UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Departament de Teoria del Senyal i Comunicacions

CTTC
Centre Tecnològic de Telecomunicacions de Catalunya

Privacy-Preserving Energy Management Techniques and Delay-Sensitive Transmission Strategies for Smart Grids

Ph.D. Thesis

By

Onur Tan

Submitted to the Universitat Politècnica de Catalunya (UPC)
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Barcelona, June 2016

Supervised by Dr. Deniz Gündüz and Dr. Jesús Gómez Vilardebó
Ph.D. program on Signal Theory and Communications

A esta etapa de mi vida

This work has been supported by the Spanish Government under the grant BES-2011-048206 and by the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC) under the Ph.D. scholarship program.

Abstract

The smart grid (SG) is the enhancement of the traditional electricity grid that allows bidirectional flow of electricity and information through the integration of advanced monitoring, communication and control technologies. With these technologies, the SG is expected to yield efficiency, reliability and robustness in generation, transmission and distribution of energy, as well as to reduce costs and carbon emissions. In this thesis, we focus on important design problems affecting particularly two critical enabling components of the SG infrastructure that facilitate these monitoring and communication capabilities: smart meters (SMs) and wireless sensor networks (WSNs).

SMs measure the energy consumption of the users and transmit their readings to the utility provider in almost real-time. Fine-grained SM readings enable real-time optimization of load management. However, possible misuse of SM readings raises serious privacy concerns for the users. The challenge is thus to design techniques that can increase the privacy of the users while maintaining the critical monitoring and control capabilities SMs provide. Demand-side energy management (EM), achieved thanks to the utilization of storage units and alternative energy sources, has emerged as a potential technique to tackle this challenge.

WSNs consist of a large number of low power sensor nodes, which monitor physical parameters and transmit their measurements to control centers (CCs) over wireless links. CCs utilize these measurements to reconstruct the system state. For the reliable and efficient management of the SG, near real-time and accurate reconstruction of the system state at the CC is crucial. Thus, low complexity delay-constrained transmission strategies, which enable sensors to accurately transmit their measurements to CCs, should be investigated rigorously.

To address these challenges, this dissertation investigates and designs privacy-preserving EM techniques for SMs and delay-constrained transmission strategies for WSNs. The proposed EM techniques provide privacy to SM users while maintaining the operational benefits SMs provide. On the other hand, the proposed transmission strategies enable WSNs to meet low latency transmission requirements, which in turn, facilitate real-time and accurate state

reconstruction; and hence, the efficient and robust management of the SG.

First, we consider an SM system with energy harvesting and storage units. Representing the system with a discrete-time finite state model, we study stochastic EM policies from a privacy-energy efficiency trade-off perspective, where privacy is measured by information leakage rate and energy efficiency is measured by wasted energy rate. We propose EM policies that take stochastic output load decisions based on the harvested energy, the input load and the state of the battery. For the proposed policies, we characterize the fundamental trade-off between user's privacy and energy efficiency.

Second, we consider an SM system with a storage unit. Considering a discrete-time power consumption and pricing model, we study EM policies from a privacy-cost trade-off perspective, where privacy is measured by the load variance as well as mutual information between the input and output loads. Assuming non-causal knowledge of the power demand profile and prices, we characterize the optimal EM policy based on the solution of an optimization problem. Then, assuming that the power demand profile is known only causally, we obtain the optimal EM policy based on dynamic programming, and also propose a low complexity heuristic policy inspired from the optimal offline policy. For the proposed policies, we characterize the trade-off between user's privacy and energy cost.

Finally, we consider the problem of transmitting delay-sensitive sensor measurements for state reconstruction in a SG. We study the delay-constrained linear transmission (LT) of composite Gaussian measurements from a sensor to a CC over a point-to-point fading channel. Assuming that the channel state information (CSI) is known by both the encoder and decoder, we propose the optimal LT strategy in terms of the average mean-square error (MSE) distortion under a strict delay constraint, and two LT strategies under general delay constraints. Assuming that the CSI is known only by the decoder, we propose the optimal LT strategy in terms of the average MSE distortion under a strict delay constraint.

Resum

La xarxa d'energia intel·ligent, en anglès Smart Grid (SG), és la millora de la xarxa elèctrica tradicional. La SG permet el flux bidireccional d'informació i incorpora tecnologies avançades de supervisió, comunicació i control per a la millor gestió de la xarxa. Amb aquestes tecnologies, la SG pretén incrementar l'eficiència, confiabilitat i robustesa de la generació, transmissió i distribució de l'energia, així com reduir els costos i les emissions de gasos d'efecte hivernacle. En aquesta tesi, ens enfoquem en les diferents problemàtiques associades al disseny de dos dels components més crítics de la infraestructura de la SG i responsables, en gran part, de les capacitats de supervisió i comunicació d'aquesta: els mesuradors de consum intel·ligents, en anglès Smart Meters (SMs), i les xarxes de sensors sense fils, en anglès Wireless Sensor Networks, (WSNs).

Els SMs mesuren el consum d'energia dels usuaris i transmeten les seves mesures al proveïdor de servei gairebé en temps real. L'alta granularitat amb la qual els SM obtenen aquesta informació permet l'optimització en temps real de la gestió de càrrega a la xarxa. No obstant això, el possible mal ús d'aquestes mesures planteja preocupacions greus en quant a la privacitat dels usuaris. El desafiament és, per tant, dissenyar tècniques que puguin augmentar la privadesa dels usuaris mantenint les capacitats crítiques de supervisió i control que proveeixen els SMs. Una solució tecnològica a aquest desafiament és el disseny de sistemes de gestió d'energia, en anglès Energy Management (EM), intel·ligents compostos per dispositius d'emmagatzematge i generació alternativa d'energia.

Les WSNs es componen d'un gran nombre de sensors de baixa potència, que mesuren paràmetres físics i transmeten les seves mesures als centres de control (CCs) mitjançant enllaços sense fils. Els CCs utilitzen aquestes mesures per estimar l'estat del sistema. Per a una gestió eficient i fiable de la SG, una bona reconstrucció de l'estat del sistema en temps real és crucial. Per això, cal investigar estratègies de transmissió per a aquestes xarxes de sensors amb estrictes requisits de complexitat i limitacions de latència.

Amb l'objectiu d'afrontar aquests desafiaments, aquesta tesi doctoral investiga i dissenya,

d'una banda, tècniques d'EM per preservar la privacitat de les dades procedents dels SMs, i d'altra banda, estratègies de transmissió per WSNs amb limitacions de latència. Les tècniques d'EM propostes proporcionen privacitats als consumidors d'energia mantenint els beneficis operacionals per la SG. Així mateix, les estratègies de transmissió proposades permeten a les WSNs satisfer els requisits de baixa latència necessaris per a la reconstrucció precisa de l'estat de la xarxa en temps real; i per tant, la gestió eficient i robusta de la SG.

En primer lloc, considerem el disseny d'un sistema d'EM compost per un SM i una unitat d'emmagatzematge i generació d'energia renovable. Representant el sistema amb un model d'estats finits i de temps discret, estudiem polítiques estocàstiques d'EM. En particular, proposem polítiques d'EM que prenen decisions estocàstiques sobre la càrrega sol·licitada la xarxa en funció de l'energia recol·lectada, la demanda dels usuaris i l'estat de la bateria. Per a les polítiques propostes, caracteritzem la relació fonamental existent entre la privadesa i l'eficiència d'energia de l'usuari, on la privacitat es mesura mitjançant la taxa de fugida d'informació i l'eficiència d'energia es mesura mitjançant la taxa d'energia perduda.

En segon lloc, considerem el disseny d'un sistema EM compost per un SM i una unitat d'emmagatzematge. Considerant un model de temps discret per al consum i el preu de l'energia, estudiem en aquest cas la relació existent entre la privacitat el cost de l'energia, on la privacitat es mesura per la variació de la càrrega, així com mitjançant la informació mútua. En primer lloc, suposant que la corba de la demanda d'energia i els preus són coneguts per endavant, caracteritzem la política d'EM òptima. En segon lloc, suposant que la demanda d'energia és coneguda només per al temps actual, obtenim la política d'EM òptima mitjançant programació dinàmica, i proposem una política heurística de baixa complexitat. Per a les polítiques propostes, caracteritzem la relació existent entre la privacitat i el cost d'energia de l'usuari.

Finalment, considerem el problema d'estimar l'estat de la SG mitjançant la transmissió de les mesures dels sensors amb limitacions estrictes de latència. En particular, considerem el disseny d'estratègies de transmissió lineal (LT) de mesures Gaussianes compostes des d'un sensor a un CC sobre un canal punt a punt amb esvaïments. Suposant que la informació de l'estat del canal (CSI) és coneguda tant pel transmissor com pel receptor, proposem l'estratègia de LT òptima en termes de la distorsió d'error quadràtic mitjà (MSE) sota una restricció de latència estricta. A més, proposem dues estratègies de LT per a restriccions de latència arbitràries. Finalment, suposant que la CSI és coneguda només en el receptor, proposem l'estratègia de LT òptima en termes de la distorsió de MSE sota una restricció de latència estricta.

Resumen

La red de energía inteligente, en inglés Smart Grid, (SG) es la mejora de la red eléctrica tradicional. La SG permite el flujo bidireccional de información y incorpora tecnologías avanzadas de supervisión, comunicación y control para la mejor gestión de la red. Con estas tecnologías, la SG pretende incrementar la eficiencia, confiabilidad y robustez de la generación, transmisión y distribución de la energía, así como reducir los costes y las emisiones de gases de efecto invernadero. En esta tesis, nos enfocamos en las diferentes problemáticas asociadas al diseño de dos de los componentes más críticos de la infraestructura de la SG y responsables, en gran medida, de las capacidades de supervisión y comunicación de esta: los medidores inteligentes, en inglés Smart Meters, (SMs) y las redes de sensores inalámbricos, en inglés Wireless Sensor Networks, (WSNs).

Los SMs miden el consumo de energía de los usuarios y transmiten sus medidas al proveedor de servicio casi en tiempo real. La alta granularidad con la que los SM obtienen esta información permite la optimización en tiempo real de la gestión de carga en la red. Sin embargo, el posible mal uso de estas medidas plantea preocupaciones graves en cuanto a la privacidad de los usuarios. El desafío es, por lo tanto, diseñar técnicas que puedan aumentar la privacidad de los usuarios manteniendo las capacidades críticas de supervisión y control que proveen los SMs. Una solución tecnológica a este desafío es el diseño de sistemas de gestión de energía, en inglés Energy Management (EM), inteligentes compuestos por dispositivos de almacenamiento y generación alternativa de energía.

Las WSNs se componen de un gran número de sensores de baja potencia, que miden parámetros físicos y transmiten sus mediciones a los centros de control (CCs) mediante enlaces inalámbricos. Los CCs utilizan estas mediciones para estimar el estado del sistema. Para una gestión eficiente y fiable de la SG, una buena reconstrucción del estado del sistema en tiempo real es crucial. Por ello, es preciso investigar estrategias de transmisión para estas redes de sensores con estrictos requisitos de complejidad y limitaciones de latencia.

Con el objetivo de afrontar estos desafíos, esta tesis doctoral investiga y diseña, por un

lado, técnicas de EM para preservar la privacidad de los datos procedentes de los SMs, y por otro lado, estrategias de transmisión para WSNs con limitaciones de latencia. Las técnicas de EM propuestas proporcionan privacidad a los consumidores de energía manteniendo los beneficios operacionales para la SG. Así mismo, las estrategias de transmisión propuestas permiten a las WSNs satisfacer los requisitos de baja latencia necesarios para la reconstrucción precisa del estado de la red en tiempo real; y por lo tanto, la gestión eficiente y robusta de la SG.

En primer lugar, consideramos el diseño de un sistema de EM compuesto por un SM y una unidad de almacenamiento y generación de energía renovable. Representando el sistema con un modelo de estados finitos y de tiempo discreto, estudiamos políticas estocásticas de EM. En particular, proponemos políticas de EM que toman decisiones estocásticas acerca de la carga demandada a la red en función de la energía recolectada, la demanda de los usuarios y el estado de la batería. Para las políticas propuestas, caracterizamos la relación fundamental existente entre la privacidad y la eficiencia de energía del usuario, donde la privacidad se mide mediante la tasa de fuga de información y la eficiencia de energía se mide mediante la tasa de energía perdida.

En segundo lugar, consideramos el diseño de un sistema EM compuesto por un SM y una unidad de almacenamiento. Considerando un modelo de tiempo discreto para el consumo y el precio de la energía, estudiamos en este caso la relación existente entre la privacidad y el coste de la energía, donde la privacidad se mide por la variación de la carga, así como la información mutua. En primer lugar, suponiendo que el perfil de la demanda de energía y los precios son conocidos de antemano, caracterizamos la política de EM óptima. En segundo lugar, suponiendo que la demanda de energía es conocida sólo para el tiempo actual, obtenemos la política de EM óptima mediante programación dinámica, y proponemos una política heurística de baja complejidad. Para las políticas propuestas, caracterizamos la relación existente entre la privacidad y el coste de energía del usuario.

Finalmente, consideramos el problema de estimar el estado de la SG mediante la transmisión de las mediciones de los sensores con limitaciones estrictas de latencia. En particular, consideramos el diseño de estrategias de transmisión lineal (LT) de mediciones Gaussianas compuestas desde un sensor a un CC sobre un canal punto a punto con desvanecimientos. Suponiendo que la información del estado del canal (CSI) es conocida tanto por el trasmisor como por el receptor, proponemos la estrategia de LT óptima en términos de la distorsión de error cuadrático medio (MSE) bajo una restricción de latencia estricta. Además, proponemos dos estrategias de LT para restricciones de latencia arbitrarias. Suponiendo que la CSI es conocida sólo en el receptor, proponemos la estrategia de LT óptima en términos de la distorsión de MSE bajo una restricción de latencia estricta.

Acknowledgements

I remember the day, when I was notified of being granted a research position for pursuing a Ph.D. degree in beautiful Barcelona. This was a beginning of a new journey in my life. Time flies and every journey comes to an end. Hence, I now want to unveil some names, who took part in this journey with me, and thank them here.

First and foremost, I want to express my heartfelt gratitude to my supervisors, Dr. Deniz Gündüz and Dr. Jesús Gómez Vilardebó, for their valuable guidance and continuous encouragement, and for being always supportive and understanding throughout this tiresome Ph.D. process. I would especially like to thank Deniz for giving me this opportunity. Over the course of this long journey, Deniz and Jesús, have provided guidance and advice whenever I needed. I'm grateful to them that they have shared their knowledge and experience, which substantially helped me form this thesis.

I would also like to thank Dr. Iñaki Esnaola, Dr. Georgios Kalogridis and Dr. Luis Alonso for reading and reviewing my thesis, and serving on my comittee.

I want to thank all my colleagues at CTTC and Imperial College London for sharing part of this Ph.D. process. Special thanks to Miquel, Jessica, Pol, Iñaki, Laia, Laura, Arturo, Maria, Morteza for sharing the ups and downs of this process.

Next in line are my friends who made my life bearable and even more joyful in Barcelona. I owe my thanks to Pablo, Mete, Ethem, John Fredy, Belen, Kutlu, Alaz, Pelin for sharing a part of your lives with me and for your friendship.

Carmen, quiero agradecerte por todo el apoyo que me diste a lo largo de estos años y por hacerme sentir como en casa en Barcelona cada vez que lo necessitaba.

Finally, I thank my parents, Filiz and Cahit, and my sister, Merve, my grandmothers and grandfathers, for their endless love, encouragement and support throughout all my life. They have always been a light to the way that I paved for myself. I love you all!

Barcelona, June 2016

List of Publications

Journals

[J1] **O. Tan**, J. Gómez-Vilardebó and D. Gündüz, "Privacy-cost trade-offs in demand-side management with storage," *submitted to IEEE Transactions on Information Forensics and Security*, 2016.

[J2] **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Linear transmission of composite Gaussian measurements over a fading channel under delay constraints," *IEEE Transactions on Wireless Communications*, Vol. 15, No. 6, pp. 4335 - 4347, May 2016.

[J3] **O. Tan**, D. Gündüz and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications (J-SAC)*, Vol. 31, No. 7, pp. 1331 - 1341, July 2013.

International Conferences

[C1] **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Optimal privacy-cost trade-off in demand-side management with storage," in *Proceedings of the IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Stockholm, Sweden, June-July 2015, pp. 370–374.

[C2] **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Delay constrained linear transmission of a mixture of Gaussian measurements over a fading channel," in *Proceedings of the IEEE International Conference on Communications (ICC)*, London, UK, June 2015, pp. 4107–4112.

[C3] **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Delay constrained linear transmission of random state measurements," in *Proceedings of the IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruña, Spain, June 2014, pp. 53–56.

[C4] D. Gündüz, J. Gómez-Vilardebó, **O. Tan** and H. V. Poor, "Information theoretic privacy for smart meters," in *Proceedings of the Information Theory and Applications Workshop (ITA)*, San Diego, CA, USA, Feb. 2013, pp. 1–7.

[C5] **O. Tan**, D. Gündüz and H. V. Poor, "Smart meter privacy in the presence of energy harvesting and storage devices," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Tainan City, Taiwan, Nov. 2012, pp. 664–669.

Master Thesis

- **O. Tan**, "Terrain profile estimation over a synthetic terrain by using pulse-doppler radar," Supervisor: Prof. Dr. Orhan Arıkan (Bilkent University), June 2010.

Contents

List of Figures

List of Tables

List of acronyms

AC	Alternating Current
AMI	Advanced Metering Infrastructure
AWGN	Additive White Gaussian Noise
CC	Control Center
CSI	Channel State Information
DP	Dynamic Programming
EH	Energy Harvesting
EM	Energy Management
EMI	Electro-Magnetic Interference
EMU	Energy Management Unit
EV	Electric Vehicle
FSM	Finite State Model
i.i.d.	independent and identically distributed
KKT	Karush Kuhn Tucker
LCD	Liquid Crystal Display
LLB	Linear Transmission Lower Bound
LT	Linear Transmission
LTHM	Linear Transmission Scheme with Hard Matching

LTSM Linear Transmission Scheme with Soft Matching

MB Measurement Buffer

MMSE Minimum Mean-Square Error

MSE Mean-Square Error

NALM Non-Intrusive Appliance Load Monitoring

NILL Non-Intrusive Load Leveling

NIST U.S. National Institute for Standards and Technology

RB Rechargeable Battery

r.v. Random Variable

SG Smart Grid

SM Smart Meter

SNR Signal to Noise Ratio

TB Transmission Buffer

TLB Theoretical Lower Bound

TS Time Slot

TTP Trusted Third Party

TV Television

UP Utility Provider

WSN Wireless Sensor Network

Chapter 1

Introduction

1.1 Motivation

Technology has been evolving rapidly over the past decades, leading to significant changes in our lives and posing many new challenges to be tackled. One of the significant challenges to be addressed in the 21th century will be the upgrading of the conventional electrical grid [1–4]. The electrical grid is an interconnected network of power plants, transmission and distribution lines, substations, transformers and more, for delivering the electricity from suppliers to a myriad of consumers. However, the grid with its aging infrastructure necessitates to undergo a profound change to meet the actual requirements of the information age efficiently [5–8].

With a rapidly growing population, there has been a huge growth and variation in electricity demand over the past decades, which has further increased and varied the existing load on the grid infrastructure. According to the U.S. Department of Energy report, the electricity demand has been increasing perpetually by 2.5% per year over the last few decades [9]. The grid has difficulties in forecasting the changing conditions, diagnosing and responding to potential problems arising from the load growth and variation since it suffers from the lack of advanced and pervasive monitoring, communication and control capabilities. As a result, the grid has been facing serious problems, such as increased congestion, major blackouts, various system failures and their cascading effects, high cost energy generation, waste at peak time periods, and increased carbon emissions with massive damage to the environment and major impact to the climate change. The European Council has been discussing some of these problems, and has reported the paramount importance of reducing the greenhouse carbon emissions for the future of the world. All these factors have in turn encouraged governments to upgrade the existing grid so as to reduce carbon emissions and energy costs, provide energy efficiency and sustainability, reliability and robustness by 2020 [10]. Introducing alternative energy sources and energy storage devices into the user premises and the grid will significantly reduce the load

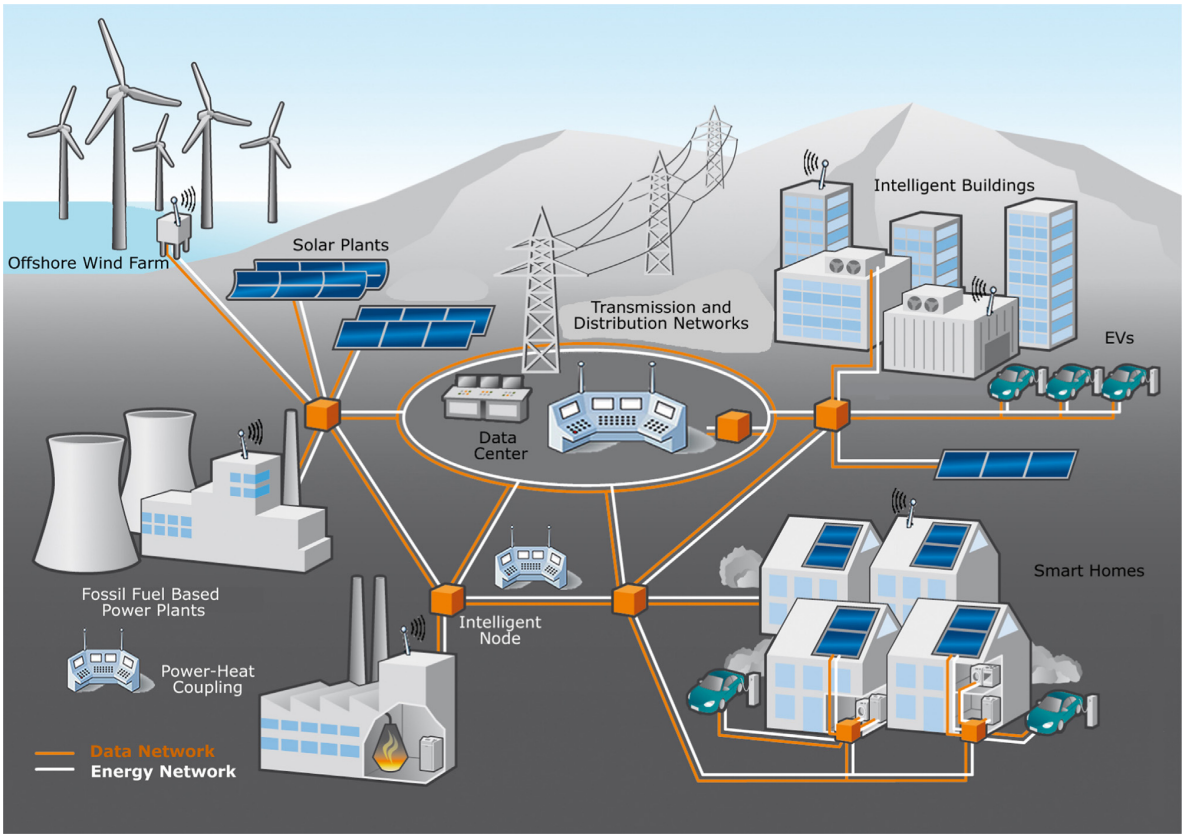


Figure 1.1: A depiction of the smart grid (SG) [16].

on the grid and play a key role for achieving these goals [11]. For instance, renewable energy sources can be integrated into the user premises through energy harvesting (EH) devices, which can harvest energy from ambient sources such as solar, thermal or wind, and reduce the users' dependence on the grid [12], [13]. Similarly, the users can become more involved in the grid operation through the usage of plug-in electric vehicles (EVs), hybrid and battery cars etc., which can be used for distributed energy storage on the distribution grid by means of their rechargeable batteries (RBs) [14]. Hence, all these suggest that new technologies for monitoring, management and control will need to be developed evolving conventional electrical grid into a more intelligent grid.

The smart grid (SG) is the next generation, modernized enhancement of the traditional power grid that allows bidirectional flow of electricity and information by the integration of computer, monitoring, communication and automation technologies [15]. As depicted in Fig. 1.1, the SG is composed of energy and data networks. To efficiently manage and control such a complex network and deliver its potential benefits, advanced and pervasive monitoring, metering and control technologies are essential. This in turn has prompted the deployment of emerging metering and monitoring technologies such as smart meter (SMs) and wireless sensor networks (WSNs).

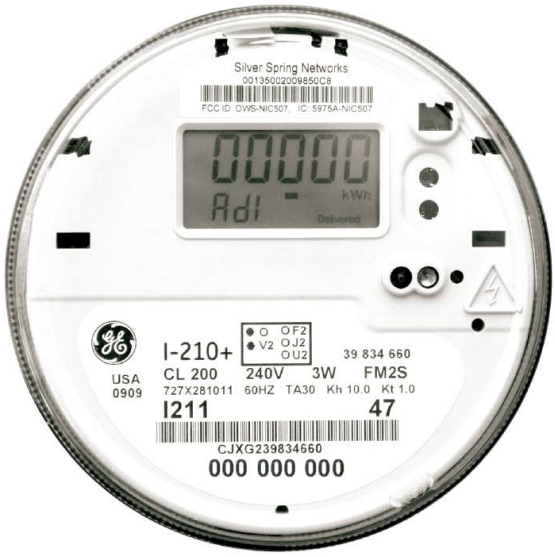


Figure 1.2: A commercial SM platform of General Electric.

1.1.1 Smart Meters (SMs)

SMs are metering and communication devices that measure the energy consumption of a user in a household and transmit their readings to the utility provider (UP) over wired or wireless links [17]. Currently, a typical SM reports the energy consumption readings to the UP every 15 minutes; however, the measuring frequency is expected to increase in the near future to provide near real-time energy consumption data to the UP. An example of a commercial SM platform produced by General Electric can be seen in Fig. 1.2. The communication infrastructure of SMs enable bidirectional transmission of data between the SM and the UP [17–19]. This allows the UP to closely monitor the grid load and manage user demands with the goal of providing potential benefits [20–22]. For instance, electricity supplier can support dynamic electricity pricing with incentive tariffs for the users and encourage the users to shift and/or reduce their demands at peak times with the promise of reducing their energy costs [23]. In this way, the users can get more involved in the grid operation. Accurate electricity bills can be generated in real-time based on fine-grained consumption data and provided to users through in-home display units as in the example of a display produced by British Gas shown in Fig. 1.3. This enables users to monitor their bills in real-time and manage their electricity consumption efficiently. Significant energy savings have been reported even solely based on the user's increased awareness of his/her real time energy consumption [24]. Besides, the UP can forecast the grid capacity by means of collected SM data, which allows the UP to do longer term energy generation contracts with low generation costs [25]. Furthermore, the UP can detect and prevent fraud attempts by analyzing aggregated consumption patterns through SMs [26]. Therefore, many governments in Europe and United States support the deployment of SMs at households. For example, the

Figure 1.3: An in-home display of British Gas.

U.K. government has already launched the installation of SMs at many households in Britain, with the goal of every home having an SM by 2020 [27].

Despite all potential benefits mentioned above, possible misuse of SM readings raises important privacy and security threats for the users [28–33]. Potential privacy and security vulnerabilities of SGs have been reported by the U.S. National Institute for Standards and Technology (NIST) [34], and specifically, advanced metering infrastructure (AMI) security requirements have been published in OpenSG [35]. According to these reports, SM data can be misused by authorized and non-authorized third parties. On the one hand, authorized third parties, such as energy companies may use SM data for marketing or advertising issues. Additionally, governments may require access to SM data for law enforcement purposes or criminal issues. On the other hand, non-authorized parties can access SM data through illegitimate methods such as hacking, and analyze fine-grained data by employing various privacy-invasive techniques. By doing so, non-authorized parties can extract and deduce private user activities, such as residential occupancy, personal behaviours, life-styles, preferences [36], and appliance usage patterns, such as detecting the television (TV) channel that is being watched [37]. Even the indication of illnesses or life-style changes of an individual can be inferred through long retention of SM data [28–30]. Hence, solid privacy assurances should be provided to users both at legal and technical levels. Regarding legislative frameworks of governments, there are guideline reports such as the one published by NIST [34]. However, there still lacks standardization for the development of robust privacy regulations and policies. For instance, the protection of personal information currently count on the rules of companies and regulators. This is overwhelmingly weak protection since these rules rely solely upon the honesty of all parties. Therefore, privacy regulations and policies should be considered more seriously in the near future. On the other hand, providing privacy assurances at the technical level is also very crucial. This gives rise

to an urgent need for studying and designing privacy-preserving technologies, that can provide solid and robust privacy assurances to users, as well as maintain the operational benefits SMs provide to the SG. Demand-side energy management (EM), achieved thanks to the utilization of storage units and alternative energy sources, is an emerging technique to tackle this challenge. Hence, these techniques should be investigated rigorously in the near future.

1.1.2 Wireless Sensor Networks (WSNs)

Another enabling technology for advanced monitoring and control of the SG is WSN [38–42]. As opposed to the traditional wired monitoring systems, which require high installation and maintenance costs for communication cables [43], WSNs bring significant benefits such as rapid deployment, low cost installation and maintenance of wireless sensor nodes [44]. To that end, WSNs have been deployed in the SG to monitor various physical parameters, such as voltage, current, active/reactive power values, and transmit their measurements to control centers (CCs) over wireless links. CCs exploit these measurements to reconstruct and update the system state. To enable the robust, reliable and efficient management of the grid, with rapid diagnosis and self-healing of potential system faults, near real-time and accurate reconstruction of the system state at the CC become critical. In this regard, wireless sensors should be able to realize near real-time, reliable and accurate transmission of their measurements to CCs.

Transmission of rich sources over wireless networks has been already enabled by recent advances in communication and hardware technology. For their applicability to the SG scenario, it's crucial to identify system limitations and performance metrics, and design wireless system that satisfies the end-to-end average distortion and delay requirements within the power constraint of the transmitter. In this context, low latency and low complexity are critical quality of service requirements that need to be met in the design of wireless transmission strategies for the SG [45], [46]. For instance, the U.S. Department of Energy identifies six major communication requirements for SG technologies in [47], and low latency is mentioned in five of them. All these suggest that the design of low complexity, delay-sensitive transmission strategies for WSNs is needed in order to provide advanced monitoring and control capabilities to SG, and enable, in turn, the robust and efficient management of the SG. Linear transmission (LT) emerges as an attractive strategy for this problem since it reduces both the delay and encoding complexity significantly; and accordingly limits the cost and energy requirements of the sensors. Hence, these strategies should be investigated thoroughly.

In summary, the study and design of privacy-preserving EM techniques for SMs are required in order to provide privacy assurances to SM users while maintaining the operational benefits SMs provide to the SG. In addition, delay-sensitive transmission strategies for WSNs

should be studied and designed so as to enable sensors to accurately transmit their measurements to CCs in near real-time, and facilitate, in turn, real-time and accurate state reconstruction; and hence, the robust and efficient management of the SG.

1.2 Dissertation Outline and Research Contributions

This dissertation investigates privacy-preserving EM techniques for SMs and delay-sensitive transmission strategies for WSNs. The proposed EM techniques aim at coping with privacy concerns of SM users while retaining the operational benefits SMs provide to the SG. On the other hand, the proposed transmission strategies aim at enabling WSNs to accommodate low complexity, low latency transmission requirements, and maintaining, in turn, the critical monitoring and control capabilities WSNs provide to the SG. The thesis is structured in six chapters. The current chapter motivates the conducted research and presents the outline and research contributions. Chapter 2 provides a brief state of the art on privacy-invasive and privacy-preserving techniques, as well as on LT strategies. The technical content of the dissertation is organized into three main chapters, namely, Chapters 3, 4 and 5. Chapters 3 and 4 focus on an SM system and study the fundamental trade-offs between privacy and energy efficiency, and privacy and energy cost, respectively. Chapter 5 considers the problem of transmitting delay-sensitive sensor measurements for state reconstruction in SG, and studies delay-constrained LT strategies in a point-to-point communication problem. Finally, Chapter 6 concludes the dissertation and points out some possible future research directions.

Chapter 3 studies privacy in an SM system from an information theoretic perspective in the presence of EH and storage units. Focusing on a discrete-time system model, we investigate stochastic battery policies at the energy management unit (EMU) based on the harvested energy, energy demand of the appliances and the state of the storage unit. We show that EH provides increased privacy by diversifying the energy source, while a storage device can be used to increase both the energy efficiency and the privacy of the user. For given input load and EH rates, which denote the probability of having one unit of energy demand and harvested energy, respectively, it is shown that there exists a trade-off between the information leakage rate, which is used to measure the privacy of the user, and the wasted energy rate, which is a measure of the energy-efficiency. The impact of the EH rate and the size of the storage device on this trade-off is also studied. For very sensitive applications, the impact of wasting of grid energy on fulfilling the increased privacy requirements of the user is also investigated. The main contributions of Chapter 3 are:

- We investigate stochastic EM policies that provide both privacy and energy efficiency to the user for an SM system with an EH device and an RB.

- For given input load and EH rates, we show that the proposed EM policies lead to an energy efficiency-privacy trade-off.
- We study the impact of EH rate on the energy efficiency-privacy trade-off, and show that the privacy of the user improves significantly as the EH rate increases. On the other hand, this also increases the amount of wasted energy.
- We numerically investigate the impact of the battery capacity on the information leakage rate, and show that the information leakage rate can significantly be reduced by increasing the RB capacity.
- For very sensitive applications, we show that even with a finite capacity RB, increased privacy can be achieved by wasting more energy from the grid.

The contributions of Chapter 3 were published in one journal publication [48] and two international conferences [49], [50]:

- **O. Tan**, D. Gündüz and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications (J-SAC)*, Vol. 31, No. 7, pp. 1331 - 1341, July 2013.
- D. Gündüz, J. Gómez-Vilardebó, **O. Tan** and H. V. Poor, "Information theoretic privacy for smart meters," in *Proceedings of the Information Theory and Applications Workshop (ITA)*, San Diego, CA, USA, Feb. 2013, pp. 1–7.
- **O. Tan**, D. Gündüz and H. V. Poor, "Smart meter privacy in the presence of energy harvesting and storage devices," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Tainan City, Taiwan, Nov. 2012, pp. 664–669.

Chapter 4 studies demand-side EM from a privacy-cost trade-off perspective for an SM system with an RB. Time-of-use pricing is considered, and privacy is measured as the variation of the output load from a fixed target value, namely, load variance. Assuming non-causal knowledge of the household's aggregate power demand profile and the electricity prices at the EMU, the privacy-cost trade-off is formulated as a convex optimization problem, and the optimal EM policy is characterized in the offline setting. Based on the necessary optimal conditions, a low complexity *backward water-filling algorithm* is proposed to compute the optimal EM policy. While the energy cost is reduced by requesting more energy when the prices are lower, privacy is achieved by a smoother output load. It is shown that both gains can be achieved simultaneously by exploiting an energy storage unit, while the actual privacy-cost

trade-off depends on the available storage capacity. Next, the problem is studied in the online setting assuming that the power demand profile is known to the EMU only causally, and the optimal EM policy is obtained numerically through dynamic programming (DP). Due to the high computational cost of DP, a low complexity heuristic EM policy with a performance close to the optimal online solution is also proposed based on the water-filling algorithm obtained in the offline setting. As an alternative, information theoretic leakage rate between the input and output load sequences is also evaluated, and it is shown to follow a similar trend as the load variance, which further supports the validity of the load variance as a measure of privacy. Finally, the privacy-cost trade-off, and the impact of the size of the storage unit on this trade-off are studied through numerical simulations using real SM data in both the offline and online settings. The main contributions of Chapter 4 are:

- We study EM policies that aim at providing both privacy and energy cost saving to the user for an SM system with an RB.
- Assuming that the user's power demands and the electricity prices are known non-causally at the EMU, we formulate the optimal privacy-cost trade-off in the offline setting as a convex optimization problem. We identify the structure of the optimal solution for this convex optimization problem and provide a backward water-filling algorithm for computing the optimal EM policy.
- Assuming that the user's power demands are known only causally at the EMU, we propose the optimal EM policy by means of DP solution. We also provide an efficient heuristic algorithm.
- We characterize the information leakage rate between the user's power demand profile and the SM readings, and show that it follows a similar trend as the load variance.
- We study the trade-off between the user's privacy and energy cost as well as the impact of the RB capacity on this trade-off for the proposed offline and online policies.

The contributions of Chapter 4 were published in one international conference [51] and were submitted for a journal publication [52]:

- **O. Tan**, J. Gómez-Vilardebó and D. Gündüz, "Privacy-cost trade-offs in demand-side management with storage," *submitted to IEEE Transactions on Information Forensics and Security*, 2016.

- **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Optimal privacy-cost trade-off in demand-side management with storage," in *Proceedings of the IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Stockholm, Sweden, June-July 2015, pp. 370–374.

Chapter 5 considers delay-constrained LT strategies for the transmission of composite Gaussian measurements over an additive white Gaussian noise (AWGN) fading channel under an average power constraint. If the channel state information (CSI) is known by both the encoder and decoder, the optimal LT scheme in terms of the average mean-square error (MSE) distortion is characterized under a strict delay constraint, and a graphical interpretation of the optimal power allocation strategy is presented. Then, for general delay constraints, two LT strategies are proposed based on the solution to a particular multiple measurements-parallel channels scenario. We show that the distortion decreases as the delay constraint is relaxed, and when the delay constraint is completely removed, both strategies achieve the optimal performance under certain matching conditions. If the CSI is known only by the decoder, the optimal LT strategy is derived under a strict delay constraint. The extension to general delay constraints is elusive. As a first step towards understanding the structure of the optimal scheme in this case, we show that for the multiple measurements-parallel channels scenario, any LT scheme that uses only a one-to-one linear mapping between measurements and channels is suboptimal in general. The main contributions of Chapter 5 are:

- We study delay-constrained LT strategies for the transmission of composite Gaussian measurements from a sensor to a CC over an AWGN fading channel. In a composite Gaussian source model, the source samples follow Gaussian distributions with different variance values. To the best of our knowledge, this source model has not been considered before in an LT framework.

- Assuming that both the encoder and decoder know the CSI, we characterize the optimal LT scheme under a strict delay constraint, and provide a graphical interpretation for the optimal power allocation scheme.

- We propose two LT strategies for arbitrary delay constraints, and show that the distortion decreases as the delay constraint is relaxed, and when the delay constraint is completely removed, both strategies achieve the optimal performance under certain matching conditions.

- Assuming that the CSI is known only at the decoder, we derive the optimal LT strategy under a strict delay constraint.

- We show that for the multiple measurements-parallel channels scenario, any LT scheme that uses only a one-to-one linear mapping between measurements and channels is sub-optimal in general.

The contributions of Chapter 5 were published in one journal publication [53] and two international conferences [54], [55]:

- **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Linear transmission of composite Gaussian measurements over a fading channel under delay constraints," *IEEE Transactions on Wireless Communications*, Vol. 15, No. 6, pp. 4335 - 4347, May 2016.
- **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Delay constrained linear transmission of a mixture of Gaussian measurements over a fading channel," in *Proceedings of the IEEE International Conference on Communications (ICC)*, London, UK, June 2015, pp. 4107–4112.
- **O. Tan**, D. Gündüz and J. Gómez-Vilardebó, "Delay constrained linear transmission of random state measurements," in *Proceedings of the IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruña, Spain, June 2014, pp. 53–56.

Chapter 2

State of the Art

This chapter is divided into three parts: while the first and second part give a brief overview of privacy-invasive and privacy-preserving techniques, respectively, the third part briefly overviews LT strategies.

2.1 Privacy-Invasive Techniques

2.1.1 Non-Intrusive Appliance Load Monitoring (NALM)

Non-intrusive appliance load monitoring (NALM) has been proposed as a set of techniques that analyze the aggregated power consumption data with the goal of identifying and tracking detailed appliance usage patterns in a household [56]. NALM techniques are called as non-intrusive since they only need to gather the aggregated power consumption data contrary to the intrusive techniques, which need to gather the power consumption data of individual appliances by connecting intrusive sensors to them. Hence, NALM techniques eliminate the need for deployment of expensive and intrusive sensors.

NALM techniques can be used for various purposes such as forecasting the load, detecting failures and enabling demand-side load management with the goal of reducing the energy demand. These potential benefits lead to further research in NALM techniques for extracting individual appliance signatures from the aggregated power consumption. Accordingly, the authors in [57] study the pattern recognition techniques in which energy consumption patterns of domestic appliances can be accurately identified from daily aggregated energy consumption taken at household's meter every 15 minutes. The authors in [58] present a feasibility study showing that the recognition and identification of a particular appliance from the aggregate current load is possible. The authors in [59] evaluate the performance of an energy monitoring system that recognizes active appliances based on their acoustic signatures, and provide device-

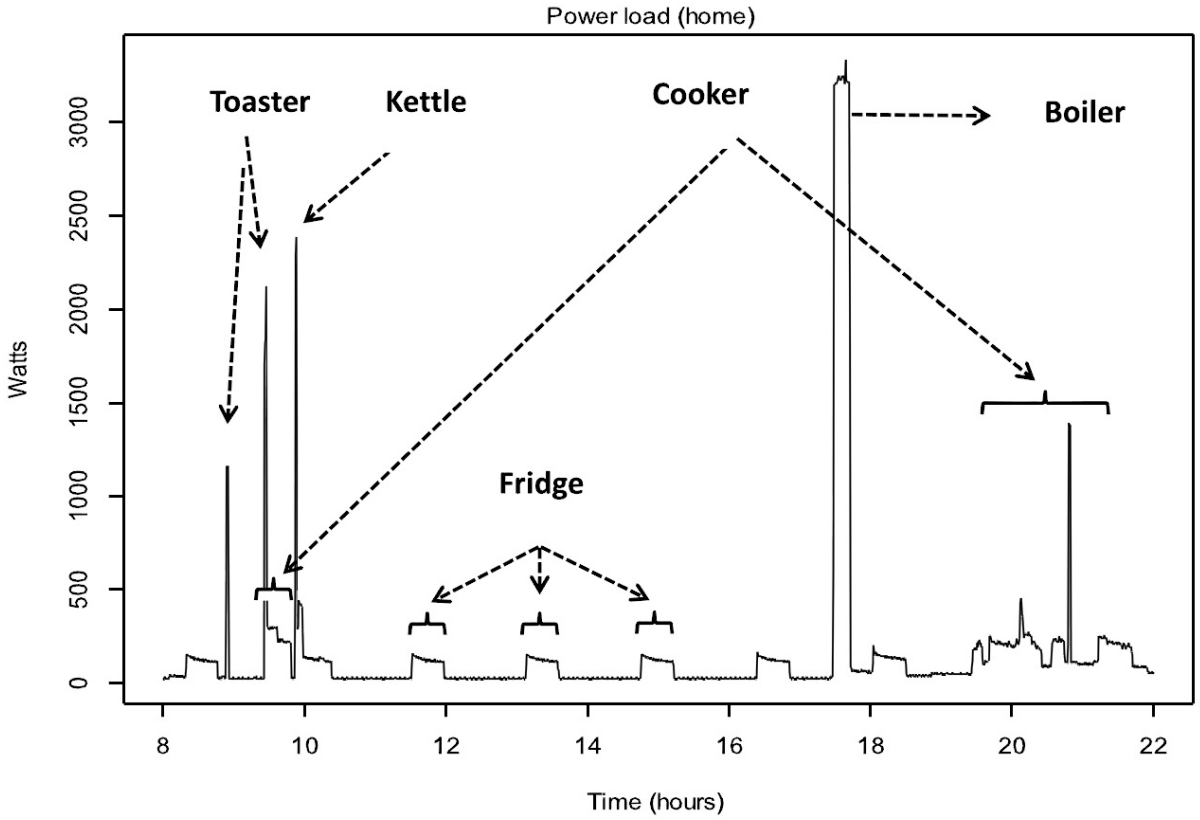


Figure 2.1: Appliance detection in an electricity demand profile obtained at a household with a time resolution of 30 seconds [5].

level power consumption profiles by using the correlation between the acoustic signatures and the overall power consumption data obtained from a meter. According to their experiments, the power consumption of individual appliances can be reported within a 10% margin.

To extract the trends of a power consumption signal, a data mining algorithm based on an empirical probability distribution is proposed in [60]. The authors consider two types of signals, namely, unprotected signals which are not protected, and protected signals which are protected by a specific privacy algorithm. The authors applied the proposed method both to unprotected and protected signals with the goal of analysing the operation of a set of appliances and evaluating the privacy. They consider different sampling frequencies from 30 seconds to 30 minutes, and observe that the privacy of personal behaviours can be exposed even in the presence of a low sampling rate. They observe that the specific privacy protection algorithm used for protecting the signal leads to a great variation in the empirical probability distribution of the protected signal compared to that of the unprotected signal. They use the proposed method in order to provide a better insight for the performance of the privacy protection algorithm.

