberg. *Supervision and Control for Industrial Processes: Using Grey Box Models, Predictive Control and Fault Detection Methods.* Springer, 1998.

[76] M. Song, K. Alvehag, J. Widen, and A. Parisio. Estimating the impacts of demand response by simulating household behaviours under price and co$_2$ signals. In *Electric Power Systems Research*, pages 4051–4058, 2014.

[77] K. C. Sou, M. Kordel, J. Wu, H. Sandberg, and K. H. Johansson. Energy and CO$_2$ efficient scheduling of smart home appliances. In *Control Conference (ECC), European*, pages 4051–4058, 2013.

[78] K. C. Sou, H. Sandberg, and K. H. Johansson. Electric power network security analysis via minimum cut relaxation. In *50th IEEE Conference on Decision and Control*, December 2011.

[79] K. C. Sou, J. Weimer, H. Sandberg, and K. H. Johansson. Scheduling smart home appliances using mixed integer linear programming. In *Decision and Control and European Control Conference (CDC-ECC), 50th IEEE Conference on*, pages 5144–5149, 2011.

[80] P. Stoll, N. Brandt, and L. Nordstrom. Including dynamic CO_2 intensity with demand response. *Energy Policy*, 65:490 – 500, 2014.

[81] S. Sundaram and C.N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *Automatic Control, IEEE Transactions on*, 56(7):1495–1508, 2011.

[82] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R.B. Bobba, and A. Valdes. Security of smart distribution grids: Data integrity attacks on integrated Volt/VAR control and countermeasures. In *American Control Conference*, pages 4372–4378, June 2014.

[83] A. Teixeira, K. Paridari, H. Sandberg, and K.H. Johansson. Voltage control for interconnected microgrids under adversarial actions. In *IEEE International Conference on Emerging Technology and Factory Automation*, 2015.

[84] A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson. Optimal power flow: closing the loop over corrupted data. In *American Control Conference*, 2012.

[85] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135 – 148, 2015.

[86] J. S. Vardakas, N. Zorba, and C. V. Verikoukis. A survey on demand response programs in smart grids: Pricing methods and optimization algorithms. *IEEE Communications Surveys Tutorials*, 17(1):152–178, 2015.

[87] R. Verschae, H. Kawashima, T. Kato, and T. Matsuyama. Coordinated energy management for inter-community imbalance minimization. *Renewable Energy*, 2015.

[88] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg. Network-aware mitigation of data integrity attacks on power system state estimation. *IEEE Journal on Selected Areas in Communications*, 30(6):1108–1118, 2012.

[89] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *First IEEE International Conference on Smart Grid Communications*, 2010.

[90] Z. Xu, Q.-S. Jia, and X. Guan. Supply demand coordination for building energy saving: Explore the soft comfort. *Automation Science and Engineering, IEEE Transactions on*, pages 1–10, 2014.

[91] Z. Xu, J. Ostergaard, and M. Togeby. Demand as frequency controlled reserve. *Power Systems, IEEE Transactions on*, 26:1062–1071, 2011.

[92] Kemin Zhou, John C. Doyle, and Keith Glover. *Robust and Optimal Control*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1996.

[93] Q. Zhu, C. Rieger, and T. Basar. A hierarchical security architecture for cyber–physical systems. In *Resilient Control Systems (ISRCS), 2011 4th International Symposium on*, pages 15–20, 2011.

[94] J. P. Zimmermann. End-user metering campaign in 400 households in Sweden, assessment of the potential electricity savings. In *ENERTECH, Tech. Rep.*, pages 4051–4058, 2009.