ENERGY-EFFICIENT AND SECURE DEVICE-TO-DEVICE COMMUNICATIONS IN THE NEXT-GENERATION WIRELESS NETWORK

Thesis

Submitted to

The School of Engineering of the

UNIVERSITY OF DAYTON

In Partial Fulfillment of the Requirements for

The Degree of

Master of Science in Electrical Engineering

By

Daidong Ying

Dayton, Ohio

August, 2018

ENERGY-EFFICIENT AND SECURE DEVICE-TO-DEVICE COMMUNICATIONS IN THE NEXT-GENERATION WIRELESS NETWORK

Name: Ying, Daidong

APPROVED BY:

Feng Ye, Ph.D.
Advisor Committee Chairman
Assistant Professor, Department of
Electrical and Computer Engineering

Guru Subramanyam, Ph.D.
Committee Member
Professor, Department of Electrical
and Computer Engineering

Eric Balster, Ph.D.
Committee Member
Associate Professor, Department of
Electrical and Computer Engineering

Robert J. Wilkens, Ph.D., P.E.
Associate Dean for Research and Innovation
Professor
School of Engineering

Eddy M. Rojas, Ph.D., M.A., P.E.
Dean, School of Engineering

ABSTRACT

ENERGY-EFFICIENT AND SECURE DEVICE-TO-DEVICE COMMUNICATIONS IN THE NEXT-GENERATION WIRELESS NETWORK

Name: Ying, Daidong
University of Dayton

Advisor: Dr. Feng Ye

Device-to-device (D2D) communication is a promising technology to improve energy efficiency and spectrum efficiency of the next-generation mobile networks. In this thesis, we first propose a D2D data off-loading scheme using game theoretical approach to reduce energy consumption for a wireless mobile network service provider. In the meantime, our proposed scheme provides a fair incentive mechanism to motivate D2D relay users for participation. The D2D scenario studied in this work focuses on downlink communications from the service provider to some users who request the same service, e.g., live streaming of a sports game. As an incentive, the service provider rewards some data usage to D2D relay users. In particular, we formulate a Stackelberg game to find the optimal portion of off-loading data for the relay users and the optimal incentive mechanism settings for the base station. With the proposed D2D off-loading scheme, a base station can maximize the energy saving while providing the most attraction to D2D relay users.Moreover, we propose a security scheme on the physical layer. The simulation results demonstrate that our proposed scheme will enhance the network energy efficiency and be attractive to D2D relay users. In particular, this scheme is to protect the data receivers in D2D communication

areas form the eavesdroppers. In the proposed scheme, we derive the optimal transmitting power for each D2D relay so that data receivers can be provided with the highest security capacity. For each D2D relay, we consider the data receiver at the edge of the D2D communication area as it has the lowest signal-to-noise-and-interference ratio (SINR) compared to other receivers in this D2D coverage. We propose a near-far problem to guarantee that all the data receivers on the edge of D2D communication areas have the same SINR. Thus, all the data receivers are equally protected. For the attackers, we consider the one with the highest receiving SINR. Simulation result demonstrate that all data receivers can have a high security throughput.

I dedicate this work to:

Zhaoan Ying

Xiulin Ying

Yamei Chen

who offered unconditional love and support to me.

ACKNOWLEDGMENTS

I would like to acknowledge and thank Dr. Feng Ye who brought me to the research world and supported me to finish this work. I could not publish my first paper without his guidance and help.

I would also like to thank my committee member, Dr. Subramanyam and Dr. Balster for their guidance and support.

I would like to express my gratitude to everyone who offered help to me in this work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION

Nowadays, people are more and more rely on the smart devices. With the rapid development of many Internet services like 4k video and game on mobile devices, people are eager to have a better mobile Internet service with high speed and lower latency. The data usage will increase rapidly in the near future and the current mobile network service(LTE) will no longer capable to handle such a huge data usage.

The next generation wireless mobile network will be upgraded to support the ever increasing mobile data usage in the near future [1, 2]. For example, mobile multimedia consumption such as music and video streaming, especially high-resolution and high-definition ones, would require better wireless network from service providers. In this thesis, we propose a device-to-device (D2D) off-loading scheme based on game theoretical approach to maximize the energy saving for a service provider, while providing the most attractive incentive to D2D relay users. On the other hand, the demand of security in 5G will be improved as well. In this thesis, we proposed a physical layer security scheme to protect the D2D users.

1.1 Improving Energy Efficiency with D2D Technology

D2D is a promising technology to enhance the next-generation wireless mobile networks [3, 4, 5, 6]. Due to limited transmitting power, D2D communications do not cause much interference to other cellular users. Spectrum reuse is also available in different D2D communication cells. Therefore, both energy efficiency and spectrum efficiency can be much

improved to support better service requirements. In the recent years, D2D off-loading schemes have been widely studied [7, 8, 9, 10]. For example, the authors of [7] proposed to use local cache and formulated a Stackelberg game to make the base station select the best source and let the relay node sell its power with the highest price. The authors of [8] studied the scenario where a user receives data from both the base station and a D2D relay. Some researchers also proposed to use more than two hops for D2D communications [9, 10]. In this work, we assume all downlink data is originated from the base station, e.g. public safety information or live streaming video that is not available from a local cache. Note that in the studied scenario, the D2D relay users are also part of the service requester thus the downlink transmission to those users are inevitable with or without having D2D relays.

While many research works have been conducted for D2D communications, most of them assume to offload all data to one D2D relay [3, 4]. In practice, a D2D relay user may not be able to offload arbitrary amount of data since the battery power of a relay user is limited. Moreover, even if a D2D user is capable of being a relay, he/she may not volunteer. To solve this issue, researchers have proposed incentive mechanisms to motivate D2D relay users. For example, the authors of [11] proposed to reward some resources from the service provider or the data requester. The authors of [11] proposed an incentive mechanism with linear relationship between data off-loading time and energy efficiency, given a determined transmit power. However, those mechanisms were not proven to have the most attraction to recruit D2D relay users.