The authors in [61] study the representation of load characteristics and construction of load taxonomy using the measured voltage and current waveforms of appliances in a household. They propose a taxonomy methodology, which constructs the load signatures as two

dimensional voltage-current trajectories, extracts shape features, and clusters the appliances by applying hierarchical clustering methods. Then, they compare their taxonomy methodology with the taxonomy methodologies based on the traditional power metrics, and observe that voltage-current trajectories reveal better results in classifying the loads.

An example of appliance detection in an aggregated power consumption data is given in Fig. 2.1 [5]. As it can be seen in the figure, active appliances with their unique power signatures can be detected and disaggregated from the total power consumption data. The potential benefits of NALM techniques can be provided through these extracted consumption signatures. However, the possible misuse of the extracted power consumption of individual appliances can raise privacy concerns. These concerns were first expressed by G.W. Hart in [62]. He claimed that NALM techniques could be potentially used as an adverse surveillance technique. For example, burglars can use NALM mechanisms in order to extract the time slots (TSs) in which the users are not at home, and can plan their burglaries.

2.1.2 Use-Mode Detection

Use-mode detection techniques go one step beyond and try to recognize the actual activities of particular appliances. As a striking example, the authors in [63] illustrate the possibility of identifying the video being displayed on a TV by analyzing the electro-magnetic interference (EMI) signals being produced by that TV on the power line. The authors conducted an extensive analysis over 8 different TV sets from 3 sizes and 3 manufacturers. They observe that EMI traces produced by the same video are repeatable on the same TV set and highly correlated between different TV sets. They show that movies out of a pool of 1200 known movies can be identified with high accuracy from EMI traces. This gives rise to the identification of TV channels for a known programme and time. Finally, the authors analyze 20 movies in an experimental setting and show that the EMI signature model of an arbitrary TV can be dynamically learned from a known video content without requiring access to that TV.

The authors in [37] propose another approach for detecting the channel displayed on a TV and even identifying the content. Using the 0.5Hz SM readings, the authors develop a function that predicts the power consumption of a dynamic back lighting liquid crystal display (LCD) monitor, which is related to the brightness of the content displayed on the TV. They carry out an experiment with three movies displayed on a TV and observe a high correlation between the actual and predicted power consumptions. Then, they show how their approach can be used for identifying the audiovisual content that is displayed on a TV set with dynamic backlighting.

The identification of the browsing activity of the user is studied in [64]. Monitoring the computer's alternating current (AC) power consumption with a sampling rate 1kHz, the authors

investigate the detection of the website, out of the collection of 8 websites, that a computer is rendering on the browser. They show that a very good accurracy can be achieved on the identification of the website thanks to the different classification techniques. They also analyze the performance of these classification techniques with website changes.

In [65], an interesting approach is proposed to recognize and infer the use-mode of kitchen appliances from their power consumption. Sensors are being installed for monitoring the appliances. First, the authors extract characteristic features of appliances in different operating modes. To do so, they measure the power consumption of appliances in different use-mode scenarios, such as the juicer with different amount of orange, the cutting machine cutting bread, coffee machine with different size of coffee, etc. Based on these measurements, the authors propose classification algorithms for infering the use-mode of the appliances. They carry out multi-user experiments to validate their approach, and show that 80-90% accuracy can be achieved in the prediction of the use-mode of the appliances.

2.1.3 Behaviour Deduction

SM readings can be analyzed for deducing the personal behaviours of the consumers. In this context, a behaviour extraction algorithm is proposed in [66]. The authors conducted an experiment in a flat and gathered both electrical and video data. Their proposed system detects several events from the electrical data and extracts behaviours of the consumers categorized as presence, sleep/wake schedule, appliance use, meal times, etc. They evaluate the performance of their behaviour extraction algorithm by using the reference video data. For the degree of disclosure of the categorized behaviours, they provide a metric that measures the performance of their behaviour extraction algorithm in revealing those behaviours.

In addition to SM electricity readings, gas or water consumption traces can also be used to infer occupant's behaviour. In [67], a pressure-sensor is employed in home's water infrastructure to measure the amount of water usage. Based on the water consumption readings, the authors show that activities at individual water fixtures such as particular toilet, a kitchen sink, can be inferred.

The authors in [68] show the privacy implications that can occur when both electricity and water consumption data are collected synchronously. In their experiments, they use a matched filter mechanism, and reveal several water and electrical events happening in the house. For example, they observe someone that flushes the toilet twice and discover another that flushes only once and does not use the sink. At the same time, they expose that one does not use the bathroom light while the other switches the bathroom light on.

2.2 Privacy-Preserving Techniques

2.2.1 Anonymization

Anonymization techniques are based on the idea of thwarting the UP or a third party, to associate the information obtained from the SM data with a specific SM user. The UP can process the anonymized data to deduce energy consumption traces aggregated from a specific location; however, these deductions can not be associated with particular users.

In this respect, the authors in [69] study SM data anonymization. They consider two types of data that can be generated by SMs, namely, high-frequency metering data sampled on the order of few minutes and low-frequency metering data sampled on the order of weeks or months. The authors assume that high-frequency data can be used to infer consumption patterns of specific electrical appliances in the household; and hence, it may expose private information. They also assume that low frequency data is attributable to specific users for billing and account management. Under these assumptions, the authors propose an escrow protocol for anonymizing the high-frequency metering data without compromising the operations of the utility and distribution network. In this protocol, the identity relation between the anonymized high-frequency data and the low-frequency data is assumed to be known only by an escrow service or trusted third party (TTP).

An SM privacy model based on a cryptographic game is presented in [70]. The authors assume that an aggregated energy consumption of a group of users, as well as the sum of the electricity consumption of a single user during a billing period are sent to the UP. They propose two solutions with and without TTP. In the first solution, TTP as an aggregation proxy, realizes anonymization through arbitrary aggregation of energy consumptions of different users and forwards the aggregated consumption data to the UP. In the second solution, every user adds a random noise to his/her readings in order to mask their own values. Then, the perturbed data of different users are aggregated and sent to the UP. The authors show that they can provide perfect privacy by using their solution with TTP.

The authors in [36] propose a zero-knowledge protocol to provide privacy, while allowing the UP to achieve metering operations such as billing. In their system, the consumption data is sent to neighbourhood gateways without identity information, and then forwarded to the UP. Therefore, their protocol aims at hiding the origin of data. The authors show how their protocol allows an SM to report its computed bill, while hiding how or when electricity was used.

The authors in [71] propose a protocol which uses the grid operator to anonymize the data. Accordingly, the users sign their data with pseudoynms and certificates provided by a TTP. They send the signed consumption data to the grid operator. The grid operator as a data

collector checks the authenticity of the signature and the certificate, and removes them from the message. Then, it forwards the data without signatures to the UP. Since the UP does not receive the consumption data directly from SMs, it can only link this data to a city. The authors assume that the grid operator is thrustworthy. Despite this assumption, the authors indicate that the grid operator does not pose any privacy threats as it only sees encrypted data.

In [72], a protocol that provides privacy to consumers based on anonymous reporting is presented. As opposed to other existing solutions, a TTP is not needed for key and group management, which makes their solution more interesting for realistic implementations. The authors indicate that the protocol has been implemented on hardware platforms and performance results are provided.

The authors in [73] show the lack of the user privacy guarantees achieved by anonymization techniques. The authors expose the possibility of inferring the identity of the user or distinguishing between users, when the attacker can access to an external indicator in addition to anonymized data. They develop two attacks threating the privacy of pseudonymized consumption traces. In the first attack, it is shown that the identity of a household and its consumption trace can be linked by correlating anomalies, which are series of unusual consumer behaviors that are reflected in the energy consumption. This enables the attacker to deduce the behaviour of the household. In the second attack, it is demonstrated that the origin of a consumption trace can be tracked across re-pseudonymization or different databases by exploiting patterns in the electricity consumption. The authors provide a data analysis framework that allows to apply these attacks to consumption databases, and then evaluate these attacks by conducting experiments on real consumption traces.

2.2.2 Trusted Computation

In trusted computation, either the user himself or an additional entity, i.e., TTP, performs the aggregation of the data. The UP does not know the personal power consumption data, but the aggregated consumption data. The privacy guarantees depend directly on the assumption of the protocol regarding the trustworthiness of the entity. If the entity can be trusted, the UP is not able to deduce the individual power consumption traces from the aggregate information even though this aggregate is sufficiently accurate.

The authors in [74] consider a distributed data aggregation solution over all users involved in the route from the source to the destination. In the aggregation tree construction, each node (user) collects data from its children, aggregates them with its own data and sends the result to the parent node. Homomorphic encryption is used to protect the privacy of the data in the route. Hence, users cannot see the intermediate or final aggregates in the route; however, the

aggregation is still performed correctly. The authors mention that the possible manipulation of aggregation by any adversary needs to be detected so as to prevent false data aggregations. They also mention that their approach provides efficient data aggregation with encryption while protecting the privacy of the user.

A secure architecture integrating privacy-preserving data aggregation and access control is proposed in [75]. In this scheme, users encrypt their readings using homomorphic encryption technique with the public key of the TTP and transmit them to the TTP at the root of aggregation tree. The measurements of each user have specific attributes. At each node of the aggregation tree, encrypted measurements of the same attributes are aggregated. The TTP first decrypts the aggregated measurements of each attribute, and then encrypts it using an attribute-based encryption for achieving the access control to the stored consumer data. Several key distribution centers distribute cryptographic keys to users, TTP and UP in order to provide a distributed access control.

2.2.3 Cryptographic Computation

Cryptographic computation protocols are based on homomorphism in the encryption schemes or secret sharing schemes. These protocols allow the UP to decrypt the aggregate of consumption data. On the other hand, the individual consumption data can not be decrypted.

In this context, the authors in [76] propose protocols combining the use of additive homomorphic encryption and additive secret sharing. For the current SM infrastructure, they assume a multilateral architecture in which the SMs have a trusted component and enjoy a certain level of autonomy. They mention that guarantees about the measurements for both grid operators and consumers should be provided by a trustworthy system. They show that several tasks like billing, grid optimization, etc., can be realized in a privacy-friendly manner with the proposed protocols. They also indicate that the proposed protocols can be implemented in practical scenarios.

The authors in [77] define an SM infrastucture with trusted privacy-preserving nodes. Each user masks its consumption data by means of a secret sharing scheme with homomorphic propoperties, and send the masked data to privacy-preserving nodes. The masked data with different spatial and temporal granularities is aggregated in the privacy-preserving nodes according to some rules identified by the configurator. The UP and market operators can obtain aggregated measurements, but can not access to the personal information of any user. The authors evaluate the scability of the proposed framework using an integer linear programming formulation and a greedy algorithm.

A family of comparison protocols that provide the private aggregation of the SM readings

without disclosing the raw metering data is presented in [78]. The authors mention that these protocols allow fraud and leakage detection as well as further processing of meter readings. The proposed protocols use different approaches to compute secret shares and to mask their readings before they are aggregated.

2.2.4 Verifiable Computation

In verifiable computation, the aggregator provides a proof together with the aggregated data in order to verify the correctness of the aggregation calculation. Thus, this kind of protocols can guarantee the integrity of the aggregation result even when the aggregation is performed by untrusted aggregators. The integrity and accuracy guarantees of these protocols make them a good canditate for providing billing capabilities. These protocols adopt the zero-knowledge proof system, in which the prover and the verifier, as two parties of the system, interact with each other. The verifier only knows the statement of the prover, which the prover intends to prove without revealing any additional information. For example, an SM user computes the aggregation of its electricity consumption, and sends this result to the UP. The UP can be persuaded about the validity of this result by the user, without being disclosed with fine-grained SM data.

2.2.5 Perturbation

Perturbation techniques are based on the idea of deliberately adding noise into individual or aggregated consumption data with the goal of preserving the privacy of the user at the expense of decreasing the utility of the data required by the UP.

A privacy-preserving SM system with a cluster of users is presented in [79]. The authors propose a private and distributed solution under the differential privacy model. Accordingly, each individual user in the cluster adds random noise to its readings according to Gamma distributions and sends them to the UP. This leads to Laplancian noise in the aggregated consumption of the cluster, which provides differential privacy to each user of the cluster, while maintaining the utility for the UP. That is, the UP can compute the perturbed and aggregated consumption of the cluster for utility purposes; however, it can not access to individual consumption values. The authors mention that they do not need to use a TTP thanks to the proposed solution. Moreover, they indicate that their scheme with differential privacy model is simple and practical, and provides strong and provable privacy guarantees.

The authors in [80] consider an untrusted aggregator that collects consumption data from a group of users with the goal of estimating statistics of the aggregarate. They propose a protocol that allows the aggregator to accurately estimate statistics even in the presence of user failures,

while providing differential privacy guarantees for users against the untrusted aggregator. The binary-tree techniques is used on the construction of the aggregation, which helps to achieve fault tolerance. Moreover, the authors indicate that their approach supports dynamic joins and leaves.

In [81], the authors propose an aggregation protocol in which an untrusted aggregator can decrypt aggregate statistics without compromising privacy of the individual users. Accordingly, each individual user adds random noise to their consumption data from a geometric distribution and sends it to an untrusted aggregator. The proposed protocol allows the aggregator to compute the aggregate of the users' consumptions and desired statistics. On the other hand, the proposed scheme is aggregator oblivious, which implies that the aggregator can not learn any information regarding the consumption of individual users. Moreover, the protocol guarantees the differential privacy for the aggregate result, even when the aggregator has some auxiliary knowledge about user's consumption data.

In [82], the authors propose a differentially private aggregation scheme for distributed time-series data which might be highly correlated. An untrusted third party aggregates user data and runs queries on the aggregate data. The proposed protocol uses fourier perturbation algorithm in order to ensure differential privacy for temporally correlated time-series data. To achieve differential privacy in a distributed setting, the proposed protocol uses the distributed laplace perturbation algorithm which adds noise in a distributed manner. According to the results of the experiments carried out with real data sets, the authors indicate that the proposed method yields accurate answers for query sequences and also scales with large number of users.

The authors in [83] provide a fault-tolerant, privacy-preserving aggregation protocol that allows an aggregator to forecast energy consumption over aggregated and encrypted data. The proposed protocol use homomorphic encryption and distributed key managing authority for aggregation. Key managing authority provides differentially private decryption services to the aggregator. The authors indicate that the proposed protocol is also secure against malicious aggregators. The authors compare their protocol with the existing procols and observe that it provides higher accuracy in the calculation of desired statistics even in the presence of failures.

In [84], the authors propose a practical privacy-preserving SM system that can support both billing and load monitoring. The proposed method provides privacy by using a trusted platform module in SMs which supports pseudorandom number generator. Accordingly, users encrpyt their readings and store them in a central storage system. The UP can access the storage system for billing and load monitoring. For billing, the UP can only access aggregate of SM readings over a time period. For load monitoring, the UP can only access aggregate of SM readings in a particular area at some recent time. The authors indicate that their proposed method provide privacy guarantees for individual SM readings when the UP realizes queries

for billing and load monitoring. Moreover, they mention that the proposed method does not tolerate failures of users.

2.2.6 Demand-Side Energy Management (EM) Techniques

In the aforementioned privacy-preserving techniques, privacy is provided by tampering the SM readings before being reported to the UP. As opposed to these techniques, demand-side EM is an emerging technique that can provide privacy to the consumer without tampering the SM readings. Demand-side EM techniques utilize storage units, such as RBs, and alternative energy sources, such as a solar panel, to partially mask the energy usage patterns of the consumers against the UP. Moreover, since the SM readings are reported to the UP without tampering, these techniques maintain unaltered the operational utility of the SM readings.

Various EM algorithms have been proposed in the literature to provide privacy to users. In this regard, [85] proposes the best effort algorithm, which intends to hide the load signatures of the consumer from the UP with the utilization of RB. The proposed algorithm charges and discharges the RB in order to maintain a constant SM load level so that appliance usage events cannot be detected. The authors consider three different privacy metrics, namely, relative entropy, cluster classification and correlation/regression analysis, to measure the privacy provided by the proposed algorithm. In [86], a power mixing algorithm is proposed to protect energy consumption events of selected appliances with the utilization of RB. The authors consider the privacy metrics mentioned above and evaluate the performance of the proposed algorithm by using the SM data collected from individual home appliances. The authors indicate that some major factors, such as battery capacity and power, can have an effect on the performance of the proposed algorithm.

In [87], a simple RB system is studied. The authors consider a discrete-time system model with binary input-output loads and battery states, and propose stochastic battery policies to provide privacy to the users. Mutual information between the input and output loads is considered as a measure of privacy. The authors compute the mutual information applying a trellis algorithm on the finite state model (FSM). They consider two types of stochastic policies, namely, battery-conditioned policies and battery/output-conditioned policies, and indicate that these policies can leak 26% less information than the algorithm proposed in [85].

In [88], the authors propose a novel technique for hiding sensitive power consumption signatures of the appliances in the total power consumption load of a household. The proposed method modifies the power consumption of the household through the utilization of RB connected to the household's power supply, with the goal of providing privacy assurances in terms of differential privacy. The authors consider capacity and throughput constraints of batteries

in realistic scenarios, and propose an integrated method of noise cascading that maintains the differential privacy.

The authors in [89] propose a non-intrusive load leveling (NILL) algorithm to protect privacy of the user against the potential privacy invasion that can stem from NALM techniques. The proposed algorithm is used to flatten the consumption of the user to a constant target load, with the goal of removing appliances' features. NILL uses RBs to flatten the power consumed by appliances. When an appliance turns to ON state, the exerted load exceeds the target load; and thus, NILL discharges the battery for partially satisfying the exerted load and maintaining the target load. Similarly, when an appliance turns to OFF state, the exerted load falls below the target load; and hence, NILM charges the battery with the energy drawn from the UP and maintains the target load. The proposed NILL system comprises an RB along with a control system that charges or discharges the RB based on the present load and battery state.

In [90], the authors propose three techniques, namely, fuzzing, targeted entropy maximization and targeted fuzzing. The proposed techniques intend to mask individual load changes with the utilization of RB. These techniques have different ways of choosing load offsets. The first proposed technique is fuzzing. This technique changes the observed load to a desired observed signal, which is chosen randomly over an interval by using a uniform distribution. At first glance, uniform distribution would seem to create the greatest obfuscation for an actual signal change. However, since the sampling interval is built around the actual load change, there are cases where this technique can choose an output signal value that has only one possible underlying actual event. This would lead to the fact that there is no obfuscation at all. The second proposed technique is targeted entropy maximization. This technique chooses the desired load level that maximizes the entropy of possible individual events. To do so, the proposed technique uses the information about the individual loads that contribute to the aggregate signal, and picks up an offset value to minimize the ability of the third parties to deduce any information about the individual appliances in the aggregate load. This technique assumes that the observer is unaware of the masking technique, the battery capacity and the charging/discharging rate. The authors indicate that this technique might fail in providing privacy if this information is available at the observer side, in which case the observer could decode the observed signal to reveal the original signal. The third technique is targeted fuzzing. This technique builds a probability distribution for an observed event taking into account the fact that how this event can be interpreted by an observer. The distribution has bias towards samples that larger numbers of possible actual events can explain. This technique randomly samples an observed change from this distribution, while eliminating any samples that only one actual event can explain. The authors mention that the targeted fuzzing technique prevents the deficiencies of the previous techniques against potential attacks.

In [91], the authors propose battery-based load hiding methods to hide appliance loads. They first evaluate the performance of two well-known battery control algorithms, namely, best effort [85] and NILL [89], against the attack of an intruder, and reveal privacy vulnerabilities of these algorithms. Then, they propose a stepping-based algorithms based on maximizing the error between the input and output loads under the RB capacity and charging/discharging rate constraints. They use the mutual information as the privacy measure, and compare the performances of the proposed stepping algorithms against the best effort and NILL algorithms. Using a real energy consumption data, they show that their methods outperform the best effort and NILL algorithms in general.

The authors in [92] propose a stochastic control method that jointly decorrelates the SM readings from the user's actual usage and reduces the energy cost of the user with the utilization of RB. The proposed method is founded based on a stochastic DP. The authors indicate that their method reduces the correlation between the SM readings and the user's real consumption while maximizing the energy savings of the users. The cost savings are achieved by charging the battery in the low-price zone and satisfy the energy demand from the stored battery energy in the high-price zone. According to their experiments, the authors indicate that the proposed technique achieves higher privacy and cost savings in the presence of low-frequency components in the load profile of the user.

In [93], the authors study a DP framework that jointly provides SM data privacy and reduces the energy cost of the user. Assuming that the energy demands and prices are known causally, they reformulate the original problem so that it can be solved by using only the current demand and price information. Then, they propose a low complexity online algorithm based on the Lyapunov optimization technique. The proposed algorithm is parametrized by a positive value, which enables to quantify the impact of the battery capacity on its performance. Using a real energy demand data, the authors demonstrate that their algorithm can provide privacy to the user in a cost-effective manner.

2.3 Linear Transmission (LT) Strategies

Shannon's source-channel separation theorem states that the optimal end-to-end distortion is achieved by concatenating the optimal source and channel codes when there is no delay or complexity constraints, and the source and channel distributions are ergodic [94]. However, if the delay and complexity are considered as system constraints, the optimality of this theorem fails. This gives rise to the need of designing transmission strategies that can accommodate low latency and low complexity constraints. In this regard, LT emerges as a promising strategy, since it reduces both the delay and encoding complexity significantly.

2.3.1 Linear Coding

In [95], the authors obtain the optimal linear coding solution for the transmission of a vector of sources over a vector channel. They consider the problem of designing the optimal linear vector coding method to transmit an r-dimensional vector signal over a k-dimensional AWGN vector channel under a given power constraint and MSE distortion criterion. They assume an r-dimensional discrete-time memoryless Gaussian vector source and a k-dimensional discrete-time memoryless AWGN vector channel. They also assume that the source signal and the channel noise are independent from each other, while the individual samples of the source and the channel noise vectors are correlated, i.e., the covariance matrices of the source and noise signals are not necessarily diagonal. They design the linear encoder and decoder that minimize the weighted MSE distortion under the total channel power constraint. In the first step of the optimal linear transformation strategy, the correlated source signal vector and the correlated channel noise vector are transformed into uncorrelated source signal and channel noise vectors; and hence, the original problem is reduced to an equivalent vector signal transmission system with uncorrelated source and noise sequences. In this equivalent system, the optimal decoder is the linear minimum mean-square error (MMSE) estimator, whereas the optimal linear encoder is found based on the following linear transformation steps. In the first step, considering the eigenvalues of the source and channel noise covariance matrices, the source and noise samples are sorted in descending and ascending orders, respectively. The authors measure the quality of the source and the channel noise samples through the eigenvalues of the source and channel noise covariance matrices, i.e., the better source sample implies the larger eigenvalue of the source covariance matrix and the better channel implies the smaller eigenvalue of the channel noise covariance matrix, respectively. Then, the sorted source signal vector is matched to the sorted channel vector in such a way that the largest eigenvalue of the source covariance matrix is assigned to the smallest eigenvalue of the channel noise covariance matrix, and the second largest eigenvalue of the source covariance matrix to the second smallest eigenvalue of the channel noise covariance matrix, and so on so forth. In this optimal matching, each source sample is scaled by its corresponding encoder constant and transmitted through the corresponding channel. The authors also derive the optimal encoder for the special case in which each subchannel has its individual power constraint.

In [96], the authors study the transmission of delay-sensitive SG system state measurements over wireless channels. In the SG system under consideration, wireless sensors obtain noisy observations of the system state measurements and deliver them to CCs with the goal of monitoring and controlling the grid. Since the state measurements are delay-sensitive, the authors focus on low complexity memoryless linear coding and decoding strategies under the channel power constraint and MSE distortion criterion. Assuming fading channel, the authors

propose the optimal power allocation strategy over the system state measurements and the fading channels. If there is only one system state measurement, the optimal power allocation over time (fading states) is found as the sticky water-filling solution, which is a modified version of the well-known water-filling solution, with a main difference that the water level changes for different values of the fading state. For the multiple system state measurements, the authors consider two cases, namely, the diagonal observation matrix and the general observation matrix. If the observation matrix is diagonal, the optimal power allocation over time is shown to be the sticky water-filling solution. On the other hand, the authors show that the optimal power allocation over the system state measurements is to allocate all available power to the most important measurement. For the general observation matrix, the authors propose a power allocation scheme, which is shown to be asymptotically optimal.

In [97], the authors study linear coding for a discrete memoryless Gaussian source transmitted over a discrete memoryless AWGN fading channel under average power constraint and MSE distortion criterion. In linear coding, the encoder linearly maps the source symbols into the channel symbols. The authors analyze the performance of linear coding under the system model mentioned above, and show that among all single-letter codes, linear coding achieves the optimal performance. If the CSI is known both by the transmitter and the receiver, the optimal power allocation is provided in terms of the channel fading state and the average power constraint. If the CSI is known only by the receiver, the optimal power allocation is shown to be uniform over fading states. The authors indicate that increasing the block length does not provide any gain in the performance of linear coding. Hence, the Shannon's theoretical bound can not be achieved with linear coding in general. However, if the magnitude of the fading gain is constant, then linear coding is shown to achieve the Shannon's theoretical bound. The gap between the performance of linear coding and the Shannon's theoretical bound is bounded in terms of the channel fading state and the average power constraint. In the numerical simulations, the authors observe that this gap becomes negligible if the average power constraint or the variance of the channel fading state is relatively small.

In [98], the authors study LT of correlated Gaussian vector sources over multi-antenna channels. For static multi-antenna channels, they derive the necessary and sufficient conditions for the optimality of linear coding in terms of MSE and show that the linear coding is optimal when the signal-to-noise ratio (SNR) is below a threshold. Then, the authors consider fast fading multi-antenna channels, and show that the optimal decay rate of the average distortion in the low SNR regime can be achieved by linear coding. They also show that linear coding achieves the optimal exponential decay rate of the average distortion in the high SNR regime under certain settings.

In [99], the authors study linear coding of vector Gaussian sources transmitted over fading

multi-antenna channels under average power constraint and MSE distortion criterion. Assuming that the CSI is known only by the receiver, they derive the optimal linear coding solution for the encoder and decoder, and compare its performance with the theoretically achievable optimal performance. For the Rayleigh fading channel model, the authors show that linear coding is suboptimal in general. However, they prove that the performance of linear coding is close to the theoretically achievable optimal performance in the low SNR regime. For some special cases, they prove the same for the Rician fading channel model as well.

Chapter 3

Increasing Smart Meter Privacy Through Energy Harvesting and Storage Devices

3.1 Introduction

As it has been argued previously, SM data can be easily analyzed for surveillance purposes by tracking appliance usage patterns, employing non-intrusive appliance load monitors and data mining algorithms [56], [60], [61]. At the very least, through SM readings it is possible to infer whether a user is at home or not. But, through more advanced pattern recognition techniques, energy consumption patterns of individual appliances can be identified with high accuracy even when the SM can read only the aggregated household energy consumption [57]. As a striking example, [37] illustrates the possibility of detecting the channel displayed on a TV, and even identifying the content, just by analyzing the power profile of the household. Even assuming that the SM readings are transmitted to the UP in an encrypted manner, preventing third parties from accessing the user's private energy consumption data, the UP will receive significant personal information about the user. Thus, even if only partially, assuring the privacy of the household's electrical load profile is essential for users.

In this chapter, we study SM privacy from the fundamental information theoretic perspective. We measure the privacy of the user's energy profile with respect to the UP in terms of the *information leakage rate*, which denotes the mutual information rate between the real energy consumption of the appliances and the SM readings. Using Shannon entropy to measure privacy is not new. Minimizing the information leakage rate is equivalent to maximizing the *equivocation*, which was introduced by Shannon in [100] in the context of secure communications. Mutual information has previously been proposed as a measure of privacy in SM systems and several works in [48–50, 52, 86, 87, 89–91, 101–108]. Modeling the input load as

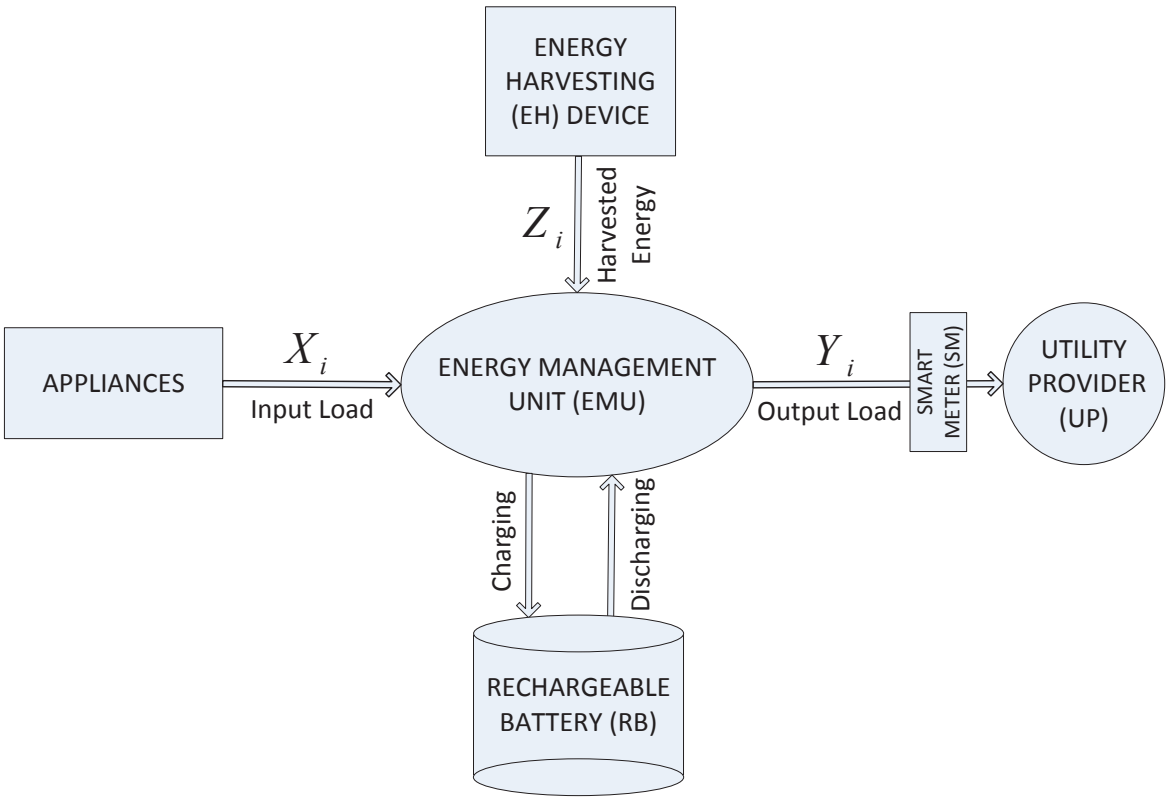


Figure 3.1: An SM system diagram with energy and information flows. The user, in addition to its connection to the energy grid, also has an EH device and an RB at its use. The energy flow in the system is managed by the EMU. The SM reads only the energy that is supplied by the UP at each interval. The readings are reported to the UP correctly without any tampering, but potentially in an encrypted manner.

a discrete-time random process, the information leakage rate measures the amount of information the UP learns about the input load after observing the output load, i.e., the energy requested by the user. We assume that the UP may know the statistics of the input load as well as the stochastic behavior of the EM policy; however, it cannot observe the input load or harvested energy directly. The UP has to estimate the realization of the input load based on its statistical knowledge and its observation of the output load. The user wants to minimize the information leakage rate to achieve the highest level of privacy. While cryptographic algorithms rely on mathematical operations and the complexity of their computation by using encryption keys, information theoretic security does not depend on encryption keys and assures reliable privacy regardless of the computational power of an intruder, the UP in our case [109].

We study the privacy of an SM system from the perspective of a single user. In our system model, depicted in Fig. 3.1, we integrate an EH device as an alternative energy source and an RB as an energy storage unit. The energy flow is managed by the EMU. We consider a discrete-time system. At each time instant i, the appliances request a certain amount of energy, denoted

by X_i. This amount is reported to the EMU which is responsible for providing this exact amount to the appliances; that is, we do not allow energy outages or rescheduling of appliance operations in this work. We also consider only the real power consumption of the devices and assume that the SM only reads and reports this quantity. Moreover, we also ignore inefficiencies and mismatches in providing the energy requirement of the appliances from different energy sources, and consider only the energy that is consumed by the appliances. The EMU has access to three different energy sources: the energy grid, the EH device and the energy storage unit. At any time instant it can provide the energy requested by the appliances from one or more of these sources. The goal of the EMU is to increase both the energy efficiency of the system and the privacy of the user.

We employ stochastic battery policies based on the harvested energy, energy demand of the appliances and the state of the storage unit. We model the energy generation profile of an EH device as a stochastic process whose behavior depends on the characteristics of the underlying energy source and the device itself. Therefore, it is likely that the harvested energy sometimes does not match the energy required by the system and the extra energy would be wasted if not stored. Introducing an RB for energy storage into the system is essential for better utilization of the harvested energy. On the other hand, considering the increasing use of alternative energy sources (such as solar panels) by households, and the availability of rechargeable storage units (such as EVs) with significantly large storage capacities, it is meaningful to exploit these devices not only to decrease the dependency on the SG and to increase the energy efficiency, but also to provide additional privacy for the users. The equivocation of the UP about the real energy consumption can be manipulated by charging and discharging the RB and by using the harvested energy. Hence, the benefits of the RB are twofold: i) it can increase the energy efficiency of the system by storing extra harvested energy; and ii) it can increase the privacy of the user by hiding the energy consumption profile from the UP. We show in this chapter that there exists a trade-off between energy efficiency and privacy for the optimal EMU operation, and the operating point on this trade-off can be chosen based on the privacy sensitivity of the underlying input load and the cost of energy.

As it has been presented in the state of the art in Chapter 2, various techniques have recently been proposed to provide a certain level of privacy for SM users. Anonymization [69], aggregation [70], homomorphism [76] and obfuscation [110] are some of the techniques that have been studied in the literature. In [88], the authors present a method for establishing privacy assurances in terms of differential privacy, i.e., RB is used to modify the energy consumption by adding or subtracting noise and thereby, the energy consumption of the individual appliances can be hidden. Moreover, they also consider various constraints on the RB such as capacity and throughput. In [89] a method to provide privacy against potential NALM techniques is

proposed. A NILL algorithm is used to flatten the consumption of the user by means of an RB. Similarly, [90] proposes three techniques, i.e., fuzzing, targeted entropy maximization and targeted fuzzing. The authors intend to obfuscate the load by masking the individual loads with the use of an RB. Basically, fuzzing changes the load randomly over an interval, the targeted entropy maximization technique chooses the desired load level that maximizes the entropy of possible individual events, and targeted fuzzing builds a probability distribution to do so.

Most of the earlier work on SM privacy assumes that the user has control over the SM readings and can manipulate these readings before sending the data to the UP. For example, Bohli et al. [70] propose sending the aggregated energy consumption of a group of users to the UP. Li et al. [19] consider using compressed sensing techniques for the transmission of the SM readings of active users based on the assumption that SM data transmission is bursty. Bartoli et al. [111] propose data aggregation together with encryption to forward SM readings. Marmol et al. [112] propose using "additively homomorphic encryption", which allows the UP to decode only the total energy consumption of a group of users while keeping the individual readings secure. Rajagopalan et al. [113] propose compression of the SM data before being transmitted to the UP. Unlike this line of research, we assume that the SM reads the amount of energy that the user gets from the grid at each time interval and the meter readings are reported to the UP without being tampered by the user. Hence, privacy in our model is achieved by differentiating the output load, i.e., the energy received from the UP, from the input load, i.e., the real energy consumption of the user, as much as possible.

A similar approach has been taken in some other previous work as well. RBs have been proposed to partially obscure the energy consumption of the user in [85–89]. The main goal of the proposed EM algorithms in these works is to protect the privacy of the user. References [85] and [86] study variational distance, cluster similarity and regression analysis to measure privacy and propose various heuristic techniques, such as the power mixing and best-effort algorithms. A discrete-time system model is considered in [87] and stochastic battery policies are studied with mutual information between the input and output loads as the measure of privacy. In [104] a similar information theoretic privacy analysis is carried out in the presence of an EH device that can provide energy limited by peak and average power constraints.

The main contributions of this chapter can be summarized as follows:

- We introduce an energy efficiency-privacy trade-off in an SM system considering the availability of an EH device and an RB. To the best of our knowledge, this is the first work that provides an analytical study on the effect of an alternative energy source on SM privacy.

- Focusing on a discrete-time system model, we investigate stochastic EM policies that

provide both privacy and energy efficiency to the user.

- We study the effect of EH rate on the energy efficiency-privacy trade-off, and observe that as the EH rate increases, the information leakage rate decreases significantly.
- We illustrate numerically that the increased battery capacity significantly reduces the information leakage rate.
- While no grid energy is allowed to be wasted in the above analysis, we also study the increased privacy that can be achieved by wasting the grid energy for very sensitive applications.

We use the following notation in the rest of the chapter. Random variables (r.v.s.) are denoted with uppercase letters, e.g., X, and their realizations are denoted with lowercase letters, e.g., x. A r.v. takes values from a finite set $\mathcal{X}$ following a probability mass function $p_X(x)$. The subscript X will be omitted when it is obvious from the context. An n-length random sequence is denoted by $X^n = X_1, \ldots, X_n$. $E[X]$ denotes the expectation of the r.v. X. The entropy of a r.v. X is defined by:

$$H(X) \triangleq -\sum_{x \in \mathcal{X}} p(x) \log p(x). \tag{3.1}$$

$H(\cdot|\cdot)$ and $H(\cdot,\cdot)$ denote conditional entropy and joint entropy, respectively, which are defined similarly. The mutual information between r.v.s. X and Y is defined as:

$$I(X;Y) = H(X) - H(X|Y). \tag{3.2}$$

The rest of the chapter is organized as follows. In Section 3.2, we introduce the system model. Section 3.3 describes the technique to compute the information leakage rate. In Section 3.4, we present our results and compare them with the existing results in the literature. Finally, we conclude the chapter in Section 3.5.

3.2 System Model

We study the energy input/output system illustrated in Fig. 3.1 under a discrete-time system model. The input load X_i represents the total energy demand of the appliances at time instant i. The output load Y_i denotes the amount of energy that the system requests from the UP,

while Z_i denotes the amount of harvested energy at time instant i. We assume that there is a minimum unit of energy; and hence, at each time instant i, the input load, harvested energy and output load are all integer multiples of this energy unit. Over time, we assume that the input load $X^n = X_1, X_2, \ldots, X_n$ is an independent and identically distributed (i.i.d.) sequence with marginal distribution p_X over $\mathcal{X} = \{0, 1, \ldots, N\}$. The harvested energy is also modelled as a discrete-time stochastic process, where $Z^n = Z_1, Z_2, \ldots, Z_n$ is an i.i.d. sequence with marginal distribution p_Z over $\mathcal{Z} = \{0, 1, \ldots, M\}$. The characteristics of the EH distribution, p_Z, depend on the design of the energy harvester. For example, for a solar energy harvester the average harvested energy can be increased by scaling the size and the efficiency of the solar panel. Note that the energy consumed by the appliances and the harvested energy are independent of each other.

The output load is the amount of energy that is demanded from the UP, and is denoted by $Y^n = Y_1, Y_2, \ldots, Y_n$ with Y_i taking values in $\mathcal{Y} = \{0, 1, \ldots, L\}$. We denote the energy in the battery at time instant i by B_i. We assume that the RB has a maximum capacity of K energy units, i.e., $B_i \leq K$, $\forall i$, while the system is not bounded by the maximum amount of energy that can be provided by the UP, i.e., $L \geq (N + K)$[1].

We consider stochastic EM policies at the EMU that depend on the instantaneous input load, harvested energy and the battery state. An EM policy maps the energy requested by the appliances, X_i, the harvested energy, Z_i, and the battery state, B_{i-1}, to the output load, Y_i, and the next battery state, B_i. Note that in general a larger set of EM policies is possible. The EMU can decide its actions based on all the past input/output loads, harvested energy amounts and the battery states. For example [87] considers policies that take into account the previous output load, Y_{i-1}. Similarly, the best effort policy proposed in [85], in which the EMU aims to keep the output load value as stable as possible, is simply a special case of the battery/output load conditioned policies in [87]. To keep the complexity of possible EM policies simple, we restrict our attention to EM policies that depend only on (X_i, Z_i, B_{i-1}), and satisfy,

$$Z_i + (B_i - B_{i-1}) + Y_i \geq X_i, \tag{3.3}$$

which guarantees that the energy demand of the appliances is always satisfied.

[1]The energy we consider in this model is the real energy measured by the SM and we ignore the reactive power or the power factor which can also be used to make deductions about the input load. Moreover, we also assume that the energy demand of the appliances is satisfied by transferring an equivalent amount of energy from the RB, EH unit or UP; that is, we do not consider the effect of the supply voltage, frequency or the characteristics of the appliances on the amount of energy that needs to be requested from the corresponding energy source. Such quantities could also be incorporated into our model by considering vector-valued measurements, but this added complexity is not necessary for studying the fundamental trade-offs considered here.

We assume that the SM provides the output load Y_i at each time instant to the UP perfectly. That is, we do not allow the user to manipulate the SM reading. Moreover, we also assume that p_X and p_Z are known by the UP, whereas no information about the realizations of either the input process x^n, or the EH process z^n, is available at the UP, which observes only the output load, y^n. The equivocation, $H(X^n|Y^n)$, measures the uncertainty of the UP about the real energy consumption after observing the output load. We have,

$$H(X^n|Y^n) = H(X^n) - I(X^n;Y^n). \tag{3.4}$$

Since $H(X^n)$ is a characteristic of the appliances and is assumed to be known, the EMU tries to minimize $I(X^n;Y^n)$ in order to maximize the equivocation. Accordingly, the privacy achieved by an EM policy is measured by the *information leakage rate*, defined as:

$$I_p \triangleq \lim_{n\to\infty} \frac{1}{n} I(X^n;Y^n), \tag{3.5}$$

where $X^n = (X_1, X_2, \ldots, X_n)$, $Y^n = (Y_1, Y_2, \ldots, Y_n)$, and $I(X^n;Y^n)$ is the mutual information between vectors X^n and Y^n.

Due to the finite capacity of the RB and the stochastic nature of the input and EH processes, some of the harvested energy will be wasted. To measure the proportion of the energy wasted by an EM policy, we define the *wasted energy rate* as follows:

$$E_w \triangleq \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} (Z_i + Y_i - X_i). \tag{3.6}$$

We say that an information leakage-wasted energy rate pair (I_p, E_w) is *achievable* if there exists an EM policy satisfying (3.5) and (3.6). The closure of the set of all achievable rate pairs is called the *rate region* Γ. In general the EM policy that minimizes the information leakage rate does not necessarily minimize the wasted energy rate. From the classical time-sharing arguments [94] we can readily see that the rate region Γ is convex. Since the region is also closed by definition, it is sufficient to identify the boundary of region Γ, which characterizes the optimal trade-off between privacy and energy efficiency.

To illustrate the privacy benefits of having an EH device, we first consider a system without an RB. In this case, the EMU uses as much as possible from the harvested energy, and asks for energy from the UP only when the harvested energy is not sufficient. Therefore, we can define Y_i as a deterministic function of X_i and Z_i as follows:

$$Y_i = (X_i - Z_i)^+ \triangleq \begin{cases} X_i - Z_i, & \text{if } X_i - Z_i > 0, \\ 0, & \text{if } X_i - Z_i \leq 0. \end{cases} \tag{3.7}$$

In general, it is possible to ask for energy from the UP even when $X_i = 0$. This will increase the privacy by confusing the UP, but waste energy. We do not allow wasting energy from the UP unless otherwise stated, as this would be costly in practical systems. Obviously, when there is no harvested energy, i.e., $\Pr\{Z = 0\} = 1$, then we have $Y_i = X_i$ for $\forall i$, and $I_p = \frac{1}{n}H(X^n) = H(X)$, i.e., the UP knows the input load perfectly. On the other hand, if there is always harvested energy sufficient to supply the appliances, i.e., $M = N$ and $\Pr\{Z = N\} = 1$, then $Y_i = 0$ for $\forall i$, and we have $I_p = 0$. When $I_p = 0$ we say that *perfect privacy* is achieved. Basically, as we harvest more and more energy, we reduce our dependence on the grid energy, and decrease the information leaked to the UP about our real energy consumption. However, note that, at each time instant harvested energy that is not used by the consumer is wasted. For example, when $\Pr\{Z = N\} = 1$, we have $E_w = N - E[X]$ while $E_w = 0$ when $\Pr\{Z = 0\} = 1$. In other words, there is a trade-off between privacy and energy efficiency provided by the EH unit. Introducing an RB into this system will have a dual use and improve this trade-off. RBs can act as a filter for the energy usage profile and decrease I_p further while reducing the wasted energy at the same time.

