

ABSTRACT

Title of dissertation: ENERGY EFFICIENCY AND
PRIVACY PROTECTION
IN CELLULAR NETWORKS

Tuan Minh Ta
Doctor of Philosophy, 2014

Dissertation directed by: Professor John S. Baras
Institute for Systems Research
Department of Electrical and Computer Engineering

Smartphones have become an essential part of our society. The benefits of having an always present, highly capable device cannot be overstated. As more aspects of our life depend on our smartphones, it is more important than ever to ensure the availability of those devices. However, their big advantages also come with big risks. The fact that we have our smartphones with us all the time means that it is easier than ever to collect our information, sometimes without our consent. In this dissertation, we study the two pressing concerns in cellular communications: energy efficiency and privacy protection. We focus on LTE networks, the current most advanced global standard for cellular communications.

In the first part of the dissertation, we study the energy efficiency problem from both device and network perspectives. From the device point of view, we introduce a new angle to address the battery life concern. We recognize that the value of battery for the users is not always the same, and that it depends on the user usage.

We also identify, and show in real network, *diversity of usage*, the phenomenon that at any instant, there is a diverse distribution of smartphone usage among cellular users. We propose “Battery Deposit Service” (BDS), a cooperative system which makes use of device-to-device (D2D) communications underlying cellular networks to provide energy sharing in the form of load sharing. We design BDS to take advantage of diversity of usage to maximize the utility of smartphone battery. We show that our system increases battery life of cellular users, at almost no cost to the rest of the network. BDS is designed to be compatible to LTE architecture.

From the network point of view, we design an energy efficient D2D relay system underlying LTE networks. We minimize transmission power of smartphones by considering relay selection, resource allocation and power control. The overall problem is prohibited due to its exponential search space. We develop a divide-and-conquer strategy which splits the overall problem into small sub-problems. We relate these sub-problems to well-studied graph theoretic problems, and take advantage of existing fast algorithms. We show that our algorithms meet the runtime requirement of real-time LTE operations.

In the second part of the dissertation, we address a privacy concern in LTE networks. In particular, we show that user location can be leaked in current LTE paging architecture. We propose a mechanism based on signal processing to remedy this vulnerability. Our method makes use of physical layer identification, which are low-power tags embedded on the wireless waveform, to signal paging messages to user devices. We show that our method is stealthy and robust, and that it mitigates the aforementioned privacy issue.

ENERGY EFFICIENCY AND PRIVACY PROTECTION IN
CELLULAR NETWORKS

by

Tuan Minh Ta

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:

Professor John S. Baras, Chair/Advisor

Professor Richard J. La

Professor Sennur Ulukus

Professor Charalampos (Babis) Papamanthou

Professor S. Raghuraghavan

© Copyright by
Tuan Minh Ta
2014

Acknowledgments

I would like to express my deepest gratitude to my advisor, professor John S. Baras, for his continual support and guidance throughout my research. His incredible energy and work ethic, as well as his astounding vision, have been my inspiration. His genuine care and interest in my success have always been my strong support. I have learned a great deal from his depth and breadth of expertise. I would also like to thank professor Richard J. La, professor Sennur Ulukus, professor Charalampos Papamantou, and professor S. Raghu Raghavan for spending their valuable time serving in my defense committee, and providing me with helpful advice and suggestions.

I would like to thank my friends and colleagues in HyNet and SEIL labs for giving me valuable feedbacks. I am especially thankful to my labmate, Shalabh Jain, who spent countless hours brainstorming with me, and offered numerous intelligent ideas and insights. I would like to specially thank Doohyun Sung for his valuable inputs from the practical system viewpoint. I would also like to thank Chenxi Zhu for helping me at the crucial early stage of identifying research needs. I also greatly appreciate Mrs. Kim Edwards for her generous and timely assistance, which allowed me to fully focus on my research.

My research was supported by Defense Advanced Research Projects Agency (DARPA) and the Semiconductor Research Corporation Focused Center Research Program through contract award number SA00007007, by the Army Research Office through MURI grant award W911-NF-0710287, by the AFOSR through MURI grant

award FA9550-10-1-0573, and by the National Science Foundation (NSF) through grant awards CNS-1018346 and CNS-1035655.

Last but not least, my family has always been my strongest foundation. Their unconditional love gave me strength to overcome the many obstacles and challenges. Their unwavering faith motivated me to extend my horizon, pushed me to reach higher. I am truly grateful for my grandparents, my parents and my lovely sister, Kieu Anh. This dissertation is dedicated to them.

Table of Contents

List of Tables	vii
List of Figures	viii
1 Introduction	1
1.1 Energy concerns for mobile devices in cellular networks	1
1.1.1 Device-to-device communications underlying cellular networks	4
1.2 Privacy concerns for mobile devices in cellular networks	8
1.2.1 Physical layer security	9
1.3 Contributions of the dissertation	10
1.4 Organization of the dissertation	13
2 Diversity of usage	15
2.1 Overview	15
2.1.1 Related work	15
2.1.2 Our approach	17
2.1.3 Summary of contributions	18
2.1.4 Outline of chapter	18
2.2 Smartphone battery distribution over user population	18
2.2.1 Data set	18
2.2.2 Data collection method	20
2.2.2.1 Twitter streaming API	20
2.2.2.2 Filtering and image gathering	21
2.2.2.3 Optical character recognition	22
2.2.2.4 Charging symbol detection	23
2.2.2.5 Duplication removal	24
2.3 Results	25
2.3.1 Distribution of battery levels at different time of day	25
2.3.2 User charging behavior	29
2.4 Conclusions	31

3	Energy efficiency from device perspective:	
	Battery Deposit Service	32
3.1	Overview	32
	3.1.1 Related work	33
	3.1.2 Summary of contributions	37
	3.1.3 Outline of chapter	38
3.2	System architecture	38
3.3	Cooperative rules	43
	3.3.1 General utility analysis framework	44
	3.3.1.1 Example: Renewable energy system for cloud computing	45
	3.3.1.2 Terminology	46
	3.3.1.3 User utility	47
	3.3.1.4 Beneficial cooperation	50
	3.3.1.5 Two categories of systems	53
	3.3.2 Battery Deposit Service	58
	3.3.2.1 Battery consumption process $\zeta_L(t)$	59
	3.3.2.2 Distribution of time until outage T_O	61
	3.3.2.3 Beneficial cooperation	69
	3.3.2.4 Design of cooperative rules	71
	3.3.2.5 Evolution of user utility over time	73
3.4	User incentive	74
	3.4.1 Virtual currency	75
	3.4.2 Real currency	75
3.5	Performance analysis	76
3.6	Conclusions	81
4	Energy efficiency from network perspective:	
	Relay selection, resource allocation and power control for minimizing transmission power in device-to-device relay-enabled LTE networks	84
4.1	Overview	84
	4.1.1 Related work	85
	4.1.2 Summary of contributions	86
	4.1.3 Outline of chapter	86
4.2	Uplink scheduling and power control in LTE	87
4.3	Current state of D2D communications underlying LTE	88
4.4	Problem statement	89
	4.4.1 Relay selection	89
	4.4.2 Resource allocation and power control	92
	4.4.2.1 RAPC for fixed MCS	96
	4.4.2.2 Heuristic search for MCS	99
4.5	Simulations	101
4.6	Conclusions	104

5	Enhancing privacy in LTE paging system using physical layer identification	106
5.1	Overview	106
5.1.1	Related work	107
5.1.2	Summary of contributions	109
5.1.3	Outline of chapter	110
5.2	LTE Paging System	110
5.3	Privacy-Enhanced Paging Messages	114
5.3.1	eNodeB Operations	117
5.3.2	User Equipment Operations	118
5.3.2.1	Decode DCI	118
5.3.2.2	Tag detection	119
5.4	Simulations	122
5.5	Conclusions	126
	Bibliography	129

List of Tables

2.1	Data set collected from April 30 - July 8, 2014	25
3.1	Target usage duration and remaining resource of the helper and helpee before and after cooperation	51
3.2	Simulation parameters	78
3.3	Overall network gains in valued usage time	80
3.4	Overall network gains in probability of survival	80
3.5	Probability that a BDS request is accepted	81
4.1	Modulation and coding schemes	94
4.2	Simulation parameters	103

List of Figures

1.1	Use cases for ad hoc networks underlying cellular networks [Bonta et al., 2007]	6
2.1	Data collection procedure	21
2.2	A typical top portion of a smartphone screenshot	23
2.3	Average of battery levels across smartphone population as a function of time of day.	26
2.4	CDF of battery levels across smartphone population. Each CDF is plotted using data within 10 minutes from the denoted time instant.	27
2.5	Entropy of the distribution of battery levels as function of time of day.	28
2.6	Heat map of battery levels among charging phones. The fraction of phones with 100% battery has been omitted for clarity.	30
3.1	Signaling flow for establishment of a BDS cooperative relay session. UE1 is the helpee, UE2 is the selected helper.	40
3.2	Renewable energy system providing energy to computing sites.	46
3.3	A sample utility surface. The resource B and target usage duration T are normalized. Following a curve with constant target usage time, the utility function increases with B - property (3.1). Following a curve with constant resource, the utility function decreases with T - property (3.2).	49
3.4	Utility as functions of target usage time for user categories C1 and C2. The amount of available resource is fixed. Both utility functions show two clear extremes.	58
3.5	Continuous time Markov Chain for remaining battery states	63
3.6	CDF of time until outage T_O calculated by stochastic analysis (3.34), Markovian analysis (3.46), Gaussian approximation (3.52), and Monte Carlo simulation. The time duration t is plotted with reference to the mean usage duration $\mathbb{E}[T_O]$	68
3.7	Utility as functions of available battery for user categories C1 and C2. The target usage time T is fixed. $\mu_B = \lambda T / \nu$	72
3.8	Evolutions of user's utility. Notice the scale difference.	74

3.9	Cumulative distribution functions of the valued usage time for 3 cooperative algorithms and no cooperation. The higher battery capacity is 14% more than the lower battery capacity.	79
4.1	Equivalent minimum weight matching on a bipartite graph problem of (RS).	93
4.2	Equivalent minimum-cost flow problem of (S-RAPC). The total flow is $\sum_{n=1}^N D_n$. Each link is annotated with a (capacity, cost) pair. The circular nodes represent UEs, the squared nodes represent RBs.	97
4.3	Runtime comparison of CPLEX, Algorithm 1, and minimum-cost flow (S-RAPC), as functions of the number of concurrent UEs to schedule.	101
4.4	Average transmission power of a UE with resource allocation and power control in (RAPC). The performance of Algorithm 1 and CPLEX are compared.	102
5.1	An example of positions of paging PDCCH and PDSCH in an LTE downlink subframe. Pilots and other types of physical channels are omitted for clarity.	113
5.2	(a) Simple scenario with one old UE (Alice) and one new UE (Bob) being paged at the same subframe. The eavesdropper, Eve, can listen on the paging broadcast channel and analyze the PDCCH waveform; (b) PDCCH and PDSCH paging messages	115
5.3	Flow charts for (a) eNodeB and (b) User Equipment. Dashed boxes are additional operations required by the scheme.	116
5.4	DCI decoding performance as a function of SNR. Here the DCI size is 44 bits. The PDCCH size is (a) 144 bits, (b) 288 bits	123
5.5	PDCCH BER for various values of tag power allocation. Here the PDCCH size is 288 bits, 16 tags are embedded.	124
5.6	Probability of tag detection for PDCCH size (a) 144 bits, (b) 288 bits.	127
5.7	Eavesdropper's received constellation at SNR = 20dB, $N_t = 4$	128

Chapter 1: Introduction

In this dissertation we address two pressing problems in cellular communications: energy efficiency and user privacy.

1.1 Energy concerns for mobile devices in cellular networks

Smartphones have become an essential part of our society. They have been outselling PC since 2010 [Arthur, 2011]. The number of smartphones as well as the amount of data they generate keep increasing at a dramatic pace [Cisco, 2014]. Competition between manufacturers drives a very rapid smartphone hardware evolution. The advancement in software is happening at an even quicker pace. Many application developers are now thinking “mobile first”. Not only do individual smartphones assist individual users, groups of smartphones are also being leveraged to provide significant benefits. Cooperative relay using smartphones has been shown to be a viable solution to prolong battery life, improving network reliability, and expanding coverage [Ta et al., 2014, Ng and Yu, 2007, Sadek et al., 2006]. Participatory sensing proposes to use smartphones, utilizing their pervasiveness, as distributed sensors to collect location-aware data, allowing us to observe previously unobservable phenomena [Burke et al., 2006]. Collaborative applications provide higher utility than

the sum of the parts, such as combining capacity of cellular links to speed up the download of large files [Ananthanarayanan et al., 2007].

Traditionally, improving network throughput has been the main concern in the wireless communication community. Many advanced techniques such as OFDMA, MIMO have been proposed to improve the spectral efficiency of the network. Recently, energy efficiency has gained much attention. A big challenge, perhaps the biggest, to the applications described above is that smartphones are battery-limited. Battery technology is still not able to keep up with expanding demand for usage of these devices. A recent survey by the International Data Corporation, which collected answers from 50,000 people from 25 countries, showed that battery life is the number one concern for new smartphone purchasers [Jeronimo, 2014].

The traditional goal of energy efficient designs is to maximize the number of bits transmitted per energy unit. Solutions are proposed across layers of wireless networks. On network planning level, the impact of cell size as well as mixed cell deployment on energy consumption of the devices have been studied [Badic et al., 2009]. On MAC layer, energy efficiency has been incorporated in resource allocation algorithms [Meshkati et al., 2009]. On PHY layer, adaptive MIMO modulation orders according to channel condition have been proposed [Miao et al., 2010].

By maximizing the number of bits transmitted per unit energy, existing work make an implicit assumption that energy, in absolute quantity (Joules), is worth the same for all users at any time instant. We, on the other hand, realize that ***smartphone battery does not always have the same value for the users.*** A straightforward argument is that a user will not value his battery as much when

he has a high battery bar compared to when he has a low battery bar. We take this argument one step further. The user will not value his battery much, even if he has a low battery bar, if he is only a few minutes from home. Therefore the value of the battery to a user involves both the absolute amount as well as the user's target usage. In particular, we introduce the notion of *valued battery*, defined as the battery of the smartphone when the user is active and does not have access to a power source. Similarly, *valueless battery* is defined as the battery of the smartphone when the user has access to a power source. We argue that the user's experience depends only on his valued battery. Smartphone users often are quite concerned when they are on the road, and their (valued) battery drops low. However, the abundant number of occasions when they are at home and their (valueless) battery is high often go unnoticed.

In realistic cellular networks, users have varied amount of remaining battery. When the state of the battery (with respect to access to a charging source) is taken into account, this variation becomes even larger. We call this phenomenon *diversity of usage*. It is intuitive that the network as a whole will benefit from converting valueless battery into valued battery. Since we are still far away from efficient long-distance wireless energy transfer [Garnica et al., 2013], a more practical approach to "sharing" battery among users needs to be developed.

We propose a cooperative system, the "Battery Deposit Service" (BDS), which makes use of D2D communications underlying LTE, to provide energy sharing in the form of load sharing. Our system allows users with high battery level to help relay traffic of users with low battery level through a D2D connection. Since the

direct link costs much less power than the cellular link, the usage time of users with low battery level is prolonged. The cooperative selection criteria are designed carefully such that the amount of energy the helpers expend does not reduce their usage time to below their target usage. Thus they only spend valueless battery. As a result, our system takes advantage of diversity of usage to raise the overall amount of valued battery in the network.

We summarize advancements in D2D research in the following section.

1.1.1 Device-to-device communications underlying cellular networks

Device-to-device (D2D) communications in the broader sense refer to autonomous connection between wireless devices in a close neighborhood. These devices include sensors, mobile phones, vehicular transceivers, etc. The majority of the work on D2D communication consider the ad-hoc case, where there is no centralized control unit. In a distributed fashion, nodes find their neighbors, perform random access to the wireless medium, create and sustain routes. Because everything is autonomous, these networks normally operate on unlicensed spectrum (e.g. Wifi, Bluetooth, Zigbee).

In the next phase of the evolution of D2D communication research, ad-hoc networks are considered concurrently with infrastructured networks. As the wireless terminals become more capable, they can operate in both networks (e.g. smart phones). There are two benefits in this hybrid architecture. Firstly, the ad-hoc nodes can make use of the synchronization provided by the infrastructured network.

Secondly, the cellular nodes can off load local traffics to ad-hoc networks and save on the scarce cellular spectrum. The design challenge is to find the optimum switching point [Michael et al., 2000, Chang et al., 2003]. In the early work, the hybrid infrastructure is simply the combination of existing infrastructures, i.e. the ad hoc mode is considered only for the unlicensed spectrum.

In the most recent advancement in D2D communication, ad-hoc and infrastructured (in particular cellular) networks are allowed to use the same licensed spectrum. Advantages of D2D underlying cellular network over ad-hoc mode in unlicensed band include:

- A licensed band can guarantee a controlled interference environment and local service providers might prefer to pay a small amount of money to offer guaranteed services avoiding the uncertainties of the license exempt bands.
- The D2D operation itself can be fully transparent to the user. Since both D2D devices already have a secure connection to the cellular network, it is easy to setup a secure D2D connection. Thus, compared to WLAN or Bluetooth, no manual pairing is required. This is very important when user mobility is considered. Furthermore, mobility is arguably the number one advantage of wireless communications.

Some use cases of D2D underlying a cellular network are illustrated in Fig 1.1.

Coming from a different direction, cognitive radio aims to utilize spectrum sharing techniques to gain from the inefficient use of the licensed spectrum. In fact, through measurements from 4 locations in Germany, Netherlands, California, [Kone

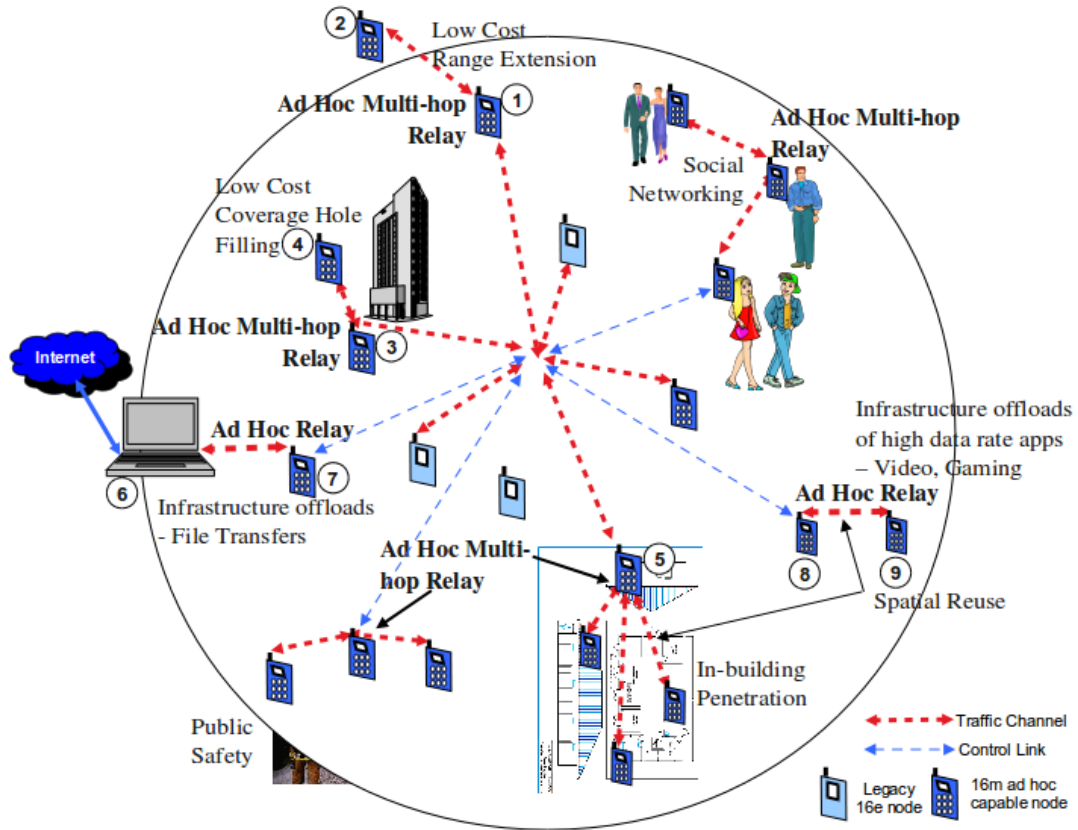


Figure 1.1: Use cases for ad hoc networks underlaying cellular networks [Bonta et al., 2007]

et al., 2010] observes that on average, 50% of the spectrum is never used, 26% is only partially used. In cellular bands (GSM and UMTS), while downlink channels are heavily occupied, uplink channels are mostly idle because their signals are significantly weaker and thus are harder to detect even with high-end spectrum analyzers. A particular difficulty for cognitive radio in cellular bands is that even though the spectrum are mostly idle on average, the instantaneous idle bands are scattered randomly. However, in D2D underlaying cellular network, the BS can assist in setting up the D2D links and thus it knows exactly which channels are available. Recently

the cognitive radio community have looked at cooperative schemes between primary and secondary users, which is similar to the scenario of D2D underlying cellular network.

To get the most benefit out of D2D communications underlying cellular networks, resource allocation and interference management has to be carefully considered. The D2D links can be allocated dedicated resources in a similar fashion as regular cellular links. This case is no different, as far as interference to the cellular network is concerned, than using unlicensed band for D2D. A better method which has a potential to significantly increase system throughput is to allow D2D communications to use the same time-frequency resources as cellular links, either in the uplink, downlink, or both. However, managing interference is a big challenge here as the D2D nodes and the cellular nodes can be anywhere within the cell.

In summary, D2D communication underlying cellular network is a viable solution to handle high-bandwidth local communication. Enabling D2D has been shown to improve system throughput significantly when there is local communication among cellular nodes in the same cell. The amount of performance gain is proportional to the percentage of local communication. The Battery Deposit Service (BDS) makes use of the underlying D2D structure to allow low cost (in term of power) links between cellular users to be used instead of high cost links to the base station. At a very rudimental stage, the BDS can be enabled by dedicating resource for D2D links. In this case no interference management is needed. The only requirement for the BS is to be able to find helpers within the proximity of the user with low battery. In Chapter 3, we describe our design to solve this requirement.

1.2 Privacy concerns for mobile devices in cellular networks

It is no secret that the telecommunication operators keep detailed records of their customers. Those giant operators know precisely where we are, what we are doing as long as our phones are active. This is the tradeoff that we are willing to make to enjoy the conveniences our smartphones provide. However, when the news broke that the National Security Agency had been keeping taps on all American phone records, there was an outrage. It showed that people still care dearly about their privacy. They are not fond of the idea that someone can get their information without their consent.

While stopping the NSA is a matter of laws and public policy, stopping individual evildoers is very much a research problem. The open nature of the wireless medium makes the job of eavesdroppers much easier compared to wired communications. GSM, the first worldwide cellular standard, was developed in the 1990s. The popularity of GSM makes it an attractive target for hackers. In fact, GSM has been shown time and time again to leak user information [Nohl and Munaut, 2010, F-Secure, 2011, Soyez, 2012]. Some well-recognized problems with GSM include: the lack of network authentication which enables fake base stations, weak encryption that can be cracked in seconds on a regular PC, no authentication for Home Location Register queries which permits trivial coarse user location leaks. As GSM is currently being phased out, LTE has become the new global standard for cellular communications. LTE has addressed most of the well-known security vulnerabilities with GSM.

However, LTE has not fixed all of the issues existed for GSM. In [Kune et al., 2012], it has been showed that, with inexpensive equipment, *anyone* can learn about the location of a target by exploiting a vulnerability in the paging architecture of GSM. After studying LTE paging architecture, we showed in [Ta and Baras, 2012] that the most advanced cellular standard also has the same vulnerability. While the security community has been mainly focused on MAC layer and above, we proposed a solution on the physical layer.

1.2.1 Physical layer security

Traditionally security and privacy protection has been relied on cryptographic solutions (e.g., block ciphers, digital signatures, keyed hashes). Cryptography techniques deter the adversary from defeating the system by requiring the adversary to spend tremendous amount of computation and memory. However, as computer hardware evolves, previously considered hard computational problems have been solved one after another by commonplace PCs.

Physical layer security is the research initiative which tries to identify communication and information theoretic security guarantees that cannot be circumvented regardless of adversarial computational capacity. Physical layer security techniques exploit the physical layer properties of the communication system (most often wireless) such as thermal noise, interference, and the time-varying nature of fading channels. The original, and still the most common, technique is to take advantage of the weaker adversarial channel compared to the legitimate channel. The differ-

ence in capacity can be used to transmit secure information. The main drawback, and the reason it is still a theoretical approach, is that it requires knowledge of the adversarial channel. This knowledge cannot be assumed in practice.

We choose a more practical branch of physical layer security research: signal processing approach. In particular, our solution is based on physical layer watermarking. The authentication problem is solved by superimposing a low-power watermark, a physical layer identification, into the baseband constellation of the wireless signal. The watermark has low power such that it is almost indistinguishable from thermal noise. The legitimate communicators, which in our case are the base station and the smartphone, can collect enough statistics through multiple data symbols to *detect* if the watermark is present. We show that our technique effectively solves the vulnerability of LTE paging architecture.

1.3 Contributions of the dissertation

We introduce a new angle to address the energy concerns for smartphones compared to existing works. From the device point of view, instead of minimizing the amount of battery consumption, we maximize the utility that smartphone battery provides the users. We identify that the value of battery for the users is not always the same. *Diversity of usage* among smartphone users provides us with opportunities to raise the overall utility in the network. These opportunities have not been considered in the literature. We propose “Battery Deposit Service” (BDS), a cooperative system which makes use of device-to-device (D2D) communications

underlying LTE to provide energy sharing in the form of load sharing. Our system allows users with high battery level to help relay traffic of users with low battery level through a D2D connection. Since the direct link costs much less power than the cellular link, the usage time of users with low battery level is prolonged. The cooperative selection criteria are designed carefully such that the amount of energy the helpers expend does not reduce their usage time to below their target usage. Thus they only spend valueless battery and their utility is not degraded.

From the network point of view, we consider the problems of relay selection, resource allocation and power control in designing an energy efficient D2D relay system underlying LTE networks. The main challenge is the stringent runtime requirement for real-time operations in LTE. The overall problem is prohibited due to the presence of binary decision variables, which lead to exponential search spaces. We adopt a divide-and-conquer strategy and split the overall problem into sub-problems, which can be related to well-studied problems in graph theory. By taking advantage of existing fast algorithms to solve these sub-problems, our design meets the runtime requirement of LTE.

Our contributions in addressing the energy efficiency problem are

1. We collect real smartphone data to show the existence of diversity of usage
2. We develop BDS as a Proximity Service for future releases of LTE, as defined by 3GPP. By doing so, we position our system to have immediate application in real networks.
3. We develop a general framework to study utility of smartphone battery, which

can be applied to other types of resource.

4. We formulate the problems of relay selection, resource allocation and power control to minimize total transmission power in D2D relay-enabled LTE networks. We develop a strategy to solve these problems, satisfying LTE runtime requirement. This mechanism as well as other energy consumption reduction techniques can be used in conjunction with BDS.

We introduce a physical layer security solution for a user privacy vulnerability in LTE. The majority of existing security researches consider solutions on MAC layer and above. Solutions on the physical layer promise to solve security problems in a more fundamental way, without relying on limitation of adversarial computational capacity. However, most physical layer security works are still theoretical. We show that our solution is practical and can be readily incorporated into current LTE networks.

Our contributions in addressing user privacy problem are

1. We show that LTE paging architecture suffers from the same vulnerability as GSM. As a result, user location privacy can be leaked.
2. We develop a signal processing technique which makes use of physical layer identification to address this vulnerability.

1.4 Organization of the dissertation

This dissertation is organized into four primary parts (four chapters). The first three chapters address the energy efficiency problem. The last chapter addresses the user privacy problem.

In Chapter 2, we show the existence of diversity of usage among smartphones through real user data. We clearly describe our data source and data collection methods.

In Chapter 3, we describe our cooperative system, the “Battery Deposit Service” (BDS), which takes advantage of diversity of usage to raise the overall utility of smartphone battery in a cellular network. We illustrate how our system can be implemented as a Proximity Service in future releases of LTE. We introduce a framework to study utility of smartphone battery as a function of user usage. Our framework is general so that it can also be applied to other types of resource. We show the utility gain through detailed system level simulation.

In Chapter 4, we formulate and solve the problem of minimizing total transmission power, through relay selection, resource allocation and power control, in a device-to-device relay-enabled LTE network. This technique can be used in conjunction with BDS to further improve network energy efficiency. The performance gain is confirmed through simulation.

In Chapter 5, we show that LTE paging architecture also suffers from a previously identified vulnerability of GSM networks. We propose a solution based on physical layer identification to address this vulnerability. We illustrate why the

adversary is not capable of performing the mentioned attack.