In order to close the gap, we propose a D2D downlink off-loading scheme that saves the most amount of energy for a service provider and being attractive to D2D relay users based on game theoretical approach. In the proposed scheme, multiple D2D users may be selected as relay users where each offloads a given amount of data. Generally, all the users who are

interested in being relay user can join the data off-loading scheme. A two-level Stackelberg gamer is formulated, where the lower level includes D2D relay users, and the higher level includes the base station. Given a rewarding mechanism setting, D2D relay users find their optimal off-loading data portion. The base station, on the other hand, adjust the rewarding mechanism settings with the amounts of off-loading data reported by D2D relay users. We theoretically analyze the proposed scheme and prove that the Nash equilibrium and the Stackelberg equilibrium of the game can be found. Therefore, our scheme guarantees the most energy saving for the service provider when using D2D wireless communications in the studied scenario. At the same time, D2D relay users are motivated with the optimal setting of awards. The major contribution of this part of thesis is a new D2D downlink off-loading scheme that achieves mutual benefits to a service provider and D2D relay users.

1.2 Improving Security with D2D Technology

Physical layer security is to provide security services for the users in the cellular network. Physical layer security focuses on using interference between the data links. Usually, the interference is a negative component in the cellular network. However, the interference can be used in some positive way in the physical layer security area. In this work, we focus on using physical security to protect the data receivers form the attackers. We assume that there are some users who is curious about the data in the network. They are trying to leak massage from the all the D2D link in the mobile network, we call them eavesdroppers [12]. There are many exiting work about physical layer security [13, 14]. In [15], the authors proposed a physical layer scheme to provide the highest security throughput for the cellular users by determining the optimal threshold of the data link. In [16], the authors proposed a physical layer security scheme to maximize the success and secured data link in cellular

network. In this thesis, the cellular data links are protected by a corresponding D2D pair. There are some works try to provide security service to D2D users [17], the authors proposed a scheme to generate some noise in the data link spectrum. Then, the receivers are able to cancel the noise and the attackers will be greatly effected by the noise. However, all these works consider only one D2D relay in the network.

In order to close the gap, we propose a new physical layer security scheme for the D2D users. We assume that there are many D2D communication areas in the cellular network. All the D2D communication areas are using the same spectrum. And the D2D spectrum is orthogonal to the cellular spectrum. In this network, there are a group of eavesdroppers who distribute as Poisson point process (PPP). The eavesdroppers trying to leak the message from the data link that they are interested in. The relay users will cause interference to other D2D links. However, these interference will effect the eavesdroppers as well. We assume that the data links are exposed to the eavesdroppers. All the D2D relay will adjust their transmitting power to find the optimal SINR for the receiver at the edge of the D2D communication area to provide the highest secured capacity. So all the D2D communication link will be protected by the interference generated by other relay users. At the same time, we also consider the fairness of D2D users. We assume that the SINR of all the data receiver in at the D2D communication area edge have the same SINR so that all these user will have the same data rate. The eavesdroppers are passively listening to the channels and never send data.

1.3 Summary of Major Contributions

In summary, the major contribution in this thesis work include 1) we proposed our own network with some users who have D2D communication capability. Then we proposed a

data offloading scheme to improve the energy efficiency of the base station by using D2D communication technology. 2) We proposed the scheme that using multiple relay users. 3) We proposed a physical-layer security scheme. In this scheme every relay users will protect all other D2D communication area.

CHAPTER II

ILLUSTRATION OF THE STUDIED NETWORK

In this chapter, background of the next-generation mobile network (also known as the 5G network). The studied network model is also illustrated in this chapter.

2.1 Introduction of 5G

Compared to the LTE, 5G not only provides higher speed Internet service, but also support to applications such as Internet of things (IoT), device-to-device communication (D2D), Internet of Vehicles (IoV), etc. There are seven major requirements for 5G [18, 19, 20]:

- *Higher data rate:* 5G are required to achieve almost 10 times data rates from LTE whose peak data rate is 150 Mbps. (1 to 10 Gbps data rates in real networks)
- *Lower latency:* 5G will have only 1 ms round trip latency which is 10 times reduction from LTE.
- *High bandwidth in unit area:* The higher bandwidth in unit area not only improves the data rate of transmission in a certain area, but enable more devices.
- *Enormous number of connected device:* With the development of IoT and IoV, there will be enormous wireless mobile users in the near future. 5G should able to enable all the users who are authorized to use cellular network and ensurer the availability.

- *Wider coverage:* 5G will cover more area than LTE. Wherever the user go, they could get 5G service at anytime.
- *Higher availability:* Authorized 5G users should be allowed to get Internet access.
- *Higher energy efficiency:* The energy saving of the service provider should be improved to 90%. The energy efficiency of users should be improved as well so that the battery life of user device will be much longer in 5G.

