2017

Cybersecurity of Demand Side Management in the Smart Electricity Grid

Jiyun Yao
Lehigh University

CYBERSECURITY OF DEMAND SIDE MANAGEMENT IN THE SMART ELECTRICITY GRID

Privacy Protection, Battery Capacity Sharing and Power Grid under Attack

By

Jiyun Yao

A dissertation

Presented to the Graduate and Research Committee

of Lehigh University

in Candidacy for the Degree of

Doctor of Philosophy

in

Electrical Engineering

August, 2017

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Date

Dissertation Director

Accepted Date

Committee Members:

Prof. Parv Venkitasubramaniam
(Committee Chair)

Prof. Shalinee Kishore

Prof. Rick S. Blum

Prof. Lawrence V. Snyder

Acknowledgements

First and foremost, I would like to thank my advisor Prof. Parv Venkitasubramaniam. He taught me the constant effort for striving for the perfection and the foremost requirement of discipline in research and in life.

I also thank Parv for teaching me courses, named: Information Theory, Fundamentals of Data Networks and Stochastic Control. I would like to emphasize here that these courses proved really helpful for me to understand the literature of stochastic optimization and game theory which turn out to be crucial in proving some optimality results in this work.

I also thank Parv to provide me financial help during my Ph.D. research, therefore, without any thought of financial trouble, I was able to conduct my thesis.

I would like to thank Professor Shalinee Kishore for teaching me course Advanced Topics in Smart Grid Communication, collaborating with me in the SEEDS project on DSM Misuse and for being in my thesis committee. I would like to emphasize here that the course Advanced Topics in Smart Grid Communication proved really helpful for me to understand the literature of Smart Grid which turn out to be crucial in the completion of this work.

I would like to thank Professor Rick S. Blum for teaching me the course Signal Detection and Estimation, collaborating with me in the SEEDS project on DSM Misuse and for being a member of my thesis committee. I am really thankful for the Signal Detection and Estimation course to Prof. Blum and especially for some interesting discussion in this course.

I would like to thank Professor Lawrence V. Snyder for collaborating with me in the SEEDS project on DSM Misuse and for being a member in my thesis committee. I am really thankful for many insightful discussions and helpful suggestions.

I would like to thank my office mates, Abhishek Mishra, Omid Javidbakht, Ruochi Zhang, Parth Pradhan, Basel Alnajjab for discussions on various research topics and presenting interesting papers that motivated me to look further into that direction.

I would like to thank four of my friends, named: Xueqin Lin, Chen Ji, Xingchao

Wang with whom discussions on various topics leads to some very good and interesting contributions in my research.

Contents

List of Tables

List of Figures

Abstract

The presented research investigates two areas in security of Demand Side Management (DSM) systems in Smart Grid including privacy aware energy storage management and risk assessment of cyber attack on DSM communication infrastructure.

The first topic studies the privacy-cost saving tradeoff of an in-home energy storage system in demand response for an individual user. DSM systems in the electricity grid, which rely on two way communication between the consumers and utility, require the transmission of instantaneous energy consumption to utilities. Perfect knowledge of a user's power consumption profile by a utility is a violation of privacy and can be detrimental to the successful implementation of demand response systems. It has been shown that an in-home energy storage system (such as a battery/inverter) that provides a viable means to achieve the cost savings of instantaneous electricity pricing without inconvenience can also be used to hide a user's power usage pattern. A fundamental tradeoff exists between the costs saved and the degree of privacy achievable, and in this work, the tradeoff achievable by a finite capacity battery assuming a zero tolerance for activity delay is studied using a Markov process model for user's demands and instantaneous electricity prices. Due to high computational complexity (continuous state-action space) of the stochastic control model, inner and upper bounds are presented on the optimal tradeoff. In particular, a class of battery charging policies based on minimizing "revealing states" is proposed to derive achievable privacy-cost savings tradeoffs. The performance of this algorithm is compared with inner bounds derived using a greedy heuristic and upper bounds derived using an information theoretic rate distortion approach. The framework proposed is shown to be applicable even when users only desire partial information protection such as presence/absence of activity or specific appliances they wish to hide.

The second topic studies the competitive energy storage sharing in demand response. Deregulated electricity markets with time varying electricity prices and opportunities for consumer cost mitigation makes energy storage such as a battery an attractive proposition. Sharing a large capacity battery across a group of homes in a community, can not only alleviate the economic deterrents but also exploit the fact that users' activity patterns do not necessarily overlap. However, battery sharing induces competition for battery capacity between the users in general as they may want to maximize their own cost savings by occupying more battery capacity when the electricity price is low. Importantly, users might have privacy concerns when they communicate with the shared battery controller. The privacy

aware management of such a shared battery is the focus of this work. A game theoretical framework was proposed to capture the competitive behaviors of users sending messages through a communication network to an independent battery controller with an infinite horizon limiting average signaling game formulation. The privacy requirement serves as a constraint on messaging behaviors. The battery controller manages the charging and discharging based on the received, albeit incomplete, information transmission. With such a framework, we study the battery sharing when users are cooperative and completely private. When the privacy requirement is relaxed, the competitive behaviors of users sending messages to the battery controller is studied. A credit based battery management strategy is designed for the battery controller to ensure an equilibrium of the game and achieves the social optimality. However, the credit based battery management requires long time established observations and may also "coerce" users to share their energy demands accurately with the controller. We therefore, propose, a class of stationary suboptimal privacy preserving battery management strategy in which the message set being restricted to be completely private or partially private. In addition, we demonstrate that by changing the size of the message set, different pairs of preserved privacy and cost savings can be achieved. Through numerical simulations on real electricity pricing and usage data, we demonstrate the cost effectiveness of battery capacity sharing and the tradeoff between privacy preserving and cost mitigation using privacy preserving battery management strategy.

The third topic study the risk assessment of cyber attack on DSM system including economically motivated meter tampering and malicious cyber attack. Cyber-enabled Demand Side Management (DSM) plays a crucial role in smart grid by providing automated decision-making capabilities that selectively schedule loads on these local grids to improve power balance and grid stability. Security and reliability of the cyber infrastructure that enables DSM is therefore critical to ensuring reliability and safety in energy delivery systems. The DSM communication are usually built on Advanced Metering Infrastructure (AMI). However, by virtue of topological weaknesses, it is vulnerable to cyber attacks that are undetectable or stealthy. In this work, we investigate the topological vulnerabilities of DSM networks that could result in potential theft of electricity through hacked smart meters. In particular, a provably correct risk assessment protocol is proposed to identify completely the individual nodes in mesh network based AMIs that are potential targets of such economically motivated stealthy cyber attacks. The protocol proposed utilizes knowledge of the network topology and data obtained from existing system monitoring technologies. A case study is provided to demonstrate the protocol and its effectiveness. Another major challenge in DSM security is that the feedback mechanism in the load management may

aggravate the impact of cyber attack on the DSM system. We investigate the behavior of such feedback loop under the intentional cyber attack and evaluate its potential risk of overloading the power grid components. In particular, a tight upper bound is provided to characterize the potential risk when a fixed portion of the controllable loads are compromised.

1. Introduction

Renewable energy share had increased to more than a quarter of global electricity production at the end of 2015 and this number has been rising every year [1]. Due to increased volatility of renewable energy and the emergence of flexible load scheduling through energy management systems, grid operators have already begun to rely on *demand side management* (DSM) technology to match anticipated demand with the temporal generation profile [2].

1.1 Utility-Privacy Tradeoff of Energy Storage Management

Demand response, as is well known, requires two way communication between the consumer and the utility; the utility transmits instantaneous prices, and the consumer's instantaneous (or granulated) consumption is transmitted back to the utility. The time varying prices provide incentive for the consumer to change his/her usage patterns providing operational benefit to the utility and cost benefit to the consumer. When this two way communication is perfect, in the absence of any consumer side action, or in other words, if the consumer's consumption pattern does not adapt to the demand response mechanism, i) there is no cost-saving due to instantaneous prices ii) user's privacy can be violated due to non-intrusive load monitoring by the utility [3,4]. The primary theme is to study a demand response scenario that aims to alleviate both these concerns, or in other words, save costs and maintain privacy.

Cost-savings alone can be accomplished by the consumer should he choose to alter his consumption pattern, for instance, by turning on appliances when prices are low and reducing activities when prices are high. Such strategies save costs by reducing user convenience (due to delay in activities) and do not alleviate the privacy issue.

An alternative mechanism to save costs without incurring much delay is the use of an in-home battery. Many recent studies [5–7] have investigated optimal charging and discharging

policies for batteries that balance cost savings with user convenience. In addition, practical experiments by ABB and GM in the United States [8] have demonstrated the viability and cost effectiveness for small scale storage to supply up to 3 hours of electricity usage for a group of 2-3 homes. An in-home battery can be charged when prices are low and be an alternative source of electricity when prices are high thus achieving cost-savings even under the assumption that "all demand is met immediately" either from the grid or from the battery. Most notably, in addition to providing cost-savings while guaranteeing convenience, the use of a battery can also provide privacy of actual demand– at any given time, the total consumption as measured by the utility would be an aggregate of the demand and the battery charge or discharge and without knowing exactly the amount of inflow or outflow of electricity from the battery, there is uncertainty in the *real* demand. From the consumer perspective, there are two objectives, cost-savings and privacy protection, accomplished to varying degrees through the use of an in-home battery. These objectives are not necessarily aligned and the primary purpose is to investigate the tradeoff between these objectives such that users can tailor their battery charging/discharging mechanism to satisfy their desires for cost-savings and privacy.

In this work, we study the design of battery charging and discharging algorithms under practical limitations in response to time varying demand and prices assuming a zero tolerance for delay. For this purpose, we investigate a formal mathematical framework using Markov modeled systems and use Shannon's equivocation [9] to characterize the uncertainty of the demand from the utility's perspective.

The notion of privacy we consider is *acausal* in the sense that the eavesdropper/utility can observe the entire time horizon of consumption data (the prices and fine grained electricity purchase data) to estimate the usage pattern in a household. Under this framework, we demonstrate that the optimal policy is in fact a solution to a Partially Observable Markov Decision Process with non linear belief dependent rewards (ρ-POMDP). Due to the continuous state-action space in this model, deriving optimal policies is computationally infeasible. We therefore propose a class of battery charging policies based on minimizing the frequency of "revealing states" so as to obtain an achievable privacy-cost savings tradeoff for users. When the underlying model is limited to i.i.d. demand and price processes, we show that the parameters of this class can be optimized analytically. We compare the resulting performance with a greedy heuristic that aims to maximize instantaneous privacy and cost savings rewards, as well as with an upper bound on the privacy-cost savings tradeoff which we derive using classical information theoretic rate-distortion optimization. The closeness of the derived bounds, as shown in Section 3.5 based on real electricity usage and pricing

data, demonstrate the efficacy of the proposed class of algorithms. In some scenarios, a user may only be interested in hiding some basic information such as his presence/absence, or a particular usage pattern; we extend our formulation to measure such *partial information leakage* and analyze the protection our proposed policies can provide.

1.2 Privacy Aware Management of Distributed End-user Energy Storage Sharing

Renewable energy share had increased to more than a quarter of global electricity production at the end of 2015 and this number has been rising every year [1]. The increased penetration of unpredictable renewable energy sources and the emergence of flexible load scheduling through energy management systems, have led grid operators to start relying on *demand response* technology to match anticipated demand with the temporal generation profile [2]. A popular tool in demand response is time-varying prices, which induces consumers to modulate their electricity usage to facilitate better planning and maximize grid efficiency; for instance price variation can be used to shave off the peak power consumption and consequently reduce the need for inefficient peak power generators. The success of demand response relies on time varying prices providing the opportunity for consumers to save costs should they choose to alter their consumption pattern, for instance, by turning on appliances when prices are low and reducing activities when prices are high. Such strategies save costs by reducing user convenience (due to delay in activities).

The time varying pricing also provides an opportunity for consumers to save cost *without sacrificing convenience* through the use of an energy storage system such as a battery and inverter; consumers can charge the battery when prices are low and discharge the battery for activities when prices are high thus limiting the need to delay their activities while still saving costs. However, we notice that the installation of in-home energy storage does incur fixed purchase costs and recurring maintenance costs and could be expensive for an individual consumer [10]; sharing a large battery by a group of homes in a community or apartments in a building can eliminate the economic deterrents through cost-sharing. In addition, a large scale battery can also provide increased supply to users whose activity patterns do not overlap significantly– each user can share his unused battery capacity with other users or access other users' unused capacity. Practical experiments by ABB and GM in the United States [8] have demonstrated the viability and cost effectiveness for small scale storage to supply up to 3 hours of electricity usage for a group of 2-3 homes. Such

shared storage is inherent to the vision of sustainable microgrids– groups of interconnected loads and distributed energy resources within clearly defined boundaries that act as a single controllable entity with respect to the grid.

However, since the battery is shared among users instead of belonging to a single party, it should be managed by an independent controller on behalf of the commonwealth of all users. Meanwhile, a direct electricity consumption monitoring is not possible and the controller usually relies on a communication network to receive users' reports on their status. Based on the received information, the battery controller decide how much electricity to be stored for each user. Two questions rise naturally in this scenario:

- Competition among users for the limited battery capacity. This is because more capacity can leads additional cost savings. As as a result, users may not be honest about their real demands with the controller. A simple strategy would be exaggerating upcoming electricity demands when price is expected to increase.

- The privacy concerns for reporting accurate detailed energy consumption. As demonstrated in [4], user's in-home activities can be revealed using appliance signatures if detailed energy consumption is known by an adversary.

Therefore, it is essential to understand the competitive behaviors across users with privacy requirement when sharing the battery and be prepared for the possible uncertainty in users' messaging over the communication network.

It is towards the privacy aware management of such a shared battery that this article provides theoretical contributions beside a more comprehensive and complete formulation of the battery sharing problem.

In particular, we propose a game theoretical framework to characterize the messaging behaviors of users with privacy requirements when they share a energy storage and aim to maximize their own cost reductions individually. The corresponding battery management strategies are studied, which are adaptive to time varying demands and prices assuming a zero tolerance for activity delay. With such a framework, we analyze the battery sharing when users are cooperative, privacy aware and completely private. When privacy is not a concern, we show that there always exists a non-stationary social optimal battery control policy – a credit based battery management scheme that ensures game theoretical equilibrium among all players. With this strategy, no user can have any economic incentives by forfeiting electricity demand information to the battery controller. Meanwhile, the battery controller optimizes the social welfare for all users thanks to the complete and accurate information on the whole system.

In this battery sharing system, different users may have different priorities to the shared battery since the purchase and maintenance costs of the battery could be divided unequally across them. Consequently, there exists an achievable cost savings region in which each point corresponds to a simultaneously achievable set of cost-savings for the group of users. Depending on the users' priority, the energy storage sharing system can operate at any point in the region. To characterize such cost savings region, the controller assigns different weights to the users and aims to optimize the social welfare which is a weighted objective.

We note that any shared resource management system requires certain operational policies or axioms that all users and the controller adhere to. However, the objective of every user is to minimize its own electricity cost by choosing an appropriate message to send. In order to capture the potential dishonest messaging behaviors, we do not specify the communication protocols that all users adhere to, but rather make them implicit through the definition of the battery controller and the users' actions and objective. In contrast, based on battery status, electricity price, received messages and other public information including the environment condition, the battery controller decides the amount of electricity to be charged or discharged in battery for each user simultaneously. These quantities are chosen to optimize a weighted sum of the cost-savings across users. By sweeping across all possible weightings, we can characterize an achievable cost savings region.

There are two flavors to time varying pricing in demand response. Time-of-use pricing provides 'on-peak' and 'off-peak' price levels where the price level depends on the time of day and season of the year. These price schedules are determined in advance and don't change frequently. Real-time pricing is more adaptive to market forces wherein the retail electricity price changes hourly or half-hourly and are based on instantaneous prices at the wholesale energy market. To encourage the efficient use of electricity, an increasing number of utilities start to use real time pricing in the retail market to coordinate the customers demand responses to the benefit of individual customers and the overall system. The focus of this work is on investigating the users' competition over battery capacity, the battery control policies and achievable cost savings when certain privacy protection is required under real-time pricing. Mathematically, we formulate the problem as an infinite horizon limiting average stochastic signaling game with privacy constraints and multiple players in a scenario that "net-metering" – where users can sell stored electricity back to the grid for profit– is allowed. But our major results can also be generalized to the scenario where net-metering is not allowed as the they share similar principals.

Through the mathematical analysis, we will show that when privacy is not a concern,

a non-stationary policy, the credit based battery management scheme, always optimizes a weighted sum of user costs – social optimal – and achieves a game theoretical equilibrium. In this policy, users will provide detailed and honest demand information to the battery controller since one user's access to the battery is strictly denied whenever he is found giving an "dishonest" message. Therefore, the battery management is simplified to a centralized control problem which was formulated as an infinite horizon limiting average Markov Decision process. Through the mathematical optimization, we will show that, the optimal centralized battery control yields a policy structure wherein the optimal action of the controller is always independent of current state of the battery, i.e., amounts of energy stored for each user in the battery. We then show that the dynamic policy optimization can be reduced to an integer linear programming solution with largely reduced complexity.

However, the social-optimal battery management, the credit based battery management, require long time established observations and also "coerces" users to share their energy demands accurately with the controller which leads to privacy concerns. We therefore propose a suboptimal privacy preserving battery management strategy in which the message set is restricted to be completely private or partially private. In the special case that the electricity price and users' demands are independent conditioned on the core state, we demonstrate that the completely private battery management strategy relying on only public available information is optimal for the battery management. We also demonstrate the cost effectiveness of battery capacity sharing and the tradeoff between privacy preserving and cost mitigation using privacy preserving battery management strategy with real electricity usage and pricing data.

1.3 Quantitative Risk Assessment of Cyber Attack on DSM

Cyber-enabled DSM relies heavily on real-time, two-way communication capabilities between a central controller and various system elements, including flexible loads. Security and reliability of the cyber infrastructure that enables DSM is therefore critical to ensuring the reliability and safety in such systems.

In the electricity retail market with variable-electricity pricing, the real-time, two-way communication capabilities of Advanced Metering Infrastructures (AMI) enables a utility/load aggregator to collect fine grained usage from consumers and provide electricity pricing schedules to them. In addition, as an existing network infrastructure, it is also being considered as a preferred network access point for other DSM applications including direct load control and distributed energy resource management [11]. The critical role

placed on these embedded devices, AMIs, arises significant security concerns since they are physically attached to users' properties and directly accessible by the users. Large-scale deployments of AMIs encourage the use of marginally cheaper hardware which results in limited computational resources to support advanced security functions such as intrusion monitoring. This also stymies the ability to produce sufficient randomness to create secure cryptographic keys [12]. We also note that the use of public-key-infrastructure (PKI) in AMI network is still rare which naturally raises the problem of key management and potential cyber attacks, such as man-in-the-middle data injection attack.

In Black Hat Europe 2014, researchers Javier Vazquez Vidal and Alberto Garcia Illera demonstrated how they were able to reverse engineer smart meters widely used in Spain, finding blatant vulnerabilities in the hardware [13]. While most smart meters currently installed in Spain used strong symmetric encryption standard AES-128, all AMI units shared the same encryption key which is stored in plain text in the flash memory. In other words, malicious party with access to one AMI device can launch a man-in-the-middle attack and spoof all communication traffic from/to any other smart meters easily. At the same time, the trend of open source tools makes access to AMI hacking tools and tutorials easier than ever. One example is the open source smart meter security test tool, Termineter, released by SecureState on Github [14] which allows users to interact with a smart meter with one of its I\O interface. Though the intention of these tools is to enable authorized users to test the security of AMI and to promote the awareness of AMI security, it nevertheless allows malicious parties from taking advantage of this tool.

Though there is no specific standard on AMI communication networks, mesh network structure has been widely adopted or proposed in industry [15,16]. A mesh network will use each node to relay data and will reconfigure itself if one path is broken. Though it is robust to node failures and easy to scale, the security level of a mesh network can suffer when the network is not well connected [17, 18]. The vulnerabilities of an AMI communication network can be exploited by disabling attacks on the underlying communication infrastructure, insertion of false user requests, unauthorized alteration of DSM schedules and illegal market manipulation; all of which can impact system operations and result in both power shortage and economic losses. If one meter is hacked, not only can its own communication with the utility be altered, but all other communication transmitted through it may also be exposed to manipulation if man-in-the-middle attacks are launched [19].

While the majority of these vulnerabilities can be modelled using false data injection attacks, there are various strategies in system monitoring to detect and identify bad measurements, including nonrandom false data injection attacks [20]. However, it has been

demonstrated that undetectable attacks are still possible if attackers are aware of the system monitoring configuration [21]. We demonstrate that this weakness of traditional system monitoring technology can be exploited for electricity theft through hacked smart meters in AMI relying on mesh networks to communicate between consumers and the utility.

To analyze the topological vulnerabilities of an AMI network against economically motivated stealthy cyber attack, traditional topology analysis or system monitoring technology alone are not sufficient. In this work, a novel risk assessment protocol is proposed to analyze potential targets within existing AMI communication networks that are vulnerable to stealthy, uncoordinated, and economically-motivated cyber attacks. In doing so, we incorporate existing system monitoring technologies. While this protocol can help to assess the potential vulnerabilities of AMI communication network, it also assists to plan a more secure and robust communication network infrastructure. The AMI network designer can utilize the provided warnings and reduce the risk by placing additional AMI data collectors or system monitoring devices. In addition, the study of risk assessment is also a starting point of automated and optimal secure AMI network planning. Case study is provided to demonstrate the process of this method and its effectiveness.

After the quantitative evaluation of the economically motivated AMI hacking, we want to evaluate the potential risk of malicious cyber attacks on the DSM system.

The challenges of the DSM security lie in the feedback mechanism of the load management and the geographically distributed controllable loads and communication resources. Though each load contributes only a small amount of power and its compromising might not cause a noticeable impact on the energy delivery system, a carefully planned cyber attack can spread and impact a wide range of controllable loads. Meanwhile, the attacker can utilize the feedback mechanism of the load management to aggravate its impact and eventually cause overloads on certain critical devices or major power line and jeopardize the energy delivery system.

The key motivation is the fact that constructing an attack-proof DSM communication network is almost impossible and cost ineffective. For instance, the classic method to prevent the man-in-the-middle cyber attack is to treat the communication link as unreliable and to use the public key encryption to conduct key exchange when starting a new communication session between any DSM device and the data collectors. However, key generation is difficult due to the limited randomness that can be produced from an embedded device [12]. In addition, certificate management in PKI which is already an open problem is even harder to guarantee in this context [22]. Even if there is an currently unbreakable security mechanism, it can fail eventually due to the improved hardware and algorithm or

later discovered vulnerabilities. Consequently, the man-in-the-middle attack is very much a realistic possibility in this context. Therefore, we propose a framework to assess the potential risk when part of the distributed system is compromised and detect those vulnerabilities whose compromise can cause a severe impact on the power delivery system. The objective is to help the construction of a more robust and secure communication network for DSM from a topological perspective.

While this framework can help to assess the potential vulnerabilities of DSM communication network, it also assists to plan a more secure and robust communication network infrastructure. The communication network designer can utilize the provided warnings and reduce the risk by placing additional secure communication access points or encryption resources. In addition, the study of risk assessment is also a starting point of automated and optimal secure DSM communication network planning. From another angle, grid operator can also utilize this framework to "patch" those vulnerable link of the power grid bearing in mind that the communication network is not attack proof.