Chapter 2: Diversity of usage

2.1 Overview

In realistic cellular networks, users have varied amount of remaining battery. Moreover, the value of smartphone battery depends on user usage, such as how soon the users will get access to a charging source. We call this phenomenon *diversity of usage*. As discussed in Chapter 1, this phenomenon provides great opportunities for cooperative applications which allow low-usage users to help high-usage users in a load-sharing fashion. As a result, the probability of user starving is reduced. Hence, the overall utility of all users is improved. Therefore, it is very important for us to understand diversity of usage. We base our study on understanding the distribution of smartphone battery over user population.

2.1.1 Related work

A direct approach to understand the distribution of smartphone battery is to study smartphone battery consumption. The most popular method is to ask volunteers to install a logger in the their phones. The logger routinely collects battery information, aggregating and sending this information to a remote server for

analysis. The main drawback of this method is the limited sample size (usually in the tens [Rahmati et al., 2007, Jiang et al., 2013], with a few in the low hundreds [Falaki et al., 2010, Laurila et al., 2012]). In general, it is hard to find volunteers outside the circle of contacts of the researchers. Privacy concern is a major issue. Even with the assurance of the researchers, most people are wary about installing an unknown piece of software into their phones. Objectiveness is another issue. Since the participants know that their smartphone usage is being tracked, they may divert from their normal behavior.

A rare exception is [Oliver and Keshav, 2011], where battery information is collected from 20,100 BlackBerry smartphones. The method of recruiting participants was not discussed in the paper. We conjecture that the authors achieve this through the help of the original equipment manufacturer (BlackBerry Ltd, previously known as Research In Motion). Whether user consent was addressed is also not mentioned. Regardless of recruiting method, this paper possesses the largest sample size that we found in the literature. It provides valuable insights into *user charging patterns*. However, only the mean of the distribution of smartphone battery was presented. Important insights into the variation of the distribution was not discussed.

The majority of existing work focuses on battery information on a single device. What we found to be missing is detailed treatment of the distribution of battery over user population. This distribution is very important to the understanding of diversity of usage. The availability of battery of the smartphones at any instant dictates the level of participation that a cooperative scheme can expect. In searching for our data, we want to avoid the aforementioned drawbacks of previous data

collection methods. Since we do not have access to an OEM, we looked for a different approach.

2.1.2 Our approach

The explosion of web and social network traffic has led us into the era of Big Data. The impact of data abundance reaches almost every corner of our society. Examples include business, political sciences, public health, and of course, mobile computing research. Twitter is the most popular platform among the research community. Similar to many other data sources, Twitter provides unstructured (or raw) data. These data need to be further processed to draw intelligent conclusions. An example is a natural language processing application which builds an algorithm to classify user sentimental states based on tweet texts.

While textual information is still the largest output provided by tweets, we tap into an increasingly popular Twitter data type: media, and particularly, images. Twitter users' main concern is to disseminate real-time information; and the quickest and most illustrative way to capture information from a smartphone is to take a screenshot. As a result, there is a growing popularity of tweets that include screenshots. A smartphone screenshot has exactly the information that we need: the battery level and a timestamp.

To obtain the results presented in this chapter, we mined Twitter over the period of 9 weeks, collecting over half a million data samples. We collect only public information, therefore user privacy is not an issue. The users are also not biased

because they are not aware of our study.

2.1.3 Summary of contributions

Our contributions in this chapter are

1. We provide the first large-scale study focusing on the distribution of smartphone battery over user population. The results of this study help us confirm the diversity of usage among smartphone users.
2. We make our tools and data publicly available for quick replication/improvement from interested parties.

2.1.4 Outline of chapter

This chapter is structured as follows. In Section 2.2.1, we bring to the attention of the readers potential biases in our data set. We thoroughly describe our data collection method in Section 2.2.2. We show our results and analysis in Section 2.3. We close with some conclusions and remarks in Section 4.6.

2.2 Smartphone battery distribution over user population

2.2.1 Data set

Similar to other empirical research works, it is important to understand how well our data represent the subject under study. We are interested in the distribution of smartphone battery, and our data source is Twitter user smartphone screenshots.

There are three main sources for bias:

- *Fraction of smartphone users who tweet.* Prior researches have shown that Twitter user demographic is not uniform. There are higher relative portions of young, urban and educated people who use Twitter [Brenner and Smith, 2013]. At the same time, there are also higher relative portions of young, urban and educated people who own smartphones [PRC, 2014]. Therefore we can see that there is a positive correlation between smartphone owners and Twitter users.
- *Fraction of smartphone Twitter users who post screenshots.* This statistics is harder to obtain. We did not find any study that addressed this question. However, it is reasonable to assume that younger people are more likely to choose this method of sharing information. It is not difficult to identify a number of our older acquaintances who do not know how to take a phone screenshot.
- *Fraction of data we can collect from Twitter.* We obtain our data from Twitter Streaming API [Twitter,]. This API returns about 1% of all public tweets. The sampling mechanism used by Twitter to return that 1% fraction of tweets is unknown. A study last year showed that the sampler is most likely not uniform [Morstatter et al., 2013]. However, the sampler has little effect on our results, unless Twitter designs their sampler based on the battery information on the tweets that contain screenshot images. We do not see any reason supporting that hypothesis.

The exact correlation between our data and the distribution of battery over all smartphones depends on many other factors such as the composition of age groups, educational levels, and other demographic categories. In fact, as can be seen from the three points above, our data are likely biased toward the behavior of younger smartphone owners. As any other empirical researches, it is not possible to give an exact value for the correlation coefficient. Nevertheless, we believe our findings to be informative in providing insights into the battery distribution over smartphone population. By fully disclosing the data collection process, we hope to provide parties who are interested in using our data with enough information to make conclusions for their specific applications.

2.2.2 Data collection method

Our data collection procedure is captured in Figure 2.1.

2.2.2.1 Twitter streaming API

We use an open-source Python library, *tweepy* [Tweepy,], to access Twitter Streaming API [Twitter,]. By connecting to the `GET statuses/sample` public endpoint, we effectively open a long-lived HTTP request to Twitter servers. The servers return a constant stream of tweets in `json` format. As stated above, this stream contains approximately 1% of all public tweets. Each tweet has a number of information fields. The basic fields include user ID, the time the tweet was created, the content of the tweet, and the retweet status. Optional information fields include

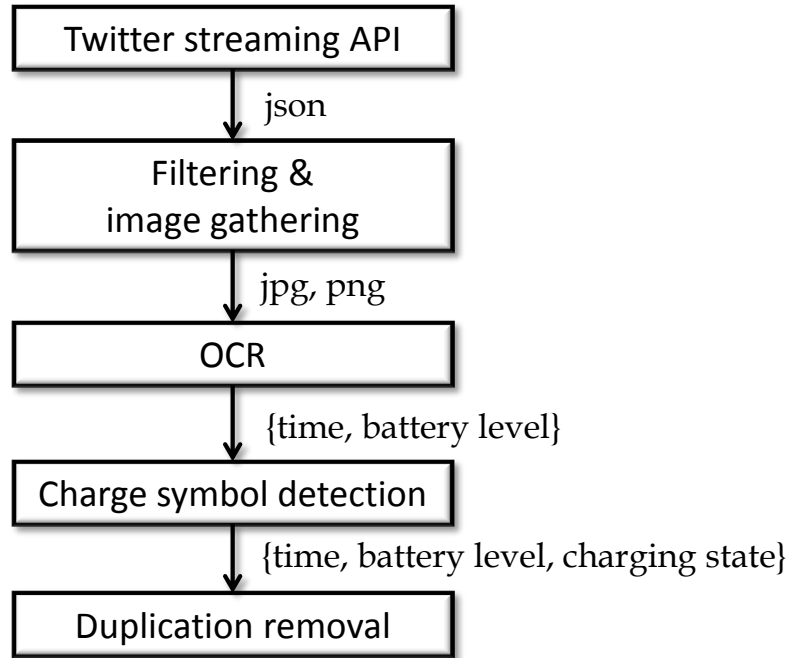


Figure 2.1: Data collection procedure

location of the tweet, reply/favorite status, language, etc. The list of all fields can be obtained from Twitter developer website.

2.2.2.2 Filtering and image gathering

We are interested in tweets which contain images. The `json` of those tweets contain the keyword `"media_url"`. We use this keyword to filter incoming tweets. A very important consideration in our data gathering process is to exclude duplicates as they create biases in the resulting statistics. Duplicates are created in two ways: 1) retweets, and 2) different users posting the same image.

A typical Twitter image URL has the following format `http://pbs.twimg.com/media/BaskppuIYAA8H90.jpg`. As we can see, the images

are indexed by a 15-character long string. Retweets will result in the same string appearing in different `jsons`. We keep a log of unique strings gathered and compare every new string against this log. To avoid excessive processing during this step, we refresh the log every day. We rely on post-processing to detect duplicates that span over multiple days, as shown subsequently.

After passing the check against the log of processed images, a new image is downloaded. The majority of Twitter images are in `jpg` format, with a small portion in `png` format.

2.2.2.3 Optical character recognition

Next, we want to determine if the downloaded image is a smartphone screenshot. Since the time and battery information always appear on the top of a screenshot, we only need to focus on this portion of the image. A typical top portion of a smartphone screenshot is illustrated in Figure 2.2a. We can see that the time always appear as `HH:MM`. The display of the battery level information depends on user settings. We decide to focus on images in which the user displays the battery level as a percentage, i.e. `BB%`. In doing so we have excluded images which only have the battery symbol. We recognize that some low-resolution information about the battery level can be deduced from these symbols (e.g. whether the battery is above or below 50%). However, given the large amount of data gathered from Twitter, we decide to trade off quantity for quality.

To get the time and battery level information, we apply optical character



(a) The top portion

uoooo au "3 23:32 28% C"!.

(b) *Tesseract* output

Figure 2.2: A typical top portion of a smartphone screenshot

recognition (OCR) on the cropped top portion of an image. We use an open-source Linux OCR engine *tesseract* [Tesseract,]. The *tesseract* output of our example is given in Figure 2.2b. As expected, even though the graphical part of the image is recognized into garbage, the textual part is recognized correctly. We filter the OCR outputs to retain only images that contain both of the following patterns `HH:MM` and `BB%`¹.

2.2.2.4 Charging symbol detection

To determine if the phone was being charged at the instant the tweet was created, we need to detect the charging symbol from the image. Since there are a large variety of smartphones, there are many types of charging symbols. iPhone screenshots have a few symbols, depending on the version of iOS. Android charging symbols vary a lot more since on top of various operating system versions, different phone manufactures often create their own custom Android themes. The vast majority of the screenshots we collected are from those two operating systems. There

¹The battery level can range from 1 to 3 digits

is a much smaller portion from the other operating systems such as Windows Phone or BlackBerry.

We use template matching to detect charging symbol from the cropped images. Template matching only works for exact fits, while there are a wide variety of screenshot sizes. Again, Android phones contribute a large number of these sizes. It is not practical to have a version of the templates for each screenshot size, because we do not have a full list of all sizes. In our algorithm, we selected a default width of 600 pixels and scaled the source images to this size before extracting the templates. During detection, we scaled the testing images to the default width before applying template matching.

We created 15 charging symbol templates from reviewing 500 images. We ran our template matching algorithm against a different set of 1000 test images. After manual verification, only 2 images were detected incorrectly, giving us 99.8% detection rate.

2.2.2.5 Duplication removal

As described above, our first attempt to remove duplication is only applied to images obtained within the same day. There are many cases where a popular image can appear in tweets weeks apart (e.g. a tweet showing Harry Styles, a popular singer, started to follow a particular user). To remove these duplicates, we cross-checked any set of images that return the same OCR value (time, battery level), and match the same charging template. We perform cross correlation on images within

Table 2.1: Data set collected from April 30 - July 8, 2014

	Number of tweets	Tweets with images	Images are screenshots
Overall	226,535,001	22,955,047	404,248
Daily ²	4,474,500	455,660	8,422

a set (rescaled to the same size) and declare that those with correlation greater than a threshold (we use 0.95) are duplicates.

2.3 Results

During the period from April 30 to July 8, 2014, we gathered 226 millions tweets. Among those, 23 millions have images. After pre-processing, we collected over 400 thousands screenshots with time and battery percentage. The summary of our data set is listed in Table 2.1. From Table 2.1, we can see that the probability of getting a good smartphone screenshot from a random tweet is roughly 0.18%.

2.3.1 Distribution of battery levels at different time of day

First let us consider the amount of available battery as function of time of day. Figure 2.3 illustrates the average battery level over the whole user population. We can see that the amount of available battery peaks at 7 AM, when most users leave

²We missed a few days at the beginning due to technical difficulty. The daily statistics are reported from May 28 - July 8, during which our script ran consistently and flagged new-day marks.

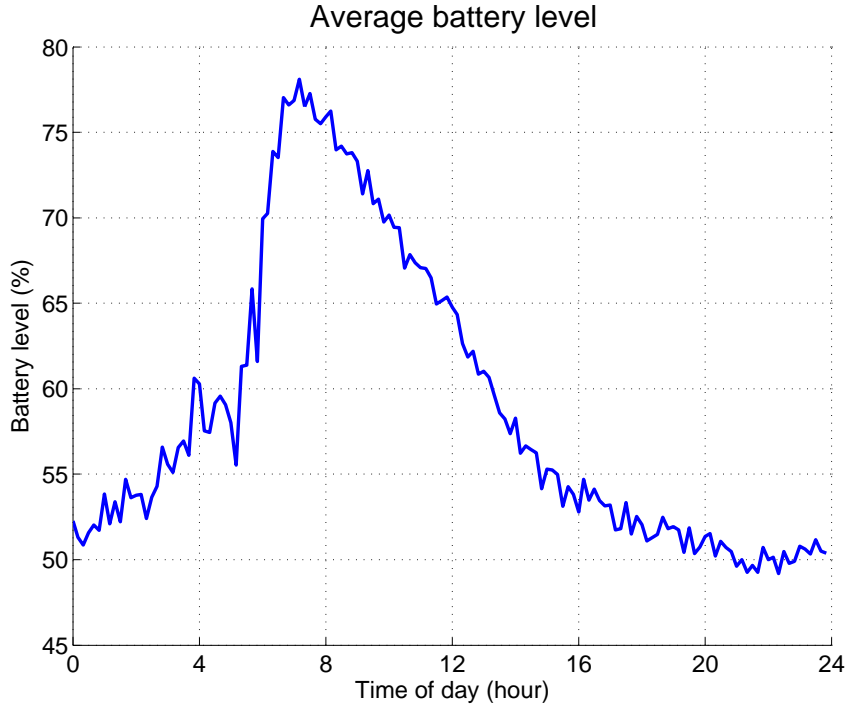


Figure 2.3: Average of battery levels across smartphone population as a function of time of day.

for work. It drops gradually as the usage increases. The dropping rate is steady from 7 AM to 4 PM, at roughly 3%/hour. It should be noted that this rate is the result of the combination of battery consumption and charging. The dropping rate slows down to about 1%/hour from 4 PM to 9 PM. This is likely to be the result of reduction in usage. The rate stays flat from 9 PM to 12 AM. It shows that the overall amount of consumption and charging is leveled during this period. As most users charge their phones before going to bed, the amount of available battery grows rapidly from 12 AM to 7 AM, when the cycle starts over.

Next, we investigate the distribution of available battery over user population at different times of the day. The cumulative distribution functions of battery levels

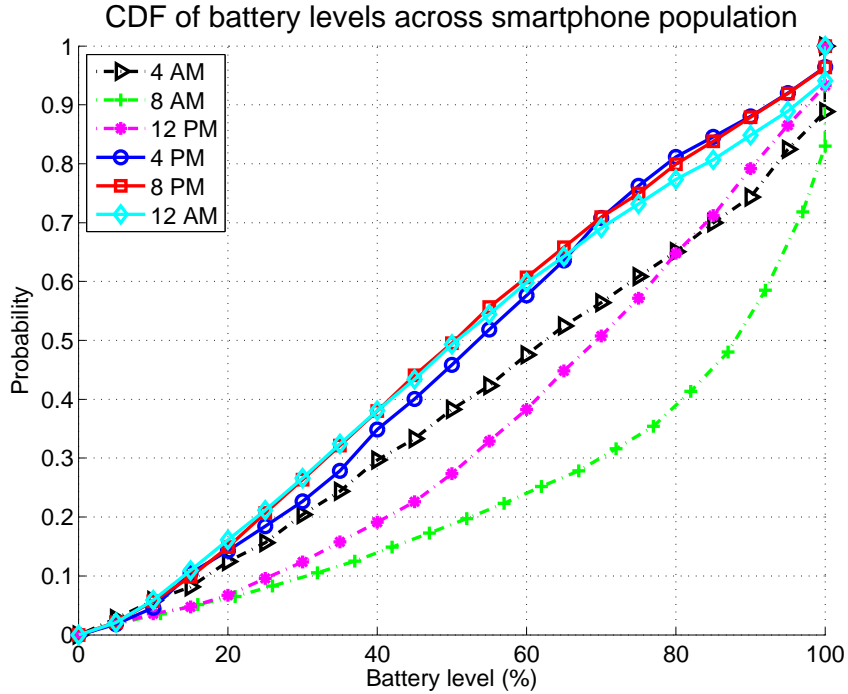


Figure 2.4: CDF of battery levels across smartphone population. Each CDF is plotted using data within 10 minutes from the denoted time instant.

taken at 6 time instants spread out over the day are illustrated in Figure 2.4. The curve at 8 AM shows that there is a large fraction of users with high battery early in the morning. The median battery level is 90%. Going into noon, the fraction of users with high battery shrinks. The median battery level reduces to 70% at 12 PM. Interestingly, the curves at 4 PM, 8 PM and 12 AM almost overlap. Moreover, without counting about 5% of users with full battery, these 3 CDFs resemble the CDF of a uniform distribution. This fact shows that the variation of user smartphone battery is the highest during late afternoon to evening. The curve at 4 AM illustrates the that during bedtime, charging dominates over consumption.

The previous discussion shows us that smartphone users start their working

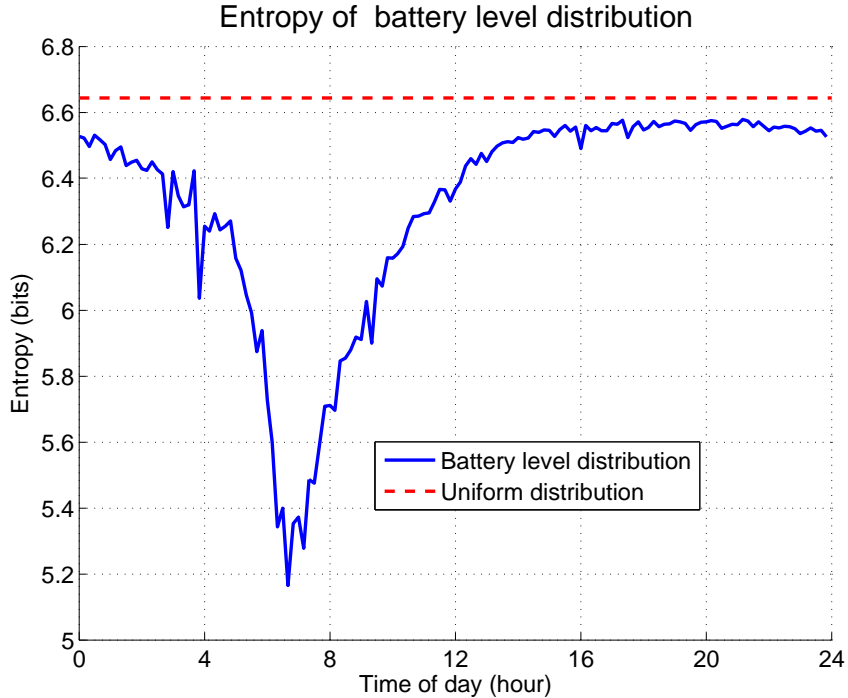


Figure 2.5: Entropy of the distribution of battery levels as function of time of day.

day relatively similarly, with high battery level. They end their working day much more diversely. This fact is further illustrated in Figure 2.5, where the entropy of the distribution of battery levels is plotted. The entropy (in bits) of a discrete distribution with PMF $\mathbf{p} = \{p_i\}$ is defined as

$$H(\mathbf{p}) = - \sum_i p_i \log_2(p_i)$$

$H(\mathbf{p})$ measures the uncertainty, or variation, of the distribution. The higher the entropy, the more varied the distribution. The uniform distribution has the highest entropy among those with the same support ($[1, 100]$ in the case of battery levels).

We can see from Figure 2.5 that from 4 PM to 12 AM, the distribution of battery levels is very close to this maximum entropy.

2.3.2 User charging behavior

In this section, we investigate user charging behavior across time and battery levels. We proceed using the fraction of our data in which a charging symbol is detected. Figure 2.6 shows the heat map of the distribution of charging phones, an equivalent to the 2-D PDF. The brighter the color, the higher the density. In our data set, over 13% of the charging phones have full battery. Many users do not unplug after their phone is fully charged. Since this fraction is too high compared to the rest, we exclude 100% battery level from Figure 2.6 for clarity.

First, let us consider the time dimension. It can be seen that the fraction of users with their phones plugged in drops significantly around 6 - 7 AM. This fraction stays low until around 3 PM. Afterwards, it raises up rapidly. This explains why the average amount of available battery stays above 50% despite usage. This is in accordance with what we expect from the typical user behavior.

A noteworthy observation can be drawn from the bottom half of Figure 2.6. We can see that from 3 PM - 12 AM, there are a larger portion of users with low battery charging their phones. This distinction is less clear at first but gradually exemplifies towards the end of the day. The high density at the bottom left corner of Figure 2.6 shows that there are many users who wait until the end of the day, when their phones run very low, before charging.

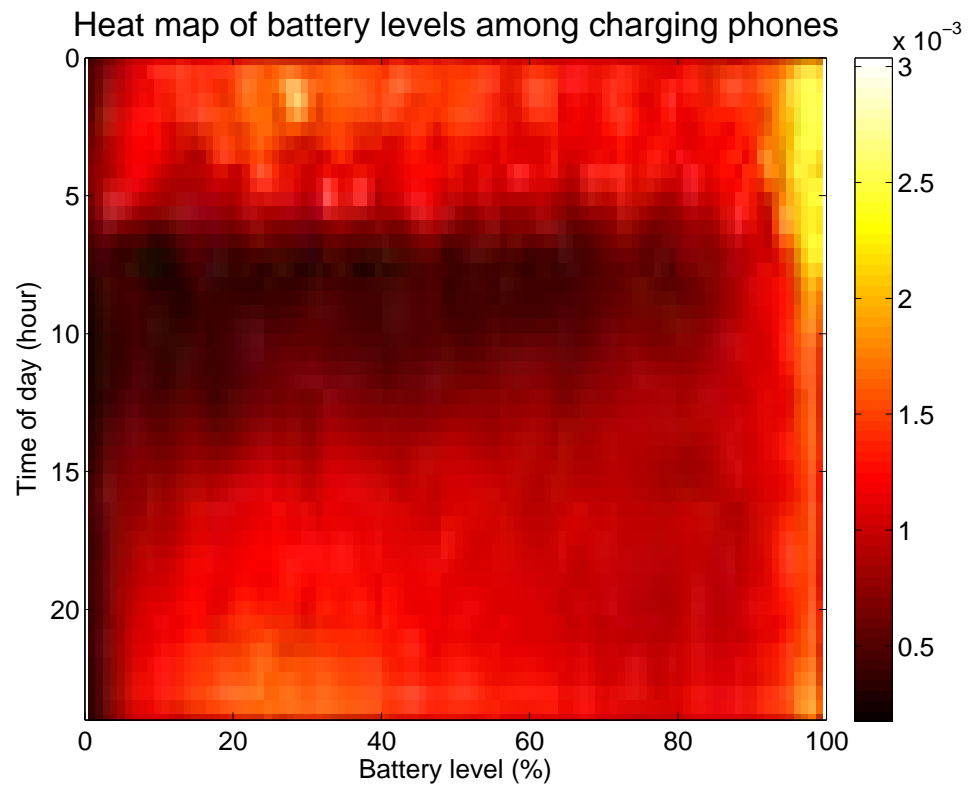


Figure 2.6: Heat map of battery levels among charging phones. The fraction of phones with 100% battery has been omitted for clarity.

2.4 Conclusions

In this chapter we have described our study on smartphone battery distribution over user population. It is clear from the obtained results that smartphone battery levels vary widely among users. Thus the *diversity of usage* phenomenon is confirmed. It is especially apparent in the later half of the day, where the entropy of the battery distribution approaches the maximum entropy of the uniform distribution. This period provides the best opportunities for our cooperative system.

We believe the findings discussed in this chapter can also be useful to other designers of cooperation systems utilizing smartphones. Like any other empirical studies, our results are likely to suffered from biases. We discussed in details three potential sources for biases. By thoroughly disclosing our data collection method, we hope to provide interested parties with enough information to decide how to best use our findings. All of our data are be made publicly available.

Chapter 3: Energy efficiency from device perspective:

Battery Deposit Service

3.1 Overview

In Chapter 2 we have discussed diversity of usage in cellular networks. In this chapter we will describe in detail a system which makes use of diversity of usage to improve smartphone energy efficiency.

Our system, called the “Battery Deposit Service” (BDS), makes use of D2D communications underlying LTE, to provide energy sharing in the form of load sharing. BDS allows users with high battery level to help relay traffic of users with low battery level through a D2D connection. Since the direct link costs much less power than the cellular link, the usage time of users with low battery level is prolonged. The cooperative selection criteria are designed carefully such that the amount of energy the helpers expend does not reduce their usage time to below their target usage. We introduce the notion of *valued battery*, defined as the battery of the smartphone when the user is active and does not have access to a power source. Similarly, *valueless battery* is defined as the battery of the smartphone when the user has access to a power source. In BDS, the helpers only spend valueless battery.

As a result, our system takes advantage of diversity of usage to raise the overall amount of valued battery in the network.

We develop BDS as a proximity service in LTE networks. There are four main technical areas that need to be addressed in developing our system. The first area is system architecture. This includes invoking appropriate entities within the Evolved Packet System (EPS) and developing signaling protocols for UEs to request and provide help. The second area is studying the utility of battery for the users to design cooperative criteria such that the overall network performance is improved. The third area is management of user incentive. The fourth area is accurate estimation of user target usage. Machine learning algorithms, assisted by a vast amount of user data, are continuing to produce better prediction [Chon et al., 2013]. In this chapter, we will assume that we receive accurate user target usages and address the first three areas.

3.1.1 Related work

We introduced the idea of our system in [Ta et al., 2014]. In that work, we used two widely accepted channel models, IST WINNER II model [Kyosti et al., 2007] and UMTS model [3GPP, 1998] to show that the power consumption in a D2D connection can be 3 to 4 orders of magnitude less than that of a cellular connection. Therefore, when a user (the *helper*) relays uplink traffic for another user (the *helpee*), the helper carries the cost of that communication session for the helpee. Effectively, the helper “transfers” some of his energy to the helpee. Equivalently, the helper

and helpee can be thought of as “depositing” energy into and “withdrawing” energy out of the network. The diversity of usage in the network ensures that with high probability, the helper will run low on battery at some other time and receive help. The depositing and withdrawing analogies are appropriate because they signify that the helping relationship needs not be immediate or reciprocal. The helper can receive help from a different user at a different time. These analogies give rise to the name of our system, the “Battery Deposit Service” (BDS).

We created a simulator (written in MATLAB) [Ta,] to evaluate the performance of BDS under some realistic channel, traffic, and mobility models. In [Ta et al., 2014], we formulated the cooperative decisions based only on the amount of available battery of the users. As discussed above, the target usage also plays an important role. We have improved our simulator to address both values in the design of cooperative rules.

D2D communications can operate on both unlicensed (out-of-band) and licensed spectrum (in-band). In BDS, we choose to use in-band D2D communications, which is also the preferred method by 3GPP. The main advantage of having D2D links on licensed spectrum is that interference can be managed. This leads to predictable performance of the D2D links. Moreover, in-band D2D connection setup can be transparent to the users. Since each device context has already been established with the cellular network, a secure D2D connection can be set up automatically (as opposed to manual pairing in Wifi and bluetooth). Since guaranteeing QoS and low-latency connection setup are a crucial features of our cooperative relay system, using in-band D2D communications is the nature choice.

Prior work on in-band D2D have been mainly concerned with interference management and resource allocation [Janis et al., 2009, Yu et al., 2011, Elkotby et al., 2012]. If done properly, they enable D2D connections to exist concurrently with regular cellular connections at “no cost”. In fact, through measurements on a wide spectrum range (20MHz - 6GHz) from 4 locations in Germany, Netherlands, California, [Kone et al., 2010] observes that on average, 50% of the spectrum is never used, 26% is only partially used. In particular, the cellular uplink bands (GSM and UMTS) are mostly idle because the uplink signals are very weak to be detected even with high-end spectrum analyzers. For BDS, it means that the D2D relay links can coexist with other cellular links with minimal impact on system throughput. In this chapter we will assume the eNodeB knows the optimal way to allocate resource for D2D links and focus on the energy sharing problem.