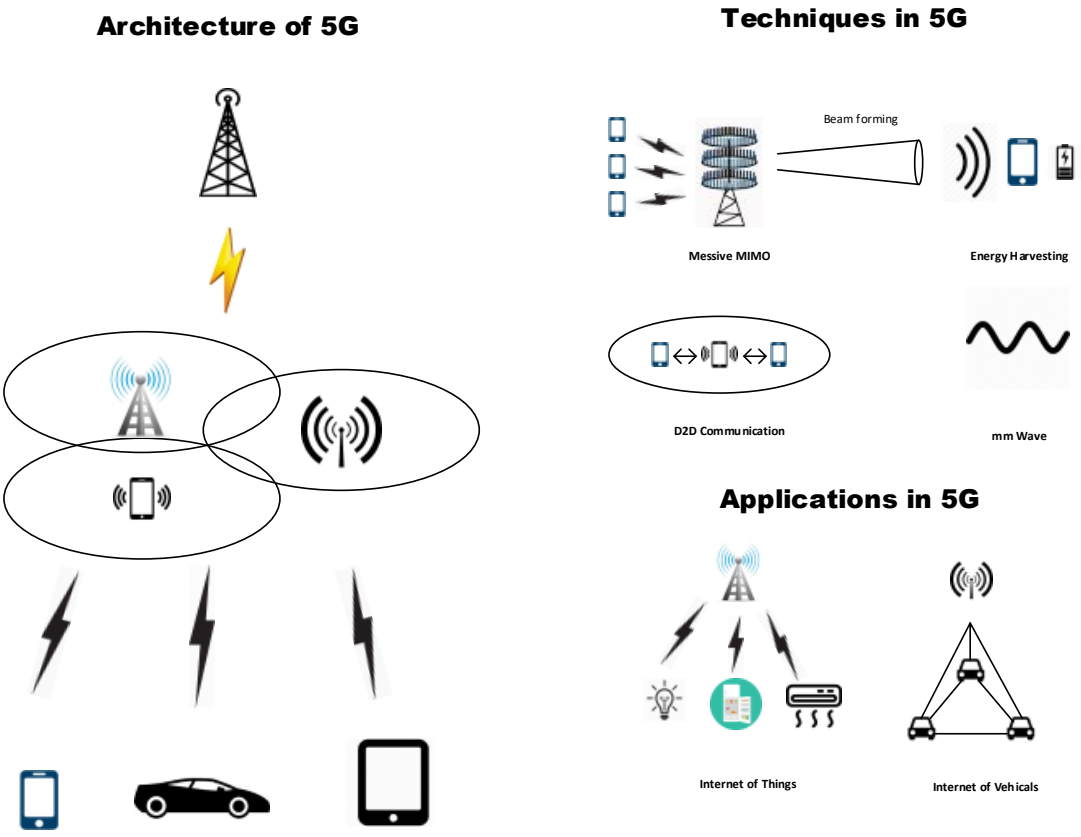

Figure 2.1: Illustration of the next-generation network

Compared with LTE, the technique, application and architecture are changed.

2.1.1 5G Network Structure

In 5G, the structure are changed from LTE. In the current cellular network, users are communicating with the base station directly in a big cell. The whole cell is covered by the base station [21]. However, in 5G, there will be small cells in a network. The biggest cell is called macro cell which is similar to the big cell in LTE. There will be many micro cells which are covered by small base stations. Each small base station can communicate with the big base station through fast link e.g., backhaul network, mm-wave. Each small base station will cover a small cell in the network. Users only need to communicate with the small base station when they want to transmit data. The advantage of the small cell is that small cells can reuse the same spectrum when they are communicating and cause interference to other devices in another cell. However, the distance between the users and small base station are much shorter than the distance between the big base station and the user devices, so the transmitting power will be much lower in the micro cell. The micro cells are not only created by the small stations, user devices are also allowed to act as transmitting relays so that this device will cover a small area as well e.g., device-to-device(D2D) communication areas, smart home networks. Therefor, the 5G network will be a cellular netwrok with dense small cells.

All the devices and base stations are supposed to have data registers so that some popular data will be cached locally. When some devices are requesting the same data, the D2D relay or the small base station will transmit the requested date to the users so that the usage of the backhaul network can be reduced.

2.1.2 New Techniques in 5G

Many new techniques will be used in 5G. D2D is a promising technology to improve the energy efficiency and spectrum efficiency. D2D communication allows users communicate with each other directly in the licensed spectrum. So the D2D relays will create a micro cell for the users in a certain area. The relay will transmit data for these users. If there are two users in this area request same content form the base station, the base station will send the data to the relay first, then the relay will send the content to those two data requesters. In this situation, the base station only has to transmit once, the energy efficiency will be improved. If the requested data in the data catch of relay, it will be transfered to the data requester from the relay. To motivate a user to be the relay, the service provider should reward him/her.

Because the density of the devices is very high, there might be enormous data flows in the network. To handle this huge amount of data flow, the massive multiple-input multiple-output(MIMO) system will be introduced in 5G [22]. In a massive MIMO, there are many individual antennas. Each antenna can transmitting signal in a certain frequency. So the devices with massive MIMO are able to receive data from or send data to different devices simultaneously. Another application of massive MIMO is beamforming. Beamforming is a technology that forms a strong signal beam in a certain direction. This technology will be used in many applications e.g. wireless charging, data transmitting, etc.

As we mentioned before, 5G will remarkably improve the energy efficiency. To achieve this goal, green communication is always considered [23]. In green communication, energy efficiency and new energy source are considered e.g., D2D, energy harvesting and so on.

To achieve higher data rates, researchers are trying to utilize mm-wave to transmitting data [24]. Mm-wave is the microwave that between 3 to 300 GHz. Currently, almost all wireless communications are using the spectrum between 300MHz to 3 GHz. Compared with mm-wave, the bandwidth used presently is really narrow. However, not all the spectrum in mm-wave could be used. The 57-64 GHz band is the Oxygen Absorption Band, and the bandwidth between 164-200 GHz is the Water Vapor Absorption Band. Because the micro wave in these two bands are easily decay, it is not practical to utilize these two bands to transmit data. The available band width left is 252 GHz which has huge potential to improve the transmitting capacity.

The high density users might cause security problems e.g. eavesdrop. The data flows are easily leaked to malicious devices. To encounter this, we propose to apply physical layer security schemes. When two devices are communicating in a small cell, there will be another data sender who transmits data in the same frequency e.g., a D2D relay. Because the eavesdropper has to listen to the same frequency, the D2D relay will cause interference to the eavesdropper so that the SINR of the malicious device will be remarkably decreased.

2.1.3 New Application in 5G

In 5G, many new applications will be supported e.g. Internet of Things (IoT), Internet of Vehicles (IoV) and Machine to Machine (M2M) communication. IoT technology enables Internet constructions and data inter-operability for numerous smart objects [18]. It not only allows the users control some electronic devices by using a central controller e.g., cell-phones and tablets, the electronic devices are able to automatically obtain some information and adjust its state. These procedure rely on huge data flow between the devices and Internet. IoV is a network formed by the vehicles. It focus on the robust traffic management

and reducing collision probabilities. The cars are supposed to form a temporary network called Vehicular ad hoc network(VANET). In the meantime, the security in these two areas are also considered. Because Zigbee are considered to be utilized in IoT and IoV. But the security scheme of Zigbee is too weak [25].