1.4 Outline of The Proposal

The proposal is organized as follows. Chapter 2 presents existing works relating to our research topics. Chapter 3 presents our work on privacy-cost savings tradeoff of an in-home energy storage for a single user in demand response. Next, in Chapter 4, our research regarding the end-user energy storage sharing is presented. Next, Chapter 5, presents our research on quantitative Impact of DSM cyber attack. Finally, we conclude our research and discuss promising future directions in Chapter 6.

2. Related Works

2.1 Utility-Privacy Tradeoff of Energy Storage Management

Different approaches have been proposed to hide the information revealed through smart metering data. When using a trusted escrow service, encryption and data aggregation methods are studied in [23,24]. In the absence of trusted escrow, [25,26] propose "distorting" the data to prevent information retrieval by shifting loads or filtering energy usage data which is limited to the short time scale such as the exact time of switch action. A simple stochastic battery policy using a storage device at home to distort the instantaneous energy consumption while incurring zero delay is studied in [27]. But the fact that eavesdropper can use observations to estimate the past energy consumption is neglected. One recent approach to address the privacy preserving and cost saving tradeoff [28] defines privacy as the "flatness" of power consumption profile and proposes an online control algorithm. We note that "flatness" of a power profile is an indirect measure of privacy and their approach cannot prevent an eavesdropper from successfully inferring a user's electricity profile when the battery control policy is available to the eavesdropper which is a key assumption in this chapter. Entropy as used in this chapter is a direct measure of an observer's uncertainty, using which the primary purpose of this chapter is to characterize the tradeoff between privacy and cost savings. There is another recent work [29] presents the existence of tradeoff between privacy and energy efficiency through energy harvesting and storage wherein a numerical analysis on an i.i.d. binary model is presented.

2.2 Privacy Aware Management of Distributed End-user Energy Storage Sharing

Different approaches have been proposed to provide cost savings through in-home energy storage. The optimal cost saving policies for a single user in-home storage system are studied in [5,6]. In [5], the authors model a system of an energy storage serving a single user with joint Markov price and demand processes and a continuous state space. They show that a threshold policy on the battery level is the optimal. In [6], the authors consider a more complex model of a user with non-controllable renewable energy, an energy selling back mechanism and a convenience utility.

The policies for energy storage sharing using a predetermined time-of-use pricing scheme are studied in [30, 31]. With a finite horizon formulation, an optimal centralized policy is proposed in [30]. In [31], a game theoretic approach is presented with a distributed algorithm to determine each user's energy production and storage a day-ahead. However, counterparts of [30, 31] in real time pricing scheme are still lacking. As the electricity storage control is also stock management, it is related to the newsvendor model problem with dynamic pricing [32]. But this model does not characterize the dynamics of multiple users sharing one energy storage.

In addition to cost savings, an in-home battery can also provide privacy protection of actual demand against smart metering's detailed electricity usage monitoring. A simple stochastic battery policy using a storage device at home to distort the instantaneous energy consumption while incurring zero delay is studied in [27]. But the fact that eavesdropper can use observations to estimate the past energy consumption is neglected. There is another recent work [29] presents the existence of tradeoff between privacy and energy efficiency through energy harvesting and storage wherein a numerical analysis on an i.i.d. binary model is presented.

2.3 Quantitative Risk Assessment of Cyber Attack on DSM

In the context of AMI cyber security, the attacks studied in literature have focused on user privacy risks [33, 34]. In the broader context of demand side management, data injection attacks on a real-time electricity market was first presented in [35] and [36]. The authors in [35] presented the financial risks induced by the malicious attack and proposed a heuristic technique for finding a profitable attack. In [36], the authors introduced a

geometric framework based on which upper and lower bounds on the optimal data attack are obtained.

In [37], smart grid network topology attacks were first studied in which an adversary intercepts network and meter data to mislead the control center with incorrect topology information. The authors studied the condition for the existence of an undetectable attack for strong adversaries who can observe all meter and network data and for weak adversaries with only local information. They showed that with certain connectivity criteria satisfied, undetectable attacks do not exist.

While there are similarities between [37] and our work, there are major differences. [37] studied topology attacks in which the adversary is assumed to be destructive instead of selfish with the objective to mislead the control center with incorrect topology information. In addition, system monitoring constraints have not been considered in [37].

3. Privacy Analysis of Battery Control Mechanisms in Demand Response

DSM systems in the electricity grid, which rely on two way communication between the consumers and utility, require the transmission of instantaneous energy consumption to utilities. Perfect knowledge of a user's power consumption profile by a utility is a violation of privacy and can be detrimental to the successful implementation of demand response systems. It has been shown that an in-home energy storage system (such as a battery/inverter) that provides a viable means to achieve the cost savings of instantaneous electricity pricing without inconvenience can also be used to hide a user's power usage pattern. A fundamental tradeoff exists between the costs saved and the degree of privacy achievable, and in this work, the tradeoff achievable by a finite capacity battery assuming a zero tolerance for activity delay is studied using a Markov process model for user's demands and instantaneous electricity prices. Due to high computational complexity (continuous state-action space) of the stochastic control model, inner and upper bounds are presented on the optimal tradeoff. In particular, a class of battery charging policies based on minimizing "revealing states" is proposed to derive achievable privacy-cost savings tradeoffs. The performance of this algorithm is compared with inner bounds derived using a greedy heuristic and upper bounds derived using an information theoretic rate distortion approach. The framework proposed is shown to be applicable even when users only desire partial information protection such as presence/absence of activity or specific appliances they wish to hide.

3.1 Model

Consider a household consumer with stochastic energy requirements that can be satisfied by direct purchase from the grid or by discharging an in-home battery. A pictorial representation of the energy and information flow is shown in Fig. 3.1. Time and energy

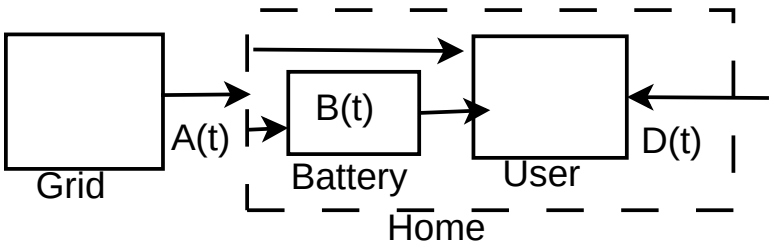

Figure 3.1: A graphical representation of the model

levels are assumed to be discretized. Specifically, let $t = 1, 2, \cdots$ denote the time slots over an infinite horizon. Let $\{D_t \in \mathcal{D}\}, \{P_t \in \mathcal{P}\}, \{B_t \in \mathcal{B}\}$ denote the respective sequences of random variables characterizing user's demand, instantaneous price and battery evolution process with finite supports. The demand and price are modeled using two Markovian processes with initial state D_1, P_1 and transition probability $p^D_{i,j} = \Pr\{D_{t+1} = j | D_t = i\}$, $p^P_{i,j} = \Pr\{P_{t+1} = j | P_t = i\}$ respectively. The battery level is controlled by the given policy as will be explained subsequently. The notation $X_1^t = X_1, ..., X_t$.

Policy: A_t denotes the units of electricity purchased by the user from the grid at time t. The choice of A_t at time t can be random. Privacy necessitates creating uncertainty in instantaneous demands from the eavesdropper's perspective, which can be increased by using probabilistic actions. Let $Q_t = \{q_t(d, b, a, p) = \Pr\{A_t = a | D_t = d, B_t = b, P_t = p\}, \forall b, d, p, a\}$, the probability distribution of purchasing A_t units of power given D_t units of demand and battery level B_t. Let μ_t denote the function that maps all available knowledge at time t to the probability distribution Q_t, and let $\mu = \mu_1, \mu_2, \cdots$ define the policy of the user in determining the level of energy to be purchased.

A simple policy to provide privacy protection is to charge the battery when it is empty and consume energy from the battery as long as it is not drained. This policy aggregates the electricity usage during a period into one short pulse and hides the electricity pattern during the discharging period. Although the intuitive policy provides some uncertainty (during the discharge), it is limited by its determinism and does not adapt to price changes.

From the user's point of view, instantaneous demand, price and battery level are available at time t and consequently the user only has control on the probabilistic electricity purchase action Q_t at the specific state $(b, d, p) \in \mathcal{B} \times \mathcal{D} \times \mathcal{P}$ at time t. However, since the utility is unaware of the demand at time t, an uncertainty exists from the perspective of the utility over the present demand and battery level, and the privacy of the present demand will depend on the complete conditional distribution of action given demand and battery. Consequently, we pose the problem as one of optimizing the entire conditional

distribution $\{\Pr\{A_t|B_t = b, D_t = d, P_t = p\}, p \in \mathcal{P}, d \in \mathcal{D}, b \in \mathcal{B}\}$ as opposed to the point conditional distribution.

Battery evolution: For the remainder of this chapter, the battery efficiency is assumed to be perfect. Battery efficiency depends on the type of battery. We do note that the major type of commercial use battery, Li-ion battery has a charging and discharging efficiency close to 100% [38]. While this model does not completely capture the behavior of all types of batteries in all applications, it does capture the influence of a controllable storage to minimize information leakage through in-out traffic analysis, which is our primary purpose.

We require that all demand must be met immediately from a combination of direct purchase and battery discharging (zero delay inconvenience). So the battery level evolves:

$$B_t = B_{t-1} + A_{t-1} - D_{t-1} \tag{3.1}$$

Utility/Eavesdropper: We assume that anybody interested in compromising a user's privacy can observe A_t, the electricity purchased, and the energy price P_t at time t. The goal of an eavesdropper is to estimate the full history of demands using all observations. We also assume the eavesdropper has perfect information about the strategy used by the controller. Since the strategy is random, the realization of the randomness used by the controller is unavailable to the eavesdropper, and is an important factor in increasing privacy.

Privacy Measure: We quantify the privacy of user energy demand from an external eavesdropper's perspective using conditional entropy:

$$\mathcal{P}(\mu) = \liminf_{t\to\infty} \frac{H(D_1^t|A_1^t, P_1^t)}{t}. \tag{3.2}$$

The conditional entropy for a pair of random vectors $\bar{X}, \bar{Y}$,

$$H(\bar{X}|\bar{Y}) = -\sum_{\bar{x},\bar{y}} \Pr\{\bar{X} = \bar{x}, \bar{Y} = \bar{y}\} \log \Pr\{\bar{X} = \bar{x}|\bar{Y} = \bar{y}\}$$

is an accepted measure of privacy since it quantifies the uncertainty in $\bar{X}$ from the perspective of an observer of $\bar{Y}$, and by virtue of Fano's inequality [39], provides a good lower bound to the observer's probability of error in estimating $\bar{X}$ from $\bar{Y}$. Our entropic measure of privacy is computed based on the complete posterior distribution across time generated by the policy given the set of observations. In other words the privacy defined as above

assumes that an eavesdropper can use all future observations to determine the demand at any time.

Expected Cost Savings: The instantaneous cost savings at time t is $D_tP_t - A_tP_t - C_B(B_{t+1} - B_t)^+$ under the constraint of $B_t \in \mathcal{B}, D_t \in \mathcal{D}, P_t \in \mathcal{P}$, where C_B is the electricity storage cost which reflects the battery purchase cost towards every 1 kWh electricity stored. For mathematical convenience, we express the energy cost at each time slot as a function of the key variables:

$$u(D_t, B_{t+1}, A_t, P_t) = \begin{cases} D_tP_t - A_tP_t - C_B(A_t - D_t)^+, & B_{t+1} \in \mathcal{B} \\ -\infty, & B_{t+1} \notin \mathcal{B} \end{cases}$$

We consider an infinite horizon average cost saving model in this chapter. Many of the reductions presented can be incorporated into finite horizon models as well. The average cost saving per time slot is given by:

$$\mathcal{U}(\mu) = \liminf_{t\to\infty} \frac{\mathbb{E}(\sum_t u(D_t, B_{t+1}, A_t, P_t))}{t}$$

where the expectation is over the realization of the demands and prices, and the probabilistic strategy at each time slot.

Weighted Reward: In order to study the tradeoff between privacy and cost savings, we define a weighted reward:

$$\mathcal{R}(\mu, \lambda) = \lambda\mathcal{P}(\mu) + (1 - \lambda)\mathcal{U}(\mu)$$

For desired weight $\lambda \in [0, 1]$, our objective is to find the optimal weighted reward:

$$J^*(\lambda) = \sup_{\mu}[\lambda\mathcal{P}(\mu) + (1 - \lambda)\mathcal{U}(\mu)]$$

and to design a policy that performs as close to the optimal tradeoff as possible. As long as the cost saving function is bounded, the solution to the weighted reward optimization is the same as the solution to privacy maximization with cost saving constraint (or cost saving maximization with privacy constraint). Sweeping λ from 0 to 1, the tradeoff is characterized. Users, depending on their preferences, can choose any operating point on the tradeoff curve.

3.2 A ρ-POMDP Formulation

The key to reducing the weighted optimization problem to the recursive Bellman equation form is in expressing the *non-causal reward* as a sum of instantaneous rewards, one at each time step. In particular, this requires the instantaneous reward to be causal. While the cost savings, by virtue of definition, is indeed a sum of costs earned at each step, the privacy as defined in the previous section is not directly so. In the subsequent analysis, we express the total privacy in terms of the sum of information leaked in every time step.

3.2.1 Privacy as a Stepwise Additive Metric

Using the chain rules of entropy and joint information [39], the privacy metric can be transformed:

$$H(D^n|A^n, P^n) = H(A^n|D^n, P^n) + H(D^n|P^n) - H(A^n|P^n) \tag{3.3}$$

Since the demand is assumed independent of price (zero delay assumption), we can rewrite $H(D^n|P^n)$ in (3.3) as:

$$H(D^n|P^n) = H(D^n) = \sum_{t=1}^{n} H(D_t|D_{t-1}) = nH_D \tag{3.4}$$

where H_D is the *entropy rate* of the demand process. For any policy μ, the action at time step t is only dependent on the past history up to time t and is necessarily independent of the future demands D_{t+1}^n and prices P_{t+1}^n. Therefore $H(A^n|P^n)$ can be expressed as:

$$H(A^n|P^n) = \sum_{t=1}^{n} H(A_t|A^{t-1}, P^n) = \sum_{t=1}^{n} H(A_t|A^{t-1}, P^t)$$

Similarly, $H(A^n|D^n, P^n)$ can be upper bounded by:

$$H(A^n|D^n, P^n) \leq \sum_{t=1}^{n} H(A_t|A^{t-1}, D_t, B_t, P^t) \tag{3.5}$$

Note that $B_t = \sum_{\tau=1}^{t-1} A_\tau - \sum_{\tau=1}^{t} D_\tau + B_1$, and consequently entropy $H(A^n|D^n, P^n) = \sum_{t=1}^{n} H(A_t|A^{t-1}, D^t, B_t, P^t)$. Inequality (3.5) is due to the fact that conditioning reduces entropy. Further note that if the policy at time t were independent of all past variables

conditioned on B_t, D_t, P^t, A^{t-1}, then the upper bound in (3.5) is achieved. We can therefore restrict ourselves to such Markov policies. Within this reduced class of policies,

we combine (3.4) - (3.5) with (3.3) to get:

$$H(D^n|A^n, P^n) = \sum_{t=1}^{n} [H_D + H(A_t|A^{t-1}, P^t, D_t, B_t) - H(A_t|A^{t-1}, P^t)] \tag{3.6}$$

Consequently, the privacy metric can be expressed as

$$\mathcal{P}(\mu) = \lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} \mathbb{E}(r_p(D_t, B_t, P^t, A^t))$$

where:

$$r_p(D_t, B_t, P^t, A^t) = H_D + H(D_t, B_t|A^t, P^t) - H(D_t, B_t|A^{t-1}, P^{t-1}) \tag{3.7}$$

which is indeed a causal instantaneous reward.

3.2.2 Dynamic Programming

The causal instantaneous reward as expressed in (3.7) is dependent on conditional distributions with dimensions increasing across time (A^{t-1}, P^{t-1}), which can be captured using a *belief vector* that measures the probability distribution of state variables given all past history. Since the instantaneous rewards are causal, the belief at every step can be updated upon new actions and observations. We denote a prior distribution at the beginning of time step t, $\pi_t^{\text{pr}}(d, b) = \Pr\{D_t = d, B_t = b|A^{t-1} = a^{t-1}, P^{t-1} = p^{t-1}\}$, and a posterior probability distribution upon observing A_t, as $\pi_t^{\text{po}}(d, b) = \Pr\{D_t = d, B_t = b|A^t = a^t, P^t = p^t\}$. Accordingly, the entropy term $H(D_t, B_t|A^{t-1}, P^{t-1})$ is then the entropy of the prior distribution and

$$H(D_t, B_t|A^t, P^t) \leq H(D_t, B_t|A_t, P_t, \pi_t^{\text{pr}}) \tag{3.8}$$

is the entropy of the posterior distribution. Note that, as before, the inequality in (3.8) can be achieved by making decisions solely based on present demand, battery, price status and the prior probability distribution π_t^{pr}. Therefore, we restrained ourselves to such strategies, with which present demand, battery, price status are independent of past eavesdropper's observation conditioned on the present observation A_t, P_t and knowledge of the prior probability distribution π_t^{pr}.

Given a policy μ with the constraint that decision making is only based on $D_t, B_t, P_t, \pi_t^{\mathrm{pr}}$, we can rewrite the conditional probability distribution of the amount of energy purchase $Q_t = \{q_t(d,b,a) = \Pr\{A_t = a | D_t = d, B_t = b\}, d \in \mathcal{D}, b \in \mathcal{B}, a \in \mathcal{A}\}$. The evolution of prior and post probability distribution can then be described recursively:

$$\pi_t^{\mathrm{po}|a}(d,b) = \frac{\pi_t^{\mathrm{pr}}(d,b) q_t(d,b,a)}{\sum_{d,b} \pi_t^{\mathrm{pr}}(d,b) q_t(d,b,a)}$$

$$\pi_{t+1}^{\mathrm{pr}}(\bar{d},\bar{b}) = \sum_d \pi_t^{\mathrm{po}|a}(d,b) p_{d,\bar{d}}^D, \text{ where } b = \bar{b} - a + d \tag{3.9}$$

$\bar{d}, \bar{b}$ is an arbitrary pair of demand and battery level at time t. Using the prior probability, we can also acquire the probability distribution of energy purchase A_t, $\gamma_t(a)$, conditioned on the past energy purchase and price history:

$$\gamma_t(a) = Pr\{A_t = a | A^{t-1}, P^t\} = \sum_{d,b} \pi_t^{\mathrm{pr}}(d,b) q_t(d,b,a)$$

The weighted reward at time slot t can then be expressed as:

$$R_\lambda(\pi_t^{\mathrm{pr}}, Q_t) = \lambda \left[H(\pi_t^{\mathrm{po}}) + H_D - H(\pi_t^{\mathrm{pr}})\right] + (1-\lambda)\left[\pi_t^{\mathrm{pr}}(d,b) q_t(d,b,a) u(d,b,a,P_t)\right]$$

Using the technique in [40] (Chapter 6), we can write the Bellman equation for stationary strategies:

$$J^* + \omega(\pi^{\mathrm{pr}}) = \sup_Q \{R_\lambda(\pi^{\mathrm{pr}}, Q) + \sum_a \gamma(a) \omega(\pi^{\mathrm{po},a} Q)\} \tag{3.10}$$

where $\omega(\pi^{\mathrm{pr}}) = \lim_{t\to\infty}[V_t(\pi^{\mathrm{pr}}) - tJ^*]$, and:

$$\frac{V_t(\pi^{\mathrm{pr}})}{t} = \sup_Q \{R_\lambda(\pi^{\mathrm{pr}}, \mathrm{Q}) + \sum_a \gamma_t(a)[V_{t-1}(\pi_t^{\mathrm{po},a}, \mathrm{Q}) - V_t(\pi^{\mathrm{pr}})] + \frac{V_t(\pi^{\mathrm{pr}})}{t}\}$$

If a unique solution to (3.10) exists, then it would be the unique optimal strategy which is stationary. Note that the stationary strategy in this problem is a mapping $\mu : \mathcal{D} \times \mathcal{P} \times \mathcal{B} \times \mathbb{P}(\mathcal{D} \times \mathcal{B}) \mapsto \mathbb{P}(\mathcal{A})$ where $\mathbb{P}(\mathcal{S})$ is the probability simplex over space $\mathcal{S}$. Further, different from classic POMDP, the instantaneous reward here is non-linear and belief dependent due to the entropy function. In general, computing the optimal stationary strategy and finding the solution of the Bellman equation, if it exists, is computationally complex for

continuous state-action spaces. In subsequent sections, we therefore study specific policies to derive achievable inner bounds on the optimal tradeoff and use rate distortion theory to provide outer bounds on the optimal tradeoff. Prior to presenting the bounds, we propose an extension of this framework to study *partial privacy* in the application.

Privacy of Partial Information In some scenarios, a user may not be interested in hiding the complete usage pattern in a home. Partial information such as "whether there is a high power device running" or "whether the house is occupied or empty" alone may be sufficient– privacy has always been a subjective idea. In the subsequent argument we show that the framework described thus far can be adapted to study the privacy of a deterministic function of demands as well.

Assuming the user's requirement is not the protection of the exact demand process D^n but instead the protection of the sequence of functions $\phi(D_1)...\phi(D_t)...$, where

$$\phi : \mathcal{D} \to \Omega$$

where Ω is the space of the partial information of D. Consider a simple example wherein a user wishes to hide his presence or absence. The sequence of indicator functions $\phi(D_t) = \mathbb{1}_{\{D_t>0\}}$ would need to be protected. Similarly, for a given threshold D_{th}, a function $\phi(D_t) = 1$ if $D_t > D_{th}$ and $\phi(D_t) = 0$ if $D_t \leq D_{th}$ can be used to represent the timing sequence of high power demands.

Using similar techniques as in (3.3)-(3.6), we get:

$$\mathcal{P}_\phi(\mu) = \frac{1}{n}\sum_{t=1}^{n}[H_{\phi(D_t)} + H(A_t|A^{t-1}, P^t, \phi^t(D)) - H(A_t|A^{t-1}, P^t)] \tag{3.11}$$

where $H_{\phi(D_t)}$ is the entropy rate of $\phi(D_t)$ process. The average partial information privacy protection of a given policy in a finite time horizon can be numerically calculated by (3.11) while an upper bound can be provided using rate distortion optimization as will be discussed in Section 3.4.2.

Based on the described framework, our key objective is to provide computable solutions that are close to optimal for the general model with multiple levels of battery, price and demand that any practical system can be approximated by. In the subsequent discussion, we first study the greedy algorithm that optimizes the instantaneous tradeoff between privacy protection and cost savings at every step. We then propose a "Battery Centering" policy that aims to exploit the fact that minimum information is revealed when the purchase can

be made probabilistically independent of demand. Upper bounds on the optimal privacy-cost savings tradeoff are then derived using classical rate distortion theory.