In order to utilize D2D communications in a systematic way, 3GPP created a work item named “Study on Proximity-based Services” (ProSe) for release 12 [3GPP, 2013]. To enable ProSe, changes need to be made on both network architecture, Non-access Stratum (NAS) and Access Stratum (AS) protocols. In [Raghothaman et al., 2013, Yang et al., 2013], additional logical entities are proposed in the Evolved Packet Core (EPC) to manage D2D-capable devices and ProSe applications. A new type of data bearer between D2D UEs, D2D bearer, is also proposed. Additional control signaling to manage D2D bearers is considered. We use these suggestions in developing our system architecture.

Even though not studied in cellular contexts, energy harvesting networks share some similarities with our utility analysis. In an energy harvesting network, nodes

rely on energy from some natural sources to operate. Since the amount of energy and the harvesting instants are usually random, the value of energy for a node changes over time. This characteristic is similar to our observation that the value of smart-phone battery is dependent upon both the amount and the time (with respect to the user target usage). Prior research on energy harvesting networks have proposed scheduling algorithms for nodes to adapt to their harvesting process [Kansal et al., 2007]. The goal is to control the energy expenditure to reduce the probability of exhausting available resource, thus disrupting network operations. In contrast to these work, in cellular context, the smartphones do not control the user usage. Therefore the research questions are fundamentally different. Usage, instead of being the output, is given as the input to BDS (in the form of some probabilistic model). The decision space is to find the best cooperative rules (instants and duration), given that model and the amount of available battery. In addition, nodes in energy harvesting networks are all under the designer’s control. In our case, the users need to be incentivized to cooperate.

Incentive schemes in wireless networks have been studied for over a decade. Most existing works aim to create an incentive system for nodes in a mobile ad-hoc network to forward packets from their neighbors [Buttayan and Hubaux, 2001, Anderegg and Eidenbenz, 2003, Chen and Chan, 2010, Duan et al., 2012]. Three main incentive mechanisms have been proposed: reputation, Tit-for-Tat, and currency. In a reputation system, each time a node cooperates truthfully, its reputation in the network is increased. Highly reputable nodes receive good service from others. Nodes with low reputation may be denied from participating. In a Tit-for-Tat

system, a pair of nodes take turn to perform services for each other in multiple rounds. Each node therefore has incentive to act honestly in fear of not getting service from the other in future rounds. In a currency system, nodes buy and sell services. The price of the service is determined by the market. The currency can either be real dollars or virtual.

Since in our case, we want a node to be able to interact with many other nodes, Tit-for-Tat is not suitable. Reputation works well in distributed systems, but the performance is hard to be predicted exactly. Currency fits our needs the best. It gives us an *exact* method to keep track of the transactions in the networks. The network plays a major role here, as a bank/moderator. In currency system without a central control entity, accounting is a major challenge. For virtual currency systems, the amount of virtual money is normally attached to each packet, protected by cryptographic measures. Not only does it incur processing overhead, cryptographic key distribution and management also poses as a big problem. Fake virtual money as well as double spending need to be taken into account as well. Some notable implementations of distributed virtual currency include Bitcoin [Nakamoto, 2009], Nuglets [Buttayan and Hubaux, 2001], and WhoPay [Wei et al., 2006].

3.1.2 Summary of contributions

Our contribution in this chapter is to identify new cooperative opportunities in cellular networks, by taking advantage of diversity of usage, to prolong battery life on mobile devices. We develop a proximity service as defined by 3GPP for UEs

to participate in cooperation.

1. System architecture: We identify responsible entities in the Evolved Packet System and develop signaling for service request and setup.
2. System cooperative rules: We propose a general framework to study utility of resource and apply that framework to our system. We show that by using appropriate utility thresholds as cooperative rules, the system performance can be guaranteed to improve.
3. User incentive: We consider currency systems that provide incentive for users to participate faithfully.

3.1.3 Outline of chapter

BDS system architecture is described in Section 3.2. In Section 3.3 we introduce a general framework to study utility of resource and apply it to BDS. We discuss user incentive in Section 3.4. We analyze BDS performance through simulation in Section 3.5. We conclude and discuss future work in Section 5.5.

3.2 System architecture

We envision Battery Deposit Service (BDS) as a Proximity Service (ProSe) in future releases of LTE. It is clear that to support ProSe, there need to be additional entities in EPC as well as new NAS and AS protocols [Raghothaman et al., 2013, Yang et al., 2013]. We assume that the Mobility Management Entity (MME) has an

additional function, *ProSe Management* (PSM), which manages D2D-related device capabilities, identifier allocation, connection establishment, mobility tracking, etc. We also assume there is an *Application Server* (AppSer) that communicates with the Policy and Charging Rules Function (PCRF) to enforce policy compliance for ProSe applications. The AppSer can make request to the PSM in the MME to setup D2D connections for ProSe applications.

We introduced the basic flow of BDS in [Ta et al., 2014]. In this work, we make use of the additional entities PSM and AppSer to propose a detail signaling procedure to set up a BDS cooperative relay session. This signaling procedure is illustrated in Figure 3.1. We consider an example where the helpee UE1 is associated with eNodeB1. The PSM, which manages UE1’s D2D connections, knows that UE1’s potential D2D peers are connected to eNodeB1 and eNodeB2. In this example, UE2, which is connected to eNodeB2, is selected to be the helper for UE1. The PSM notifies the serving gateway (S-GW) to update UE1’s data path, which changes from $UE1 \leftrightarrow eNodeB1 \leftrightarrow S-GW$ to $UE1 \leftrightarrow UE2 \leftrightarrow eNodeB2 \leftrightarrow S-GW$.

The overall procedure can be divided into three smaller subroutines: discovery, D2D bearer establishment, and BDS cooperative relay.

Discovery

1. The helpee UE1, under some conditions, decides to request for BDS service. It sends `BDSInitSerReq` to the PSM inside the MME.
2. The PSM forwards the request, together with UE1 ID, to the AppSer in the form of `BDSSerReq`.

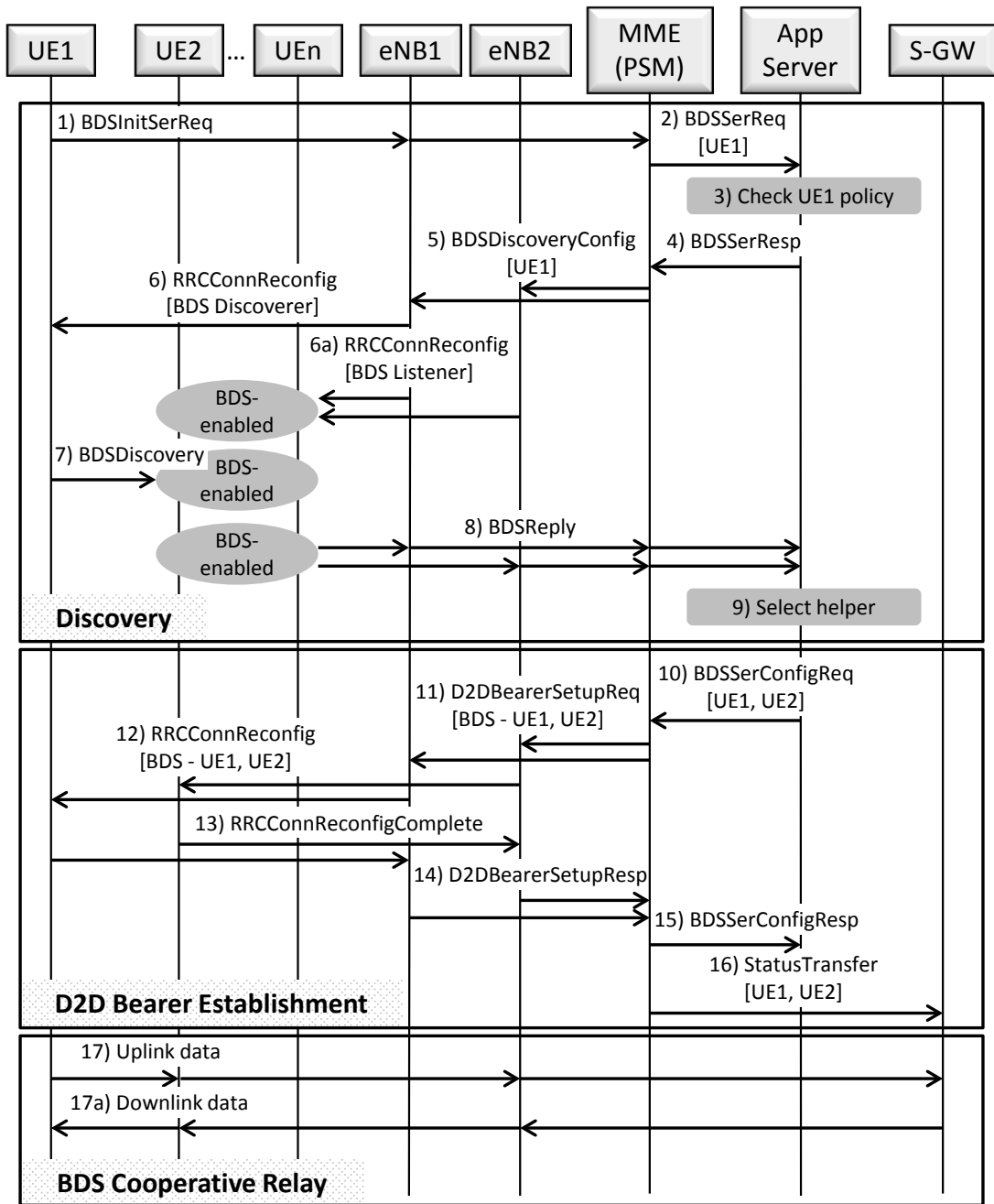


Figure 3.1: Signaling flow for establishment of a BDS cooperative relay session. UE1 is the helpee, UE2 is the selected helper.

3. The AppSer checks UE1 policy (by contacting the PCRF) to decide if UE1 is allowed to use BDS service.
4. Once confirmed, it sends a response `BDSerResp` to the PSM.
5. The PSM sends `BSDDiscoveryConfig` message with the helpee ID (UE1) to eNodeB1 and eNodeB2.
6. eNodeB1 and eNodeB2 agree on a time/frequency resource for a BDS discovery signal and send this information to UE1 (the discoverer) through a `RRConnReconfig` message. (6a) This time/frequency resource is also sent to all BDS-enabled UEs within their cells (the listeners) through `RRConnReconfig` messages. We envision that there can be a group control message format to make this process more efficient.
7. UE1 sends the discovery signal `BSDDiscovery`.
8. The subset of listeners who were able to hear UE1's `BSDDiscovery` send their replies, in the form of `BDSReply` messages, to the PSM. The PSM forwards them to the AppSer.
9. `BDSReply` messages contain information required by the AppSer to select the optimal helper for UE1. Some possible decision rules include
 - Max-battery: in `BDSReply`, the UEs include their remaining battery levels. The AppSer selects the UE with highest remaining battery to help.
 - Proximity: in `BDSReply`, the UEs include the received signal strength of

UE1's `BSDDiscovery` signal. The `AppSer` selects the UE with highest received signal strength (i.e. it is closest to UE1).

- **Currency:** to ensure fairness and manage user incentive, a currency system is set up by the `AppSer`. The selection rule in this system is discussed in Section 3.4.

Let UE2 be the chosen helper. At the end of the discovery phase, the helper/helpee association is determined.

D2D Bearer Establishment

10. The `AppSer` sends a request, `BDSerConfigReq`, to the PSM to create a D2D connection for BDS with UE1 and UE2 IDs.
11. The PSM sends `D2DBearerSetupReq` to request `eNodeB1` and `eNodeB2` to allocate resource for a D2D connection between UE1 and UE2. The QoS of the D2D connection can also be included.
12. `eNodeB1` and `eNodeB2` send `RRConnReconfig` commands to UE1 and UE2 to inform them of the D2D resource.
13. UE1 and UE2 confirm that they are ready to use the allocated resource for D2D communications by sending `RRConnReconfigComplete`.
14. `eNodeB1` and `eNodeB2` inform the PSM that the D2D bearer setup is complete by sending `D2DBearerSetupResp`.

15. The PSM informs the AppSer that the BDS service configuration is complete by sending `BDSSerConfigResp`.
16. The PSM informs the S-GW to update UE1's status by sending `StatusTransfer`. Future IP data packets to UE1 should be routed through eNodeB2.

At the end of the D2D bearer establishment, UE2 is ready to relay UE1's data traffic.

BDS Cooperative Relay

17. During the cooperative session, UE1's data path is updated to UE1 \leftrightarrow UE2 \leftrightarrow eNodeB2 \leftrightarrow S-GW.

3.3 Cooperative rules

BDS system architecture allows the UEs to request for service whenever they want. The potential helpers can also choose when they want to respond to `BDSDiscovery`. Intuitively, we want the UEs to only request for service when they cannot satisfy their own usage demand. At the same time, the UEs should only respond to help requests if doing so does not hurt their ability to meet their target usage. In this section, by studying battery utility for the UEs, we design cooperative rules to enforce those behaviors.

BDS belongs to a general class of systems in which the resource for each user is generated and/or consumed according to some random processes. Because of the randomness, there are possibilities that the available resource of some users

cannot meet their consumption requests. At the same time, other users may have unused resource. Therefore the users can benefit from resource transferring among themselves. We start with a general framework to study resource utility and apply that utility analysis to design cooperative rules. We then study BDS as a specific case.

3.3.1 General utility analysis framework

Our framework considers a system in which the users consume a limited amount of resource over time. The system has two main characteristics

- The resource consumption or the resource generation, or both, are random
- Resource can be transferred between users according to a transfer graph

The goal of the users is to satisfy the resource consumption, given the resource generation process. We use the notion of a target usage duration to study user utility. The target usage duration is the period until the next arrival of resource. Given the current amount of available resource, the utility for a user is related to his ability to meet this usage.

We first introduce an example of another system that fits our framework. We then define our terminology. Next, we discuss user performance in term of utility. Using utility, we consider conditions in which cooperation is beneficial for participants. Finally, we consider two broad categories of systems and two specific utility functions that are appropriate to those categories.

3.3.1.1 Example: Renewable energy system for cloud computing

Cloud computing, or utility computing, offers a way to increase computing capacity and add capabilities on the fly without investing in new infrastructure. Cloud service providers such as Amazon, Google, Microsoft have very large data centers that allow them to easily perform dynamic provisioning of computing and networking resources. However, these concentrated centers pose huge energy concerns [Berl et al., 2010]. An alternative approach is to distribute computing power over a large number of smaller sites, and to dispatch energy as demanded to these sites, rather than to guarantee a high level of available power at all time [Gelenbe, 2012].

Consider a network of geographically distributed renewable energy sources and the small or large data centers that are the energy consumers, as illustrated in Figure 3.2. Each energy source has a finite energy storage capacity. A distribution network connects these sites. For simplicity, let us assume that each energy source is responsible for a number of energy consumers. The energy consumers which are connected with multiple energy sources can be thought of as several virtual consumers, each connects to an energy source and have proportional energy consumption demand.

The goal of the network is to use as much renewable energy as possible before having to resort to conventional backup sources. Since renewable energy generation is in general random, and the computational demand in the data centers are also random, this energy distribution system fits into our framework. The distribu-

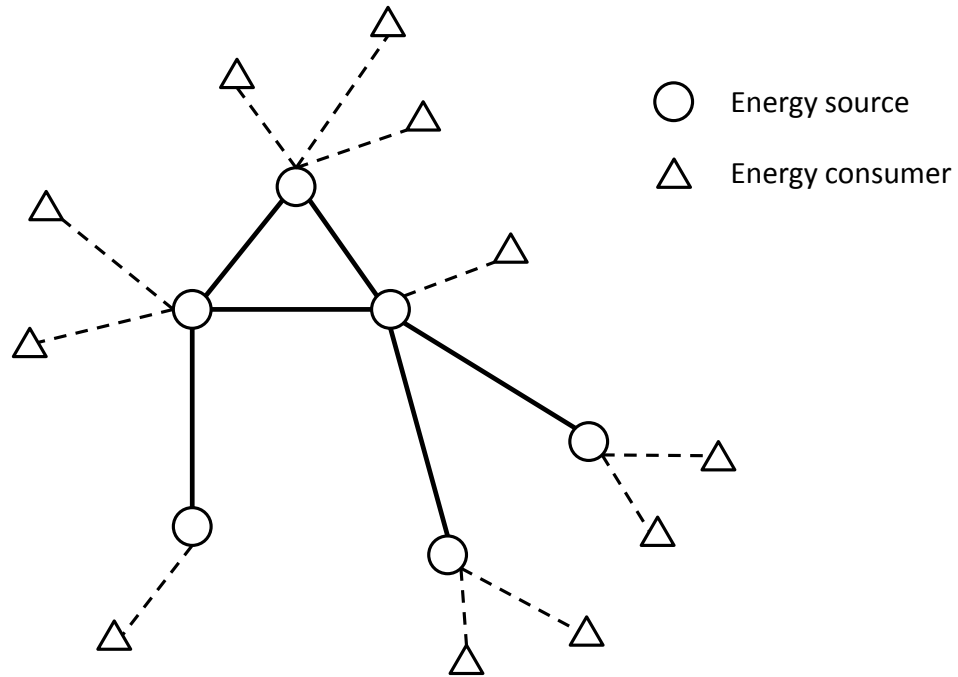


Figure 3.2: Renewable energy system providing energy to computing sites.

tion network creates a graph according to which energy can be transferred between sources. For a solar energy harvesting source, the target usage duration could be the time until the next sunny day. For a wind farm, the target usage duration could be the period of the wind speed fluctuation process.

3.3.1.2 Terminology

Let us consider a system with multiple users, indexed by $i = 1, 2, \dots$. At each instance, the state of user i consists of the following quantities

- B_i : the amount of remaining resource, $B_i \geq 0$.

- T_i : the target usage duration, $T_i \geq 0$.
- L_i : the parameter for the resource consumption process.

From those instantaneous state variables, the following future quantities can be derived

- $\zeta_{L_i}(\tau)$: the amount of resource consumed for usage duration τ , given the parameter L_i . $\zeta_{L_i}(\tau)$ is a random process, $\forall L, \forall \tau \geq 0 : \zeta_L(\tau) \geq 0$.
- T_{O_i} : the duration until the resource runs out (*time until outage*). T_{O_i} is a random variable which satisfies $\zeta_{L_i}(T_{O_i}) = B_i$. $T_{O_i} \geq 0$.
- T_{V_i} : the amount of valued usage time. Valued usage time is smaller of the time until outage and the target usage. T_{V_i} is a random variable defined as $T_{V_i} = \min(T_i, T_{O_i})$. $T_{V_i} \geq 0$.

Subsequently, we will drop the subscript i when it is clear from the context that we are talking about a general user.

3.3.1.3 User utility

Since the users have limited resource, there is a possibility that they do not meet their target usage. The likelihood of this possibility depends on future resource consumption. In this framework, we will consider users to receive maximum utility if their target usage is met. In the case where the users' target usage is not met, their utility depends on the specific type of resource and application. We investigate

two broad categories of applications in subsequent sections. First, we discuss some properties of a general utility function.

We consider users with higher utility to be in better states. For the same target usage, more resource gives better utility. Similarly, with the same level of remaining resource, the user with shorter target usage has higher utility. Therefore, the utility function has to be monotonically non-decreasing in B and monotonically non-increasing in T . In other words,

$$u(B_1, T, L) \geq u(B_2, T, L) \quad \text{for } B_1 \geq B_2 \quad (3.1)$$

$$u(B, T_1, L) \geq u(B, T_2, L) \quad \text{for } T_1 \leq T_2 \quad (3.2)$$

Through cooperation, resource can be transferred between users, which alters the time until outage for both parties. The novelty in our approach is the consideration of the target usage time T . In Figure 3.3 we show an example of a utility function for visualization. The resource B and target usage duration T are normalized to some B^* and T^* . The values of B^* and T^* are not important for the current discussion. Here we are only interested in the shape of the utility surface. A user i with low resource (B_i small), but requires usage for only a short duration (T_i small) can have higher utility than a user j with more resource (B_j large), but also requires usage for a long period (T_j large). As a result, user i can potentially provide more help than user j . This way we utilize cooperative opportunities that otherwise were not available in previous frameworks that only consider the amount of available resource B .

Any utility function needs to have the following properties

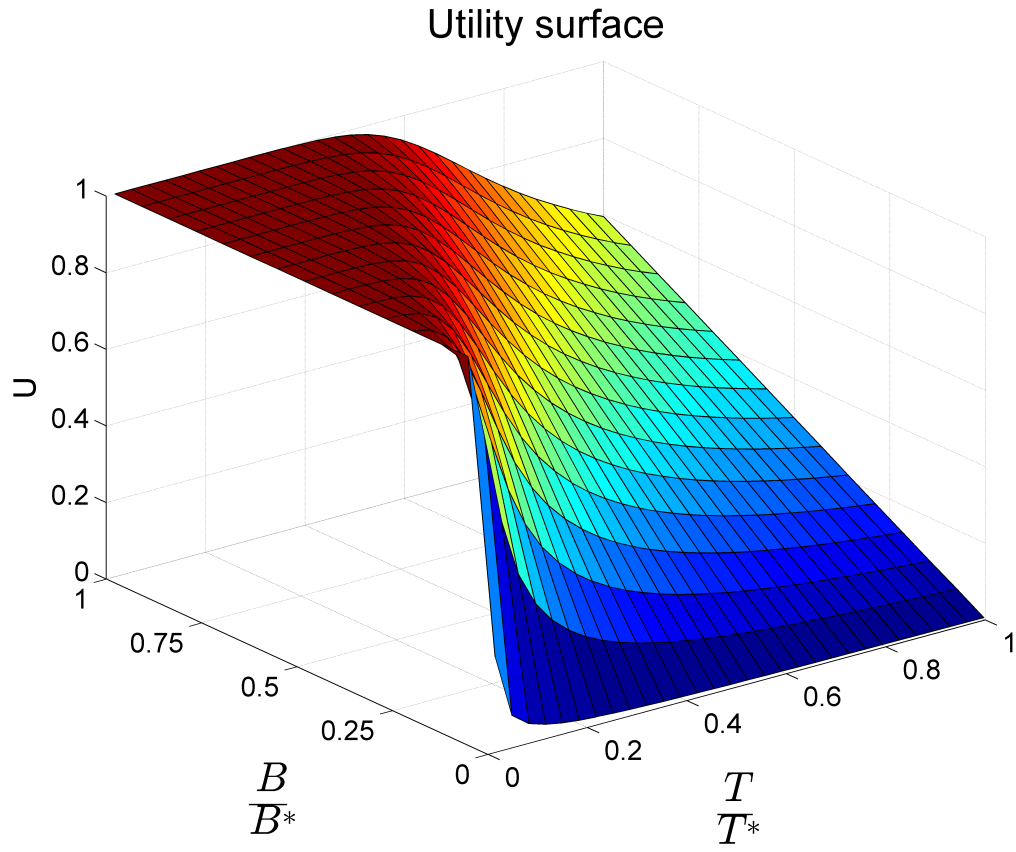


Figure 3.3: A sample utility surface. The resource B and target usage duration T are normalized. Following a curve with constant target usage time, the utility function increases with B - property (3.1). Following a curve with constant resource, the utility function decreases with T - property (3.2).

- P1. Ease of computing: The users need to monitor their utility frequently, therefore the utility calculation should be very fast.
- P2. Ease of deriving cooperation rules: The purpose of the utility function is to determine cooperation rules for the users. Therefore, a good utility function simplifies these rules.

3.3.1.4 Beneficial cooperation

Let us consider a cooperative session in which user i is the helpee and user j is the helper. The cooperative session has duration T_c . During this session, the helper transfers an amount of resource, $\Delta B_{ji} \geq 0$, to the helpee. The resource transferring loss is denoted δ_{ji} . Without loss of generality, the transferring loss is associated with the helpee. Table 3.1 illustrates the condition of the helper and helpee before and after cooperation.

Definition 1. A cooperative session is **beneficial** if the total utility with cooperation is at least the total utility without cooperation.

$$\begin{aligned}
& u_i(B_i - \zeta_{L_i}(T_c) + \Delta B_{ji} - \delta_{ji}, T_i - T_c, L_i) \\
& \quad + u_j(B_j - \zeta_{L_j}(T_c) - \Delta B_{ji}, T_j - T_c, L_j) \\
& \geq u_i(B_i - \zeta_{L_i}(T_c), T_i - T_c, L_i) \\
& \quad + u_j(B_j - \zeta_{L_j}(T_c), T_j - T_c, L_j). \tag{3.3}
\end{aligned}$$

Equivalently, the cooperative utility gain of the helpee is, in magnitude, at least

Table 3.1: Target usage duration and remaining resource of the helper and helpee before and after cooperation

		Helpee (i)		Helper (j)	
		Target usage	Remaining resource	Target usage	Remaining resource
Before		T_i	B_i	T_j	B_j
After	Non-coop		$B_i - \zeta_{L_i}(T_c)$		$B_j - \zeta_{L_j}(T_c)$
	Coop	$T_i - T_c$	$B_i - \zeta_{L_i}(T_c) + \Delta B_{ji} - \delta_{ji}$	$T_j - T_c$	$B_j - \zeta_{L_j}(T_c) - \Delta B_{ji}$

equal to the cooperative utility loss of the helper.

$$\begin{aligned}
& u_i(B_i - \zeta_{L_i}(T_c) + \Delta B_{ji} - \delta_{ji}, T_i - T_c, L_i) \\
& \quad - u_i(B_i - \zeta_{L_i}(T_c), T_i - T_c, L_i) \\
& \geq u_j(B_j - \zeta_{L_j}(T_c), T_j - T_c, L_j) \\
& \quad - u_j(B_j - \zeta_{L_j}(T_c) - \Delta B_{ji}, T_j - T_c, L_j). \tag{3.4}
\end{aligned}$$

If the system is designed such that only beneficial cooperative sessions are allowed, the overall utility of the network will increase in cooperation.

Lemma 1. A necessary condition for a cooperative session to be beneficial is that the resource transferring loss is no greater than the amount of resource transferred by the helper.

$$\delta_{ji} \leq \Delta B_{ji}. \tag{3.5}$$

Proof. Since the consumption process $\zeta_L(\cdot)$ is non-negative, and the utility function is monotonically non-decreasing in B , the helper will never gain utility after a cooperative session

$$\begin{aligned} & u_j(B_j - \zeta_{L_j}(T_c), T_j - T_c, L_j) \\ & - u_j(B_j - \zeta_{L_j}(T_c) - \Delta B_{ji}, T_j - T_c, L_j) \geq 0. \end{aligned} \quad (3.6)$$

From (3.4)

$$\begin{aligned} & u_i(B_i - \zeta_{L_i}(T_c) + \Delta B_{ji} - \delta_{ji}, T_i - T_c, L_i) \\ & - u_i(B_i - \zeta_{L_i}(T_c), T_i - T_c, L_i) \geq 0. \end{aligned} \quad (3.7)$$

(3.5) follows from property (3.1) of the utility function. \square

In a beneficial cooperative session, if the transferring loss is positive, the total amount of resource consumed is greater than that of the non-cooperative case. However, by definition, the total utility is improved. This is achieved because the helper and the helpee are on different operating points with respect to their utilities. For the case where the cooperative session length is much smaller than the target usage time of both users, $T_c \ll T_i, T_j$, from (3.4) we see that the helpee must be operating on a “steeper” resource-slope than the helper. In other words,

$$\frac{\partial}{\partial B} u_i(B_i, T_i, L_i) > \frac{\partial}{\partial B} u_j(B_j, T_j, L_j). \quad (3.8)$$

As a result, a larger change in resource for the helper results in a smaller change in utility. This knowledge can be used to design cooperative rules.

3.3.1.5 Two categories of systems

In this section we discuss two broad categories of systems and the appropriate utility function for each category.

C1. The users only concern with whether or not their task is done (all or nothing).

If a user's target usage is satisfied, he receives utility 1, otherwise he receives utility 0.

C2. The users concern with the amount of usage they receive, up to the target usage. Users whose target usage is met receive maximum utility. Whereas users whose target usage is not met receive utility proportional to their usage time. Another way to think about this category is that if the users do not meet their target usage, they incur a cost proportional to the amount of time they come short. Users who meet their target usage have zero cost.

We consider two utility functions, one for each category of systems, and their computational complexity. As discussed in Section 3.3.1.3, it is desirable that a utility function is easy to compute.

Category C1 - Probability of survival

For users who receive utility 1 when their usage is satisfied, and utility 0 otherwise, the *probability of survival*, $\mathbb{P}[T_O > T]$, is their expected utility. First we define *probability of outage*, the probability that a user (with state B, T, L) will run out of

resource before his target usage

$$P_O = \mathbb{P}[T_O \leq T] = \mathbb{P}[\zeta_L(T) \geq B]. \quad (3.9)$$

The utility function is thus

$$u_1(B, T, L) = 1 - P_O. \quad (3.10)$$

Category C2 - Expected valued usage time

For this category, the expected amount of valued usage time as a fraction of the target usage time, $\mathbb{E}[T_V]/T$, is a good performance metric. The reason for normalization can be better understood by an example. Let us consider user A who wants to use his phone for 4 hours without charging. If his expected valued usage time is 3 hours, his utility will be 0.75. User B with a 2-hour target usage but only 1 hour of expected valued time has utility 0.5. Notice that in both cases, the user needs 1 extra hour to meet his target usage. The fact that user A has higher utility illustrates that one hour is not worth as much for him as it is for user B. This is justified considering that user A has a larger amount of target usage compared to user B.