2.2 The Studied Network Model

As shown in Fig. 2.2, our studied network model comprises a macro base station (e.g., an eNodeB in LTE-A) and several end users with D2D capability. Without loss of generality, our focus in this work is to find the trade-off between the energy efficiency of the network service provider and incentive settings to some D2D users that are in the same small cell. For simplicity, the studied network model excludes the components that are not sensitive to incentives, e.g., small cell base station, non-3GPP users, etc.

In particular, we study the scenario where several users in a close range have the same data request, e.g., streaming the same game broadcast in a sport bar. D2D relays could reduce energy consumption of a service provider by off-loading some data stream from the macro base station using D2D communications. In order to promote D2D communications and motivate users to be relays, we propose to apply an incentive mechanism by rewarding some data usage to the relays. We assume the total number of end users who request the same service is N. The relay users are denoted as: $\mathbf{RU} = \{RU_1, RU_2, ...RU_i, ...RU_n\}$. We assume the battery power of a single relay user device is not enough to offload all the data from the base station. There are multiple D2D relays in this area and act sequentially. Without loss of generality, we assume all the users who are willing to be a relay will be assigned some off-loading data. The amount of the off-loading data assigned to a relay user, e.g., RU_i, is computed from the proposed scheme. The base station provides service to

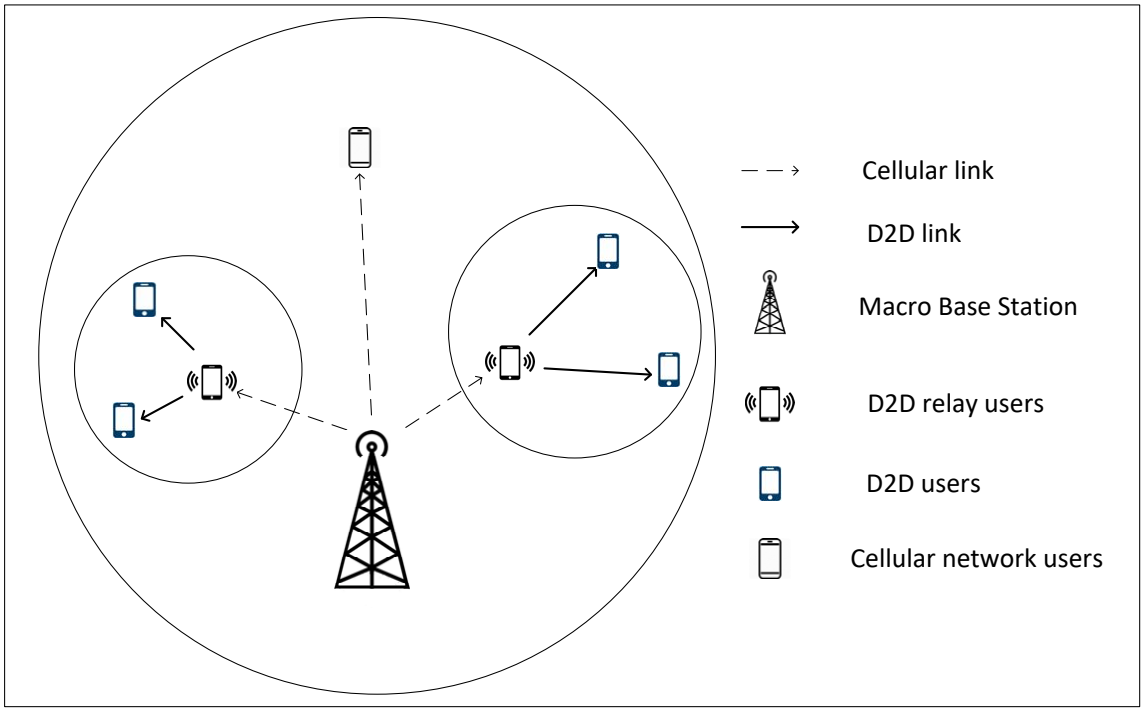

Figure 2.2: Studied network model with D2D communications.

the relay users with traditional cellular communications. The D2D relays and the service provider will configure an incentive mechanism setting according to the proposed scheme. The offloaded data will be multi-cast to other D2D users from the relay. Secure multi-cast protocols to be used in this D2D scenario are beyond the scope of this work. The base station will cover the rest of the service to all the users with LTE. Assuming that the D2D communications use orthogonal channels to the macro cell communications, the overall spectrum efficiency and energy efficiency will be enhanced due to less interference to regular users.

2.3 Summary

In this chapter, we introduced some background of 5G including the structure, new technologies and the applications. Then we present the studied network model. We defined the users and the base station in the model.

CHAPTER III

ENERGY-EFFICIENT AND INCENTIVE D2D OFF-LOADING SCHEME

In this chapter, we propose an incentive D2D off-loading scheme. The proposed scheme aims to improve energy efficiency for the base station. In the meantime, we also propose an incentive mechanism to motivate the regular users to be the relay users. Base station will offload some data flow to the relay users to reduce energy consumption.

3.1 Preliminaries of the Proposed Scheme

Assuming that the total energy consumption for the base station is $\mathbf{E} = \sum_{j=1}^{N} E_j$, where E_j is the energy consumed for user j. We assume the cost of per unit energy for the base station is C_B. In D2D downlink transmission, the base station could save some energy saving by off-loading some downlink traffic to a relay node, e.g., user RU_i. The saved energy is denoted as $\bar{e_i}$. As an incentive mechanism to recruit D2D relays, we propose to reward a relay user some data from the service provider. The rewarding data for relay node RU_i is estimated to consume some energy (denoted as e_i^r) from the base station in the future. In practice, the awarded data may be transmitted from other D2D relay nodes, thus to further reduce energy consumption of the base station. Therefore e_i^r is defined as the maximum energy consumption for rewarding the relay user RU_i from the service provider.