Due to the discrete-time nature of the system, it can be represented by an FSM [87]. The FSM representation of the system with all the transitions and states evolving as a Markov chain depends on the input load level N, the output load level L, the harvested energy level M and the RB capacity K. As we have mentioned earlier, we consider EM policies that depend only on the current input load X_i, harvested energy Z_i, and the previous battery state B_{i-1}[2]. We have $s \triangleq (K + 1)$ states in our FSM, where state b_i denotes the state of the RB, i.e., the amount of energy stored in the RB at time i. We assume $b_0 = 0$. The battery-conditioned transitions occur from state b_i to b_{i+1} depending on the battery state b_i, the input load x_{i+1} and the harvested energy z_{i+1}. The FSM is simply a Markov chain, and the transitions specify the map to proceed in the chain. Possible transitions are depicted in Fig. 3.2 for different (x, z, y) triplets and transition probabilities.

[2]In [87] in addition to battery-conditioned policies, battery/output load conditioned policies are also studied. However, the authors indicate that they have not found any battery/output load conditioned policy that performs better than the optimal policy that acts solely based on the battery state. We have made the same observation in our numerical analysis.

3.2.1 A Simplified Binary Model

Similarly to [87] to keep the presentation and the numerical analysis simple, we initially consider a binary model; that is, we assume $N = L = M = K = 1$. However, we note here that the following arguments and evaluation techniques extend to non-binary models directly. From a practical perspective, this binary model corresponds to a system with a single appliance that can be ON or OFF at various time instants with a certain probability, and both the capacity of the RB and the energy generated by the EH are equivalent to the energy used by this device when it is ON. In Sections 3.4.3 and 3.4.4 we will consider non-binary battery capacity cases as well.

While the EM policies can be time-varying in general, we consider time-invariant fixed policies in which the transition probabilities and parameters of the policy are fixed throughout the operation. The probability distributions of the input load and the harvested energy are chosen as Bernoulli distributions, i.e., $\Pr\{X = 1\} = p_x$ and $\Pr\{Z = 1\} = p_z$, respectively. The output load Y^n is also a binary sequence which can provide 0 or 1 units of energy to the input load at any time instant i. Battery state $b_i = 0$ denotes that the RB is empty while $b_i = 1$ denotes that the RB is fully charged at time instant i. We assume that within each time duration, i to $i + 1$, the RB can be charged to battery state, $b_i = 1$, discharged to battery state, $b_i = 0$, or remain in the same state depending on the transition probabilities. We do not take into consideration the charging and discharging rates of the RB, and assume that this time duration is enough for fully charging or discharging.

Let the RB be discharged at time instant i, i.e., $b_i = 0$. There are six possible transitions that can occur as illustrated in Fig. 3.2. If the appliances demand zero energy and no energy is harvested, i.e., $(x_{i+1} = 0, z_{i+1} = 0)$, the EMU chooses either to charge the RB by asking energy from the UP, i.e., $(y_{i+1} = 1, b_{i+1} = 1)$ with probability p^a_{01}, or keeps the RB discharged, i.e., $(y_{i+1} = 0, b_{i+1} = 0)$ with probability $(1 - p^a_{01})$. If the appliances demand zero energy and one unit of energy is harvested, i.e., $(x_{i+1} = 0, z_{i+1} = 1)$, the UP does not provide any energy to prevent waste and the RB is charged with harvested energy, i.e., $(y_{i+1} = 0, b_{i+1} = 1)$. If the appliances demand one unit of energy and no energy is harvested, i.e., $(x_{i+1} = 1, z_{i+1} = 0)$, the UP must provide one unit of energy to fulfill the energy demand and the RB remains discharged, i.e., $(y_{i+1} = 1, b_{i+1} = 0)$. If the appliances demand one unit of energy and one unit of energy is harvested at the same time, i.e., $(x_{i+1} = 1, z_{i+1} = 1)$, either the RB is charged by means of the output load, i.e., $(y_{i+1} = 1, b_{i+1} = 1)$ with probability p^b_{01}, or it remains discharged, i.e., $(y_{i+1} = 0, b_{i+1} = 0)$ with probability $(1 - p^b_{01})$.

Similarly, let the RB be charged at time instant i, i.e., $b_i = 1$. In this case, there are five possible transitions that can occur as depicted in Fig. 3.2. If the appliances demand zero energy and no energy is harvested, i.e., $(x_{i+1} = 0, z_{i+1} = 0)$, the UP does not provide energy so as

not to cause waste and the RB remains charged, i.e., $(y_{i+1} = 0, b_{i+1} = 1)$. If the appliances demand zero energy and one unit of energy is harvested, i.e., $(x_{i+1} = 0, z_{i+1} = 1)$, the UP is not expected to provide any energy and the RB remains charged, i.e., $(y_{i+1} = 0, b_{i+1} = 1)$, while the harvested energy is wasted in this situation. If the appliances demand one unit of energy and no energy is harvested, i.e., $(x_{i+1} = 1, z_{i+1} = 0)$, the EMU chooses between keeping the RB charged, i.e., $(y_{i+1} = 1, b_{i+1} = 1)$ with probability $(1 - p_{10})$, or discharging it, i.e., $(y_{i+1} = 0, b_{i+1} = 0)$ with probability p_{10}. If the appliances demand one unit of energy and one unit of energy is harvested, i.e., $(x_{i+1} = 1, z_{i+1} = 1)$, there is no need to ask for energy from the UP and the RB remains charged, i.e., $(y_{i+1} = 0, b_{i+1} = 1)$.

3.3 Information Leakage Rate Computation

In this section we focus on the computation of the information leakage rate, I_p. From an information theoretic perspective the operation of the EMU which decides on the energy flow in the system using the EH and RB units resembles data compression where the compression is accomplished through a finite state machine. In this analogy, the input load X^n corresponds to an i.i.d. data sequence to be compressed, and the output load Y^n is the compressed version. The problem is similar to a rate-distortion problem in which the goal is to minimize the mutual information between the source sequence and the compressed version while satisfying the distortion requirement. In our model, the energy provided from the EH device is similar to a distortion requirement. While we want to minimize the mutual information between the original data sequence and the compressed version, we are limited by the allowed distortion, the available harvested energy in our case. A different rate-distortion approach for the SM privacy problem is taken in [113]. In [113] the SM is allowed to introduce a certain amount of distortion to its readings before reporting them to the UP, while in our setting distortion is introduced on the real energy consumption values, making the rate-distortion formulation less explicit. See [104] for more on the connection with the rate-distortion theory, where a single-letter information theoretic expression is obtained for the optimal privacy in the absence of an RB. Due to the memory introduced into the system through the battery, a single letter expression is elusive for our problem. However, for a fixed EMU policy, the information leakage rate I_p between the input and the output loads can be estimated numerically using the computation method studied in [114]. In the following we summarize this computation method.

We first set the values for the transition probabilities and the number of states s in the FSM. For instance, we specify $\{p^a_{01}, p^b_{01}, p_{10}\}$ labeled on Fig. 3.2 for $s = 2$, i.e., $b_i \in \{0, 1\}$. Afterwards, we sample very long sequences (large n) of X^n, Z^n and Y^n by using the FSM. We then compute $p(y_1, y_2, \cdots, y_n)$ and $p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$. Finally, the information

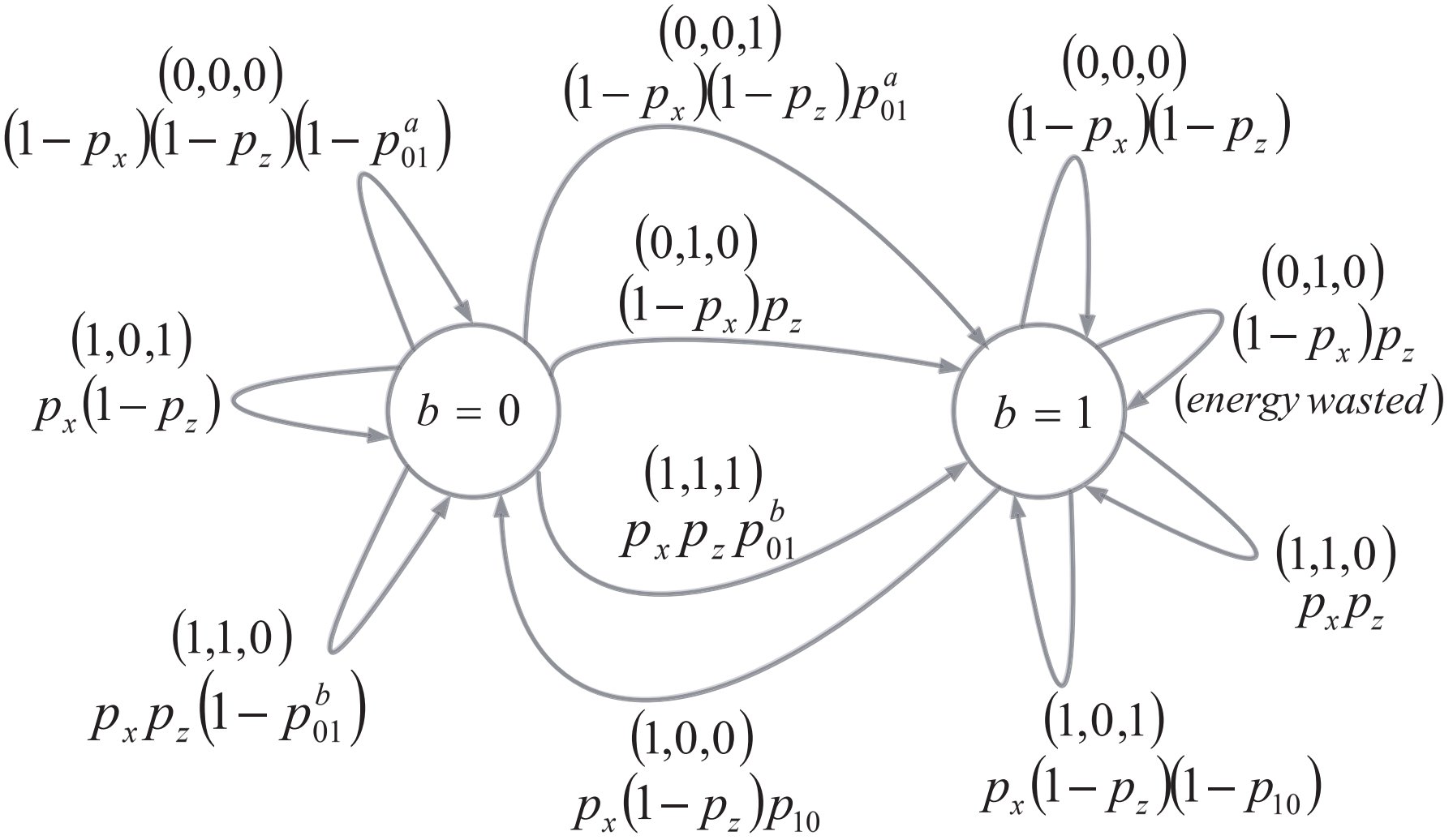


Figure 3.2: Finite state diagram for the battery-conditioned EM policy with $s = 2$ states. Each triplet in the figure corresponds to the (x, z, y) values for the corresponding transition. Transition probabilities are also included in the figure.

leakage rate I_p between X^n and Y^n is estimated as follows:

$$\begin{aligned} I_p &= \frac{1}{n}\big[H(X^n) + H(Y^n) - H(X^n, Y^n)\big] \\ &\approx H(X) - \frac{1}{n}\log p(y_1, y_2, \cdots, y_n) \\ &+ \frac{1}{n}\log p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n). \end{aligned} \tag{3.8}$$

The FSM can be represented as a trellis diagram with the state sequence $\{s_0, s_1, \cdots, s_n\}$ for the computation of the probabilities $p(y_1, y_2, \cdots, y_n)$ and $p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$. This computation is basically the forward sum-product recursion of the BCJR algorithm [115]. We define the state metrics as follows:

$$\mu_k(s_k) \triangleq p(s_k, y_1, y_2, \cdots, y_k), \tag{3.9}$$

$$\nu_k(s_k) \triangleq p(s_k, x_1, x_2, \cdots, x_k, y_1, y_2, \cdots, y_k). \tag{3.10}$$

Initially, we set the state metrics as follows:

$$\begin{aligned} \mu_0(0) &= 1, \\ \nu_0(0) &= 1, \\ \mu_0(m) &= 0, \text{ for } m \neq 0, \\ \nu_0(m) &= 0, \text{ for } m \neq 0. \end{aligned}$$

Here, we emphasize that the initial values of the state metrics do not affect the final values of $p(y_1, y_2, \cdots, y_n)$ and $p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$ due to the convergence for long sequences.

We then compute the state metrics recursively using the transition probabilities $p(x_{k+1}, z_{k+1}, y_{k+1}, s_{k+1}|s_k)$. For the binary system we use the transition probabilities labeled in Fig. 3.2. We have,

$$\mu_{k+1}(s_{k+1}) = \sum_{z_{k+1}} \sum_{x_{k+1}} \sum_{s_k} \mu_k(s_k) p(x_{k+1}, z_{k+1}, y_{k+1}, s_{k+1}|s_k), \tag{3.11}$$

$$\nu_{k+1}(s_{k+1}) = \sum_{z_{k+1}} \sum_{s_k} \nu_k(s_k) p(x_{k+1}, z_{k+1}, y_{k+1}, s_{k+1}|s_k). \tag{3.12}$$

We can compute the probabilities $p(y_1, y_2, \cdots, y_n)$ and $p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$ as the sum of all the final state metrics as follows:

$$p(y_1, y_2, \cdots, y_n) = \sum_{s_n} \mu_n(s_n), \tag{3.13}$$

$$p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \sum_{s_n} \nu_n(s_n). \tag{3.14}$$

For large n values, the state metrics $\mu_k(\cdot)$ and $\nu_k(\cdot)$ tend to zero. Therefore, in practice the recursion is computed with scale factors as follows:

$$\mu_{k+1}(s_{k+1}) = \lambda_{\mu_{k+1}} \sum_{z_{k+1}} \sum_{x_{k+1}} \sum_{s_k} \mu_k(s_k) p(x_{k+1}, z_{k+1}, y_{k+1}, s_{k+1}|s_k), \tag{3.15}$$

$$\nu_{k+1}(s_{k+1}) = \lambda_{\nu_{k+1}} \sum_{z_{k+1}} \sum_{s_k} \nu_k(s_k) p(x_{k+1}, z_{k+1}, y_{k+1}, s_{k+1}|s_k), \tag{3.16}$$

where positive scale factors $\{\lambda_{\mu_1}, \lambda_{\mu_2}, \cdots, \lambda_{\mu_n}\}$ and $\{\lambda_{\nu_1}, \lambda_{\nu_2}, \cdots, \lambda_{\nu_n}\}$ are chosen such that,

$$\sum_{s_n} \mu_n(s_n) = 1, \tag{3.17}$$

$$\sum_{s_n} \nu_n(s_n) = 1. \tag{3.18}$$

Finally, the joint probabilities can be computed from the following equations:

$$-\frac{1}{n} \log p(y_1, y_2, \cdots, y_n) = \frac{1}{n} \sum_{i=1}^{n} \log \lambda_{\mu_i}, \tag{3.19}$$

$$-\frac{1}{n} \log p(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \frac{1}{n} \sum_{i=1}^{n} \log \lambda_{\nu_i}. \tag{3.20}$$

We note here that this computation method applies to any discrete model, including an

input load with memory, and is not limited to the binary system model considered in this chapter. However, identification of the optimal system parameters becomes computationally intractable with an increase in the size of the input and output alphabets, or the battery size.

3.4 Numerical Results and Observations

In this section, we analyze the trade-off between the information leakage rate and energy efficiency numerically using the computation method presented in Section 3.3. Based on these numerical results we provide various observations and conclusions regarding the optimal operation of the EMU from a joint privacy-energy efficiency perspective. In our simulations we focus on the binary model illustrated in Fig. 3.2. We focus on a binary system for its simplicity, as otherwise, the transitions in the state diagram get very complicated and the numerical computation outlined in Section 3.3 becomes intractable. Later in Section 3.4.3 we also consider the system with $K > 2$ in the absence of an EH unit, and study the effects of the battery capacity on the performance. Furthermore, in Section 3.4.4 we consider a system with high privacy requirements in the absence of an EH unit, and allow the user to waste grid energy in order to increase privacy. In our simulations, we perform an exhaustive search by varying the transition probabilities in Fig. 3.2 with 0.1 increments and calculate the information leakage rate for each EMU policy. We use $n = 10^6$ for the computations.

3.4.1 Effects of Energy Harvesting Rate on Privacy and Energy Efficiency

We illustrate the effects of EH rate on both privacy and energy efficiency for an EH system with and without an RB, and also show how privacy and energy efficiency change in the presence of an RB. Fig. 3.3 illustrates the minimum information leakage rate I_p and the corresponding wasted energy rate E_w with respect to the EH rate p_z for an EH system with and without an RB. The results are obtained for an equiprobable input load $p_x = 0.5$ and different p_z values. In a system with an EH device the privacy improves with increasing values of p_z. This is expected since more energy is provided from the energy harvester as p_z increases; and hence, the UP can learn less about the actual energy consumption of the user. On the other hand, an increase in the EH rate leads to an increase in the wasted energy rate as well. This is due to the independence of the energy generation process and the input load. When the EH device harvests a unit of energy, if there is no demand from the appliances and the RB is already charged, this harvested energy will be wasted. Therefore, we can easily notice the trade-off between the information leakage rate I_p and the wasted energy rate E_w in the system when there is no storage unit.

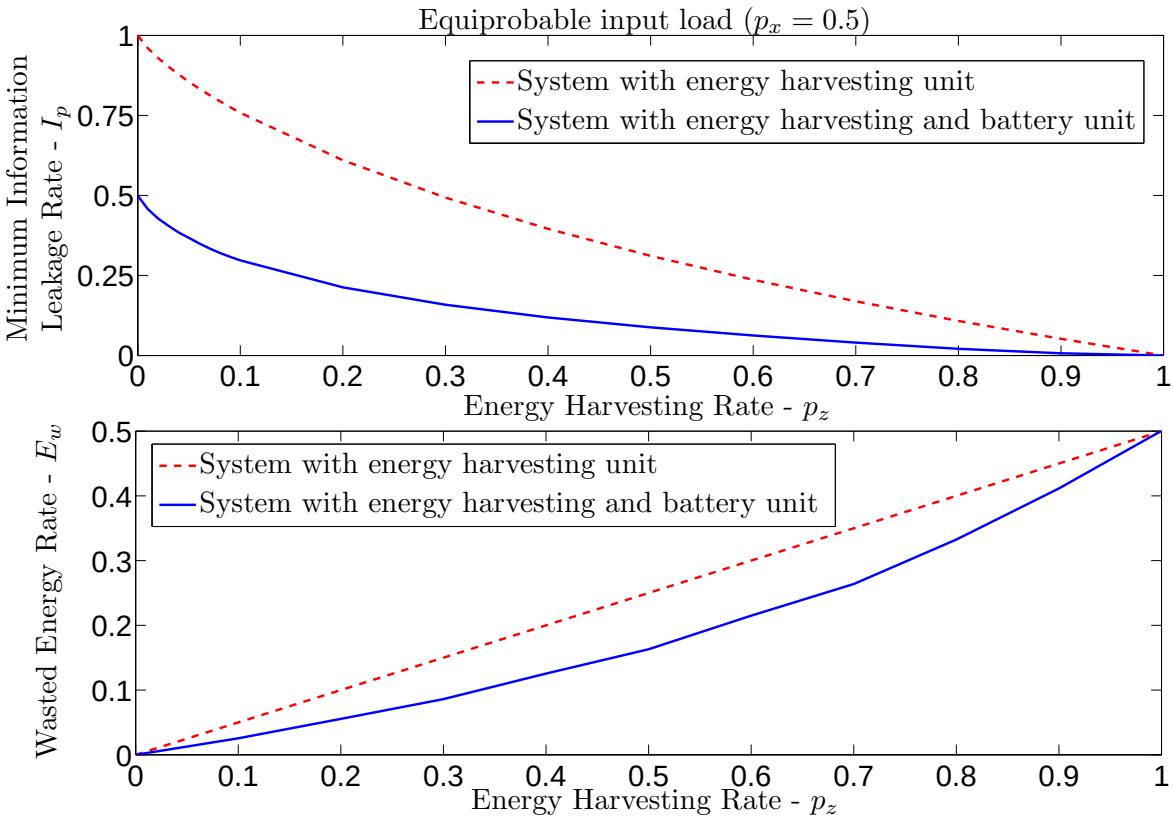


Figure 3.3: Minimum information leakage rate, I_p, and the corresponding wasted energy rate, E_w, with respect to harvested energy rate for an EH system with and without an RB.

Comparing the two curves in Fig. 3.3, we observe that introducing an RB into the system improves the trade-off to a certain extent. It reduces both the minimum information leakage rate I_p and the corresponding wasted energy rate E_w. When there is no EH, i.e, $p_z = 0$, the system reduces to the model studied in [87]. In this case, the minimum information leakage rate is found to be $I_p = 0.5$ for $p_x = 0.5$. However, when there is an alternative energy source in the system, i.e., $p_z \neq 0$, the information leakage rate can be reduced significantly. The EH rate can be considered as a system parameter that defines the achievable privacy-energy efficiency trade-off, and needs to be chosen by the system designer depending on the input load and the desired operating point.

3.4.2 Privacy-Energy Efficiency Trade-Off

In Section 3.4.1 we have found the wasted energy rate corresponding to the battery policy that minimizes the information leakage rate. Here, we characterize the whole trade-off between the privacy and energy efficiency for given EH rates. The trade-off for the values of $p_x = p_z = 0.5$ is illustrated in Fig. 3.4. Each circle in the figure marks an $\left(I_p, E_w\right)$ pair that can be achieved by assigning different transition probabilities labeled on Fig. 3.2. The Pareto optimal trade-off

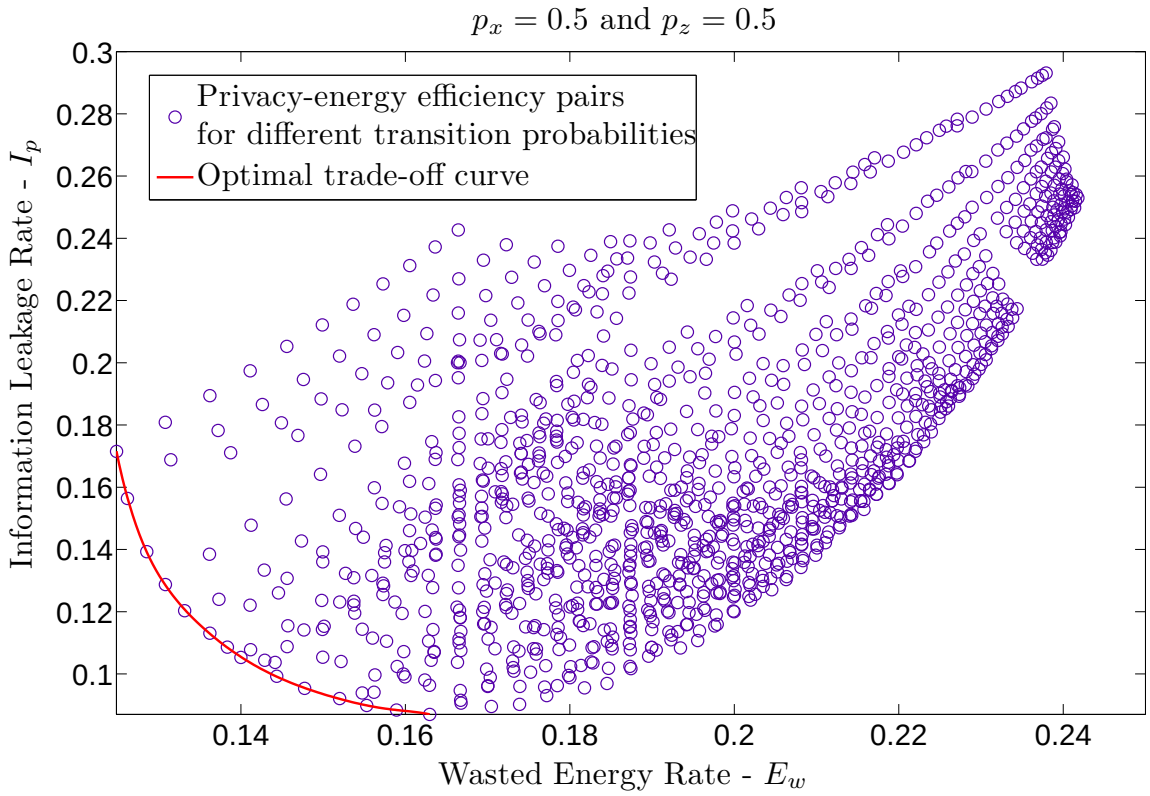


Figure 3.4: Information leakage rate, I_p, versus wasted energy rate, E_w, for $p_x = 0.5$ and $p_z = 0.5$.

curve is the one that is formed by the points on the lower-left corner of the figure, i.e., the points for which I_p and E_w cannot be improved simultaneously. The minimum information leakage rate value is $I_p = 0.088$ for which we have $E_w = 0.163$. The minimum wasted energy rate is $E_w = 0.125$ for which we have $I_p = 0.171$. These two pairs correspond to the corner points of the trade-off curve in Fig. 3.4. According to the requirements of the system, the operating point can be chosen anywhere on the trade-off curve. Note that, we can apply a convexification operation on the set of achievable (I_p, E_w) pairs using time-sharing arguments.

We also study the trade-off between the information leakage rate, I_p, and the wasted energy rate, E_w, for different p_z values to observe the effect of the EH rate on the achievable privacy-energy efficiency trade-off. Fig. 3.5 illustrates the Pareto optimal $\left(I_p, E_w\right)$ pairs for $p_x = 0.5$ and for different p_z values. Each marker in the figure marks an $\left(I_p, E_w\right)$ pair achieved by assigning different transition probabilities, and we include only the points that are not Pareto dominated by any other point. We obtain a different privacy-energy efficiency trade-off for each p_z value as illustrated in Fig. 3.5. The corner points of these trade-off curves are listed in Table 4.1 for different p_z values. Since there is no harvested energy in the system for $p_z = 0$, there is no wasted energy and as a result, the optimal operating point is found as the minimum information leakage rate, $I_p = 0.5$ and wasted energy rate, $E_w = 0$, which is the same as the

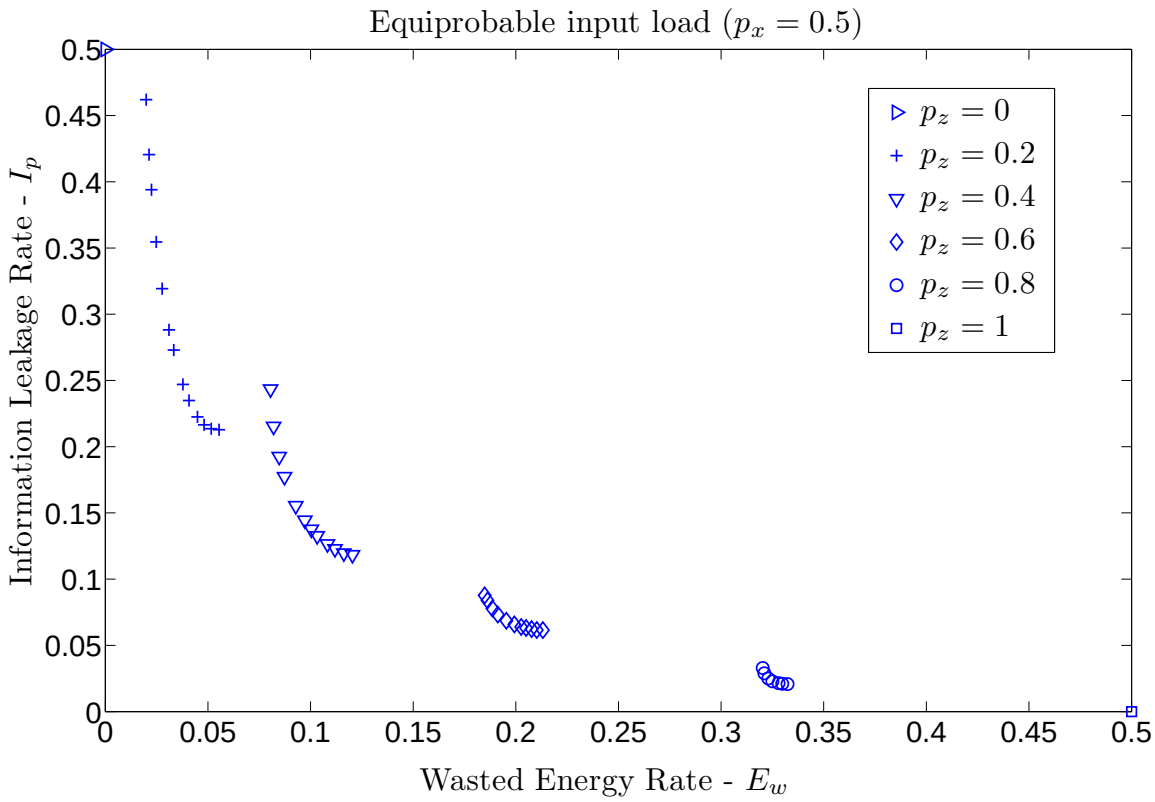


Figure 3.5: The Pareto optimal (I_p, E_w) pairs for $p_x = 0.5$ and for different p_z values. Optimal pairs for different p_z values are illustrated with different markers.

model studied in [87]. Note that while the minimum information leakage rate decreases with increasing values of p_z, the minimum wasted energy rate increases. When energy is harvested with $p_z = 1$, the optimal point is found to be $I_p = 0$ and $E_w = 0.5$, that is, perfect privacy can be achieved at the expense of wasting half of the harvested energy on average. In this case, there is no information leakage since the user never asks energy from the UP and the wasted energy rate converges to $Pr\{X = 0\} = 1 - p_x$.

We also study biased input loads by considering the two cases with $p_x = 0.89$ and $p_x = 0.11$, which we call the *heavy load* and *light load* scenarios. The entropy rate of the input load for both the heavy and light load cases is $H(X) = 0.5$. Note that the input load is biased towards $X = 1$ for the heavy load system, i.e., the appliances are more likely to demand energy. For the heavy load case when we do not have an EH unit in the system, i.e., $p_z = 0$, we find the minimum information leakage rate to be $I_p = 0.23$ [87]. When there is an energy harvester in the system with $p_z = 0.5$, the minimum information leakage rate reduces significantly to $I_p = 0.026$ while the corresponding wasted energy rate is $E_w = 0.043$. The minimum wasted energy rate is obtained as $E_w = 0.011$ for which we have $I_p = 0.105$. It is obvious that wasting energy is less likely in the heavy load case. The energy is wasted only when we have $b_i = 1, x_{i+1} = 0, z_{i+1} = 1$ as shown in Fig. 3.2. Thus, when the appliances have higher energy

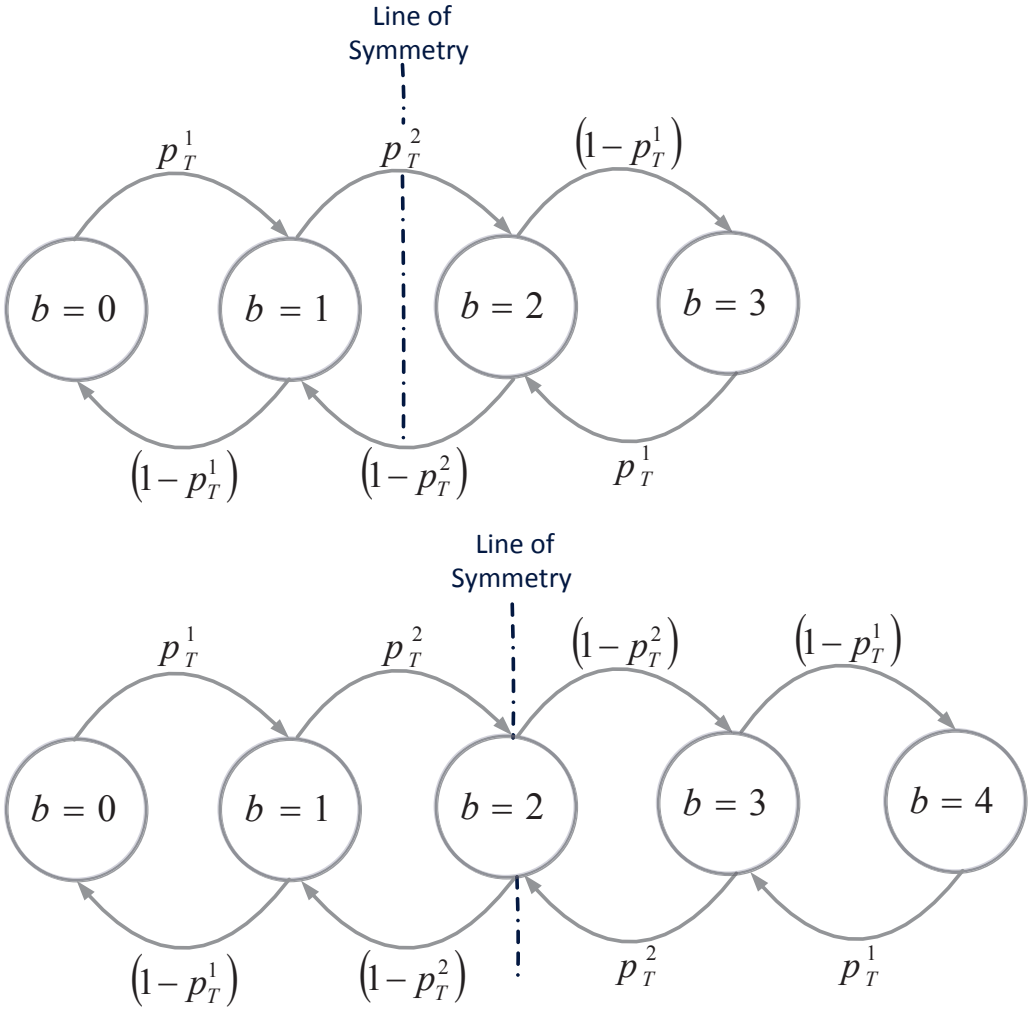


Figure 3.6: Finite state diagrams for battery-conditioned EM policies with battery capacities $K = 3$ and $K = 4$. Symmetric and complementary transition probabilities are illustrated for the computation of the minimum information leakage rate in case of an equiprobable input load, i.e., $p_x = 0.5$.

Table 3.1: RESULTS FROM THE TRADE-OFF PAIRS FOR DIFFERENT p_z VALUES

p_z	$\min I_p$	E_w for $\min I_p$	$\min E_w$	I_p for $\min E_w$
0	0.5	0	0	0.5
0.2	0.213	0.055	0.02	0.462
0.4	0.118	0.12	0.081	0.243
0.6	0.062	0.213	0.185	0.088
0.8	0.02	0.332	0.32	0.032
1	0	0.5	0.5	0

demands, the user is less likely to face the condition for energy wasting. Similarly, in the light load case, i.e., $p_x = 0.11$, E_w increases as less energy is required by the appliances. For example, the minimum information leakage rate is found to be $I_p = 0.027$ with $E_w = 0.088$, and the minimum wasted energy rate is found to be $E_w = 0.087$ for $I_p = 0.03$. We observe that both the heavy and light load systems can achieve almost the same level of maximum privacy while the wasted energy rate of the light load system is double the rate of the heavy load system at this point of operation.

3.4.3 Effects of Battery Capacity on Privacy

We have observed that alternative energy sources can help reduce the information leakage rate significantly while RBs help improve the energy efficiency as well as privacy. Next, we study the effects of the RB capacity on privacy. It is expected that if we increase the RB capacity K, the trade-off curve illustrated in Fig. 3.4 will move toward the origin, i.e., the privacy and energy efficiency will be improved simultaneously. For example, in the asymptotic limit of infinite storage capacity, perfect privacy can be achieved by charging the battery initially, and never asking for any energy from the UP afterwards. To highlight the effects of the battery capacity on the achievable privacy we consider an RB with capacity K, and no EH device. While the complexity of the numerical analysis grows quickly with the battery size, we have observed that for an equiprobable input load, i.e., $p_x = 0.5$, there is a symmetry and complementarity among the optimal transition probabilities in the finite state diagram which significantly reduces the computation time of the minimum information leakage rate. The minimum information leakage rate is achieved when, $1)$ the sum of transition probabilities between two states is equal to one, and $2)$ there is a symmetry in the transition probabilities of the two sides of the finite state diagram separated by the line of symmetry. Fig. 3.6 depicts this symmetry and

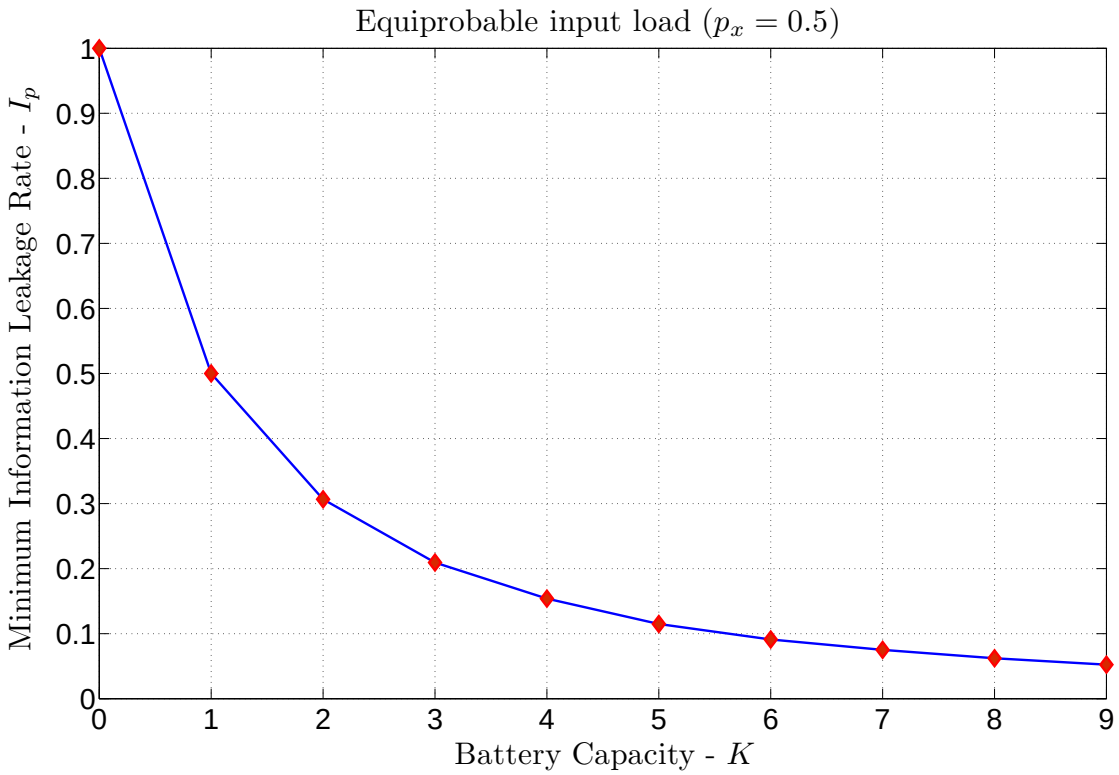


Figure 3.7: Minimum information leakage rate, I_p, versus battery capacity, K.

complementarity on a finite state diagram for battery capacity $K = 3$ and $K = 4$, respectively. Using this observation which reduces the complexity of the computation, we have increased the battery capacity K and obtained the minimum information leakage rates corresponding to different values of K. For moderate battery capacity values Fig. 3.7 illustrates the effects of the battery capacity on the minimum information leakage rate I_p for $p_x = 0.5$. The minimum information leakage rate falls below 0.1 even with an RB of 6 units of capacity. This result shows that even a small increase in the RB capacity leads to a significant reduction in the minimum information leakage rate. As RB capacity increases more, the minimum information leakage rate I_p continues to decrease, but with a decreasing slope.

3.4.4 Privacy at the Expense of Wasting Grid Energy

We have already shown that whenever the user has higher privacy requirements, the system with EH and RB units can provide strong privacy assurances by simply increasing the EH rate, p_z. When there is no EH unit in the system, we need to increase the capacity of the RB to cope with high privacy requirements. However, increasing the capacity of the RB can be costly or even physically impossible. In this case the privacy of the user can be improved by allowing the user to demand energy from the UP even when there is no energy demand from the appliances,

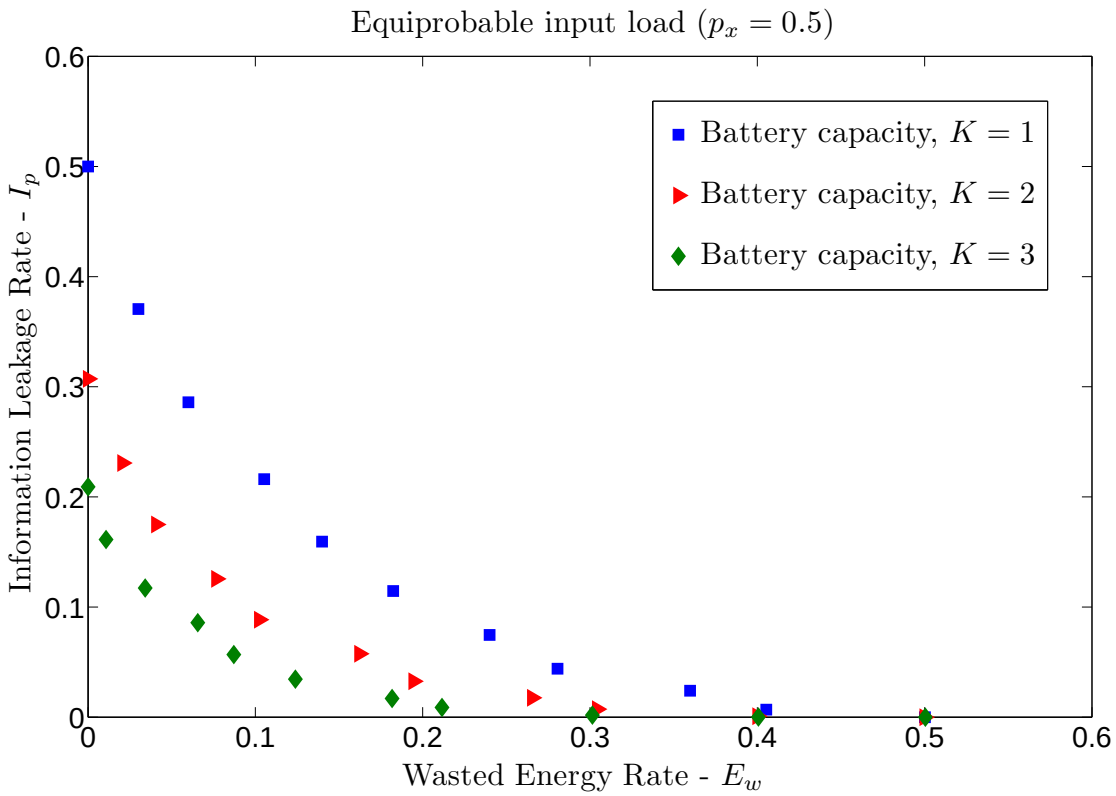


Figure 3.8: Information leakage rate, I_p, versus wasted energy rate, E_w, for the case of wasting grid energy.

i.e., $x_i = 0$, and the RB is already full, i.e., $b_i = K$. Through wasting additional energy from the UP, which is likely to be more expensive than the harvested energy, the energy consumption profile of the appliances can be further hidden from the UP and privacy can be increased up to perfect privacy by increasing the energy waste level.

To study the effects of wasting grid energy on privacy, we consider battery-conditioned policies with binary input/output load values and an RB with capacity of K units. Let RB be fully charged at time instant i, i.e., $b_i = K$. Even if the appliances do not consume any energy at time instant $i+1$, i.e., $x_{i+1} = 0$, we allow the EMU to demand energy from the UP, i.e., $y_{i+1} = 1$, with probability p_w, and $y_{i+1} = 0$ with probability $(1-p_w)$. In other words, we allow wasting the grid energy with probability p_w, by which we obscure the information of the UP about the real energy consumption. Fig. 3.8 illustrates the achievable points on the $\left(I_p, E_w\right)$ trade-off, obtained for an equiprobable input load, $p_x = 0.5$, and for increasing RB capacity values, $K = 1$, $K = 2$, and $K = 3$. In this simulation, to keep the simulation time reasonable we find the achievable points for each capacity value K, by considering only complementary transition probabilities as depicted in Fig. 3.6, such that the sum of the transition probabilities between two states is equal to 1. Moreover, we compute the wasted energy rate by using Eqn. (3.6), but we choose $Z_i = 0$ in the equation since there is no EH unit in the current scenario. We can

see that the privacy can be significantly improved by wasting more energy, i.e., by increasing p_w. For instance, when perfect privacy is required by the system, the information leakage rate can be reduced to zero by wasting energy with $p_w = 1$. The wasted energy rate converges to $Pr\{X = 0\} = 1 - p_x$ on average for $p_w = 1$, i.e., $E_w = 0.5$, because we waste energy only when the RB is fully charged, $b_i = K$, and there is no input load, $X_i = 0$. If we increase the RB capacity K, as we can see in Fig. 3.8, both the information leakage rate and the wasted energy rate are improved for the same energy waste probability, p_w. The operating point on the trade-off curve can be chosen according to the privacy requirement of the system and the cost of energy provided by the UP.