The expected usage time is

$$\begin{aligned}\mathbb{E}[T_V] &= \mathbb{E}[\min(T_O, T)] \\ &= \int_0^T \tau f_{T_O}(\tau) d\tau + \int_T^\infty T f_{T_O}(\tau) d\tau \\ &= \mathbb{E}[T_O] - \int_T^\infty (\tau - T) f_{T_O}(\tau) d\tau\end{aligned}\tag{3.11}$$

$$= T - \int_0^T (T - \tau) f_{T_O}(\tau) d\tau.\tag{3.12}$$

The utility function for this category of users is defined as

$$u_2(B, T, L) = \frac{\mathbb{E}[T_V]}{T}.\tag{3.13}$$

Here $f_{T_O}(\cdot)$ denotes the PDF of the time until outage, the CDF of which is given by the consumption process

$$\mathbb{P}[T_O \leq \tau] = \mathbb{P}[\zeta_L(\tau) \geq B].\tag{3.14}$$

Computation of $u_1(\cdot)$ and $u_2(\cdot)$

It can be easily verified that both $u_1(\cdot)$ and $u_2(\cdot)$ satisfy (3.1) and (3.2). Moreover, we can see that both utility functions depend crucially on the time until outage T_O , which in turn depends on the consumption process $\zeta_L(\cdot)$. Therefore, the computational speed of these utility functions also depends on the underlying consumption process. While there are no closed-form expressions for $u_1(\cdot)$ and $u_2(\cdot)$ for a general consumption process, we discuss a few cases where efficient approximations can be used to speed up the computation.

First we consider the two extremes. If the user's resource is very high compared to his target usage, i.e. the distribution of T_O increases much slower than linear

before the target usage, then he is very unlikely to go into outage: $P_O \approx 0$. In this case the target usage dominates in calculation of the valued usage time. (3.12) can be used to approximate $\mathbb{E}[T_V]$.

If $(T - \tau)f_{T_O}(\tau) \approx 0$ for $\tau \leq T$:

$$u_1 = 1 - P_O \approx 1 \quad (3.15)$$

$$u_2 = \frac{\mathbb{E}[T_V]}{T} \approx 1. \quad (3.16)$$

Similarly, if the user's resource is very low compared to his target usage, i.e. the distribution of T_O decreases much faster than linear after the target usage, then he is very likely to go into outage: $P_O \approx 1$. Whereas the time until outage dominates in the calculation of the valued usage time. (3.11) can be used to approximate $\mathbb{E}[T_V]$.

If $(\tau - T)f_{T_O}(\tau) \approx 0$ for $\tau \geq T$:

$$u_1 = 1 - P_O \approx 0 \quad (3.17)$$

$$u_2 = \frac{\mathbb{E}[T_V]}{T} \approx \frac{\mathbb{E}[T_O]}{T}. \quad (3.18)$$

Outside of the two extremes, a special case where the utility functions can be efficiently approximated is when the consumption process is Gaussian. In other words, $\zeta_L(\tau) \sim \mathcal{N}(\mu_L(\tau), \sigma_L^2(\tau))$. From (3.14), the CDF of time until outage is

$$\mathbb{P}[T_O \leq \tau] = \mathbb{P}[\zeta_L(\tau) \geq B] = \Phi\left(\frac{\mu_L(\tau) - B}{\sigma_L(\tau)}\right). \quad (3.19)$$

Where $\Phi(\cdot)$ denotes the standard Normal CDF. The probability of survival is simply

$$u_1 = 1 - \Phi\left(\frac{\mu_L(T) - B}{\sigma_L(T)}\right) = \Phi\left(\frac{B - \mu_L(T)}{\sigma_L(T)}\right). \quad (3.20)$$

If the mean of the consumption process scales linearly with the duration, i.e.

$\mu_L(\tau) = \lambda_L \tau$, then

$$\mathbb{P}[T_O \leq \tau] = \Phi \left(\frac{\tau - B/\lambda_L}{\sigma_L(\tau)/\lambda_L} \right). \quad (3.21)$$

By approximating τ in $\sigma_L(\tau)$ by B/λ_L , we get $\sigma_L(\tau)/\lambda_L \approx \sigma_L(B)$. Denote $\mu_L(B) = B/\lambda_L$, (3.21) becomes

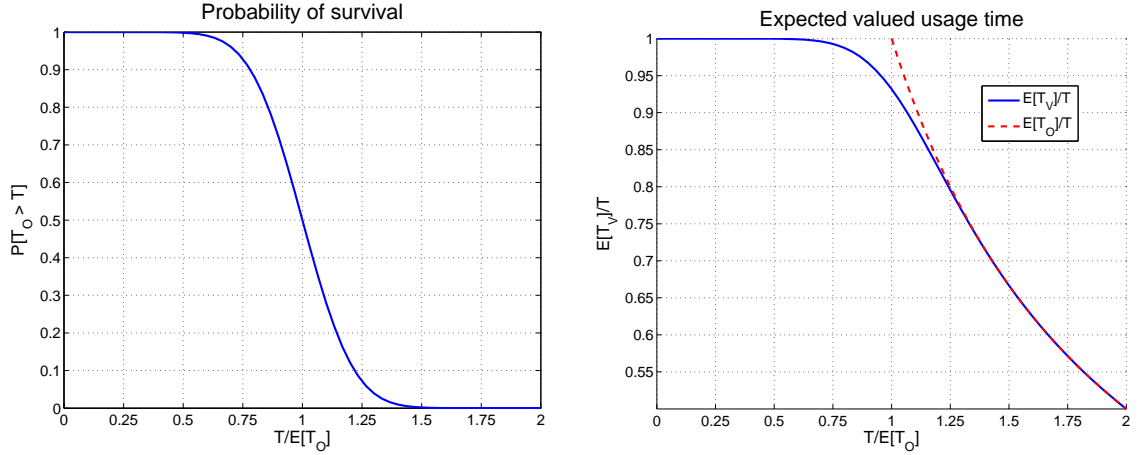
$$\mathbb{P}[T_O \leq \tau] \approx \Phi \left(\frac{\tau - \mu_L(B)}{\sigma_L(B)} \right). \quad (3.22)$$

As a result, the time until outage can be approximated as having a Gaussian distribution $\mathcal{N}(\mu_L(B), \sigma_L^2(B))$. The calculation of expected valued usage time according to (3.12) becomes (see Appendix)

$$\begin{aligned} \mathbb{E}[T_V] \approx & T - (T - \mu_L(B)) \Phi \left(\frac{T - \mu_L(B)}{\sigma_L(B)} \right) \\ & + \frac{\sigma_L(B)}{\sqrt{2\pi}} \left(e^{-\frac{\mu_L(B)^2}{2\sigma_L(B)^2}} - e^{-\frac{(T - \mu_L(B))^2}{2\sigma_L(B)^2}} \right). \end{aligned} \quad (3.23)$$

With the closed forms (3.20) and (3.23), the utility functions can be computed efficiently.

Figure 3.4 illustrates the two utility functions when the consumption process is Gaussian. The utility functions are plotted against the target usage duration T while fixing the amount of available resource B . The mean usage duration, $\mathbb{E}[T_O]$, is used as the reference. For both utility functions, we can see clearly the two discussed extremes. At their lower (higher) extreme, u_1 is very close to 1 (0), whereas u_2 is very close to 1 ($\mathbb{E}[T_O]/T$).



(a) C1 - Probability of survival (3.20) (b) C2 - Expected valued usage time (3.23)

Figure 3.4: Utility as functions of target usage time for user categories C1 and C2. The amount of available resource is fixed. Both utility functions show two clear extremes.

3.3.2 Battery Deposit Service

In this section, we apply the previous framework for mobile UEs in a BDS system. The resource here is the communication energy budget of the UEs. When we talk about the battery of a user, we refer to the communication energy budget. As discussed in [Ta et al., 2014], uplink transmission power dominates other communication-related components in term of energy consumption. Therefore we will only consider the uplink transmission power in the theoretical analysis. Other factors such as idle circuit power and downlink reception power are considered in simulation. As seen in Section 3.3.1, the main component of the system is the battery consumption process $\zeta_L(t)$.

3.3.2.1 Battery consumption process $\zeta_L(t)$

First, we describe the uplink power consumption of UEs in LTE networks. We then introduce the user's data traffic model. These two components make up the battery consumption process.

LTE uplink power control

The battery consumption for the UEs follows LTE uplink power control [Baker, 2011, 3GPP, 2011c]. The uplink transmission power in dB is

$$P_{\text{UL}} = \underbrace{P_0 + \alpha\text{PL}}_{\text{open-loop}} + \underbrace{\Delta_{\text{TF}} + f(\Delta_{\text{TPC}})}_{\text{dynamic offset}} + 10 \log_{10}(M). \quad (3.24)$$

P_{UL} consists of two components. The first component depends on the state of the UE with respect to the eNodeB. This component is further comprised of two subcomponents: a basic open-loop operating point and a dynamic offset. The second component depends on the amount of uplink data, which is realized in term of M , the number of allocated resource blocks. A resource block (RB) is the basic unit of time-frequency resource allocation in LTE. It consists of 12 OFDM subcarriers (for the total bandwidth of 180 kHz with 15 kHz subcarrier spacing) over one slot (0.5 ms).

P_0 is a semi-static nominal power level set by the eNodeB. αPL is the path loss compensation component, where α controls the degree of compensation. PL is derived from the downlink Reference Signal Received Power. It includes shadowing but not fast fading. The dynamic control of UE uplink transmit power is designed

to be an offset from the base operating point. This offset depends on two factors: the allowed modulation and coding scheme (TF stands for Transport Format) and a UE-specific transmitter power control (TPC) command.

While P_0 , PL as well as the dynamic control of P_{UL} change over time, a complete model of these quantities depends on many factors such as user movement, traffic load within the cell, eNodeB strategy etc. In this work, we use instantaneous values of these quantities in the formulation of the consumption process. Each time a UE computes its utility, it updates these quantities.

The battery consumption process is

$$\zeta_L(t) = 10^{\frac{P_0 + \alpha PL + DO}{10}} M(t) = \rho_0 M(t), \quad (3.25)$$

where DO is the dynamic offset. $M(t)$ is the data arrival process, in unit of resource blocks.

Traffic model

We model $M(t)$ as a Poisson burst process with rate λ . Each burst size is modeled as a geometric random variable with parameter ν . Poisson processes are commonly used in traffic modeling because they capture well the aggregate traffic caused by a large number of sources (e.g. applications in a smartphone). Similar models were used by Nokia and Renesas Mobile Europe in their recent 3GPP contributions [Nokia Corporation, 2012, Renesas Mobile Europe Ltd., 2012].

Let us denote the Poisson arrival process $N(t)$, and the size of each arrival M (in resource blocks). M is assumed i.i.d. between different arrivals.

We have, for $n \geq 0$

$$\mathbb{P}[N(t) = n] = \frac{(\lambda t)^n}{n!} e^{-\lambda t}, \quad (3.26)$$

and for $m \geq 1$

$$\mathbb{P}[M = m] = (1 - \nu)^{m-1} \nu. \quad (3.27)$$

From (3.25),

$$\zeta_L(t) = \rho_0 M(t) = \rho_0 \sum_{i=1}^{N(t)} M_i \quad (3.28)$$

$\zeta_L(t)$ is a Poisson burst process with rate λ and takes values as integer multiples of ρ_0 . As a result, we can discretize the battery using ρ_0 as a basic unit.

As seen in Section 3.3.1, computing the distribution of the time until outage, $\mathbb{P}[T_O \leq t]$, is the most important task for the utility methods of BDS. In the following section, we discuss in detail this computation.

3.3.2.2 Distribution of time until outage T_O

In this section we describe two methods to compute exactly the CDF of T_O and an approximation for quick calculation.

Stochastic analysis

Recall that for a UE with state (B, T, L) , $\mathbb{P}[T_O \leq t] = \mathbb{P}[\zeta_L(t) \geq B]$. From (3.28), with the available battery B written as multiples of ρ_0 , we can write the compliment

of the CDF of T_O as

$$\begin{aligned}
\mathbb{P}[T_O \geq t] &= \mathbb{P}[\zeta_L(t) \leq B] \\
&= \sum_{n=0}^{\infty} \mathbb{P}[N(t) = n] \mathbb{P}\left[\sum_{i=1}^n M_i \leq B\right] \\
&= \sum_{n=0}^B \mathbb{P}[N(t) = n] \mathbb{P}\left[\sum_{i=1}^n M_i \leq B\right]. \tag{3.29}
\end{aligned}$$

Since M_i are i.i.d. $\text{geometric}(\nu)$ random variables, we can think of $\sum_{i=1}^n M_i$ as the total number of Bernoulli trials before the first n successes. Each Bernoulli trial has success probability ν . Since each $M_i \geq 1$, $\mathbb{P}[\sum_{i=1}^n M_i \leq B] = 0$ for $n > B$.

For $n \leq B$, we have

$$\begin{aligned}
&\mathbb{P}\left[\sum_{i=1}^n M_i = B\right] \\
&= \underbrace{\binom{B-1}{n-1}}_{\text{first } n-1 \text{ successes in } B-1 \text{ trials}} (1-\nu)^{B-n} \underbrace{\nu}_{\text{last success}} \nu^{n-1}. \tag{3.30}
\end{aligned}$$

This is the probability mass function of a negative binomial random variable $\text{NB}(n, \nu)$.

The CMF of which is

$$\mathbb{P}\left[\sum_{i=1}^n M_i \leq B\right] = \sum_{k=n}^B \binom{k-1}{n-1} (1-\nu)^{k-n} \nu^n \tag{3.31}$$

$$= \sum_{j=n}^B \binom{B}{j} (1-\nu)^{B-j} \nu^j \tag{3.32}$$

$$= I_\nu(n, B-n+1), \tag{3.33}$$

(3.31) can be interpreted as while fixing the number of success n we sum over the cases when the total number of trials is at most B . (3.32) can be interpreted as

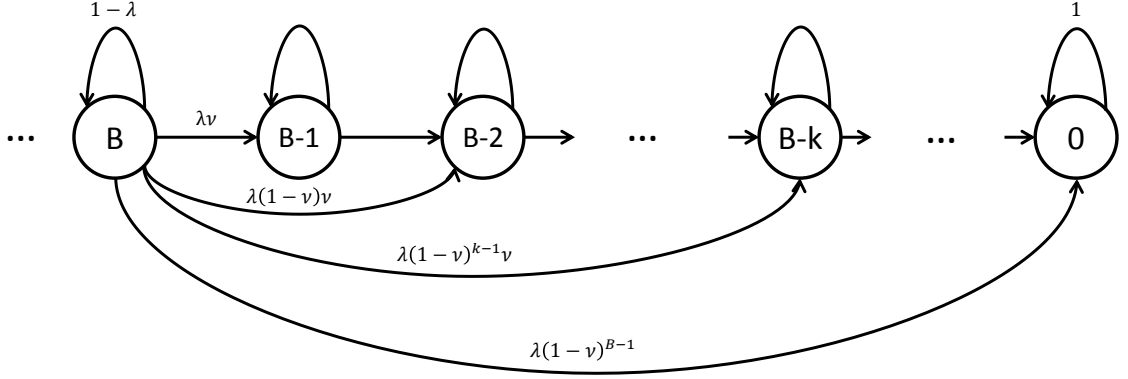


Figure 3.5: Continuous time Markov Chain for remaining battery states

while fixing the total number of trials B , we sum over the cases when the number of successes are at least n . $I_\nu(\cdot, \cdot)$ is the regularized incomplete beta function, whose expression is given in (3.32) [NIST, 2014].

Plugging (3.33) into (3.29) we have

$$\begin{aligned}
 \mathbb{P}[T_O \leq t] &= 1 - \mathbb{P}[T_O \geq t] \\
 &= 1 - \sum_{n=0}^B \frac{(\lambda t)^n}{n!} e^{-\lambda t} I_\nu(n, B - n + 1). \tag{3.34}
 \end{aligned}$$

Markovian analysis

We can see that $\zeta_L(t)$ is a jump process, therefore it can be analyzed under Markovian theory. The state space is discrete, with each state being the number of remaining battery units. As a result, we have a homogeneous continuous time Markov Chain as shown in Figure 3.5.

Let the state variable be $X \in \mathbb{N}$, the transition probability is defined as

$$p_{ij}(t) = \mathbb{P}[X(t) = j | X(0) = i], \quad i, j \in \mathbb{N}. \tag{3.35}$$

From (3.30) and (3.33), we have

$$\left\{ \begin{array}{l} p_{00}(t) = 1, \\ p_{ii}(t) = e^{-\lambda t}, \quad i > 0 \\ p_{ij}(t) = \sum_{n=1}^{i-j} \frac{(\lambda t)^n}{n!} e^{-\lambda t} \binom{i-j-1}{n-1} (1-\nu)^{i-j-n} \nu^n, \quad i > j > 0 \\ p_{i0}(t) = \sum_{n=1}^{\infty} \frac{(\lambda t)^n}{n!} e^{-\lambda t} (1 - I_{\nu}(n, i-n)), \quad i > 0 \\ p_{ij}(t) = 0, \quad i < j \end{array} \right. \quad (3.36)$$

Define the *local characteristics* for any state i

$$q_i = \lim_{h \rightarrow 0} \frac{1 - p_{ii}(h)}{h}, \quad (3.37)$$

and for any pair of states $i \neq j$

$$q_{ij} = \lim_{h \rightarrow 0} \frac{p_{ij}(h)}{h}. \quad (3.38)$$

For the Poisson arrival process, as time duration $h \rightarrow 0$, the probability of having 2 or more arrivals during h vanishes. Therefore we only need to account for $n = 1$ in the third and fourth terms of (3.36). Taking the limits, we get

$$\left\{ \begin{array}{l} q_{0,j} = 0, \quad \forall j \\ q_i = \lambda, \quad i > 0 \\ q_{ij} = \lambda(1-\nu)^{i-j-1} \nu, \quad i > j > 0 \\ q_{i0} = \lambda(1-\nu)^{i-1}, \quad i > 0 \end{array} \right. \quad (3.39)$$

The last equation of (3.39) is derived by plugging in $n = 1$ in the fourth equation of (3.36) and using the following properties of the regularized incomplete beta function [NIST, 2014].

$$\begin{aligned}
1 - I_\nu(1, i - 1) &= I_{1-\nu}(i - 1, 1) \\
&= \nu \sum_{j=i-1}^{\infty} (1 - \nu)^j \\
&= (1 - \nu)^{i-1}
\end{aligned} \tag{3.40}$$

Let $q_{ii} = -q_i$, the matrix $\mathbf{A} = \{q_{ij}\}$ is called the *infinitesimal generator* of the Markov Chain. It takes the form $\mathbf{A} = -\lambda\mathbf{\Lambda}$, where

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ -(1 - \nu) & -\nu & 1 & 0 & 0 & \dots \\ -(1 - \nu)^2 & -(1 - \nu)\nu & -\nu & 1 & 0 \\ -(1 - \nu)^3 & -(1 - \nu)^2\nu & -(1 - \nu)\nu & -\nu & 1 \\ & & \vdots & & \ddots \end{bmatrix} \tag{3.41}$$

Denote the transition matrix $\mathbf{P}(t) = \{p_{ij}(t)\}$. From the definition of the local characteristics q_{ij} in (3.37) and (3.38), we have

$$\mathbf{A} = \lim_{h \rightarrow 0} \frac{\mathbf{P}(h) - \mathbf{P}(0)}{h}, \tag{3.42}$$

where $\mathbf{P}(0) = \mathbf{I}$. Since this Markov Chain is homogeneous

$$\frac{\mathbf{P}(t+h) - \mathbf{P}(t)}{h} = \mathbf{P}(t) \frac{\mathbf{P}(h) - \mathbf{I}}{h} = \frac{\mathbf{P}(h) - \mathbf{I}}{h} \mathbf{P}(t). \tag{3.43}$$

Therefore

$$\frac{d}{dt} \mathbf{P}(t) = \mathbf{P}(t) \mathbf{A} = \mathbf{A} \mathbf{P}(t) \tag{3.44}$$

(3.44) is referred to as the Kolmogorov's differential system [Bremaud, 1999], the solution to which is

$$\mathbf{P}(t) = e^{t\mathbf{A}} = \sum_{n=0}^{\infty} \frac{(t\mathbf{A})^n}{n!} \quad (3.45)$$

Since $X = 0$ is an absorbing state, the CDF of the time until outage, $\mathbb{P}[T_O \leq t]$, is the probability that the UE enters state $X = 0$ at or before t , starting with B battery units at time 0. It can be obtained from $\mathbf{P}(t)$ as follows

$$\mathbb{P}[T_O \leq t] = \mathbb{P}[X(t) = 0 | X(0) = B] = p_{B0}(t). \quad (3.46)$$

Gaussian approximation

In this section we follow the analysis in Section 3.3.1.5 for the case in which the consumption process is Gaussian. First we establish that $\zeta_L(t)$ can indeed be approximated as a Gaussian random process. Recall from (3.28) that $\zeta_L(t) = \rho_0 \sum_{i=1}^{N(t)} M_i$. Since M_i are i.i.d., if $N(t)$ is sufficiently large, we can use the Central Limit Theorem to approximate $\zeta_L(t)$ as a Gaussian random process $\mathcal{N}(\mu_L(t), \sigma_L^2(t))$. We proceed to find the mean and variance of this process.

Recall that each M_i is distributed as a geometric random variable M with parameter ν . We have

$$\begin{aligned} \mathbb{E}[M] &= \frac{1}{\nu} \\ \text{Var}[M] &= \frac{1 - \nu}{\nu^2}. \end{aligned} \quad (3.47)$$

From the law of total expectation,

$$\begin{aligned}
\mu_L(t) &= \mathbb{E} \left[\mathbb{E} \left[\rho_0 \sum_{i=1}^{N(t)} M_i \middle| N(t) \right] \right] \\
&= \rho_0 \mathbb{E}[N(t)] \mathbb{E}[M] \\
&= \rho_0 \frac{\lambda t}{\nu}
\end{aligned} \tag{3.48}$$

From the law of total variance,

$$\begin{aligned}
\sigma_L^2(t) &= \mathbb{E} \left[\text{Var} \left[\rho_0 \sum_{i=1}^{N(t)} M_i \middle| N(t) \right] \right] + \text{Var} \left[\mathbb{E} \left[\rho_0 \sum_{i=1}^{N(t)} M_i \middle| N(t) \right] \right] \\
&= \rho_0^2 \mathbb{E}[N(t)] \text{Var}[M] + \rho_0^2 \text{Var}[N(t)] \mathbb{E}[M]^2 \\
&= \rho_0^2 \lambda t \frac{1-\nu}{\nu^2} + \rho_0^2 \lambda t \frac{1}{\nu^2} \\
&= \rho_0^2 \lambda t \frac{2-\nu}{\nu^2}
\end{aligned} \tag{3.49}$$

From (3.19), by using the remaining battery B as multiple of the battery unit ρ_0 , we have

$$\mathbb{P}[T_O \leq t] = \Phi \left(\frac{\frac{\lambda t}{\nu} - B}{\sqrt{\lambda t \frac{2-\nu}{\nu^2}}} \right). \tag{3.50}$$

Using the approximation in (3.22), we replace the value of t on the denominator of (3.50) with $\frac{B\nu}{\lambda}$. (3.50) becomes

$$\begin{aligned}
\mathbb{P}[T_O \leq t] &\approx \Phi \left(\frac{t - \frac{B\nu}{\lambda}}{\frac{\nu}{\lambda} \sqrt{\lambda \frac{B\nu}{\lambda} \frac{2-\nu}{\nu^2}}} \right) \\
&= \Phi \left(\frac{t - \frac{B\nu}{\lambda}}{\sqrt{\frac{B\nu(2-\nu)}{\lambda^2}}} \right).
\end{aligned} \tag{3.51}$$

Therefore, for a given amount of battery B , the time until outage T_O can be approximated as a Gaussian random variable $\mathcal{N}(\mu_{T_O}, \sigma_{T_O}^2)$, with

$$\mu_{T_O} = \frac{B\nu}{\lambda}, \quad \sigma_{T_O}^2 = \frac{B\nu(2-\nu)}{\lambda^2}. \tag{3.52}$$

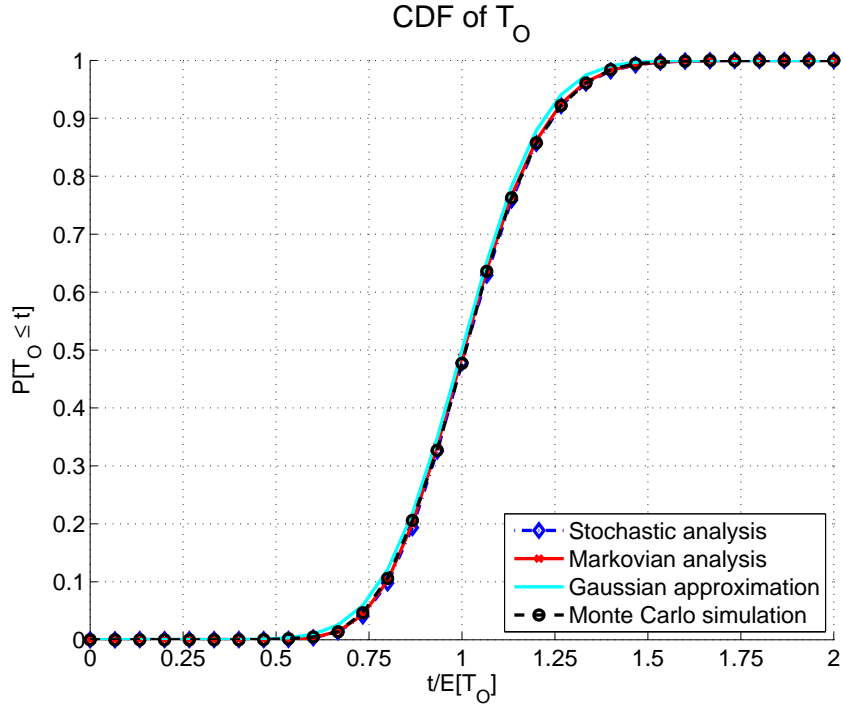


Figure 3.6: CDF of time until outage T_O calculated by stochastic analysis (3.34), Markovian analysis (3.46), Gaussian approximation (3.52), and Monte Carlo simulation. The time duration t is plotted with reference to the mean usage duration $\mathbb{E}[T_O]$.

We compare the CDF of the time until outage T_O calculated by stochastic analysis (3.34), Markovian analysis (3.46), Gaussian approximation (3.52), and Monte Carlo simulation in Figure 3.6. It can be clearly seen that the stochastic and Markovian analyses agree with the Monte Carlo simulation. The Gaussian approximation is very close to this precise distribution.

3.3.2.3 Beneficial cooperation

In this section we study the conditions which a helpee i and a helper j engaging in a beneficial cooperative session (Definition 1) must satisfy. Let the duration of this cooperative session be T_c . The helpee's consumption process parameter L_i comprises of the battery unit $\rho_{0,i}$ and the helpee's data arrival characteristics λ_i, ν_i . $\rho_{0,i}$ depends on the helpee's uplink power control parameters, of which the main component is the path loss PL_i . Similarly, the helper's consumption process parameter L_j comprises of $\rho_{0,j}, \lambda_j$, and ν_j . Because the helper relays the helpee's data during the cooperative session, the consumption process parameter L_{ij} of the cooperative session consists of the D2D path loss PL_{ij} (thus battery unit $\rho_{0,ij}$) and the helpee's data arrival characteristics λ_i, ν_i . Here we make an implicit assumption that the transmission power in D2D mode is proportional to the path loss between the devices. If 3GPP chooses to use constant D2D transmission power then L_{ij} only depends on λ_i, ν_i .

During the cooperative session, the helpee transmits its data through the D2D link. Its battery consumption is

$$\Delta B_i = \rho_{0,ij} \sum_{k=1}^{N_i(T_c)} M_{i,k} \quad (3.53)$$

During the cooperative session, the helper transmits both of its data and the helpee's data to the eNodeB. The amount of battery consumed by receiving D2D data is very small compared to the uplink transmission, thus can be ignored. The helper's

battery consumption is

$$\Delta B_j = \rho_{0,j} \left(\sum_{k=1}^{N_i(T_c)} M_{i,k} + \sum_{l=1}^{N_j(T_c)} M_{j,l} \right) \quad (3.54)$$

Refer to Table 3.1, the amount of battery “transferred” by the helper is

$$\Delta B_{ji} = \rho_{0,j} \sum_{k=1}^{N_i(T_c)} M_{i,k}. \quad (3.55)$$

The transferring loss at the helpee is

$$\delta_{ji} = (\rho_{0,j} - \rho_{0,i}) \sum_{k=1}^{N_i(T_c)} M_{i,k} + \rho_{0,ij} \sum_{k=1}^{N_i(T_c)} M_{i,k}. \quad (3.56)$$

According to Lemma 1, to have beneficial cooperation, we need $\delta_{ji} \leq \Delta B_{ji}$.