The energy consumption from the service provider is illustrated in Fig. 3.1. The net energy saving by off-loading data to RU_i is denoted as:

$$e_i^s = \bar{e_i} - e_i^r. \tag{3.1}$$

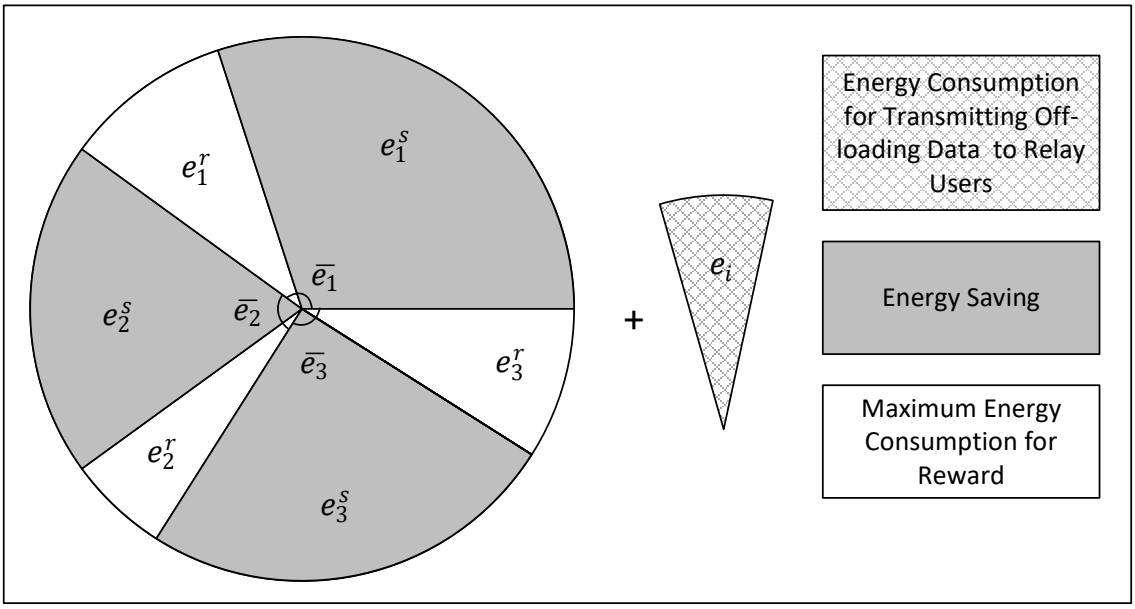

Figure 3.1: Energy consumption of the base station.

The example shows in Fig. 3.1 assumes 3 relay users. Note that the base station still provides full service to the relay users, denoted as the extra piece in the figure. The energy consumed for a user (e.g., user j) is estimated as:

$$E_j = P_B \frac{D_j}{r_j}, \tag{3.2}$$

where P_B is the transmit power form the base station, D_j is the amount of the service data required, and r_j is the achievable data rate. Data rate r_j depends on several factors, including interference, receiving gain and other factors of user j. For simplicity, we assume $r_1 = r_2 = ... = r_N$. The cost of the base station to transmit per unit of data is denoted as c_B. Denote $\bar{d}_i$ as the off-loading data to RU_i; d_i^r is the rewarded data to RU_i. The utility of the base station is defined as:

$$u_B = c_B \sum_{i=1}^{n} ((N-1)\bar{d}_i - d_i^r). \tag{3.3}$$

For better illustration, we denote $\eta_i = d_i^r/\bar{d}_i$ as the ratio of rewarding data to off-loading data; and $\rho_i = \bar{d}_i/D_j$ as the ratio of off-loading data to directly transmitted data. Base station will adjust ρ_i and η_i to maximize its utility. The utility of the base station is equivalent to:

$$u_B = c_B \sum_{i=1}^{n} (N - 1 - \eta_i)\bar{d}_i. \tag{3.4}$$

Given an η_i from the base station, RUs will decide the amount of off-loading data they want to relay by maximizing their utilities. We assume the price that the RU to buy a unit data from the base station is π. Then the revenue per off-loading data relayed by RU_i is denoted as:

$$p_i = \eta_i \pi - C_i \bar{d}_i, \tag{3.5}$$

where $C_i\bar{d}_i$ is the cost of RU_i to relay per unit off-loading data. The competition from other relay users is defined as $\bar{d}_{-i} = \sum_{i \neq j} \bar{d}_j$. The competition cost is defined as:

$$C_i^G = l_{-i}\bar{d}_{-i}, \tag{3.6}$$

where l_{-i} is defined as the competition cost coefficient. The utility of the relay user is denoted as:

$$u_i = (p_i - C_i^G)\bar{d}_i, \forall RU_i \in \mathbf{RU}, \tag{3.7}$$

The relay user RU_i maximize u_i by computing best $\bar{d}_i$.

3.2 The Stackelberg Game Based D2D Off-loading Scheme

The core of the proposed D2D off-loading scheme is a two-level Stackelberg game:

$$\mathcal{G} = (\mathcal{G}_{\mathcal{D}}, \mathcal{G}_{\mathcal{B}}). \tag{3.8}$$

The top layer game is formulated as:

$$\mathcal{G}_{\mathcal{B}} : (B, S_B, u_B), \tag{3.9}$$

where B is the base station, S_B is the strategy of the base station. The strategy of the base station is the setting for the incentive mechanism, denoted as:

$$\eta_i = a + b(1 - exp(-\mu\rho_i\beta))^\beta, \tag{3.10}$$

where β is a coefficient of this incentive scheme. a and b are two coefficients set by the service provider. In other words, the strategy of the base station is to adjust the value of β. μ is a constant value determined by the service provider. u_B is the utility of the base station we defined before. The base station is to maximize its utility by finding β^* as follows:

$$\beta^* = \underset{0<\beta<\infty}{\arg\max}\, u_B(\beta, S), \tag{3.11}$$

$$s.t. \quad 0 \leq \eta_i \leq 1, \tag{3.12}$$

$$0 \leq \rho_i \leq 1, \tag{3.13}$$

where S is the strategy set of the relay users.