3.5 Conclusions

In this chapter, we have studied the privacy-energy efficiency trade-off for SM systems in the presence of EH and storage units. We have considered an EH unit that provides energy packets at each time instant in an i.i.d. fashion, and a finite capacity RB that provides both energy efficiency by storing extra energy for future use, and increased privacy by hiding the load signature of the appliances from the UP. We have used an FSM to represent the whole system, and studied the information leakage rate between the input and output loads to measure the privacy of the user from an information theoretic perspective.

We have used a numerical method to calculate the information leakage rate. Due to the memory introduced by the RB, obtaining a closed-form expression for the information leakage rate is elusive. For the sake of simplicity, we have considered binary input and output loads and focused on battery-dependent EM policies in our simulations, and numerically searched for the EM strategy that achieves the best trade-off between privacy and energy-efficiency. We have shown that the information leakage rate can be significantly reduced when both an energy harvester and an RB are present. As the EH rate increases, we have observed that the privacy of the system significantly improves. On the other hand, this also increases the amount of wasted energy. For a fixed EH rate, we have numerically obtained the optimal trade-off curve between the achievable information leakage and wasted energy rates. Different points on this trade-off curve can be achieved by changing the stochastic battery policy used by the EMU. According to the needs and priorities of the system, an operating point can be chosen on this trade-off curve. We have also obtained the corresponding trade-off curves for different EH rates.

We have studied the effects of the battery capacity on the achievable privacy by focusing on a system with only an RB. We have observed that increasing the capacity of the RB has a significant impact on the reduction of the information leakage rate, and thereby, on the privacy. Moreover, we have examined the wasting of grid energy to fulfill the increased privacy require-

ments of the user when there is only an RB in the system. We have observed that even in the absence of an EH device and with a finite capacity RB, the privacy level can be increased up to perfect privacy by wasting more energy from the grid.

Chapter 4

Privacy-Cost Trade-offs in Demand-Side Management with Storage

4.1 Introduction

In the previous chapter, we studied an SM system in the presence of EH and storage units, where the storage unit was utilized to increase the privacy of the user by hiding the energy consumption profile from the UP and increase the energy efficiency of the system by storing extra harvested energy. Demand-side EM with the help of a storage device can also be used to provide cost benefits to users. For example, the UPs can support time-of-use electricity pricing based on fine-grained SM readings and encourage the users to dynamically shift their demands to off-peak hours with the promise of reducing their energy costs. Demand shifting can also help avoid peak-to-average ratio in energy consumption, which typically increases the cost of energy generation and distribution. Accordingly, in this chapter we consider the scenario, in which the storage unit is utilized to provide privacy and energy cost savings to the user.

We consider the SM system depicted in Fig. 4.1. The power flow is managed by the EMU. Considering the real power flows through the system, the EMU satisfies the power demands of the appliances, X_i, from the power grid and the RB. We do not allow any outages or shifting of user demands. The SM realizes the information flow between the user and the UP, that is, it measures the output load, Y_i, and reports it to the UP at certain time instants without any tampering. Assuming that the electricity price is time-varying, the EMU utilizes the RB to reduce the user's energy consumption cost, as well as to mask the power consumption profile of the user from the UP and other third parties. We assume that perfect privacy can be achieved if a constant SM reading is reported to the UP over time [85]. Consequently, we measure user privacy in terms of the variation of the output load, Y_i, from a constant target consumption value

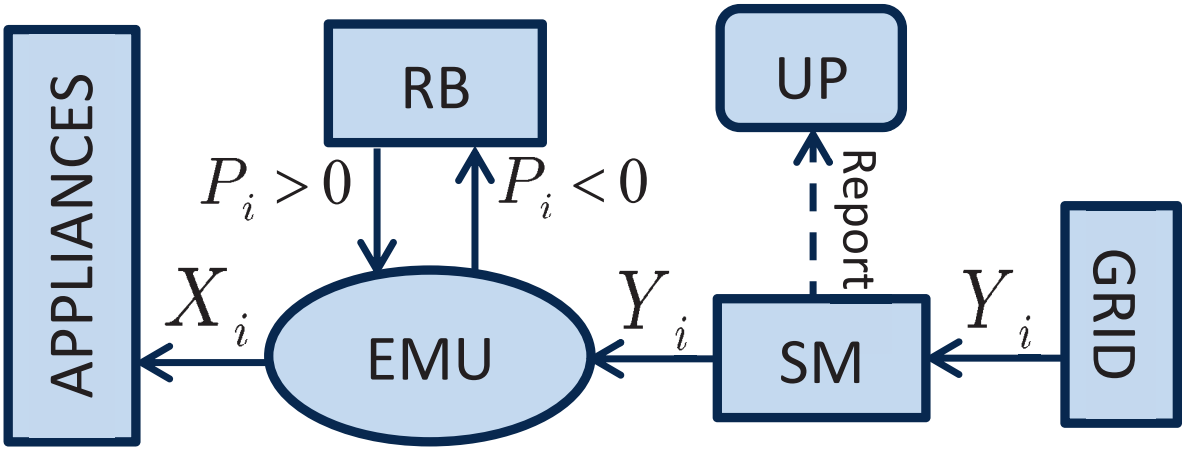


Figure 4.1: An SM system diagram with an EMU and an RB at the user's household. The EMU manages the power flows (solid lines) among the power grid, the appliances and the RB. The SM realizes the information flow (dashed line) by reporting its power readings to the UP at certain time instants.

over the period of interest. In addition to the load variance, we evaluate an information theoretic privacy measure, *the information leakage rate*, which is defined as the mutual information rate between the power demands of the appliances and the SM readings. Mutual information has previously been proposed as a measure of privacy in SM systems and several works in [48–50, 52, 86, 87, 89–91, 101–108]. Note that information theoretic privacy takes into account the statistics of the input load, X_i. Hence, the information leakage rate, which measures the average mutual information between the input and output loads, is also studied as a complementary privacy measure in order to support the validity of the load variance as a valid and robust privacy measure. On the other hand, the average energy cost is measured with a time-varying time-of-use electricity pricing model. Our goal here is to characterize EM policies that jointly increase the privacy of the user and reduce the energy cost over a given period of time under an RB capacity constraint.

We first characterize the optimal EM policy under the offline optimization framework which assumes that the energy demands as well as the electricity prices are known non-causally by the EMU over the period of interest. We formulate the joint privacy-energy cost minimization as a convex optimization problem. We identify the structure of the optimal EM policy by solving this convex optimization problem, and based on this structure, we provide a *backward water-filling algorithm*, which efficiently finds the optimal EM policy. For ease of exposure, we provide a graphical interpretation for the proposed algorithm, in which the energy received from the grid can only be shifted to earlier TSs, and the water levels can be equalized to the extend the RB capacity allows.

We next study the online optimization problem considering only causal knowledge of the

power demands at the EMU, that is, the EMU knows only the energy demand at the current TS. We characterize the optimal online policy using DP. Since DP algorithms are prohibitively complex, we propose a simple yet efficient heuristic online algorithm based on the backward water-filling algorithm obtained in the offline setting. Finally, we numerically evaluate the load variance and the information leakage rate privacy measures, and characterize the trade-off between the user's privacy and energy cost resulting from the proposed offline and online EM policies. The operating points on this trade-off can be chosen based on the user's requirements on privacy and energy cost. We also investigate the impact of the RB capacity on the performance of the proposed EM policies.

As it has presented in the state of the art in Chapter 2, several techniques have been studied in the literature to provide a certain level of privacy to SM users. On the one hand, privacy can be provided by tampering the SM readings before being reported to the UP. Following this approach, [101] proposes the compression of SM data, [70] considers sending the aggregated energy consumption of a group of users, and [116] considers adding random noise to the SM readings to protect user's privacy. On the other hand, without tampering the SM readings, privacy can also be achieved by demand-side management with the utilization of storage units, such as RBs [48–52, 85, 87, 89, 91–93, 102], and alternative energy sources, such as a renewable energy source like a solar panel [48–50], [103], [104]. In [48] and [50] user's privacy is protected by using an RB and a renewable energy source from an information theoretic perspective. Heuristic algorithms are proposed in [85], [89] and [91]. The joint optimization of privacy and energy cost for SMs with the utilization of an RB is addressed in [92], [93] and [102]. The authors in [92] and [93] propose online control algorithms based on stochastic DP and Lyapunov optimization techniques, respectively. The authors in [102] and [108] study a stochastic control model, formulated as a partially observeable Markov decision process. The optimal stochastic strategy is computationally challenging to obtain due to the continuous state-action space; while approximate solutions can be obtained numerically through discretization, or upper and lower bounds can be derived.

The main contributions of this chapter are summarized next:

- We consider the SM system illustrated in Fig. 4.1, and study the design of EM policies that aim at minimizing a joint privacy-cost objective.
- Assuming non-causal knowledge of the user's power demands and the electricity prices at the EMU, we formulate the optimal privacy-cost trade-off in the offline setting as a convex optimization problem. We identify the structure of the optimal solution, and provide a backward water-filling algorithm for computing it.
- Assuming causal knowledge of the user's power demands at the EMU, we solve the on-

line optimization problem by means of DP. Additionally, we provide an efficient heuristic algorithm that uses the optimal offline algorithm to solve a particular subproblem constructed at each iteration.

- The information leakage rate between the user's power demand profile, i.e., the input load X^N, and the SM readings, i.e., the output load Y^N, is evaluated and compared to the load variance as a privacy measure. Finally, the performances of the proposed offline and online EM policies are assessed through numerical simulations, using a real power consumption data set. The trade-off between the user's privacy and the energy cost, as well as the impact of the RB capacity on this trade-off are characterized for the proposed policies.

The remainder of the chapter is structured as follows. In Section 4.2, we describe the system model. In Section 4.3, we characterize the optimal offline EM policy and provide the backward water-filling algorithm. The optimal and heuristic online EM policies are proposed in Section 4.4. In Section 4.5, we explain how to characterize the information leakage rate. In Section 4.6, extensive numerical results are presented. Finally, Section 4.7 concludes the chapter.

4.2 System Model

We consider a discrete-time power consumption model in a household (see Fig. 4.2(a)). In this model, each appliance consumes constant power for an arbitrary duration when it is active. Appliances can be in active or inactive state at any time. Let $t^p_0 = 0 < t^p_1 < \cdots < t^p_{(K-1)} < T$ be the time instants at which there is a change in the state of at least one appliance. We denote the total power consumption within $[t^p_{(k-1)}, t^p_k]$ by X^p_k (kW) for $k = \{1, 2, \ldots, K\}$.

We also consider a time-varying electricity pricing model in which the cost per unit energy changes over time at certain time instants, and remains constant in between (see Fig. 4.2(b)). Let $t^c_0 = 0 < t^c_1 < \cdots < t^c_{(M-1)} < T$ be the time instants at which the cost of energy changes. We denote the cost per unit energy within $[t^c_{(m-1)}, t^c_m]$ by C^c_m (cent/kWh) for $m = \{1, 2, \ldots, M\}$. We can combine the time instants at which the power consumption or the cost per unit energy changes into a single time series $t_0 = 0 < t_1 < \cdots < t_{N-1} < t_N = T$ (see Fig. 4.2(c)). The duration of the TS between two consecutive time instants is denoted by $\tau_i \triangleq t_i - t_{i-1}$ (sec), for $i = 1, 2, \ldots, N$. We denote the total power consumption and the cost per unit energy within TS i as X_i (kW) and C_i (cent/kWh), respectively. Note that for any two consecutive TSs, either the power demand or the cost per unit energy, or both may change, whereas they remain constant within each TS. In our model, TSs do not necessarily have the

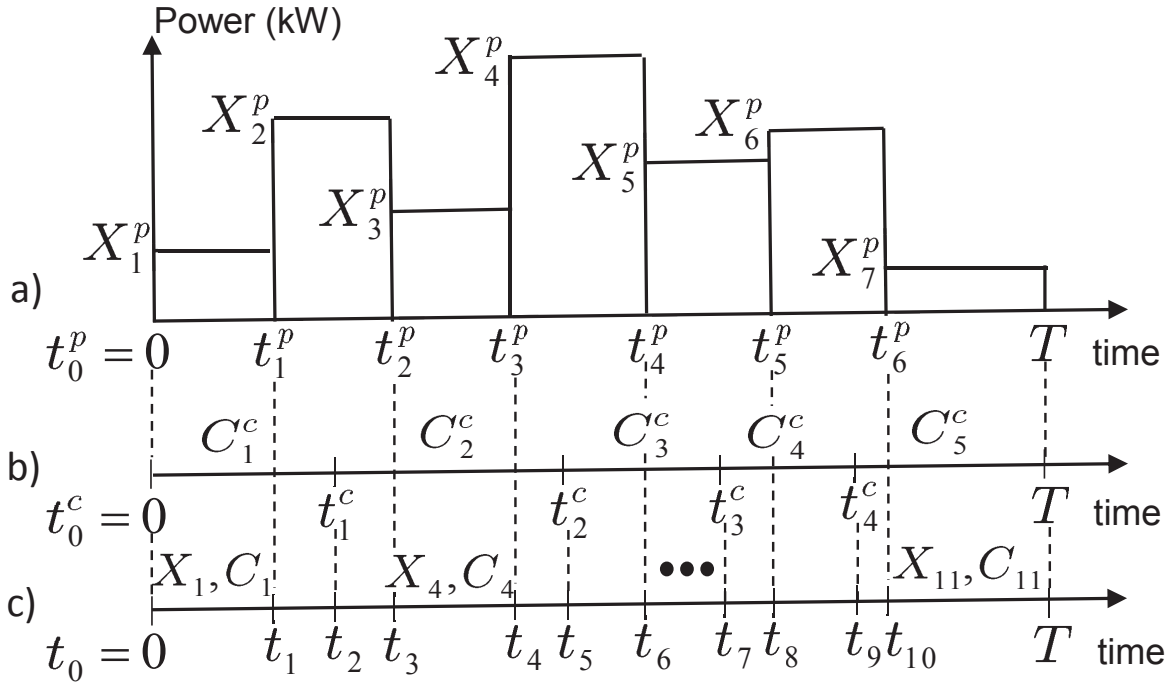


Figure 4.2: Illustration of the timelines for the total power demand of the household, and the cost per unit energy. The total power demand, i.e., the input load, changes at time instants $t_1^p, t_2^p, \ldots, t_6^p$, while the price of energy changes at time instants $t_1^c, t_2^c, t_3^c, t_4^c$.

same duration.

Following the discrete-time power consumption and pricing model illustrated in Fig. 4.2, we study the power input/output system depicted in Fig. 4.1. The input load X_i (kW) and the output load Y_i (kW) denote the real power consumption of appliances and the real power drawn from the grid at TS i, respectively. We consider an SM that reports the output load, Y_i, to the UP at each TS i, correctly without any tampering[1]. We integrate an RB with a finite capacity B_{max} (kWh), and an EMU which manages the power flow among the grid, the appliances and the RB. The EMU can use both the power grid and the RB to satisfy the user's power demand X_i, as $X_i = Y_i + P_i$, where P_i (kW) is the power charged to ($P_i < 0$), or discharged from ($P_i > 0$) the RB during TS i, and $Y_i \in \mathbb{R}^+$, where $\mathbb{R}^+$ denotes the set of nonnegative real numbers. In this framework, we consider EM policies that jointly increases the privacy and reduces the energy cost of the user within the time frame $[0, T]$ by utilizing the RB. Let us define the input and output load vectors as $X^N = (X_1, X_2, \ldots, X_N)$ and $Y^N = (Y_1, Y_2, \ldots, Y_N)$, respectively. Note that an EM policy corresponds to the vector of output loads Y^N.

We assume that perfect privacy is achieved if the output load Y_i is equal to a constant value $\bar{E}$ within $[0, T]$. Ideally, if the user has a flat power demand from the grid at all times, we

[1]We assume that Y_i remains constant within each TS i. In the sequel, we will show that this assumption is indeed optimal. Accordingly, there is no loss of information on the UP side by SM reporting once per TS.

assume that the UP cannot learn anything about the user's energy consumption behaviour [85]. Accordingly, the privacy of an EM policy is measured by the *load variance*, defined as:

$$\mathcal{V} \triangleq \frac{1}{T}\sum_{i=1}^{N} \tau_i \cdot (Y_i - \bar{E})^2. \tag{4.1}$$

Observe that perfect privacy is achieved when $\mathcal{V} = 0$, in which case $Y_i = \bar{E}$ for $\forall i$.

The *average energy cost* of an EM policy is defined as:

$$\mathcal{C} \triangleq \frac{1}{T}\sum_{i=1}^{N} \tau_i \cdot Y_i \cdot C_i. \tag{4.2}$$

We assume that all the energy demands of appliances must be satisfied at the time that they are requested, i.e., we guarantee that the appliances do not incur any outages, and we do not allow rescheduling; hence, assuming that the RB is empty at $t = 0$, the output load values have to satisfy the following constraints:

$$\sum_{j=1}^{i} \tau_j \cdot X_j \leq \sum_{j=1}^{i} \tau_j \cdot Y_j, \;\; i = 1, \ldots, N. \tag{4.3}$$

On the other hand, the energy that has been drawn prior to the demand of the appliances needs to be stored in the RB. Since the RB capacity is finite, the battery energy at TS i should satisfy:

$$B_i \triangleq \sum_{j=1}^{i} \tau_j \cdot (Y_j - X_j) \leq B_{max}, \;\; i = 1, \ldots, N. \tag{4.4}$$

We note here that the constraint in (4.4) assumes that energy cannot be drawn from the grid to be wasted solely for the sake of privacy. However, we do not constraint the final battery state to be empty; therefore, more energy than requested by the appliances can be drawn to be left in the battery at the end of TS N.

It is possible to show that the set of all achievable $(\mathcal{V}, \mathcal{C})$ pairs under constraints (4.3) and (4.4) form a convex region. Then the optimal operating points are characterized by the Pareto boundary of this region. Hence, we use the weighted average of $\mathcal{V}$ and $\mathcal{C}$ to identify all the points on the Pareto boundary. The convex optimization problem can be written as follows:

$$\begin{aligned}
\underset{Y_i \geq 0}{\text{minimize}} \quad & \sum_{i=1}^{N} \left[\theta \cdot \tau_i \cdot \left(Y_i - \bar{E} \right)^2 + (1-\theta) \cdot \tau_i \cdot Y_i \cdot C_i \right] \\
\text{subject to} \quad & \sum_{j=1}^{i} \tau_j \cdot (X_j - Y_j) \leq 0, \qquad i = 1, \ldots, N, \\
& \sum_{j=1}^{i} \tau_j \cdot (Y_j - X_j) \leq B_{max}, \quad i = 1, \ldots, N,
\end{aligned} \tag{4.5}$$

where $0 < \theta \leq 1$ is the parameter that adjusts the trade-off between privacy and energy cost. The value of θ can be set in advance by the user. If $\theta = 1$, then the user is interested only in maximizing the privacy; and if $\theta = 0$, the user aims at only minimizing the energy cost. Since the cost per unit energy and the input load remain constant over each TS, it follows from the convexity of the objective function in (4.5) that the optimal output load must remain constant within a TS [117]. Hence, the assumption of having the SM report only once per TS does not lead to any loss of information on the UP side.

In Section 4.3, we identify the *optimal offline EM policy* as the optimal solution to (4.5), in which all power demands and prices are known non-causally by the EMU in advance at $t_0 = 0$. While non-causal knowledge of the user's future energy consumption may not be realistic for certain appliances, activity patterns of majority of appliances, such as refrigerators, heating, programmable washing machines and dish washers, electrical vehicle charging, etc., are either deterministic or highly predictable during their operation periods [118]. Alternatively, we will also study the online optimization of the EM policy in Section 4.4.

4.3 Optimal Offline Energy Management (EM) Policy

We provide the optimal offline EM policy as the solution to the convex optimization problem in (4.5) for $0 < \theta \leq 1$. We define the Lagrangian function [119] with Lagrangian multipliers $\lambda_i \geq 0$, $\mu_i \geq 0$ and $v_i \geq 0$, $i = 1, \ldots, N$, as follows:

$$\begin{aligned}\mathcal{L} = &\sum_{i=1}^{N}\Big[\theta\tau_i\big(Y_i-\bar{E}\big)^2+(1-\theta)\tau_i Y_i C_i\Big]\\ &+\sum_{i=1}^{N}\lambda_i\Big(\sum_{j=1}^{i}\tau_j(X_j-Y_j)\Big)\\ &+\sum_{i=1}^{N}\mu_i\Big(\Big(\sum_{j=1}^{i}\tau_j(Y_j-X_j)\Big)-B_{max}\Big)\\ &-\sum_{i=1}^{N}v_i Y_i. \end{aligned} \tag{4.6}$$

Corresponding complementary slackness conditions are:

$$\lambda_i\Big(\sum_{j=1}^{i}\tau_j(X_j-Y_j)\Big)=0,\ \ i=1,\dots,N, \tag{4.7}$$

$$\mu_i\Big(\Big(\sum_{j=1}^{i}\tau_j(Y_j-X_j)\Big)-B_{max}\Big)=0,\ \ i=1,\dots,N, \tag{4.8}$$

$$v_i Y_i=0,\ \ i=1,\dots,N. \tag{4.9}$$

We apply the Karush Kuhn Tucker (KKT) necessary conditions on the Lagrangian function:

$$\frac{\partial\mathcal{L}}{\partial Y_i}=2\theta\tau_i\big(Y_i^*-\bar{E}\big)+(1-\theta)\tau_i C_i+\tau_i\sum_{j=i}^{N}(\mu_j-\lambda_j)-v_i=0. \tag{4.10}$$

Then the optimal output load at TS i, Y_i^*, is found in terms of the Lagrange multipliers, the weighted cost level, $\bar{C}_i$, and the trade-off parameter θ, as follows:

$$Y_i^*=\left[\left(\frac{\sum_{j=i}^{N}(\lambda_j-\mu_j)}{2\theta}+\bar{E}\right)-\bar{C}_i\right]^+,\ \ \forall i, \tag{4.11}$$

where $[x]^+$ is equal to x if $x\geq 0$, and 0 otherwise, and the *weighted cost level*, $\bar{C}_i$, at TS i is defined as:

$$\bar{C}_i \triangleq \frac{(1-\theta)C_i}{2\theta}, \ \forall i. \tag{4.12}$$

We note that the solution in (4.11) resembles the classical waterfilling solution [94], where $Y_i + \bar{C}_i$ corresponds to the *water level* in TS i. With this correspondence, one can interpret the optimal EM policy as pouring water over TSs. In our model water corresponds to the energy allocated to each TS, and it has to satisfy certain conditions. We next identify some properties of the optimal EM policy based on the KKT conditions in (4.7)-(4.10), which are both necessary and sufficient due to the convexity of the optimization problem in (4.5). Then, we discuss the implications of these properties.

Lemma 4.1. *In the optimal EM policy, given $Y_i > 0 \ \forall i$, whenever the water level, i.e., $Y_i + \bar{C}_i$, increases (decreases) from TS i to TS $i+1$, i.e., $Y_i + \bar{C}_i < Y_{i+1} + \bar{C}_{i+1}$ ($Y_i + \bar{C}_i > Y_{i+1} + \bar{C}_{i+1}$), the RB must be full (empty) at TS i, i.e., $B_i = B_{max}$ ($B_i = 0$). Moreover, if the RB is neither empty nor full at TS i, i.e., $0 < B_i < B_{max}$, then the water level does not change from TS i to TS $i+1$, i.e., $Y_i + \bar{C}_i = Y_{i+1} + \bar{C}_{i+1}$.*

Proof. From the slackness conditions in (4.7) and (4.8), we can argue that the RB is full whenever $\lambda_i = 0$ and $\mu_i > 0$, and the RB is empty whenever $\lambda_i > 0$ and $\mu_i = 0$. Note that λ_i and μ_i cannot be positive simultaneously. This is because whenever the i-th constraint in (4.4) is satisfied with equality, i.e., $\mu_i > 0$, the i-th constraint in (4.3) cannot be satisfied with equality, i.e., $\lambda_i = 0$, and vice versa. From (4.11), we see that $Y_i + \bar{C}_i < Y_{i+1} + \bar{C}_{i+1}$ implies $\lambda_i = 0$ and $\mu_i > 0$, and $Y_i + \bar{C}_i > Y_{i+1} + \bar{C}_{i+1}$ implies $\lambda_i > 0$ and $\mu_i = 0$. Therefore, we can conclude that whenever the water level increases (decreases) from TS i to TS $i+1$, the RB must be full (empty) at TS i. Moreover, if the RB is neither empty nor full at TS i, i.e., $0 < B_i < B_{max}$, the i-th constraints in (4.3) and (4.4) are satisfied with strict inequality. This implies from the slackness conditions in (4.7) and (4.8) that $\lambda_i = 0$ and $\mu_i = 0$. From (4.11), we can conclude that the water level does not change from TS i to TS $i+1$, i.e., $Y_i + \bar{C}_i = Y_{i+1} + \bar{C}_{i+1}$, if the RB is neither empty nor full at TS i. □

Lemma 4.2. *In the optimal EM policy, given $Y_i^* > 0 \ \forall i$, if the RB is never full from TS i to TS N, i.e., $B_j < B_{max}$ for $j = i, i+1, \ldots, N$, then the optimum water levels from TS i to TS N, i.e., $Y_j^* + \bar{C}_j$, for $j = i, i+1, \ldots, N$, must satisfy $Y_j^* + \bar{C}_j \geq \bar{E}$. If the RB is neither empty nor full from TS i to TS N, i.e., $0 < B_j < B_{max}$, for $j = i, i+1, \ldots, N$, then the optimum water levels from TS i to TS N should be equal to $\bar{E}$, i.e., $Y_j^* + \bar{C}_j = \bar{E}$, for $j = i, i+1, \ldots, N$.*

Proof. If the RB is never full from TS i to TS N, i.e., $B_j < B_{max}$ for $j = i, i+1, \ldots, N$, the constraints in (4.4) are satisfied with strict inequality. It follows from the slackness conditions

in (4.8) that $\mu_j = 0$, for $j = i, i+1, \ldots, N$. From (4.11), this implies that $Y_j^* + \bar{C}_j \geq \bar{E}$, and we can conclude that, if the RB is never full from TS i to TS N, the optimum water levels from TS i to TS N should satisfy $Y_j^* + \bar{C}_j \geq \bar{E}$, for $j = i, i+1, \ldots, N$. If the RB is neither empty nor full from TS i to TS N, i.e., $0 < B_j < B_{max}$, for $j = i, i+1, \ldots, N$, the constraints in (4.3) and (4.4) are satisfied with strict inequality. It follows from the slackness conditions in (4.7) and (4.8) that $\lambda_j = 0$ and $\mu_j = 0$, for $j = i, i+1, \ldots, N$. From (4.11), this implies that $Y_j^* + \bar{C}_j = \bar{E}$, and we can conclude that, if the RB is neither empty nor full from TS i to TS N, the optimum water levels from TS i to TS N should be equal to $\bar{E}$, i.e., $Y_j^* + \bar{C}_j = \bar{E}$, for $j = i, i+1, \ldots, N$. □

4.3.1 Implications of Lemmas

Here we discuss the implications of Lemma 4.1 and Lemma 4.2 on the optimal solution. For clarity, we first consider the solution for the infinite RB case, and then discuss the finite RB solution. If B_{max} is infinite, the RB is never full and the constraints in (4.4) are never satisfied with equality, i.e., $\mu_i = 0$, $\forall i$. Then, it follows from Lemma 4.1 that the water level is monotonically decreasing from one TS to the next. This is because the water (energy) can only flow backwards in our model, i.e., the output load can be assigned only to previous TSs, rather than the future ones. Accordingly, whenever the constraint in (4.3) is not satisfied with equality at TS i, i.e., $\lambda_i = 0$, then some energy for future use is drawn in advance within current TS i; in other words, some future output load is allocated to the current TS. Hence if, in the optimal EM policy, some output load is transferred from future TSs to the current one, the water level remains the same from the current TS to the next. Conversely, when there is a water level decrease from the current TS to the next, that is, if $\lambda_i > 0$, no output load is allocated from future TSs to the current, i.e., the RB is empty at TS i, as argued in Lemma 4.1. Moreover, from Lemma 4.2, we can conclude that all optimal water levels, i.e., $Y_i^* + \bar{C}_i$, $\forall i$, must satisfy $Y_i^* + \bar{C}_i \geq \bar{E}$, $\forall i$, since the RB is never full.

If B_{max} is finite, the amount of energy drawn for future use within TS i is limited by the remaining RB capacity at TS i, i.e., $B_{max} - B_i$. When the energy transferred from future TSs to the current one is less than $B_{max} - B_i$, the constraints in (4.3) and (4.4) are satisfied with strict inequality, i.e., $\lambda_i = 0$ and $\mu_i = 0$, respectively, and the water level does not change from TS i to TS $i+1$, as argued in Lemma 4.1. Conversely, when there is a water level increase from TS i to TS $i+1$, that is, if $\lambda_i = 0$ and $\mu_i > 0$, the amount of energy allocated from future TSs to the current one is equal to $B_{max} - B_i$, which implies that the RB is full at TS i. Note that when the RB is full at current TS, this implies that no energy can be allocated from future TSs to the current and previous TSs anymore due to the RB capacity limitation. When there is a water level decrease from TS i to TS $i+1$, that is, if $\lambda_i > 0$ and $\mu_i = 0$, no energy is allocated

from future TSs to the current one, i.e., the RB is empty at TS i, as argued in Lemma 4.1. If the RB is never full from TS i to TS N, i.e., $B_j < B_{max}$ for $j = i, i+1, \ldots, N$, we can conclude from Lemma 4.2 that the optimum water levels from TS i to TS N, i.e., $Y_j^* + \bar{C}_j$, for $j = i, i+1, \ldots, N$, must satisfy $Y_j^* + \bar{C}_j \geq \bar{E}$, for $j = i, i+1, \ldots, N$.

4.3.2 Backward Water-Filling Algorithm

All the aforementioned implications of Lemma 4.1 and Lemma 4.2 suggest that, we can satisfy each input load by backward power allocation over the current and previous TSs, starting from the first non-zero input load to the last, under the RB capacity constraint. The RB capacity introduces an upper bound on the output load at each TS, and the water levels can be equalized to the extent the previous water levels and the RB constraints allow. Based on these observations, we next describe the backward water-filling algorithm through an example in Fig. 4.3. The height of the white rectangles correspond to the weighted cost levels, $\bar{C}_i$'s, while their widths correspond to the TS durations, τ_i's, for $i = 1, 2, 3$. We also fix a target consumption value $\bar{E}$ illustrated in Fig. 4.3. Fig. 4.3(a) depicts the input loads, X_i, as the height of the corresponding filled areas on top of the white rectangles. Thus, the initial water levels are given by $X_i + \bar{C}_i$, $\forall i$. Observe that the RB is initially empty at every TS. Observe also that the trade-off between privacy and energy cost can be adjusted through the parameter θ, which affects the value of the weighted cost levels. Accordingly, when $\theta \to 1$, the significance of user's energy cost diminishes, i.e., the weighted cost levels become smaller, and when $\theta \to 0$, the significance of user's energy cost increases, i.e., the weighted cost levels become larger. Considering the example in Fig. 4.3(a), in Fig. 4.3(b) and Fig. 4.3(c) we illustrate the optimal offline EM policy in the presence of an infinite and a finite capacity RB, respectively.

In the infinite RB case, the first power demand X_1 is satisfied from the grid within the first TS, as seen in the first plot of Fig. 4.3(b). For the input load X_2, the algorithm allocates the output load from the second TS to the first by using the water-filling in reverse direction. Since the electricity price is relatively more expensive in the second TS, part of X_2 is drawn in advance within the first TS, and stored in the RB as seen in the second plot in Fig. 4.3(b). The rest of X_2 is drawn from the grid within the second TS. Hence, X_2 is fulfilled from both the RB and the grid. Observe that the RB is not empty at the end of first TS; and hence, the water level does not change from the first TS to the second as argued in Lemma 4.1. For the input demand X_3, the algorithm allocates the output load from the third TS to the second and first TSs as seen in the third plot in Fig. 4.3(b). This implies that part of X_3 is drawn in advance within the first and second TSs and stored in the RB. Hence, X_3 is satisfied from both the RB and the grid. Observe that the RB is not empty at the end of first and second TSs; and hence, all water levels are equalized as argued in Lemma 4.1. On the other hand, the RB is empty at the end

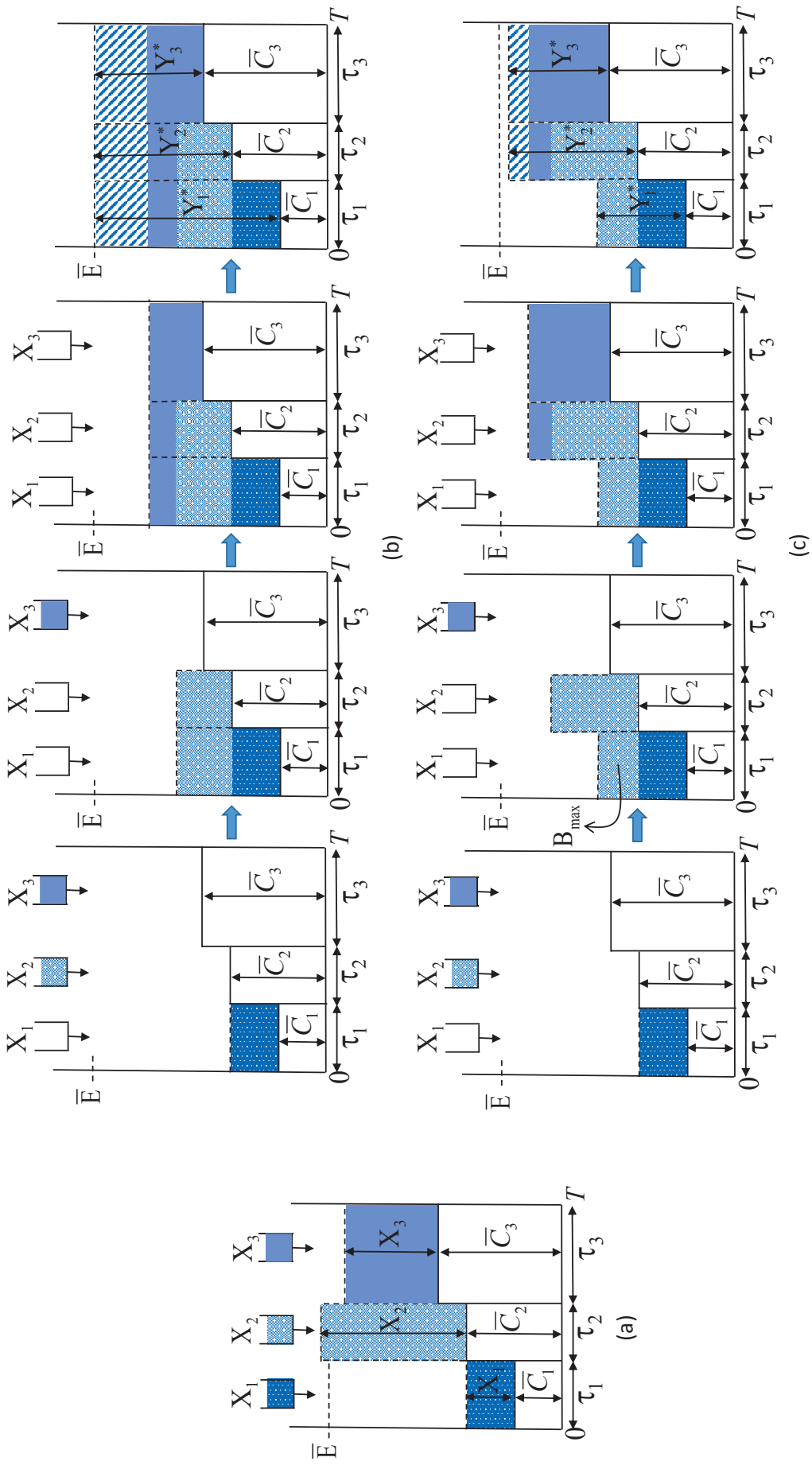


Figure 4.3: Depiction of the input loads and initial water levels (a), and the optimal backward water-filling algorithm in the presence of (b) infinite, and (c) finite capacity RBs, respectively.

of the third TS. If the current water levels satisfy the conditions argued in Lemma 4.2 in this step, the algorithm leads to the optimal solution. As depicted in the third plot in Fig. 4.3(b), all water levels are smaller than the target value $\bar{E}$; and hence, Lemma 4.2 is not satisfied. To eliminate this contradiction, the algorithm needs to allocate further grid energy to all TSs. Accordingly, all water levels are raised up to $\bar{E}$ as seen in the fourth plot in Fig. 4.3(b), leading to the optimal output loads Y_i^*, as the height of the filled areas above $\bar{C}_i$, $\forall i$. Observe that the optimal output load in the first TS, Y_1^*, depends on the input loads and the weighted cost levels in the following TSs. For N TSs, the optimal output load values can be obtained by $N+1$ iterations of the backward water-filling algorithm.

Fig. 4.3(c) depicts the optimal backward water-filling solution and the optimal output load values, Y_i^*, in the presence of a finite capacity RB. The first power demand X_1 is satisfied from the grid within the first TS, and the RB is empty at the end of the first TS, as seen in the first plot of Fig. 4.3(c). In contrast to the infinite capacity RB case, the portion of the input load, X_2, drawn in advance within the first TS is limited by the RB capacity B_{max}, as seen in the second plot in Fig. 4.3(c). In other words, the energy allocated from the second TS to the first is equal to B_{max}, which leads to the fact that the RB gets full at the end of first TS. This explains the water level increase from the first TS to the second as argued in Lemma 4.1. For the input demand X_3, the algorithm allocates the output load from the third TS only to the second TS since the RB is full at the end of the first TS as seen in the third plot in Fig. 4.3(c). This implies that the part of X_3 is drawn in advance within the second TS and stored in the RB. Hence, X_3 is satisfied from both the RB and the grid. Observe that the RB is neither empty nor full at the end of the second TS; and hence, the water level does not change from the second TS to the third as argued in Lemma 4.1. Similarly to the infinite RB capacity case, if the current water levels satisfy the conditions argued in Lemma 4.2 in this step, the algorithm leads to the optimal solution. As seen in the third plot in Fig. 4.3(c), all water levels are smaller than $\bar{E}$. Observe that the RB is full at the end of the first TS; and hence, the water level at the first TS can not be raised further due to the RB capacity limitation. On the other hand, the water levels at the second and third TSs do not satisfy the optimality conditions argued in Lemma 4.2 as the RB is neither empty nor full at the second TS, and empty at the third TS. Therefore, the algorithm needs to allocate further grid energy to the second and third TSs. As depicted in the fourth plot of Fig. 4.3(c), the algorithm allocates the same amount of energy to the second and third TSs, and raises water levels, leading to the optimal output loads, Y_i^*, $\forall i$. Observe that the water levels at the second and third TSs are raised in accordance with Lemma 4.1 satisfying the RB capacity constraint. Accordingly, the RB gets neither empty nor full at the end of the second TS; and hence, the water level does not change from the second TS to the third. The water levels at the second and third TSs do not reach $\bar{E}$, since the RB gets full at the end of the

third TS.

4.4 Online Energy Management (EM) Policies

In this section, we consider causal (online) knowledge of the input load at the EMU. As in the previous section, we consider non-causal knowledge of the electricity prices at the EMU[2]. First we provide the optimal online EM policy by solving the associated DP problem [120]. As DP algorithms quickly become computationally intractable with the increasing size of the state space of the problem, we also propose an efficient heuristic online policy that iteratively uses the offline backward water-filling algorithm developed in the previous section. For simplicity in this case, we assume unit TS durations, i.e., $\tau_i = 1$, $\forall i$. Similarly to the offline setting, we assume that the target value $\bar{E}$ is a constant parameter and is known by the online EM policies in advance.

4.4.1 Optimal Online Policy

The state of the system at the beginning of TS i is determined by the energy demand, $X_i \in \mathcal{X}$, and the battery state, $B_{i-1} \in \mathcal{B}$. The sets $\mathcal{X}$ and $\mathcal{B}$ are finite discrete sets generated by discretizing the feasible state spaces of the energy demand and battery state with particular energy quantizers, which are detailed in Section 4.6. We assume that the discrete energy demands follow a stationary first-order Markov relation, with transition probabilities q_{mn} between energy demand states x_m and x_n, i.e., $q_{mn} = \Pr\{X_{i+1} = x_n | X_i = x_m\}$. The online EM policy at TS i, i.e., $\pi_i(X_i, B_{i-1})$, maps each state to an output load, Y_i, that is selected from the finite discrete set $\mathcal{Y}_i$, i.e., $\pi_i : \mathcal{X} \times \mathcal{B} \rightarrow \mathcal{Y}_i$. The battery state at the end of TS i, B_i, is given by:

$$B_i = B_{i-1} + Y_i - X_i. \tag{4.13}$$

Following (4.13), $\mathcal{Y}_i$ can be defined as the set of feasible decisions under the energy demand, X_i, and the battery state, B_{i-1}, at the beginning of TS i:

$$\mathcal{Y}_i = \{Y_i \in \mathbb{R}^+ | Y_i = B_i - B_{i-1} + X_i, B_i \in \mathcal{B}\}. \tag{4.14}$$

[2]Since the prices do not change in real-time in the current SG structure, they can be reported to the consumer in advance.

The EMU is not allowed to waste any energy by limiting the battery state B_i to be lower than B_{max}. Following the objective function in (4.5), we can write the cost function for decision Y_i as follows:

$$g_i(Y_i) \triangleq \left[\theta \cdot \left(Y_i - \bar{E}\right)^2 + (1-\theta) \cdot Y_i \cdot C_i\right]. \tag{4.15}$$

We aim at minimizing the average cost over N TSs. The optimal online policy is a collection of decision functions, i.e., $\pi^* = \{\pi_1^*, \pi_2^*, \ldots, \pi_N^*\}$, which leads to the optimal output load values $Y_i^* = \pi_i^*(X_i, B_{i-1})$, and is found as the solution to the following optimization problem:

$$\begin{aligned}
&\underset{\pi_i}{\text{minimize}} \ \sum_{i=1}^{N} \mathrm{E}\Big[g_i(\pi_i(X_i, B_{i-1}))\Big] \\
&\text{subject to } \pi_i(X_i, B_{i-1}) \geq 0, && i = 1, \ldots, N \\
&\qquad B_{i-1} + \pi_i(X_i, B_{i-1}) - X_i \geq 0, && i = 1, \ldots, N, \\
&\qquad B_{i-1} + \pi_i(X_i, B_{i-1}) - X_i \leq B_{max}, && i = 1, \ldots, N,
\end{aligned} \tag{4.16}$$

where the expectation is taken with respect to the statistics of the input load. The optimal online policy, $\pi_i^*(X_i, B_{i-1})$, can be obtained through DP by proceeding backwards from the N-th TS to the first as follows:

$$\begin{aligned}
J_N^*(X_N, B_{N-1}) &\triangleq \underset{Y_N \in \pi_N(X_N, B_{N-1})}{\text{minimize}} g_N(Y_N), \\
J_i^*(X_i, B_{i-1}) &\triangleq \underset{Y_i \in \pi_i(X_i, B_{i-1})}{\text{minimize}} \mathrm{E}\Big[g_i(Y_i) + J_{i+1}^*(X_{i+1}, B_i)\Big], \\
&= \underset{Y_i}{\text{minimize}} \Big\{g_i(Y_i) + \sum_n q_{mn} J_{i+1}^*(x_n, B_{i-1} + Y_i - x_m)\Big\}, \\
&\qquad\qquad i = N-1, \ldots, 1,
\end{aligned} \tag{4.17}$$

where J_i^* denotes the optimal cost function at TS i that assigns to the energy demand, X_i, and the battery state, B_{i-1}, the optimal cost $J_i^*(X_i, B_{i-1})$. We recursively solve (4.17) and generate the optimal policy $\pi_i^*(X_i, B_{i-1})$, $\forall i$. The EMU records this function as a look-up table. Whenever the EMU receives an energy demand X_i, it checks the battery state B_{i-1}, and uses this look-up table to decide the optimal output load Y_i^* to be withdrawn from the grid.