From (3.55) and (3.56), this condition is equivalent to

$$\rho_{0,ij} \sum_{k=1}^{N_i(T_c)} M_{i,k} \leq \rho_{0,i} \sum_{k=1}^{N_i(T_c)} M_{i,k}. \quad (3.57)$$

In other words, the helpee needs to spend less energy in a D2D link than he would in the cellular link. This is typically the case, unless the helpee is very close to the eNodeB. In BDS, we enforce a maximum D2D path loss PL_{D2D} such that only helpers who receive the `BDSDiscovery` signal with received path loss smaller than this value will respond with `BDSReply` (see Figure 3.1). This threshold essentially limits the range of the D2D connections, keeping them “local”. The condition in Lemma 1 can be enforced by only allowing the helpees to request for help when their path loss is greater than PL_{D2D} . More formally, we have

$$\rho_{0,i} \geq \rho_{0,D2D} \geq \rho_{0,ij} \quad (3.58)$$

where $\rho_{0,D2D}$ is calculated based on PL_{D2D} .

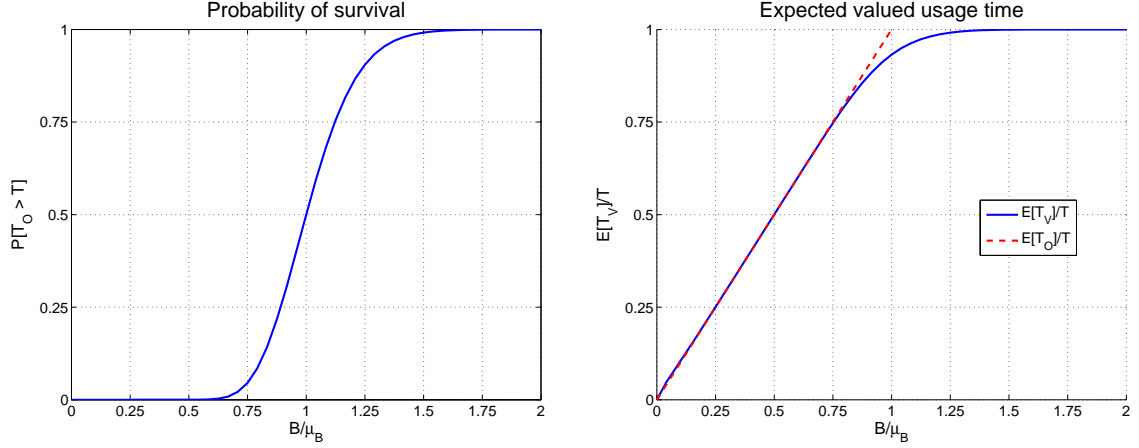
3.3.2.4 Design of cooperative rules

In BDS, the cooperative duration T_c is kept small so that user mobility does not make the D2D link go out of range. If after T_c , the helper and the helpee still satisfy the beneficial cooperative conditions, they can request the eNodeB to extend the cooperative duration to another T_c . This will reduce the amount of signaling as the helpee does not need to go through the full help requesting procedure. With this choice, (3.8) can be used to guide the design of cooperative rules.

According to (3.8), the rate of change of the helpee's utility with respect to battery must be greater than that of the helper. Since we have established that the battery consumption process under our model can be approximated as a Gaussian random process, we can use (3.20) and (3.23) to calculate the utility functions discussed in Section 3.3.1.5. We plot the values of those two functions with respect to the available battery in Figure 3.7. Notice that we are looking at the resource dimension of the utility, as opposed to the time dimension as in Section 3.3.1.5.

In Figure 3.7, the available battery B is normalized with respect to μ_B , the amount of battery that would give the expected time until outage $\mathbb{E}[T_O]$ equal to the target usage time T . From (3.52), we know that $\mathbb{E}[T_O] = B\nu/\lambda$. Therefore, $\mu_B = \lambda T/\nu$. In Figure 3.7b, the dashed line represents the expected valued usage time when there is much less battery than required to meet target usage, as seen in (3.18). Since $\mathbb{E}[T_O]/T = B/\mu_B$, this line has slope 1.

We can see that for both utility functions, there exists a utility value above which the resource-slope decreases. Therefore we can use thresholding for our co-



(a) C1 - Probability of survival (3.20) (b) C2 - Expected valued usage time (3.23)

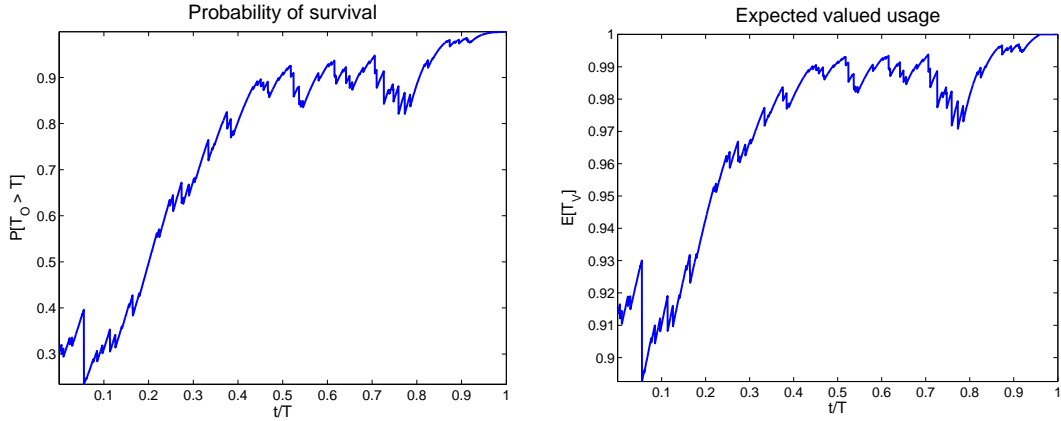
Figure 3.7: Utility as functions of available battery for user categories C1 and C2. The target usage time T is fixed. $\mu_B = \lambda T/\nu$.

operative rules and design appropriate thresholds that guarantee beneficial cooperation. To achieve the condition in (3.8), we set an upper cooperative threshold (the helping threshold) γ_2 such that the helper is operating above this threshold, and thus on the slope-decreasing region. The helpee has to be operating below another threshold γ_1 ($\gamma_1 \leq \gamma_2$). For utility type 2, that is all we need to do to ensure that the helpee's resource-slope is greater than the helper's. For utility type 1, the helpee needs to be *above* $1 - \gamma_2$ to have a steeper slope. The intuition is that if the helpee's available battery is so far off his target usage, a cooperative session will not improve his probability of survival much, and he is still very likely to go into outage. This is a characteristic of the all-or-nothing utility type.

3.3.2.5 Evolution of user utility over time

In this section we describe what happens to the utility of a user as time progresses. For the simplicity of the discussion, let us assume that the consumption parameter L does not change. In this case, there are only two factors affecting the user's utility: the remaining time until the target usage T and the amount of remaining battery B . Between data bursts, the amount of remaining battery stays the same. The user's utility thus increases as the time until target usage decreases. When the user has a new data burst, the battery drops suddenly, which also leads to a sudden drop in utility.

To illustrate these evolutions, we simulate a user with random data bursts and plot the values of the two utility functions over time for this user in Figure 3.8. For this case, the two types of utility function follow a quite similar path, albeit on different scales. This user starts out with a 0.3 probability of meeting his target usage. His expected usage duration at the beginning is 0.91 of his target usage duration T . There is a big data burst at $t = 0.05T$, resulting in a large dip in the user's utility. As time progresses from $t = 0.05T$ to $0.5T$, the user has less data than expected, thus his utility increases (on average). From $t = 0.5T$ to $0.7T$, the user uses the typical amount of data. His utility stays constant on average over this range. From $t = 0.7T$ to $0.8T$ he uses more data than expected, which results in a dip in utility values. His usage decreases to less than typical from $t = 0.8T$ to the target usage T . He ends up meeting his target usage. However, he becomes relatively certain about that fact only at $t = 0.95T$.



(a) Utility for user category C1 - Probability of survival

(b) Utility for user category C2 - Expected valued usage time

Figure 3.8: Evolutions of user's utility. Notice the scale difference.

3.4 User incentive

As we discussed in Section 3.1, the helpers do not get any immediate benefit from a cooperative BDS session. Therefore they need to be incentivized. A currency system is most suitable for BDS because we can leverage the centralized infrastructure. We discussed two such currency systems: virtual currency (token-based) and real currency.

The advantage of a virtual currency system is that it is self-contained. The amount of credits in the system is controlled by the network. Therefore the behavior of the users is predictable (as long as they are rational). The advantage of a real currency system is that it can potentially provide more cooperation as the users can always request for BDS service. However user interaction is required and the behavior is harder to predict.

3.4.1 Virtual currency

In a token-based incentive system, each user is initialized with a number of tokens, k_0 , when they activate their phone number. To request BDS service, the user has to pay one token. The selected helper receives that token. Since the number of tokens of each user is kept by the network, fake tokens are not an issue. The network also sees data connections. Therefore a helper cannot lie that he relayed the helpee's traffic while he did not. Security of the token system therefore is not a major concern because of the centralized nature of BDS.

When a UE with k tokens receives `RRCConnReconfig` for BDS listeners (Figure 3.1), it estimates the utility cost c for helping in a cooperative session. If the cost is less than the utility gain then the UE listens for `BDSDiscovery`. Let the value of k tokens be V_k . The UE listens for `BDSDiscovery` if $V_{k+1} - V_k > c$. [Xu and van der Schaar, 2013] studies a token system for downlink relay service with the goal of improving data rates. It is shown that the optimal strategy for users is thresholding. A user receiving help request accepts if his number of tokens is smaller than a threshold, $k \leq K(c)$. If all users follow this optimal strategy, the network designer can control the total number of tokens in the network to achieve the maximum efficiency, i.e. the probability of a BDS request being accepted.

3.4.2 Real currency

We envision a real auction system where the helpee set a maximum amount of dollars that he is willing to pay for a help session, d_{\max} . This information is sent

with `BDSInitSerReq`. Each potential helper sends an amount they want to receive for the service, d_i , in `BDSReply`. If there are more than one helpers whose request fees are less than d_{\max} , the AppSer selects the helper with the lowest request fee, and pays him the amount equal to the second lowest fee. This is known in the literature as a reversed auction. It is proven that the second lowest request fee is a form of Vickrey-Clarke-Groves (VCG) payment [Nisan et al., 2007], and it achieves the optimal social outcome of everybody telling their true price.

A real currency system is simple to implement. However, user interaction is expected to prevent “surprised” large phone bills. In crowded area (e.g. malls), there are plenty of potential helpers (high supply). Therefore the service will be cheaper. In remote area (e.g. parks), there are fewer potential helpers (low supply). As a result the service will be more expensive. The users, with some level of software automation, have to adjust their prices based on the area. We foresee a tendency that the users will keep their battery high in order to gain money. This change of behavior is interesting to study, but it is out of the scope of this work.

3.5 Performance analysis

We established in Section 3.3.2 that by using thresholding, we can ensure that the cooperative sessions in BDS improve the overall network performance. In this section, we analyze this performance improvement through simulation. Our simulation setup is described in [Ta et al., 2014]. In particular, we use 3GPP reports [Nokia Corporation, 2012, Renesas Mobile Europe Ltd., 2012, 3GPP, 2012]

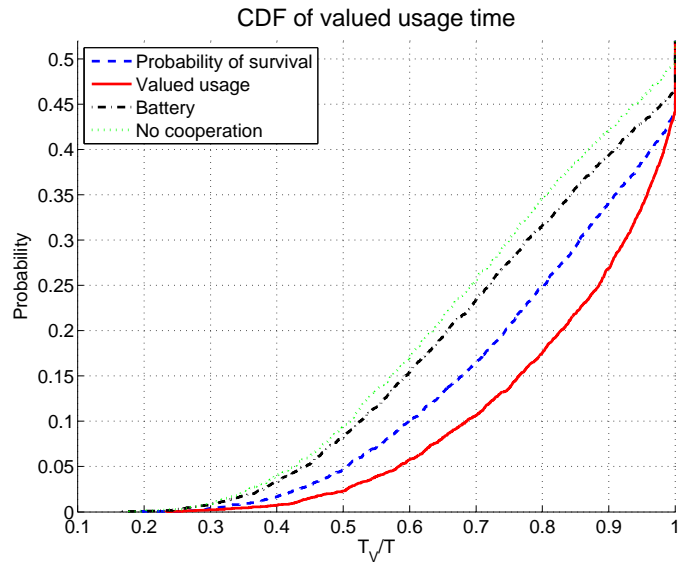
to set the parameters of our traffic model. We use WINNER II channel models [Kyosti et al., 2007] for our communication links. We use a modified version of the random waypoint model to simulate user mobility. The reception and idle circuit energy consumption is modeled as a constant factor, the value of which is derived from [Nokia Corporation, 2012]. In this work, we implement new functionalities to calculate battery utility to use in cooperative decisions. The simulation parameters are shown in Table 3.2. Our simulator source code is available at [Ta,].

We compare the performance of the UEs when they do and do not cooperate. When cooperation is used, we compare the cooperative rules using probability of survival $u_1(\cdot)$ (category C1 - Section 3.3.1.5), expected valued usage time $u_2(\cdot)$ (category C2), and battery level B (used in [Ta et al., 2014]) as thresholds. The valued usage time as a fraction of the target usage time, T_V/T , of the UEs for those algorithms are shown in Figure 3.9. The probability of survival for all 4 algorithms can also be inferred from Figure 3.9. The intersecting points of the curves with the right-most vertical line, $T_V/T = 1$, are the probabilities of outage. In addition, we study the level of cooperation, which leads to performance gain, as the amount of resource in the network changes. In Figure 3.9a, the users have low battery capacity, resulting in a probability of outage of 0.5. In Figure 3.9b, we increase the battery capacity of the users by 14%, which results in a lower probability of outage of 0.41. We show the overall network gains in valued usage time as a percentage in Table 3.3. The overall gains in probability of survival are shown in Table 3.4.

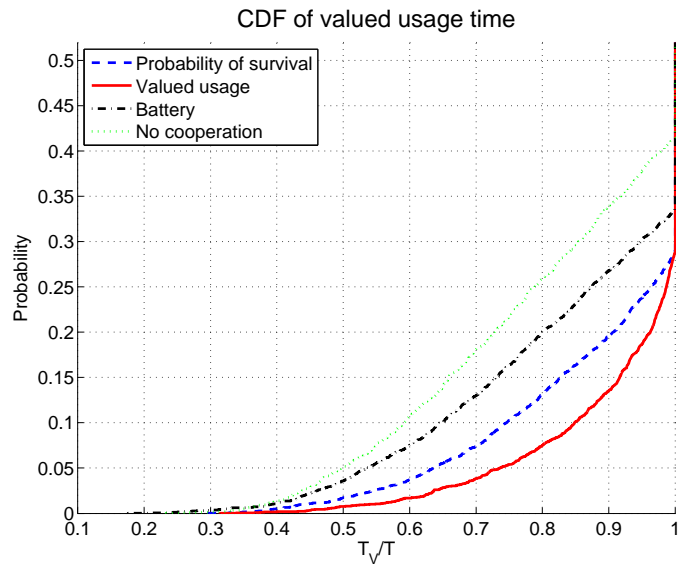
We can clearly see that cooperation provides benefit over no cooperation. We also see that using utility functions as thresholds is better than using battery level.

Table 3.2: Simulation parameters

Parameter	Value
Cell radius	300 m
Number of UEs	500
Mean data inter-arrival time	30 s
Mean burst size	7800 bytes
Speed	0.1 - 6 m/s
Pause duration	0 - 300 s
Walk duration	30 - 300 s
Path loss compensation factor α	0.8
Constant energy cost factor	15 mJ
Base power P_0	-69 dBm
Maximum transmit power	24 dBm
Modulation order	QAM16
Code rate	1/3
Carrier frequency	2 GHz
eNodeB antenna height	25 m
UE antenna height	1.5 m
Number of walls for indoor NLOS	1
Cooperation threshold γ_1, γ_2	0.5, 0.9
Cooperation path loss threshold	110 dB
Cooperation radius	30 m



(a) Lower battery capacity



(b) Higher battery capacity

Figure 3.9: Cumulative distribution functions of the valued usage time for 3 cooperative algorithms and no cooperation. The higher battery capacity is 14% more than the lower battery capacity.

Table 3.3: Overall network gains in valued usage time

	$u_1(\cdot) = \mathbb{P}[T_O > T]$	$u_2(\cdot) = \mathbb{E}[T_V]/T$	B
Lower battery capacity	7%	11%	2%
Higher battery capacity	7%	10%	1%

Table 3.4: Overall network gains in probability of survival

	$u_1(\cdot) = \mathbb{P}[T_O > T]$	$u_2(\cdot) = \mathbb{E}[T_V]/T$	B
Lower battery capacity	6%	6%	4%
Higher battery capacity	13%	13%	8%

As we discussed in Section 3.1, by factoring in the target usage, we can take advantage of more cooperative opportunities than considering the battery level alone. Between the two utility functions, $u_2(\cdot)$ performs better when we consider valued usage time. This is consistent because it is designed for this performance metric. Interestingly, it can be seen that $u_2(\cdot)$ does not have any significant performance loss compared to $u_1(\cdot)$ for category C1. Therefore we can conclude that the cooperative thresholds perform well in limiting the impact on the helpers.

We can see from Table 3.3 that the overall network gains in valued usage time (as a ratio) are similar for lower and higher battery capacity cases. However the helpes in the latter clearly benefit more, as can be seen from their CDF curves. This is because when the overall network resource increases, there are more helpers

Table 3.5: Probability that a BDS request is accepted

	$u_1(\cdot) = \mathbb{P}[T_O > T]$	$u_2(\cdot) = \mathbb{E}[T_V]/T$	B
Lower battery capacity	0.46	0.57	0.25
Higher battery capacity	0.51	0.65	0.27

and fewer helpees. As a result, each helpee receives a higher benefit. In addition, the fraction of helpees brought out of outage also becomes more significant. This leads to a larger increase in probability of survival, as evident from Table 3.4.

We further quantify the level of cooperation by studying the probabilities that a BDS request is accepted in the 2 cases of varying battery capacity. These probabilities are shown in Table 3.5. We can see that using utility functions creates at least twice the amount of cooperation compared to using battery level B . In addition, $u_2(\cdot)$ consistently leads to more cooperation than $u_1(\cdot)$. This explains the larger amount of valued usage time created by using $u_2(\cdot)$. It is also clear that there are more chances for cooperation to take place when the network resource is high.

3.6 Conclusions

In this chapter we have shown that we can prolong the battery life of mobile devices by utilizing diversity of usage in cellular networks. In particular, we developed a Proximity Service (ProSe) for future LTE networks which allows UEs to cooperatively relay traffic of one another. We named our system the “Battery Deposit Service” (BDS). To utilize diversity of usage, we must understand the value

of battery for the UEs. We proposed a general framework to study utility of a resource. We applied this framework to BDS and showed that by setting appropriate thresholds as cooperative rules, the performance of the network is guaranteed to improve. We discuss currency systems using virtual tokens and real money to incentivize user cooperation.

Appendix

Expected valued usage time for Gaussian consumption process

We want to calculate the expected valued usage time $\mathbb{E}[T_V]$ for the case the consumption process $\zeta_L(t)$ is Gaussian. As seen in (3.22), the time until outage T_O is approximated as a Gaussian random variable $\mathcal{N}(\mu, \sigma^2)$. From (3.12)

$$\begin{aligned} \mathbb{E}[T_V] &= T - \int_0^T (T - \tau) \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\tau-\mu)^2}{2\sigma^2}} d\tau \\ &= T - (T - \mu) \int_0^T \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\tau-\mu)^2}{2\sigma^2}} d\tau + \int_0^T (\tau - \mu) \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\tau-\mu)^2}{2\sigma^2}} d\tau. \end{aligned} \quad (59)$$

Since $T_O \geq 0$, for the approximation $T_O \sim \mathcal{N}(\mu, \sigma)$ to hold we need $\Phi\left(\frac{-\mu}{\sigma}\right) \approx 0$.

This is true for sufficiently large μ . Consequently, we have

$$(T - \mu) \int_0^T \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\tau-\mu)^2}{2\sigma^2}} d\tau \approx (T - \mu) \Phi\left(\frac{T - \mu}{\sigma}\right). \quad (60)$$

To compute the last term of (59), we make the change of variable $u = \frac{(\tau-\mu)^2}{2\sigma^2}$.

We have $(\tau - \mu)d\tau = \sigma^2 du$. Therefore,

$$\begin{aligned} \int_0^T (\tau - \mu) \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\tau-\mu)^2}{2\sigma^2}} d\tau &= \int_{\frac{\mu^2}{2\sigma^2}}^{\frac{(T-\mu)^2}{2\sigma^2}} \frac{\sigma}{\sqrt{2\pi}} e^{-u} du \\ &= \frac{\sigma}{\sqrt{2\pi}} \left(e^{-\frac{\mu^2}{2\sigma^2}} - e^{-\frac{(T-\mu)^2}{2\sigma^2}} \right). \end{aligned} \quad (61)$$

Finally (59) becomes

$$\mathbb{E}[T_V] = T - (T - \mu)\Phi\left(\frac{T - \mu}{\sigma}\right) + \frac{\sigma}{\sqrt{2\pi}}\left(e^{-\frac{\mu^2}{2\sigma^2}} - e^{-\frac{(T-\mu)^2}{2\sigma^2}}\right). \quad (62)$$

Chapter 4: Energy efficiency from network perspective:

Relay selection, resource allocation and power control for minimizing transmission power in device-to-device relay-enabled LTE networks

4.1 Overview

In Chapter 3, we have studied energy efficiency from the device perspective. In this chapter, we will look at the problem from the network point of view. It is well-known that multi-hop communications reduce the total transmission power. Our goal is to formulate the power minimization problem when D2D relay is enabled, while taking into account practical LTE constraints. The problems we consider include relay selection, resource allocation and power control. These optimization problems have binary decision variables, and thus exponential search spaces. Tackling these problems directly is not suitable for real-time operations. Therefore, we need to develop faster algorithms to cope with LTE runtime requirement (subframe level, which is 1 ms).

4.1.1 Related work

The problem of joint optimization of relay strategies and resource allocation has been considered in the past. However, past works mainly focus on maximizing rate, and therefore maximum power is always used. In the context of LTE, quality of service (QoS) is provided in term of minimum guaranteed bit rate. As a result, it is more applicable to consider minimizing transmission power while satisfying this rate requirement. A prominent work in this direction is [Ng and Yu, 2007]. The authors consider the problem of maximizing an utility function, concave in rate of each data stream, by relay selection and resource allocation. The solution in [Ng and Yu, 2007] bases on the assumption that the amount of schedulable resource is abundant (go to infinity). Even though this assumption may be appropriate for the number of OFDM tones, it cannot be applied to the number of resource blocks, the unit schedulable resource in LTE. Furthermore, [Ng and Yu, 2007] proposes to use an exhaustive search for the optimal relay strategy. This approach limits the application of their solution in real-time operations.

The majority of existing work use Shannon's formula to calculate the achievable rate of the UEs. Even though it makes the problem simpler because of the convexity of Shannon's formula, it is unrealistic. In real LTE networks, the UEs are assigned a Modulation and Coding Scheme (MCS) for each transmission. The achieved rate of the UEs is a function of their assigned MCS. The introduction of MCS adds another dimension to the variables of the optimization problem, which makes the search space much larger. As a result, finding real-time algorithms be-

comes more challenging. In the context of downlink transmission for femtocells, the authors of [Lopez-Perez et al., 2014] propose to separate MCS from the resource allocation problem. We follow this idea in our work.

4.1.2 Summary of contributions

Our contributions in this chapter are

1. We formulate the relay selection, resource allocation and power control problems for minimization of transmission power in a D2D relay-enabled LTE network. We take into account practical LTE constraints.
2. We develop a divide-and-conquer strategy, splitting the overall problem into sub-problems. We relate these sub-problems to well-studied problems in graph theory, so that we can make use of existing fast solutions.
3. We compare the performance of our algorithms with the solution obtained from CPLEX, an industrial-grade solver. Our algorithms perform very close to CPLEX, while requiring 3 orders of magnitude less runtime.

4.1.3 Outline of chapter

The chapter is structured as follows. We briefly introduce LTE uplink resource allocation and power control in Section 4.2. In Section 4.3, we introduce the current state of D2D development in 3GPP. In Section 4.4, we formulate the power minimization problem through relay selection, resource allocation and power control. We describe our simulation setup and results in Section 4.5. We conclude in Section 4.6.

4.2 Uplink scheduling and power control in LTE

In LTE, the UEs transmit data to the eNodeB on physical uplink shared channels (PUSCH). The eNodeB sends control messages to the UEs on physical downlink control channels (PDCCH). The UEs with uplink data send buffer status reports (BSR) to the eNodeB, indicating how much and what type of data they need to transmit. The eNodeB takes into account buffer status of all served UEs in allocating PUSCH resource. With dynamic scheduling, resource allocation is done for every subframe (1ms). To notify the UEs of the resource assignment, the eNodeB sends uplink grants using downlink control information (DCI) messages on PDCCH. DCI format 0 is used for uplink grants of single transport block, while format 4 is used for uplink grants of multiple transport blocks. Also included in the DCI are the modulation and coding scheme (MCS), and transmission power control (TPC) messages. The DCI is sent 4 subframes prior to the actual uplink transmission to allow time for the UEs to process these uplink grants.

In LTE, a UE's uplink transmission power (in dBm) is controlled by equation (4.1) (see [Baker, 2011, 3GPP, 2011c]).

$$P = \underbrace{P_0 + \alpha\text{PL}}_{\text{open-loop}} + \underbrace{\Delta_{\text{TF}} + f(\Delta_{\text{TPC}})}_{\text{dynamic offset}} + 10 \log_{10}(M) \quad (4.1)$$

The per-resource block (RB) power control consists of two components: a basic open-loop operating point and a dynamic offset. M is the number of allocated RBs.

P_0 is a semi-static nominal power level set by the eNodeB. αPL is the path loss compensation component, where α controls the degree of compensation. PL

is derived from the downlink Reference Signal Received Power. It includes shadowing but not fast fading. The dynamic control of UE uplink transmission power is designed to be an offset from the base operating point. This offset depends on two factors: the allowed modulation and coding scheme (TF stands for Transport Format) and a UE-specific transmitter power control (TPC) command.

4.3 Current state of D2D communications underlying LTE

Proximity services and public safety usage are the main drivers for development of D2D in LTE. The target for release 12 is discovery and communication for public safety. Even though D2D communications have not been fully standardized in 3GPP, some features have been agreed upon [3GPP, 2014a]. D2D operations will be considered in two modes: in-coverage (Mode 1), and out-of-coverage (Mode 2). A D2D link is considered in Mode 1 if both UEs are connected to the cellular networks, and Mode 2 otherwise. We focus on Mode 1 in our work.

For Mode 1, the time/frequency resource for D2D communication (for discovery, scheduling, and data) are configured by the eNodeB. A new DCI format will be used to relay this scheduling information to the UEs. This new DCI format will have the same size as DCI format 0. It is also agreed that, at least in the beginning, D2D communication will occupy the uplink frequency (FDD) or uplink subframes (TDD). For Mode 1, the eNodeB has the flexibility to optimize system performance. In this chapter we will consider system performance in term of minimizing UE uplink transmission power.

4.4 Problem statement

In this work we consider a single cell with N UEs. All UEs are assumed capable of D2D. The objective is to design a cooperative relay system that reduces the overall transmission power on the uplink. Inactive UEs are allowed to receive data from active UEs through D2D connections, decode and forward to the eNodeB. Currently, the eNodeB schedules uplink transmissions based on buffer status reports and channel quality from the UEs. We add one more dimension to this decision process: relay selection.

Ideally, relay assignment can be done every subframe (1ms). However, the overhead for signaling such assignment will be too excessive. In fact, the current consideration for a D2D transmission time interval is 2 frames (20 ms) [3GPP, 2014b]. As a result, in our design, the relay selection is carried out at a large time scale. During such a period, each UE keeps record of at most one relay. If the relay is inactive, the eNodeB signals the UE to transmit through the relay. Resource allocation and power control can be done on a per-subframe basis to cope with fast fading.

4.4.1 Relay selection

The objective of this phase is to select a relay for each UE such that the total transmission power is minimized. For fairness, each UE can only choose at most one other UE as relay and each UE only serves as relay for at most one other UE.