3.3 A Greedy Algorithm

An intuitive sub optimal policy is to optimize the instantaneous reward. While the greedy algorithm is not guaranteed to converge, the average reward obtained computationally is expected to do so, and further the optimal policy is easy to calculate for each step as a function of state and belief. The greedy optimal action distribution Q^* for the greedy policy is given by solving at each time step t:

$$Q^* = \arg\sup_{Q}\{\lambda\left[H(\pi_t^{\mathrm{p}o}) + H_D - H(\pi_t^{\mathrm{p}r})\right] + (1-\lambda)\left[\pi_t^{\mathrm{p}r}(d,b)q_t(d,b,a)u(d,b,a,P_t)\right]\}$$

Due to the convexity of the instantaneous reward, the greedy algorithm can be implemented using iterative descent at every step to determine the optimal action and the belief in the subsequent state. It is also possible to extend the greedy algorithm to provide partial information protection. The instantaneous privacy reward in (3.11) can be bounded as:

$$r_{\mathcal{P}_\phi}(\mu) \leq H_{\phi(D_t)} + H(A_t|\pi_t^{\mathrm{p}r,1}, P_t, \phi_t(D)) - H(A_t|\pi_t^{\mathrm{p}r,2}, P_t)$$

$$\text{where } \pi_t^{\mathrm{p}r,1} = \Pr\{D_t, B_t|A^{t-1}, P^{t-1}, \phi^t(D)\}$$
$$\pi_t^{\mathrm{p}r,2} = \Pr\{D_t, B_t|A^{t-1}, P^{t-1}\}$$

as conditioning reduces entropy. The bound can be achieved by constraining A_t to be independent of all past variables conditioned on $B_t, D_t, \pi_t^{\mathrm{p}r,1}, \pi_t^{\mathrm{p}r,2}, P_t, \phi(D_t)$. We therefore restrict ourselves to such policies. Therefore, the greedy optimal action distribution Q^*_{greedy} for the partial information protection and cost savings is given by solving:

$$\begin{aligned} Q^*_{greedy} = &\arg\sup_{Q}\{(1-\lambda)\left[\pi_t^{\mathrm{p}r}(d,b)q_t(d,b,a)u(d,b,a,P_t)\right] \\ &+ \lambda\left[H(A_t|\pi_t^{\mathrm{p}r,1}, P_t, \phi_t(D)) + H_D - H(A_t|\pi_t^{\mathrm{p}r,2}, P_t)\right]\} \end{aligned}$$

The greedy algorithm is a natural heuristic to avoid a global optimization over the whole time horizon. In order to design a better algorithm that can balance the current reward and future rewards, we propose a method that aims to create long term uncertainty in the demand process by decoupling the probabilistic actions from the recurring demand to the extent possible. Our numerical comparisons will demonstrate that the performance of this strategy is much closer to the maximum possible in comparison with the greedy algorithm.

3.4 A "Revealing State" Approach

In the entropy based stochastic control problem described in previous sections, the battery and demand process are estimated jointly using the electricity purchase along the complete time horizon. Note that if the battery level is at a medium level, the purchase action Q_t need not be constrained by either battery or demand. This is a desirable situation where the system state can be hidden, and a good policy would let this situation persist as long as possible. In contrast, if the battery reaches its maximum or minimum level, the electricity purchase action Q_t is severely constrained by the battery evolution (3.1) and the resulting battery state estimation by the eavesdropper/utility will have high accuracy. Such a situation reveals the state of the system to the eavesdropper and is expectedly undesirable from a privacy perspective. This idea forms the motivation for the "battery centering" policy described heretofore.

In the battery centering strategy, we classify the system state into three stages $S(t) \in \{0, 1, 2\}$. Assuming that battery starts from a medium level b_0 in stage 0, the electricity purchase action is made according to a probability distribution (3.12) which is independent of battery level and demand until the battery reaches its maximum or minimum.

$$\pi_a^A(p) = \Pr\{a_t = a | P_t = p, p \in \mathcal{P}\} \tag{3.12}$$

The system transfers to stage 1 if the battery reaches maximum or to stage 2 if the battery reaches minimum. When the system is in stage 1 or 2, the electricity purchase is respectively large enough or small enough so that the battery level can traverse back to the medium point b_0 to go back to stage 0 again. We refer to the time duration between the system entering and leaving a stage as the *staying time* $T_{stay}(t) = \max\{t_2 - t_1 | S(k) = S(t) \text{ if } k, t \in [t_1, t_2)\}$.

At any time step t, we define the process to be in a *hiding state* if the purchase A_t

Algorithm 1 "Battery Centering" Strategies

procedure BATTERY STORAGE B_t MAINTAINING
    Initialization $B_0 = b_0$
    System state $\leftarrow$ Stage 0
    while System state == Stage 0 **do**
        generate a_t according to distribution $\pi_a^A(p)$
        if $B_t + a_t - D_t \in \mathcal{B}$ **then**
            purchase $A_t \leftarrow a_t$
            System state $\leftarrow$ Stage 0
        else if $B_t + a_t - D_t > B_{\max}$ **then**
            purchase $A_t \leftarrow B_{\max} - B_t + D_t$
            System state $\leftarrow$ Stage 1
        else
            purchase $A_t \leftarrow B_{\min} - B_t + D_t$
            System state $\leftarrow$ Stage 2
    while System state == Stage 1 **do**
        if $B_t - D_t \geq b_0$ **then**
            purchase $A_t \leftarrow 0$
            System state $\leftarrow$ Stage 1
        else
            purchase $A_t \leftarrow b_0 - B_t + D_t$
            System state $\leftarrow$ Stage 0
    while System state == Stage 2 **do**
        if $B_t + D_{\max} - D_t \leq b_0$ **then**
            purchase $A_t \leftarrow D_{\max}$
            System state $\leftarrow$ Stage 2
        else
            purchase $A_t \leftarrow b_0 - B_t + D_t$
            System state $\leftarrow$ Stage 0

is independent of battery level B_t and demand D_t. For the Battery Centering policy, as long as the stage of the battery remains fixed, the system remains in a hiding state. A *revealing state* is defined to have occurred at time t if A_t is deterministically related to B_t and D_t. For the Battery Centering policy, the system reaches a revealing state only when the stage of the battery changes. As an example, when the system moves from stage 0 to stage 1, $A_t = B_{\max} - B_t + D_t$ is a deterministic function of B_t and D_t. The resulting battery state is fully revealed and it is a revealing state. For the Battery Centering policy, the system remains in a hiding state until the battery stage changes at which point the system hits a revealing state for one time step before reverting back to a hiding state. Therefore, reducing the frequency of one will increase the frequency of the other. Our goal is to therefore optimize the parameters of the policy so that the frequency of occurrence of the revealing states is minimized. When the battery is in stage 1 or 2, this can be accomplished by setting the purchase speed to 0 or $D_{\max}$ respectively.

Although the proposed algorithm can be used for any demand and price evolution model, the analytical optimization of the parameters of the algorithm is facilitated when the underlying model is i.i.d.. In the following, we assume i.i.d. underlying models and present the mathematical background to maximize the staying time $T_{stay}(t)$ of stage 0 in the system for this class of policies.

Lemma 1. *The battery level evolution in every stage of Algorithm 1 is equivalent to a bounded random walk process:*
Stage 0: $B_{t+1} = B_1 + X_1^0 + ... + X_t^0$, *with* $\Pr(X_t^0 = x) = \sum_{a,d,p|a-d=x}[\pi_a^A(p) p_d^D p_p^P]$
Stage 1: $B_{t+1} = B_1 + X_1^1 + ... + X_t^1$, *with* $\Pr(X_t^1 = x) = p_{-x}^D$
Stage 2: $B_{t+1} = B_1 + X_1^2 + ... + X_t^2$, *with* $\Pr(X_t^2 = x) = p_{D_{\max}-x}^D$

Proof: This lemma follows if we treat the difference of battery level in every time slot as the random step. As X_t^i, $i = 0, 1, 2$ are i.i.d. in each stage and their sums $\sum_{\tau=t_0}^{t} X_\tau^i + B_{t_0}$ are typical random walks. ■

Theorem 2. *For battery centering strategies described in Algorithm 1, if* $\mathbb{E}\, a = \sum_{a\in\mathcal{A}, i\in\mathcal{P}} a\pi_a^A(i) p_i^P \neq \mathbb{E}\, D$ *then* $\mathbb{E}\,|B_t - b_0| = O(t)$. *If* $\mathbb{E}\, a = \mathbb{E}\, D$ *then* $\mathbb{E}\,|B_t - b_0| = O(\sqrt{t})$.

Proof: Lemma 1 ensures that the movement of the states can be modeled as a random walk. According to the result in Chapter 2, [41], the distance between a random walk at time t and the original position at time 0 is $O(t)$ if it is a biased walk or $O(\sqrt{t})$ if it is an unbiased walk. For a random walk with step $X_t^0 = a_t - D_t$, $\mathbb{E}\,|B_t - b_0| = O(t)$ if $\mathbb{E}\, X_t^0 \neq 0$; $\mathbb{E}\,|B_t - b_0| = O(\sqrt{t})$ if $\mathbb{E}\, X_t^0 = 0$. As the electricity purchase amount is fixed at 0 and $D_{\max}$

in stage 1 and 2 respectively in Algorithm 1, the expected staying time is fixed. Therefore, in order to reduce the frequency of "revealing" state, we design $\pi_a^A(p)$ in such a way that $\mathbb{E}\, a = \mathbb{E}\, D$. ■

In addition, as the equivalent random walk in stage 0 is unbiased, we want to maximize $\min\{|B_{\max} - b_0|, |B_{\min} - b_0|\}$ to increase the staying time in stage 0 which results in $b_0 = \frac{1}{2}(B_{\max} + B_{\min})$.

Theorem 3. *For battery centering strategies described in Algorithm 1, the frequency of revealing state increases with σ_a.*

Proof: Following Lemma 1, the battery level process in stage 0 is equivalent to a random walk process with step move $X_t^0 = a_t - D_t$. Therefore, we have an estimation of battery level at time t: $\Pr(B_t - b_0 = k) \simeq \{2\pi\sigma^2_{X_0^0} t\}^{-0.5} \exp\{-\frac{k^2}{2\pi\sigma^2_{X_0^0} t}\}$ according to Central Limit Theorem [41]. Noticing that a_t is independent of D_t, which leads to $\sigma^2_{X_t^0} = \sigma^2_{a_t} + \sigma^2_{D_t}$. With these argument, we can notice that the increase of σ_a will lead the increase of $\Pr(B_t - b_0 \geq B_{\max} - b_0$ or $B_t - b_0 \leq B_{\min} - b_0)$. Theorem 3 then follows. ■

The above theorem proves that reducing the variance of X_t^0 will increase the time spent at stage 0. Therefore, minimizing $\sigma_{X_t^0} = \sigma_{a_t}$ can minimize the frequency of system traversing from one stage to another and consequently the frequency with which a system state is revealed to the eavesdropper. Such an approach would work very well if cost savings were not a consideration. In order to trade cost savings for privacy, the electricity purchase needs to depend on the price, which would in turn increase σ_{a_t}. Optimizing the tradeoff between privacy and cost savings is equivalent to optimizing the privacy protection with different minimum cost savings constraint. Using theorems 2 and 3, the optimization of privacy with cost savings constraint using the battery centering strategies can be solved by linear programming (see (3.13)) to minimize σ_a given equality constraint $\mathbb{E}\, a = \mathbb{E}\, D$ and inequality constraint $\mathbb{E}\, ap \leq s$, where s sweeps from $\mathbb{E}\, D P_{\min}$ to $\mathbb{E}\, D\, \mathbb{E}\, P$.

$$\begin{aligned} &\text{minimize} \sum_{a\in\mathcal{A}, i\in\mathcal{P}} (a - \mathbb{E}\, D)^2 \pi_a^A(i) p_i^P \\ &\text{subject to} \sum_{a\in\mathcal{A}, i\in\mathcal{P}} a\pi_a^A(i) p_i^P = \mathbb{E}\, D, \sum_{a\in\mathcal{A}, i\in\mathcal{P}} ap\pi_a^A(i) p_i^P \leq s \end{aligned} \tag{3.13}$$

The proposed battery centering algorithm is an easily stated policy and can be implemented in practice by keeping track of the battery "stage" while the determination of

electricity purchase A_t is either generated according to a predetermined probability distribution or the result of a simple computation.

3.4.1 Analysis of "Battery Centering" Strategy

When implementing Algorithm 1 on a system with multiple albeit finite levels of battery state, demand and price, π_t^{pr} follows a positive recurrent Markov Chain with countable states. It is easily verified that revealing states are indeed *positive recurrent states*. Based on this fact, we can calculate the expected privacy and cost savings of strategy Algorithm 1 numerically. Under i.i.d. assumptions, we can also calculate the expected privacy and cost savings analytically for the battery centering strategy with given parameters using random walk theory as follows.

Step 1 Calculate the expected step privacy of every stage. Denote the time between two revealing state as η^i. By the definition of expected step privacy in each stage, the law of conditional entropy and the facts that η^i is totally dependent on D^n and demand is i.i.d.. We have:

$$\mathbb{E}\, r_P^i = H_D - \frac{\mathbb{E}\, H(\eta^i)}{\mathbb{E}\, \eta^i}$$

Step 2 The expected privacy of the complete time horizon

$$\mathbb{E}\, r_P = H_D - \frac{2\,\mathbb{E}\, H(\eta^0) + \mathbb{E}\, H(\eta^1) + \mathbb{E}\, H(\eta^2)}{2\,\mathbb{E}\, \eta^0 + \mathbb{E}\, \eta^1 + \mathbb{E}\, \eta^2} \tag{3.14}$$

Equation (3.14) is due to the fact that random walk of stage 0 is unbiased and will end in stage 1 or 2 with equal likelihood while stage 1 and stage 2 will always end in stage 0.

Step 3 The expected cost savings:

$$\mathbb{E}\, r_S = \frac{2\,\mathbb{E}\, \eta^0 [\sum_{p\in\mathcal{P}, d\in\mathcal{D}} \pi_P(p)\pi_D(d) - \sum_{p\in\mathcal{P}} f_a(p) p \pi_P(p)]}{2\,\mathbb{E}\, \eta^0 + \mathbb{E}\, \eta^1 + \mathbb{E}\, \eta^2}$$

where $\mathbb{E}\, r_S$ is the expected cost savings over the complete time horizon. It is known that the accurate analysis of η for general step distribution is an open problem [41].

3.4.2 Upper Bound

In order to evaluate the closeness to optimality of the proposed battery centering strategies, we provide an upper bound by considering a weak eavesdropper who does not

update his belief. We appeal to the fact that conditioning reduces entropy [39] to limit the information used by the eavesdropper. Specifically, removing the conditioning variables that the eavesdropper uses to determine the state can increase the entropy achievable without compromising the costs. Indeed, if we assume the eavesdropper only uses observations of m previous steps, then the maximum privacy achievable against such an eavesdropper will be an upper bound on that achievable by any policy against the original eavesdropper (3.2).

$$\mathcal{P}(\mu) \leq \sup_{P_{A_1^m|D_1^m}(a_1^m|d_1^m)} \frac{H(D_1^m|A_1^m, P_1^m)}{m}$$

Under this model, the resulting system is an $m-$horizon problem and we make one more additional assumption that the entire $m-$horizon demand and price realization is available to the controller at the time of optimization (non-causality). The optimal weighted reward achievable by a non-causal controller against a weakened eavesdropper will provide a strict upper bound on any tradeoff achievable for the original problem. Under these assumptions, this problem is a variant of classical rate distortion minimization [39].

$$\begin{aligned}\mathcal{R}(\mu, \lambda) \leq & \frac{1}{m}[\lambda H(D_1^m) + (1-\lambda)(\sum_{t=1}^{m} D_t P_t + B_m) \\ & - \min_{P_{A_1^m|D_1^m}(a_1^m|d_1^m)} (\lambda I(A_1^m; D_1^m|P_1^m) + (1-\lambda)\sum_{t=1}^{m} A_t P_t + C_B(A_t - D_t)^+)] \end{aligned} \quad (3.15)$$

where $\min I(A_1^m; D_1^m|P_1^m)$ is the minimum mutual information rate between D_1^m and A_1^m given the constraint posed by battery evolution which are easily computed using standard convex optimization techniques. The generalized Blahut-Arimoto algorithm provided in [42] provides an efficient computational technique to obtain the upper bound in (3.15). The upper bound thus derived forms a *fundamental limit* to the privacy-cost savings tradeoff.

3.5 A Numerical Example

In this section, we validate our theoretical results through numerical simulations using real electricity usage and pricing data to demonstrate that the battery centering algorithm optimized by the revealing state approach works well in practice. Specifically we use the electricity usage data of a home [43] and the time-of-use pricing data published by NY ISO [44]. The electricity usage is discretized into 20 levels and price is discretized into 10 levels. We assume that an electricity storage is available to provide both privacy protection

and cost savings. Both the system and eavesdropper treat the demand process D_t and price process P_t as i.i.d.. Fig. 3.2 presents the activity of the energy storage system with capacity of 2 kWh and \$ 0.02 per kWh energy storage cost using the battery centering algorithm and the greedy algorithm. As it is a relatively small electricity consumer with a peak power consumption of only 1.5 kW, a battery with 2 kWh is reasonable in this case. With battery centering algorithm, the privacy was well protected as the battery level touched its limit only twice and revealing states occurred on an average about 4 times in a total 48 hours. The privacy $\mathcal{P}/H_D = 0.992$ while the cost is reduced by 15.87%. However, with the same cost savings requirement, the greedy algorithm performed much worse, $\mathcal{P}/H_D = 0.857$.

The privacy-cost savings tradeoff of battery centering algorithm is presented in Fig. 3.3 when battery capacity is 0.5, 1, 2 kWh. We only plot privacy-cost savings tradeoff of greedy algorithm when battery capacity is 2 kWh. The upper bound is calculated using a 4-step horizon rate distortion computation. The presented results demonstrate the closeness in performance of the battery centering policy to the fundamental limit in real cases. Furthermore, even when utilized with a cost savings first requirement, the policy provides substantial privacy. We also plot the point of cost savings optimal algorithm in [5] in Fig. 3.3 as a comparison. The proposed algorithm is shown to provide substantial privacy protection with very little savings reduction.

We also investigated partial information leakage where the partial information function $\phi(D_t)$ is defined as:

$$\phi(D_t) = \begin{cases} 0 \text{ if } D_t < 200W \\ 1 \text{ if } 200W \leq D_t \leq 1000W \\ 2 \text{ if } D_t > 1000W \end{cases} \tag{3.16}$$

Fig. 3.4 presents the partial information protection and cost savings tradeoff of the greedy algorithm and battery centering algorithm when the battery capacity is 0.5, 2, 4 kWh based on numerical computation method of partial information protection described in (3.11). Upper bound is provided by the rate distortion technique. It shows that the performance of our proposed battery centering algorithm can provide slightly better partial information protection compared to the greedy algorithm and both algorithms can provide good partial information protection with large capacity battery. The relatively worse performance when battery capacity is limited is due to the fact that the battery centering algorithm is not explicitly designed to treat demand levels differently, and the rate distortion upper bound exacerbates the eavesdroppers weak prior information.

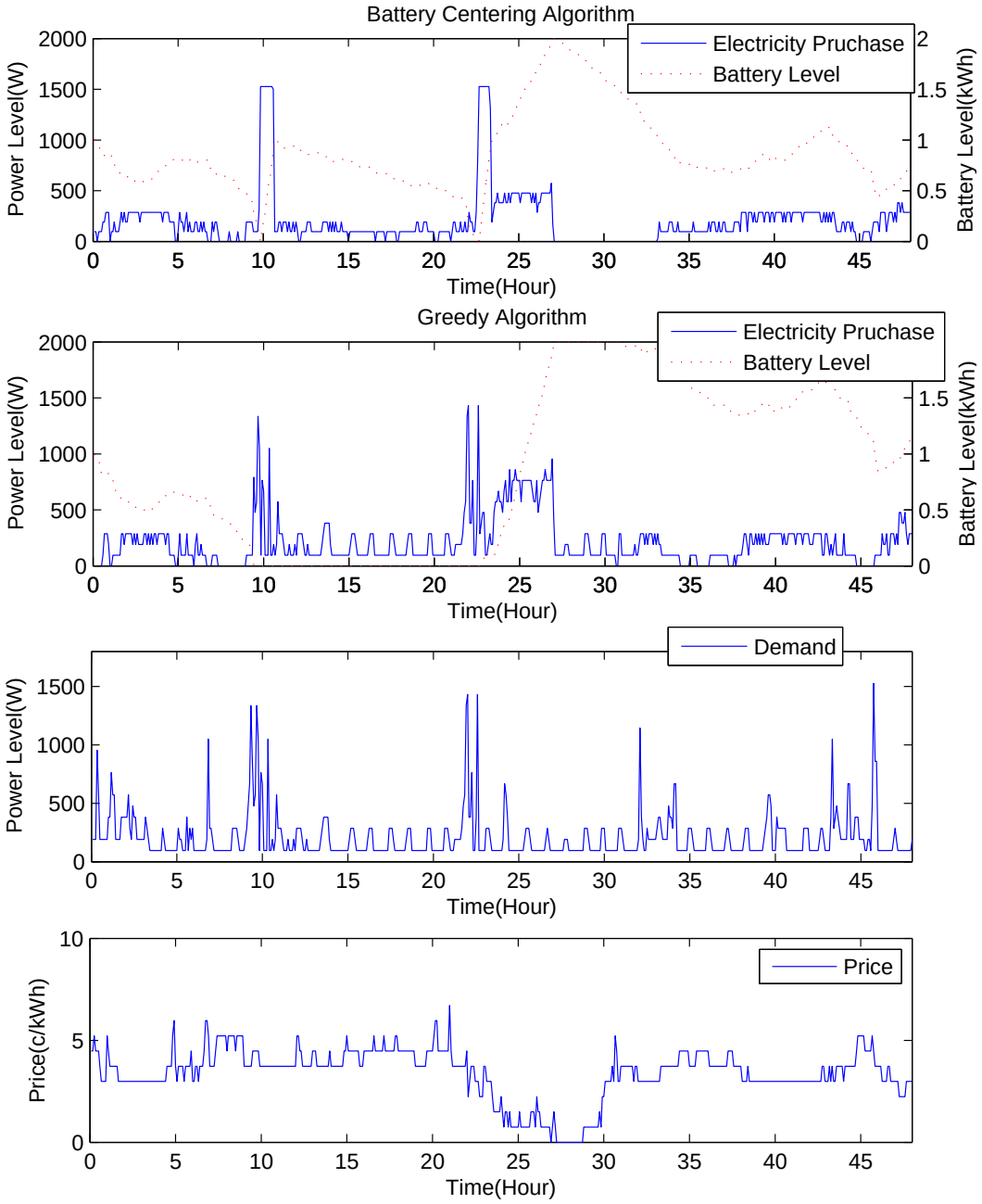

Figure 3.2: The system activity with an energy storage of 2 kWh

3.6 Summary

Although the policy that solves the optimal tradeoff between privacy and cost savings remains an open problem, we believe that our bounds using the revealing state approach are quite close. While an in home battery provides an individual with the opportunity to make

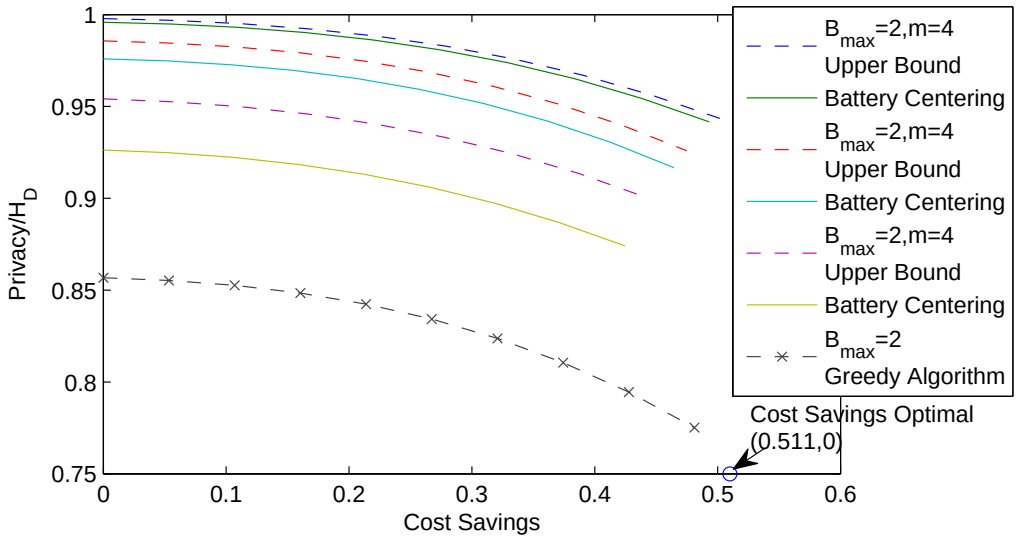

Figure 3.3: Privacy-cost savings for a real system

a choice about an operating point on the price-privacy curve, we believe that aggregation of demand with larger batteries would be an interesting new dimension to explore, particularly with the possibility of users have differing requirements and shared resources. Operating costs are an important consideration for the mechanism proposed in this chapter. While the key mathematical contributions in this chapter do not consider operating costs, the framework does not preclude such costs per se. For instance, a marginal amount can be added to the purchase price when charging the battery, and a marginal cost incurred every time the battery is discharged. The policy simulated with these inclusions would provide a tradeoff that is closer to practice.