Algorithm 4.1 Heuristic Online Policy

$B_0 \leftarrow 0$ ▷ Initially battery is empty

for i = 1 to N **do** ▷ TS i

1. Subproblem Construction:

Set the power demands for two TSs

$\hat{X}_1 \leftarrow [X_i - B_{i-1}]^+$, $\hat{X}_2 \leftarrow 3\bar{E}$

Set the battery energies for two TSs

$\hat{B}_1 \leftarrow [B_{i-1} - X_i]^+$, $\hat{B}_2 \leftarrow \hat{B}_1$

Set the electricity prices for two TSs

$\hat{C}_1 \leftarrow C_i$, $\hat{C}_2 \leftarrow \frac{1}{N}\sum_{i=1}^{N} C_i$

2. Subproblem Solution:

Solve the constructed subproblem by using the backward water-filling algorithm.

Feed the optimal output load, $\hat{Y}_1^*$, into the real timeline.

3. Output Load Decision:

$Y_i \leftarrow \hat{Y}_1^*$ ▷ Set the output load at TS i

$B_i \leftarrow B_{i-1} + (Y_i - X_i)$ ▷ Update the battery energy

end for

4.4.2 Heuristic Online Policy

Due to the high computational complexity of DP solutions, here we propose a low complexity heuristic online algorithm described in Algorithm 4.1. At each TS i, this algorithm creates a two-TS subproblem. Accordingly, each subproblem consists of the power demands, the electricity prices and the battery states for two TSs, which are denoted as $(\hat{X}_1, \hat{X}_2)$, $(\hat{C}_1, \hat{C}_2)$ and $(\hat{B}_1, \hat{B}_2)$, respectively. At each subproblem, the first TS is representative for the past and present information, while the second TS is representative for future information. In accordance with this, the parameters for the first TS of the subproblem, i.e., $\hat{X}_1$, $\hat{C}_1$, $\hat{B}_1$, are set based on the current information available at the EMU, such as, the current power demand, X_i, the current electricity price, C_i, and the battery state, B_{i-1}. The algorithm sets $\hat{X}_1$ as the part of the current power demand, X_i, which can not be satisfied from the available energy in the battery, $[X_i - B_{i-1}]^+$, $\hat{B}_1$ as the remaining energy in the battery after satisfying part of the current power demand, $[B_{i-1} - X_i]^+$, and $\hat{C}_1$ as the current electricity price, C_i. The parameters for the second TS of the subproblem, i.e., $\hat{X}_2$, $\hat{C}_2$, $\hat{B}_2$, are set as follows. The algorithm sets $\hat{X}_2$ as three times the target power demand[3] $\bar{E}$, $\hat{C}_2$ as the mean of the electricity prices,

[3]We set $\hat{X}_2$ more than the target power demand $\bar{E}$ in order to consider a future peak demand in the subproblem. This allows the algorithm to charge the RB further, so that any possible peak demand that can occur in future TSs can be tackled.

and $\hat{B}_2$ as $\hat{B}_1$. At each step, the algorithm optimally solves the constructed subproblem using the backward water-filling algorithm developed in Section 4.3.2. The output loads arising from the optimal solution for the first and second TSs are denoted by $\hat{Y}_1^*$ and $\hat{Y}_2^*$, respectively. The algorithm is only interested in the optimal solution for the first TS, i.e., $\hat{Y}_1^*$. Therefore, the algorithm sets the output load decision Y_i at TS i as $\hat{Y}_1^*$. Finally, it updates the battery state, B_i, by using B_{i-1}, X_i and Y_i. Note that since the algorithm considers the available battery energy at the construction of each subproblem, the output load decisions will always satisfy the RB capacity constraint. Numerical comparisons of the optimal offline and online policies as well as the proposed heuristic online policy will be provided in Section 4.6.

4.5 Information Leakage Rate

In the previous sections, we have considered the load variance, $\mathcal{V}$, in (4.1) as the privacy measure. An information theoretic privacy measure is the information leakage rate [48], which is defined as the average mutual information between the input and output load sequences:

$$I_p \triangleq \frac{1}{N} I(X^N; Y^N). \tag{4.18}$$

Although the load variance can be considered as a privacy measure, the information leakage rate can be argued to be more accurate privacy measure as it takes into account the statistical behaviour of the input load. Note that the information leakage rate measures the reduction in the UP's uncertainty (entropy) about user's energy consumption, X^N, after receiving meter readings, Y^N, as we have $I_p = \frac{1}{N}\left[H(X^N) - H(X^N|Y^N)\right]$. As an information theoretic privacy measure, the information leakage rate provides privacy guarantees regardless of the computational power of the attacker. However, the optimal decision policy in terms of the information leakage rate is significantly harder to characterize [108]. In this section, we provide a computational expression for the information leakage rate. In the next section, we will numerically evaluate and compare the load variance and the information leakage rate privacy measures, and demonstrate that the two follow similar trends.

As a first step towards computing the information leakage rate, we quantize the input and output load vectors. Let $\tilde{X}^N = (\tilde{X}_1, \tilde{X}_2, \dots, \tilde{X}_N)$ and $\tilde{Y}^N = (\tilde{Y}_1, \tilde{Y}_2, \dots, \tilde{Y}_N)$ denote the quantized versions of X^N and Y^N, respectively. The samples of $\tilde{X}^N$ and $\tilde{Y}^N$ take values from finite discrete sets $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{Y}}$, respectively. For simplicity, we assume that the samples in $\tilde{X}^N$ and the joint samples in $(\tilde{X}^N, \tilde{Y}^N)$ follow stationary first-order Markov relations, with which we can write the distribution of $\tilde{X}^N$ and the joint distribution of $(\tilde{X}^N, \tilde{Y}^N)$ as follows:

$$p(\tilde{X}^N) = p(\tilde{X}_1)\prod_{i=2}^{N} p(\tilde{X}_i|\tilde{X}_{i-1}), \tag{4.19a}$$

$$p(\tilde{X}^N, \tilde{Y}^N) = p(\tilde{X}_1, \tilde{Y}_1)\prod_{i=2}^{N} p(\tilde{X}_i, \tilde{Y}_i|\tilde{X}_{i-1}, \tilde{Y}_{i-1}). \tag{4.19b}$$

Note that the condition (4.19b) holds when (4.19a) holds, and the output load at time i, Y_i, depends only on the current input load, X_i, and the previous input and output loads, (X_{i-1}, Y_{i-1}). Under these two assumptions, we derive an upper bound on the information leakage rate, I_p, as follows:

$$\begin{aligned}
I_p &= \frac{1}{N} I(\tilde{X}^N; \tilde{Y}^N), \\
&= \frac{1}{N}\Big(H(\tilde{X}^N) + H(\tilde{Y}^N) - H(\tilde{X}^N, \tilde{Y}^N) \Big), \\
&\overset{\text{(a)}}{=} \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}^{i-1}) + H(\tilde{Y}_i|\tilde{Y}^{i-1}) - H(\tilde{X}_i, \tilde{Y}_i|\tilde{X}^{i-1}, \tilde{Y}^{i-1}) \Big), \\
&\overset{\text{(b)}}{\leq} \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) + H(\tilde{Y}_i|\tilde{Y}_{i-1}) - H(\tilde{X}_i, \tilde{Y}_i|\tilde{X}_{i-1}, \tilde{Y}_{i-1}) \Big), \\
&\overset{\text{(c)}}{=} \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) + H(\tilde{Y}_i|\tilde{Y}_{i-1}) - \Big(H(\tilde{X}_i|\tilde{X}_{i-1}, \tilde{Y}_i, \tilde{Y}_{i-1}) + H(\tilde{Y}_i|\tilde{X}_{i-1}, \tilde{Y}_{i-1}) \Big) \Big), \\
&\overset{\text{(d)}}{=} \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) + H(\tilde{Y}_i|\tilde{Y}_{i-1}) \\
&\qquad - \Big(H(\tilde{X}_i, \tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) + H(\tilde{Y}_i|\tilde{X}_{i-1}, \tilde{Y}_{i-1}) \Big) \Big) \\
&= \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) + H(\tilde{Y}_i|\tilde{Y}_{i-1}) - H(\tilde{X}_i, \tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) \\
&\qquad - \Big(H(\tilde{Y}_i|\tilde{X}_{i-1}, \tilde{Y}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) \Big) \Big), \\
&\overset{\text{(e)}}{=} \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) + H(\tilde{Y}_i|\tilde{Y}_{i-1}) - H(\tilde{X}_i, \tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) \\
&\qquad - \Big(H(\tilde{Y}_i, \tilde{X}_{i-1}|\tilde{Y}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_{i-1}) - \Big(H(\tilde{Y}_i, \tilde{X}_{i-1}|\tilde{Y}_{i-1}) - H(\tilde{Y}_i|\tilde{Y}_{i-1}) \Big) \Big) \Big) \\
&= \frac{1}{N}\sum_{i=1}^{N} \Big(H(\tilde{X}_i|\tilde{X}_{i-1}) - H(\tilde{X}_i, \tilde{X}_{i-1}|\tilde{Y}_i, \tilde{Y}_{i-1}) + H(\tilde{X}_{i-1}|\tilde{Y}_{i-1}) \Big),
\end{aligned}$$

$$
\begin{aligned}
&\overset{\text{(f)}}{=} \frac{1}{N}\sum_{i=1}^{N}\Big(H(\tilde{X}_i,\tilde{X}_{i-1}) - H(\tilde{X}_{i-1}) - H(\tilde{X}_i,\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1}) + H(\tilde{X}_{i-1}|\tilde{Y}_{i-1})\Big)\\
&= \frac{1}{N}\sum_{i=1}^{N}\Big(\Big(H(\tilde{X}_i,\tilde{X}_{i-1}) - H(\tilde{X}_i,\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1})\Big) - \Big(H(\tilde{X}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_{i-1})\Big)\Big),\\
&\overset{\text{(g)}}{=} \frac{1}{N}\Bigg(\sum_{i=2}^{N}\Big(H(\tilde{X}_i,\tilde{X}_{i-1}) - H(\tilde{X}_i,\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1})\Big) - \sum_{i=3}^{N}\Big(H(\tilde{X}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_{i-1})\Big)\Bigg),\\
&\overset{\text{(h)}}{=} \frac{1}{N}\Bigg(\sum_{i=2}^{N} I(\tilde{X}_i,\tilde{X}_{i-1};\tilde{Y}_i,\tilde{Y}_{i-1}) - \sum_{i=3}^{N} I(\tilde{X}_{i-1};\tilde{Y}_{i-1})\Bigg),
\end{aligned}
$$

where (a) follows from the chain rule of entropy; (b) follows from the first-order Markov assumption for $\tilde{X}_i$ and $(\tilde{X}_i,\tilde{Y}_i)$ in (4.19) and the fact that conditioning reduces entropy; (c) follows from the chain rule applied to $H(\tilde{X}_i,\tilde{Y}_i|\tilde{X}_{i-1},\tilde{Y}_{i-1})$ in (b); (d) follows from replacing the term $H(\tilde{X}_i|\tilde{X}_{i-1},\tilde{Y}_i,\tilde{Y}_{i-1})$ in (c) with its equal expression, i.e., $H(\tilde{X}_i|\tilde{X}_{i-1},\tilde{Y}_i,\tilde{Y}_{i-1}) = H(\tilde{X}_i,\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1})$, where this equality is arising from the chain rule applied to $H(\tilde{X}_i,\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1})$; (e) follows from first replacing $H(\tilde{Y}_i|\tilde{X}_{i-1},\tilde{Y}_{i-1})$ and $H(\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1})$ in (d) with their equal expressions, i.e., $H(\tilde{Y}_i|\tilde{X}_{i-1},\tilde{Y}_{i-1}) = H(\tilde{Y}_i,\tilde{X}_{i-1}|\tilde{Y}_{i-1}) - H(\tilde{X}_{i-1}|\tilde{Y}_{i-1})$ and $H(\tilde{X}_{i-1}|\tilde{Y}_i,\tilde{Y}_{i-1}) = H(\tilde{Y}_i,\tilde{X}_{i-1}|\tilde{Y}_{i-1}) - H(\tilde{Y}_i|\tilde{Y}_{i-1})$, where these equalities are arising from the chain rule applied to $H(\tilde{Y}_i,\tilde{X}_{i-1}|\tilde{Y}_{i-1})$ and $H(\tilde{Y}_i,\tilde{X}_{i-1}|\tilde{Y}_{i-1})$, respectively, and then doing the necessary cancellations; (f) follows from replacing $H(\tilde{X}_i|\tilde{X}_{i-1})$ in (e) with its equal expression, i.e., $H(\tilde{X}_i|\tilde{X}_{i-1}) = H(\tilde{X}_i,\tilde{X}_{i-1}) - H(\tilde{X}_{i-1})$, where this equality is arising from the chain rule applied to $H(\tilde{X}_i,\tilde{X}_{i-1})$; (g) is obtained by reorganizing (f), and (h) follows from the definition of the mutual information.

We note that (b) holds with equality if we assume that the output load sequence $\tilde{Y}^N$ is also a stationary first-order Markov process. This assumption has been made in [91] for the computation of the information leakage rate; however, adding this extra Markov assumption together with the initial ones may not lead to any realistic model or non-trivial EM strategy. Accordingly, the information leakage rate upper bound obtained above will be evaluated numerically as a measure of the information theoretical privacy leakage for the EM policies derived in Section 4.3 and Section 4.4.

To numerically evaluate the mutual information expressions for given input and output load sequences, we can explicitly write the information leakage rate I_p, as follows:

$$I_p = \frac{1}{N}\Bigg(\sum_{i=2}^{N} \sum_{\substack{x_{i-1}\in\tilde{\mathcal{X}} \\ \tilde{y}_{i-1}\in\tilde{\mathcal{Y}}}} \sum_{\substack{x_i\in\tilde{\mathcal{X}} \\ \tilde{y}_i\in\tilde{\mathcal{Y}}}} p(\tilde{x}_i,\tilde{x}_{i-1},\tilde{y}_i,\tilde{y}_{i-1}) \log \frac{p(\tilde{x}_i,\tilde{x}_{i-1},\tilde{y}_i,\tilde{y}_{i-1})}{p(\tilde{x}_i,\tilde{x}_{i-1})p(\tilde{y}_i,\tilde{y}_{i-1})} - \sum_{i=3}^{N} \sum_{\substack{x_{i-1}\in\tilde{\mathcal{X}} \\ \tilde{y}_{i-1}\in\tilde{\mathcal{Y}}}} p(\tilde{x}_{i-1},\tilde{y}_{i-1}) \log \frac{p(\tilde{x}_{i-1},\tilde{y}_{i-1})}{p(\tilde{x}_{i-1})p(\tilde{y}_{i-1})} \Bigg), \tag{4.20}$$

We can compute I_p by estimating all the joint and marginal distibutions in (4.20). We use emprical distributions as the estimates for these distributions, i.e., we count the number of joint or single appearances over all realizations, and normalize them to obtain the corresponding probabilities.

Note that, when there is no RB in the system, i.e., $B_{max} = 0$, we have $\tilde{Y}_i = \tilde{X}_i$, $\forall i$, and $I_p = \frac{1}{N}H(\tilde{X}^N)$, i.e., the UP knows the input load perfectly. In this case, the information leakage rate I_p simplifies to:

$$\begin{aligned} I_p &= \frac{1}{N}H(\tilde{X}^N), \\ &\overset{\text{(a)}}{=} \frac{1}{N}\sum_{i=1}^{N} H(\tilde{X}_i|\tilde{X}_{i-1}), \\ &\overset{\text{(b)}}{=} \frac{1}{N}\sum_{i=1}^{N} \sum_{\tilde{x}_{i-1}\in\tilde{\mathcal{X}}} \sum_{\tilde{x}_i\in\tilde{\mathcal{X}}} -p(\tilde{x}_{i-1},\tilde{x}_i)\log p(\tilde{x}_i|\tilde{x}_{i-1}), \end{aligned} \tag{4.21}$$

where (a) follows from the chain rule of entropy and the first-order Markov assumption for $\tilde{X}_i$, and (b) follows from the definition of the conditional entropy.

4.6 Numerical Results and Observations

In this section, we provide further insights into the proposed offline and online EM policies through numerical simulations. We analyze the trade-off between the user's privacy and energy cost as well as the effect of the RB capacity on this trade-off. We use the real SM readings obtained from [121] with a time resolution on the order of three seconds. For our simulations we consider the readings from one household for a period of one month and convert the load profile to a time resolution of one-minute. Particularly, the simulations results illustrated in Fig. 4.8 and Fig. 4.9 are obtained by considering a whole-day power consumption data. To

be consistent with our power consumption model, we assume that the discrete-time instants in Fig. 4.2(a) correspond to the sampling times of the SM. We set the electricity price in our simulations based on the real pricing tariffs [122]: the off-peak price is 5 cent per kWh during $00{:}00$ to $12{:}00$, the on-peak price is 20 cent per kWh during $12{:}00$ to $20{:}00$, and the medium-peak price is 10 cent per kWh during $20{:}00$ to $00{:}00$. For the simulations, we consider the target value $\bar{E}$ as the average power demand of the user, i.e., $\bar{E} = \frac{1}{T}\sum_{i=1}^{N} \tau_i \cdot X_i$.[4]To discretize the state space for the online problem, we use a 4-bit non-uniform mu-law quantizer for the energy demand, and a 2-bit uniform quantizer for the battery state, respectively. For the characterization of the information leakage rate, we discretize the input and output load sequences resulting from the proposed policies by using a 5-bit non-uniform mu-law quantizer.

In Fig. 4.4, we illustrate the trade-offs between the user's privacy and energy cost resulting from the proposed offline and online EM policies with an RB capacity $B_{max} = 0.5$ kWh. The Pareto optimal trade-off curves between the load variance, $\mathcal{V}$, and the average energy cost, $\mathcal{C}$, in Fig. 4.4(a), and the trade-off curves between the information leakage rate, I_p, and the average energy cost, $\mathcal{C}$, in Fig. 4.4(b), are formed by varying θ values. For all the proposed policies, the average energy cost increases, while the load variance and the information leakage rate diminish as θ increases. According to the requirements of the system, the operating point can be chosen anywhere on the trade-off curve. We observe that the load variance and the information leakage rate behave similarly for all the policies. Based on this observation, we can argue that the load variance can be used as a meaningful privacy measure for SM systems. The corner points of the trade-off curves for the proposed policies in Fig. 4.4 are given in Table 4.1. Observe that the heuristic online policy performs close to the optimal online policy both at the maximum privacy and the minimum cost corner points, while the optimal offline policy outperforms both of them as expected.

Next, we investigate the effect of the battery capacity on the maximum privacy and minimum cost achieved by the proposed policies, respectively. Regarding the maximum privacy, we plot the load variance, $\mathcal{V}$, versus the RB capacity, B_{max}, in Fig. 4.5(a), and the information leakage rate versus B_{max} in Fig. 4.5(b), resulting from the proposed offline and online policies for $\theta = 1$. Observe that both the load variance and the information leakage rate diminish as RB capacity increases. Similar behaviours of the load variance and the information leakage rate with respect to the RB capacity further consolidates the argument that the load variance can be used as a proxy for the information leakage rate in SM systems. When there is no RB in the system, i.e., $B_{max} = 0$, the UP knows the input load sequence perfectly, and the information leakage rate reduces to the entropy rate of the input load sequence, which is found to be $I_p = 0.952$. Observe that the information leakage rate achieved by the optimal offline and

[4]The target value $\bar{E}$ is known by the offline and online policies in advance.

Table 4.1: CORNER POINTS OF THE TRADE-OFF CURVES in Fig. 4.4

	Heuristic Policy	Optimal Online Policy	Optimal Offline Policy
$\min \mathcal{V}$	0.157	0.139	0.085
$\min I_p$	0.612	0.481	0.19
$\mathcal{C}$	0.792	0.796	0.801
$\mathcal{V}$	0.204	0.178	0.103
I_p	0.758	0.536	0.249
$\min \mathcal{C}$	0.721	0.715	0.702

online policies drops very quickly with even a small RB capacity. While the information leakage rate achieved by the optimal offline policy saturates to its minimum value, the information leakage rates achieved by the optimal and heuristic online policies decrease smoothly as the RB capacity increases. Observe that the heuristic online policy performs close the optimal online policy for both privacy measures. The gain on the performances of the proposed policies can be achieved by virtue of the degree-of-freedom provided by the RB. When $B_{max} = 1.5$ (kWh), the information leakage rate of the heuristic online policy is found to be $I_p = 0.49$, and that of the optimal online and offline policies are found to be $I_p = 0.354$ and $I_p = 0.141$, respectively. These results show that a moderate RB capacity leads to a significant reduction in the information leakage rate. For RB capacities beyond 1.5 kWh, we do not expect a significant privacy gain. We also expect that the information leakage rate of the heuristic policy approaches to the optimal online policy when RB capacity becomes sufficiently large.

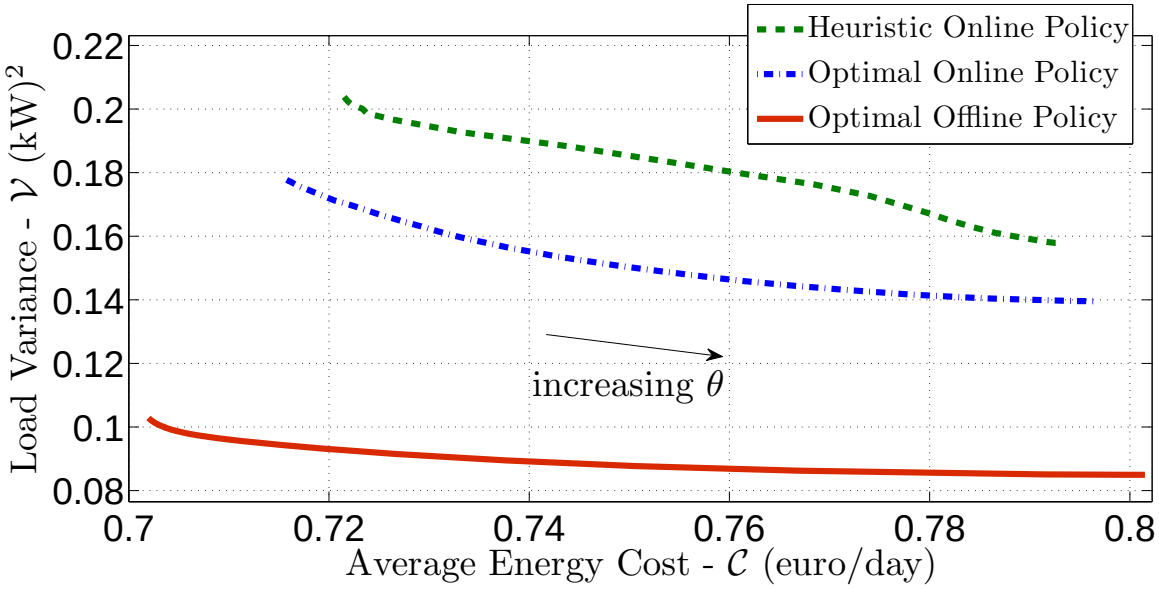
Fig. 4.6 illustrates the average energy cost, $\mathcal{C}$, versus the RB capacity, B_{max}, resulting from the proposed offline and online policies under $\theta = 0.001$, which corresponds to the scenario in which the consumer is more interested in minimizing the cost of energy rather than privacy. When there is no RB in the system, i.e., $B_{max} = 0$, the consumer has no degree-of-freedom to reduce the energy cost. The highest value for the average energy cost is found to be $\mathcal{C} = 0.778$ (euro/day). The average energy cost decreases with the increasing RB capacity. Observe that the heuristic online policy performs very close to the optimal online policy. When $B_{max} = 1.5$ (kWh), the average energy cost of the heuristic online policy is found to be $\mathcal{C} = 0.624$ (euro/day), and that of the optimal online and offline policies are found to be $\mathcal{C} = 0.61$ (euro/day) and $\mathcal{C} = 0.57$ (euro/day), respectively. We see that the user can reduce his/her energy consumption cost significantly with the proposed policies in the presence of a moderate capacity RB.

We compare the original load profile with the output load profiles resulting from the proposed offline and online EM policies with an RB of capacity, $B_{max} = 1.5$ kWh, and $\theta = 1$ and $\theta = 0.001$ values, in Fig. 4.7(a) and (b), respectively. When $\theta = 1$, the proposed policies intend to maximize the privacy of the user. That is, they intend to generate smooth output load profiles in order to mask the peaks in the original load profile. Observe in Fig. 4.7(a) that the optimal offline policy generates a smoother output load profile than the optimal and heuristic online policies as expected. Particularly, if we focus on the peak power of the original load profile between 20.00 and 22.00, we can see that the optimal offline policy masks most of the peak signal, while the optimal and heuristic online policies still have significant peaks in their output loads. On the other hand, they both perform well in masking the peak values at other times of the day. When $\theta = 0.001$, the proposed policies intend to minimize the energy cost of the user. As seen in Fig. 4.7(b), the proposed policies store extra energy in the RB during the off-peak price period, and satisfy the demand of the peak period from the RB in order to reduce the cost. Observe that, in the peak period between 12.00 and 20.00, the optimal offline policy draws nearly constant power from the grid, and satisfies the rest of the demand from the RB; on the other hand, the optimal and heuristic online policies satisfy the demand more from the RB between 12.00 and 16.00, and more from the grid between 16.00 and 20.00. We can envision that as the RB capacity increases, the optimal and heuristic online policies can store more energy in the battery to be used in the peak period, which would reduce the average energy cost.

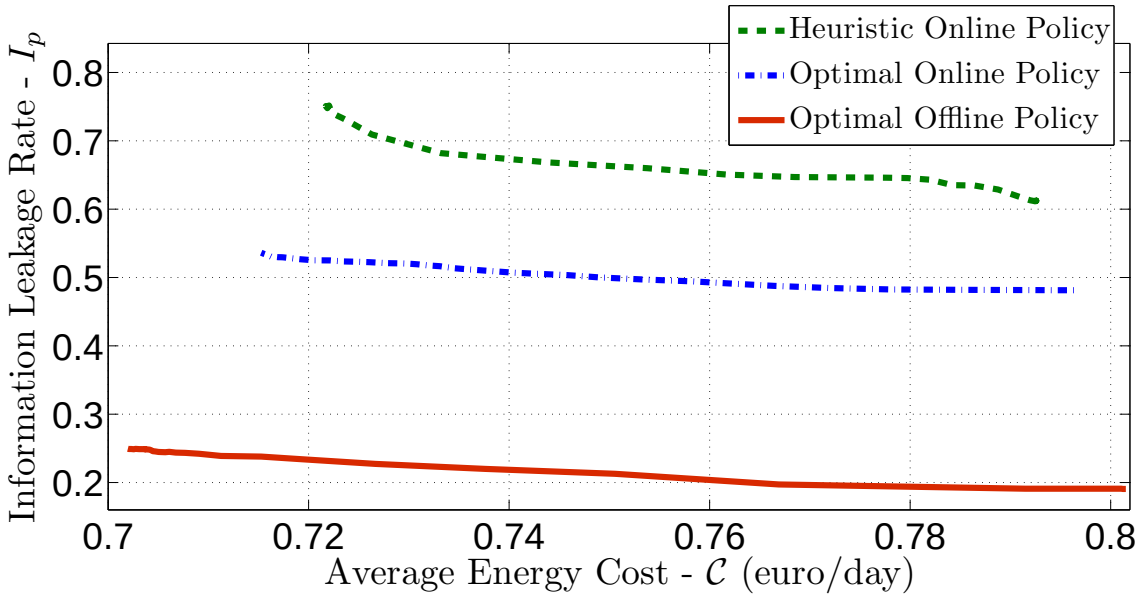
In Fig. 4.8, we characterize the trade-off between the user's privacy and energy cost resulting from the proposed offline policy for RB capacities $B = \{1, 1.5, 2\}$ kWhs, respectively, and investigate the effect of the RB capacity on this trade-off. The Pareto optimal trade-off curves between the load variance and the average energy cost are formed by varying θ values. For the proposed offline policy, the average energy cost increases, while the load variance diminishes as θ increases. When $\theta = 1$, the load variance achieves its minimum value; on the other hand, the average energy cost achieves its minimum value as θ becomes close to 0. According to the requirements of the system, the operating point can be chosen anywhere on the trade-off curve. Observe that the Pareto optimal trade-off curve moves towards the origin as the RB capacity increases. This implies that with increasing RB capacity, the load variance can be reduced further under a fixed average energy cost, and the average energy cost can be reduced further under a fixed load variance. Both gains can be achieved by virtue of the degree-of-freedom provided by the RB.

Finally, we investigate the impact of the SM resolution on the trade-off between the user's privacy and energy cost in Fig. 4.9. To that end, we modify the original load profile into new load profiles with lower resolutions. Accordingly, the new load profiles have time resolutions

varying on the order of 5, 10, 15 minutes, and 1 hour, respectively. We then characterize the Pareto optimal trade-off between the total load variance, $N\mathcal{V}$, and the average energy cost, $\mathcal{C}$, for the load profiles with given resolutions and the RB capacity $B = 1.5$ kWh in Fig. 4.9. We see that the Pareto optimal trade-off curve moves downwards as the SM resolution gets lower. This implies that with a decreasing resolution, the EM policy can provide higher energy consumption privacy under a fixed average energy cost. This is due to the fact that a load sampled at a lower-resolution is smoother, and has a smaller variance compared to the same load sampled at a higher-resolution.

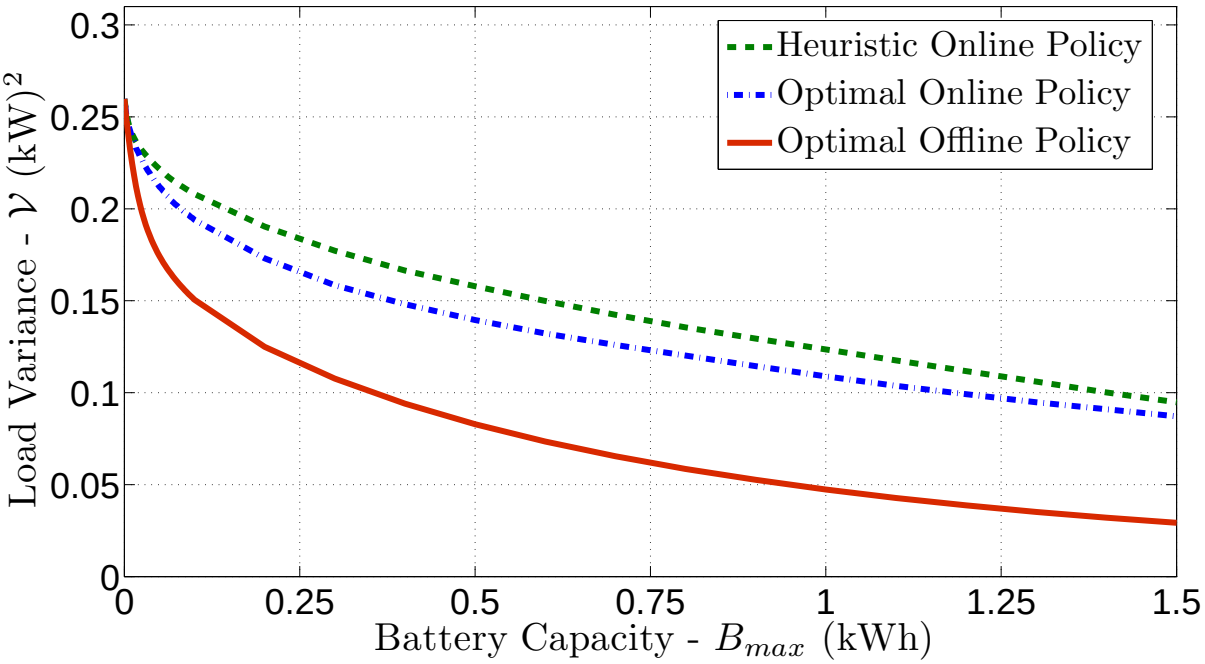


(a)

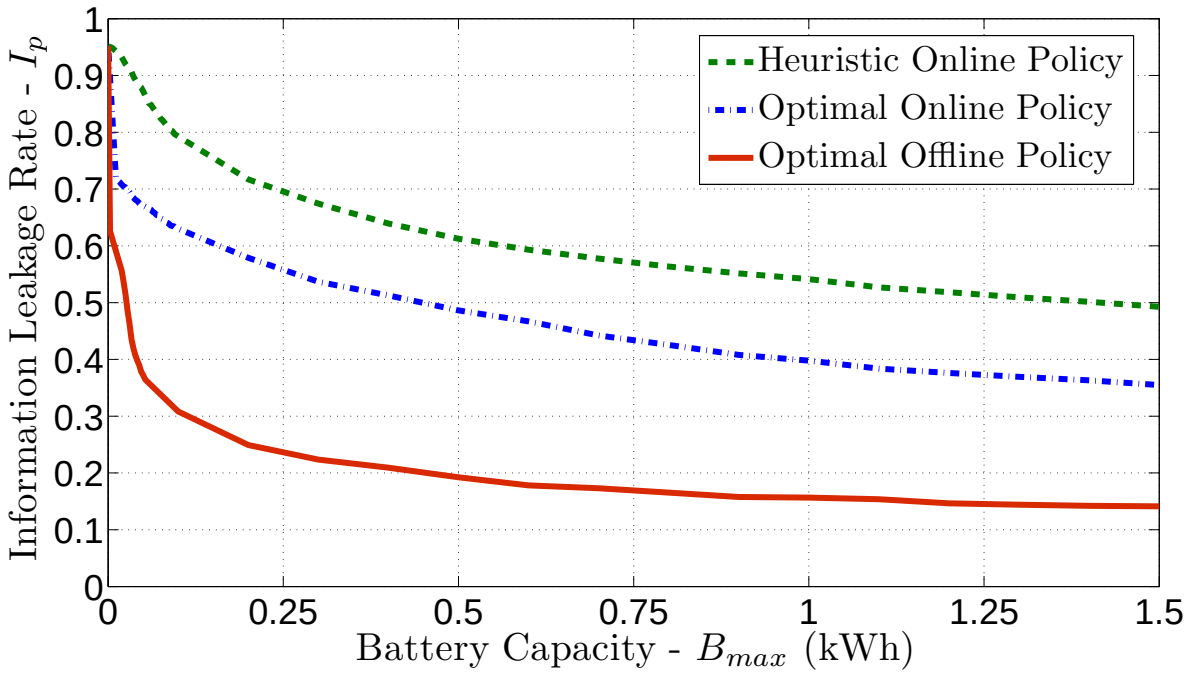


(b)

Figure 4.4: (a) The load variance, $\mathcal{V}$, versus the average energy cost, $\mathcal{C}$, and (b) the information leakage rate, I_p, versus the average energy cost, $\mathcal{C}$, resulting from the proposed offline and online EM policies under the RB capacity, $B_{max} = 0.5$ kWh.



(a)



(b)

Figure 4.5: (a) The load variance, $\mathcal{V}$, versus battery capacity, B_{max}, and (b) the information leakage rate, I_p, versus battery capacity, B_{max}, for the proposed offline and online EM policies under $\theta = 1$.

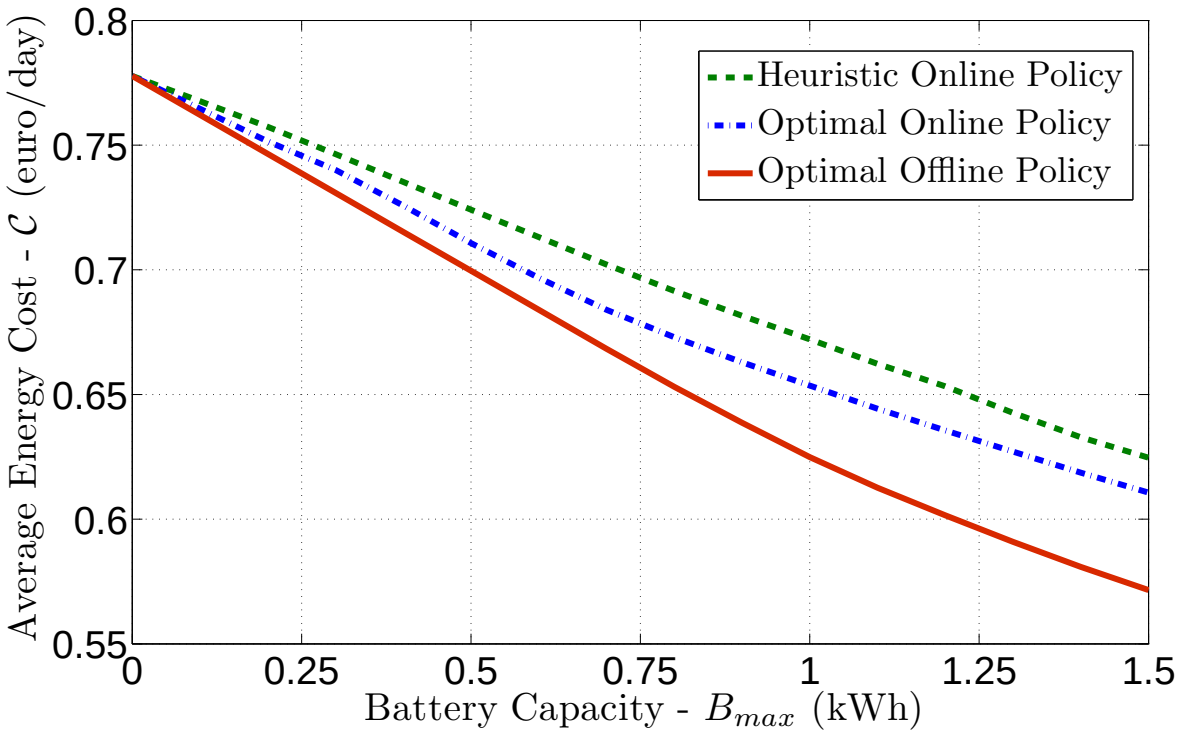


Figure 4.6: The average energy cost, $\mathcal{C}$, versus battery capacity, B_{max}, resulting from the proposed offline and online EM policies under $\theta = 0.001$.

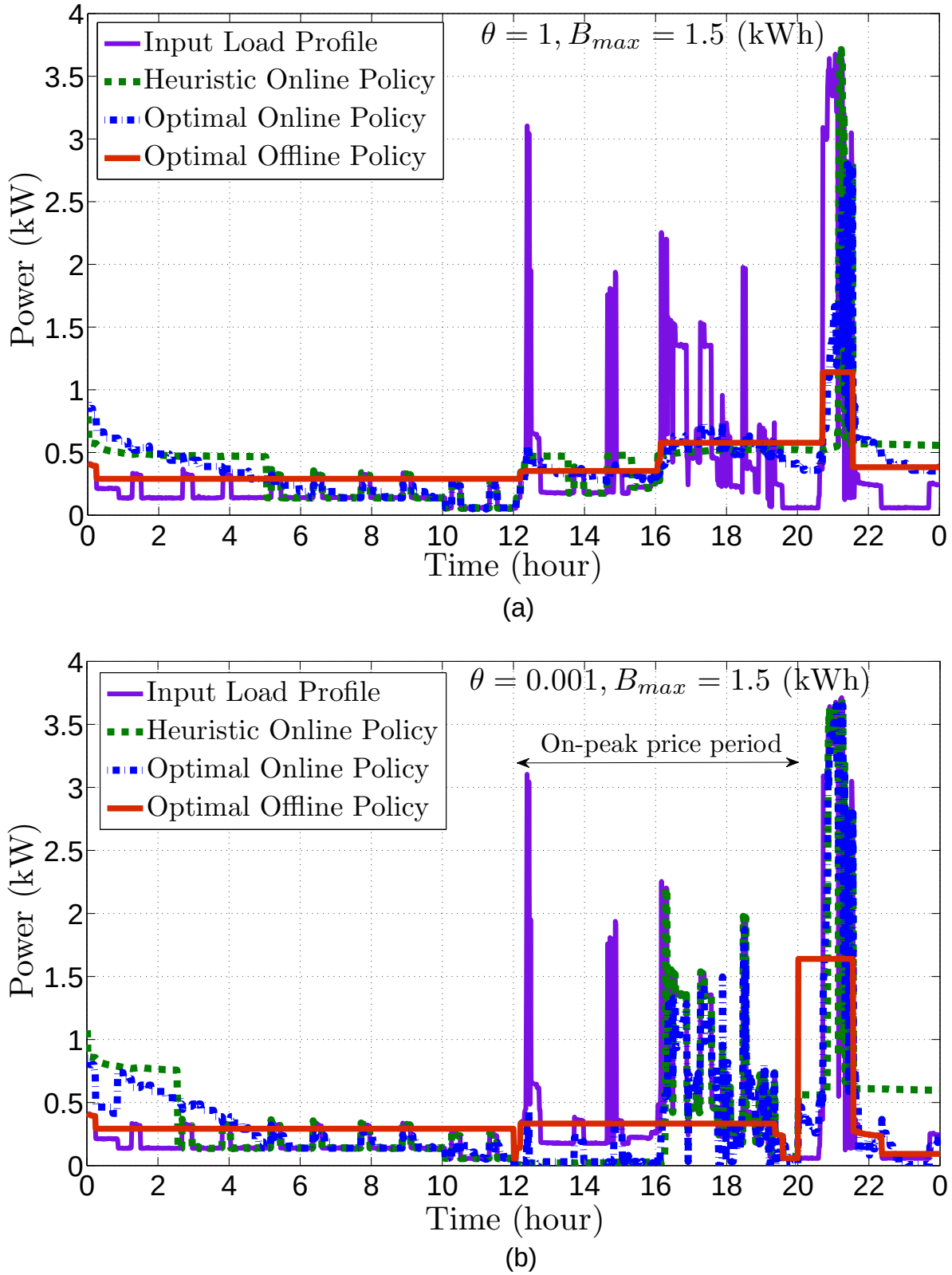


Figure 4.7: Comparison of the original input load profile with the output load profiles resulting from the proposed offline and online EM policies under the RB capacity, $B_{max} = 1.5$ kWh, and, (a) $\theta = 1$, (b) $\theta = 0.001$, respectively.

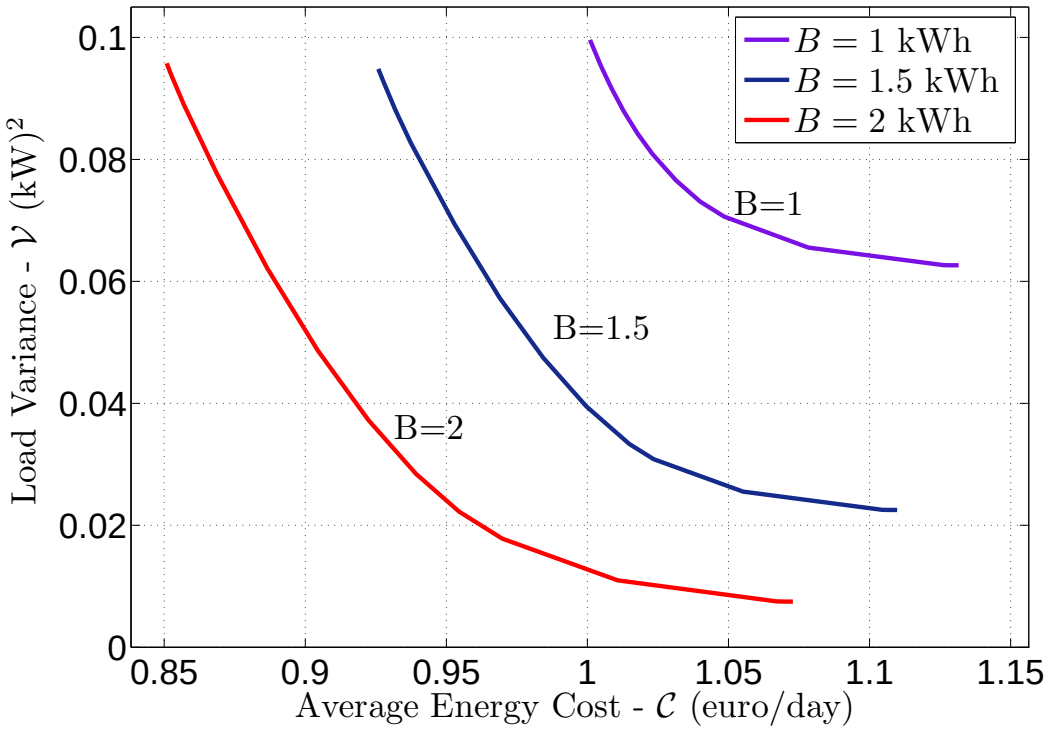


Figure 4.8: The load variance, $\mathcal{V}$, versus the average energy cost, $\mathcal{C}$, for the RB capacities, $B = 1$ kWh, $B = 1.5$ kWh and $B = 2$ kWh, respectively.