Since the relay selection problem is considered in a large time scale, average

channel statistics can be used. This design also allows time for the eNodeB to aggregate D2D channel information. The freshness requirement of this channel information is not stringent, thus the control signaling overhead can be kept low. Consequently, we will assume that the eNodeB knows the average channel statistics of all D2D links.

In addition, operating at a large time scale allows us to use Shannon capacity formula, instead of discrete MCS levels, to determine the average UE rate. We consider orthogonal resource allocation and assume no inter-cell interference. For UE n ,

$$R_n = W_n \log_2 \left(1 + \frac{P_n G_n}{W_n N_0} \right) \quad (4.2)$$

Where R_n is the achievable rate, P_n is the transmission power, G_n is the average channel gain, W_n is the allocated bandwidth, and N_0 is the thermal noise power density.

To achieve rate R_n , the required SNR for UE n is

$$\gamma_n = 2^{R_n/W_n} - 1 \quad (4.3)$$

In this phase, the same bandwidth is considered for all UEs. As a result, γ_n can be determined from the rate requirement, and the thermal noise power are the same for all UEs. Let us denote this noise power σ^2 . The QoS (SNR) requirement for UE n is

$$\frac{P_n G_n}{\sigma^2} \geq \gamma_n \quad (4.4)$$

Since decode-and-forward relaying is used, if UE m is selected as relay for UE n , both the D2D link between UEs n and m and the cellular link from UE m to the

eNodeB have to satisfy the SNR requirement of UE n .

$$\frac{P_n G_{n,m}}{\sigma^2} \geq \gamma_n \quad (4.5)$$

$$\frac{P_m^r G_m}{\sigma^2} \geq \gamma_n \quad (4.6)$$

Where P_m^r denotes the power used by UE m in D2D relay transmission. $G_{n,m}$ is the channel gain of the link between UE n and m .

The problem of minimizing the total transmission power of both relay and direct transmissions can be formulated as the following Mixed Binary Linear Program

$$\min_{P_n, P_n^r, x_{n,m}} \sum_{n=1}^N P_n + P_n^r \quad (\text{RS})$$

$$\text{s.t.} \quad \frac{P_n G_{n,m}}{\sigma^2} \geq x_{n,m} \gamma_n \quad \forall n, m \quad (4.7)$$

$$\frac{P_m^r G_m}{\sigma^2} \geq x_{n,m} \gamma_n \quad \forall n, m \quad (4.8)$$

$$\sum_{m=1}^N x_{n,m} = 1 \quad \forall n \quad (4.9)$$

$$\sum_{n=1}^N x_{n,m} - x_{m,m} \leq 1 \quad \forall m \quad (4.10)$$

$$P_n \geq 0 \quad \forall n \quad (4.11)$$

$$P_n^r \geq 0 \quad \forall n \quad (4.12)$$

$$x_{n,m} \in \{0, 1\} \quad \forall n, m \quad (4.13)$$

We introduce the binary variables $x_{n,m}$ to denote that UE m is selected as the relay for UE n . Constraints (4.7), (4.8) ensure the SNR requirements of selected links are met. We adopt the convention $G_{n,n} = \infty$ so that when $x_{n,n} = 1$, UE n always transmits directly to the eNodeB, and thus $P_n = 0$ and P_n^r is the direct transmission power. Constraint (4.9) ensures that each UE selects exactly one relay

(including itself). Constraint (4.10) ensures that each UE serves as the relay of at most one other UE. Constraints (4.11),(4.12),(4.13) indicate the domain of the decision variables. We do not enforce maximum transmission power so that the optimization problem always has a feasible solution.

We can see that the most important variable of (RS) is $x_{n,m}$. Once this relay selection is determined, the transmission power will follow by solving for equality in (4.7) and (4.8). (RS) is equivalent to the *minimum weight matching problem on a bipartite graph* for the graph illustrated in Figure 4.1. Each side of the graph has N nodes representing the UEs. A link between node n on the left half to node m on the right half signifies that $x_{n,m} = 1$, or UE m is selected as the relay for UE n . The cost on this link is

$$P_n + P_m^r = \gamma_n \sigma^2 \left(\frac{1}{G_{n,m}} + \frac{1}{G_m} \right) \quad (4.14)$$

The Hungarian algorithm [Kuhn, 1955] can be used to solve the minimum weight matching problem in $\mathcal{O}(N^3)$.

4.4.2 Resource allocation and power control

During each subframe, let us denote the set of UEs with non-empty buffer by \mathcal{A} , the set of UEs with empty buffer by \mathcal{I} . Consider an active UE $n \in \mathcal{A}$ with relay m . If the relay is inactive, i.e. $m \in \mathcal{I}$, n always use the relay instead of direct transmission. As a result, at the beginning of each frame, the eNodeB knows how much D2D resource is needed. In this section, we formulate the resource allocation and power control problem. It can then be applied separately for D2D relay and for

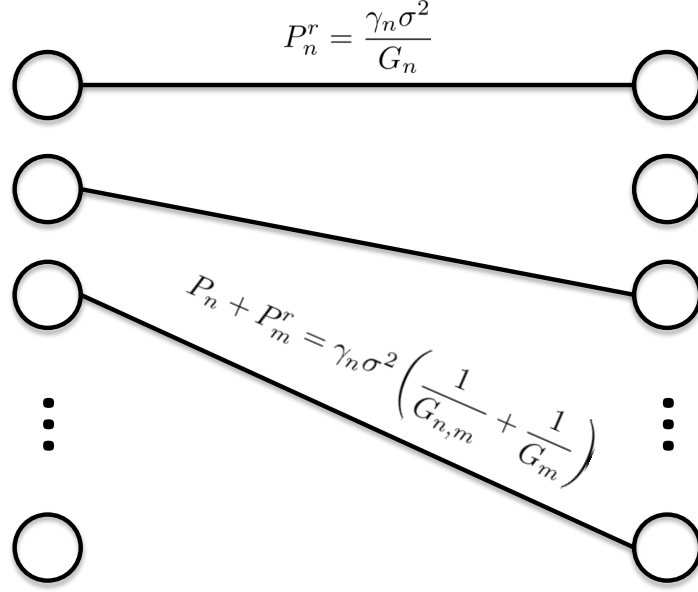


Figure 4.1: Equivalent minimum weight matching on a bipartite graph problem of (RS).

cellular uplink.

In LTE, the unit for resource allocation is RB pair. Each RB pair consists of one RB per slot. For localized allocation, the two RBs occupy the same frequency. Let us denote by K the number of RBs for each slot. K depends on the system bandwidth and how much frequency resource is allocated for D2D communication versus cellular uplink. Orthogonal resource allocation is used such that each RB is only allocated to 1 link.

Let $s = 1, \dots, S$ be the allowable MCS levels. Each MCS consists of a modulation order (e.g. QPSK), and an effective code rate (e.g. 3/4). In LTE, each UE only uses one MCS per transmission. Without considering HARQ between several transmissions, the rate of each UE is therefore a function of the MCS level and the

Table 4.1: Modulation and coding schemes

	Modulation	Code rate	SNR (dB)	Efficiency (bits/symbol)	Rate ¹ (Mbps/RB)
MCS1	QPSK	1/2	2.88	1.00	0.168
MCS2	QPSK	3/4	5.74	1.50	0.252
MCS3	16QAM	1/2	8.79	2.00	0.336
MCS4	16QAM	3/4	12.22	3.00	0.504
MCS5	64QAM	2/3	15.88	4.00	0.672
MCS6	64QAM	3/4	17.50	4.50	0.756

number of allocated RBs. For each MCS s , there is a corresponding required SNR γ_s to achieve some predetermined packet error rate (e.g. 10%). These SNR requirements are usually obtained by simulation. In this work, we will use the MCS values, and the corresponding required SNR, from Table 4.1, introduced in [Lopez-Perez et al., 2014].

Let the allocation variable $x_{n,k,s} = 1$ denotes that RB k and MCS s are assigned to UE n ; $x_{n,k,s} = 0$ otherwise. The rate of UE n is

$$r_n = \sum_{s=1}^S \sum_{k=1}^K x_{n,k,s} \Phi_s \quad (4.15)$$

Where Φ_s is the per-RB rate of MCS s . For normal cyclic prefix, each RB consists of 7 OFDM symbols and 12 subcarriers. Without accounting for reserved reference and control elements, each RB has 84 resource elements. Since the duration of a slot is 0.5 ms, we can calculate Φ_s for each MCS s , as noted in Table 4.1.

¹The rates per RB are calculated assuming all 84 resource elements are used for data.

In LTE, demodulation reference signals (DM-RS) and sounding reference signals (SRS) are transmitted by the UEs to help the eNodeB estimate the channel gains. In this work we will assume that the eNodeB knows the channel gains on all RBs for all UEs. We also assume that the UEs are capable of using different transmission power on different RBs. Furthermore, we do not consider infeasible cases, i.e. there are always enough RBs to satisfy QoS requirement of the UEs.

The resource allocation and power control problem can be formulated as the following Mixed Binary Linear Program

$$\min_{P_{n,k,s}, x_{n,k,s}, y_{n,s}} \sum_{n=1}^N \sum_{s=1}^S \sum_{k=1}^K P_{n,k,s} \quad (\text{RAPC})$$

$$\text{s.t.} \quad \frac{P_{n,k,s} G_{n,k}}{\sigma^2} \geq x_{n,k,s} \gamma_s \quad \forall n, k, s \quad (4.16)$$

$$\sum_{s=1}^S y_{n,s} = 1 \quad \forall n \quad (4.17)$$

$$x_{n,k,s} \leq y_{n,s} \quad \forall n, k, s \quad (4.18)$$

$$\sum_{n=1}^N \sum_{s=1}^S x_{n,k,s} \leq 1 \quad \forall k \quad (4.19)$$

$$\sum_{s=1}^S \sum_{k=1}^K x_{n,k,s} \Phi_s \geq R_n \quad \forall n \quad (4.20)$$

$$P_{n,k,s} \geq 0 \quad \forall n, k, s \quad (4.21)$$

$$x_{n,k,s} \in \{0, 1\} \quad \forall n, k, s \quad (4.22)$$

$$y_{n,s} \in \{0, 1\} \quad \forall n, s \quad (4.23)$$

Here $P_{n,k,s}$ is the transmission power of UE n on RB k for MCS s , $G_{n,k}$ is the channel gain for UE n on RB k , the binary variable $y_{n,s} = 1$ if MCS s is assigned to UE n .

Constraint (4.16) ensures that the SNR requirement for assigned MCS is met.

Constraints (4.17) and (4.18) ensure that each UE is assigned only one MCS. Constraint (4.19) ensures that each RB is assigned to at most one UE. Constraint (4.20) ensures the required rate of each UE. Constraints (4.21), (4.22), (4.23) indicate the domain of the decision variables.

The decision variables of (RAPC) are 3-dimensional. Their large search spaces make solving the optimization problem time-consuming, not appropriate to a real-time operation. Since the channel conditions do not change significantly subframe by subframe, the MCS levels do not need to be updated that frequently. As a result, we can consider a sub-problem of (RAPC) where the MCS is predetermined. This sub-problem is only 2-dimensional and can be solved in real time. We provide a heuristic algorithm to search for the best MCS. This heuristic algorithm is carried out at a larger time scale (e.g. frame level). For every subframe within each such large time scale, the eNodeB solves the sub-problem to obtain resource assignment and power allocation.

4.4.2.1 RAPC for fixed MCS

When MCS s is selected for UE n , the SNR requirement and the per-RB rate

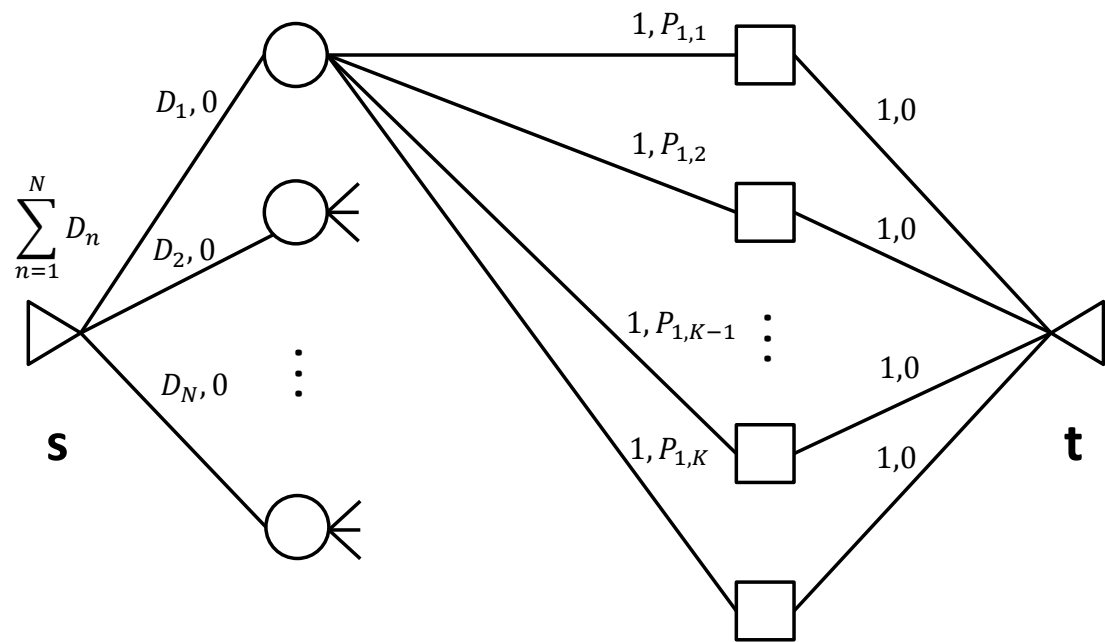


Figure 4.2: Equivalent minimum-cost flow problem of (S-RAPC). The total flow is $\sum_{n=1}^N D_n$. Each link is annotated with a (capacity, cost) pair. The circular nodes represent UEs, the squared nodes represent RBs.

can be associated to the UE so that $\gamma_n = \gamma_s, \Phi_n = \Phi_s$. (RAPC) reduces to

$$\min_{P_{n,k}, x_{n,k}} \sum_{n=1}^N \sum_{k=1}^K P_{n,k} \quad (\text{S-RAPC})$$

$$\text{s.t.} \quad \frac{P_{n,k} G_{n,k}}{\sigma^2} \geq x_{n,k} \gamma_n \quad \forall n, k \quad (4.24)$$

$$\sum_{n=1}^N x_{n,k} \leq 1 \quad \forall k \quad (4.25)$$

$$\sum_{k=1}^K x_{n,k} \Phi_n \geq R_n \quad \forall n \quad (4.26)$$

$$P_{n,k} \geq 0 \quad \forall n, k \quad (4.27)$$

$$x_{n,k} \in \{0, 1\} \quad \forall n, k \quad (4.28)$$

Similar to the relay selection problem (RS), here we also observe that the assignment variable $x_{n,k}$ is the most important. Once $x_{n,k}$ is determined, we can obtain $P_{n,k}$ by solving for equality in (4.24). For a fixed MCS, the rate of each UE is proportional to the number of allocated RBs. We can easily see that the rate requirement (4.26) can be equivalently written as

$$\sum_{k=1}^K x_{n,k} = \left\lceil \frac{R_n}{\Phi_n} \right\rceil \quad (4.29)$$

Let us denote $D_n = \left\lceil \frac{R_n}{\Phi_n} \right\rceil$ as the required number of RBs for UE n . (S-RAPC) is equivalent to the *minimum-cost flow problem* for the graph illustrated in Figure 4.2. The circular nodes represent the UEs, while the squared nodes represent the RBs. Each link is annotated with a (capacity, cost) pair. The links from the source \mathbf{s} to the UEs have capacity equal to the required number of RBs D_n . All other links have capacity 1. The link between UE n and RB k has cost (determined

from (4.24))

$$P_{n,k} = \frac{\gamma_n \sigma^2}{G_{n,k}} \quad (4.30)$$

The total flow of the network is $\sum_{n=1}^N D_n$.

Similar to the minimum weighted matching on a bipartite graph, minimum-cost flow is a well-studied problem. Algorithms with polynomial time complexity as well as fast practical implementation have been developed [Király and Kovács, 2012].

4.4.2.2 Heuristic search for MCS

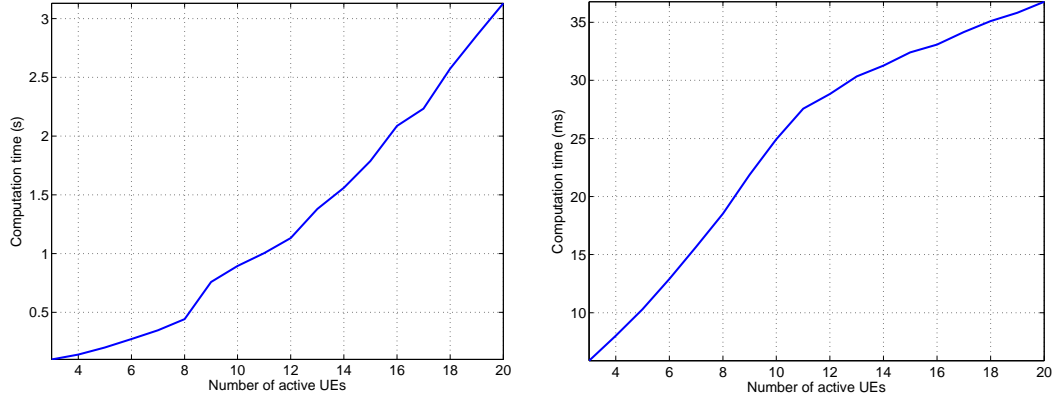
We observe that if MCS s satisfies the rate requirement of UE n using only one RB, then all MCS higher than s will not be selected. This is because an MCS higher than s will require higher transmission power. Therefore, we first determine the maximum MCS levels for all UEs.

Next, we sort the UEs by their average channel gains. We initialize all UEs with their max MCS. We then find the best MCS for one UE at a time, starting from the UE with the worst average channel gain. Since this UE will likely to require the most transmission power, the gain from optimizing for this UE is likely to be the largest.

Our heuristic algorithm to search for the best MCS is illustrated in Algorithm 1. Algorithm 1 essentially runs (S-RAPC) NS times, where S is the number of MCS. Since (S-RAPC) can be solved in polynomial time, so can Algorithm 1.

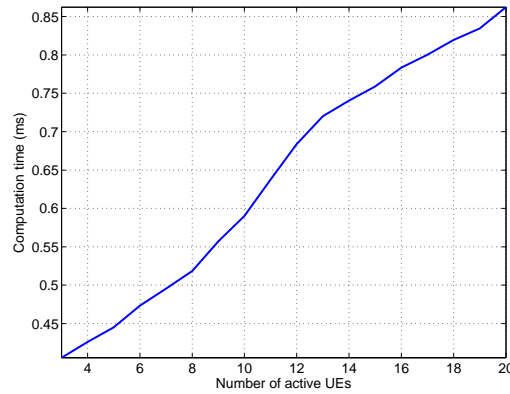
Algorithm 1 Heuristic search for MCS

```
1:  $R \in \mathbb{R}^N$  ▷ Required rate vector
2:  $\Phi \in \mathbb{R}^S$  ▷ Rate per RB based on MCS
3:  $U = \text{permutation}(1, \dots, N)$  ▷ Sorted UE index by average channel gain
   (ascending)
4:  $\mathbf{G} \in \mathbb{R}^{N \times K}$  ▷ Channel gain matrix
5:  $\mathbf{s}, \mathbf{s}_{\max}, \mathbf{s}_{\min} \in \{1, \dots, S\}^N$  ▷ MCS vectors
6:  $P, P_{\min} \in \mathbb{R}$  ▷ Total transmission power
7:  $\mathbf{x}, \mathbf{x}_{\min} \in \{0, 1\}^{N \times K}$  ▷ Resource assignment matrix
8: procedure GETMAXMCS( $R, \Phi$ )
9:   for  $n = 1$  to  $N$  do
10:    if  $R(n) \leq \Phi(1)$  then
11:       $\mathbf{s}_{\max}(n) \leftarrow 1$ 
12:    else if  $R(n) > \Phi(S - 1)$  then
13:       $\mathbf{s}_{\max}(n) \leftarrow S$ 
14:    else
15:      for  $s = 2$  to  $S - 1$  do
16:        if  $R(n) \leq \Phi(s)$  then
17:           $\mathbf{s}_{\max}(n) \leftarrow s$ 
18:        break
19:    return  $\mathbf{s}_{\max}$ 
20: procedure MCSSEARCH( $\mathbf{G}, \mathbf{s}_{\max}, R, U$ )
21:    $\mathbf{s} \leftarrow \mathbf{s}_{\max}$ 
22:    $\mathbf{s}_{\min} \leftarrow \mathbf{s}_{\max}$ 
23:    $[P_{\min}, \mathbf{x}_{\min}] \leftarrow \text{s-rapc}(\mathbf{G}, \mathbf{s}, R)$ 
24:   for  $n = 1$  to  $N$  do
25:      $u \leftarrow U(n)$ 
26:     for  $s = 1$  to  $\mathbf{s}_{\max}(u) - 1$  do
27:        $\mathbf{s}(u) \leftarrow s$ 
28:        $[P, \mathbf{x}] \leftarrow \text{s-rapc}(\mathbf{G}, \mathbf{s}, R)$ 
29:       if  $P < P_{\min}$  then
30:          $P_{\min} \leftarrow P$ 
31:          $\mathbf{s}_{\min} \leftarrow \mathbf{s}$ 
32:          $\mathbf{x}_{\min} \leftarrow \mathbf{x}$ 
33:      $\mathbf{s} \leftarrow \mathbf{s}_{\min}$ 
34:   return  $\mathbf{s}_{\min}, P_{\min}, \mathbf{x}_{\min}$ 
```



(a) CPLEX

(b) Algorithm 1



(c) S-RAPC

Figure 4.3: Runtime comparison of CPLEX, Algorithm 1, and minimum-cost flow (S-RAPC), as functions of the number of concurrent UEs to schedule.

4.5 Simulations

We simulate a single circular cell of N UEs, with no sectorization. The UEs are dropping uniformly within the cell. We use ITU channel models to calculate large scale channel loss (pathloss and shadowing) [3GPP, 2010]. We use the urban marocell model (UMa) for cellular links, and urban microcell (UMi) model for D2D links. UMi is currently used by 3GPP in evaluating D2D performance, while waiting

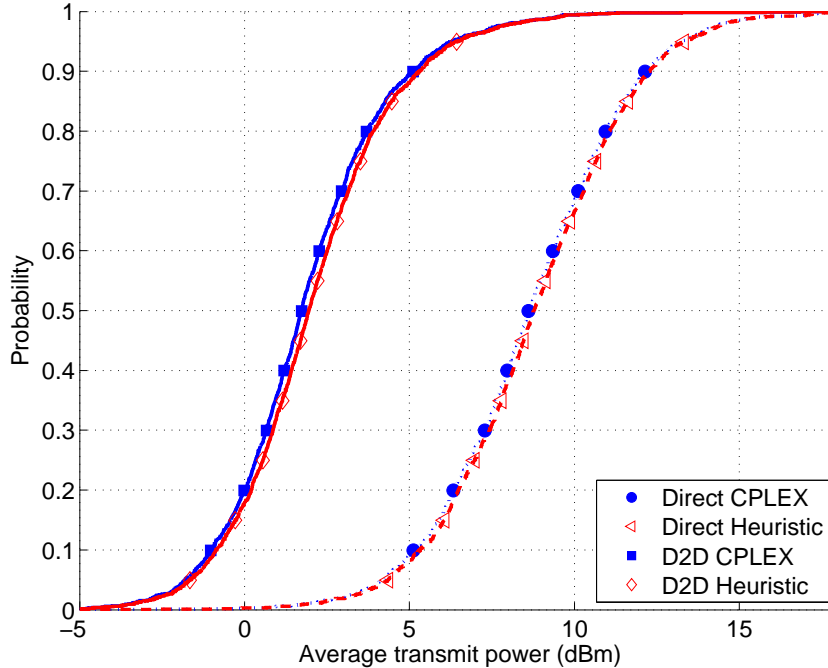


Figure 4.4: Average transmission power of a UE with resource allocation and power control in (RAPC). The performance of Algorithm 1 and CPLEX are compared.

for a more accurate model to be developed [3GPP, 2014c]. To simulate frequency selectivity, we include independent Rayleigh fast fading to each RB of each link. The parameters for our simulation is included in Table 4.2.

We illustrate the performance gain of enabling D2D relay in Figure 4.4. In addition, we compare the performance of our heuristic algorithm with CPLEX, an industrial-grade solver [cpl,]. Figure 4.4 shows the average transmission power of a UE with and without D2D relay. We can see that D2D relay can reduce the average transmission power by roughly 6 dB. Figure 4.4 also shows that Algorithm 1 performs very close to the optimal solution obtained by CPLEX.

The advantage of our heuristic algorithm is illustrated in Figure 4.3. Here we compare the average runtime of CPLEX, Algorithm 1, and minimum-cost flow prob-

Table 4.2: Simulation parameters

Parameter	Value
Cell radius	500 m
Number of UEs	180
UE dropping	Uniform
Carrier frequency	2 GHz
System bandwidth	10 MHz
eNodeB antenna gain	14 dBi
eNodeB antenna height	25 m
eNodeB noise figure	5 dB
UE antenna gain	0 dBi
UE antenna height	1.5 m
UE noise figure	9 dB
Thermal noise density	-174 dBm/Hz
Required rate	1 Mbps
Pathloss UE - eNodeB	UMa
Pathloss UE - UE	UMi
Fast fading	Rayleigh

lem (S-RAPC). We use the open source library LEMON [lem,] to solve (S-RAPC). These algorithms are run on our lab desktop machine, with quadcore Intel i7 2.8 GHz CPU, 4 GB RAM. We can see that CPLEX takes seconds to solve (RAPC), not suitable for real-time operation. Algorithm 1 runs in the order of tens of ms, suitable to be done in LTE frame level. Meanwhile, (S-RAPC) can be solved in less than 1 ms. As a result, it can be carried out on LTE subframe level. Moreover, with specialized hardware, an eNodeB should be able to finish our algorithms even faster. Figure 4.3 shows that our algorithms can be applied to the current LTE networks.

4.6 Conclusions

In this chapter we have introduced a mechanism to enable device-to-device relay in LTE networks. We show that with proper relay selection, resource allocation and power control, D2D relay can significantly reduce the transmission power of the UEs. Our mechanism contributes to addressing the pressing energy concern in cellular communications. We divide the overall problem into two parts: relay selection, and resource allocation & power control. We formulate the relay selection problem as an equivalent minimum weight matching problem on a bipartite graph, which has fast algorithms. For resource allocation and power control, we separate out MCS selection. We show that with a fixed MCS, the resource allocation and power control problem can be equivalently seen as a minimum-cost flow problem, which also has fast algorithms. We compare the performance of our heuristic MCS search to CPLEX solution and show that we perform very close to CPLEX solution.

While solving the resource allocation and power control problem directly in CPLEX requires too much time, we show that our two-level approach makes it feasible for the real-time requirements of current LTE networks. For future work, we will address the requirement of SC-FDMA that the resource blocks allocated to a UE have to be contiguous. We will also consider the impact of UE circuit energy consumption.

Chapter 5: Enhancing privacy in LTE paging system using physical layer identification

5.1 Overview

In all cellular networks, mobile stations (MS) mostly run on battery. To prolong the operational time of the MSs, the network architecture allows them to go into idle mode after being inactive for a certain period of time. In idle mode, the MSs do not sustain a connection with the serving base stations (BS). When there is a need to create a connection with an idle MS, e.g. voice calls, data, or system information updates, the BS sends out a notification to the MS in the form of a paging message. The location of an idle MS may have changed since the last time it was in communication. Therefore, the network maintains a tracking area for each idle MS. A tracking area consists of several cells. The MS has to report if it moves out of the assigned tracking area. In general, paging messages are sent without any confidentiality protection. As a result, everybody can listen to those messages. The privacy of those who are being paged is provided through the use of temporary IDs. Those are IDs which only have meaning in the context of the idle MS and the serving network within the tracking area. Recently, it has been shown that despite

the use of temporary IDs, the location of a user’s cellphone in a GSM network can still be leaked.

After reviewing the paging architecture in LTE and proving that the same attack is possible in LTE networks, we propose a solution using physical layer identification tags. Most security measures operate on the bit level and above. We go further down, to the physical level of electromagnetic transmissions. Our method does not rely on cryptographic primitives.

5.1.1 Related work

In [Kune et al., 2012], Kune *et al.* show that despite the use of temporary IDs, the location of a user’s cellphone in a GSM network can still be leaked. In particular, they show that an attacker can check if a user’s cellphone is within a small area, or absent from a large area, without the user’s awareness. As the authors highlighted, such vulnerability can lead to serious consequences. For example, in an oppressive regime, locations of dissidents are revealed to suppressive agents without cooperation from reluctant service providers. Another example is that a thief, who attempts a break-in, can use the knowledge of the absence of the target to reduce the threat of encounter.