The lower layer game is denoted as:

$$\mathcal{G}_\mathcal{D} : (\mathbf{RU}, S, u_i), \forall RU_i \in \mathbf{RU}, \tag{3.14}$$

where $S = \left\{\bar{d_1}, ..., \bar{d_n}\right\}$ is the strategy set of the relay users. Each strategy is to determine the amount of the off-loading data they want to relay. u_i is the utility of RU_i. Given strategy from all other players, the best response of RU_i is defined as:

$$\bar{d_i} = \underset{0<\bar{d_i}<\bar{d_i}^{max}}{\arg\max}\, u_i(\eta_i, \bar{d}_{-i}, \bar{d_i}). \tag{3.15}$$

where $\bar{d_i}^{max}$ is the maximum value of off-loading data that RU_i can relay. The value is estimated as follows. Denote the remianing battery power of RU_i as ϵ_i. We assume relay users only spend part of battery power on off-loading data. Denote λ as the willingness of a D2D user to be a relay. For example, if a user has used a large portion of the monthly

data subscription, he/she will be more willing to serve as a relay to get extra data. In this work, we assume λ is computed as:

$$\lambda = \delta m_d M / m_r, \tag{3.16}$$

where δ is a weight defined by the service provider; M is the monthly subscribed data plan of the relay user; m_r is the remaining data; and m_d is the remaining days in the billing cycle. The battery power that the relay user willing to spend on off-loading data is calculated as: $\epsilon_i^r = e^{-1/\lambda}\epsilon_i$. The maximum value of the off-loading data that RU_i can relay is calculated as:

$$\bar{d_i}^{max} = r_i^t \frac{\epsilon_i^r}{P_i}, \tag{3.17}$$

where r_i^t is the transmitting rate of RU_i, P_i is the transmitting power of the RU_i.

3.3 Solution of Stachelberg Game

3.3.1 Solution to the Lower Layer Game

The lower layer game is a non-cooperative game. The Nash equilibrium of $\mathcal{G}_\mathcal{D}$ is defined as $S^* = \{\bar{d_1}^*, ..., \bar{d_n}^*\}$, if it satisfies that, for any RU_i,

$$u_i(\bar{d_i}^*, \bar{d}^*_{-i}, \eta_i) \geq u_i(\bar{d_i}, \bar{d}^*_{-i}, \eta_i), \tag{3.18}$$

where $\bar{d}^*_{-i} = \sum_{i \neq j} \bar{d_j}^*$, η_i is given by the base station.

Lemma 1: The best response of RU_i uniquely exists, given η_i, $\bar{d}_{-i}$, $-1 < -l_{-i}/2C_i < 0, i \in \mathbf{RU}$ and $\eta_i \pi / 2C_i > 0$.

Proof. The best response can be calculated when the first order derivative of u_i w.r.t $\bar{d_i}$ equals 0, s.t.,

$$\frac{\partial u_i}{\partial \bar{d_i}} = -2C_i \bar{d_i} + \eta_i \pi - l_{-i} \bar{d}_{-i} = 0 \tag{3.19}$$

$$\bar{d_i}^* = \frac{\eta_i \pi - l_i \bar{d}_{-i}}{2C_i}. \tag{3.20}$$

Then the second order derivative of u_i w.r.t $\bar{d_i}$ can be calculated as

$$\frac{\partial^2 u_i}{\partial \bar{d_i}^2} = -2C_i \tag{3.21}$$

Because C_i is a positive value, the second order derivative of u_i is always less than 0, which means the utility of RU_i is a convex function.

Because $-1 < -l_{-i}/2C_i < 0$, the Nash equilibrium uniquely exists for $\mathcal{G}_\mathcal{D}$. If the value of $-l_{-i}/2C_i$ and $\eta_i \pi/2C_i$ are the same for two relay users, they will have the same strategy in the Nash equilibrium. Since the strategy space is convex and compact, and u_i is a continue and convex function, we draw the conclusion that the bottom layer game has a Nash equilibrium. Initial η_i is set according to the maximum $\bar{d}_i^{max}$ from all relay users. □

The algorithm to compute Nash equilibrium to $\mathcal{G}_\mathcal{D}$ is summarized in Alg. 1.

Algorithm 1 Compute Nash equilibrium to $\mathcal{G}_\mathcal{D}$

Require: S,$\{\eta_1, ...\eta_n\}$
Ensure: S^*

convergence threshold $= \varepsilon$
$a = 1$
while $|\bar{d_i}^{(a)} - \bar{d_i}^{(a-1)}| > \varepsilon$, $\forall RU_i \in$ **RU** **do**
    $a = a + 1$
    for $i = 1 : n$ **do**
        $\bar{d}_{-i}^{new} = \sum_{i \neq j} \bar{d}_j^{new}$
        $\bar{d_i}^* = \frac{\eta_i \pi - l_i \bar{d}_{-i}^{new}}{2C_i}$
        $\bar{d_i}^{new} = \bar{d_i}^*$
        $\bar{d_i}^{(a)} = \bar{d_i}^{new}$
    end for
end while

3.3.2 Approach to the Stackelberg Equilibrium

In the higher layer game, the base station computes the optimal β^* given S^* as follows:

$$\beta^* = \underset{0<\beta<\infty}{\arg} \frac{\partial u_B}{\partial \beta} = 0. \tag{3.22}$$

The strategy profile (S^*, β^*) is the Stackelberg Equilibrium of the Stackelberg game if:

$$u_B(\beta^*, S^*) \geq u_B(\beta, S^*), \tag{3.23}$$

$$u_i(\bar{d_i}^*, \bar{d}^*_{-i}, \eta_i) \geq u_i(\bar{d_i}, \bar{d}^*_{-i}, \eta_i), \forall RU_i \in \mathbf{RU}. \tag{3.24}$$

The approach to the Stakelberg equilibrium is summarized in Alg. 2.