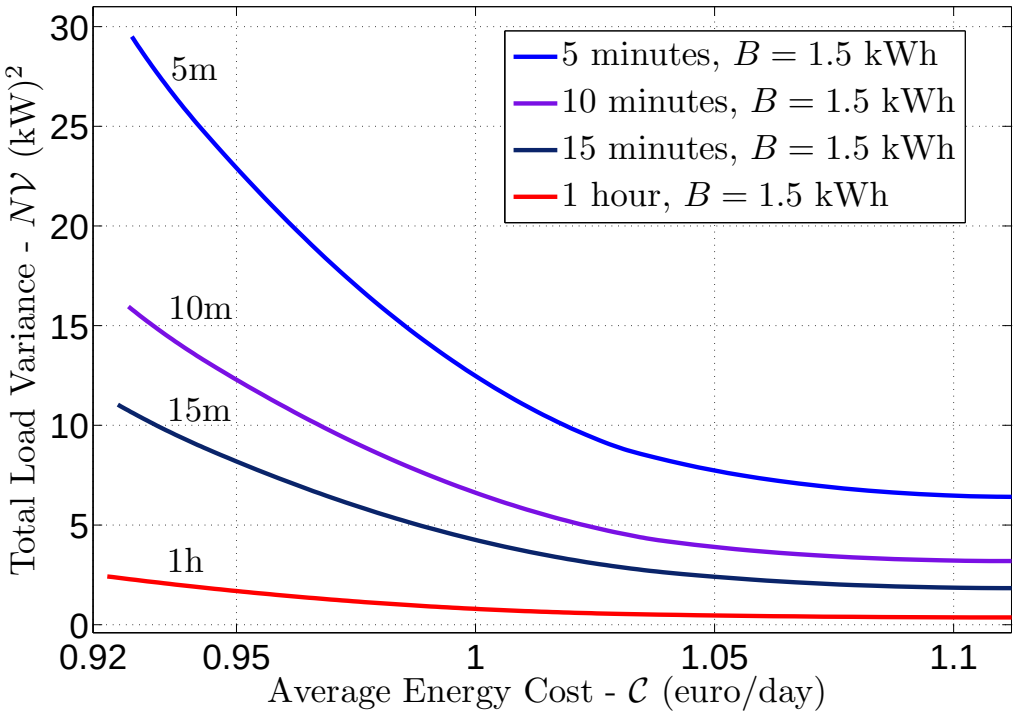


Figure 4.9: The total load variance, $N\mathcal{V}$, versus the average energy cost, $\mathcal{C}$, for the RB capacity, $B = 1.5$ kWh, and the load profiles with a time resolution varying on the order of 5, 10, 15 minutes, and 1 hour, respectively.

4.7 Conclusions

In this chapter, we have studied demand-side EM policies from a joint privacy-energy cost optimization perspective for an SM system with a finite-capacity energy storage unit. We have considered a discrete-time energy consumption model, in which both the power consumption of the consumer and the electricity prices vary over time. We have considered the variance of the output load around a predetermined constant target value as a measure of privacy for the consumer. First, assuming that the user's energy demand profile and the electricity prices are known non-causally, we have formulated the optimal privacy-cost trade-off as a convex optimization problem, and identified the properties of the optimal offline EM policy. Then, we have proposed a backward water-filling algorithm which efficiently computes the optimal offline EM policy. We have observed that the energy cost can be reduced by requesting more energy when the prices are lower, and the privacy is obtained by generating a smoother output load. Both gains can be achieved simultaneously by utilizing the available RB intelligently.

Next, assuming that the user's power consumption profile is known only causally, we have characterized the optimal online policy using DP. We have also proposed a low complexity heuristic online algorithm, and have shown through numerical simulations that, it performs close to the optimal online solution. In addition to the output load variance, we have also characterized the information leakage rate between the input and output load sequences. Extensive numerical simulations have been presented using real SM consumption data to illustrate the trade-offs between privacy and energy cost resulting from the proposed offline and online policies. Our results indicate that the privacy-cost trade-offs for the output load variance and the information leakage rate have very similar behaviours; and therefore, the output load variance can be used as a privacy measure for SM systems. These numerical results have shown that the proposed heuristic online algorithm performs very close to the optimal solution based on DP, which requires significantly higher computational complexity. We have also shown that most of the privacy gains can be obtained with a relatively small capacity RB.

Chapter 5

Linear Transmission of Composite Gaussian Measurements over a Fading Channel under Delay Constraints

5.1 Introduction

In Chapters 3 and 4, we have considered EM techniques for SM systems, which can provide privacy assurances to the SM users and retain the operational benefits SMs provide to the SG. In this chapter, we turn our focus to another key technology deployed in SGs, namely, WSNs. As it has been argued previously, near real-time monitoring of a physical phenomena is of great significance to many emerging SG functionalities, such as monitoring of voltage, current magnitudes, active/reactive power values in SGs [1]. To this end, wireless sensors are deployed throughout SG, and the sensor measurements are delivered to a CC over wireless links. For the robust, reliable and efficient management of the SG, near real-time and accurate reconstruction of the measurements at the CC becomes imperative. For example, in conventional state estimation for the electricity grid, measurements are collected once every two to four seconds and the state is updated once every few minutes [45], [46], [123], [124]. However, more frequent state measurements and estimations are required for modern SGs, which inevitably imposes strict delay constraints on the transmission of measurements. Thus, zero-delay LT, rather than advanced compression and channel coding techniques that span large codewords, is an attractive strategy for the transmission of sensor measurements in intelligent networks. This is because LT restricts the encoding and decoding functions to be zero-delay linear transformations, which in turn, allows to reduce both the delay and encoding complexity significantly; and accordingly to limit the cost and energy requirements of the sensors.

Accordingly, in this chapter, we aim at exploring LT strategies, with which sensors can accommodate low latency and low complexity transmission requirements, and in turn, can provide advanced control and monitoring capabilities to SGs; and hence, can facilitate real-time and accurate state reconstruction, and the efficient management of the SG. We consider a wireless sensor node that collects measurements from J Gaussian parameters. We discretize time into TSs, and assume that the CC asks for a measurement of a particular parameter from the sensor at each TS. The sensor takes one sample of the requested parameter at each TS, and transmits these samples to the CC over an AWGN fading channel under a given delay constraint. Note that, in contrast to multi-dimensional Gaussian source models studied in [95], [99], [125], where the sensor has the measurements of all the J Gaussian parameters at the beginning of a TS, we assume that only one measurement is taken from the requested parameter at each TS.

We assume that each measurement must be delivered within d TSs. Thereby, after each transmission, the CC estimates the measurement whose deadline is just about to expire. We assume that the channel gain from the sensor to the CC is i.i.d. over TSs. We consider two different scenarios regarding the CSI: In the first scenario, the CSI is assumed to be available to both the encoder and decoder, while in the second scenario, only the decoder has CSI. Our goal is to estimate all the requested measurements at the CC within their delay constraints with the minimum MSE distortion.

We focus explicitly on LT strategies. Assuming that the CSI is known by both the encoder and decoder, we first derive the optimal LT strategy under a strict delay constraint $(d = 1)$, and show that the optimal power allocation and the corresponding distortion can be interpreted as *water-filling reflected on a reciprocal mirror*. Exploiting the results of [95], we also derive the optimal LT strategy under a strict delay constraint for a particular scenario in which the sensor transmits the measurement vector over parallel AWGN fading channels at each TS. Then, exploiting the optimal LT strategy derived for multiple measurements-parallel channels scenario above, we propose two LT strategies for general delay constraints. In both strategies, measurements are first collected and stored in a buffer whose size depends on the delay constraint, and then, are transmitted to the CC over multiple channel accesses within the delay constraint. The two strategies consider different measurement selection criterias, which are used to select the appropriate stored measurement to be transmitted at each channel access. We then derive the theoretical lower bound (TLB) and the LT lower bound (LLB) on the achievable MSE distortion. We characterize the MSE distortion achieved by the proposed LT schemes, as well as the TLB and the LLB under various power and delay constraints. We show that the MSE distortion diminishes as the delay constraint is relaxed if the sensor is capable of measuring more than one system parameter, i.e., $J > 1$. However, if $J = 1$, then relaxing the delay constraint does not provide any improvement in LT performance as argued in [95]. When the fading channel

follows a discrete distribution and the delay constraint is completely removed, we show that the proposed LT strategies meet the TLB under certain matching conditions between the channel states and the paramater variances; and hence, achieve the optimal performance.

When the CSI is known only by the decoder, we first derive the optimal LT strategy under a strict delay constraint. Then, we consider the multiple measurements-parallel channels scenario under a strict delay constraint and $J > 1$ assumption, and show that the optimal LT performance cannot be achieved by an LT scheme that is constrained to use only a one-to-one linear mapping between measurements and channels, as opposed to the $J = 1$ case [97], and the CSI is known by both the encoder and decoder [95], respectively. Since the optimal LT strategy is elusive for $J > 1$, we do not consider LT strategies for larger delay constraints. Finally, we derive the TLB on the achievable MSE distortion.

As it has been presented in the state of the art in Chapter 2, LT of Gaussian sources has been extensively studied in the literature. Goblick showed in [126] that zero-delay LT of a Gaussian source over an AWGN channel achieves the optimal MSE distortion. In [95], the optimal LT scheme that matches an r-dimensional Gaussian signal to a k-dimensional AWGN vector channel is characterized. It is shown that the optimal LT performance can be achieved by mapping ordered sources to ordered channels in a one-to-one fashion. LT of a Gaussian source over a fading AWGN channel is studied in [97]. It is shown that the optimal LT performance can be achieved by symbol-by-symbol processing, and increasing the block length does not provide any gain, as opposed to nonlinear coding schemes. In [96], LT of noisy vector measurements over a fading AWGN channel is studied under diagonal and general observation matrices. LT of vector Gaussian sources over static and fading multi-antenna channels is studied in [98] and [99], respectively. There is also growing interest in the performance of LT for multi-user systems. For example, zero-delay LT of bivariate Gaussian source and noisy Gaussian observations over Gaussian multiple access channels are studied in [127] and [128], respectively. The optimality of zero-delay LT holds in these models as well, up to a certain SNR threshold in the former, and at all SNR values in the latter.

The main contributions of this chapter can be summarized as follows:

- We study delay-constrained LT strategies for the transmission of composite Gaussian measurements from a sensor to a CC over an AWGN fading channel.
- Assuming that both the encoder and decoder know the CSI, we characterize the optimal LT scheme under a strict delay constraint, and provide a graphical interpretation for the optimal power allocation scheme.
- We propose two LT strategies for general delay constraints, and show that the distortion decreases as the delay constraint is relaxed. When the delay constraint is completely

removed, both strategies achieve the optimal performance under certain matching conditions.

- Assuming that the CSI is known only at the decoder, we derive the optimal LT strategy under a strict delay consraint.
- Then, we show that for the multiple measurements-parallel channels scenario, any LT scheme that uses only a one-to-one linear mapping between measurements and channels is suboptimal in general.

The rest of the chapter is structured as follows. The system model is presented in Section 5.2. In Sections 5.3 to 5.5 CSI is assumed at both the encoder and decoder. In Section 5.3, we study the optimal LT strategy under a strict delay constraint. Two LT strategies are proposed for general delay constraints in Section 5.4. In Section 5.5, we characterize the TLB and LLB on the achievable MSE distortion. In Section 5.6, the optimal LT strategy is derived under a strict delay constraint along with the TLB, when the CSI is known only by the decoder. In Section 5.7, we consider a particular symmetric scenario with multiple sensors and parallel channels. Section 5.8 presents extensive numerical results, and finally, Section 5.9 concludes the chapter.

5.2 System Model

We consider a CC that monitors the operation of a system through a wireless sensor (Fig. 5.1), which is capable of measuring J distinct system parameters. The jth system parameter is modelled as a zero-mean Gaussian r.v. with variance σ_j^2, i.e., $\mathcal{N}(0,\sigma_j^2)$, for $j \in [1{:}J]$, where $[1{:}J]$ denotes the set $\{1,2,\dots,J\}$. These system parameters are independent from each other, and their realizations are i.i.d. over time. In order to monitor the network operation, the CC requests the measurement of one system parameter from the sensor at each TS. The index of the requested system parameter at each TS is a r.v. denoted by $M \in [1{:}J]$, with distribution $p_M(m)$, which is also i.i.d. over time. Based on these requests, the sensor takes one measurement of the requested parameter m at each TS. Thereby, the model is that of a composite source introduced in Chapter 6 of [129]. The source S can be described as a composite source comprised of J distinct components (subsources), each operating independently of the others. In our model, each component produces data according to a Gaussian probability distribution $P(\cdot|m) = \mathcal{N}(0,\sigma_m^2)$. The set G of all subsources comprises the composite source. In our case,

$$G = \left[\mathcal{N}(0,\sigma_1^2), \mathcal{N}(0,\sigma_2^2), \dots, \mathcal{N}(0,\sigma_J^2)\right]. \tag{5.1}$$

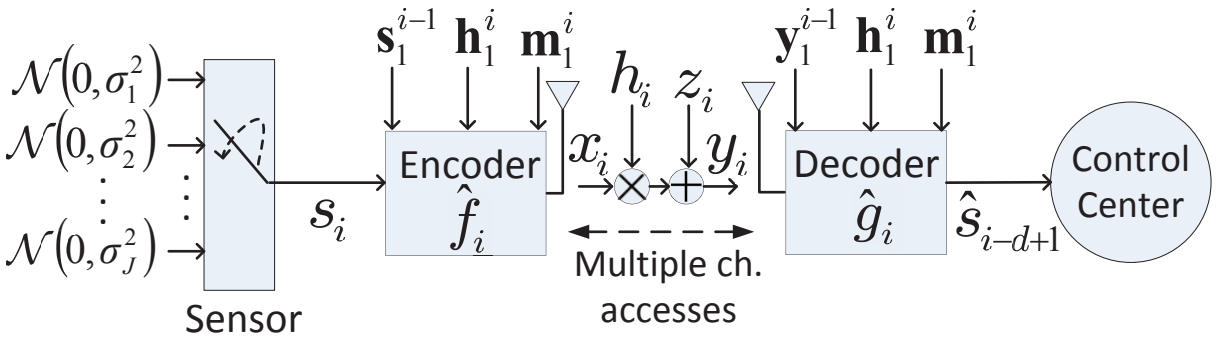


Figure 5.1: The illustration of the transmission model from the perspective of the sensor with multiple channel accesses.

The index of the requested system parameter m generates the sequence of positions assumed by the switch in Fig. 5.1. In our model both the encoder and the decoder possess the exact knowledge of this sequence. Notice that, in the particular case in which the encoder and decoder are uninformed about this sequence, the composite source is equivalent to a mixture of Gaussian distributions, i.e., $P_S(s) = \sum_{m=1}^{J} P_M(m) P_{S|M}(s|m)$.

We assume that the CC imposes a maximum delay constraint of $d \in \mathbb{Z}^+$ on the measurements, that is, the measurement requested in a TS needs to be transmitted within the following d TSs; otherwise, it becomes stale. The collected sensor measurements are transmitted to the CC over a fading channel with zero-mean and unit variance AWGN. The channel output at TS i is given by:

$$y_i = h_i x_i + z_i,$$

where x_i is the channel input, z_i is the additive noise with $Z \sim \mathcal{N}(0,1)$, and h_i is the fading state of the channel. We consider a fading channel model, and assume that the fading coefficient $H_i \in \mathbb{R}$ is modelled as a r.v. i.i.d. over time with probability distribution $p_H(h)$.

We define $\mathbf{m}_i^l = [m_i, m_{i+1}, \ldots, m_l]$ as the sequence of indices of requested parameters at TSs $[i{:}l]$ for $i \leq l$. The measurement sequence is defined similarly as $\mathbf{s}_i^l = [s_i, \ldots, s_l]$, where the i-th entry s_i is the measured value of the requested parameter m_i at TS i. Therefore, the sequence $\mathbf{s}_i^l$ has independent entries, where the i-th entry comes from a Gaussian distribution with variance $\sigma_{m_i}^2$. Note that in our composite Gaussian measurements model, conditioned on the requested parameter index, which is known by both the encoder and decoder, the source samples follow Gaussian distributions with different variance values.

The channel state and the output sequences at TSs $[i{:}l]$ are similarly defined as

$\mathbf{h}_i^l = [h_i, \ldots, h_l]$ and $\mathbf{y}_i^l = [y_i, \ldots, y_l]$, respectively. We assume that both the encoder and decoder at TS i know all the past channel states, $\mathbf{h}_1^{i-1}$, and the indices of requested parameters, $\mathbf{m}_1^i$, as well as the statistics of the measured parameters, σ_m^2, the parameter requests, $p_M(m)$, and the channel, $p_H(h)$. In the first part of this chapter we assume that both the encoder and decoder know the current channel state, h_i. Note that this assumption might be hard to realize for a fast fading channel model; on the other hand, our system model can be considered as instances of a slow fading channel. Typically, there will be a large number of sensors in the system, and each sensor is going to be scheduled only once in a while; and hence, each TS in our system model can be considered as one instance of a slow fading channel when a particular sensor is scheduled to transmit. Since these instances are separated from each other due to the transmission of other sensors, corresponding channel states are modeled as i.i.d., and are assumed to be known by both the encoder and decoder, as channel estimation and CSI feedback can be carried out between two transmissions of the same sensor. In Section 5.6 we will consider the scenario in which the CSI is known only by the decoder.

Encoding Function

The encoding function $\hat{f}_i : \mathbb{R}^i \times \mathbb{R}^i \times \mathbb{R}^i \to \mathbb{R}$, maps $\mathbf{s}_1^i$, $\mathbf{h}_1^i$, and $\mathbf{m}_1^i$ to a channel input x_i at each TS i, i.e., $x_i = \hat{f}_i(\mathbf{s}_1^i, \mathbf{h}_1^i, \mathbf{m}_1^i)$. An average power constraint of P is imposed on the encoding function:

$$\bar{P} \triangleq \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathrm{E}_{M,H,S}\left[|X_i|^2\right] \leq P,$$

where $\mathrm{E}_{M,H,S}[\cdot]$ denotes the expectation over M, H and S. For any generic transmission policy, the encoding function $\hat{f}_i$, at TS i, may consider to use any combination of $\mathbf{s}_1^i$, $\mathbf{h}_1^i$, and $\mathbf{m}_1^i$ to generate x_i. This gives rise to a time-varying encoding scheme.

Decoding Function

At the end of TS i, the goal of the CC is to estimate with the minimum MSE distortion, the measurement s_{i-d+1}, which has been requested exactly $d-1$ TSs ago, and is about to expire. The decoding function $\hat{g}_i : \mathbb{R}^i \times \mathbb{R}^i \times \mathbb{R}^i \to \mathbb{R}$, estimates $\hat{s}_{i-d+1}$ based on $\mathbf{y}_1^i$, $\mathbf{h}_1^i$, and $\mathbf{m}_1^i$, i.e., $\hat{s}_{i-d+1} = \hat{g}_i(\mathbf{y}_1^i, \mathbf{h}_1^i, \mathbf{m}_1^i)$. The MSE distortion is given by:

$$\bar{D} \triangleq \lim_{n\to\infty} \frac{1}{n} \sum_{i=d}^{n} \mathrm{E}_{M,H,S,Z}\left[|S_{i-d+1} - \hat{S}_{i-d+1}|^2\right].$$

The decoding function $\hat{g}_i$, at TS i, reconstructs the measurement using $\mathbf{y}_1^i$, $\mathbf{h}_1^i$, and $\mathbf{m}_1^i$.

Hence, similarly to the encoder, the decoder may be time-varying.

We are interested only in LT policies in which $\hat{f}_i$'s are restricted to be linear functions of the sensor measurements, s_i's, i.e., $\hat{f}_i(\mathbf{s}_1^i, \mathbf{h}_1^i, \mathbf{m}_1^i) \triangleq f_i(\mathbf{h}_1^i, \mathbf{m}_1^i)\mathbf{s}_1^i$, where $f_i(\mathbf{h}_1^i, \mathbf{m}_1^i)$ is a vector. Under this linearity constraint, the optimal estimators at the receiver, $\hat{g}_i$'s, are also linear functions of the channel outputs, y_i's, i.e., $\hat{g}_i(\mathbf{y}_1^i, \mathbf{h}_1^i, \mathbf{m}_1^i) \triangleq g_i(\mathbf{h}_1^i, \mathbf{m}_1^i)\mathbf{y}_1^i$, where $g_i(\mathbf{h}_1^i, \mathbf{m}_1^i)$ is a vector. Hereafter, we will refer to f_i and g_i for the encoding and decoding functions at TS i, respectively.

5.3 Strict Delay Constraint

We first derive the optimal LT strategy under a strict delay constraint $(d = 1)$, and characterize the minimum achievable MSE distortion. In this scenario, optimal LT performance is achieved by transmitting only the most recent measurement since all the previous measurements have expired, and transmitting an expired measurement cannot help the estimation of the current measurement since the measurements are independent. Then the encoding function $f_i(h_i, m_i)$ at TS i is a scalar. Given the encoding function, the decoding function $g_i(h_i, m_i)$ that minimizes the MSE for Gaussian r.v.s is the linear MMSE estimator [130], and is also a scalar.

In particular, for a measurement s_i with variance $\sigma^2_{m_i}$, and channel output $y_i = h_i f_i(h_i, m_i)s_i + z_i$ at TS i, the decoding function can be written explicitly as:

$$g_i(h_i, m_i) = \frac{\mathrm{E}_{S,Z}[S_i Y_i]}{\mathrm{E}_{S,Z}[Y_i^2]} = \frac{|h_i| f_i(h_i, m_i)\sigma^2_{m_i}}{|h_i|^2 f_i(h_i, m_i)^2\sigma^2_{m_i} + 1}. \tag{5.2}$$

In the following lemma we show that there is no loss of optimality by limiting the encoding function to be time-invariant.

Lemma 5.1. *Under a strict delay constraint there is no loss of optimality by considering only time-invariant encoding functions, i.e., $f_i(h_i, m_i) = f(h_i, m_i)\ \forall i$.*

Proof.

$$\begin{aligned}
\bar{D} &= \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathrm{E}_{M,H,S,Z}\left[|S_i - \hat{S}_i|^2\right], \\
&= \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathrm{E}_{M,H}\left[\frac{\sigma_m^2}{|h|^2 f_i(h,m)^2\sigma_m^2 + 1}\right], &(5.3)\\
&\geq \mathrm{E}_{M,H}\left[\frac{\sigma_m^2}{|h|^2 f(h,m)^2\sigma_m^2 + 1}\right], &(5.4)
\end{aligned}$$

where (5.3) is the average MSE distortion under a strict delay constraint $(d = 1)$; and defining $f(h,m)^2 \triangleq \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f_i(h,m)^2$ such that $f(h,m)$ satisfies the average power constraint P, (5.4) follows from the convexity of the function $\mathrm{E}_{M,H}\left[\frac{\sigma_m^2}{|h|^2 f_i(h,m)^2\sigma_m^2+1}\right]$ in terms of $f_i(h,m)^2$, and the equality holds iff $f_i(h,m) = f(h,m)$ for $\forall i$ and due to the strict convexity of the aforementioned function. Thus, the time-invariant encoding function $f(h,m)$, which is a function of only h and σ_m^2, does not lead to any loss in optimality. □

The time-invariant encoding function $f(h,m)$ leads to a time-invariant decoding function $g(h,m)$. In the rest of this chapter, we will consider time-invariant encoding and decoding functions without loss of optimality. Then, the MSE distortion, $\bar{D} = \mathrm{E}_{M,H,S,Z}[|S - \hat{S}|^2]$, and the average power, $\bar{P} = \mathrm{E}_{M,H,S}[|X|^2]$, can be written explicitly as functions of h and σ_m^2, as follows:

$$\bar{D} = \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} \frac{\sigma_m^2}{|h|^2 f(h,m)^2\sigma_m^2 + 1} p_H(h)\mathrm{d}h, \tag{5.5}$$

$$\bar{P} = \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} f(h,m)^2\sigma_m^2 p_H(h)\mathrm{d}h. \tag{5.6}$$

The optimal linear encoding function $f^*(h,m)$ is found as the solution to the convex optimization problem $\bar{D}^* \triangleq \underset{f(h,m)}{\text{minimize}}\, \bar{D}$, subject to the average power constraint $\bar{P} \leq P$, which can be written explicitly as follows:

$$\begin{aligned} \bar{D}^* \triangleq \underset{f(h,m)}{\text{minimize}} \; & \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} \frac{\sigma_m^2}{|h|^2 f(h,m)^2\sigma_m^2 + 1} p_H(h)\mathrm{d}h \\ \text{subject to} \; & \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} f(h,m)^2\sigma_m^2 p_H(h)\mathrm{d}h \leq P. \end{aligned} \tag{5.7}$$

From the KKT optimality conditions [119], we obtain:

$$f^*(h,m) = \sqrt{\left[\frac{\lambda^*}{|h|\sigma_m} - \frac{1}{|h|^2\sigma_m^2}\right]^+}, \tag{5.8}$$

where λ^* is the optimal Lagrange multiplier, such that $\bar{P} = P$.

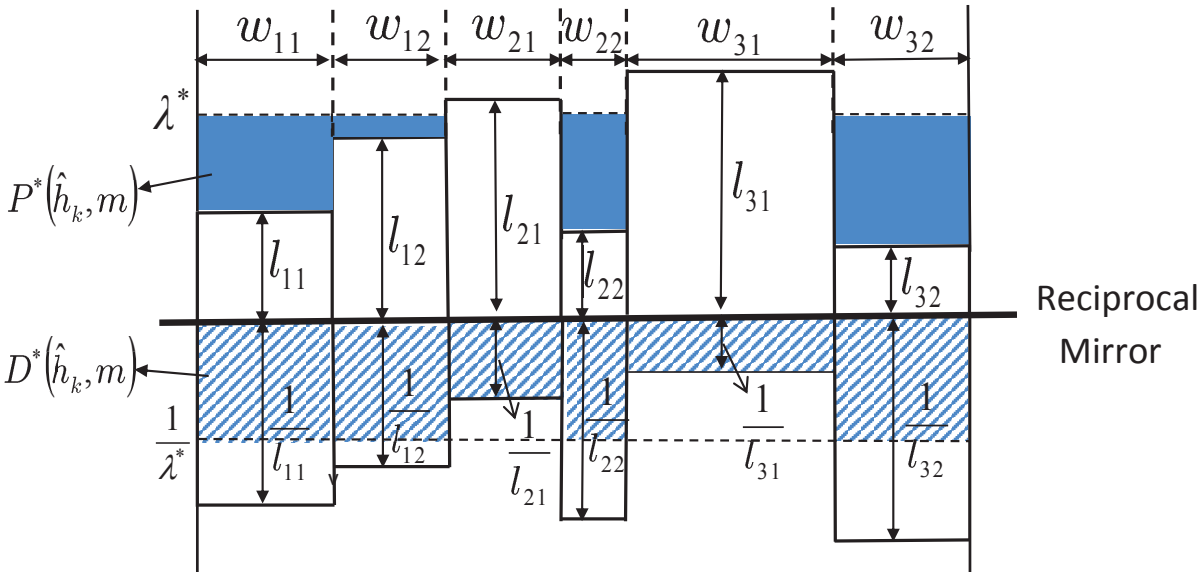


Figure 5.2: Water-filling reflected on a reciprocal mirror.

The optimal power allocation and the corresponding distortion are given by:

$$P^*(h,m) = \frac{\sigma_m}{|h|}\left[\lambda^* - \frac{1}{|h|\sigma_m}\right]^+, \tag{5.9}$$

$$D^*(h,m) = \frac{\sigma_m}{|h|}\min\left(\frac{1}{\lambda^*}, |h|\sigma_m\right), \tag{5.10}$$

where $\bar{D}^* = \mathrm{E}_{M,H}\left[D^*(h,m)\right]$ and $\mathrm{E}_{M,H}\left[P^*(h,m)\right] = P$.

In Fig. 5.2, we present a graphical interpretation of the optimal power allocation and the corresponding distortion for $J = 2$ parameters with variances σ_1^2 and σ_2^2, which are requested with probabilities $p_M(1), p_M(2)$, respectively. We also consider a discrete fading channel with three states, where the kth state, $\hat{h}_k$, is observed with probability $p_H(\hat{h}_k)$, $k = 1, 2, 3$. Fig. 5.2 depicts rectangles that are placed upon a mirror surface and their reciprocally scaled images below. Rectangles represent all possible source-channel pairs $\{\sigma_m, \hat{h}_k\}$, where $l_{km} \triangleq \frac{1}{|\hat{h}_k|\sigma_m}$ and $w_{km} \triangleq \frac{\sigma_m}{|\hat{h}_k|}$ indicate the height and width of the rectangles, respectively. The total power is poured above the level l_{km} up to the water level λ^* across the rectangles placed upon the mirror. The optimal power allocated to the source-channel pair $\{\sigma_m, \hat{h}_k\}$ is given by the shaded area below the water level and above l_{km}. The corresponding distortion values are found by simply looking at the reciprocally scaled reflections of the rectangles and the water level on the mirror. If $\frac{1}{l_{km}} > \frac{1}{\lambda^*}$, distortion is given by the width w_{km} times the reciprocal of the water level $\frac{1}{\lambda^*}$, and if $\frac{1}{l_{km}} \leq \frac{1}{\lambda^*}$, distortion is σ_m^2, which are illustrated as dashed areas in Fig. 5.2. We call this as *water-filling reflected on a reciprocal mirror*.

5.3.1 Multiple Measurements and Parallel Channels

Next, we assume that the CC requests $N > 1$ measurements from the sensor at each TS, and the sensor transmits a length-N measurement vector over N parallel orthogonal AWGN fading channels under a strict delay constraint $(d = 1)$. For this scenario, we characterize the optimal LT strategy by generalizing the results of [95] derived for Gaussian vector sources to our composite Gaussian measurements model. This scenario differs from the system model defined in Section 5.2, since we allow to take N measurements at each TS as opposed to taking only one measurement at each TS. However, we will exploit the optimal LT strategy in this setting for the construction of the proposed transmission strategies in Section 5.4, as well as for characterizing the LLB in Section 5.5.2.

Only for this scenario, we define $\mathbf{m} = [m_1, \ldots, m_N]$ as the vector of indices of N requested parameters at a particular TS. Then, the sensor takes the length-N measurement vector $\mathbf{s} = [s_1, \ldots, s_N]$ according to the parameters indicated by $\mathbf{m}$, i.e., s_1 is the measured value of parameter m_1. For a strict delay constraint $(d = 1)$, the optimal LT performance is achieved by transmitting only the most recent measurement vector. We assume that the N channels are i.i.d with distribution $p_H(h)$, and $\mathbf{H}$ is defined as the $N \times N$ diagonal channel matrix. The diagonal elements of $\mathbf{H}$ are denoted by a channel vector $\mathbf{h} = [h_1, \ldots, h_N]$ at a particular TS. Similarly to Lemma 5.1, the encoding function can be limited to a time-invariant $N \times N$ square matrix $\mathbf{F}_{\mathbf{h},\mathbf{m}}$ without loss of optimality, where subscripts $\mathbf{h}$ and $\mathbf{m}$ indicate the dependence of the encoding matrix on the realizations of $\mathbf{h}$ and $\mathbf{m}$. The length-N channel output vector at that particular TS is given by:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z},$$

where $\mathbf{x}$ is the length-N channel input vector and $\mathbf{z}$ is the length-N additive noise vector with $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$.

The encoder at any TS maps its measurement vector $\mathbf{s}$, to a channel input vector $\mathbf{x}$, i.e., $\mathbf{x} = \mathbf{F}_{\mathbf{h},\mathbf{m}}\mathbf{s}$. An average power constraint of P is imposed on the encoding function:

$$\begin{aligned} \bar{P} &= \frac{1}{N} \operatorname{Tr}\left\{ \mathrm{E}_{M,H,S}[\mathbf{x}\mathbf{x}^T] \right\}, \\ &= \frac{1}{N} \operatorname{Tr}\left\{ \mathrm{E}_{M,H}[\mathbf{F}_{\mathbf{h},\mathbf{m}} \mathbf{C}_{\mathbf{s}} \mathbf{F}_{\mathbf{h},\mathbf{m}}^T] \right\} \leq P, \end{aligned} \tag{5.11}$$

where $\mathbf{C}_{\mathbf{s}} = \mathrm{E}_S[\mathbf{s}\mathbf{s}^T]$.

Given the encoding function, the decoding function that minimizes the MSE for a Gaussian random vector is the $N \times N$ linear MMSE estimator matrix $\mathbf{G_{h,m}}$ [130], which is also time-invariant. Similarly to $\mathbf{F_{h,m}}$, subscripts $\mathbf{h}$ and $\mathbf{m}$ indicate the dependence of the decoding matrix on the realizations of $\mathbf{h}$ and $\mathbf{m}$. For the measurement vector $\mathbf{s}$, and the channel output vector $\mathbf{y}$, at any TS, we have:

$$\mathbf{G_{h,m}} = \mathbf{C_{sy}}\mathbf{C_y^{-1}} = \mathbf{C_s}\mathbf{F_{h,m}^T}\mathbf{H}^T\mathbf{\Phi}, \tag{5.12}$$

where $\mathbf{C_{sy}} = \mathrm{E}_{S,Z}[\mathbf{s}\mathbf{y}^T]$, $\mathbf{C_y} = \mathrm{E}_{S,Z}[\mathbf{y}\mathbf{y}^T]$ and $\mathbf{\Phi} \triangleq (\mathbf{H}\mathbf{F_{h,m}}\mathbf{C_s}\mathbf{F_{h,m}^T}\mathbf{H}^T + \mathbf{I})^{-1}$.

At any TS, the CC estimates the most recent measurement vector $\mathbf{s}$ as $\hat{\mathbf{s}}$, i.e., $\hat{\mathbf{s}} = \mathbf{G_{h,m}}\mathbf{y}$. The MSE distortion is given by:

$$\begin{aligned}\bar{D} &= \frac{1}{N}\,\mathrm{Tr}\left\{\mathrm{E}_{M,H,S,Z}[\big(\mathbf{s}-\hat{\mathbf{s}}\big)(\mathbf{s}-\hat{\mathbf{s}})^T]\right\},\\ &= \frac{1}{N}\,\mathrm{Tr}\left\{\mathrm{E}_{M,H}[\mathbf{C_s} - \mathbf{C_s}\mathbf{F_{h,m}^T}\mathbf{H}^T\mathbf{\Phi}\mathbf{H}\mathbf{F_{h,m}}\mathbf{C_s}]\right\}.\end{aligned} \tag{5.13}$$

The optimal linear encoding matrix $\mathbf{F^*_{h,m}}$, is found as the solution to the convex optimization problem $\bar{D}^* \triangleq \underset{\mathbf{F_{h,m}}}{\text{minimize}}\ \bar{D}$, subject to the average power constraint $\bar{P} \leq P$, which can be written explicitly as follows:

$$\begin{aligned}\bar{D}^* \triangleq \underset{\mathbf{F_{h,m}}}{\text{minimize}}\ & \frac{1}{N}\,\mathrm{Tr}\left\{\mathrm{E}_{M,H}[\mathbf{C_s} - \mathbf{C_s}\mathbf{F_{h,m}^T}\mathbf{H}^T\mathbf{\Phi}\mathbf{H}\mathbf{F_{h,m}}\mathbf{C_s}]\right\}\\ \text{subject to}\ & \frac{1}{N}\,\mathrm{Tr}\left\{\mathrm{E}_{M,H}[\mathbf{F_{h,m}}\mathbf{C_s}\mathbf{F_{h,m}^T}]\right\} \leq P.\end{aligned} \tag{5.14}$$

For a set of static parallel AWGN channels and Gaussian vector sources, the optimal linear encoding matrix transmits one measurement over each channel [95]. The optimal mapping between channels and measurements is as follows: We first reorder the measurement vector $\mathbf{s}$ to obtain $\bar{\mathbf{s}} = [s_{(1)}, \ldots, s_{(N)}]$, such that $\sigma^2_{m_{(1)}} \leq \sigma^2_{m_{(2)}} \leq \cdots \leq \sigma^2_{m_{(N)}}$, and reorder the channel vector $\mathbf{h}$ to obtain $\bar{\mathbf{h}} = \big[h_{(1)}, \ldots, h_{(N)}\big]$, such that $|h_{(1)}| \leq |h_{(2)}| \leq \cdots \leq |h_{(N)}|$. Then, the optimal linear encoding matrix $\mathbf{F^*_{h,m}}$ is diagonal with entries $\big[f_{(1)}(h_{(1)}, m_{(1)}), \ldots, f_{(N)}(h_{(N)}, m_{(N)})\big]$, and it maps the ordered measurements to ordered channel states. In order to find the diagonal entries of $\mathbf{F^*_{h,m}}$, we can explicitly rewrite the convex optimization problem in (5.14) by using the optimal mappings derived in [95], as follows:

$$\begin{aligned}\bar{D}^* \triangleq \underset{f_{(t)}(h_{(t)},m_{(t)})}{\text{minimize}}\ & \mathrm{E}_{M_{(t)},H_{(t)}}\left[\frac{1}{N}\sum_{t=1}^{N}\frac{\sigma^2_{m_{(t)}}}{|h_{(t)}|^2 f_{(t)}(h_{(t)},m_{(t)})^2\sigma^2_{m_{(t)}}+1}\right] \\ \text{subject to } & \mathrm{E}_{M_{(t)},H_{(t)}}\left[\frac{1}{N}\sum_{t=1}^{N} f_{(t)}(h_{(t)},m_{(t)})^2\sigma^2_{m_{(t)}}\right] \le P,\end{aligned} \tag{5.15}$$

where the expectation is taken over $M_{(t)}$ and $H_{(t)}$ for $t \in [1{:}N]$. The t-th smallest entry of the requested parameter vector $\mathbf{m} = [m_1, m_2, \ldots, m_N]$, is denoted by the r.v. $M_{(t)} \in [1{:}J]$ with the order statistics $p_{M_{(t)}}(m)$. Without loss of generality, we assume that ordering the entries of $\mathbf{m}$ in ascending order, i.e., $m_{(1)} \le m_{(2)} \le \cdots \le m_{(N)}$, implies ordering the entries of the measurement vector $\mathbf{s}$ in ascending variances, i.e., $\sigma^2_{m_{(1)}} \le \sigma^2_{m_{(2)}} \le \cdots \le \sigma^2_{m_{(N)}}$. Similarly, the t-th smallest entry of the channel vector $\mathbf{h} = [h_1, h_2, \ldots, h_N]$ is denoted by the r.v. $H_{(t)} \in \mathbb{R}$ with the order statistics $p_{H_{(t)}}(h)$.

The optimal linear encoding matrix $\mathbf{F}^*_{\mathbf{h},\mathbf{m}}$ with diagonal entries $f^*_{(t)}(h_{(t)}, m_{(t)})$ for $t \in [1{:}N]$, can be found from the Lagrange and the KKT conditions as follows:

$$f^*_{(t)}(h_{(t)},m_{(t)}) = \sqrt{\left[\frac{\delta^*}{|h_{(t)}|\sigma_{m_{(t)}}} - \frac{1}{|h_{(t)}|^2\sigma^2_{m_{(t)}}}\right]^+}, \tag{5.16}$$

where δ^* is the optimal Lagrange multiplier, such that $\bar{P} = P$ in (5.15).

Similarly, the optimal power allocation and the corresponding distortion can be found by using the *water-filling reflected on a reciprocal mirror* interpretation. The optimal Lagrange multiplier δ^* depends on $p_{M_{(t)}}(m)$ and $p_{H_{(t)}}(h)$, which can be found explicitly by using the order statistics. In the following lemma, we give the t-th order statistics $p_{M_{(t)}}(m)$ and $p_{H_{(t)}}(h)$, for $t \in [1{:}N]$.

Lemma 5.2. *Let $F_M(m)$ and $F_H(h)$ denote the cumulative distribution functions of $p_M(m)$ and $p_H(h)$, respectively. Given $F_M(m)$, $p_M(m)$, $F_H(h)$, $p_H(h)$ and N, the t-th order statistics $p_{M_{(t)}}(m)$ and $p_{H_{(t)}}(h)$, $t \in [1{:}N]$, are found as*:

$$p_{H_{(t)}}(h) = t p_H(h)\binom{N}{t}(F_H(h))^{t-1}(1-F_H(h))^{N-t}, \tag{5.17}$$

$$p_{M_{(t)}}(m) = \sum_{b=t}^{N}\binom{N}{b}\left[F_M(m)^b(1-F_M(m))^{N-b} - F_M(m-1)^b(1-F_M(m-1))^{N-b}\right]. \tag{5.18}$$

Proof. The proof is trivial and achieved through the definition of the cumulative distribution functions of $H_{(t)}$ and $M_{(t)}$.

$$F_{H_{(t)}}(h) = \Pr\{H_{(t)} \leq h\} = \Pr\{\text{at least } t \text{ of } H\text{'s are} \leq h\}, \tag{5.19}$$

$$= \sum_{b=t}^{N} \frac{N!}{(N-b)!b!} F_H(h)^b (1 - F_H(h))^{N-b}, \tag{5.20}$$

where (5.19) implies a binomial distribution with at least t successes and can be formulated as (5.20). The t-th order statistics $p_{H_{(t)}}(h)$ is found by taking the derivative of (5.20) with respect to h. The same proof holds for $M_{(t)}$. □

5.4 LT Strategies

In this section, we propose two LT strategies for general delay constraints $d \geq 1$. The block diagram of the proposed LT strategies is illustrated in Fig. 5.3. Both strategies are composed of two main blocks, namely, storage and transmission blocks. There are two buffers of size $\bar{d}$ measurements, namely, the measurement buffer (MB) and the transmission buffer (TB). Here, we present these two schemes for an odd delay constraint, i.e., $d \in \{1, 3, 5, \ldots\}$, but they can be easily adapted to the case when d is even. In the storage block, given a delay constraint of $d = 2\bar{d} - 1$ for $\bar{d} \in [1{:}\infty]$, the sensor collects a block of $\bar{d}$ consecutive measurements after $\bar{d}$ consecutive TSs, and stores them in the MB. The consecutive blocks of $\bar{d}$ measurements, taken over successive time intervals, are indexed by $\bar{k} = \{1, 2, \ldots\}$. Then, the $\bar{k}$-th block consists of the measurements taken within TSs $[(1 + (\bar{k} - 1)\bar{d}){:}\bar{k}\bar{d}]$, i.e., $\mathbf{s}_{(1+(\bar{k}-1)\bar{d})}^{\bar{k}\bar{d}}$. When the MB gets full with the $\bar{d}$ measurements of the $\bar{k}$-th block, the sensor removes $\mathbf{s}_{(1+(\bar{k}-1)\bar{d})}^{\bar{k}\bar{d}}$ from the MB and loads them into the TB. Then, for the next consecutive $\bar{d}$ TSs $[\bar{k}\bar{d}{:}((\bar{k}+1)\bar{d} - 1)]$, the sensor accesses the channel and transmits a linear function of the measurements in the TB, i.e., $\mathbf{s}_{(1+(\bar{k}-1)\bar{d})}^{\bar{k}\bar{d}}$, over the channel states $\mathbf{h}_{\bar{k}\bar{d}}^{((\bar{k}+1)\bar{d}-1)}$ satisfying the delay constraint d. The specifics of these linear functions will be explained below.

Note that, while the sensor transmits the measurements in the TB, it starts refilling the MB with new measurements $\mathbf{s}_{(\bar{k}\bar{d}+1)}^{(\bar{k}\bar{d}+\bar{d})}$. After $\bar{d}$ channel accesses within TSs $[\bar{k}\bar{d}{:}((\bar{k}+1)\bar{d} - 1)]$, the MB gets full again and its new $\bar{d}$ measurements are transferred to the TB for transmission over the next $\bar{d}$ TSs.