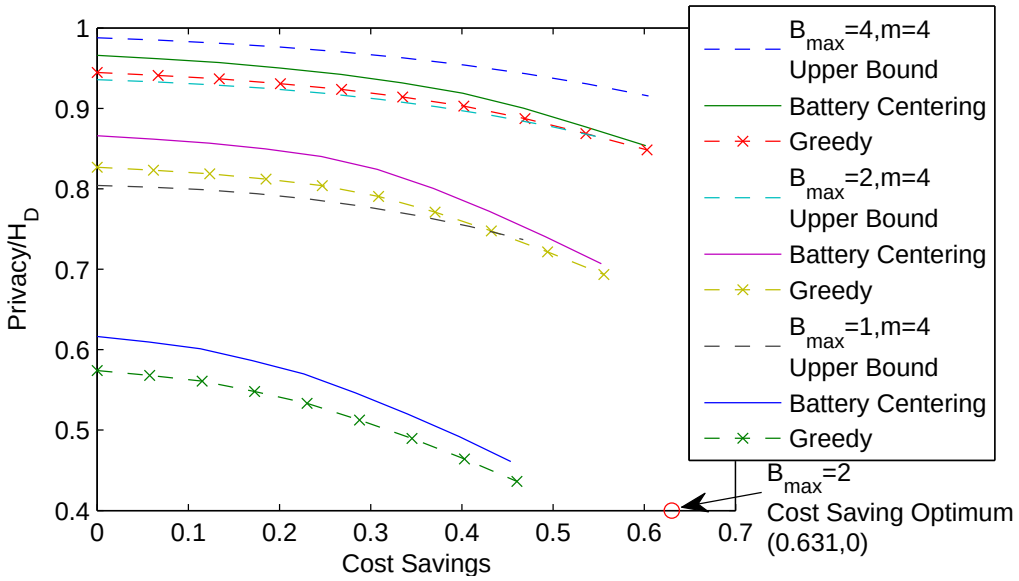

Figure 3.4: Partial information protection - Cost savings for a real system

4. Privacy Aware Management of Distributed End-user Energy Storage Sharing

Deregulated electricity markets with time varying electricity prices and opportunities for consumer cost mitigation makes energy storage such as a battery an attractive proposition. Sharing a large capacity battery across a group of homes in a community, can not only alleviate the economic deterrents but also exploit the fact that users' activity patterns do not necessarily overlap. However, battery sharing induces competition for battery capacity between the users in general as they may want to maximize their own cost savings by occupying more battery capacity when the electricity price is low. Importantly, users might have privacy concerns when they communicate with the shared battery controller. The privacy aware management of such a shared battery is the focus of this work. A game theoretical framework was proposed to capture the competitive behaviors of users sending messages through a communication network to an independent battery controller with an infinite horizon limiting average signaling game formulation. The privacy requirement serves as a constraint on messaging behaviors. The battery controller manages the charging and discharging based on the received, albeit incomplete, information transmission. With such a framework, we study the battery sharing when users are cooperative and completely private. When the privacy requirement is relaxed, the competitive behaviors of users sending messages to the battery controller is studied. A credit based battery management strategy is designed for the battery controller to ensure an equilibrium of the game and achieves the social optimality. However, the credit based battery management requires long time established observations and may also "coerce" users to share their energy demands accurately with the controller. We therefore, propose, a class of stationary suboptimal privacy preserving battery management strategy in which the message set being restricted to be completely private or partially private. In addition, we demonstrate that by changing the size of the message set, different pairs of preserved privacy and cost savings can be achieved. Through

numerical simulations on real electricity pricing and usage data, we demonstrate the cost effectiveness of battery capacity sharing and the tradeoff between privacy preserving and cost mitigation using privacy preserving battery management strategy.

4.1 System Model and Stochastic Game Formulation

4.1.1 Operational Model

In this work, we consider the management of an energy storage system shared by n household as demonstrated in Fig. 4.1. As the electricity price is changing in real time, users want to take advantage of the energy storage system to cut their energy cost. Without any sacrifice of the convenience, a user's energy demand must be satisfied instantaneously from the combination of real time purchase from the grid and battery discharging. However, as a shared property, such energy storage is installed independent of any users. Therefore, instead of controlling the energy storage directly, the users rely on an independent battery controller to manage the storage on behalf of the commonwealth of users. At every time step, the battery controller decides the electricity storage level maintained for each user, then purchase or sell back electricity on behalf of each user to achieve the designated storage level. We make two assumptions on the electricity sell back mechanism:

- Although energy is stored in the battery separately for each user, the stored energy can be traded among users.
- The stored electricity can be sold back to the grid – a policy referred to as net metering which is widely permitted in the US.

For simplicity and fairness, we assume the electricity trading price is identical to the price from the grid at the time of trading.

The controller relies on not only battery state and pricing information to make the optimal battery management decision, but also the real time energy demands of users. Since the shared battery is installed separately from the users, monitoring their demands directly is not realistic. With a more feasible formulation, the battery controller communicates with the users via data links as shown in Fig. 4.1. Ideally, the users notify the controller the actual energy demands so that the social optimality is achieved. However, the messages from the users may not be complete or honest for two reasons:

- To occupy more battery capacity when electricity price is low to gain unfair amount of cost savings. For instance, when the battery controller trusts all users, a user

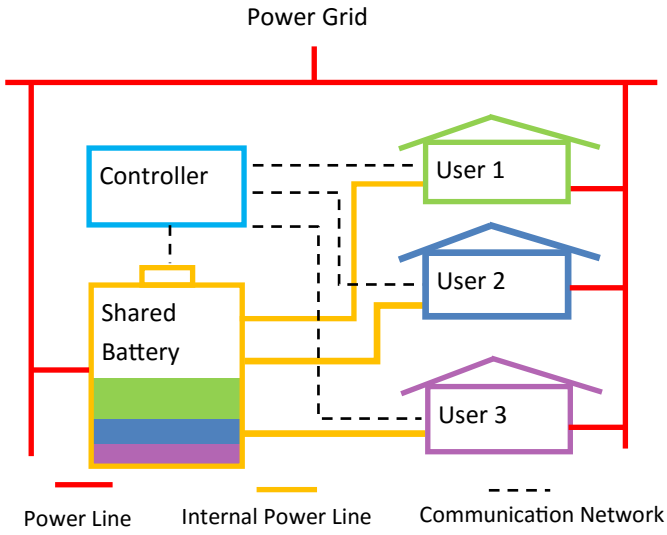

Figure 4.1: A battery sharing system with multiple users and the directional energy flow

can occupy more capacity by reporting a fake demand or internal state so that the controller believes that its demand will increase rapidly in the near future.

- To hide the actual electricity consumption from the battery controller for privacy concerns. As demonstrated in [4], user's in-home activities can be analyzed using appliance signatures.

Therefore, we don't make any assumptions on the messages transmitted from the users to the battery controllers. The messages can carry no information in the "blind" battery management strategy as shown in Section 4.3.3. The messages can also be equivalent to the actual energy demands in the cooperative battery management as shown in Section 4.3.1. The use of the messages depends on the strategy and privacy preference of the user.

Our approach in this work is to build a stochastic game theoretical framework to understand equilibrium policies for the users and controller. Privacy preserving battery management can be realized by constraining the message set to be partially private. When the privacy is not a concern, the social optimal cost savings can be achieved with a carefully designed battery management strategy which ensures the equilibrium of the battery sharing game.

4.1.2 The Stochastic Game Model

The game theoretical model for n users with a shared battery is formulated as below where time and energy level are assumed to be discrete. Let $t = 1, 2, ...$ denote the time

slots over an infinite horizon.

Core State: Based on a common setup in [6, 7, 30], we use a core state $\omega_t \in \Omega$ to describe the environmental state including the weather, the temperature, the time of the day and etc. Users' energy demands and electricity price are partially determined by the core state ω_t, which is a Markovian process with initial state ω_0 and the transition probability $P_\Omega(\omega, \omega') = \Pr(\omega_{t+1} = \omega' | \omega_t = \omega)$.

Electricity Price: We use $P_t \in \mathcal{P}$ to denote the sequence of random variables characterizing the instantaneous electricity price with finite supports:

$$P_t = \gamma_P(\omega_t) + \delta_t^P$$

The price contains two components in which, $\gamma_P(\omega_t)$ is the environment dependent component of electricity price and δ_t^P is the independent unforeseeable component. $\gamma_P(\cdot)$ is a function describing the predictable power generation under given environment and its resulting electricity price. $\delta_t^P \in \Delta^P$ is a Markovian process with initial state δ_0^P and transition probability $P_{\Delta^P}(\delta^P, \delta^{P\prime}) = \Pr(\delta_{t+1}^P = \delta^{P\prime} | \delta_t^P = \delta^P)$.

We assume that electricity price P_t is a public information available to both users and the battery controller.

Users: In this work, we consider n users whose energy demands also contain the environment dependent component and the independent unforeseeable additives:

$$D_t^i = \gamma_i(\omega_t) + \delta_t^i, \forall i = 1, ..., n$$

where $\gamma_i(\cdot)$ is the function describing the user's environment deciding energy demand. $\delta_t^i \in \Delta^i$ is the unforeseeable component of demand which follows a Markovian process with initial state δ_0^i and transition probability $P_{\Delta^i}(\delta^i, \delta^{i\prime}) = \Pr(\delta_{t+1}^i = \delta^{i\prime} | \delta_t^i = \delta^i)$. We define $\boldsymbol{\delta}_t = \{\delta_t^1, \cdots, \delta_t^n, \delta_t^P\}$ to characterize the system condition at time t.

Though the demand D_t^i is private information only accessible by the user i itself, its statistical properties γ_i and $\mathbf{P}_{\Delta^i}$ are assumed to be known by the battery controller.

All Markovian processes $\omega_t, \delta_t^i, \forall i$ discussed in this work are assumed to be aperiodic and irreducible.

Battery: In order to alleviate the cost burden when taking advantage of the time varying prices, the users share a battery with limited capacity. For the sake of analytical convenience, we assume that the possible levels of storage in the battery have finite support $\mathcal{B}$. B_t^i denotes the energy storage level for user i at time t which is a private information

only shared between the battery controller and user i. We have no additional constraints on B_t^i except $B_t^i \in \mathcal{B}$ and $\sum_{i=1}^n B_t^i \in \mathcal{B}$ since the storage capacity can be shared among users. $\mathbf{B}_t = \{B_t^1, \cdots, B_t^n\}$ is referred to as the state of the battery at time t.

The battery efficiency is assumed to be perfect. Although battery efficiency can vary depending on the type of battery, we do note that the major type of commercial use battery, Li-ion battery has a charging and discharging efficiency close to 100% [38]. We don't put constraint on the battery charging and discharging speed since common residential circuit capacity permits the full charging and discharging of a typical capacity energy storage in an hourly base.

Battery Controller: Since the battery is a shared property, it is managed by an independent controller on behalf of the common wealth of the users. The controller decides the energy storage level to be maintained for each user B_{t+1}^i. To distinguish the difference between the battery management action and energy storage level, we use $\beta_t^i = B_{t+1}^i$ to denote the decision of the battery controller for user i. $\boldsymbol{\beta_t} = \{\beta_t^1, \cdots, \beta_t^n\}$ is referred to as the overall action of the battery controller.

To optimally manage the battery, the controller relies on public information – core state ω_t and electricity price P_t – and the private messages sent by individual users. While this is a more realistic assumption, it enables the users to compete for maximum cost reduction and arises the concern of privacy leakage through the message transmission.

Electricity Cost: As we stated in Section 4.1.A, the electricity price is unified as P_t for electricity purchase from the grid, electricity sell back and in-battery energy trading at time t. Therefore the electricity cost for user i at time t would be U_t^i and is determined by:

$$U_t^i = u(D_t^i, P_t, B_t^i, B_{t+1}^i) = P_t(D_t^i + B_{t+1}^i - B_t^i) \tag{4.1}$$

Privacy Aware Messaging: To communicate with the battery controller, users send private messages M_t^i over the communication network which are only observable by transmitters and the receiver. To reflect different possibilities of users' messaging behavior, we don't make assumptions on the message M_t^i except that the message set $\mathcal{M}^i$ should be finite and discrete. Two basic types of messaging behaviors have been studied in Section 4.3: Complete honest messaging and zero information messaging.

When the users actively choose the messaging strategy instead of following a prefixed protocol, they can be competitive for the battery capacity or reluctant to reveal enough information for privacy concern. If the electricity cost is the top concern of users, we show that there exists an equilibrium where users are coerced to be honest and comprehensive on

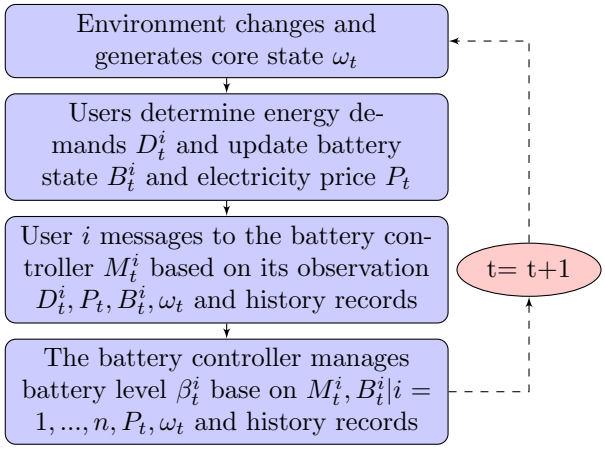

Figure 4.2: The decision making process

D_t^i or δ_t^i, and the battery controller is actively monitoring the messages M_t^i for credibility.

When the users and the battery controller have an agreement on the privacy concern, a class of partially private messaging strategies can be used, where $|\mathcal{M}^i| < |\Delta^i|$. For example, $\mathcal{M}^i = \{High, Low\}$. In this setup, a message M_t^i only delivers an ambiguous information of D_t^i and δ^i. We also present the optimal battery management assuming the message set $\mathcal{M}^i$ are restricted to be partially private $|\mathcal{M}^i| < |\Delta^i|$ and certain messaging strategies of users are being acknowledged and accepted between the controller and the user. Performance comparison is presented among different privacy preserved messaging setups.

Strategies: The order of decision making in each time slot is illustrated in the flowchart shown in Fig. 4.2. In each time slot, the battery controller first collects messages from users and then make the battery management decision. In this work, we don't constrain ourselves to pure strategies or stationary strategies.

We let $\mu_t^i(\omega_0, P_0, B_0^i, \delta_0^i, ..., \omega_t, P_t, B_t^i, \delta_t^i)$ denote the function that maps all available knowledge of user i at time t to the messaging action M_t^i, and let $\mu^i = \mu_0^i, \mu_1^i, ...$ denote the dynamic strategy of the user i. The available knowledge includes public information: core state ω_t, pricing P_t, its own private states: independent demand component δ_t^i, electricity demand D_t^i, battery storage B_t^i and history records.

On the other hand, the battery controller manages the battery storage for each user but only has access to public information ω_t, P_t, the messages sent by the users $\boldsymbol{M}_t = \{M_t^i | i = 1, ..., n\}$, battery state $\mathbf{B}_t$ and history records. We let $\mu^C = \mu_0^C, \mu_1^C, ...$ denote the dynamic strategy of the controller where $\mu_t^C(\omega_0, P_0, \mathbf{B}_0, \boldsymbol{M}_0, ..., \omega_t, P_t, \mathbf{B}_t, \boldsymbol{M}_t)$ denote the function that maps all available knowledge of the controller at time t to the battery management action $\boldsymbol{\beta}_t$.

Privacy Metric To evaluate the users' privacy quantitatively, we use Shannon's equiv-

ocation [9] to characterize the uncertainty of the electricity demands preserved from the message receiver's perspective:

$$r_p(\mu^i) = \lim_{\tau\to\infty} \frac{1}{\tau} H(D_1^i, ..., D_\tau^i | \omega_0, M_1^i, ..., \omega_\tau, M_\tau^i) \tag{4.2}$$

where $H(\cdot|\cdot)$ denotes the conditional entropy.

The mathematical notations used through this work are summarized in Table. 4.1 while some notations only used in one section are not included due to space limit.

$t = 1, 2, ...$	Time
$\omega_t \in \Omega$	Core state at time t
$P_t \in \mathcal{P}$	Electricity price at time t
$\gamma_P(\cdot)$	Environment deciding price function
$\delta_t^P \in \Delta^P$	Unforeseeable price fluctuation
$D_t^i \in \mathcal{D}$	Electricity demand of user i at time t
$\gamma_i(\cdot)$	Environment deciding demand function for user i
$\delta_t^i \in \Delta^i$	Unforeseeable demand fluctuation for user i
$\boldsymbol{\delta}_t$	The composite unforeseeable system condition $\boldsymbol{\delta}_t = \{\delta_t^1, \cdots, \delta_t^n, \delta_t^P\}$
$\mathbf{P}_{\Delta^i}, \mathbf{P}_\Omega$	Transition matrix of Markovian process δ_t^i and ω_t
$\phi_t \in \Phi$	The composite system state $\phi_t = \{\omega_t, \boldsymbol{\delta}_t\}$
$B_t^i \in \mathcal{B}$	Energy storage level for user i
$\mathbf{B}_t$	the state of the battery $\mathbf{B}_t = \{B_t^1, \cdots, B_t^n\}$
$\beta_t^i \in \mathcal{B}$	Battery management decision for user i by the controller
U_t^i	the electricity cost for user i at time t
$M_t^i \in \mathcal{M}^i$	Messages sent from user i
μ^i	The messaging strategy for user i
μ^C	The battery management strategy for the controller
$\boldsymbol{\mu}$	the composite strategies by all players including users and the battery controller
$r_p(\mu^i)$	Privacy preserved for user i with messaging strategy μ^i
$\underline{r}_p^i$	Minimum privacy requirement of user i
$\mathcal{U}_{\boldsymbol{\mu}}^i(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$	Limiting average electricity cost of user i
λ^i	Weight assigned to cost of user i
$\mathcal{R}_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$	Weighted sum of electricity costs
$\rho \in [0, 1)$	Discount factor

Table 4.1: Summary of Notations

4.2 A Stochastic Signaling Game Formulation

In this section, we build a game theoretical framework to capture the competitive messaging behaviors of users in the energy storage sharing with requirements on privacy preserving. Upon this framework, we can study different messaging strategies of users and the corresponding optimal battery managements. When the privacy requirement is relaxed, a Nash equilibrium point is presented to achieve the social optimality.

We model the long term electricity costs of users using a limiting average formulation and it is given by:

$$\mathcal{U}^i_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \mathbb{E} \limsup_{T\to\infty} \frac{\sum_{t=0}^{T} u(D^i_t, P_t, B^i_t, B^i_{t+1})}{T} \tag{4.3}$$

which is a function of system states $\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0$. $\boldsymbol{\mu} = \{\mu^i | i = 1, ..., n, C\}$ denotes the messaging strategies by all players including users and the battery controller. The expectation is over all possible realizations of the system states and the randomized strategies.

Though the energy storage system is a shared property, different users may have different priorities to the shared battery since the purchase and maintenance costs of the battery could be divided unequally across them. Consequently, we want to characterize the achievable cost savings region in which each point corresponds to a simultaneously achievable set of cost-savings for the group of users. Depending on the users' priority, the energy storage sharing system can operate at any point in the region. To study this cost savings region among different users, we define a weighted cost with weight $\lambda^i \in [0, 1]$ for user i and $\sum_{i=1}^{n} \lambda^i = 1$:

$$\mathcal{R}_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \sum_{i=1}^{n} \lambda^i \mathcal{U}^i_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) \tag{4.4}$$

By swapping $\lambda^i, i = 1, \ldots, n$ in its feasible region, different users' priority pairs can be characterized.

Assumed to be rational, each user aims to minimize its own electricity cost individually by choosing appropriate messaging strategies with privacy preserving requirement:

$$\begin{aligned} &\underset{\mu^i}{\text{minimize}}\ \mathcal{U}^i_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) \\ &\text{subject to: } \mu^i \text{ s.t. } M^i_t \in \mathcal{M}^i, \forall t \\ &r_p(\mu^i) >= \underline{r}^i_p \end{aligned} \tag{4.5}$$

where $\underline{r}_p^i$ denotes the requirement on the privacy preserving.

When the privacy is a concern, $\underline{r}_p^i > 0$, the battery controller can not completely determine the actual energy demands by observing the messages and other public information. However, when the privacy is not a concern, $\underline{r}_p^i = 0$, the second constraint of (4.5) is satisfied by default. Note that, independent of the privacy concern, the user's electricity cost as modeled in (4.5) always incentivize dishonest reporting for additional cost savings.

On the other hand, the battery controller aims to minimize the weighted cost (4.4) based on the information available and messages received:

$$\begin{aligned} \underset{\mu^C}{\text{minimize}}\ & \mathcal{R}_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \sum_{i=1}^{n} \lambda^i \mathcal{U}_{\boldsymbol{\mu}}^i(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) \\ \text{subject to: } & \mu^C \text{ s.t. } B_t^i \in \mathcal{B}, \forall i, \sum_{i=1}^{n} B_t^i \in \mathcal{B}, \forall t \end{aligned} \tag{4.6}$$

Since the cost function is bounded, the weighted cost optimization is equivalent to the constrained optimization of one user's cost with inequality constraints on others' costs [45]. Sweeping $\lambda^i, i = 1, \ldots, n$ across its valid region which is a n-simplex, the achievable cost savings region can be characterized completely.

When privacy is not a concern and all users act honestly, the battery sharing becomes a centralized management problem which is studied in Section 4.3.1. In contrast, when privacy is the top priority, the messages carry minimal information about the users' actual electricity usage. The battery sharing becomes a message blind management problem which is studied in Section 4.3.3.

The focus of this work is to study the battery management when all players aim to minimize their own objectives individually. The battery sharing is a general sum, multi-player limiting average signaling game. The equilibrium of this category of stochastic games usually does not exist or is difficult to find even if it exists. However, if the privacy requirement is relaxed $\underline{r}_p^i = 0$, due to the relatively advantageous position of the battery controller, we shall demonstrate that a Nash equilibrium exists in this game using a non stationary strategy, and furthermore, the performance is identical to that of the optimal demand aware centralized energy management system.

4.3 Complete Honest and Maximum Privacy Messaging

Before we present our results on the equilibrium point of the stochastic messaging game of battery sharing, we first study two special cases of users' messaging strategy and the corresponding optimal battery management strategy. Though they are not necessary results of our stochastic game equilibrium analysis in Section 4.4, they help to illustrate the structure of the proposed credit based battery management strategy which ensures the game equilibrium and the social optimality.