Algorithm 2 Finding the Stackelberg equilibrium to $(\mathcal{G}_\mathcal{B}, \mathcal{G}_\mathcal{D})$

Require: $\{\bar{d_1}^{max} ... \bar{d_n}^{max}\}$, μ, π, c_B, $\{l_{-1}/2C_1, ..., l_{-n}/2C_n\}$
Ensure: S^*, β^*

```
a = 1
while β_p ≠ β^{*(a)} do
    a = a + 1
    calculate β^{*(a)} according to (3.22)
    β_p = β^{*(a−1)}
    calculate {η_1, ..., η_n}
    update S* according to Alg.1.
end while
```

3.4 Simulation and Numerical Result

In this section, we show the simulation results to justify the existence and uniqueness of the equilibrium of the proposed Stackelberg game and evaluate the energy efficiency of the proposed data off-loading scheme. For better illustration, the parameters are normalized: $\mu = 0.2$; $c_B = 1$; $C_1 = C_2 = ... = C_n = 0.1$; $\pi = 1$; $a = 0.2$; $b = 0.5$; $D_j = 1$. 3 relay users will be adopted in this simulation.

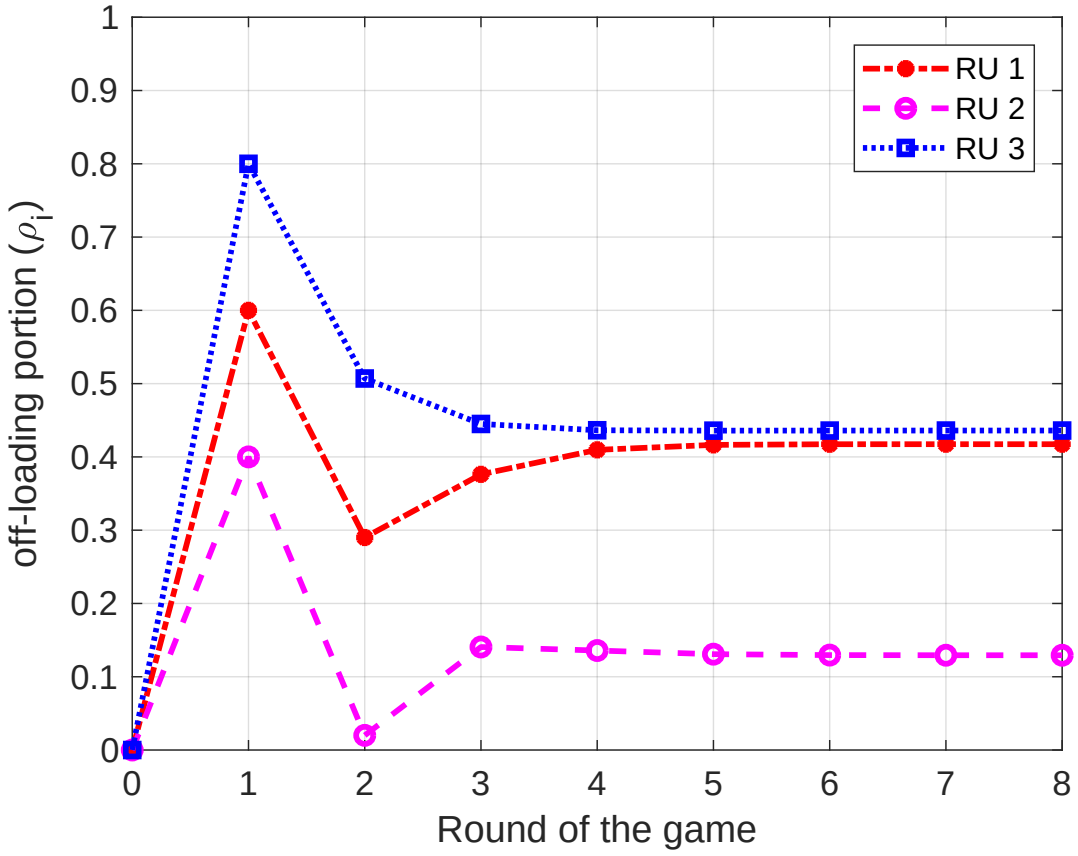

Figure 3.2: Convergence to the Nash equilibrium of $\mathcal{G}_{\mathcal{D}}$.

First, we evaluate the convergence of the Nash equilibrium of the lower layer game. As shown in Fig. 3.2, all users converge to the Nash equilibrium in a few rounds. The results are: $\rho_1 = 0.4173$, $\rho_2 = 0.1293$, $\rho_3 = 0.4360$, which indicate that 98.27% of the data will be offloaded to the relay nodes. Fig. 3.3 shows the utilities of the three D2D relay users. The maximum utilities are achieved at the equilibrium points respectively. In practice, the value of the utility depends on actual settings from users.

Then, we evaluate the incentive setting from the base station. As shown in Fig. 3.4. Based on different reward settings, the base station could always have the best reward