The proposed transmission strategies consist of two sub-blocks, namely, the measurement selection and scaling sub-blocks. This division is motivated by the results of [95] presented in Section 5.3.1, in which N ordered measurements are mapped one-to-one to N ordered chan-

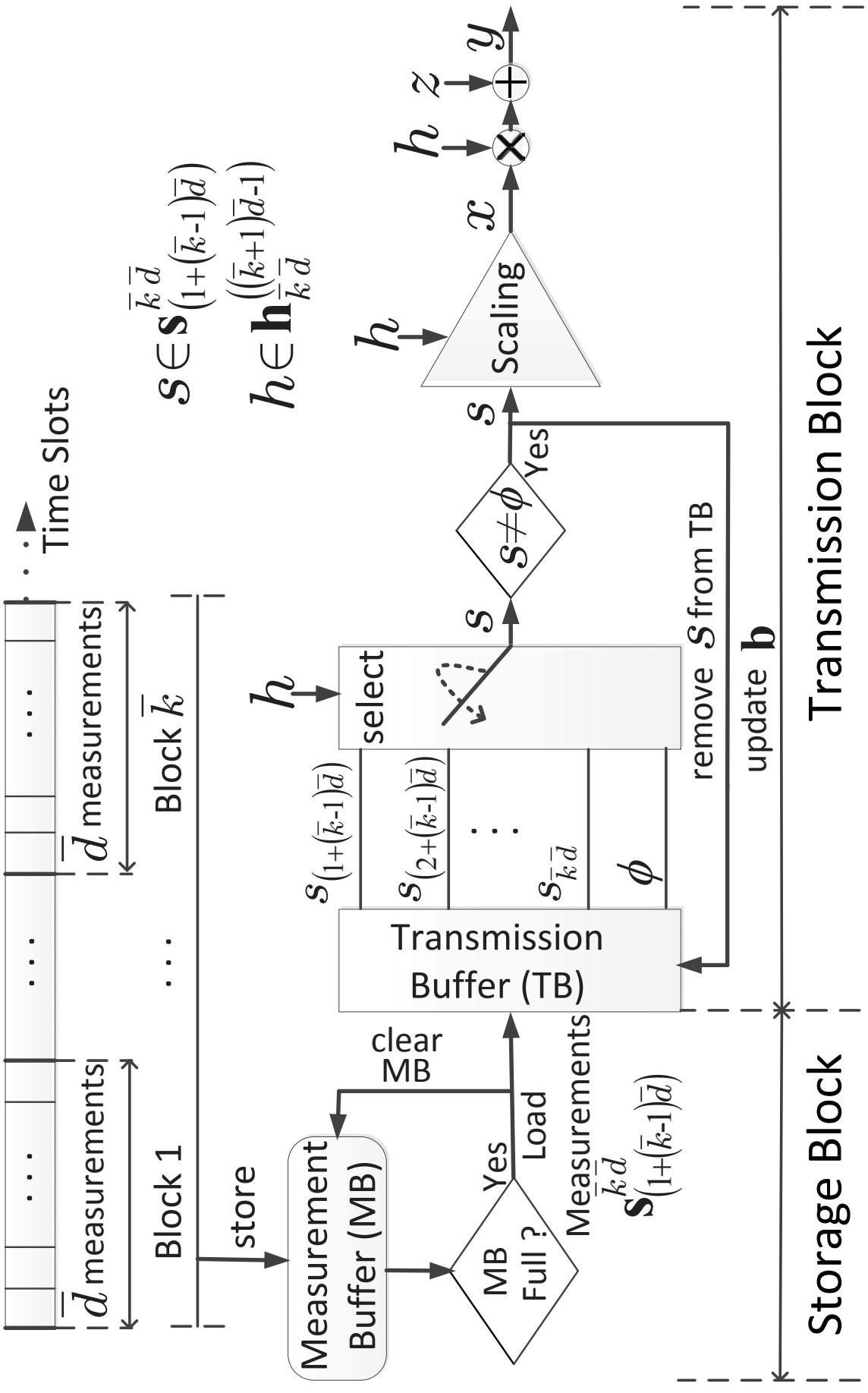


Figure 5.3: The block diagram illustration of the proposed LT strategies.

nels, and each measurement is transmitted over its corresponding channel. Hence, we assume that, at each channel access, the sensor selects only one measurement and scales it to a channel input value. However, in this case, we cannot directly use the optimal LT scheme in [95] and guarantee that the selected measurement and the channel state satisfy the optimal matching. This is because even though $\bar{d}$ measurements are available in the TB in advance, the states of the next $\bar{d}$ channels are not available to the transmitter as in the parallel channel model of [95]; and instead, they become available over time. The two proposed LT strategies differ in the way they choose the measurement to be transmitted at each TS.

Algorithm 5.1 LTHM and LTSM

Initialization:

Load measurements of MB, $\mathbf{s}_{(1+(\bar{k}-1)\bar{d})}^{\bar{k}\bar{d}}$, into TB and update $\mathbf{b}$.

for $i = \bar{k}\bar{d}$ to $(\bar{k}+1)\bar{d}-1$ **do** ▷ TSs for $\bar{d}$ channel accesses

  if $|h_i| \in \mathcal{H}_m$ and $b_m \neq 0$ **then** ▷ LTHM and LTSM

  Measurement selection:

  Select one measurement of parameter m from TB.

  Scaling:

  Transmit the measurement over $|h_i|$ with an allocated power of Eqn. (5.21).

  $b_m \leftarrow b_m - 1$ ▷ update $\mathbf{b}$

  else if $|h_i| \in \mathcal{H}_m$ and $b_m = 0$ **then** ▷ only LTSM

  Find ς by solving $\min_{b_\varsigma \neq 0} \left||h_i| - h'_\varsigma\right|$.

  Measurement selection:

  Select one measurement of parameter ς from TB.

  Scaling:

  Transmit the measurement over $|h_i|$ with an allocated power of Eqn. (5.21).

  $b_m \leftarrow b_m - 1$ ▷ update $\mathbf{b}$

  end if

end for

$\bar{k} \leftarrow \bar{k} + 1$ and go to **Initialization**

5.4.1 Linear Transmission Scheme with Hard Matching (LTHM)

This transmission scheme has the following measurement selection criteria. Assume, without loss of generality, that parameters are ordered such that $\sigma_1^2 > \sigma_2^2 > \cdots > \sigma_J^2$. We divide the channel magnitude space ($\mathbb{R}^+$) into J ordered channel intervals as, $\mathcal{H}_m = [H'_m, H'_{(m-1)})$, where $H'_m < H'_{(m-1)}$ for $m \in [1{:}J]$. The boundary values are chosen as $H'_0 = \infty$, $H'_J = 0$ and $H'_m = F_H^{-1}(1 - \sum_{j=1}^{m} p_M(j))$, for $m \in [1{:}(J-1)]$, where $F_H^{-1}(\cdot)$ denotes the inverse of the cumulative distribution function of the channel magnitude $|h|$, $F_H(|h|)$. Observe that according to this choice, the probability of the channel magnitude belonging to $\mathcal{H}_m$ is $\Pr\{|h| \in \mathcal{H}_m\} = p_M(m)$.[1]

The algorithmic description of LTHM is given in Algorithm 5.1. Let $\mathbf{b} = [b_1, b_2, \ldots, b_J]$ be a J-length vector, where the m-th entry, $b_m \in [0{:}\bar{d}]$, denotes the number of measurements of parameter m in the TB, for $m \in [1{:}J]$. At each channel access, if $|h| \in \mathcal{H}_m$ and $b_m \neq 0$, then the sensor selects one measurement of the parameter type m from the TB and feeds it to the scaling sub-block. If there are multiple measurements of the same parameter type m in the TB, i.e., $b_m > 1$, then the sensor selects one of them randomly. The selected measurement is removed from the TB and $\mathbf{b}$ is updated by reducing the m-th entry, b_m, by one. Thereby, each measurement is transmitted only once. On the other hand, if $|h| \in \mathcal{H}_m$ and $b_m = 0$, no measurement is transmitted in that TS. Hence, LTHM considers a hard matching condition for selecting measurements, in which each parameter has a corresponding interval of channel states, and only measurements of that parameter can be transmitted over a channel state from that interval. Note that, since the channel state is known at the receiver, it also knows which type of measurement is transmitted at each TS.

For the scaling sub-block we use the power allocation strategy derived in Section 5.3. Thus, the selected measurement of the parameter type m is transmitted at the current channel state $|h| \in \mathcal{H}_m$, for $m \in [1{:}J]$, by allocating power $P(h, m)$, leading to distortion $D(h, m)$:

[1] If channel fading follows a discrete distribution, we define sets of channel states as opposed to intervals. With abuse of notation, we denote the mth set as $\mathcal{H}_m$, for $m \in [1{:}J]$. Suppose that the discrete channel states are ordered as $|\hat{h}_1| > |\hat{h}_2| > |\hat{h}_3| > \cdots$. We allocate the discrete states into J sets such that the probability of channel state falling into set $\mathcal{H}_m$ is $p_M(m)$. However, it may be possible that the channel states cannot be grouped to satisfy this equality exactly for all m. In that case we create virtual states to satisfy these equalities, as explained below.

Let j be the minimum index for which $\sum_{i=1}^{j} p_H(|h| = \hat{h}_i) > p_M(1)$. Define $p_M^1 = p_M(1) - \sum_{i=1}^{j-1} p_H(|h| = \hat{h}_i)$. We define a new virtual channel state $\hat{h}_j^1$, whose gain is equivalent to $\hat{h}_j$. Whenever the real channel state is $\hat{h}_j$, we randomly assign the channel state to $\hat{h}_j^1$ with probability $p_M^1/p_H(\hat{h}_j)$. We let $\mathcal{H}_1 = \{\hat{h}_1, \ldots, \hat{h}_{j-1}, \hat{h}_j^1\}$. We repeat the same process for $p_M(2)$, starting with channel state $\hat{h}_j$ whose probability is now $p_H(\hat{h}_j) - p_M^1$.

$$P(h,m) = \begin{cases} \left[\frac{\mu\sigma_m}{|h|} - \frac{1}{|h|^2}\right]^+, & \text{if hard matching holds,} \\ 0, & \text{otherwise.} \end{cases} \tag{5.21}$$

$$D(h,m) = \begin{cases} \frac{\sigma_m^2}{|h|^2 P(h,m)+1}, & \text{if hard matching holds,} \\ \sigma_m^2, & \text{otherwise,} \end{cases} \tag{5.22}$$

where μ is chosen such that the average power constraint is satisfied.

After every transmission, the CC estimates the transmitted measurement s by using the channel output y. It is noteworthy that after $\bar{d}$ channel accesses, we may have untransmitted measurements in the TB. TB is emptied anyway since these measurements have expired, and they are estimated with the maximum distortion σ_m^2. As we show next, the average number of untransmitted measurements decreases with the increasing delay constraint d. However, for a finite delay constraint the untransmitted measurements dominate the distortion even for a high average transmission power constraint. In order to combat this drawback, we propose an alternative LT scheme.

5.4.2 Linear Transmission Scheme with Soft Matching (LTSM)

The algorithmic description of LTSM is given in Algorithm 5.1. The LTSM retains the hard matching condition of LTHM, i.e., at each channel access, if $|h| \in \mathcal{H}_m$ and $b_m \neq 0$ for $m \in [1{:}J]$, LTSM selects one measurement of the parameter type m from the TB. Hence, LTSM also gives the highest selection priority to the measurement of the parameter type that satisfies the hard matching condition with the channel state. However, if $|h| \in \mathcal{H}_m$ and $b_m = 0$, LTSM does not waste the channel state; and instead, selects one measurement based on the following measurement selection criteria:

Assume that each interval $\mathcal{H}_m$ is further divided into two equally probable intervals by the boundary value $h'_m = F_H^{-1}\left(\frac{F_H(H'_{(m-1)})+F_H(H'_m)}{2}\right)$, for $\forall m \in [1{:}J]$[2]. If $|h| \in \mathcal{H}_m$ and $b_m = 0$, then LTSM selects one measurement of parameter ς, which is the parameter that minimizes the following distance metric:

$$\min_{b_\varsigma \neq 0} \left||h| - h'_\varsigma\right|. \tag{5.23}$$

[2]If the channel follows a discrete fading distribution, we find h'_m by taking the mean value of all elements of channel set $\mathcal{H}_m$.

When the hard matching condition is not satisfied, the LTSM considers a soft matching condition for selecting measurements; that is, among all parameter types of the measurements in the TB, it selects a measurement of the parameter whose corresponding interval of channel states has the value h'_{ς} closest to the channel state magnitude $|h|$. If two distinct ς values satisfy the solution of Eqn. (5.23), then LTSM chooses the smallest value of ς. LTSM allocates the power as in Eqn. (5.21), and transmits the selected measurement, leading to distortion in Eqn. (5.22). Note that the optimal Lagrange multiplier μ is chosen such that the average power constraint is satisfied. At the end of $\bar{d}$ channel accesses, the sensor will have transmitted all the measurements in the TB, albeit some might have been allocated zero power as a result of the water-filling algorithm.

5.5 Distortion Lower Bounds

We characterize two lower bounds on the MSE distortion, namely, the TLB and the LLB. While the TLB is the theoretical performance bound derived without any delay or complexity constraints on the transmission, the LLB is a performance lower bound only for LT strategies. We also prove that the proposed LT strategies meet the TLB under infinite delay and certain matching conditions between the channel states and parameter variances.

5.5.1 The Theoretical Lower Bound (TLB)

Shannon's source-channel separation theorem states that the optimal end-to-end distortion is achieved by concatenating the optimal source and channel codes when there is no delay or complexity constraints, and the source and channel distributions are ergodic [94]. When we remove the delay and linear encoding constraints in our system model, then the sensor can transmit to the CC at the ergodic capacity, $\bar{C}_e$, of the underlying fading channel, while the minimum distortion, $\bar{D}_e$, is found by evaluating the distortion-rate function for a composite Gaussian source model at the ergodic capacity.

Since the channel state is known by both the transmitter and receiver, the ergodic capacity, in terms of the optimal power allocation scheme $P_e^*(h)$, is given by:

$$\bar{C}_e \triangleq \mathrm{E}_H \left[\frac{1}{2} \log \left(1 + |h|^2 P_e^*(h) \right) \right], \tag{5.24}$$

where $P_e^*(h)$ is found by the water-filling algorithm as:

$$P_e^*(h) = \left[\alpha^* - \frac{1}{|h|^2}\right]^+, \tag{5.25}$$

where α^* is chosen to satisfy $\bar{P}_e \triangleq \mathrm{E}_H\left[P_e^*(h)\right] = P$.

From Eqn. (6.1.21) of [129], the distortion-rate function of a composite Gaussian source with m components, $\mathcal{N}(0, \sigma_m^2)$, each of which is observed with probability $p_M(m)$ for $m \in [1{:}J]$, is defined as:

$$\bar{D}_e \triangleq \mathrm{E}_M\left[\sigma_m^2 2^{-2R_e^*(\sigma_m)}\right], \tag{5.26}$$

where the optimal rate allocated to source m, $R_e^*(\sigma_m)$, and the corresponding distortion, $D_e^*(\sigma_m)$, are given by:

$$R_e^*(\sigma_m) = \frac{1}{2}\left[\log\left(\frac{\sigma_m^2}{\beta^*}\right)\right]^+, \tag{5.27}$$

$$D_e^*(\sigma_m) = \min\left(\beta^*, \sigma_m^2\right), \tag{5.28}$$

where β^* is chosen such that $\bar{R}_e \triangleq \mathrm{E}_M\left[R_e^*(\sigma_m)\right] = \bar{C}_e$.

Hence, the optimal distortion is found as $\bar{D}_e = \mathrm{E}_M\left[D_e^*(\sigma_m)\right]$, which is the TLB on the achievable MSE distortion by any transmission strategy. Note that we have removed both the delay constraint and the linearity requirement on the encoder and decoder.

Asymptotic Optimality of LT

In general, the TLB cannot be achieved by LT strategies even if the delay constraint is removed. However, it can be shown that LTHM and LTSM meet this lower bound when the delay constraint is removed under certain matching conditions between the channel states and the parameter variances.

Assume that the channel follows a discrete fading distribution, where the channel state h can take one of the J values $\hat{h}_m$ with probability $p_H(\hat{h}_m)$ for $m \in [1{:}J]$. The discrete values are ordered as $|\hat{h}_1| > |\hat{h}_2| > \cdots > |\hat{h}_J|$. The next theorem states the necessary conditions in this discrete channel model under which LTHM and LTSM achieve the optimal distortion

performance when the delay constraint is removed.

Theorem 5.1. *For the discrete AWGN fading channel model, if the parameter variances and the discrete channel states satisfy* $\frac{\sigma_1}{|\hat{h}_1|} = \cdots = \frac{\sigma_J}{|\hat{h}_J|}$, *and* $p_M(m) = p_H(\hat{h}_m)$, *for* $\forall m \in [1{:}J]$, *then the TLB is achieved by LTHM and LTSM when the delay constraint is removed, i.e.,* $d \to \infty$.

Proof. The proof can be found in Appendix. □

5.5.2 The Linear Transmission Lower Bound (LLB)

We next derive a lower bound on the achievable MSE distortion as a function of the delay and power constraints for any LT strategy. In order to derive this lower bound, we relax the assumption on the causal knowledge of the measurements and channel states, and instead assume that the sensor has the offline (non-causal) knowledge of a certain number of future measurements and channel states. Accordingly, we assume that at any TS the sensor non-causally knows the length-$\bar{u}$ measurement vector, i.e., $\mathbf{s} = [s_1, \ldots, s_{\bar{u}}]$, taken over the next $\bar{u}$ TSs. Observe that, for a delay constraint d, each measurement of $\mathbf{s}$ can only be transmitted over the following d channel states observed after it is taken, thus the transmission of the vector $\mathbf{s}$ spans the following $\bar{c} = (d + \bar{u} - 1)$ channel states observed after the first measurement s_1 is taken. We further assume that the sensor non-causally knows the length-$\bar{c}$ channel vector $\mathbf{h} = [h_1, \ldots, h_{\bar{c}}]$. Henceforth, the problem is reduced to optimally transmitting $\bar{u}$ measurements over $\bar{c}$ parallel channels, which is attained by using the optimal LT scheme presented in Section 5.3.1. Accordingly, we first reorder $\mathbf{s}$ to get $\bar{\mathbf{s}} = [s_{(1)}, \ldots, s_{(\bar{u})}]$, where the variances of the ordered measurements satisfy $\sigma^2_{m_{(1)}} \leq \sigma^2_{m_{(2)}} \leq \cdots \leq \sigma^2_{m_{(\bar{u})}}$, and reorder $\mathbf{h}$ to get $\bar{\mathbf{h}} = \left[h_{(1)}, \ldots, h_{(\bar{c})}\right]$, such that the ordered fading states satisfy $|h_{(1)}| \leq |h_{(2)}| \leq \cdots \leq |h_{(\bar{c})}|$. Then, the $\bar{c} \times \bar{u}$ optimal linear encoding matrix $\mathbf{F}^*_{\mathbf{h},\mathbf{m}}$ consists of a $\bar{u} \times \bar{u}$ size diagonal partition with entries $\left[f_{(1)}(h_{(1+\bar{e})}, m_{(1)}), \ldots, f_{(\bar{u})}(h_{(\bar{u}+\bar{e})}, m_{(\bar{u})})\right]$, and a $\bar{e} \times \bar{u}$ size partition with zero entries, where $\bar{e} = \bar{c} - \bar{u}$, and it maps $\bar{u}$ ordered measurements to the $\bar{u}$ channels with the largest gains. The optimal entries of $\mathbf{F}^*_{\mathbf{h},\mathbf{m}}$ are found as the solution of the following convex optimization problem:

$$\begin{aligned} \bar{D}^*(d, \bar{u}, P) \triangleq \underset{f_{(t)}(h_{(t+\bar{e})}, m_{(t)})}{\text{minimize}} \; & \mathrm{E}_{M_{(t)}, H_{(t+\bar{e})}} \left[\frac{1}{\bar{u}} \sum_{t=1}^{\bar{u}} \frac{\sigma^2_{m_{(t)}}}{|h_{(t+\bar{e})}|^2 f_{(t)}(h_{(t+\bar{e})}, m_{(t)})^2 \sigma^2_{m_{(t)}} + 1} \right] \\ \text{subject to } \bar{P} \triangleq & \; \mathrm{E}_{M_{(t)}, H_{(t+\bar{e})}} \left[\frac{1}{\bar{u}} \sum_{t=1}^{\bar{u}} f_{(t)}(h_{(t+\bar{e})}, m_{(t)})^2 \sigma^2_{m_{(t)}} \right] \leq P, \end{aligned} \tag{5.29}$$

where the expectation is taken over $M_{(t)}$ and $H_{(t+\bar{e})}$ for $t \in [1{:}\bar{u}]$. The t-th and $(t+\bar{e})$-th order

statistics $p_{M_{(t)}}(m)$ and $p_{H_{(t+\bar{e})}}(h)$, are given by Lemma 5.2. The optimal linear encoding matrix with diagonal entries is found as:

$$f^*_{(t)}(h_{(t+\bar{e})}, m_{(t)}) = \sqrt{\left[\frac{\zeta^*}{|h_{(t+\bar{e})}|\sigma_{m_{(t)}}} - \frac{1}{|h_{(t+\bar{e})}|^2\sigma^2_{m_{(t)}}}\right]^+}, \tag{5.30}$$

where ζ^* is the optimal Lagrange multiplier, such that $\bar{P} = P$ in (5.29).

Assuming non-causal knowledge of $\bar{u}$ measurements and $\bar{c}$ channel states under the delay constraint d and the average power constraint P, we obtain the optimal distortion $\bar{D}^*(d, \bar{u}, P)$ for any LT strategy. Then, the LLB is derived by finding the $\bar{u}$ value, which maximizes $\bar{D}^*(d, \bar{u}, P)$:

$$\bar{D}_l(d, P) \triangleq \max_{\bar{u}} \bar{D}^*(d, \bar{u}, P). \tag{5.31}$$

Note that we have relaxed the constraint for the causal knowledge of measurements and channel states both at the encoder and decoder. The numerical comparisons of the LLB with the proposed schemes will be presented in Section 5.8.

5.6 No CSI at the Encoder

In this section, we assume that the CSI is known only at the decoder. We derive the optimal LT strategy under a strict delay constraint $(d = 1)$, as well as the TLB on the achievable MSE distortion. Additionally, for the multiple measurements-parallel channels scenario studied in Section 5.3.1, we show that if the CSI is available only at the receiver, any LT scheme that is limited to a one-to-one linear mapping from the measurements to the channel input is suboptimal in general. The optimal LT strategy is elusive and it will be a non-trivial function of the source variances and the channel distribution.

5.6.1 Strict Delay Constraint

Under a strict delay constraint, the most recent measurement is transmitted at each TS. By applying Lemma 5.1 to this scenario, we can similarly show that there is no loss of optimality by considering time-invariant encoding functions, i.e., $f_i(m) = f(m), \forall i$. Hence, the encoding function $f(m)$ is a scalar and time-invariant. The decoding function $g(h, m)$ that minimizes the MSE is the linear MMSE estimator [130], and is also a scalar and time-invariant. Then,

the MSE distortion, $\bar{D} = \mathrm{E}_{M,H,S,Z}[|S - \hat{S}|^2]$, and the average power, $\bar{P} = \mathrm{E}_{M,S}[|X|^2]$, can be written explicitly as:

$$\bar{D} = \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} \frac{\sigma_m^2}{|h|^2 f(m)^2 \sigma_m^2 + 1} p_H(h) \mathrm{d}h, \tag{5.32}$$

$$\bar{P} = \sum_{m=1}^{J} p_M(m) f(m)^2 \sigma_m^2, \tag{5.33}$$

where $P(m) \triangleq f(m)^2 \sigma_m^2$. The optimal linear encoding function, $f^*(m)$, is found as the solution to the convex optimization problem $\bar{D}^* \triangleq \underset{f(m)}{\text{minimize}}\, \bar{D}$, subject to the average power constraint $\bar{P} \leq P$, which can be written explicitly as follows:

$$\begin{aligned} \bar{D}^* \triangleq \underset{f(m)}{\text{minimize}} \; & \sum_{m=1}^{J} p_M(m) \int_{\mathbb{R}} \frac{\sigma_m^2}{|h|^2 f(m)^2 \sigma_m^2 + 1} p_H(h) \mathrm{d}h \\ \text{subject to} \; & \sum_{m=1}^{J} p_M(m) f(m)^2 \sigma_m^2 \leq P. \end{aligned} \tag{5.34}$$

From the KKT conditions [119], we have:

$$f^*(m) = \sqrt{\frac{\left[\Psi^{-1}\left(\frac{\lambda^*}{\sigma_m^2}\right)\right]^+}{\sigma_m^2}}, \tag{5.35}$$

where $\Psi^{-1} : \mathbb{R} \to \mathbb{R}$ is the inverse of the function $\Psi : \mathbb{R} \to \mathbb{R}$, that is defined as, $\Psi(P(m)) \triangleq \int_{\mathbb{R}} \frac{|h|^2}{(|h|^2 P(m)+1)^2} p_H(h) \mathrm{d}h$. The optimal Lagrange multiplier λ^* is chosen such that $\bar{P} = P$ in (5.34).

5.6.2 Multiple Measurements and Parallel Channels

Next we consider the multiple measurements-parallel channels scenario studied in Section 5.3.1, under the strict delay constraint and the assumption that the CSI is known only at the decoder, and $J > 1$. In such a scenario, the optimal LT scheme of [95], in which the ordered measurements are mapped one-to-one to ordered channel states, cannot be used directly. This is because, even though the encoder knows the N measurements, it does not know any of the channel states, and hence; cannot order them. For the special case where N measurements are observed from a single Gaussian source ($J = 1$), in [97] the authors show that the optimal

performance is achieved by transmitting one measurement over each channel. When $J = 1$, since N measurements all have the same variance, all orderings are equivalent, and the optimal LT performance is achieved by an LT scheme that uses only a one-to-one mapping between measurements and channels. However, this is not the case in general when $J > 1$. Since N measurements follow a composite Gaussian source model, the encoder can have measurements with different variances; and hence, we can exploit the diversity of the fading channel by transmitting a single measurement over multiple channels, instead of transmitting each measurement only once. Depending on the source variances, the former may surpass the best LT performance achieved by using only a one-to-one linear mapping. This is shown in the following lemma by considering a particular example.

Lemma 5.3. *Consider the LT of N measurements of a composite Gaussian source with $J > 1$ components over N parallel AWGN fading channels. If the CSI is known only by the decoder, then the LT scheme that uses a one-to-one linear mapping between measurements and channels is suboptimal in general.*

Proof. The proof can be found in Appendix. □

5.6.3 The Theoretical Lower Bound (TLB)

Similarly to Section 5.5.1, we derive the TLB on the achievable MSE distortion by using Shannon's source-channel separation theorem. If the CSI is available only at the decoder and the average power constraint is P, then the ergodic capacity is given by:

$$\bar{C}_e \triangleq \mathrm{E}_H \left[\frac{1}{2} \log \left(1 + |h|^2 P \right) \right]. \tag{5.36}$$

The distortion-rate function of a composite Gaussian source is defined as in Eqn. (5.26) of Section 5.5.1, which leads to the optimal rate allocated to source m, $R_e^*(\sigma_m)$, as in Eqn. (5.27) and the corresponding distortion, $D_e^*(\sigma_m)$, as in Eqn. (5.28), respectively. The Lagrangian multiplier β^* for this case is chosen such that $\mathrm{E}_M \left[R_e^*(\sigma_m) \right]$ is equal to the ergodic capacity $\bar{C}_e$ in (5.36). Then the TLB on the achievable MSE distortion by any strategy when the encoder does not have the CSI is given by $\bar{D}_e = \mathrm{E}_M \left[D_e^*(\sigma_m) \right]$.

5.7 Multiple Sensors and Parallel Channels

Following the system model introduced in Section 5.2, here we consider a particular symmetric scenario with multiple sensors and parallel channels. In this symmetric scenario, there are N sensors, each capable of measuring J distinct system parameters locally, and N orthogonal fading channels for the transmission of the requested measurements. The jth system parameter is modelled as a zero-mean Gaussian r.v. with variance σ_j^2, i.e., $\sim \mathcal{N}(0, \sigma_j^2)$, for $j \in [1{:}J]$. These system parameters are independent from each other, and their realizations are i.i.d. over time and sensors. In order to monitor the network operation, the CC requests the measurement of one system parameter from each sensor at each TS. The index of the requested system parameter at each TS is a r.v. denoted by $M \in [1{:}J]$, with distribution $p_M(m)$, which is also i.i.d. over time and sensors. Based on these requests, each sensor takes one measurement of the requested parameter m at each TS. As in Section 5.2, the encoder and the decoder possess the exact knowledge of the index of the requested system parameter of each sensor; and thereby, the model is that of a composite source introduced in Chapter 6 of [129].

The maximum delay in transmitting a measurement to the CC is $d \in \mathbb{Z}^+$, which is same for all the sensors and parameters. There are N orthogonal fading channels available. Let $\mathbf{h} = [h_1, \ldots, h_N]$ denote the channel vector at any TS, whose entries are i.i.d. with probability distribution $p_H(h)$. The channels have AWGN with zero-mean and unit-variance. In this symmetric system model, we assume that the statistics of the measured parameters, σ_m^2, the measurement requests, $p_M(m)$, and the channels, $p_H(h)$, are all i.i.d. over sensors. We assume that both the encoder and decoder know all the past and current channel states and the indices of requested parameters, as well as the statistics of the measured parameters, the parameter requests, and the channels.

Scheduling of channels to sensors is done in advance; i.e., it cannot depend on the realizations of the measurements or the channel states. At each scheduled TS for transmission, a sensor transmits all its samples that have been taken within the last d TSs. We are interested only in LT policies in which encoding and decoding functions are restricted to be linear functions of the sensor measurements. We consider an average power constraint of P at each sensor. The goal is to have an estimate of each requested measurement at the CC within the delay constraint. The performance measure is the total MSE distortion for the requested measurements.

5.7.1 Scheduling Algorithm

In this scenario, we consider a round-robin scheduling algorithm. Given a delay constraint d, assuming N is an integer multiple of d, we group sensors into N/d groups. Each group

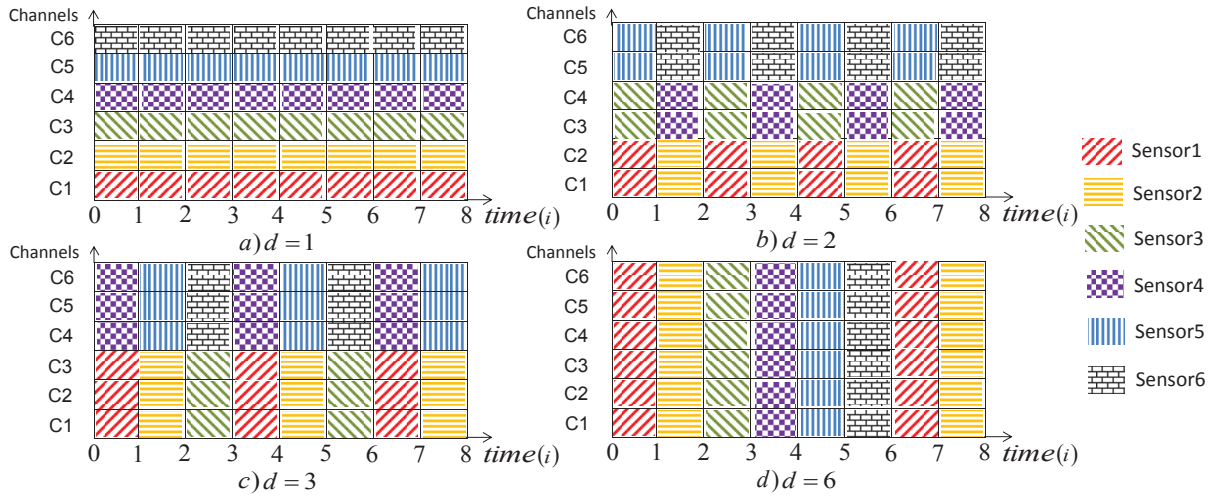


Figure 5.4: Illustration of the round-robin scheduling policy for different delay constraints.

is assigned d orthogonal channels. Each sensor transmits once every d TSs, using all the d channels assigned to its own group, and transmits all its measurements from the last d TSs. This round-robin scheduling of channels provides additional degrees-of-freedom to the sensors to match their measurements to a larger number of channels at each transmission round. Fig. 5.4 depicts an example of how $N = 6$ channels are scheduled to $N = 6$ sensors for different delay constraints $d = \{1, 2, 3, 6\}$. Notice that for $d = 1$, one channel is assigned to each sensor for all the TSs; hence, the sensor has no control on matching the measurements to the channel states. On the other hand, for $d > 1$, at each transmission round, a sensor can reorder its measurements to match them to the available channels in an optimal manner, or transmit their linear combinations.

In this symmetric model, the system performance can be analyzed for a single sensor. Due to symmetry, results will apply to all the sensors. For a delay constraint d, the sensor collects d measurements to be transmitted over d orthogonal fading AWGN channels. The optimal LT strategies under strict and general delay constraints, and the TLB can be obtained by using the solutions proposed in Section 5.3, Section 5.3.1 and Section 5.5.1, respectively.

5.8 Numerical Results and Observations

Here we provide numerical results to compare the performances of LTHM and LTSM with the lower bounds, and to analyze the impact of the delay and power constraints on the performance. In our simulations, we consider $J = 4$ Gaussian parameters with variances $\{10, 5, 1, 0.5\}$, which are requested with probabilities $\{0.1, 0.3, 0.4, 0.2\}$, respectively. For a continuous fading channel, we consider Rayleigh distribution with mean value $3\sqrt{\frac{\pi}{2}}$, and for a discrete fading channel, we consider four states $\{\sqrt{10}, \sqrt{5}, 1, \sqrt{0.5}\}$, which are observed with probabilities

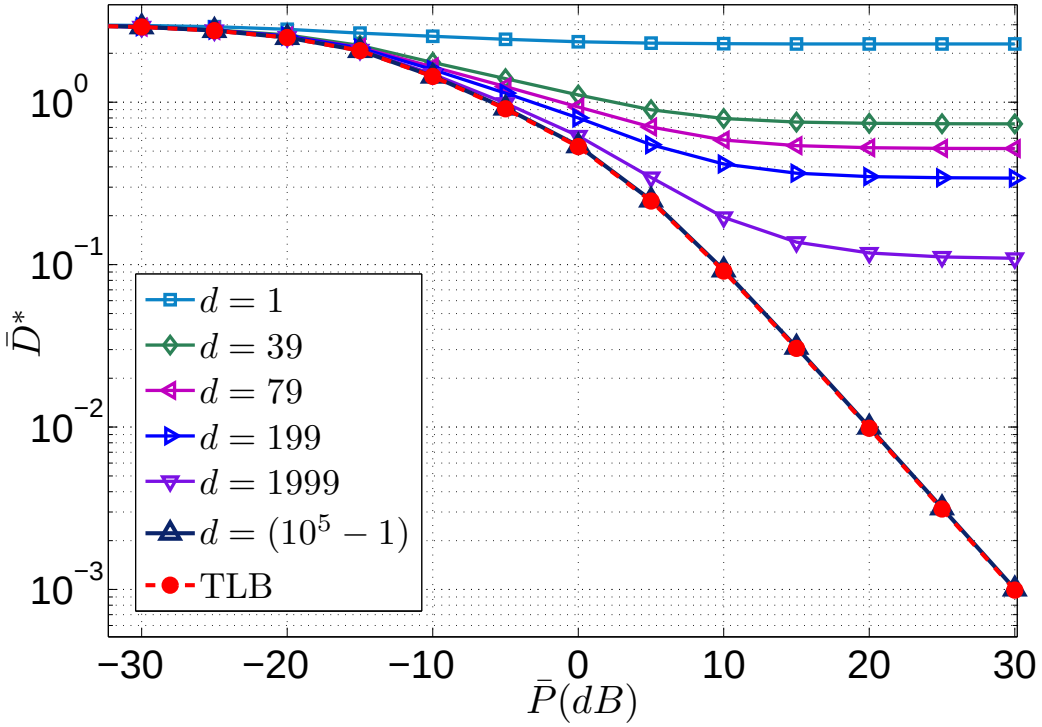


Figure 5.5: Achievable MSE distortion with LTHM with respect to average power for different delay constraints in the discrete fading channel model.

$\{0.1, 0.3, 0.4, 0.2\}$, respectively.

We illustrate the achievable MSE distortion versus average power under various delay constraints with LTHM in the discrete channel setting in Fig. 5.5. We observe that the MSE distortion diminishes as the delay constraint is relaxed. This is because a relaxed delay constraint provides a larger number of measurements in the TB; and hence, more flexibility for the sensor in selecting the appropriate measurement for each TS. We note that this statement does not hold when $J = 1$, in which case increasing the block length does not provide any improvement [95]. As it can be seen in Fig. 5.5, the MSE distortion converges to a fixed value as the average power value increases. This is due to the additional distortion brought in by the untransmitted measurements in the TB. The average number of untransmitted measurements and their effect on the MSE distortion decreases as the delay constraint is relaxed, since having a larger number of measurements in the TB increases the probability of finding a measurement that satisfies the hard matching condition. In particular, when the delay constraint is removed, as seen in Fig. 5.5, LTHM achieves the TLB, and becomes the optimal LT scheme, since the source-channel matching conditions in Theorem 5.1 are satisfied for the setup considered here.

In Fig. 5.6, we illustrate the achievable MSE distortion with LTSM with respect to average power under various delay constraints in the continuous channel model. Similarly to LTHM, the MSE distortion diminishes as the delay constraint increases. On the other hand, as opposed

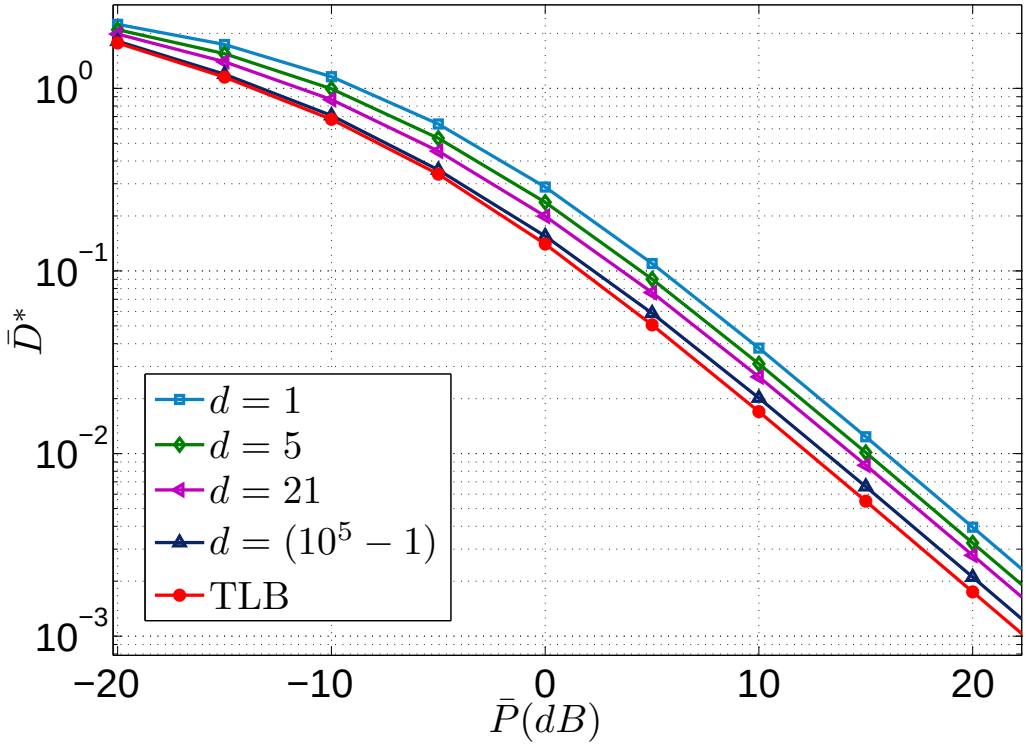


Figure 5.6: Achievable MSE distortion with LTSM with respect to average power for various delay constraints in the continuous fading channel model.

to LTHM, the MSE distortion achieved by LTSM decreases monotonically with the average power as illustrated in Fig. 5.6. This is because the performance of LTSM does not suffer from a fixed distortion component due to the untransmitted measurements. In addition, LTSM also approaches the TLB as the delay constraint is relaxed. Although we do not expect the LTSM to meet the TLB in this setting since the matching conditions of Theorem 5.1 do not hold, we observe in Fig. 5.6 that it is very close to the TLB.

Next, we compare the performances of LTHM and LTSM with each other and with the TLB and the LLB. Fig. 5.7 shows the achievable MSE distortion of LTHM, LTSM, the LLB and the TLB with respect to delay constraint in the continuous fading channel model for an average power constraint $\bar{P} = 10$ dB. As seen in the figure, the performance of the TLB is constant since it is derived by completely removing the delay and complexity constraints. On the other hand, the LLB decays slowly as the delay constraint increases. As expected, the MSE distortion of LTHM and LTSM decrease as the delay constraint increases. We can see that LTSM meets the LLB under the strict delay constraint. As expected, LTSM always outperforms LTHM, while the gap between the two schemes decreases with the increasing delay constraint. The gap between the TLB and two schemes also decreases with the increasing delay constraint even though we do not expect either of the schemes converge to the TLB in this setting since the matching conditions of Theorem 5.1 do not hold.

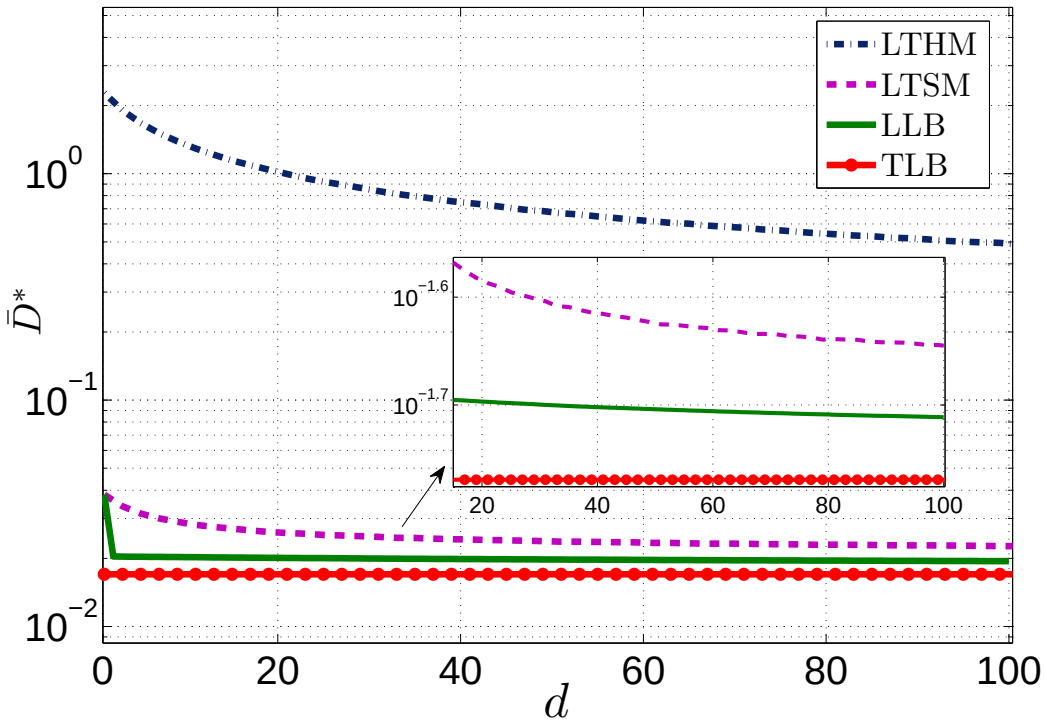


Figure 5.7: MSE distortion versus delay constraint, d, in the continuous fading channel model for an average power constraint $\bar{P} = 10$ dB.

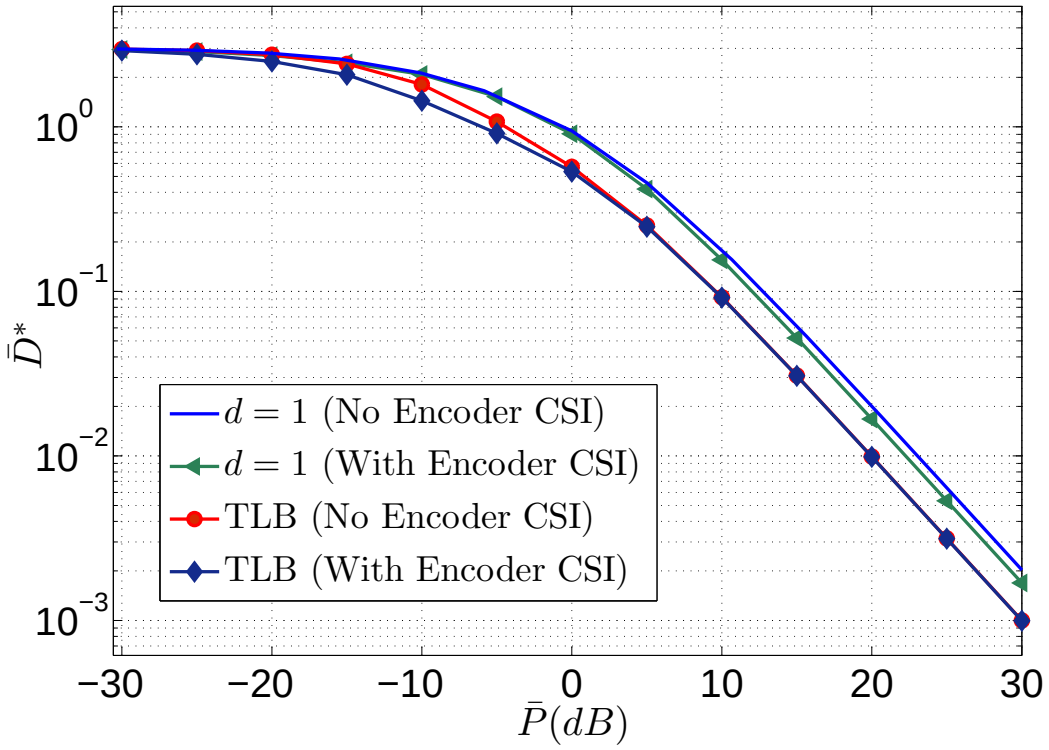


Figure 5.8: The achievable MSE distortion of LT and the TLB with respect to average power in the discrete fading channel model with and without encoder CSI.