4.3.1 A Lower Bound On The Weighted Cost Summation: Centralized Battery Management

To characterize the upper bound of the social welfare or the lower bound of the weighted summation of users' cost $\mathcal{R}_{\mu}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$, we assume that none of the users desire privacy and they are completely honest and comprehensive to the battery controller about their unforeseeable demand component δ_t^i.

$$\mu^{i*} : M_t^i = \delta_t^i, i = 1, ..., n \tag{4.7}$$

The battery management strategy μ^C can now utilize the users' demand information D_t^i directly, $\mu_t^C \left(\omega_0, P_0, \mathbf{B}_0, D_0^i, \ldots, \omega_t, P_t, \mathbf{B}_t, D_t^i, i = 1, ..., n\right)$ which is equivalent to $\mu_t^C(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0, ..., \omega_t, \boldsymbol{\delta}_t, \mathbf{B}_t)$.

A discounted cost formulation approach: To derive the corresponding optimal battery management strategy $\mu^{C\dagger}$, we first study the ρ-discounted cost formulation. The weighted cost in the ρ-discounted formulation is written as:

$$\mathcal{R}_{\rho,\mu^C}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \sum_{i=1}^{n} \rho^i \left[\lim_{T\to\infty} \mathbb{E} \sum_{t=0}^{T} \lambda^i U_t^i \right] \tag{4.8}$$

where $\rho \in [0, 1)$ is the discount factor. Since the immediate cost function (4.1) is always bounded, the average weighted cost for any policy μ^C always exists. The battery management optimization in limiting average formulation can be approximated by ρ-discounted weighted cost formulation when $\rho \to 1$. Our objective is to find the optimal weighted cost:

$$\mathcal{R}^*_{\rho,\mu^C}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \inf_{\mu} \mathcal{R}_{\rho,\mu^C}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) \tag{4.9}$$

and the policy $\mu_\rho^{C\dagger}$ that minimizes the cost.

Such an optimization can be formulated as a **Markov Decision Process** (MDP) with *state* $(\omega_t, \boldsymbol{\delta}_t, \mathbf{B}_t)$, *action* $\boldsymbol{\beta}_t$, *transition*

$$\begin{aligned}&\Pr(\omega_{t+1}, \boldsymbol{\delta}_{t+1}^i, B_{t+1}|\omega_t, B_t, \boldsymbol{\beta}_t)\\ &\quad= \begin{cases} P_\Omega(\omega_t, \omega_{t+1})\Pi P_{\Delta^i}(\delta_t, \delta_{t+1}), & \mathbf{B}_{t+1} = \boldsymbol{\beta}_t \\ 0, & o.w. \end{cases}\end{aligned} \tag{4.10}$$

discount factor ρ and *immediate cost function*:

$$r(\omega_t, \boldsymbol{\delta}_t, \boldsymbol{b}_t, \boldsymbol{\beta}_t) = \sum_{i=1}^{n} \lambda^i (d_t^i + \beta_t^i - b_t^i) p_t. \tag{4.11}$$

For a Markov decision process with finite state space and bounded immediate cost function, proposition 1.2.3 in [46], proves that the optimal policy is stationary and given by the solution to the following fixed point equation.

$$\begin{aligned}J(\omega, \boldsymbol{\delta}, \boldsymbol{b}) &= \inf_{\boldsymbol{\beta}} r(\omega_t, \boldsymbol{\delta}_t, \boldsymbol{b}_t, \boldsymbol{\beta}_t)\\ &\quad + \rho \sum_{\omega', \boldsymbol{\delta}'} P_\Omega(\omega, \omega')\Pi P_{\Delta^i}(\delta_t, \delta_{t+1}) J(\omega', \boldsymbol{\delta}', \boldsymbol{\beta})\end{aligned} \tag{4.12}$$

where $\boldsymbol{\beta} = \mu^C(\omega, \boldsymbol{\delta}, \boldsymbol{b})$, $\boldsymbol{\beta}' = \mu^C(\omega', \boldsymbol{\delta}', \boldsymbol{\beta})$.

This Bellman equation can be solved using value iteration method which can be time consuming because the state space and action space grow exponentially with number of users. But if there exist specific structures on the optimal policy, the problem solving time can be significantly simplified. In this work, we present a linear programming solution for centralized battery management which significantly reduced the computation complexity.

Structure of optimal policy: Minimizing the discounted weighted cost (4.8) yields an optimal policy structure in which the cost minimizing choice for user's battery level $\mu_\rho^{C\dagger}(\omega, \boldsymbol{\delta}, \boldsymbol{b})$ is always independent of $\boldsymbol{b}$ as shown in Fig.4.3:

Lemma 4. *There exists function* $\mu_\rho^{C\dagger}(\omega, \boldsymbol{\delta})$ *independent of* $\boldsymbol{b}$ *such that the optimal policy that solves the Bellman equation (4.12):*

$$\mu_\rho^{C\dagger}(\omega, \boldsymbol{\delta}, \boldsymbol{b}) = \mu_\rho^{C\dagger}(\omega, \boldsymbol{\delta}) \tag{4.13}$$

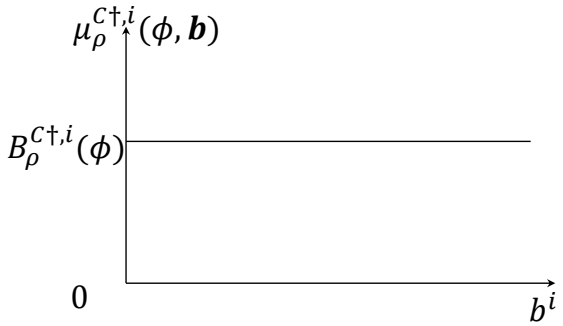

Figure 4.3: The optimal centralized battery management strategy structure

Proof: First, we prove that the minimal discounted weighted cost function $J(\omega, \boldsymbol{b}) = \inf_{\boldsymbol{\beta} \in \mathbb{C}_A^{\boldsymbol{\beta}}(\omega, \boldsymbol{b})} \text{ or } {}_{\mathbb{C}_B^{\boldsymbol{\beta}}(\omega, \boldsymbol{b})} \mathcal{C}(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is convex on $\boldsymbol{b}$.
$\mathbb{C}_A^{\boldsymbol{\beta}}(\omega, \boldsymbol{b}) = \{\boldsymbol{\beta} \in \mathcal{B}^n | \sum_{i=1}^n \beta^i \in \mathcal{B}\}$
$\mathbb{C}_B^{\boldsymbol{\beta}}(\omega, \boldsymbol{b}) = \{\boldsymbol{\beta} \in \mathcal{B}^n | \sum_{i=1}^n \beta^i \in \mathcal{B}, \sum_{i=1}^n \beta^i - b^i + d^i \geq 0\}$.

Assume the minimal total discounted weighted cost is $J(\omega, \boldsymbol{b}) = \inf_{\boldsymbol{\beta}(\omega, \boldsymbol{b}) \in U_{\boldsymbol{\beta}}} \mathcal{C}(\omega, \boldsymbol{b}, \boldsymbol{\beta}(\omega, \boldsymbol{b}))$, where $U_{\boldsymbol{\beta}} = \{\boldsymbol{\beta} \in \mathcal{B}^n | \sum_{i=1}^n \beta^i \in \mathcal{B}\}$ and define:

$$H(\omega, \boldsymbol{b}, \boldsymbol{\beta}) = c(\omega, \boldsymbol{b}, \boldsymbol{\beta}) + \rho \sum_{\omega'} P_\Omega(\omega, \omega') J(\omega', \boldsymbol{\beta}) \tag{4.14}$$

The Bellman equation states that:

$$J(\omega, \boldsymbol{b}) = \inf_{\boldsymbol{\beta} \in U_{\boldsymbol{\beta}}} H(\omega, \boldsymbol{b}, \boldsymbol{\beta}) \tag{4.15}$$

Let $J^n(\omega, \boldsymbol{b})$ denote the minimal n-step discounted weighted cost starting from state ω and battery level $\boldsymbol{b}$. Similar to (4.14), define

$$H^n(\omega, \boldsymbol{b}, \boldsymbol{\beta}) = c(\omega, \boldsymbol{b}, \boldsymbol{\beta}) + \rho \sum_{\omega'} P_\Omega(\omega, \omega') J^{n-1}(\omega', \boldsymbol{\beta})$$

Then, $J^n(\omega, \boldsymbol{b})$ satisfies

$$J^n(\omega, \boldsymbol{b}) = \inf_{\boldsymbol{\beta} \in U_{\boldsymbol{\beta}}} H^n(\omega, \boldsymbol{b}, \boldsymbol{\beta})$$

This series of finite-horizon costs converge as $\lim_{n \to \infty} J^n(\omega, \boldsymbol{b}) = J(\omega, \boldsymbol{b})$. Thus, in order to show that $J(\omega, \boldsymbol{b})$ is convex, it is sufficient to show by induction that this holds for all $J(\omega, \boldsymbol{b})$.

When $n = 0$, it is trivial that $J^0(\omega, \boldsymbol{b}) = 0$ is convex. Assume that $J^{n-1}(\omega, \boldsymbol{b})$ is

convex on $\boldsymbol{b}$. $c(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is linear and therefore convex. $H^n(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is convex as it is a linear combination of convex functions (4.14). By induction, $J^n(\omega, \boldsymbol{b}) = \inf_{\boldsymbol{\beta} \in U_{\boldsymbol{\beta}}} H^n(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is convex on $\boldsymbol{b}$.

Now we know that $J(\omega, \boldsymbol{b})$ is a convex function over $\boldsymbol{b}$, so is the $H(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ over $\boldsymbol{\beta}$ as $c(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ and $J(\omega', \boldsymbol{\beta})$ in (4.14) are both convex on $\boldsymbol{\beta}$. The partial derivative of $H(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ to β_i is given by:

$$\frac{\partial H(\omega, \boldsymbol{b}, \boldsymbol{\beta})}{\partial \beta_i} = \lambda^i p + \rho \sum_{\omega'} P_\Omega(\omega, \omega') \frac{\partial J(\omega', \boldsymbol{\beta})}{\partial \beta_i} \tag{4.16}$$

which is independent of $\boldsymbol{b}$. Therefore the gradient $\nabla_{\boldsymbol{\beta}} H(\omega, \boldsymbol{b}, \boldsymbol{\beta}) = (\frac{\partial H(\omega, \boldsymbol{b}, \boldsymbol{\beta})}{\partial \beta_1}, ..., \frac{\partial H(\omega, \boldsymbol{b}, \boldsymbol{\beta})}{\partial \beta_n})$ is also independent of $\boldsymbol{b}$.

As $H(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is convex on $\boldsymbol{\beta}$ and the gradient $\nabla_{\boldsymbol{\beta}} H(\omega, \boldsymbol{b}, \boldsymbol{\beta})$ is independent of $\boldsymbol{b}$, the optimal policy would be independent of $\boldsymbol{b}$, $\boldsymbol{\beta}^*(\omega, \boldsymbol{b}) = \mathbf{B}^*(\omega)$, if following such policy would satisfy the constraint $\mathbb{C}_A$. Particularly, No selling back constraint $\sum_{i=1}^n A_t^i \geq 0$ results in $\sum_{i=1}^n b^i \leq \sum_{i=1}^n (B_\omega^{*,i} + d^i)$. Otherwise, $\boldsymbol{\beta}^*(\omega, \boldsymbol{b})$ should be the closest valid battery level to $\mathbf{B}^*(\omega)$. The structure of cost minimizing policy for 2 users when the total electricity storage in the battery (4.8) is above the threshold follows immediately. ■

An equivalent problem for the discounted weighted cost minimization: Even though we have shown that the optimal policy $\mu_\rho^{C\dagger}(\omega, \boldsymbol{\delta}, \boldsymbol{b})$ is independent of $\boldsymbol{b}$, the immediate cost function (4.11) comprises $\omega, \boldsymbol{\delta}, \boldsymbol{b}$. Therefore the state space when minimizing (4.12) can increase rapidly as n increases. Such a state space can be tremendous even when more than a few users share the battery. We however present a linear integer programming optimization problem that only requires states $\omega, \boldsymbol{\delta}$ which yields the same optimal policy in order to simplify the problem. We use $\phi = (\omega, \boldsymbol{\delta})$ as a composite system state, where $\Phi = \Omega \times \Pi \Delta^i$ is the state space and P_Φ is the resulting transition matrix. $\mathbf{p}$ is the price column vector and $[\mathbf{p}]_j$ is the price at state ϕ_j.

$\mathbf{B}_\rho^{C\dagger}$ is the optimal policy matrix in which $[\mathbf{B}_\rho^{C\dagger}]_{i,j} = B_\rho^{C\dagger,j}(\phi_i)$ is the weighted cost minimizing decision on the electricity storage of user j with state ϕ_i.

Theorem 5. *The solution of the weighted cost minimization (4.9) is equivalent to:*

$$\boldsymbol{B}_\rho^{C\dagger} = \arg\min_{\boldsymbol{B}_\rho^C} \mathbb{1}_{1 \times |\Phi|} [I - \rho P_\Phi]^{-1} \left[((I - \rho P_\Phi) \boldsymbol{p}) \circ (\boldsymbol{B}_\rho^C \boldsymbol{\lambda}) \right] \tag{4.17}$$

where $\circ$ is the Hadamard product. $\mathbb{1}_{m \times n}$ is $m \times n$ matrix with all elements 1. I is an identity matrix. $\mathbf{B}_\rho^C$ is a $|\Phi| \times n$ matrix with constraint $\mathbb{C}^{\mathbf{B}_\rho^C} = \{\mathbf{B}_\rho^C \in \mathcal{B}^{|\Phi| \times n} | \sum_{j=1}^n [\mathbf{B}_\rho^C]_{i,j} \in \mathcal{B}, \forall i\}$. $\boldsymbol{\lambda} = [\lambda^1, ..., \lambda^n]^T$ is the assigned weight for each user. *Proof:* In order to

prove Theorem 2, we need to first construct a MDP and then transform it into a linear programming problem. First, we propose an infinite horizon discounted MDP with the same definition of state $\omega = \{d^1, ..., d^n, p\} \in \Omega$, decision $\boldsymbol{\beta} \in \{\boldsymbol{\beta} \in \mathcal{B}^n | \sum_{i=1}^n \beta^i \in \mathcal{B}\}$ as the original MDP and define the transition using $P_\Omega(\omega, \omega')$ which is independent of $\boldsymbol{\beta}$. $\boldsymbol{\gamma}(\omega)$ is used to denote a stationary policy mapping state space Ω to the action space $\{\boldsymbol{\beta} \in \mathcal{B}^n | \sum_{i=1}^n \beta^i \in \mathcal{B}\}$. The immediate cost function is defined as

$$c'(\omega, \boldsymbol{\beta}) = \sum_{i=1}^{n} (p - \rho {p'}_\omega) \lambda^i \beta^i + \sum_{i=1}^{n} \lambda^i d^i p \tag{4.18}$$

where λ, ρ is also the same as in the original problem. ${p'}_\omega = \sum_{\omega' \in \Omega} P_\Omega(\omega, \omega') p', \omega' = \{{d'}^1, ..., {d'}^n, p'\}$ is the expected price of next step given the current state ω.

Therefore, the expected total discounted cost for any stationary policy $\boldsymbol{\gamma}(\omega)$ in this process is

$$\mathcal{C}'(\omega, \boldsymbol{\gamma}(\omega)) = c'(\omega, \boldsymbol{\gamma}(\omega)) + \rho \sum_{\omega'} P_\Omega(\omega, \omega') \mathcal{C}'(\omega', \boldsymbol{\gamma}(\omega')) \tag{4.19}$$

There exists a linear integer programming optimization whose solution $\mathbf{B}^*(\omega)$ can minimize the discounted weighted cost (4.8) with constraint $\mathbb{C}_A$:

$$\begin{aligned} &\text{minimize } \mathbb{1}_{1\times|\Omega|}[I - \rho P_\Omega]^{-1} [((I - \rho P_\Omega)\mathbf{p}) \circ (\boldsymbol{\beta}\boldsymbol{\lambda})] \\ &\text{subject to } \boldsymbol{\beta} \in \mathcal{B}, \boldsymbol{\beta}\mathbb{1}_{1\times n} \in \mathcal{B} \end{aligned} \tag{4.20}$$

Lemma 6. *Minimization of (4.19) yields the same optimal policy $\boldsymbol{B}^*(\omega)$ as in the original discounted weighted cost minimization problem (4.8) with constraints $\mathbb{C}_A$.*

To prove Lemma 6 we just need to compare $\mathcal{C}'(\omega, \boldsymbol{\gamma}(\omega))$ with $\mathcal{C}(\omega, \boldsymbol{b} = 0, \boldsymbol{\beta}(\omega, 0) = \boldsymbol{\gamma}(\omega))$ terms by terms.

Solving the equivalent stochastic control problem of (4.19) would result in a linear integer programming optimization [46].

$$\begin{aligned} &\text{minimize } \mathbb{1}_{1\times|\Omega|}[I - \rho P_\Omega]^{-1} [((I - \rho P_\Omega)\mathbf{p}) \circ (\boldsymbol{\beta}\boldsymbol{\lambda})] \\ &\text{subject to } \boldsymbol{\beta} \in \mathcal{B}, \boldsymbol{\beta}\mathbb{1}_{1\times n} \in \mathcal{B} \end{aligned} \tag{4.21}$$

■

The optimal centralized battery management in limiting average formula-

tion: Since the immediate cost function (4.1) is always bounded, the average weighted cost for any policy μ^C always exists. When $\rho \to 1$, we derive the linear programming solution of the optimal centralized battery management in limiting average formulation:

$$\mathbf{B}^{C\dagger} = \arg\min_{\mathbf{B}^C} \mathbb{1}_{1\times|\Phi|}[I - P_\Phi]^{-1}\left[((I - P_\Phi)\mathbf{p}) \circ (\mathbf{B}^C\boldsymbol{\lambda})\right] \tag{4.22}$$

The performance of the optimal centralized battery management strategy provides a lower bound on the weighted summation of electricity cost of users. We will show in Section 4.4 that this lower bound can be achieved at a non-stationary equilibrium which is ensured by the proposed credit based battery management strategy.

4.3.2 Privacy as a Stepwise Additive Metric

In order to study the maximum privacy preserving strategy, we first analyze the privacy metric described in (4.2). Using the fact that a user's demand is completely determined by the environment and the unforeseeable additives, $D_t^i = \gamma_i(\omega_t) + \delta_t^i$, and the privacy analysis techniques provided in Chapter 3, we can represent the privacy $r_p(\mu^i)$ as:

$$r_p(\mu^i) = \lim_{\tau\to\infty} \frac{1}{\tau} H(\delta_1^i, ..., \delta_\tau^i | \omega_0, M_1^i, ..., \omega_\tau, M_\tau^i) \tag{4.23}$$

$$= H_{\delta^i} - \mathbb{E}[H_{pr}(\delta_t^i) - H_{po}(\delta_t^i)] \tag{4.24}$$

where H_{δ^i} denotes the entropy rate of δ_t^i, $H_{pr}(\delta_t^i) = H(\delta_t^i | M_1^i, M_2^i, ..., M_{t-1}^i)$ is the entropy of δ_t^i prior to the messaging M_t^i and $H_{po}(\delta_t^i) = H(\delta_t^i | M_1^i, M_2^i, ..., M_t^i)$ is the entropy of δ_t^i post to the messaging M_t^i.

Using (4.24), we can numerically compute the privacy preserving performance of a messaging strategy by tracking the message receiver's estimated probability of δ_t^i.

In addition, we can upper bound the privacy preserving using (4.23):

$$r_p(\mu^i) \leq H_{\delta^i} \tag{4.25}$$

This is due to the properties of the conditional entropy, $H(\delta_1^i, ..., \delta_\tau^i | \omega_0, M_1^i, ..., \omega_\tau, M_\tau^i) \leq H(\delta_1^i, ..., \delta_\tau^i)$. It is worth noting that upper bound H_{δ^i} of the privacy preserving is achievable when M_t^i is independent of $delta_t^i$. Such messaging strategy is studied in Section 4.3.3.

4.3.3 A Completely Privacy Preserving Strategy: Message Blind Battery Management

When privacy is the top priority of all users and therefore they want to hide as much information about their actual energy consumption as possible from the message receiver, $r_p(\mu^i) = H_{\delta^i}$. In order to do so, they send messages M_t^i independent of their unforeseeable demands δ_t^i – a completely privacy preserving scenario.

Since M_t^i is independent δ_t^i, messages M_t^i reveal no information other then what the controller already knows. Independent of battery's management strategy and the initial state of the whole system, the controller's belief on δ_t^i is going to converge to the stationary distribution $\Pr_{\Delta^i}(\delta)$. Therefore, there exists a centralized message blind battery management strategy $\mu^{C'}$ not relying on message M_t^i can preform optimally. $\mu^{C'}$ can be derived by solving the resulting battery control optimization with similar process as in Section 4.3.1. The details of the optimization are not presented due to limited space.

In $\mu^{C'}$, the battery controller uses a stationary policy which does not rely on messages M_t^i:

$$\mathbf{B}'^{*} = \underset{\mathbf{B}' \in \mathbb{C}^{\mathbf{B}'}}{\arg\min}\, \mathbb{1}_{1\times|\Phi'|}[I - P_{\Phi'}]^{-1}\left[((I - P_{\Phi'})\mathbf{p}) \circ (\mathbf{B}'\boldsymbol{\lambda})\right] \tag{4.26}$$

where $\phi' = (\omega, \delta^P)$ is the composite system state, $\Phi' = \Omega \times \Delta^P$ is the state space and P'_Φ is the resulting transition matrix. $\mathbf{p}$ is the price column vector and $[\mathbf{p}]_j$ is the price at state $\phi'_j = (\omega_{\phi'_j}, \delta^P_{\phi'_j})$. $\mathbf{B}'$ is a $|\Phi'| \times n$ matrix with constraint $\mathbb{C}^{\mathbf{B}'} = \{\mathbf{B}' \in \mathcal{B}^{|\Phi'|\times n} | \sum_{j=1}^{n} [\mathbf{B}']_{\phi',j} \in \mathcal{B}, \forall \phi'\}$ where $[\mathbf{B}']_{\phi',j}$ denotes the battery storage allocation for user j when the composite system state is ϕ'.

Theorem 7. *If all users are sending zero information to the battery controller – μ^i: M_t^i are independent of δ_t^i, then $\mathcal{R}_{\mu^{C'}}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0) = \min_{\mu^C} \mathcal{R}_{\mu^C}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0)$ for $\forall i$*

Proof: This is a direct result of the battery control optimization when the controller's belief on δ_t^i converges to $\Pr_{\Delta^i}(\delta)$. ■

In addition, we generalize this completely private messaging setup to partially private messaging where the message set $\mathcal{M}^i$ are restricted $|\mathcal{M}^i| < |\Delta^i|$ in Section 4.5.

4.4 A Non-Stationary Equilibrium Of The Stochastic Game When Privacy Requirement Is Relaxed

When privacy is not a concern $\underline{r}_p^i = 0$, the privacy constraint in (4.5) is relaxed. As all users aim to minimize their own cost individually and the battery controller aims to minimize the weighted cost sum, the stochastic game formulated in Section 4.2 is a general sum, multi-player limiting average signaling game. The equilibrium of this category of stochastic games usually does not exist or is difficult to find even if it exists. However, due to the relatively advantageous position of the battery controller, a simple equilibrium exists in this game and it performs as well as the optimal demand aware centralized energy management system.