To perform this location attack, the attacker in [Kune et al., 2012] requires 2 capabilities:

- Cause paging request messages to appear on the GSM *Paging Control Channel* (PCCH)

- Listen on the GSM PCCH broadcast channel

In GSM networks, paging messages are sent on dedicated time-division channels. The *Temporary Mobile Subscriber Identity* (TMSI) is used for paging messages. The idea behind the location attack is that the adversary initiates a connection request to the user cellphone (this of course assumes that he knows the target's number), which results in a paging message being sent in the user's tracking area. By observing the paging channel, the adversary obtains a set of possible temporary IDs for the target user. Repeating this procedure several times, the adversary collects several sets of possible temporary IDs, from which he can do set intersection to get the temporary ID associated with the user's cellphone. Practical experiments on T-Mobile and AT&T GSM networks show that after 2 or 3 repetitions, the adversary can pinpoint the temporary ID of a user's cellphone [Kune et al., 2012]. To keep the user unaware of the attack, the connection request to his cellphone has to be terminated before a connection is established, but after the paging message is sent out. In [Kune et al., 2012], the authors, through experiments, show that by calling the target's number and hanging up within 5 seconds, a paging message would be sent out, but the user's phone would not ring. Another way of achieving this goal is to send "silent SMS", a controversial method used by German and French police to track people [Nohl and Munaut, 2010], [F-Secure, 2011].

Addressing the attack, the mitigations in [Kune et al., 2012] either require additional control signaling (sending paging messages out to several tracking areas, changing TMSI more frequently), or introduce delay in response to users' requests.

We propose a solution that requires neither. In fact, it requires less signaling than the current standard. However, it does require additional signal processing steps and therefore needs to be incrementally deployed. We want to emphasize that even though the additional signal processing is not in the standard, it is not computationally expensive. Therefore the effect on power consumption of the UEs is minimal. Our technique is inspired by the physical layer authentication scheme in [Yu et al., 2008b], [Yu et al., 2008a]. In those works, Yu *et al.* describe a stealthy authentication technique in which the authenticating entity's credential is embedded as a watermark in the transmitted physical waveform. The authenticator detects the presence of the tag in the received waveform, and decides whether the waveform was transmitted by the legitimate transmitter or not. We extend this technique to the LTE paging system by assigning to each user equipment (UE) a unique tag. These tags are superimposed onto the paging transmitted waveform if the corresponding UEs are paged. The tags are transmitted with very low power such that they can only be *detected*, and not *decoded*. By detecting the presence of its tag, a UE learns that it is paged. Because of the stealth property of the tags, an eavesdropper observing the paging waveform learns nothing about who are being paged.

5.1.2 Summary of contributions

Our contributions in this chapter are

1. We show that the LTE paging architecture suffers from the vulnerability identified in [Kune et al., 2012].

2. We propose a solution based on signal processing, which makes use of physical layer identification to convey paging messages. Our solution does not require additional control signaling, and can in fact save bandwidth for downlink data transmission.

5.1.3 Outline of chapter

The chapter is structured as follows. In Section 5.2, we review the LTE paging system and show that it has the same vulnerability as the GSM system. Next, in Section 5.3, we describe our scheme. In Section 5.4, we evaluate the performance of our scheme through simulations. We finish with some conclusions and remarks.

5.2 LTE Paging System

In this section, we highlight some technical specifications of LTE which allow us to conclude that the location attack in [Kune et al., 2012] can be performed in an LTE network. We will use these details in the analysis of our scheme in subsequent sections.

Control signaling: In contrast to the GSM architecture, in LTE there is no dedicated resource for paging. Instead, the paging messages are delivered in the same frequency band as normal data; and the existence of such paging messages in each subframe (1ms) is indicated in the control channel. In normal operation mode, at the beginning of each LTE downlink subframe, there are up to 4 (out of 14) OFDM symbols used to transmit control data. These *Downlink Control Information* (DCI)

messages carry resource allocation information, Hybrid-ARQ, system information and paging indicator among others. Each control message is encapsulated in a *Physical Downlink Control Channel* (PDCCH) message. The DCI can be targeted to a specific user equipment (UE), or a group of UEs as in the case of a paging indicator. If the DCI is for a specific UE, the 16-bit CRC generated for that DCI will be XORed with the last 16 bits of the temporary ID of the targeted UE (e.g. *Cell Radio Network Temporary Identifier* C-RNTI). If the DCI is for a group of UEs, its CRC will be masked with one of the predefined IDs for group control information. The paging indicator ID, P-RNTI, is *FFFE* (in hexadecimal) [3GPP, 2011a].

UE decoding: The UEs do not know a priori which PDCCH in the control region of a subframe is intended for them. Therefore they perform *blind decoding*, in which they try all possible sizes of PDCCH. The list of such allowable sizes can be found in [3GPP, 2011c]. If after unmasking the CRC of a possible PDCCH message with either a common ID or the UE's temporary ID, the CRC check returns true, then the UE knows that it has successfully decoded a valid PDCCH message. To reduce the number of PDCCH the UEs have to try to decode, each UE is given a *search space*. The search space is all possible starting positions of a PDCCH. There are UE-specific search spaces and common search spaces. The latter are locations which all UEs have to try decoding from. Group control information, including paging indicator, is sent on the common search space. Due to the requirement that broadcast control information has to reach users with poor channel conditions, group PDCCH have bigger sizes than other PDCCH, which allows for lower code rates to be used. Two allowable sizes for these PDCCH are 72 and 144 *resource elements* [3GPP,

2011c]. Resource element is the smallest resource unit in LTE, comprising of 1 subcarrier in 1 OFDM symbol. All control information are modulated with QPSK, therefore the paging PDCCH can have either 144 or 288 bits.

The DCI format for paging indicator is either 1A or 1C [3GPP, 2011c]. Depending on the system bandwidth (1.4 - 20 MHz), DCI format 1A, and 1C can have 36 - 44, and 24 - 31 bits respectively [Baker and Mousley, 2011]. This DCI has the location of the paging record in the data portion of the subframe. The UE decodes that location in the *Physical Downlink Shared Channel* (PDSCH) to get the record. The paging record contains a list of IDs of UEs being paged, which can be either *System Architecture Evolution TMSI* (S-TMSI) or *International Mobile Subscriber Identity* (IMSI) [3GPP, 2011d]. In normal cases, the temporary ID S-TMSI is used instead of the permanent ID IMSI. If the UE sees its ID in the list, it knows that it is paged. Figure 5.1 illustrates an example of paging PDCCH and PDSCH positions in an LTE downlink subframe.

Attacker model: We will use an analogous attacker model as [Kune et al., 2012]. The only difference is that our attacker is capable of causing paging request messages in LTE networks and listen on LTE paging channels. While the first capability of the attacker remains the same as in the original paper, the above procedure serves to justify the practicality of the second capability. The attacker can listen on the control channel, and unmask PDCCH with P-RNTI. Once he decodes a paging indicator, he can go the specified location in PDSCH to obtain the list of paged IDs. In [Kune et al., 2012], Kune *et al.* use an open source GSM baseband software implementation [Osmocombb,] to read the TMSI of paged MSs.

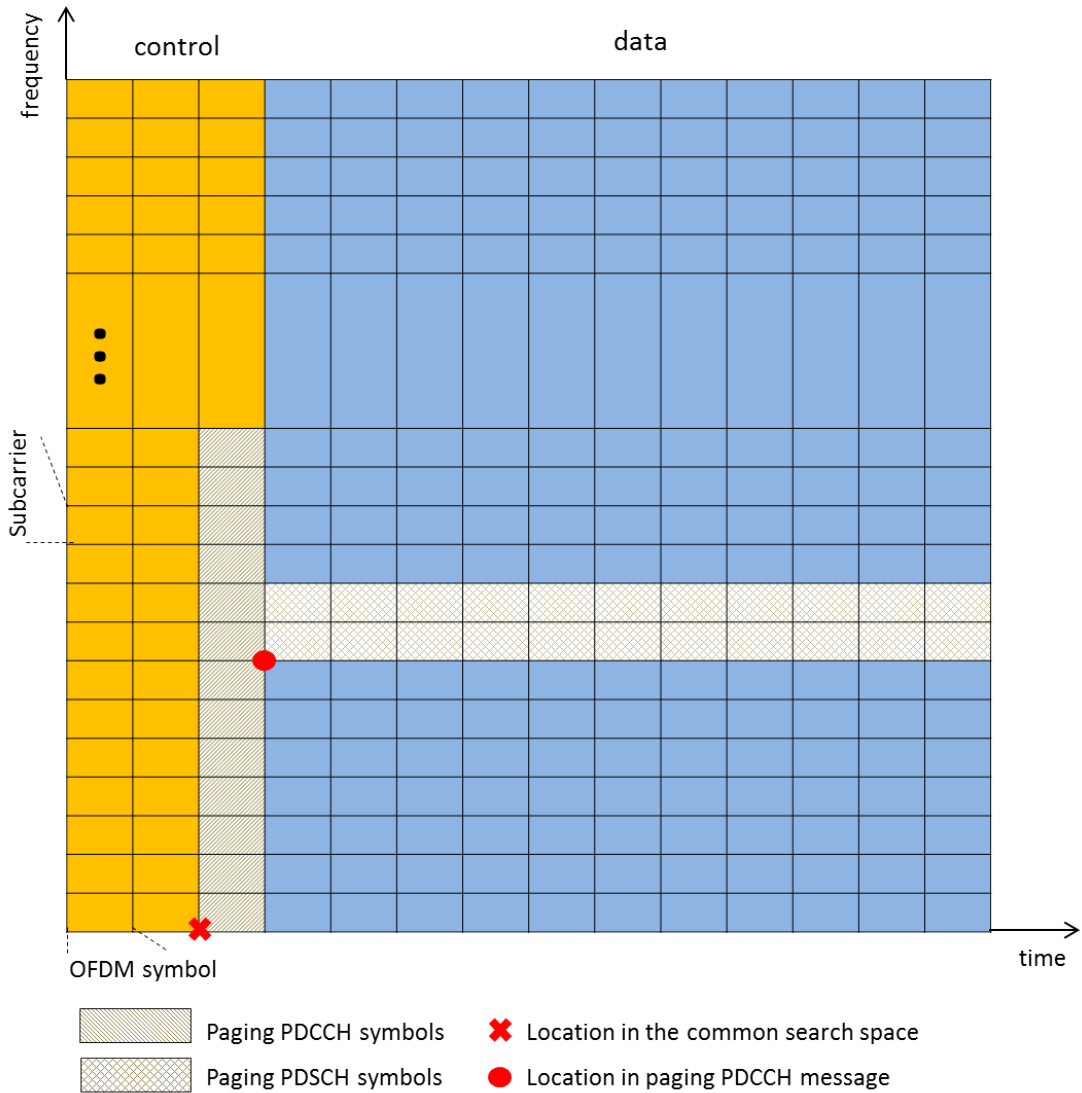


Figure 5.1: An example of positions of paging PDCCH and PDSCH in an LTE downlink subframe. Pilots and other types of physical channels are omitted for clarity.

While an equivalent open source software for LTE baseband is not available at this moment, it is reasonable to expect that one will be developed in the future. We therefore conclude that the same location attack is feasible in LTE, and security measures should be taken proactively.

5.3 Privacy-Enhanced Paging Messages

To combat the vulnerability in the LTE paging system described in Section 5.2, we propose to use a UE's temporary ID as an input to create a tag unique to that UE. If a UE is paged during a subframe, its tag is embedded onto the paging PDCCH. The only requirement for the tags is that tags from 2 different UEs are uncorrelated. Here "embed" means that the tag is superimposed onto the PDCCH QPSK symbols. To be backward compatible with older user equipment, the content of the paging indicator is left unchanged. A simple scenario where one old UE (Alice) and one new UE (Bob) are paged in the same subframe is illustrated in Figure 5.2. If the tag embedding does not cause too much degradation to the PDCCH signal quality, Alice is still able to decode the control information and follow the standard procedure to see if she is paged. Bob, however, can determine if he is paged just by detecting the presence of his unique tag in the PDCCH. Therefore he does not need to decode the PDSCH, which saves battery considering that most UEs which expect paging messages are in idle mode. Listening on the paging channel, Eve can obtain Alice's temporary ID, but she cannot get Bob's tag. As will be shown later, Bob's tag is transmitted with very low power so that nobody (including Bob) can decode it.

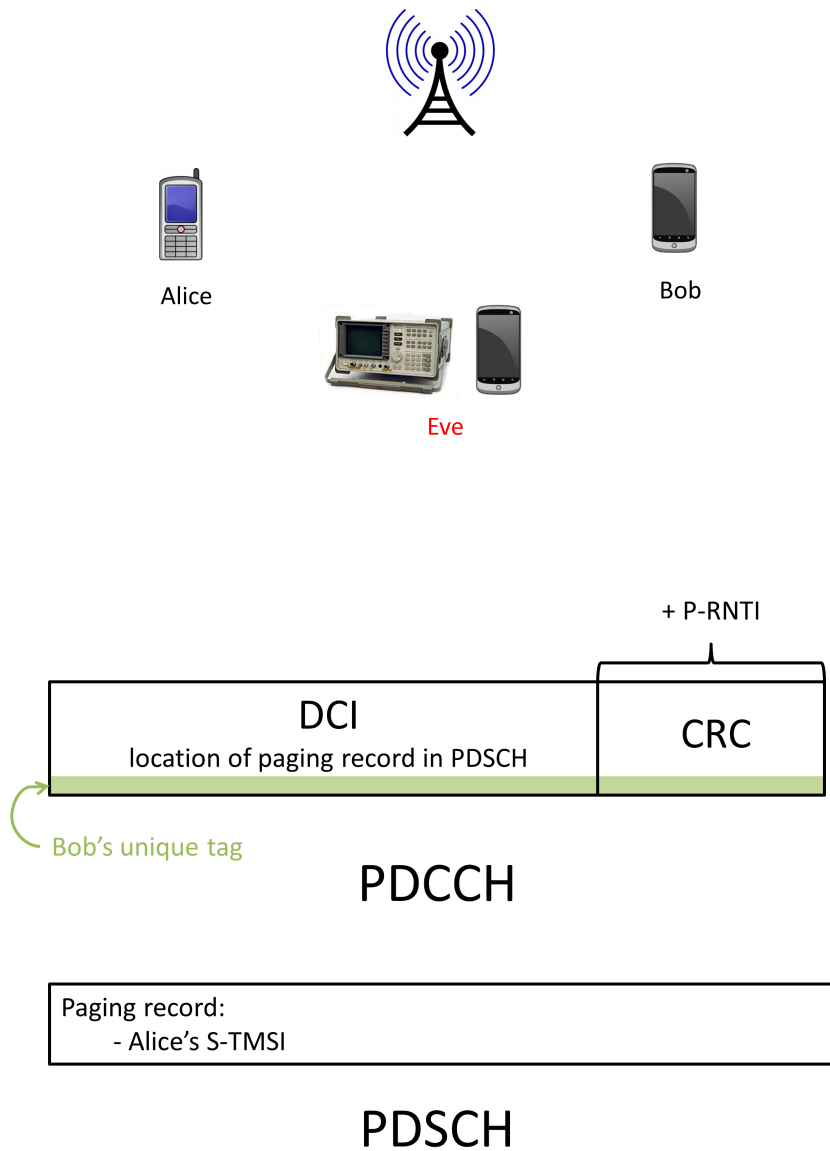


Figure 5.2: (a) Simple scenario with one old UE (Alice) and one new UE (Bob) being paged at the same subframe. The eavesdropper, Eve, can listen on the paging broadcast channel and analyze the PDCCH waveform; (b) PDCCH and PDSCH paging messages

Bob, however, can detect the presence of his tag in the paging PDCCH. Another benefit of this scheme comes in the form of downlink data bandwidth increase. Since Bob's ID is no longer needed to be transmitted in PDSCH, that bandwidth can be used for data transmission. The new UE capability as well as paging mechanism can be negotiated with the base station (eNodeB in LTE terms) at connection establishment. The operations at the eNodeB and UE are shown in Figure 5.3.

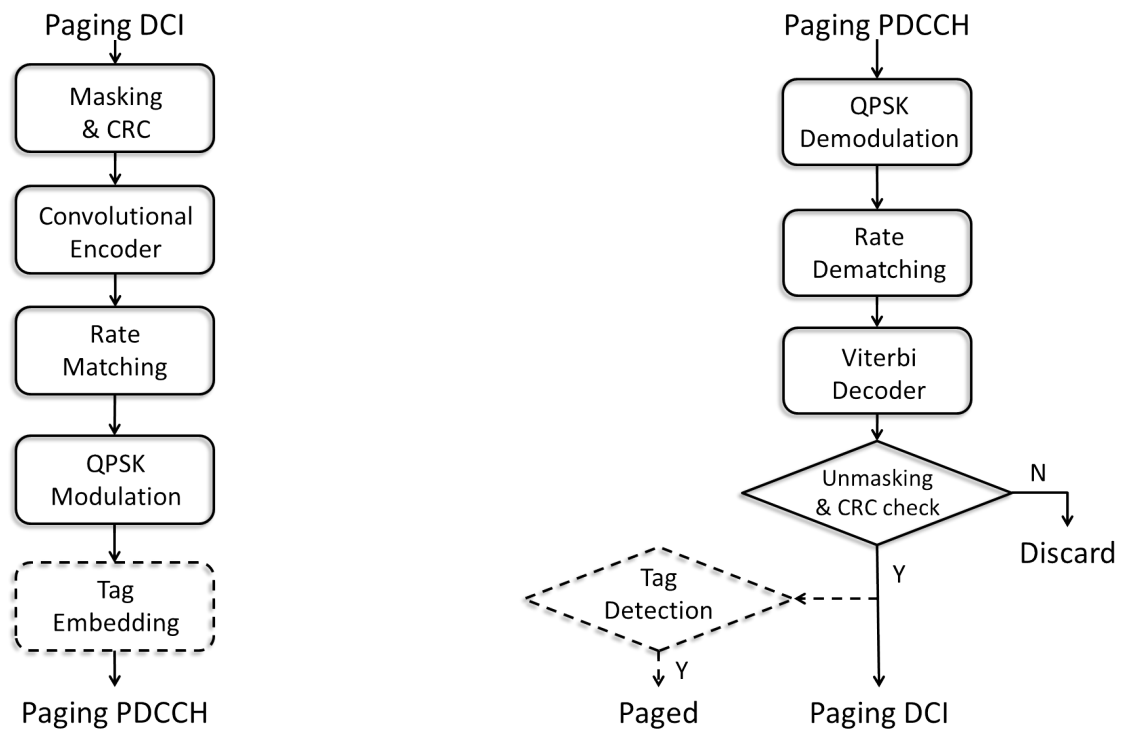


Figure 5.3: Flow charts for (a) eNodeB and (b) User Equipment. Dashed boxes are additional operations required by the scheme.

To maximize the robustness of the tags, we choose to put a tag symbol on every paging indicator PDCCH symbol. We use QPSK to modulate the tags. With this configuration, the tags have the same length as the paging indicator PDCCH, which

is either 144 or 288 bits. During a subframe, multiple tags can be superimposed on the same PDCCH, corresponding to multiple UEs being paged at the same time. In LTE standard, the maximum size of the paging record is 16 [3GPP, 2011d]. In other words, the 3GPP standard leaves room for up to 16 UEs to be paged during 1 subframe. In subsequent sections, we analyze the performance of our scheme with respect to the number of simultaneous tags, N_t .

5.3.1 eNodeB Operations

Let \mathbf{b} be the paging DCI. The PDCCH symbols that encapsulate this DCI are $\mathbf{s} = f_e(\mathbf{b})$. Here $f_e(\cdot)$ is the encoding function, which includes CRC, convolutional encoding, rate matching, and QPSK modulation. Let $\mathbf{k}_i, i = 1, \dots, N_t$, be the i^{th} paged UE's ID. Generate the tag $\mathbf{t}_i = g(\mathbf{k}_i)$. As mentioned above, the functionality of the generator function $g(\cdot)$ is to create uncorrelated tags. The elements of \mathbf{b} and \mathbf{k}_i are in bits; while the elements of \mathbf{s} and \mathbf{t}_i are in QPSK symbols $\{\pm 1, \pm i\}$. The tags are superimposed onto the PDCCH to create the transmitted message

$$\mathbf{x} = \rho_s \mathbf{s} + \frac{\rho_t}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}_i \quad (5.1)$$

Let $\mathbf{s} = (s^{(1)}, \dots, s^{(L)})$, i.e. there are L QPSK symbols in the PDCCH signal. For paging indicators, $L = 72$ or 144 . Assuming that each symbol of the PDCCH signal and of the tag has zero-mean and unit variance, we have

$$\begin{aligned} \mathbb{E}[s^{(k)}] &= 0, \mathbb{E}[|s^{(k)}|^2] = 1 & \text{for} & & k = 1, \dots, L \\ \mathbb{E}[t_i^{(k)}] &= 0, \mathbb{E}[|t_i^{(k)}|^2] = 1 & & & i = 1, \dots, N_t \end{aligned} \quad (5.2)$$

Since the tags are uncorrelated among themselves and independent of the PDCCH symbols,

$$\mathbb{E}[\mathbf{s}^H \mathbf{t}_i] = 0, \quad i = 1, \dots, N_t \quad (5.3)$$

$$\mathbb{E}[\mathbf{t}_i^H \mathbf{t}_j] = 0, \quad i, j = 1, \dots, N_t, \quad i \neq j \quad (5.4)$$

In (5.1), ρ_s and ρ_t are system parameters controlling the amount of power allocated to the signal and the tags, respectively. The power constraint is

$$\rho_s^2 + \rho_t^2 = 1 \quad (5.5)$$

From (5.1) - (5.5), we have

$$\begin{aligned} \mathbb{E}[\mathbf{s}] &= \mathbb{E}[\mathbf{t}_i] = \mathbb{E}[\mathbf{x}] = 0 \\ \mathbb{E}[|\mathbf{s}|^2] &= \mathbb{E}[|\mathbf{t}_i|^2] = \mathbb{E}[|\mathbf{x}|^2] = L, \quad i = 1, \dots, N_t \end{aligned} \quad (5.6)$$

5.3.2 User Equipment Operations

5.3.2.1 Decode DCI

Assuming a frequency selective fading channel, the received signal at the UEs is

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w} \quad (5.7)$$

where \mathbf{H} is a diagonal matrix, with the elements being the attenuations at each subcarrier frequency. \mathbf{w} is thermal noise at the transmitter and receiver circuitry.

In LTE, pilot symbols are transmitted on fixed resource elements to help in channel estimation at the receivers [3GPP, 2011b]. There are many techniques that the

receiver can use to perform channel estimation, e.g. LMMSE [Edfors et al., 1998].

In general, the channel estimate can be written as

$$\hat{\mathbf{H}} = \mathbf{H} + \nu \quad (5.8)$$

where ν is the estimation error.

Let $\hat{H}^{(k)}, k = 1, \dots, L$ be the diagonal elements of $\hat{\mathbf{H}}$, the receiver estimates the message symbols as

$$\begin{aligned} \hat{x}^{(k)} &= \frac{\hat{H}^{(k)*}}{|\hat{H}^{(k)}|^2} y^{(k)} \\ &= x^{(k)} - \frac{\nu^{(k)} x^{(k)}}{\hat{H}^{(k)}} + \frac{w^{(k)}}{\hat{H}^{(k)}} \end{aligned} \quad (5.9)$$

It then decodes the DCI

$$\hat{\mathbf{b}} = f_d(\hat{\mathbf{x}}) \quad (5.10)$$

Here $f_d(\cdot)$ is the decoding function, which maps QPSK symbols to bits, undoes rate matching, performs Viterbi decoding, and removes CRC. After unmasking with the paging ID (*FFFFE*), the CRC check returns true if the DCI is successfully decoded.

5.3.2.2 Tag detection

The UE regenerates the message symbols from the decoded DCI, $\hat{\mathbf{s}} = f_e(\hat{\mathbf{b}})$, and subtracts it from the received signal to get the residue

$$\mathbf{r} = \frac{1}{\rho_t} (\hat{\mathbf{x}} - \rho_s \hat{\mathbf{s}}) \quad (5.11)$$

Assuming that the UE performs perfect channel estimation, we have

$$\mathbf{r} = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}_i + \frac{1}{\rho_t} \hat{\mathbf{H}}^{-1} \mathbf{w} \quad (5.12)$$

It then checks for the presence of its tag, \mathbf{t} , by performing hypothesis testing on the statistic

$$\tau = \mathbf{t}^H \mathbf{r} \quad (5.13)$$

The hypotheses are

$$H_0 : \mathbf{t} \text{ is not present in } \mathbf{r} \quad (\text{null hypothesis})$$

$$H_1 : \mathbf{t} \text{ is present in } \mathbf{r} \quad (\text{alternative hypothesis})$$

The statistic under null hypothesis:

$$\tau|H_0 = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}^H \mathbf{t}_i + \frac{1}{\rho_t} \mathbf{t}^H \hat{\mathbf{H}}^{-1} \mathbf{w} \quad (5.14)$$

Condition on \mathbf{t} , the second term in (5.14) is the sum of L Gaussian random variables

$$\eta_2 = \frac{1}{\rho_t} \mathbf{t}^H \hat{\mathbf{H}}^{-1} \mathbf{w} = \frac{1}{\rho_t} \sum_{k=1}^L \frac{t^{(k)*} w^{(k)}}{\hat{H}^{(k)}} \quad (5.15)$$

The resulting Gaussian random variable has mean zero and variance

$$\sigma_{\eta_2}^2 = \frac{1}{\rho_t^2} \sum_{k=1}^L \frac{\sigma_w^2}{|\hat{H}^{(k)}|^2} = \frac{1}{\rho_t^2} \sum_{k=1}^L \frac{1}{\gamma^{(k)}} \quad (5.16)$$

where $\gamma^{(k)}$ is the SNR of the k^{th} subcarrier.

The first term in (5.14) can be written as

$$\eta_1 = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}^H \mathbf{t}_i = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \sum_{k=1}^L t^{(k)*} t_i^{(k)} \quad (5.17)$$

η_1 is the sum of $N_t L$ i.i.d. symbols from the set $\{\pm 1, \pm i\}$. According to the Central Limit Theorem, it can be approximated by a Gaussian random variable with zero-mean and variance $\sigma_{\eta_1}^2 = L$.

From (5.14) - (5.17), we have

$$\tau|H_0 \sim \mathcal{N}\left(0, L + \frac{1}{\rho_t^2} \sum_{k=1}^L \frac{1}{\gamma^{(k)}}\right) \quad (5.18)$$

The statistic under alternative hypothesis: Without loss of generality, let $\mathbf{t} = \mathbf{t}_1$.

The statistic is

$$\tau|H_1 = \frac{1}{\sqrt{N_t}} \left(|\mathbf{t}_1|^2 + \sum_{i=2}^{N_t} \mathbf{t}_1^H \mathbf{t}_i \right) + \frac{1}{\rho_t} \mathbf{t}_1^H \hat{\mathbf{H}}^{-1} \mathbf{w} \quad (5.19)$$

Condition on \mathbf{t}_1 , the term inside the parentheses in (5.19) can be approximated as a Gaussian random variable with mean $|\mathbf{t}_1|^2 = L$ and variance $(N_t - 1)L$. Therefore

$$\tau|H_1 \sim \mathcal{N}\left(\frac{L}{\sqrt{N_t}}, \frac{N_t - 1}{N_t} L + \frac{1}{\rho_t^2} \sum_{k=1}^L \frac{1}{\gamma^{(k)}}\right) \quad (5.20)$$

The UE performs a threshold test on τ to determine the presence of its tag in the residue.

$$H = \begin{cases} H_0 & \text{if } \tau \leq \tau^0 \\ H_1 & \text{if } \tau > \tau^0 \end{cases} \quad (5.21)$$

In making the comparison in (5.21), we use only the real part of τ . The imaginary parts of $\tau|H_0$ and $\tau|H_1$ have very similar statistic, and therefore do not provide much information. By abuse of notation, we still call the real part τ . The threshold τ^0 is a value between $[0, L/\sqrt{N_t}]$. The greater τ^0 is, the higher the probability of miss detection; whereas the smaller τ^0 is, the higher the probability of false alarm. We choose $\tau^0 = L/2\sqrt{N_t}$ for good performance in both criteria. With this choice of the threshold, the probability of missing a tag is

$$P_m = \Phi\left(\frac{-\frac{L}{2\sqrt{N_t}}}{\left(\frac{N_t-1}{N_t}L + \frac{1}{\rho_t^2} \sum_{k=1}^L \frac{1}{\gamma^{(k)}}\right)^{1/2}}\right) \quad (5.22)$$

where $\Phi(\cdot)$ is the standard Gaussian cumulative distribution function. To get an idea of the theoretical performance of the scheme, let us look at a special case where the channel is flat fading with SNR = 10dB. Assume 10% of the transmitted power is allocated to tags, i.e. $\rho_t^2 = 0.1$; and 288 bits are used for PDCCH message, i.e. $L = 144$. When 4 users are paged simultaneously, i.e. $N_t = 4$, we have $P_m = 0.01$. So we can see under that condition, the tags are detected 99% of the time.