Finally, in Fig. 5.8, we illustrate the achievable MSE distortion of LT and the TLB with respect to average power in the discrete channel model for the scenarios in which the CSI is known only by the decoder, and by both the encoder and decoder. The MSE distortion of LT under strict delay constraint of $d = 1$ for both scenarios diminishes as the average power increases. However, there is a constant gap between the optimal performances achieved with and without encoder CSI at higher $\bar{P}$ values. On the other hand, the TLB for both scenarios meet as the average power increases since the gain from the optimal power allocation over different channel states disappears in the high power regime.

5.9 Conclusions

In this chapter, we have studied the delay-constrained LT of composite Gaussian measurements from a sensor to a CC over an AWGN fading channel. We have considered a wireless sensor that can collect measurements from J distinct Gaussian parameters. The CC asks for a measurement of a particular parameter from the sensor with a certain probability at each TS. In this framework, we have presented the optimal LT strategy under a strict delay constraint, and have given a graphical interpretation for the optimal power allocation scheme and the corresponding distortion value. Then, we have proposed two LT strategies, called LTHM and LTSM, under general delay constraints, and have provided numerical results to investigate the impact of the delay and average power constraints on the performance. We have seen that, if the number of parameters, J, is more than one, the MSE distortion decreases as the delay constraint is relaxed. We have also derived lower bounds on the achievable MSE distortion for generic and LT strategies. While LTSM outperforms LTHM at all delay constraints, we have shown analytically that both strategies meet the lower bound when the delay constraint is removed, under certain matching conditions between the parameter and the channel statistics.

We have also studied the scenario in which the CSI is known only by the decoder. We have presented the optimal LT strategy under a strict delay constraint. We have derived a TLB on the achievable MSE distortion by relaxing the delay constraint and the linearity requirement. We have also considered the multiple measurements-parallel channels scenario under a strict delay constraint, and have shown that the optimal LT performance cannot be achieved by using only a one-to-one linear mapping between measurements and channels, as opposed to the results derived in [95] and [97]. The design of the optimal LT strategy for the multiple measurements-parallel channels scenario for arbitrary delay constraints is elusive, and is left as future work.

5.10 Appendix

5.11 Proof of Theorem 1

Given a delay constraint $d = 2\bar{d}-1$, let the r.v. $\bar{Z}_m$, $m \in [1{:}J]$, denote the total number of measurements of parameter m among $\bar{d}$ measurements loaded into the TB. $\bar{Z}_m$ follows a Binomial distribution with parameters $\bar{d}$ and $p_M(m)$. Hence, the probability of having $\bar{k}$ measurements of parameter m in the TB is given by:

$$\begin{aligned} p_{\bar{Z}_m}(\bar{k}) &= \Pr\{\bar{Z}_m = \bar{k}\}, \\ &= \binom{\bar{d}}{\bar{k}} p_M(m)^{\bar{k}}(1-p_M(m))^{\bar{d}-\bar{k}}. \end{aligned} \tag{5.37}$$

Similarly, considering the discrete fading model presented in Section 5.5.1, let the r.v. $\hat{Z}_m$, $m \in [1{:}J]$, denote the total number of channels with state $\hat{h}_m$, after $\bar{d}$ channel accesses. $\hat{Z}_m$ also follows a Binomial distribution with parameters $\bar{d}$ and $p_H(\hat{h}_m)$. Hence, the probability of observing $\hat{k}$ channels with state $\hat{h}_m$ is given by:

$$\begin{aligned} p_{\hat{Z}_m}(\hat{k}) &= \Pr\{\hat{Z}_m = \hat{k}\}, \\ &= \binom{\bar{d}}{\hat{k}} p_H(\hat{h}_m)^{\hat{k}}(1-p_H(\hat{h}_m))^{\bar{d}-\hat{k}}. \end{aligned} \tag{5.38}$$

Observe that after $\bar{d}$ channel accesses, the number of transmitted measurements selected from the TB with LTHM is given by $\min\{\bar{Z}_m, \hat{Z}_m\}$. On the other hand, the number of untransmitted measurements remained in the TB is given by $[\bar{Z}_m - \hat{Z}_m]^+$. Then, the average power, $\bar{P}_\infty$, and the achievable MSE distortion, $\bar{D}_\infty$, of LTHM when $\bar{d} \to \infty$ are given by:

$$\bar{P}_\infty \triangleq \lim_{\bar{d}\to\infty} \frac{1}{\bar{d}} \sum_{m=1}^{J} \mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\min\left\{\bar{Z}_m, \hat{Z}_m\right\}\right] P(\hat{h}_m, m), \tag{5.39}$$

$$\bar{D}_\infty \triangleq \lim_{\bar{d}\to\infty} \frac{1}{\bar{d}} \sum_{m=1}^{J} \left\{\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[[\bar{Z}_m - \hat{Z}_m]^+\right]\sigma_m^2 + \mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\min\left\{\bar{Z}_m, \hat{Z}_m\right\}\right] D(\hat{h}_m, m)\right\}, \tag{5.40}$$

where the allocated power $P(\hat{h}_m, m)$ and the distortion $D(\hat{h}_m, m)$ are chosen as in Eqn. (5.21) and Eqn. (5.22), respectively:

$$P(\hat{h}_m, m) = \left[\frac{\mu\sigma_m}{|\hat{h}_m|} - \frac{1}{|\hat{h}_m|^2}\right]^+, \tag{5.41}$$

$$D(\hat{h}_m, m) = \frac{\sigma_m^2}{|\hat{h}_m|^2\left[\frac{\mu\sigma_m}{|\hat{h}_m|} - \frac{1}{|\hat{h}_m|^2}\right]^+ + 1}. \tag{5.42}$$

In the rest of the proof, we use $p(m)$ to refer to the condition of Theorem 5.1, i.e., $p_M(m) = p_H(\hat{h}_m) = p(m)$, $\forall m$. Under this condition, the expected value and variance of $\bar{Z}_m$ and $\hat{Z}_m$ can be found respectively as:

$$\mathrm{E}[\bar{Z}_m] = \mathrm{E}[\hat{Z}_m] = \bar{d} \cdot p(m), \tag{5.43}$$

$$\mathrm{Var}[\bar{Z}_m] = \mathrm{Var}[\hat{Z}_m] = \sigma_{Z_m}^2 = \bar{d} \cdot p(m) \cdot (1 - p(m)). \tag{5.44}$$

Let $\epsilon > 0$ be any positive number. Then, the Chebyshev's inequality leads to the following inequalities,

$$\Pr\{|\bar{Z}_m - \bar{d} \cdot p(m)| \geq \epsilon \cdot \sigma_{Z_m}\} \leq \frac{1}{\epsilon^2},$$
$$\Pr\{|\hat{Z}_m - \bar{d} \cdot p(m)| \geq \epsilon \cdot \sigma_{Z_m}\} \leq \frac{1}{\epsilon^2}.$$

We define the interval $\mathcal{I}$ on the real line as,

$$\mathcal{I} = [\bar{d} \cdot p(m) - \epsilon \cdot \sigma_{Z_m}, \bar{d} \cdot p(m) + \epsilon \cdot \sigma_{Z_m}].$$

Next, we compute (5.39) and (5.40) by finding upper and lower bounds on the expectation terms under the matching condition. Observe that,

$$\lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\min\left\{\bar{Z}_m,\hat{Z}_m\right\}\right], \tag{5.45}$$

$$\leq \lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\bar{Z}_m\right],$$

$$= p(m). \tag{5.46}$$

We can also lower bound this term as,

$$\lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\min\left\{\bar{Z}_m,\hat{Z}_m\right\}\right],$$

$$\geq \lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[\min\left\{\bar{Z}_m,\hat{Z}_m\right\}\Big|_{\substack{\bar{Z}_m\in\mathcal{I},\\ \hat{Z}_m\in\mathcal{I}}}\right]\Pr\left\{\bar{Z}_m\in\mathcal{I},\hat{Z}_m\in\mathcal{I}\right\}, \tag{5.47}$$

$$\geq \lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\left(\bar{d}p(m)-\epsilon\sigma_{Z_m}\right)\left(1-\frac{1}{\epsilon^2}\right)^2, \tag{5.48}$$

$$= \lim_{\bar{d}\to\infty}\left(p(m)-\frac{\sqrt{p(m)(1-p(m))}}{\bar{d}^{\frac{1}{6}}}\right)\left(1-\frac{1}{\bar{d}^{\frac{2}{3}}}\right)^2,$$

$$= p(m), \tag{5.49}$$

where (5.47) follows from the law of total expectation; (5.48) follows from the definition of $\mathcal{I}$, and the Chebyshev's inequality; and (5.49) is obtained by setting $\epsilon=\bar{d}^{\frac{1}{3}}$. Since the upper and lower bounds in (5.46) and (5.49) are equal, we have shown that (5.45) converges to $p(m)$ as $\bar{d}\to\infty$.

Similarly,

$$\lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[[\bar{Z}_m-\hat{Z}_m]^+\right], \tag{5.50}$$

$$= \lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\Bigg\{\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[[\bar{Z}_m-\hat{Z}_m]^+\Big|_{\substack{\bar{Z}_m\in\mathcal{I},\\ \hat{Z}_m\in\mathcal{I}}}\right]\Pr\left\{\bar{Z}_m\in\mathcal{I},\hat{Z}_m\in\mathcal{I}\right\}$$

$$+\mathrm{E}_{\bar{Z}_m,\hat{Z}_m}\left[[\bar{Z}_m-\hat{Z}_m]^+\Big|_{\substack{\bar{Z}_m\notin\mathcal{I}\\ \text{or}\\ \hat{Z}_m\notin\mathcal{I}}}\right]\Pr\{\bar{Z}_m\notin\mathcal{I}\text{ or }\hat{Z}_m\notin\mathcal{I}\}\Bigg\}, \tag{5.51}$$

$$\leq \lim_{\bar{d}\to\infty}\frac{1}{\bar{d}}\left\{2\epsilon\sigma_{Z_m}+\left(\frac{2}{\epsilon^2}+\frac{1}{\epsilon^4}\right)\bar{d}\right\}, \tag{5.52}$$

$$= \lim_{\bar{d}\to\infty}\left\{\left(\frac{2\sqrt{p(m)(1-p(m))}}{\bar{d}^{\frac{1}{6}}}\right)+\left(\frac{2}{\bar{d}^{\frac{2}{3}}}+\frac{1}{\bar{d}^{\frac{4}{3}}}\right)\right\},$$

$$= 0, \tag{5.53}$$

where (5.51) follows from the law of total expectation; (5.52) follows from the from the definition of $\mathcal{I}$, and the Chebyshev's inequality; and (5.53) is obtained by setting $\epsilon = \bar{d}^{\frac{1}{3}}$. This proves that (5.50) indeed converges to zero as $\bar{d} \to \infty$. This also implies that as $\bar{d} \to \infty$, all selected measurements by the LTSM strategy satisfy the hard matching condition. Hence, LTSM and LTHM are equivalent in the asymptotic of $\bar{d} \to \infty$ under the matching condition of Theorem 5.1.

Finally, we can rewrite $\bar{P}_\infty$ and $\bar{D}_\infty$ for both LTHM and LTSM as:

$$\bar{P}_\infty = \sum_{m=1}^{J} \left[\mu^* q - \frac{1}{|\hat{h}_m|^2} \right]^+ p(m), \tag{5.54}$$

$$\bar{D}_\infty = \sum_{m=1}^{J} \left[\frac{\sigma_m^2}{|\hat{h}_m|^2 \left[\mu^* q - \frac{1}{|\hat{h}_m|^2} \right]^+ + 1} \right] p(m), \tag{5.55}$$

where we use $q \triangleq \frac{\sigma_m}{|\hat{h}_m|}$, $\forall m$, from Theorem 5.1, and μ^* is chosen to satisfy $\bar{P}_\infty = P$.

Next, we show that $(\bar{P}_\infty, \bar{D}_\infty)$ pair above, obtained under the conditions of Theorem 5.1, achieve the TLB pair $(\bar{P}_e, \bar{D}_e)$, derived in Section 5.5.1. First, under the matching condition, observe that $\mu^* q = \alpha^*$, and thus, $\bar{P}_\infty = \bar{P}_e = P$. Moreover, under the matching condition, $\bar{R}_e = \bar{C}_e$ in TLB implies $\alpha^* = \frac{q^2}{\beta^*}$. Combining the two equalities, we obtain $\mu^* = \frac{q}{\beta^*}$. Substituting this into Eqn. (5.26) together with the matching condition, we can show that $\bar{D}_e = \sum_{m=1}^{J} \min\left(\frac{q}{\mu^*}, \sigma_m^2\right) p(m) = \bar{D}_\infty$, which concludes the proof of Theorem 5.1.

5.12 Proof of Lemma 3

In order to prove Lemma 5.3, we construct a counter-example. We argue that the achievable MSE distortion of a particular LT scheme that is not constrained to use only a one-to-one mapping between measurements and channels can be smaller than the minimum achievable MSE distortion of all possible LT schemes that use only a one-to-one mapping, i.e., a diagonal encoding matrix. Suppose we have $J = 2$ zero-mean Gaussian parameters with variances σ_1^2 and σ_2^2, which are requested with probabilities $p_M(1) = p_1$ and $p_M(2) = p_2 = (1 - p_1)$, respectively, and assume an extreme case, where $\sigma_1^2 > 0$ and $\sigma_2^2 = 0$. Suppose we have a discrete fading channel with two states, which are observed with probabilities $p_{H_1}(\hat{h}_1) = p_1$ and $p_{H_2}(\hat{h}_2) = p_2$, respectively, and assume that the channel states are $\hat{h}_1 > 0$ and $\hat{h}_2 = 0$. We aim at linearly transmitting $N = 2$ measurements of parameters $m_1 \in [1{:}2]$ and $m_2 \in [1{:}2]$, over $N = 2$ channel states $h_1 \in \{\hat{h}_1, \hat{h}_2\}$ and $h_2 \in \{\hat{h}_1, \hat{h}_2\}$.

We first characterize the minimum achievable MSE distortion, $\bar{D}_1$, for all possible LT schemes with a diagonal encoding matrix. According to Eqn. (5.11), the encoding function needs to satisfy the average power constraint P, i.e., $\frac{1}{2}\left[P_{11}p_1^2 + P_{12}p_1p_2 + P_{21}p_1p_2 + P_{22}p_2^2\right] = P$, where $P_{m_1m_2}$ is the allocated power for the pair of measurements of parameters m_1 and m_2, respectively. We have $P_{22} = 0$, since $\sigma_2^2 = 0$. Then, by using Eqn. (5.13), the MSE distortion $\bar{D}_1$ can be written explicitly as follows:

$$\begin{aligned}\bar{D}_1 = \frac{1}{2}\Bigg\{ & p_1^2\left(\mathrm{E}_{H_1}\left[\frac{\sigma_1^2}{|h_1|^2\frac{P_{11}}{2}+1}\right] + \mathrm{E}_{H_2}\left[\frac{\sigma_1^2}{|h_2|^2\frac{P_{11}}{2}+1}\right]\right) \\ & + p_1p_2\left(\mathrm{E}_{H_1}\left[\frac{\sigma_1^2}{|h_1|^2P_{12}+1}\right] + \mathrm{E}_{H_2}\left[\frac{\sigma_1^2}{|h_2|^2P_{21}+1}\right]\right)\Bigg\}, \\ = p_1^2 & \left(p_1\frac{\sigma_1^2}{|\hat{h}_1|^2\frac{P_{11}}{2}+1} + p_2\sigma_1^2\right) + \frac{p_1p_2}{2}\left(p_1\frac{\sigma_1^2}{|\hat{h}_1|^2P_{12}+1} + p_1\frac{\sigma_1^2}{|\hat{h}_1|^2P_{21}+1} + 2p_2\sigma_1^2\right),\end{aligned} \tag{5.56}$$

where the minimum distortion is achieved by dividing the power, i.e., P_{11}, equally between measurements if two measurements are observed from parameter 1, i.e., $m_1 = m_2 = 1$. If one measurement is requested from each parameter, i.e., $(m_1 = 1, m_2 = 2)$ or $(m_1 = 2, m_2 = 1)$, then the minimum distortion is achieved by allocating the entire power, i.e., P_{12} or P_{21}, to the measurement of parameter 1, since $\sigma_2^2 = 0$.

Assuming the average power constraint P is satisfied as in the above scheme, we next consider a particular LT scheme. This scheme uses a diagonal encoding matrix if both measurements are observed from the same parameter; otherwise, it uses a non-diagonal matrix, where the measurement of parameter 1 is transmitted over two channels. Then, from Eqn. (5.13), the MSE distortion $\bar{D}_2$ can be written as follows:

$$\begin{aligned}\bar{D}_2 = \frac{1}{2}\Bigg\{ & p_1^2\left(\mathrm{E}_{H_1}\left[\frac{\sigma_1^2}{|h_1|^2\frac{P_{11}}{2}+1}\right] + \mathrm{E}_{H_2}\left[\frac{\sigma_1^2}{|h_2|^2\frac{P_{11}}{2}+1}\right]\right) \\ & + p_1p_2\left(\mathrm{E}_{H_1,H_2}\left[\frac{\sigma_1^2}{(|h_1|^2+|h_2|^2)\frac{P_{12}}{2}+1}\right] + \mathrm{E}_{H_1,H_2}\left[\frac{\sigma_1^2}{(|h_1|^2+|h_2|^2)\frac{P_{21}}{2}+1}\right]\right)\Bigg\}, \\ = p_1^2 & \left(p_1\frac{\sigma_1^2}{|\hat{h}_1|^2\frac{P_{11}}{2}+1} + p_2\sigma_1^2\right) + \frac{p_1p_2}{2}\left(2p_2^2\sigma_1^2 + p_1^2\frac{\sigma_1^2}{|\hat{h}_1|^2P_{12}+1} + p_1^2\frac{\sigma_1^2}{|\hat{h}_1|^2P_{21}+1}\right. \\ & \left. + 2p_1p_2\frac{\sigma_1^2}{|\hat{h}_1|^2\frac{P_{12}}{2}+1} + 2p_1p_2\frac{\sigma_1^2}{|\hat{h}_1|^2\frac{P_{21}}{2}+1}\right),\end{aligned} \tag{5.57}$$

where the minimum distortion can be achieved by dividing the power, i.e., P_{11}, equally between measurements if two measurements are observed from parameter 1, i.e., $m_1 = m_2 = 1$, similarly to the above scheme. If one measurement is requested from each parameter, i.e., $(m_1 = 1, m_2 = 2)$ or $(m_1 = 2, m_2 = 1)$, then this particular scheme divides the power, i.e., P_{12} or P_{21}, equally between two channels h_1 and h_2 for the transmission of the measurement of parameter 1, as seen in the term multiplied by $p_1 p_2$ in (5.57). If two measurements are observed from parameter 2, i.e., $m_1 = m_2 = 2$, then we do not allocate power, i.e., $P_{22} = 0$, since $\sigma_2^2 = 0$.

We can easily see that $\bar{D}_2 < \bar{D}_1$ for all P_{11}, P_{12} and P_{21}. This implies that the minimum achievable MSE distortion of LT schemes constrained to one-to-one mapping can be improved by utilizing non-diagonal encoding matrices, which concludes the proof of Lemma 5.3.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This dissertation has focused on two enabling technologies that provide advanced monitoring and control capabilities to SGs, namely, SMs and WSNs, and studied the design of privacy-preserving EM techniques for SMs and delay-sensitive transmission strategies for WSNs. The proposed EM techniques have been shown to provide privacy to SM users while maintaining unaltered the operational utility of the SM readings for the SG. In addition to privacy, the proposed EM techniques have taken into account two benefits, namely, energy efficiency and energy cost saving, which have been provided to users thanks to the utilization of storage units, and then explored the fundamental trade-offs between user's privacy and energy efficiency, and user's privacy and energy cost, respectively. On the other hand, the proposed LT strategies have been shown to enable wireless sensors to meet low latency, low complexity transmission requirements for real-time and accurate state reconstruction; and thus, efficient and robust management of the SG.

In Chapter 3, we have considered an SM system in the presence of EH and storage units, and studied the fundamental trade-off between user's privacy and energy efficiency. We have integrated an EH unit as an alternative energy source, an RB as an energy storage unit and an EMU as the management unit of the energy flow. The EH unit provides energy packets to the energy consumer at each time instant in an i.i.d. fashion and the finite capacity RB provides both energy efficiency by storing extra energy for future use and increased privacy by masking the load signature of the appliances from the UP. We have considered a discrete-time FSM to represent the whole system, and investigated stochastic EM policies at the EMU based on the harvested energy, energy demand of the appliances and the state of the storage unit. We have measured the privacy of the user from an information theoretic perspective by using the information leakage rate between the input load, i.e., the user's energy demand profile, and the

output load, i.e., the SM readings, and the energy efficiency of the user by using the wasted energy rate.

We have calculated the information leakage rate by using a numerical method. For the sake of simplicity, we have considered binary input and output loads. We have studied battery-dependent EM policies and numerically searched for the EM technique that achieves the best trade-off between user's privacy and energy-efficiency. We have observed that the information leakage rate can be significantly reduced in the presence of an energy harvester and an RB. As the EH rate increases, we have observed that the privacy of the user improves. On the other hand, this also increases the amount of wasted energy. For a given input load and EH rates, we have numerically characterized the optimal trade-off curve between the achievable information leakage and wasted energy rates. The whole trade-off curve can be characterized by changing the stochastic EM policy used by the EMU. According to the needs of the user, an operating point can be chosen on this trade-off curve. We have also characterized the trade-off curves for different EH rates. Focusing on a system with only an RB, we have studied the impact of the RB capacity on the achievable privacy. We have observed that the information leakage rate can significantly be reduced by increasing the RB capacity. For the system with only an RB, we have also studied the impact of wasting of grid energy on fulfilling the increased privacy requirements of the user. We have observed that even with a finite capacity RB, the higher privacy levels can be provided to the user by wasting more energy from the grid.

In Chapter 4, we have considered an SM system in the presence of a finite-capacity energy storage unit, and studied demand-side EM policies from a joint privacy-energy cost optimization perspective. We have considered a discrete-time energy consumption model, in which both the energy consumption and the electricity prices vary over time. We have measured the privacy of the user as the variance of the output load around a predetermined constant target value, and the energy cost by using a time-varying electricity pricing model. First, assuming that the user's energy demand profile and the electricity prices are known non-causally at the EMU, we have formulated the optimal privacy-cost trade-off as a convex optimization problem, and identified the properties of the optimal offline EM policy. Then, using the implications of these properties on the optimal solution, we have proposed a backward water-filling algorithm which efficiently computes the optimal offline EM policy. We have observed that the energy cost can be reduced by requesting more energy when the prices are lower, and the privacy is obtained by generating a smoother output load. We have shown that both gains can be achieved simultaneously by utilizing the available RB intelligently.

Next, assuming that the user's power consumption profile is known only causally, we have characterized the optimal online policy using DP. Since DP algorithms are prohibitively complex, we have also proposed a low complexity heuristic online EM policy based on the

water-filling algorithm for the offline setting. In addition to the output load variance, we have also characterized the information leakage rate between the input and output load sequences. We have assessed the performances of the proposed offline and online EM policies through extensive numerical results using real SM consumption data. We have numerically evaluated both the load variance and the information leakage rate as privacy measures and characterized the trade-offs between privacy and energy cost resulting from offline and online policies. Our results indicate that the privacy-cost trade-offs for output load variance and information leakage rate have very similar behaviours; and therefore, output load variance can be used as a privacy measure for SM systems. The operating point on the trade-offs can be chosen based on the user's requirements on privacy and energy cost. We have shown through these numerical results that the proposed heuristic online algorithm performs very close to the optimal solution based on DP, which requires significantly higher computational complexity. We have investigated the impact of the RB capacity on the trade-off between privacy and energy cost for the proposed EM policies. We have also shown that most of the privacy gains can be obtained with a relatively small capacity RB.

In Chapter 5, we have studied the delay-constrained LT strategies for the transmission of composite Gaussian measurements from a sensor to a CC over an AWGN fading channel in a point-to-point communication problem. We have considered a wireless sensor node that can collect measurements from J distinct Gaussian system parameters. Discretizing time into TSs, we have assumed that the CC asks for a measurement of a particular parameter from the sensor with a certain probability at each TS. If the CSI is known by both the encoder and decoder, we have presented the optimal LT strategy in terms of the average MSE distortion under a strict delay constraint, and have given a graphical interpretation for the optimal power allocation scheme and the corresponding distortion value. Then, for general constraints, we have proposed two LT strategies, called LTHM and LTSM, based on the solution to a particular multiple measurements-parallel channels scenario, and have provided numerical results to investigate the impact of the delay and average power constraints on the performance. We have observed that if the number of parameters is more than one, i.e., $J > 1$, the MSE distortion decreases as the delay constraint is relaxed. We have also derived lower bounds on the achievable MSE distortion for generic and LT strategies. We have observed that LTSM outperforms LTHM at all delay constraints. When the fading channel follows a discrete distribution and the delay constraint is completely removed, we have shown analytically that both strategies meet the lower bound under certain matching conditions between the channel states and the paramater variances; and hence, achieve the optimal performance.

We have also considered the case in which the CSI is known only by the decoder, and presented the optimal LT strategy in terms of the average MSE distortion under a strict delay

constraint. We have derived a lower bound on the achievable MSE distortion for generic LT strategies by relaxing the delay constraint and the linearity requirement. The design of the optimal LT strategy for arbitrary delay constraints is elusive. For this argument, we have considered the multiple measurements-parallel channels scenario under a strict delay constraint and $J > 1$ assumption, and have shown that the optimal LT performance cannot be achieved by an LT scheme that is limited to use only a one-to-one linear mapping between measurements and channels, as opposed to the results derived in [95] and [97].

6.2 Future Work

There are several possible research directions that can be considered to extend the results and findings of this thesis. From a practical standpoint, future work should extend the theoretical and numerical results of this thesis by considering more complex models. Some of the extensions are pointed out below:

Regarding the SM systems considered in Chapters 3 and 4,

- Numerous practical issues can be incorporated to the problem formulation with more complex models, i.e., storage inefficiencies, battery leakages, battery charging/discharging rates, the cost of repeated charging and discharging on the battery's lifetime, processing energy costs, voltage and frequency differences between different energy sources, etc.

- In the analysis of the proposed EM techniques, we consider SMs that only report the real power consumption of the user. However, SMs can also report variables such as the reactive power, the power factor or various harmonics, which can also be used to make deductions about the input load. These variables can be included to extend the analysis conducted for the proposed EM techniques.

- In the analysis, we assume that the energy demand of the appliances is satisfied by transferring an equivalent amount of energy from the RB, EH unit or UP. This model can be extended by considering the effect of the supply voltage, frequency or the characteristics of the appliances on the amount of energy that needs to be requested from the corresponding energy source.

- Introducing plug-in EVs, hybrid and battery-run cars, which can be used for distributed energy storage by means of their RBs, would increase the total storage capacity of the system. As an extension, it would be interesting to see the affect of these devices on the user's privacy, energy efficiency and energy cost.

- Another interesting extension would be to allow the user to sell his surplus stored or renewable energy to the UP, and see its impact on the performance metrics of the SM systems.

Regarding the WSN system considered in Chapter 5,

- An important extension would be to come up with advanced transmission techniques that can better approach the TLB for the scenario in which the sensors do not have the CSI. In particular, the design of the optimal LT strategy for the multiple measurements-parallel channels scenario for arbitrary delay constraints would be an interesting and challenging future work.
- Another challenging future work would be to study the optimal scheduling scheme in the presence of multiple sensors and parallel channels.

Bibliography

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar.-Apr. 2009.

[2] S. E. Collier, "Ten steps to a smarter grid," *IEEE Industry Applications Magazine*, vol. 16, no. 2, pp. 62–68, Mar.-Apr. 2010.

[3] M. Kolhe, "Smart grid: Charting a new energy future: Research, development and demonstration," *The Electricity Journal*, vol. 25, no. 2, pp. 88–93, Mar. 2012.

[4] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sept.-Oct. 2005.

[5] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 21–38, Jan. 2012.

[6] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, Oct. 2012.

[7] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[8] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, Sept. 2010.

[9] U. S. Department of Energy, "Annual energy outlook 2015 with projections to 2040," Washington, DC, USA, Apr. 2015.

[10] European Comission, "Energy infrastructure priorities for 2020 and beyond: a blueprint for an integrated european energy network," Nov. 2010.

[11] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, Jan.-Feb. 2010.

[12] S. Priya and D. J. Inman, *Energy Harvesting Technologies*. New York, NY, USA: Springer Science+Business Media, 2009.

[13] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 6, no. 4, art. 32, Sep. 2007.

[14] S. W. Hadley and A. A. Tsvetkova, "Potential impacts of plug-in hybrid electric vehicles on regional power generation," *The Electricity Journal*, vol. 22, no. 10, pp. 56–68, Dec. 2009.

[15] C. H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 799–821, Jul. 2012.

[16] Deutsche Telekom, "Deutsche telekom smart gridframework," available at "http://bit.ly/1UPUixJ".

[17] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews*, vol. 15, no. 6, pp. 2736–2742, Aug. 2011.

[18] I. Sadinezhad and V. G. Agelidis, "Slow sampling on-line harmonics/interharmonics estimation technique for smart meters," *Electric Power Systems Research*, vol. 81, no. 8, pp. 1643–1653, Aug. 2011.

[19] H. Li, R. Mao, L. Lai, and R. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 114–119.

[20] M. H. Albadi and E. F. El-Saadany, "A summary of demand response in electricity markets," *Electric Power Systems Research*, vol. 78, no. 11, pp. 1989–1996, Nov. 2008.

[21] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 82–88, Jun. 2010.

[22] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 3, pp. 381–388, Aug. 2011.

[23] S. Borenstein, M. Jaske, and A. Rosenfeld, *Dynamic pricing, advanced metering, and demand response in electricity markets*. Berkeley, CA: Center for the Study of Energy Markets, University of California Energy Institute, Technical Report CSEM WP 105, Oct. 2002.

[24] G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: Environment, behaviour and design," *Energy and Buildings*, vol. 35, no. 8, pp. 821–841, Sept. 2003.

[25] P. Siano, "Demand response and smart grids—A survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461–478, Feb. 2014.

[26] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, Feb. 2011.

[27] The Institution of Engineering and Technology, "What is a smart grid," Sept. 2013.

[28] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May-Jun. 2009.

[29] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network*, Feb. 2009.

[30] M. Jawurek, F. Kerschbaum, and G. Danezis, "Sok: Privacy technologies for smart grids a survey of options," Microsoft Technical Report, Nov. 2012.

[31] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 998–1010, Oct. 2012.

[32] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[33] S. Cui, Z. Han, S. Kar, T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sept. 2012.

[34] U.S. National Institute of Standards and Technology, "Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements," NISTIR 7628, Aug. 2010.

[35] AMI-SEC TF, "AMI system security requirements," OpenSG, Dec. 2008.

[36] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys)*, Zurich, Switzerland, Nov. 2010, pp. 61–66.

[37] U. Greveler, P. Glosekotter, B. Justus, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, Las Vegas, NV, USA, July 2012.

[38] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[39] R. A. Len, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *IEEE Transactions on Power Delivery*, vol. 22, no. 2, pp. 1021–1028, Apr. 2007.

[40] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi, "The deployment of a smart monitoring system using wireless sensor and actuator networks," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 49–54.

[41] B. Lu, T. G. Habetler, R. G. Harley, and J. A. Gutierrez, "Applying wireless sensor networks in industrial plant energy management systems. Part I. A closed-loop scheme," in *Proceedings of the 4th IEEE Conference on Sensors*, Irvine, CA, USA, Oct.-Nov. 2005, pp. 145–150.

[42] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Proceedings of the IEEE PES General Meeting*, Minneapolis, MN, USA, Jul. 2010, pp. 1–7.

[43] U. S. Department of Energy, "Assessment study on sensors and automation in the industries of the future," Office of Energy and Renewable Energy, Nov. 2004.

[44] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[45] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implemantation*. Boca Raton, FL, USA:CRC Press, 2004.

[46] P. Kundur, *Power System Stability and Control*. New York, NY: McGraw-Hill Inc., 1994.

[47] U. S. Department of Energy, "Communication requirements of smart grid technologies," Oct. 2010.

[48] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on selected areas in communications (J-SAC)*, vol. 31, no. 7, pp. 1331–1341, Jul. 2013.

[49] D. Gündüz, J. Gómez-Vilardebó, O. Tan, and H. V. Poor, "Information theoretic privacy for smart meters," in *Proceedings of the Information Theory and Applications Workshop (ITA)*, San Diego, CA, USA, Feb. 2013, pp. 1–7.

[50] O. Tan, D. Gündüz, and H. V. Poor, "Smart meter privacy in the presence of energy harvesting and storage devices," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Tainan City, Taiwan, Nov. 2012, pp. 664–669.

[51] O. Tan, D. Gündüz, and J. Gómez-Vilardebó, "Optimal privacy-cost trade-off in demand-side management with storage," in *Proceedings of the IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Stockholm, Sweden, Jun.-Jul. 2015, pp. 370–374.

[52] O. Tan, J. Gómez-Vilardebó, and D. Gündüz, "Privacy-cost trade-offs in demand-side management with storage," *submitted to IEEE Transactions on Information Forensics and Security*, 2016.

[53] O. Tan, D. Gündüz, and J. Gómez-Vilardebó, "Linear transmission of composite Gaussian measurements over a fading channel under delay constraints," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4335–4347, May 2016.

[54] O. Tan, D. Gündüz, and J. Gómez-Vilardebó, "Delay constrained linear transmission of a mixture of Gaussian measurements over a fading channel," in *Proceedings of the IEEE International Conference on Communications (ICC)*, London, UK, Jun. 2015, pp. 4107–4112.

[55] O. Tan, D. Gündüz, and J. Gómez-Vilardebó, "Delay constrained linear transmission of random state measurements," in *Proceedings of the IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruña, Spain, Jun. 2014, pp. 53–56.

[56] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[57] A. Predunzi, "A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel," in *Proceedings of the IEEE Power Engineering Society Winter Meeting*, New York, NY, USA, Jan. 2002, pp. 941–946.

[58] 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, Oct. 1991.

[59] Z. Taysi, M. Guvensan, and T. Melodia, "TinyEARS: Spying on house appliances with audio sensor nodes," in *Proceedings of the ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys)*, Zurich, Switzerland, Nov. 2010, pp. 31–36.

[60] G. Kalogridis and S. Z. Denic, "Data mining and privacy of personal behaviour types in smart grid," in *Proceedings of the IEEE International Conference on Data Mining Workshops (ICDMW)*, Vancouver, Canada, Dec. 2011, pp. 636–642.

[61] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy of electrical appliances based on load signatures," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 2, pp. 653–660, May 2007.

[62] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, no. 2, pp. 12–16, Jun. 1989.

[63] M. Enev and S. Gupta, "Televisions, video privacy, and powerline electromagnetic interference," in *Proceedings of the ACM Conference on Computer and Communications Security*, Chicago, IL, USA, Oct. 2011, pp. 537–550.

[64] S. S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu, and W. Xu, "Current events: Identifying webpages by tapping the electrical outlet," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, London, UK, Sept. 2013, pp. 700–717.

[65] G. Bauer, K. Stockinger, and P. Lukowicz, "Recognizing the use-mode of kitchen appliances from their current consumption," in *Proceedings of the European Conference on Smart Sensing and context (EuroSSC)*, Guildford, UK, Sept. 2009, pp. 163–176.

[66] M. A., Lisovich, D. K., Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 11–20, Jan. 2010.

[67] J. Froehlich, E. Larson, T. Campbell, C. Haggerty, J. Fogarty, and S. N. Patel, "HydroSense: Infrastructure-mediated single-point sensing of whole-home water activity," in *Proceedings of the International Conference on Ubiquitous Computing*, Orlando, FL, USA, Sept. 2009, pp. 235–244.

[68] Y. Kim, T. Schmid, M. B. Srivastava, and Y. Wang, "Challenges in resource monitoring for residential spaces," in *Proceedings of the ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys)*, Berkeley, California, USA, Nov. 2009, pp. 1–6.

[69] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 238–243.

[70] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Capetown, South Africa, May 2010, pp. 1–5.

[71] R. Petrlic, "A privacy-preserving concept for smart grids," in *Proceedings of the Sicherheit in Vernetzten Systemen: 18 DFN Workshop*, 2010, pp. B1–B14.

[72] T. Jeske, "Privacy-preserving smart metering without a trusted-third-party," in *Proceedings of the International Conference on Security and Cryptography (SECRYPT)*, Athens, Greece, Jul. 2010, pp. 114–123.

[73] M. Jawurek, M. Johns, and K. Rieck, "Smart metering de-pseudonymization," in *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, Dec. 2011, pp. 227–236.

[74] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 327–332.

[75] S. Ruj, A. Nayak, and I. Stojmenovic, "A security architecture for data aggregation and access control in smart grids," arXiv:1111.2619, 2011.

[76] F. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Proceedings of the Security and Trust Management (STM)*, Athens, Greece, Sep. 2010, pp. 226–238.

[77] C. Rottondi, G. Verticale, and A. Capone, "A security framework for smart metering with multiple data consumers," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Orlando, FL, USA, Mar. 2012, pp. 103–108.

[78] K. Kursawe, M. Kohlweiss, and G. Danezis, "Privacy-friendly aggregation for the smart-grid," in *Proceedings of the International Conference on Privacy Enhancing Technologies (PETS)*, Waterloo, Canada, Jul. 2011, pp. 175–191.

[79] G. Acs and C. Castelluccia, "I have a dream! (differentially private smart metering)," in *Proceedings of the Information Hiding Conference*, Prague, Czech Republic, May 2011, pp. 118–132.

[80] T.-H. H. Chan, E. Shi, and D. Song, "Privacy-preserving stream aggregation with fault tolerance," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, Kralendijk, Bonaire, Feb.-Mar. 2012, pp. 200–214.

[81] E. Shi, T.-H. H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, Feb. 2011, pp. 1–17.

[82] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proceedings of the International Conference on Management of Data (SIGMOD)*, Indianapolis, Indiana, USA, Jun. 2010, pp. 735–746.

[83] M. Jawurek and F. Kerschbaum, "Fault-tolerant privacy-preserving statistics," in *Proceedings of the Privacy Enhancing Technologies*, Vigo, Spain, Jul. 2012, pp. 221–238.

[84] H.-Y. Lin, W.-G. Tzeng, S.-T. Shen, and B.-S. P. Lin, "A practical smart metering system supporting privacy preserving billing and load monitoring," in *Proceedings of the Applied Cryptography and Network Security*, Singapore, Jun. 2012, pp. 544–560.

[85] G. Kalogridis, C. Efthymiou, S. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proceedings of the IEEE*

International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, Oct. 2010, pp. 232–237.

[86] G. Kalogridis, R. Cepeda, S. Z. Denic, T. Lewis, and C. Efthymiou, "Elecprivacy: Evaluating the privacy protection of electricity management algorithms," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 750–758, Aug. 2011.

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

[88] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," *IACR Cryptology ePrint Archive*, no. 183, 2012.

[89] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the ACM Conference on Computer and Communications Security*, Chicago, IL, USA, Oct. 2011, pp. 87–98.

[90] T. D. Nicol and D. M. Nicol, "Combating unauthorized load signal analysis with targeted event masking," in *Proceedings of the Hawaii International Conference on System Science (HICSS)*, Maui, HI, USA, Jan. 2012, pp. 2037–2043.

[91] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the ACM Conference on Computer and Communications Security*, Raleigh, NC, USA, Oct. 2012, pp. 415–427.

[92] J. Koo, X. Lin, and S. Bagchi, "PRIVATUS: Wallet-friendly privacy protection for smart meters," in *Proceedings of the European Symposium on Research in Computer Security*, Pisa, Italy, Sept. 2012, pp. 343–360.

[93] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *IEEE Transactions on Smart Grids*, vol. 6, no. 1, pp. 486–495, Jan. 2015.

[94] T. Cover and J. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.

[95] K. H. Lee and D. P. Petersen, "Optimal linear coding for vector channels," *IEEE Transactions on Communications*, vol. 24, no. 12, pp. 1283–1290, Dec. 1976.

[96] J. Geng, H. Li, and L. Lai, "Smart grid system state measurement estimation over wireless channels," in *Proceedings of the Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, USA, Mar. 2012, pp. 1–6.

[97] J. J. Xiao, Z. Q. Luo, and N. Jindal, "Linear joint source-channel coding for Gaussian sources through fading channels," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, San Francisco, CA, USA, Dec. 2006, pp. 1–5.

[98] I. E. Aguerri and D. Gündüz, "Linear transmission of correlated Gaussian sources over MIMO channels," in *Proceedings of the IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Ilmenau, Germany, Aug. 2013, pp. 1–5.

[99] A. Kashyap, T. Basar, and R. Srikant, "Minimum distortion transmission of Gaussian sources over fading channels," in *Proceedings of the IEEE Conference on Decision and Control*, Maui, HI, USA, Aug. 2013, pp. 80–85.

[100] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[101] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 837–846, Jun. 2013.

[102] J. Yao and P. Venkitasubramaniam, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *Proceedings of the Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Oct. 2013, pp. 115–122.

[103] J. Gómez-Vilardebó and D. Gündüz, "Smart meter privacy for multiple users in the presence of an alternative energy source," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 132–141, Jan. 2015.

[104] D. Gündüz and J. Gómez-Vilardebó, "Smart meter privacy in the presence of an alternative energy source," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Budapest, Hungary, June 2013, pp. 2027–2031.

[105] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "A theory of utility and privacy of data sources," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Austin, TX, USA, June 2010, pp. 2642–2646.

[106] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[107] D. Agrawal and C. C. Aggarwal, "On the design and quantification of privacy preserving data mining algorithms," in *Proceedings of the ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, Santa Barbara, CA, USA, May 2011, pp. 247–255.

[108] S. Li, A. Khisti, and A. Mahajan, "Privacy-optimal strategies for smart metering systems with a rechargeable battery," available at arxiv "http://bit.ly/20m8RxN", 2015.

[109] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, Apr. 2009.

[110] Y. Kim, E. Ngai, and M. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 178–183.

[111] A. Bartoli, J. H. Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation over fading and shadowing channels for smart grid m2m networks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 844–864, Dec. 2011.

[112] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Perez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 166–172, May 2012.

[113] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy tradeoff framework," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 190–195.

[114] D. M. Arnold, H. A. Loeliger, P. O. Vontobel, A. Kavcic, and W. Zeng, "Simulation-based computation of information rates for channels with memory," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3498–3508, Aug. 2006.

[115] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284–287, Mar. 1974.

[116] S. Wang, L. Cui, J. Que, D. H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1317–1324, Sep. 2012.

[117] M. A. Zafer and E. Modiano, "A calculus approach to energy-efficient data transmission with quality-of-service constraints," *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 898–911, Jun. 2009.

[118] A. Reinhardt, D. Christin, and S. S. Kanhere, "Predicting the power consumption of electric appliances through time series pattern matching," in *Proceedings of the ACM Workshop on Embedded Systems For Energy-Efficient Buildings (BuildSys)*, Rome, Italy, Nov. 2013, pp. 1–2.

[119] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.

[120] D. P. Bertsekas, *Dynamic programming and optimal control*. Athena Scientific, 2007.

[121] J. Z. Kolter and M. J. Johnson, "REDD: A public data set for energy disaggregation research," in *Proceeding of the Workshop on Data Mining Applications in Sustainability (SustKDD)*, San Diego, CA, USA, Aug. 2011, pp. 1–6.

[122] European Comission, "Energy price statistics (2013)," available at "http://bit.ly/1AigKSR".

[123] T. Yang, H. Sun, and A. Bose, "Transition to a two-level linear state estimator, part I: Architecture," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 46–53, Feb. 2011.

[124] Y. F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 33–43, Sept. 2012.

[125] I. Esnaola, A. M. Tulino, and J. Garcia-Frias, "Linear analog coding of correlated multivariate Gaussian sources," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3438–3447, Aug. 2013.

[126] T. Goblick, "Theoretical limitations on the transmission of data from analog sources," *IEEE Transactions on Information Theory.*, vol. 11, no. 4, pp. 558–567, Oct. 1965.

[127] A. Lapidoth and S. Tinguely, "Sending a bivariate Gaussian over a gaussian MAC," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2714–2752, Jun. 2010.

[128] M. Gastpar, "Uncoded transmission is exactly optimal for a simple gaussian sensor network," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5247–5251, Nov. 2008.

[129] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1971.

[130] A. E. Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge University Press, 2011.