As we presented in Section 4.3.1, The optimal centralized energy management policy under the infinite horizon limiting average weighted cost formulation $\boldsymbol{\mu}^{C\dagger}$ is a stationary mapping from current system state to the new battery state $\mathbf{B}^{C\dagger}$ as in (4.22). The performance of this stationary centralized battery control policy $\mathbf{B}^{C\dagger}$ provides the benchmark for the socially optimal solution – $\mathcal{R}_C^{\dagger}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$, which we call the "demand-aware optimal cost". As we will see in the following section, if the privacy constraint is relaxed $\underline{r}_p^i = 0$, this performance is achievable in a competitive user driven model as well by choosing an appropriate battery control policy.

4.4.1 A Credit Based Battery Management Strategy

To achieve the socially optimal cost savings we propose a credit based battery management strategy μ^{C*} for the battery controller and it achieves the equilibrium point in the limiting average signaling game we formulated in the previous section. When the battery controller is using the credit based battery management strategy μ^{C*}, the users are coerced to communicate honestly about their demand D_t^i or unforeseeable demand state δ_t^i. Since the users are now honest, the battery management can perform ideally on social optimality.

While communicating D_t^i and δ_t^i is equivalent, let us assume the battery controller expects the users to send their unforeseeable demand state δ_t^i honestly, for the sake of simplicity. The battery controller is going to record each users' messages and count each message's appearance frequency. Based on these statistical information, the battery controller will give a label L_t^i to each user to tell if it is "H", honest, or "L", lying using the

following "credit checking" mechanism:

$$L_t^i = \begin{cases} H & \text{if } \frac{N_t(\delta,\omega)}{N_t(\omega)} - \Pr_{\Delta^i}(\delta) \leq \frac{C_{\Delta^i}}{\sqrt{n}}, \forall \delta \in \Delta^i, \omega \in \Omega \\ & \text{and } \frac{N_t(\delta)}{t} - \Pr_{\Delta^i}(\delta) \leq \frac{C_{\Delta^i}}{\sqrt{n}}, \forall \delta \in \Delta^i \\ L & \text{o.w.} \end{cases} \tag{4.27}$$

where δ is any unforeseeable demand state of user i. $N_t(\delta)$ denotes the number of occurrence of messages from i, $M_t^i = \delta$ until time t and $N_t(\omega)$ denotes the number of occurrence of $\omega_t = \omega$ until time t. $\Pr_{\Delta^i}(\delta)$ is the stationary probability of δ of user i. C_{Δ^i} is a constant value depending on the transition probability P_{Δ^i}.

In the credit based battery management μ^{C*}, if $L_t^i = L$, the user i is denied to access the battery until $L_t^i = H$. When $L_t^i = H$, the electricity storage for user i is managed according to the optimal demand aware centralized battery control policy (4.22). Therefore, the credit based battery management μ^{C*} can be described as:

$$\mu^{C*} : \beta_t^i = \begin{cases} [\mathbf{B}^{C\dagger}]_{\phi_t,i} & \text{if } L_t^i = T \\ 0 & \text{if } L_t^i = L \end{cases} \tag{4.28}$$

where $\phi_t = (\omega_t, \boldsymbol{\delta}_t)$ as mentioned previously. In addition, we denote the honest messaging strategy for user i as μ^{i*} in (4.7).

In order to show $\mu^{C*}, \mu^{i*}, \forall i$ is an equilibrium point, we propose Lemma 8 to constrain the users' behaviors such that the statistical properties of M_t^i matches the probability distribution of δ_t^i, then we use Lemma 9 to show that any other policies μ^i within the constraints performs no better than μ^{i*} while the battery controller is using μ^{C*}. Meanwhile, Lemma 10 proves the optimality of μ^{C*}. The proofs of the Lemmas are presented in Appendix.

Lemma 8. *Assume that the battery controller and other users stick to the strategies:* $\boldsymbol{\mu}^{-i*} = \{\mu^{C*}, \mu^{j*}, \forall j = i\}$. *For* $\forall \mu^i$, *if there exists a* $\epsilon > 0$, *such that* $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta,\omega)}{N_t(\omega)} \neq \Pr_{\Delta^i}(\delta)\} > \epsilon$ *or* $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta)}{t} \neq \Pr_{\Delta^i}(\delta)\} > \epsilon$, *then* $\mathcal{U}_{\boldsymbol{\mu}}^i(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0) = \mathbb{E}\, P_t D_t^i$.

Proof: If $\exists \epsilon > 0$, such that $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta,\omega)}{N_t(\omega)} \neq \Pr_{\Delta^i}(\delta)\} > \epsilon$ or $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta)}{t} \neq \Pr_{\Delta^i}(\delta)\} > \epsilon$, we have $\lim_{t\to\infty} \Pr\{L_t^i = L\} = 1$. Therefore, $\lim_{t\to\infty} \Pr\{B_{t+1}^i = 0\} = 1$ according to the credit based battery management strategy μ^{C*}. $\mathcal{U}_{\boldsymbol{\mu}}^i(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \mathbb{E}\, P_t D_t^i$ comes after applying the definition of the limiting average cost (4.1) and (4.3) ■

Lemma 8 demonstrates the effectiveness of the "credit checking" – if the messages' statistical property do not match the stationary probability distribution of δ_t^i, user i will

be denied to use battery when time $t \to \infty$. In other words, even if user i decides to lie, its messaging strategy is constrained. It is also easy to see μ^{i*} satisfies this constraint using the strong law of large numbers of Markov Process [47] and VonBahr-Essen bound [48].

Lemma 9. *For $\forall \mu^i$, such that μ^i s.t. $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta,\omega)}{N_t(\omega)} \neq \Pr_{\Delta^i}(\delta)\} = 0$ and $\lim_{t\to\infty} \Pr\{\frac{N_t(\delta)}{t} \neq \Pr_{\Delta^i}(\delta)\} = 0$, the following inequality always holds.*

$$\mathcal{U}^i_{\boldsymbol{\mu}^{-i*},\mu^i}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0) \geq \mathcal{U}^i_{\boldsymbol{\mu}^*}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0) \tag{4.29}$$

where $\boldsymbol{\mu}^* = \{\mu^{C*}, \mu^{i*}, \forall i\}$ and $\boldsymbol{\mu}^{-i*} = \{\mu^{C*}, \mu^{j*}, \forall j \neq i\}$.

Proof: First, $\mathcal{U}^i_{\boldsymbol{\mu}^{-i*},\mu^i}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$ is lower bounded by the limiting average cost of user i when battery controller trust it unconditionally $\mathcal{U}^i_{\boldsymbol{\mu}^{-iC*},\mu^i,\mu^{SC}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$. μ^{SC} stands for the stationary centralized battery control policy $B^i_{t+1} = [\mathbf{B}^*]_{\phi_t,i}$. Due to the assumption that $\frac{N_t(\delta,\omega)}{N_t(\omega)} \to \Pr_{\Delta^i}(\delta)$ and $\frac{N_t(\delta)}{t} \to \Pr_{\Delta^i}(\delta)$ in probability, $\lim_{T\to\infty} \frac{\sum_{t=0}^T u(D^i_t, P_t, B^i_t, B^i_{t+1})}{T}$ exists.

As a result, $\mathcal{U}^i_{\boldsymbol{\mu}^{-iC*},\mu^i,\mu^{SC}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0) = \mathbb{E}\lim_{T\to\infty} \frac{\sum_{t=0}^T P_t(D^i_t + B^i_{t+1} - B^i_t)}{T}$ and it can be further reformed to three parts:$\mathbb{E}\lim_{T\to\infty} \frac{\sum_{t=0}^T P_t(D^i_t)}{T} - \mathbb{E}\lim_{T\to\infty} \frac{\sum_{t=0}^T P_t B^i_t}{T} + \mathbb{E}\lim_{T\to\infty} \frac{\sum_{t=0}^T P_t B^i_{t+1}}{T}$. While the first component is independent of strategy, the second and third components are also invariant of μ^i as the distribution of the messaging $m^i_t = \delta$ does not change and m^i_t is also uncorrelated with ω_t and independent of δ^P_t.

Therefore, $\mathcal{U}^i_{\boldsymbol{\mu}^{-iC*},\mu^i,\mu^{SC}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$ is equal to $\mathcal{U}^i_{\boldsymbol{\mu}^*}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$ ■

Lemma 9 shows the optimality of μ^{i*} within the constraints of the credit checking. Combining Lemma 8 and Lemma 9, we can conclude that any unilateral deviation by user i can not reduce its electricity cost when the users and the battery controller implement strategies $\mu^{C*}, \mu^{i*}, \forall i$.

Lemma 10. *$\forall \mu^C, \mu^1, ..., u^n$, $\mathcal{R}_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0)$ is lower bounded by the demand-aware optimal cost, $\mathcal{R}^*_C(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0)$ and it is achieved when the users and the battery controller implement $\mu^{C*}, \mu^{i*}, \forall i$.*

Proof: It is obvious that any messaging policy and battery control management strategy in the proposed signaling game can be realized in the centralized battery management as the users' unforeseeable state is known by the controller and all behaviors of the users and the controller in the game can be simulated. Therefore, $\mathcal{R}_{\boldsymbol{\mu}}(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$ is lower bounded by the demand-aware optimal cost, $\mathcal{R}^*_C(\omega_0, \boldsymbol{\delta}_0, \mathbf{B}_0)$.

In the following section, when the users and the controller performs on $\mu^{C*}, \mu^{i*}, \forall i$, the users are honest to the controller and the controller has the same information as the

demand aware centralized battery management. Therefore, adopting the stationary battery management strategy should yield the desired lower bound. ■

As a result of Lemma 10, the strategies $\mu^{C*}, \mu^{i*}, \forall i$ respectively for the controller and the users yields the lowest possible weighted cost. Any unilateral deviation by the battery controller can not reduce the weighted electricity cost. In the following we show that the weighted cost thus achieved at the equilibrium is indeed the social optimality as well; in other words, the competitive equilibrium performs as well as the centralized scheme with complete information at the battery controller.

Theorem 11. *$\mu^{C*}, \mu^{i*}, \forall i$ is the equilibrium point of proposed infinite horizon limiting average signaling game. From the perspective of the battery, this equilibrium point yields the optimal weighted cost.*

Proof: Combining Lemma 8 - 10, Any unilateral deviation by the battery controller will not reduce the weighted cost and any unilateral deviation by any user will not reduce its own cost. Therefore, $\mu^{C*}, \mu^{i*}, \forall i$ is the equilibrium point of proposed infinite horizon limiting average signaling game. In addition, $\mu^{C*}, \mu^{i*}, \forall i$ achieves the lower bound of the weighted cost according to Lemma 10. ■

In this section, we proved that with the proposed credit based battery management strategy, the users gain no benefits from forging messages in long term operations. Since the users are honest, the battery management performs ideally and achieves the lower bound of the electricity cost. However, we notice that there are also drawbacks with this strategy:

- It might raise privacy concerns as users are forced to report their unforeseeable demand components honestly and comprehensively.
- Even if a user is always honestly using μ^{i*}, he can be denied to access the battery storage for a certain period of time with non-zero probability. In other words, the false alert happens and can influence the users experience badly.
- The convergence rate of the accurate "credit checking" (4.27) relies on the properties of the Markov process δ_t^i and it is not fast in general as an order of $O(n^{-0.5})$.

Due to the mentioned concerns of the credit based battery management strategy, we consider a class of privacy preserving battery management strategy where the message set being restricted $|\mathcal{M}^i| < |\Delta_t^i|$.

4.4.2 A Special Case: i.i.d. Unforeseeable Demand

When the unforeseeable demand states δ_t^i are i.i.d., the message blind battery management strategy in Section 4.3.3 performs equally as the optimal centralized battery management as proved in Theorem 12.

Theorem 12. *If δ_t^i are i.i.d. for $\forall i$, then $\mathcal{U}^i_{\mu^{C'}}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0) = \mathcal{U}^i_{\boldsymbol{\mu}^{i*}, \boldsymbol{\mu}^{C\dagger}}(\omega_0, \boldsymbol{\delta}_0, \boldsymbol{B}_0)$ for $\forall i$*

Proof: This theorem can be proved by comparing the message blind battery management strategy $\mu^{C'}$ description (4.26) and the optimal centralized battery management strategy (4.22), $[P_\Phi]_{\phi_j,\phi_k} = P_\Omega(\omega_k, \omega_j) \times \prod_{i=1}^n \Pr_{\Delta^i}(\delta_k^i)$, P_Φ is a matrix consisting of block with repeating elements. So there always $\exists \mathbf{B'}$ s.t. $\mathbb{1}_{1\times|\Phi'|}[I-P_{\Phi'}]^{-1}\left[((I-P_{\Phi'})\mathbf{p})\circ(\mathbf{B'\lambda})\right] = \mathbb{1}_{1\times|\Phi|}[I-P_\Phi]^{-1}[((I-P_\Phi)\mathbf{p})\circ(\mathbf{B\lambda})]$ for $\forall \mathbf{B}$ and vice versa: there always $\exists \mathbf{B}$ s.t. $\mathbb{1}_{1\times|\Phi|}[I-P_\Phi]^{-1}\left[((I-P_\Phi)\mathbf{p})\circ(\mathbf{B\lambda})\right] = \mathbb{1}_{1\times|\Phi'|}[I-P_{\Phi'}]^{-1}\left[((I-P_{\Phi'})\mathbf{p})\circ(\mathbf{B'\lambda})\right]$ for $\forall \mathbf{B'}$. ■

A direct inference from Theorem 12 is that the message blind battery management strategy ensures the Nash equilibrium of the battery sharing game when the unforeseeable demand states δ_t^i are i.i.d.. It is easy to see that the battery controller does not have motivation to change strategy since the weighted sum (4.4) has already been optimized. The users have no intention to change their strategy since it won't influence cost savings.

Though it is not accurate to approximate the Markovian process δ_t^i using i.i.d. process, it is reasonable to presume that the message blind battery management strategy yields a close performance to optimum when δ_t^i is less correlated in time.

4.5 Privacy Preserving Battery Management Strategy

While the credit based battery management strategy optimizes the weighted sum of cost savings and the message blind battery management strategy minimizes privacy concerns of users on the battery controller, we also explore the ground lies in between, the privacy aware battery management.

Privacy Preserving Messaging Behaviors: In order to partially preserve users' privacy from the battery controller, we assume the battery controller and users have an agreement on the message set $1 \leq |\mathcal{M}^i| \leq |\Delta_t^i|$ and users' messaging behaviors:

$$\mu^i : M_t^i = f^i(\delta_t^i), i = 1, ..., n \tag{4.30}$$

where f^i is a surjective function from Δ_t^i to $\mathcal{M}^i$ and known to the user i and the battery controller. Different level of privacy can be preserved by changing the size of $\mathcal{M}^i$. When

privacy is preserved completely, $|\mathcal{M}^i| == 0$ or 1, it is equivalent to the message blind battery management strategy. On the other hand, when there is no requirement on privacy, $|\mathcal{M}^i| = |\Delta_t^i|$, it is equivalent to the centralized battery management.

Battery Management Strategy: To minimize the limiting average weighted cost (4.4), the battery controller in the privacy aware battery management setup uses a policy with similar structure of (4.13) in the centralized battery management. Since the messages do not directly describe the unforeseeable part of demands $\boldsymbol{\delta}_t$, the battery controller is going to keep track of the belief on $\boldsymbol{\delta}_t$, which is noted as $\pi_{po}(\boldsymbol{\delta}_t)$:

$$\begin{aligned}\pi_{po}(\boldsymbol{\delta}_t) &= \Pr\{\boldsymbol{\delta}_t|\boldsymbol{m}_0, ..., \boldsymbol{m}_t\} \\ &= \Pr\{\boldsymbol{\delta}_t|\pi_{po}(\boldsymbol{\delta}_{t-1}), \boldsymbol{m}_t\} \end{aligned} \tag{4.31}$$

Lemma 13. *There exists function $\mu^C(\omega_t, \pi_{po}(\boldsymbol{\delta}_t))$ independent of $\boldsymbol{b}$ such that the optimal policy that minimize the weighted cost of users in the privacy preserving battery management setup:*

$$\mu^C(\omega_0, \boldsymbol{m}_0, \boldsymbol{b}_0, ..., \omega_t, \boldsymbol{m}_t, \boldsymbol{b}_t) = \mu^C(\omega_t, \pi_{po}(\boldsymbol{\delta}_t)) \tag{4.32}$$

Proof: The proof of the structure (4.32) is similar to the proof of Lemma 4 and is omitted due to limited space. ■

Though the general privacy preserving battery management optimization can not be reduced to a linear programming problem since the composite state space $\{\omega_t, \pi_{po}(\boldsymbol{\delta}_t)\}$ can be infinite because that the transition of belief $\pi_{po}(\boldsymbol{\delta}_t)$ may not converge, it still can be optimized numerically in simulations.

It is worth noting that it is difficult to claim a general privacy preserving battery management strategy on a Nash equilibrium when $|\mathcal{M}^i| \neq |\Delta_t^i|$ and $|\mathcal{M}^i| \neq 1$. Since the transition of the belief state may not have a stationary distribution in privacy preserving battery management. Statistics of the belief state is generally not a reliable way to determine whether a user is honest or not which could be a drawback of the privacy preserving battery management. However, as we are going to show in the simulations, even the completely private messaging case – message blind battery management, preforms close to the optimal centralized battery management.

4.6 Simulation Results

In this section, we use real data to train the system model and validate our work using a numerical simulation. The core state is assumed to be the time of the day and the average electricity consumption at the same time of the day is used as environment dependent energy demand. The deviations between the demand and its same time average are formulated as the unforeseeable demand component δ_t^i. This model is applied to the electricity price as well. We use part of the electricity usage data of a home [43] to train the Markovian model of users' demands, and part of the time-of-use pricing data published by NY ISO [44] to train the price model. The rest of the data is used to numerically validate our theoretical results. The unforeseeable components are discretized into 10 levels and they are assumed to follow an Markovian Process. Time is resampled to 0.5 hour interval as the discreted price change is not very frequent. The shared battery is assumed to have 3 kWh capacity. As both users are relatively small electricity consumers with peak power consumptions less than 1.5 kW, a battery with 3kWh is reasonable in this case.

In Fig.4.4, we compare the cost savings performance of different messaging and battery management strategies. When the privacy is not the concern, the optimal two users cost savings tradeoff is achieved by running on the equilibrium point $\boldsymbol{\mu}^*$ where the battery controller uses the credit based battery management strategy. When the privacy is the top priority, the message blind battery management strategy scarifies some cost savings in exchange of privacy protection. To demonstrate the ground lies in between, we present the privacy preserving battery management when $|\mathcal{M}^i| = \frac{|\Delta_t^i|}{2}$. In contrast, we compare our results with a simple policy in which battery capacity is equally and statically allocated when each user's electricity storage is managed independently. The region of cost-savings is acquired by sweeping across all possible weightings $\boldsymbol{\lambda}$.

We can observe that the dynamic battery sharing is more efficient than static allocation, especially when users are equally weighted. Meanwhile, both the complete and partial privacy preserving battery management performs close to the optimal credit based battery management. However, both the partial privacy preserving and message blind battery managements are outperformed by the static battery allocation management at the end of the curves. When the battery allocations are extremely biased, the cost saving performance of static battery allocation strategy converges to the optimal credit based battery management. However, the insufficient demand information for privacy protection still cause the loss in cost savings, which demonstrate that the tradeoff between utility and privacy.

In order to demonstrate the tradeoff between cost savings and users' privacy in Fig.4.5,

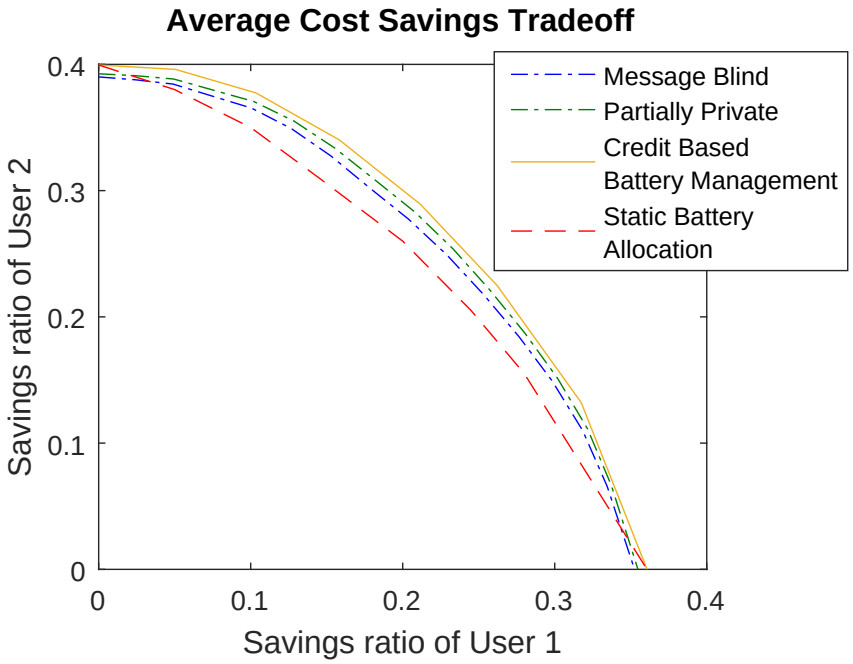

Figure 4.4: Cost savings tradeoff between 2 users with a shared battery under the limiting average signaling game formulation

we present the achievable privacy-cost savings pairs by using the privacy preserving battery management strategies with different message set $\mathcal{M}^i$ and messaging policy μ^i. We can observe that even a completely private messaging setup – message blind battery management performs close to the optimum compared to the static battery allocation setup while the unforeseeable part of demands δ_t^i has been perfectly hidden. This is because in real life, the majority of demands are environment related and predictable if sufficient historical data of a user can be collected.

We illustrate the performance convergence rates of different energy storage management strategies in Fig.4.6 including a simple static capacity allocation strategy. In this simulation, we assume users have the same priority to the battery $\boldsymbol{\lambda} = \{0.5, 0.5\}$. As demonstrated, the performance of the optimal credit based battery management takes longer time to converge than the statistical battery allocation method. The performance oscillation is due to the unavoidable possibility of false alert of credit checking. However, the performance of the message blind, privacy preserving and the statistical allocation battery management converges with the same speed since they are stationary in nature.