5.4 Simulations

As mentioned in Section 5.2, the PDCCH messages are designed to be very robust. In particular, convolutional code with low rate (1/3) is used. In addition, the paging DCI message can have 24 - 44 bits. Together with a 16-bit CRC, the size of the message before convolutionally encoded ranges from 40 to 60 bits. Thus the size of the message after convolutionally encoded ranges from 120 to 180 bits. When the PDCCH size is 144 bits, puncture may occur during rate matching. When the PDCCH size is 288 bits, redundant encoded bits are transmitted, which effectively increases the SNR at the receiving UEs. In order to evaluate the effect of our embedded tags on the probability of successfully decoding the DCI, we first simulate the DCI decoding performance with respect to different SNR levels. The result is shown in Figure 5.4. Here we use the energy per bit to noise power spectral density (EbNo) as the metric for SNR. Also shown is BER of the PDCCH message at the same EbNo levels. Figure 5.4 gives us a clear intuition of the PDCCH BER requirements for various DCI decoding performances. For instance, with PDCCH

size of 288 bits, we can see that the probability of unsuccessfully decoding a paging DCI decreases rapidly from 0.4 at $E_b/N_0 = -1$ to 10^{-5} at $E_b/N_0 = 5$. Thanks to the convolutional encoder, the BER requires for PDCCH to achieve 10^{-5} DCI error rate is only 0.03. When the size of PDCCH is 144 bits, the UEs need an additional 1dB in SNR to get equivalent performance.

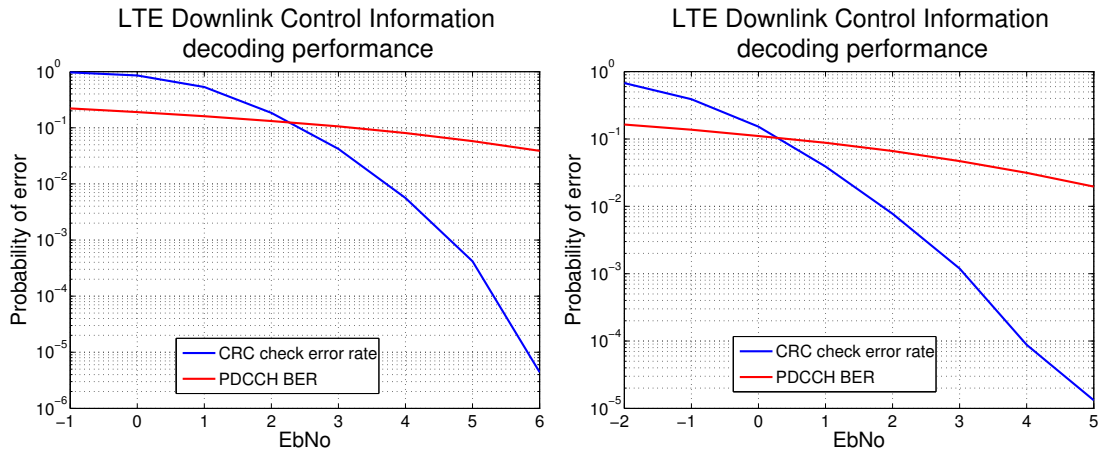


Figure 5.4: DCI decoding performance as a function of SNR. Here the DCI size is 44 bits. The PDCCH size is (a) 144 bits, (b) 288 bits

Next we want to see the effect of allocating part of the transmission power to the tags on the PDCCH BER. As long as the resulting BER conforms to the requirement obtained above, our scheme will not have negative effect on the DCI decoding performance. Figure 5.5 shows the BER of PDCCH message for various tag powers. We can see that the effect of tag embedment is minimal for $\rho_t^2 \leq 0.02$. When the channel condition is good, e.g. $E_b/N_0 = 10\text{dB}$, 20% of the power can be allocated to tags, which results in BER of 0.04. Referring back to Figure ??, this BER corresponds to a DCI decoding error rate of 10^{-4} .

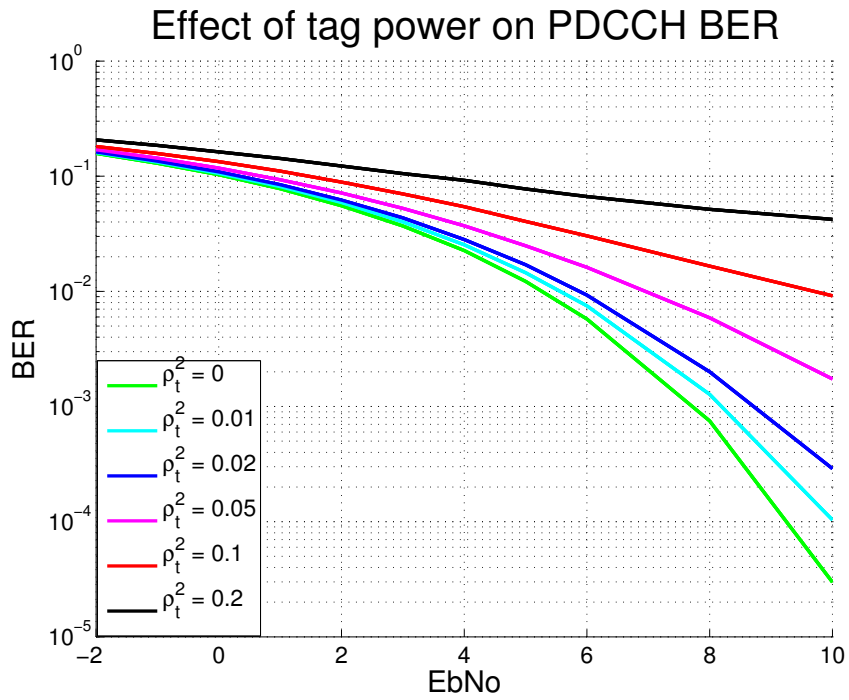


Figure 5.5: PDCCH BER for various values of tag power allocation. Here the PDCCH size is 288 bits, 16 tags are embedded.

After confirming that we can indeed allocate part of the transmission power to the identification tags, we evaluate the tag detection performance under various system settings. In particular, we alter 3 parameters: tag length, tag power and number of simultaneous tags. We expect the detection performance to increase with tag length and decrease with number of simultaneous tags. Referring back to (5.18) and (5.20), we see that the variance of the test statistic decreases monotonically with increased tag power, and therefore the detection performance will increase monotonically with increased tag power. However, we also know that increasing tag power degrades DCI decoding performance. If that degradation causes the UEs to fail to decode the paging PDCCH then the tags will be useless. Referring to Figure 5.5, we choose tag power allocation $\rho_t^2 = 0.05$ to be conservative.

Figure 5.6 shows the probability of detecting that the unique tag for a UE is present in 2 cases: the UE is being paged, and the UE is not being paged (misdetection). We can see a clear superior performance when 288-bit PDCCH is used. Let us consider a rather bad channel condition, $E_b/N_0 = 2\text{dB}$, 4 UEs are paged simultaneously. Figure 5.6 shows that our scheme still provides tag detection rate of 90% and false alarm rate of 2% if we use 288-bit PDCCH and allocate 5% of the transmission power for the tags. A natural question would be how this performance compares to the current paging system's. Both schemes rely on the successful decoding of the paging PDCCH. After this stage, our scheme's performance ties directly to the detection probability of the tags; whereas the current scheme's performance depends on the success of decoding the paging PDSCH. Since these are apples and oranges, a meaningful comparison can only be done through experiments. We are certainly

interested in pursuing them in our future work. For now, it is worth noticing that the constellation size and code rate used for data channels are a lot more aggressive than those used for control channels. Therefore it is expected that decoding performance of data channels are worse than that of control channels in the same SNR condition.

The idea behind the physical layer identification technique is to make use of channel noise to obfuscate the tags at the eavesdropper. Assuming that the eavesdropper, Eve in Figure 5.2, successfully decodes the paging PDCCH, regenerates the signal \mathbf{s} in (5.1), and subtracts it from her received waveform. What she has left is the sum of the superimposed tags and the channel noise. Since the individual tags are modulated as QPSK symbols $\{\pm 1, \pm i\}$, the normalized sum of multiple tags will have the constellation as in Figure 5.7. The identity of a UE's tag, say Bob's, is hidden under 2 layers. First, the channel noise limits Eve to only partial information about the normalized sum of the tags. Second, since the tags are uncorrelated, the sum of them does not reveal any information about Bob's tag to Eve. We conclude that Eve has no reliable way of obtaining Bob's tag, and thus she cannot perform the location attack described in Section 5.1.

5.5 Conclusions

In this chapter we have proposed a novel method to page user equipments in LTE network while protecting their privacy. The proposed method makes use of physical layer identification tags, which are designed to be robust and stealthy. Our

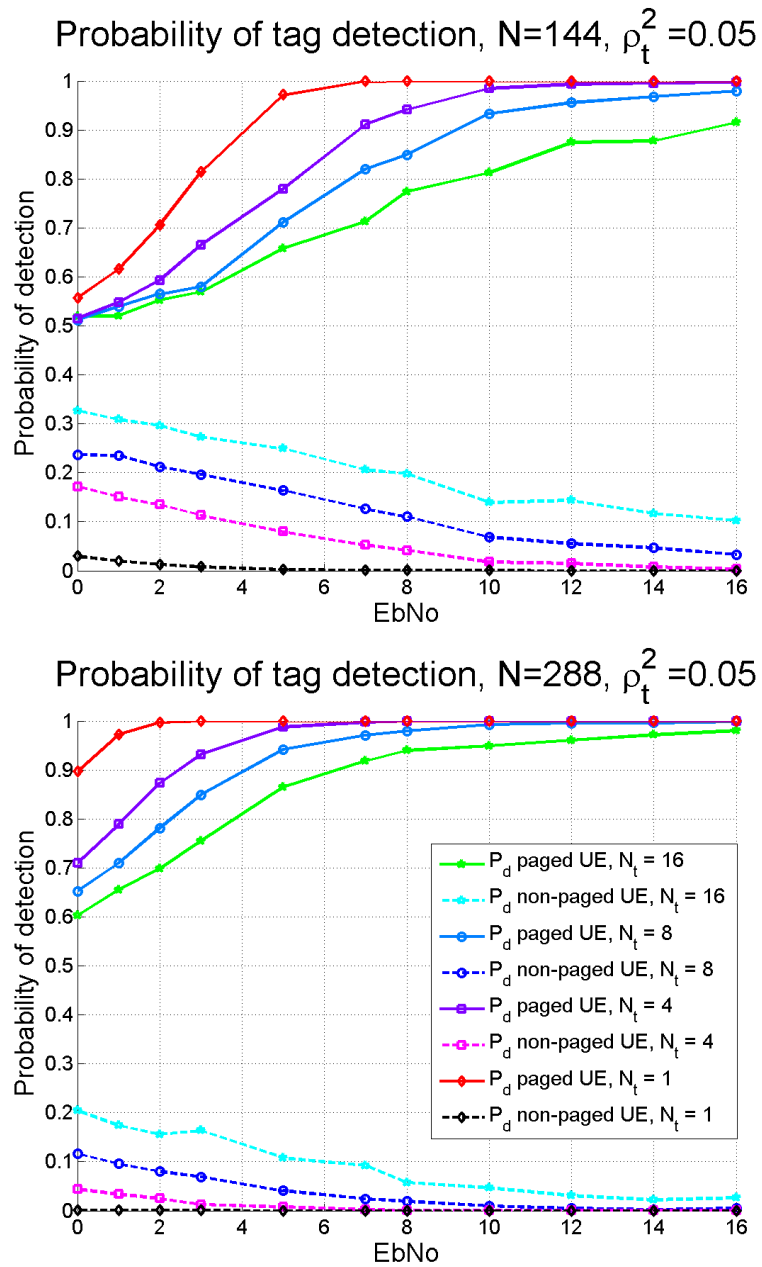


Figure 5.6: Probability of tag detection for PDCCH size (a) 144 bits, (b) 288 bits.

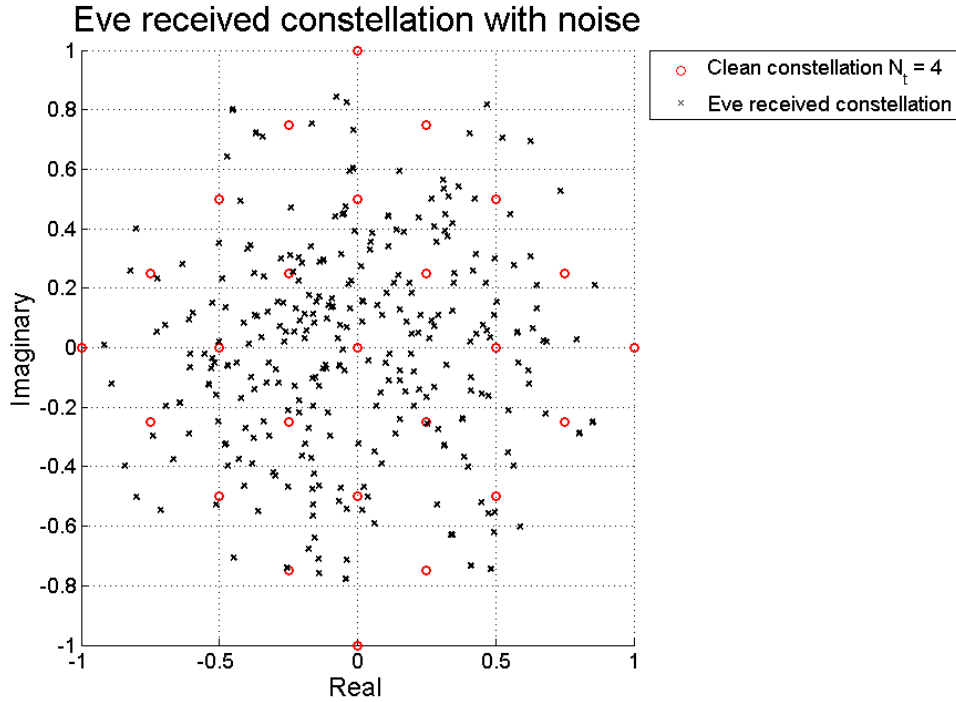


Figure 5.7: Eavesdropper’s received constellation at SNR = 20dB, $N_t = 4$.

scheme protects the privacy of paged users by hiding their ID in the transmitted waveforms. Using channel noise to our advantage, the scheme prevents an attacker from decoding the paged user’s tag. As a result, attacks on the open nature of paging channel, e.g. [Kune et al., 2012], are no longer a threat. The scheme also provides bandwidth saving by not requiring the actual user IDs to be transmitted. Here we analyze our technique specifically for an LTE network; however, our technique is also applicable to other cellular networks such as GSM, WCDMA, WiMAX.

Bibliography

- [cpl,] IBM CPLEX Optimizer. www.ibm.com/software/commerce/optimization/cplex-optimizer/.
- [lem,] Library for Efficient Modeling and Optimization in Networks. <http://lemon.cs.elte.hu/trac/lemon>.
- [3GPP, 1998] 3GPP (1998). Selection procedures for the choice of radio transmission technologies of the UMTS.
- [3GPP, 2010] 3GPP (2010). Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects (v9.0.0).
- [3GPP, 2011a] 3GPP (2011a). Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (version 10.4.0).
- [3GPP, 2011b] 3GPP (2011b). Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (version 10.4.0).
- [3GPP, 2011c] 3GPP (2011c). Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (version 10.4.0).
- [3GPP, 2011d] 3GPP (2011d). Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (v10.4.0).
- [3GPP, 2012] 3GPP (2012). LTE Radio Access Network (RAN) enhancements for diverse data applications.
- [3GPP, 2013] 3GPP (2013). Technical Specification Group Services and System Aspects; Feasibility study for Proximity Services (ProSe) (version 12.1.0).
- [3GPP, 2014a] 3GPP (2014a). Draft Report of 3GPP TSG RAN WG1 #78 v0.2.0.
- [3GPP, 2014b] 3GPP (2014b). R1-143442, WF on T-RPT Patterns for SA and Data.

- [3GPP, 2014c] 3GPP (2014c). Study on LTE Device to Device Proximity Services; Radio Aspects (v12.0.1).
- [Ananthanarayanan et al., 2007] Ananthanarayanan, G., Padmanabhan, V. N., Ravindranath, L., and Thekkath, C. A. (2007). Combine: leveraging the power of wireless peers through collaborative downloading. In *Proceedings of the 5th international conference on Mobile systems, applications and services*, pages 286–298. ACM.
- [Anderegg and Eidenbenz, 2003] Anderegg, L. and Eidenbenz, S. (2003). Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, MobiCom '03, pages 245–259, New York, NY, USA. ACM.
- [Arthur, 2011] Arthur, C. (2011). How the smartphone is killing the PC. <http://www.guardian.co.uk/technology/2011/jun/05/smartphones-killing-pc>.
- [Badic et al., 2009] Badic, B., O'Farrell, T., Loskot, P., and He, J. (2009). Energy efficient radio access architectures for green radio: Large versus small cell size deployment. In *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, pages 1–5.
- [Baker, 2011] Baker, M. (2011). *Uplink Transmission Procedures*, chapter 18, pages 449–462. John Wiley & Sons, Ltd.
- [Baker and Moulosley, 2011] Baker, M. and Moulosley, T. (2011). *Downlink Physical Data and Control Channels*, chapter 9, pages 189–214. John Wiley & Sons, Ltd.
- [Berl et al., 2010] Berl, A., Gelenbe, E., di Girolamo, M., Giuliani, G., de Meer, H., Dang, M. Q., and Pentikousis, K. (2010). Energy-Efficient Cloud Computing. *The Computer Journal*, 53:1045–1051.
- [Bonta et al., 2007] Bonta, J., Calcev, G., Fonseca, B., Mangalvedhe, N., and Smith, N. (2007). Ad Hoc Relay Mode for Mobile Coverage Extension and Peer-to-Peer Communications.
- [Bremaud, 1999] Bremaud, P. (1999). *Markov Chains, Gibbs Fields, Monte Carlo Simulations, and Queues*. Springer.
- [Brenner and Smith, 2013] Brenner, J. and Smith, A. (2013). 72% of online adults are social networking site users. *Pew Research Center, Washington, D.C.* Accessed: July 14, 2014.
- [Burke et al., 2006] Burke, J. A., Estrin, D., Hansen, M., Parker, A., Ramanathan, N., Reddy, S., and Srivastava, M. B. (2006). Participatory sensing. *Center for Embedded Network Sensing*.

- [Buttayan and Hubaux, 2001] Buttayan, L. and Hubaux, J.-P. (2001). Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Technical report.
- [Chang et al., 2003] Chang, R.-S., Chen, W.-Y., and Wen, Y.-F. (2003). Hybrid wireless network protocols. *IEEE Transactions on Vehicular Technology*, 52(4):1099 – 1109.
- [Chen and Chan, 2010] Chen, B. B. and Chan, M. C. (2010). Mobicent: a credit-based incentive system for disruption tolerant network. In *INFOCOM, 2010 Proceedings IEEE*, pages 1 –9.
- [Chon et al., 2013] Chon, Y., Ryu, W., and Cha, H. (2013). Predicting smartphone battery usage using cell tower id monitoring. *Pervasive and Mobile Computing*, (0):-.
- [Cisco, 2014] Cisco (2014). Global Mobile Data Traffic Forecast Update, 2013-2018.
- [Duan et al., 2012] Duan, L., Kubo, T., Sugiyama, K., Huang, J., Hasegawa, T., and Walrand, J. (2012). Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing. In *INFOCOM, 2012 Proceedings IEEE*, pages 1701 –1709.
- [Edfors et al., 1998] Edfors, O., Sandell, M., van de Beek, J.-J., Wilson, S., and Borjesson, P. (1998). OFDM channel estimation by singular value decomposition. *IEEE Trans. on Communications*, 46(7):931 –939.
- [Elkotby et al., 2012] Elkotby, H., Elsayed, K., and Ismail, M. (2012). Exploiting interference alignment for sum rate enhancement in d2d-enabled cellular networks. In *Proceedings of IEEE WCNC 2012*.
- [F-Secure, 2011] F-Secure (2011). 440,783 “Silent SMS” Used to Track German Suspects in 2010. <http://www.f-secure.com/weblog/archives/00002294.html>.
- [Falaki et al., 2010] Falaki, H., Mahajan, R., Kandula, S., Lymberopoulos, D., Govindan, R., and Estrin, D. (2010). Diversity in smartphone usage. In *Proceedings of the 8th international conference on Mobile systems, applications, and services, MobiSys '10*, pages 179–194, New York, NY, USA. ACM.
- [Garnica et al., 2013] Garnica, J., Chinga, R., and Lin, J. (2013). Wireless power transmission: From far field to near field. *Proceedings of the IEEE*, 101(6):1321–1331.
- [Gelenbe, 2012] Gelenbe, E. (2012). Energy packet networks: Adaptive energy management for the cloud. In *Proceedings of the 2Nd International Workshop on Cloud Computing Platforms, CloudCP '12*, pages 1:1–1:5, New York, NY, USA. ACM.

- [Janis et al., 2009] Janis, P., Yu, C.-H., Doppler, K., Ribeiro, C., Wijting, C., and Hugl, K. (2009). Device-to-device communication underlaying cellular communications systems. *International Journal of Communications, Network and System Sciences*.
- [Jeronimo, 2014] Jeronimo, F. (2014). Top 10 Smartphone Purchase Drivers. <https://twitter.com/fjeronimo/status/465896917298577409>.
- [Jiang et al., 2013] Jiang, Y., Jaiantilal, A., Pan, X., Al-Mutawa, M. A., Mishra, S., and Shi, L. (2013). Personalized energy consumption modeling on smartphones. In *Mobile Computing, Applications, and Services*, pages 343–354. Springer.
- [Kansal et al., 2007] Kansal, A., Hsu, J., Zahedi, S., and Srivastava, M. B. (2007). Power management in energy harvesting sensor networks. *ACM Transactions on Embedded Computing Systems*, 6(4).
- [Király and Kovács, 2012] Király, Z. and Kovács, P. (2012). Efficient implementations of minimum-cost flow algorithms. *CoRR*, abs/1207.6381.
- [Kone et al., 2010] Kone, V., Yang, L., Yang, X., Zhao, B. Y., and Zheng, H. (2010). On the feasibility of effective opportunistic spectrum access. In *Proceedings of the 10th annual conference on Internet measurement, IMC '10*, pages 151–164, New York, NY, USA. ACM.
- [Kuhn, 1955] Kuhn, H. W. (1955). The Hungarian method for the assignment problem. *Naval Research Logistics*, 2:83–97.
- [Kune et al., 2012] Kune, D. F., Koelndorfer, J., Hopper, N., and Kim, Y. (2012). Location leaks over the GSM air interface. In *Proc. 19th Annual Network and Distributed System Security Symposium*.
- [Kyosti et al., 2007] Kyosti, P., Meinila, J., Jamsa, T., Zhao, X., Hentila, L., Ylitalo, J., and Alatosava, M. (2007). WINNER II Channel Models.
- [Laurila et al., 2012] Laurila, J. K., Gatica-Perez, D., Aad, I., Bornet, O., Do, T.-M.-T., Dousse, O., Eberle, J., Miettinen, M., et al. (2012). The mobile data challenge: Big data for mobile computing research. In *Pervasive Computing*, number EPFL-CONF-192489.
- [Lopez-Perez et al., 2014] Lopez-Perez, D., Chu, X., Vasilakos, A., and Claussen, H. (2014). Power minimization based resource allocation for interference mitigation in ofdma femtocell networks. *IEEE Journal on Selected Areas in Communications*, 32(2):333–344.
- [Meshkati et al., 2009] Meshkati, F., Poor, H., Schwartz, S., and Balan, R. (2009). Energy-efficient resource allocation in wireless networks with quality-of-service constraints. *IEEE Transactions on Communications*, 57(11):3406–3414.

- [Miao et al., 2010] Miao, G., Himayat, N., and Li, G. (2010). Energy-efficient link adaptation in frequency-selective channels. *IEEE Transactions on Communications*, 58(2):545–554.
- [Michael et al., 2000] Michael, L., Kikuchi, S., Adachi, T., and Nakagawa, M. (2000). Combined cellular/direct method of inter-vehicle communication. In *Proceedings of the IEEE Intelligent Vehicles Symposium*, pages 534–539.
- [Morstatter et al., 2013] Morstatter, F., Pfeffer, J., Liu, H., and Carley, K. M. (2013). Is the sample good enough? comparing data from twitter’s streaming api with twitter’s firehose. In *ICWSM*.
- [Nakamoto, 2009] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
- [Ng and Yu, 2007] Ng, T. and Yu, W. (2007). Joint optimization of relay strategies and resource allocations in cooperative cellular networks. *IEEE Journal on Selected Areas in Communications*, 25(2):328–339.
- [Nisan et al., 2007] Nisan, N., Roughgarden, T., Tardos, E., and Vazirani, V. V. (2007). *Algorithmic Game Theory*. Cambridge University Press, New York, NY, USA.
- [NIST, 2014] NIST (2014). Incomplete beta functions. <http://dlmf.nist.gov/8.17>.
- [Nohl and Munaut, 2010] Nohl, K. and Munaut, S. (2010). GSM Sniffing. http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf.
- [Nokia Corporation, 2012] Nokia Corporation (2012). Further results on network signalling load and UE power consumption (R2-120367).
- [Oliver and Keshav, 2011] Oliver, E. A. and Keshav, S. (2011). An empirical approach to smartphone energy level prediction. In *Proceedings of the 13th international conference on Ubiquitous computing, UbiComp ’11*, pages 345–354, New York, NY, USA. ACM.
- [Osmocombb,] Osmocombb. Open source GSM baseband software implementation. <http://bb.osmocom.org/trac/>. Accessed: August 3, 2014.
- [PRC, 2014] PRC (2014). Cell phone and smartphone ownership demographics. *Pew Research Center, Washington, D.C.* Accessed: July 14, 2014.
- [Raghothaman et al., 2013] Raghothaman, B., Deng, E., Pragada, R., Sternberg, G., Deng, T., and Vanganuru, K. (2013). Architecture and protocols for LTE-based device to device communication. In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 895–899.

- [Rahmati et al., 2007] Rahmati, A., Qian, A., and Zhong, L. (2007). Understanding human-battery interaction on mobile phones. In *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*, pages 265–272. ACM.
- [Renesas Mobile Europe Ltd., 2012] Renesas Mobile Europe Ltd. (2012). Impact of DRX to always-on background traffic (R2-120578).
- [Sadek et al., 2006] Sadek, A. K., Han, Z., and Liu, K. R. (2006). An efficient cooperation protocol to extend coverage area in cellular networks. In *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, volume 3, pages 1687–1692. IEEE.
- [Soyez, 2012] Soyez, F. (2012). Getting the message? Police track phones with silent SMS. <http://owni.eu/2012/01/27/silent-sms-germany-france-surveillance-deveryware/>.
- [Ta,] Ta, T. Battery deposit service simulator. <https://github.com/tuan-ta/bds>.
- [Ta and Baras, 2012] Ta, T. and Baras, J. S. (2012). Enhancing Privacy in LTE Paging System using Physical Layer Identification. In *Proc. 7th International Workshop on Data Privacy Management*.
- [Ta et al., 2014] Ta, T., Baras, J. S., and Zhu, C. (2014). Improving Smartphone Battery Life Utilizing Device-to-device Cooperative Relays Underlying LTE Networks. In *IEEE International Conference on Communications*.
- [Tesseract,] Tesseract. Tesseract OCR. <https://code.google.com/p/tesseract-ocr/>. Accessed: July 14, 2014.
- [TweePy,] Tweepy. Tweepy. <http://www.tweepy.org/>. Accessed: July 14, 2014.
- [Twitter,] Twitter. Twitter Streaming API. <https://dev.twitter.com/docs/api/streaming>. Accessed: July 14, 2014.
- [Wei et al., 2006] Wei, K., Smith, A., Chen, Y.-F., and Vo, B. (2006). Whopay: A scalable and anonymous payment system for peer-to-peer environments. In *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*, pages 13–13.
- [Xu and van der Schaar, 2013] Xu, J. and van der Schaar, M. (2013). Token system design for autonomic wireless relay networks. *IEEE Transactions on Communications*, 61(7):2924–2935.
- [Yang et al., 2013] Yang, M. J., Lim, S. Y., Park, H. J., and Park, N. H. (2013). Solving the data overload: Device-to-device bearer control architecture for cellular data offloading. *IEEE Vehicular Technology Magazine*, 8(1):31–39.

- [Yu et al., 2011] Yu, C.-H., Doppler, K., Ribeiro, C., and Tirkkonen, O. (2011). Resource sharing optimization for device-to-device communication underlying cellular networks. *IEEE Transactions on Wireless Communications*, 10(8):2752–2763.
- [Yu et al., 2008a] Yu, P., Baras, J., and Sadler, B. (2008a). Multicarrier authentication at the physical layer. In *International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008.*, pages 1–6.
- [Yu et al., 2008b] Yu, P., Baras, J., and Sadler, B. (2008b). Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1):38–51.