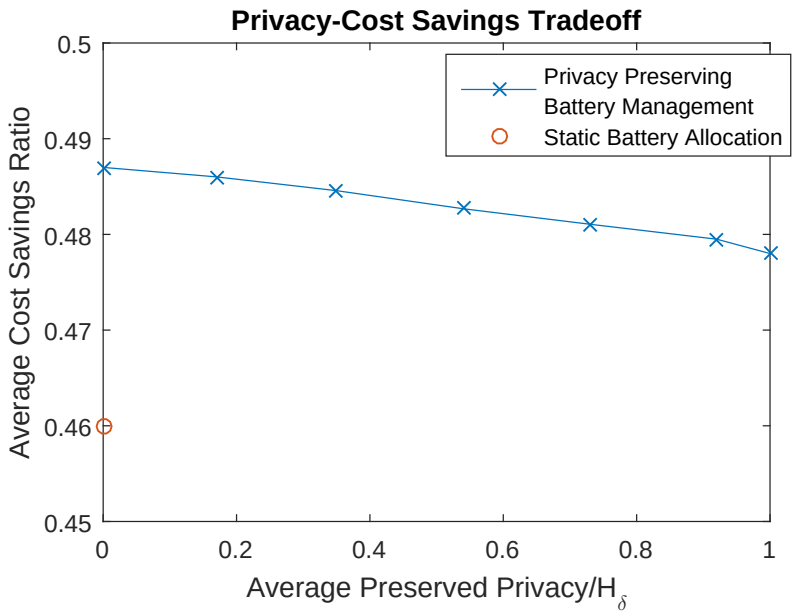

Figure 4.5: The tradeoff between cost saving and privacy using privacy preserving strategies

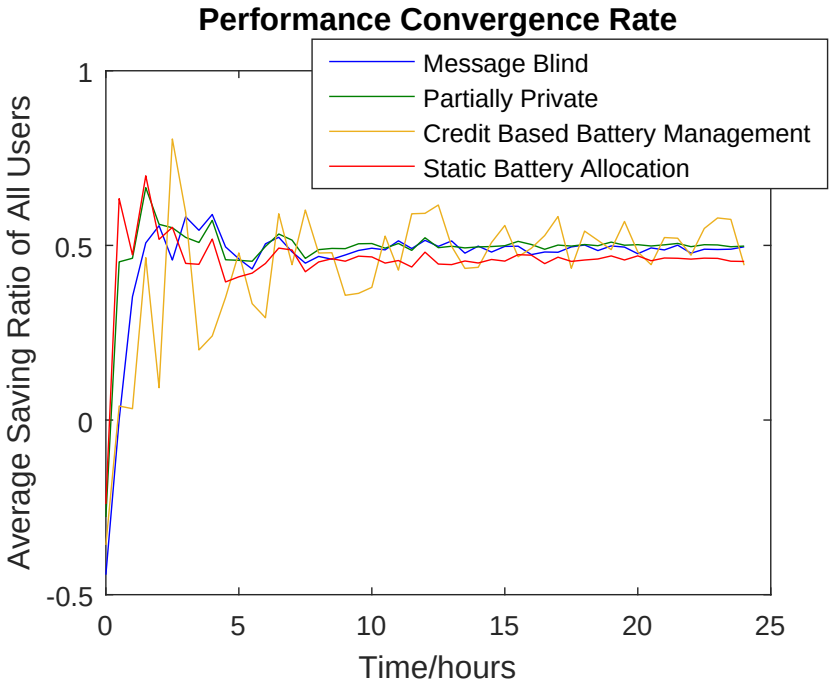

Figure 4.6: Convergence rate of $\mathcal{R}_T(\boldsymbol{\mu})$ under the limiting average signaling game formulation

4.7 Summary

In this work, we studied a privacy aware battery management problem assuming rational users and the battery controller relies on the communications with the users to make

decisions. A game theoretical framework was built with an infinite horizon limiting average signaling game formulation. The privacy requirement serves as a constraint on messaging behaviors.

When the privacy requirement is relaxed, the competitive behaviors of users sending messages to the battery controller is studied. The credit based battery management strategy is designed for the battery controller to ensure an equilibrium of the game and achieves the social optimality. In this credit based battery management strategy, one user's access to the battery is strictly denied whenever he is found giving "abnormal" messages.

When the privacy requirement is top priority, a message blind strategy is proposed to optimally manage the battery. We also present a privacy preserving battery management to achieve a tradeoff between cost savings and privacy protection.

Numerical example with real world data is provided to evaluate our proposed battery management strategies, and demonstrate the cost effectiveness of battery sharing and the tradeoff between the privacy and cost reduction.

Investigating the impact of battery value depreciation and optimization of privacy preserving messaging given cost savings constraint are interesting topics for future research.

5. Quantitative Risk Assessment of Cyber Attack on DSM

Cyber-enabled Demand Side Management (DSM) plays a crucial role in smart grid by providing automated decision-making capabilities that selectively schedule loads on these local grids to improve power balance and grid stability. Security and reliability of the cyber infrastructure that enables DSM is therefore critical to ensuring reliability and safety in energy delivery systems. The DSM communication are usually built on Advanced Metering Infrastructure (AMI). However, by virtue of topological weaknesses, it is vulnerable to cyber attacks that are undetectable or stealthy. In this work, we investigate the topological vulnerabilities of DSM networks that could result in potential theft of electricity through hacked smart meters. In particular, a provably correct risk assessment protocol is proposed to identify completely the individual nodes in mesh network based AMIs that are potential targets of such economically motivated stealthy cyber attacks. The protocol proposed utilizes knowledge of the network topology and data obtained from existing system monitoring technologies. A case study is provided to demonstrate the protocol and its effectiveness. Another major challenge in DSM security is that the feedback mechanism in the load management may aggravate the impact of cyber attack on the DSM system. We investigate the behavior of such feedback loop under the intentional cyber attack and evaluate its potential risk of overloading the power grid components. In particular, a tight upper bound is provided to characterize the potential risk when a fixed portion of the controllable loads are compromised.

5.1 Preliminaries

5.1.1 DSM System Model

Consider a local electric power distribution network consisting by a set $\mathcal{N}$ of N customers that are served by a single utility company. The utility company participates in wholesale electricity markets to purchase electricity from generators and then sell it to customers. Even though wholesale prices can fluctuate rapidly, traditional utility companies hide this volatility from their customers and offer electricity at a flat rate. To encourage the efficient use of electricity, an increasing number of utilities start to use dynamic pricing in the retail market to coordinate the customers demand responses to the benefit of individual customers and the overall system. We now present our model of such a DSM system, describe how the utility set the electricity prices dynamically, how customers typically respond and the distribution grid connects them.

We consider a discrete-time model with a infinite horizon. Time is divided into equal duration, indexed by $t \in \mathcal{T} := \{\dots, -1, 0, 1, 2, \dots\}$.

Utility company: The utility company provides enough electricity to meet the demands of the N customers. In general, there are different designs of end-user demand response program including real-time pricing, direct load management and etc. For the simplicity of presenting, we assume the real-time pricing scheme is in use. However, various types of demand response policies should also fit into this model since their load management actions are eventually equivalent to real time pricing if the consumers are modeled appropriately. For example, load shedding scheme can be modeled as real time pricing with minimum price variations but extremely sensitive users. In this example, load shedding actions can be treated as slight variation of price. Though the majority of users are insensitive with such price change, certain sensitive users shut down their controllable devices when price increase slightly. On the other hand, the design of the real-time electricity prices needs to reflect running costs of the utility company and the payments incurred in the various wholesale markets. Such topic is beyond the scope of this paper. For simplicity, we make the important assumption that this design can be summarized by a cost function $C(q)$ that specifies the cost for the utility company to provide q amount of power to the N customers in a time interval. The modeling of the cost function is an active research issue. Here we assume the cost function $C(q)$ to be stationary over time t and quadratic on q. As a result, the optimal pricing strategy for the utility company is to set the new price $p(t+1), t \in \mathcal{T}$ according to the margins of the cost function $C(q)$, which is a common

practice in industry:

$$p(t+1) = \frac{dC(x)}{dx}|_{x=q(t)} = c_1 q(t) + c_0 \tag{5.1}$$

where c_0, c_1 are fixed constants derived from cost function of $C(q)$ and $q(t)$ is the total power consumption of the N customers at time t.

Customers: For each customer $i \in \mathcal{N}$, we denote by $d_i(t)$ its power draw at time $t \in \mathcal{T}$. Now we can express the total electricity load as:

$$q(t) = \sum_{i \in \mathcal{N}} d_i(t) \tag{5.2}$$

Each customer i is characterized by two parameters:

- a utility function $U_i(d_i)$ that quantifies the utility user i obtains when he consumes d_i power at a time interval; and
- a set of linear inequalities $\underline{D_i} \leq d_i(t) \leq \overline{D_i}$ on power draw by each user.

The modeling of the utility function is very subjective and depends on the properties of the customers' loads. In this work, we assume that $U_i(d_i)$ is quadratic since it reflects utility's marginal diminishing of energy consuming which is a common practice in various researches. Therefore the net utility for costumer i to consume d_i power at time t is $U_i(d_i) - p(t)d_i$. Maximizing the net utility would result in:

$$\arg\max_x [U_i(x) - p(t)x] = u' p(t) + u'' \tag{5.3}$$

where u', u'' are fixed constants derived from utility function of $U_i(d_i)$. However, the reaction time of different appliances and the communication delay between the utility company and the customers can vary, we assume that actual power consumption of costumer i is a linear combination of prices with different delays:

$$d_i(t) = \sum_{k=0}^{\infty} u_i^k p(t-k) + u_i \tag{5.4}$$

where u_i^k and u_i are derived from $U_i(d_i)$, depending on the properties of consumer i.

Power distribution grid: In this work, we consider the impact of cyber attacks on the power distribution grid. Distribution network are usually divided into three types – radial, ring or network. For the simplicity of presenting, we assume that the power

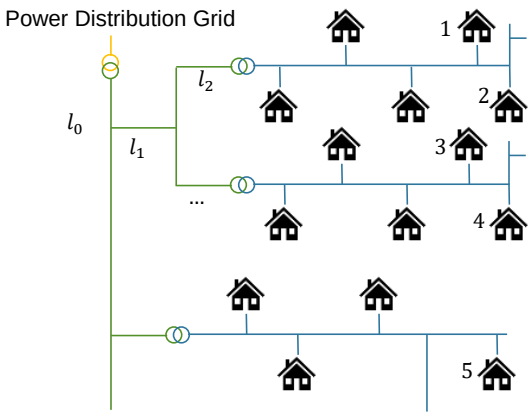

Figure 5.1: A typical radial residential distribution network

distribution grid is a radial network since it is the most common type of structure in power distribution system and the results can be easily extended to other power distribution grid structures. The

A pictorial representation of the radial power distribution network consisting of multiple costumers is shown in Fig.5.1. While the costumers are labeled as $1, 2, 3, ..., N$, power lines are labeled as $\mathcal{M} = \{l_0, l_1, l_2, ..., l_M\}$. In this work, we investigate the load $q_j(t)$ on each power line l_j at time t in existence of DSM cyber attack and determine the potential overload on these power lines. The capacity of each line is denoted as $\gamma_j, j \in M$. We denote the described power grid as $G = (\mathcal{N}, \mathcal{M})$.

5.1.2 Cyber Attack Model

In this work, we consider malicious attacker whose objective is to cause overloads on the power distribution grid by tampering with the DSM system. The communication of DSM system are usually built on AMI, which is suffering from the weak encryption and security design [13]. Since the AMI is usually located distributively in residential area and is easily accessible, it is easy for the attacker to find an access point though compromising the whole system might be impractical. In addition, the mesh structure of the AMI communication network enables the attacker to spread his impact even if only one access point in the system is compromised. In this work, we assume the malicious attacker is aware of the power distribution grid structure G and entire system states including pricing strategies c_0, c_1 and the loads preferences $u_i, u_i^0, u_i^1, \ldots | i \in \mathcal{N}$. Since the objective of this work is to evaluate the vulnerabilities of the power distribution grid and the potential risks of DSM cyber attack, it is reasonable to assume the attacker is both knowledgeable and rational.

Actions and strategies of the attacker: In this work, we assume that a subset of all the N customers are compromised by the attacker and we denote this subset as $\mathcal{D}$. These compromised customers need not to be along the same power line or under the same substation since the mesh communication network may have very different structure than the power grid. There are generally two types of cyber attacks the attacker may launch on these customers: pricing data injection in which the compromised customers receive manipulated pricing information, and direct load manipulation in which the appliances of the compromised customers are under the control of the attacker. The pricing data injection attack can happen when the communication encryption is broken and the direct load manipulation can happen when the DSM load controllers have been hacked into.

- **Pricing data injection** $\mathcal{A}_P$: The attacker can manipulate prices $p(t)$ received by each compromised costumer $i \in \mathcal{D}$, and the received price $p_i(t)$ can be different for different costumers in order to achieve the attacker's desired effect:

$$\mathcal{A}_P : p_i(t) = a_i^P(t), \forall i \in \mathcal{D} \tag{5.5}$$

- **Direct load manipulation** $\mathcal{A}_L$: The attacker can manipulate the load of each compromised costumer $d_i(t), i \in \mathcal{D}$ directly:

$$\mathcal{A}_L : d_i(t) = a_i^L(t), \forall i \in \mathcal{D} \tag{5.6}$$

where $a_i^P(t)$ and $a_i^L(t)$ for $i \in \mathcal{D}$ is the actions that the attacker can choose.

It is not difficult to see that these two types of attack are ultimately equivalent.

Theorem 14. *Given a set of customers $\mathcal{D}$ compromised by the attcker, there always exists a direct load manipulation $\mathcal{A}_L$ such that all customers behave the same as any pricing data injection attack $\mathcal{A}_P$ is in effect. Vice verse, given a set of customers $\mathcal{D}$ compromised by the attcker, there always exists a pricing data injection attack $\mathcal{A}_P$ such that all customers behave the same as any direct load manipulation $\mathcal{A}_L$ is in effect.*

Proof: When a group of costumers is under attack, to achieve the same effect of any pricing data injection $\mathcal{A}_P$, $a_i^P(t)$, the attacker can schedule the direct load manipulation $\mathcal{A}_L$ as $a_i^L(t) = u_i + \sum_{j=0}^{\infty} u_i^j a_i^P(t-j)$. In this setup, the compromised costumers behave the same way as receiving the injected prices $a_i^P(t)$. On the other hand, the attacker can forge a pricing series $a_i^P(t) = [d_i(t) - u_i - \sum_{j=1}^{\infty} u_i^j a_i^P(t-j)]/u_i^0$ to make the compromised costumers to behave as any direct load manipulation $a_i^L(t)$. ■

Since pricing data injection and direct load manipulation attacks are eventually equivalent, we now constrain ourselves on the direct load manipulation $\mathcal{A}_L$. For the ease of reading, $\mathcal{A}$ and $a_i(t)$ implies the direct load manipulation $\mathcal{A}_L$ and $a_i^L(t)$ from now on.

We let $\mu(G, \mathcal{D}, c_0, c_1, u_i, u_i^k | i \in \mathcal{N}, k \geq 0)$ denote the attack strategy that maps all known system properties $G, \mathcal{D}, c_0, c_1, u_i, u_i^k | i \in \mathcal{N}, k \geq 0$ to the direct load manipulation action series $\{a_i(t) | i \in \mathcal{D}, t = \dots, -1, 0, 1, 2, \dots\}$.

Objective of attacker: There are different harms an attacker can do on the power distribution grid. For example, an attacker can cause chaotic metering by messing the metering data transmission, efficiency loss of the energy provision by causing greater load volatility, or the energy system failure by overloading the power lines or devices. The focus of this work is on the potential system failure because of its catastrophic results and the potential influence on the critical infrastructures. Therefore, we want to determine if there exists an attack strategy for the attacker who compromised a certain customer set $\mathcal{D}$ to overload a power line l_j. In other words, we want to determine maximum load q_j^* on power line l_j given the compromised customer set $\mathcal{D}$:

$$q_j^* = \max_{\mu(G, \mathcal{D}, c_0, c_1, u_i, u_i^k | i \in \mathcal{N}, k \geq 0)} \max_t q_j(t) \tag{5.7}$$

and compare q_j^* with the line capacity γ_j. If $q_j^* > \gamma_j$, power line l_j can be overloaded and therefore vulnerable to the attacker in control of $\mathcal{D}$. As defenders, we are not sure about which power line the attacker is targeting on and our objective is to find out all vulnerable power lines in the power distribution grid efficiently given that a compromised customer set $\mathcal{D}$.

5.2 A Discrete Time Linear System Formulation

In this section, we build a connection between the cyber attack $\mathcal{A}$, $a_i(t)$ and the load $q_j(t)$ on a power line l_j which helps to derive the optimal attack strategy and the maximum load q_j^*. To do so, we first connect the attack $a_i(t)$ and the electricity price $p(t)$. Thereafter, we can determine the electricity load of all customers and the power line load $q_j(t)$.

5.2.1 Electricity Price Impacted By Attack

Consider the impact direct load manipulation (5.6) on customers in $\mathcal{D}$ and the load properties (5.4) of uninfluenced customers $\mathcal{N}\backslash\mathcal{D}$, we get the impacted total electricity load:

$$\begin{aligned} q'(t) &= \sum_{i\in\mathcal{N}\backslash\mathcal{D}} d_i(t) + \sum_{i\in\mathcal{D}} a_i(t) \\ &= \sum_{k=0}^{\infty} \left(\sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i^k \right) p(t-k) + \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i + \sum_{i\in\mathcal{D}} a_i(t) \end{aligned} \tag{5.8}$$

Plug the impacted total electricity load $q'(t)$ in the utility's pricing strategy (5.1) and shift one time interval backward:

$$\begin{aligned} p(t) =& \sum_{k=0}^{\infty} \left(c_1 \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i^k \right) p(t-k-1) + c_0 + \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i \\ &+ \sum_{i\in\mathcal{D}} a_i(t-1) \\ =& \sum_{k=0}^{\infty} \lambda^{k+1} p(t-k-1) + c_0 + \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i + \sum_{i\in\mathcal{D}} a_i(t-1) \end{aligned} \tag{5.9}$$

where we define constants λ^0 and λ^{k+1}, $k \geq 0$ to replace the coefficient terms for the ease of presentation:

$$\lambda^{k+1} = c_1 \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i^k, k \geq 0 \tag{5.10}$$

The attack-price relation (5.9) can be viewed as a feedback system as shown in Fig.5.2, where $A(Z)$ is the system input and $P(Z) = \mathcal{Z}\{p(t)\}$ is the output. $A(Z) = \mathcal{Z}(\alpha(t))$ is the $\mathcal{Z}$-transform of the bias aggregated load manipulation:

$$\alpha(t) = \sum_{i\in\mathcal{D}} a_i(t) + \sum_{i\in\mathcal{N}\backslash\mathcal{D}} u_i + c_0 \tag{5.11}$$

and $P(Z) = \mathcal{Z}\{p(t)\}$.

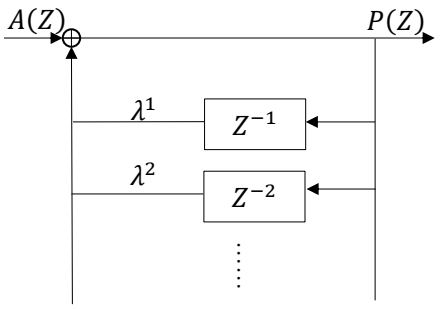

Figure 5.2: The attack-price feedback loop illustration

We can write down the system transfer equation in $\mathcal{Z}$-domain:

$$P(Z) = \frac{Z^{-1}}{1 - \sum_{k=1}^{\infty} \lambda^k Z^{-k}} A(Z) \tag{5.12}$$

5.2.2 Power Line Load Impacted By Attack

Now we determine the relation between any power line load $q_j(t)$ and the cyber attack $\mathcal{A}$, $a_i(t)$. Assume the costumers drawing electricity from this power line l_i forms a set $\mathcal{S}_j$, we can then represent the power line load $q_j(t)$ as:

$$\begin{aligned} q_j(t) &= \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} d_i(t) + \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} a_i(t) \\ &= \sum_{k=0}^{\infty} \left(\sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i^k \right) p(t-k) + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i + \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} a_i(t) \\ &= \sum_{k=0}^{\infty} \sigma_j^k p(t-k) + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i + \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} a_i(t) \end{aligned} \tag{5.13}$$

where we define constants σ_j' and σ_j^k, $k \geq 0$ to replace the coefficient terms for the ease of presentation:

$$\sigma_j^k = \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i^k, k \geq 0 \tag{5.14}$$

If we do a $\mathcal{Z}$-transform on the power line load equation (5.12), we get $Q_j(Z) =$

$\mathcal{Z}\{q_j(t)\}$:

$$Q_j(Z) = \left(\sum_{k=0}^{\infty} \sigma_j^k Z^{-k}\right) P(Z) + A_j(Z) \tag{5.15}$$

$$= \frac{\sum_{k=0}^{\infty} \sigma_j^k Z^{-k-1}}{1 - \sum_{k=1}^{\infty} \lambda^k Z^{-k}} A(Z) + A_j(Z) \tag{5.16}$$

where $A_j(Z) = \mathcal{Z}(\alpha_j(t))$ is the $\mathcal{Z}$-transform of the bias aggregated load manipulation among the costumers drawing electricity from power line l_i, $\mathcal{S}_j$:

$$\alpha_j(t) = \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} a_i(t) + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i \tag{5.17}$$

Plugging (5.12) in (5.15), we finally get the relationship between the power line load $q_j(t)$ and the cyber attack $\mathcal{A}$, $a_i(t)$ in condition of compromised customer group $\mathcal{D}$, (5.16).

Since manipulated load $a_i(t)$ is bounded by the actual load bounds $\underline{D_i}$ and $\overline{D_i}$ in the direct load manipulation attack, $\alpha_j(t)$ is also bound as $\underline{\alpha_j} \leq \alpha_j(t) \leq \overline{\alpha_j}$.

$$\begin{aligned} \underline{\alpha_j} &= \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} \underline{D_i} + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i \\ \overline{\alpha_j} &= \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} \overline{D_i} + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i \end{aligned} \tag{5.18}$$

5.3 Optimal Direct Load Manipulation Strategy

The focus of this work is to determine all vulnerable power lines in $\mathcal{M}$ such that the attacker can find a strategy to overload given that a group of customers $\mathcal{D}$ are compromised by the attacker. In order to do so, we first derive the maximum load q_j^* described in (5.14) which can be achieved with the optimal direct load manipulation strategy μ^*. Afterwards, we design an depth first search algorithm to find out all vulnerable power lines efficiently.

In order to optimize $q_j(t)$ on the cyber attack $\mathcal{A}, a_i(t)$, we first separate the aggregated load manipulation $\alpha(t)$ in (5.11) into two independent parts:

$$\alpha(t) = \alpha_j(t) + \alpha_j'(t) \tag{5.19}$$

where $\alpha_j(t)$ is the bias aggregated load manipulation down the power line l_j described in

(5.17) and $\alpha'_j(t)$ represents the remaining load manipulation:

$$\alpha'_j(t) = \sum_{i \in \mathcal{D} \setminus \mathcal{S}_j} a_i(t) + \sum_{i \in (\mathcal{N} \setminus \mathcal{S}_j) \setminus \mathcal{D}} u_i + c_0 \tag{5.20}$$

$\alpha'_j(t)$ is bound as $\underline{\alpha'_i} \leq \alpha'_j(t) \leq \overline{\alpha'_i}$.

$$\begin{aligned} \underline{\alpha'_i} &= \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} \underline{D_i} + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i + c_0 \\ \overline{\alpha'_i} &= \sum_{i \in \mathcal{S}_j \cap \mathcal{D}} \overline{D_i} + \sum_{i \in \mathcal{S}_j \setminus \mathcal{D}} u_i + c_0 \end{aligned} \tag{5.21}$$

Then we are able to reorganize the terms in (5.16):

$$Q_j(Z) = H_j A_j(Z) + H'_j A'_j(Z) \tag{5.22}$$

where $A'_j(Z)$ is the $\mathcal{Z}$-transform of $\alpha'_j(t)$. H_j and H'_j are:

$$\begin{aligned} H_j &= \frac{\sum_{k=0}^{\infty} \sigma_j^k Z^{-k-1}}{1 - \sum_{k=1}^{\infty} \lambda^k Z^{-k}} + 1 \\ H'_j &= \frac{\sum_{k=0}^{\infty} \sigma_j^k Z^{-k-1}}{1 - \sum_{k=1}^{\infty} \lambda^k Z^{-k}} \end{aligned} \tag{5.23}$$

respectively. As a result, $Q_j(Z)$ in (5.22) is separated into two independent terms which can be optimized individually. The optimization of $\mathcal{Z}^{-1}\{H_j A_j(Z)\}$ and $\mathcal{Z}^{-1}\left\{H'_j A'_j(Z)\right\}$ leads us to Theorem 15.

Theorem 15. *The maximum load q_j^* on power line l_j given the compromised customer set $\mathcal{D}$ in a power distribution network G is:*

$$q_j^* = \sum_{\tau=-\infty}^{\infty} \left[\overline{\alpha_j} h_j^+(\tau) + \underline{\alpha_j} h_j^-(\tau) + \overline{\alpha'_j} h_j'^+(\tau) + \underline{\alpha'_j} h_j'^-(\tau)\right] \tag{5.24}$$

which can be achieved by $q_j(t_0)$ at any time t_0, if attack strategy μ^* is used:

$$\mu^* : a_i(t_0 - t) = \begin{cases} \overline{D_i}, & \text{if } (i \in \mathcal{D} \cap \mathcal{S}_j) \wedge (h_j(t) > 0) \\ & \text{or } (i \in \mathcal{D} \backslash \mathcal{S}_j) \wedge (h'_j(t) > 0) \\ \underline{D_i}, & \text{otherwise} \end{cases} \tag{5.25}$$

where $h_j(t) = \mathcal{Z}^{-1}\{H_j(Z)\}$ and $h'_j(t) = \mathcal{Z}^{-1}\{H'_j(Z)\}$ as in (5.23).

Proof: It is not difficult to see that cyber attack $A, a_i(t)$ and its effect on power line l_j is indifferent when shifting along the time horizon since we assume time t is infinite on both positive and negative direction. If q_j^* can be achieved by an attack strategy $\mu^1 : a_i^1(t), \forall i \in \mathcal{N}$ at time t_1, $q_{j,\mu^1}(t) = q_j^*$, the same load can be achieved at any other time t_2 by shifting the attack strategy $\mu^2 : a_i^2(t) = a_i^1(t - t_2 + t_1), \forall i \in \mathcal{N}$. Therefore, we can choose any time t_0 to optimize the maximum load on l_j:

$$q_j^* = \max_{a_i(t), \forall i \in \mathcal{D}} q_j(t_0)$$

The remaining part of Theorem 15 is a direct result of the optimization of $q_j(t) = \mathcal{Z}^{-1}\{Q_j(Z)\}$ at time t_0 using the $Q_j(Z)$ in (5.22). Since $\alpha_j(t)$ and $\alpha'_j(t)$ is independent of each other, we can optimize terms $\mathcal{Z}^{-1}\{H_j A_j(Z)\}(t_0)$ and $\mathcal{Z}^{-1}\left\{H'_j A'_j(Z)\right\}(t_0)$ separately. Without loss of generality, we can write down the inverse $\mathcal{Z}$-transform of the first one:

$$\mathcal{Z}^{-1}\{H_j A_j(Z)\}(t_0) = \sum_{\tau=-\infty}^{\infty} \alpha_j(t_0 - \tau) h_j(\tau)$$

Since $\alpha_j(t)$ is independent along time t, the optimization of $\mathcal{Z}^{-1}\{H_j A_j(Z)\}(t_0)$ is equivalent to the optimization of $\alpha_j(t_0 - \tau)h_j(\tau)$ independently. The optimal attack strategy μ^* and the maximum load q_j^* in Theorem 15 follows naturally. ■

There are several insights we can take away from Theorem 15:

- The optimal cyber attack strategy on DSM is binary.
- When targeting on different power lines, the attacker should tailor its attack strategy accordingly.
- With a carefully planned attack strategy, the attacker can create fluctuation and even overload a power line l_j, even if it does not have any direct control on the customers

drawing electricity from the power line $\mathcal{S}_j$.

5.4 A Depth First Search Algorithm For Vulnerability Search

After deriving the close form expression of q_j^* in any power distribution network G and compromised customer set $\mathcal{D}$ as in (5.24), we can traverse $q_j^*, \forall j \in \mathcal{M}$ on all the power lines l_j and search all vulnerabilities in G.

To compute q_j^*, we have to calculate σ_j^k which has a time complexity of $l_u M$, then inverse $\mathcal{Z}$-transform which has a time complexity of $l_H \log(l_H)$. l_u is the number of nontrivial terms of load properties u_i^k in (5.4) and l_H is the number of nontrivial terms of $h_j(t)$. Therefore, the computation of one q_j^* has a time complexity of $\max\{l_u M, l_H \log(l_H)\}$. A naive traverse of $q_j^*, \forall j \in \mathcal{M}$ has a time complexity of $\max\{l_u M^2, l_H \log(l_H) M\}$.

In this section, we present a DFS algorithm to traverse all the power lines for $q_j^*, \forall j \in \mathcal{M}$ efficiently. Due to the space constraint, we only present the key component of this DFS algorithm, the update of σ_j^k, in Algorithm 2. The complexity of updating σ_j^k for all the

Algorithm 2 Depth First Search of σ_j^k

```
1: procedure UPDATE σ_j^k
2:     σ_j^k ← 0
3:     for All customer i directly connected to j do
4:         if i ∉ D then
5:             σ_j^k ← σ_j^k + u_i^k
6:     for All power lines j' connected to j do
7:         Update σ_j'^k
8:         σ_j^k ← σ_j^k + σ_j'^k
       return σ_j^k
```

power lines is reduced to $l_u M$. The resulting time complexity of the vulnerability search is $\max\{l_u M, l_H \log(l_H) M\}$. Such improvement may be unnoticeable when $l_H \log(l_H) M$ is the significant term, but it can have a big influence when the power distribution network G is large. Other values including $\overline{D_j}, \underline{D_j}$ and etc can be efficiently calculated using the same idea though they are not bottlenecking the vulnerability search time complexity.

5.5 Summary

In this work, we built a theoretical framework to evaluate the potential risks of malicious DSM cyber attacks with certain capabilities. A close form expression of maximum

power line load is derived when the DSM is under attack. An efficient depth first search algorithm is developed to search for all power grid vulnerabilities. A case study was provided to demonstrate the protocol and its effectiveness.

To continue our research, we plan to utilize our proposed vulnerability detection method to assist the design of DSM communication network planning and high value attack target protection. One naive approach is to test the vulnerabilities of different communication network plans or protection plans and choose the one with minimum vulnerabilities. However, this approach is neither performance effective nor time efficient. Our objective is to develop an efficient communication network design tool to minimize the potential targets which requires a deep understanding of the vulnerability detection and a carefully designed optimization.

6. Conclusion and Future Works

6.1 Privacy Protection in DSM

We studied the privacy protection in demand response using an in-home energy storage system. A pair of close bounds to characterize the optimal tradeoff between privacy protection and cost savings were given. Although the policy that solves the optimal tradeoff between privacy and cost savings remains an open problem, we believe that our bounds using the revealing state approach are quite close. Operating costs are an important consideration for the mechanism proposed in this research. While the key mathematical contributions in this work do not consider operating costs, the framework does not preclude such costs per se. For instance, a marginal amount can be added to the purchase price when charging the battery, and a marginal cost incurred every time the battery is discharged. The policy simulated with these inclusions would provide a tradeoff that is closer to practice.

Another approach of privacy protection in DSM is to tackle this issue from the metering mechanism design. When the smart metering network is under attack, the fine electricity profile transmitted upon it becomes an even greater privacy concern. The major objective of smart meter is to enable variable electricity pricing. Though reporting the electric usage in every short period of time can help the reliable and effective operation of power grid, it is not the only way. Instead of transmitting how much electricity a consumer uses every certain time period, the meter can calculate the bills of the users locally and only transmit how much money a consumer used for electricity once a week or even once a month. The variable pricing can be achieved by having the pricing plan broadcast to every smart meter and then billing on consumer's end. Such broadcast is necessary in classical smart metering method anyway.

Though this metering scheme has some disadvantage than transmitting electricity usage every 15 mins, it can be used as a backup plan when the communication link is exposed to cyber attacks for two benefits:

1. Longer transmission interval gives more time to eliminate the threats.

2. The aggregated electric bills are much less sensitive. The amount of money a consumer use on electricity in one week or one month reveals much less information than a detailed electricity profile.

6.2 Energy Storage Sharing in DSM

We studied a privacy aware battery management problem assuming rational users and the battery controller relies on the communications with the users to make decisions. A game theoretical framework was built with an infinite horizon limiting average signaling game formulation. The privacy requirement serves as a constraint on messaging behaviors.

When the privacy requirement is relaxed, the competitive behaviors of users sending messages to the battery controller is studied. The credit based battery management strategy is designed for the battery controller to ensure an equilibrium of the game and achieves the social optimality. In this credit based battery management strategy, one user's access to the battery is strictly denied whenever he is found giving "abnormal" messages.

When the privacy requirement is top priority, a message blind strategy is proposed to optimally manage the battery. We also present a privacy preserving battery management to achieve a tradeoff between cost savings and privacy protection.

Numerical example with real world data is provided to evaluate our proposed battery management strategies, and demonstrate the cost effectiveness of battery sharing and the tradeoff between the privacy and cost reduction.

Investigating the impact of battery value depreciation and optimization of privacy preserving messaging given cost savings constraint are interesting topics for future research.

6.3 Risk Management and Prevention of DSM Cyber Attack

We have focused on developing tools and algorithms for risk assessment and vulnerability detection in the DSM infrastructure and operation. The tools/technologies developed include:

1. Risk assessment framework of data integrity attacks on DSM. We propose a control-theoretic approach, which captures the closed-loop nature of the DSM, to derive fundamental stability conditions under data integrity attacks. The impacts of cyber

attacks on the energy delivery system that can be quantitatively evaluated in this framework include system failure caused by overloading and system instability.

2. DSM network topological vulnerabilities detection tool for undetectable cyber attack. The DSM communication networks are usually built on existing Advanced Metering Infrastructure (AMI), which are designed as mesh networks. If one meter is hacked, not only can its own communication be altered, but all other data transmitted through it may also be exposed to manipulation. Hacking of one communication module of a smart meter on the AMI network can not only impact a significant number of users but can also be conducted without being detected. We combine the network topological vulnerability analysis with fault detection techniques using grid sensor readings to provide a more comprehensive potential risk assessment on the AMI communication network.

To continue on this topic, there is a need to further improve and complete the functionality of the risk assessment and the vulnerability detection tools. By integrating accurate physical models of the electricity delivery system into this framework, We expect to achieve a more comprehensive risk assessment and a more accurate vulnerability detection in DSM. Based on this risk assessment model, secure communication network-planning tools can be developed for DSM system to minimize the potential targets utilizing our developed risk assessment framework. Such tools should fit in current existing network planning tool as an add-on function.

Bibliography

[1] REN2015, *Renewables 2015: Global status report*. Paris: REN21 Secretariat, 2015.

[2] U.S. Department of Energy, "The {Smart Grids}: An Introduction," 2009.

[3] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building - BuildSys '10*, pp. 61–66, 2010. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1878431.1878446

[4] F. Sultanem, "Using appliance signatures for monitoring residential loads at meter panel level," *IEEE Transactions on Power Delivery*, vol. 6, no. 4, pp. 1380–1385, 1991.

[5] P. M. Van De Ven, N. Hegde, L. Massoulié, and T. Salonidis, "Optimal control of end-user energy storage," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 789–797, 2013.

[6] L. Huang, J. Walrand, and K. Ramchandran, "Optimal demand response with energy storage management," *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 61–66, 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6485960

[7] Y. Xu and L. Tong, "On the value of storage at consumer locations," in *PES General Meeting— Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.

[8] L. Schmidt and A. Thomas; Ligi, *GM, ABB Demonstrate Chevrolet Volt Battery Reuse Unit*. http://media.gm.com/, 2012.

[9] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[10] E. news, *Current Lithium Ion Battery Prices*. http://www.energystoragenews.com/Current%20Lithium%20Ion%20Battery%20Prices.html, 2014.

[11] S. G. C. Committee, "Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," The Smart Grid Interoperability Panel, Tech. Rep., 2014. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7628r1

[12] P. Koopman, "Embedded system security," *Computer*, vol. 37, no. 7, pp. 95–97, 2004.

[13] A. G. Illera and J. V. Vidal, "Lights Off! The Darkness of the Smart Meters," 2014. [Online]. Available: https://youtu.be/Z_y_vjYtAWM

[14] SecureState, "Termineter," 2015. [Online]. Available: https://github.com/securestate/termineter

[15] R. Sarfi, B. D. Green, and J. Simmins, "AMI Network (AMI Head-End to/from Smart Meter)," 2011.

[16] Silver Springs Network, "How Utilities Can Capitalize on the Consumerization of Demand Response," Silver Spring Networks, Tech. Rep., 2013. [Online]. Available: http://www.silverspringnet.com/wp-content/uploads/silverspring-whitepaper-dsm-2.pdf

[17] Technical Working Group 1, "Electric Sector Failure Scenarios and Impact Analyses," National Electric Sector Cybersecurity Organization Resource (NESCOR), Tech. Rep., 2013.

[18] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," pp. 445–487, 2005.

[19] S. Jajodia, S. Noel, and B. O'Berry, "Topological analysis of network attack vulnerability," in *Managing Cyber Threats*, 2005, pp. 247–266. [Online]. Available: http://link.springer.com/chapter/10.1007/0-387-24230-9_9

[20] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *2011 IEEE GLOBECOM Workshops, GC Wkshps 2011*, 2011, pp. 1162–1167.

[21] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Ccs*, vol. 14, no. 1, pp. 1–33, 2009.

[22] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[23] F. F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," in *IEEE SmartGridComm*, 2010, pp. 327–332. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622064

[24] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 238–243, 2010.

[25] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 232–237, 2010.

[26] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, 2011, pp. 190–195.

[27] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2011, pp. 1932–1935.

[28] L. Yang, X. Chen, J. Zhang, H. V. Poor, and A. Motivation, "Optimal Privacy-Preserving Energy Management for Smart Meters," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 513–521, 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6848142

[29] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.

[30] Z. Huang, T. Zhu, Y. Gu, D. Irwin, A. Mishra, and P. Shenoy, "Minimizing electricity costs by sharing energy in sustainable microgrids," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings*. ACM, 2014, pp. 120–129.

[31] I. Atzeni, L. G. Ordóñez, G. Scutari, D. P. Palomar, and J. R. Fonollosa, "Demand-side management via distributed energy generation and storage optimization," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 866–876, 2013.

[32] G. E. Monahan, N. C. Petruzzi, and W. Zhao, "The dynamic pricing problem from a newsvendor's perspective," *Manufacturing & Service Operations Management*, vol. 6, no. 1, pp. 73–91, 2004.

[33] C. Chen, L. He, P. Venkitasubramaniam, S. Kishore, and L. V. Snyder, "Achievable Privacy in Aggregate Residential Energy Management Systems," *Journal of Energy Engineering*, vol. 141, no. 1, p. B4014007, 2014.

[34] J. Yao and P. Venkitasubramaniam, "The Privacy Analysis of Battery Control Mechanisms in Demand Response: Revealing State Approach and Rate Distortion Bounds," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2417–2425, 2015.

[35] L. X. L. Xie, Y. M. Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 226–231, 2010.

[36] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, pp. 1907–1914.

[37] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, 2013.

[38] K. C. Divya and J. Østergaard, "Battery energy storage technology for power systemsAn overview," *Electric Power Systems Research*, vol. 79, no. 4, pp. 511–520, 2009.

[39] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2005.

[40] P. R. Kumar and P. Varaiya, *Stochastic Systems: Estimation, Identification and Adaptive Control*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1986.

[41] G. F. Lawler and V. Limic, "Random Walk : A Modern Introduction," *Science*, vol. 123, pp. 1–289, 2010. [Online]. Available: http://ebooks.cambridge.org/ref/id/CBO9780511750854

[42] P. Vontobel, "A generalized Blahut-Arimoto algorithm," *IEEE International Symposium on Information Theory, 2003. Proceedings.*, p. 53, 2003. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1228067

[43] J. Z. Kolter and M. J. Johnson, "REDD : A Public Data Set for Energy Disaggregation Research," *SustKDD workshop*, vol. xxxxx, no. 1, pp. 1–6, 2011. [Online]. Available: http://users.cis.fiu.edu/ lzhen001/activities/KDD2011Program/workshops/WKS10/doc/SustKDD3.pdf

[44] N. Y. I. S. Operator, *Real-Time LBMP - Zonal*. http://www.nyiso.com/, 2014.

[45] K. Miettinen, *Nonlinear Multiobjective Optimization*, ser. International Series in Operations Research & Management Science. Springer US, 1999. [Online]. Available: http://books.google.com/books?id=ha_zLdNtXSMC

[46] D. P. Bertsekas, D. P. Bertsekas, D. P. Bertsekas, and D. P. Bertsekas, *Dynamic programming and optimal control*. Athena Scientific Belmont, MA, 1995, vol. 1, no. 2.

[47] R. Durrett, *Probability: theory and examples*. Cambridge university press, 2010.

[48] S. V. Nagaev, "Large deviations of sums of independent random variables," *The Annals of Probability*, pp. 745–789, 1979.

Biography

Jiyun Yao was born on October 6th, 1990 in Hubei, China. He attended The No.1 Middle School Affiliated To Central China Normal University in Hubei. He has received his Bachelor of Engineering in Electronic Engineering from Tsinghua University in 2012. Upon completion of his bachelor studies, he joined Lehigh University to pursue his PhD in Electrical Engineering, under the supervision of Prof. Parv Venkitasubramaniam. His Primary research interests include security and privacy in cyber physical systems, signal processing, optimization and control. He is also a knowledge seeker and a outdoor sport enthusiast.

Curriculum Vitae

Jiyun Yao

(484) 860-0961 goodboyyjy@gmail.com jiy312@lehigh.edu
15 Duh Dr. Apt 232 Bethlehem, PA, 18015

Education

- **Lehigh University** **Bethlehem, PA**

  Department of Electrical and Computer Engineering Sep 2012 - Present

  – *Ph.D.* in Electrical Engineering, Expected: May 2017, GPA: 3.77/4.0
  Research Area: Security of cyber-physical systems; Privacy protection in data collection and distribution; Anonymous network

  – *M.S.* in Electrical Engineering, May 2015, GPA: 3.76/4.00
  Relevant Courses: Adv Computer Architecture, Data Networks, Convex Optimization, Advanced Algorithm, Stochastic Control, Cryptography and Network Security

- **Tsinghua University** **Beijing, China**

  Department of Electronic Engineering Sep 2008 - July 2012

  – *B.E.* in Electronic Information Science and Technology, July 2012, GPA: 85.0/100

Technical Skills

- Programming Languages: Java, Python, C/C++, Matlab
- Operating Systems: Windows, Linux, Mac OS
- Optimization and Control Toolboxes: Markovian Decision Processes (MDP) Toolbox, Control System Toolbox, Convex Optimization(CVX) Toolbox, Linear\Quadratic Optimization Toolbox

---

Work Experience

- **Cyber Security Analysis in Distributed Energy Resource (DER) System**

  Argonne National Laboratory

  Research Aide May - Aug 2016

- Built the graph theoretical model for DER communication network with integration of DER physical properties
- Implemented a linear time algorithm for computing biconnected components and cut-points
- Developed a heuristic algorithm of padding communication links to build a biconnected DER communication network with delay constraint

---

Research Experience

- **Quantitative Risk Analysis of Demand Side Management (DSM) Misuse and Attacks**

  Lehigh University

  Research Assistant — Nov 2015 - Present

  - Built the model for Advanced Metering Infrastructure network compatible with state estimation technology
  - Implemented the algorithm to locate the network topological vulnerabilities against stealthy hacking

- **Centralized and Distributed Control Mechanisms of Multi-Users Battery Sharing**

  Lehigh University

  Research Assistant — Dec 2014 - Present

  - Discovered and proved the threshold strategy for optimal centralized multi-user battery sharing
  - Reduced the dynamic centralized battery management to linear programming and its implementation
  - Built a multi-player general sum stochastic game model for competitive multi-user battery sharing
  - Proved that the optimal centralized multi-user battery sharing is an equilibrium of the game

- **Privacy of Metering Data Collection in Demand Response**

  Lehigh University

  Research Assistant — May 2013 - Dec 2014

  - Compared different privacy metrics for metering data collection including Shannon's entropy, differential privacy and successful estimation probability

- Built the privacy leakage model for real-time metering using Shannon's entropy as privacy metric
- Discovered the method to reduce the acausal observation-privacy relation to causal and formulated the problem with the Partially Observable Markov Decision Process (POMDP)
- Developed an approximation algorithm to determine the tradeoff between privacy and cost savings of the battery and proved the convergence to optimality

- **Radar Imaging based on Compressive Sensing**
  Tsinghua University
  Student Researcher Jul 2011 - Jul 2012
  - Implemented LASSO algorithm for compressive sensing for 2-D radar image
  - Developed a novel method for the focusing of raw data in the framework of inverse synthetic aperture radar
- **Virtual Mouse and Keyboard Java Application on Feature Phone using Bluetooth**
  Tsinghua University
  Sole Developer May - Aug 2010
  - Developed a Java ME program for MOTO V3 cell phone and a Java program for Windows to build a Bluetooth connection between phone and PC
  - Realized keyboard control and adaptive mouse control using the cell phone
  - A journal paper published in Chinese

Extracurricular Experience

- **Teaching Assistant** Lehigh University
  ECE108 - Signals and Systems Sep - Dec 2015
- **Google Code Jam, 2016**
  Advanced to Round 2, Rank: 1205 Apr - May 2016

Journal Papers

1. J. Yao and P. Venkitasubramaniam, "The Privacy Analysis of Battery Control Mechanisms in Demand Response: Revealing State Approach and Rate Distortion Bounds," in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2417-2425, Sept. 2015.

2. P. Venkitasubramaniam, J. Yao and P. Pradhan, "Information-Theoretic Security in Stochastic Control Systems," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1914-1931, Oct. 2015.

3. J. Yao and P. Venkitasubramaniam, "Privacy Aware Stochastic Games of Distributed End-user Energy Storage Sharing," submitted to IEEE Transactions on Signal and Information Processing over Networks.

4. J. Yao, P. Venkitasubramaniam, S. Kishore, L. Snyder and R. Blum, "Malicious Data Injection Attack On Demand Side Management System" in preparation.

Conference Papers

1. J. Yao and P. Venkitasubramaniam, "Maximizing Privacy In Variable Bit Rate Coding," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 2959-2963.

2. J. Yao and P. Venkitasubramaniam, "On The Privacy-Cost Tradeoff Of An In-Home Power Storage Mechanism," Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on, Monticello, IL, 2013, pp. 115-122.

3. J. Yao and P. Venkitasubramaniam, "On The Privacy-Cost Tradeoff Of Battery Control Mechanisms In Demand Response: Selective Information Protection." Proc. NILM Workshop. 2014.

4. J. Yao and P. Venkitasubramaniam, "Optimal End User Energy Storage Sharing In Demand Response," 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, 2015, pp. 175-180.

5. J. Yao and P. Venkitasubramaniam, "Stochastic Games Of End-User Energy Storage Sharing." Decision and Control (CDC), 2016 IEEE 55th Conference on. IEEE, 2016.

6. J. Yao, P. Venkitasubramaniam, S. Kishore, L. Snyder and R. Blum, "Network Topology Risk Assessment Of Stealthy Cyber Attacks On Advanced Metering Infrastructure Networks" Information Science and Systems (CISS), 2016 Annual Conference on. IEEE, 2016..

Academic Honors

- Awarded P.C. Rossin Doctoral Fellowship in P.C. Rossin College of Engineering at Lehigh University in 2015.

- Awarded Gotshall Fellowship in the Department of ECE at Lehigh University in 2014.
- Awarded NSF Scholarship at IEEE North American School of Information Theory in 2014.
- Awarded Dean's Research Assistantship in the Department of ECE at Lehigh University in 2012.
- Received Second Prize of Tsinghua University Challenge Cup- Extracurricular Technological Innovation at Tsinghua University in 2010.