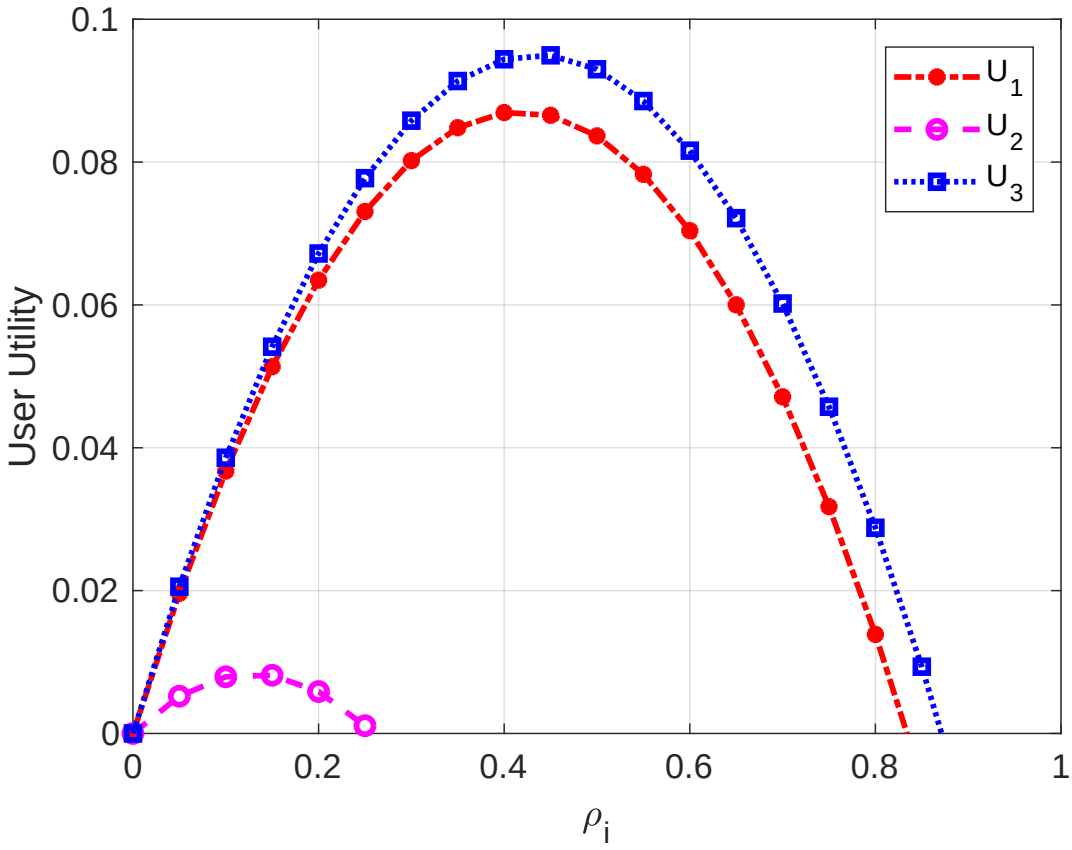

Figure 3.3: Illustration of u_i w.r.t ρ_i.

scheme to maximize the energy saving by finding β^*. The best response of the base station is denoted as the red circle on the curve.

Fig. 3.5 demonstrates the energy saving of the base station. Because the multi-cast technology is used in this scheme, the energy saving is upper bounded as $c_B(N-1)\bar{d}_i$ when $\bar{d}_i$ data is be offloaded to RU_i. In this simulation, we assume there are 3 users in the D2D network, and all of them participate in the data off-loading scheme. In the traditional cellular network, if the base station transmits to these 3 users separately, the energy cost will be 3. The solution achieved by the proposed scheme is denoted by the solid line, where

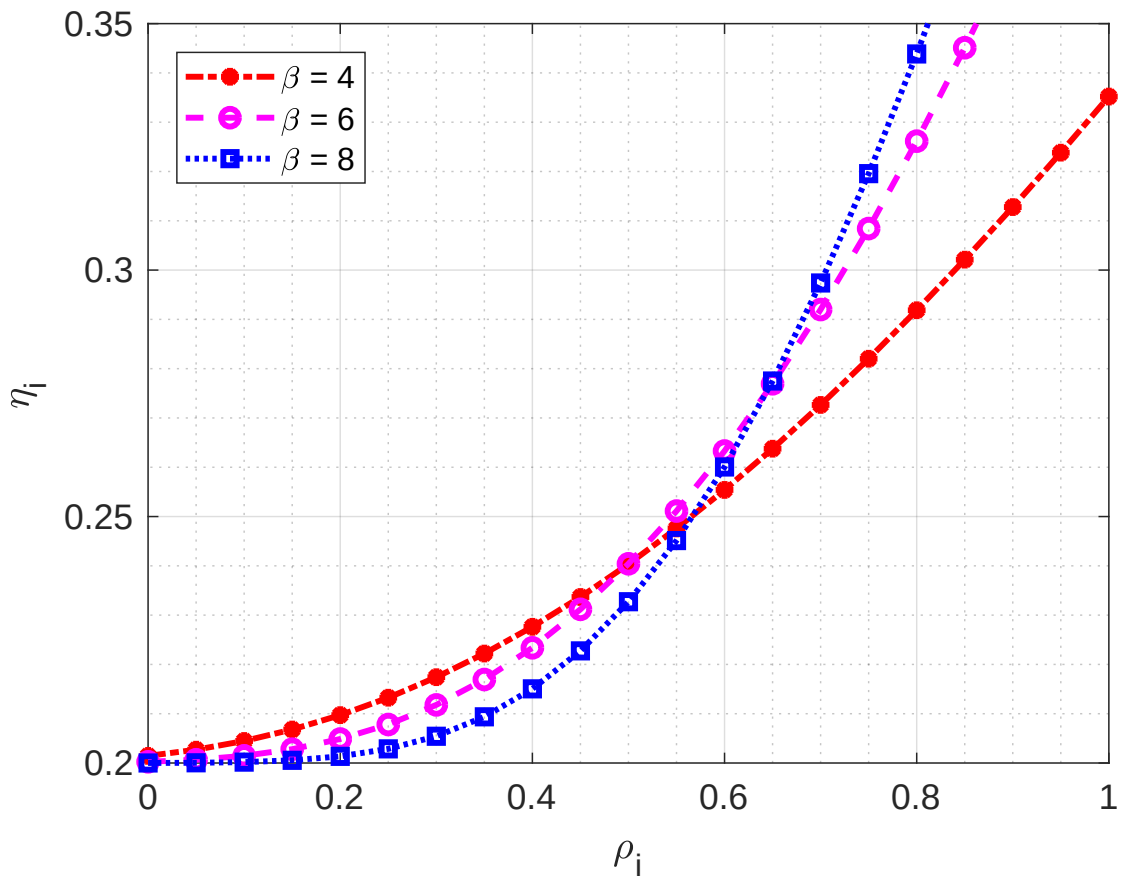

Figure 3.4: Illustration of the incentive scheme with different β.

the base station could have $1.78/3 = 59.3\%$ energy saving. Even in the situation that $\sum_{i=1}^{3} \bar{d}_i > D_j$, our proposed scheme could still provide 53% energy saving which is denoted as the second line.

3.5 Summary

In this chapter, we introduced our energy-efficiency D2D data offloading scheme. In this scheme, the regular users are motivated to be the relay users. The best strategies of Base station and the relay users is found by a Stackelberg. All the players in the game

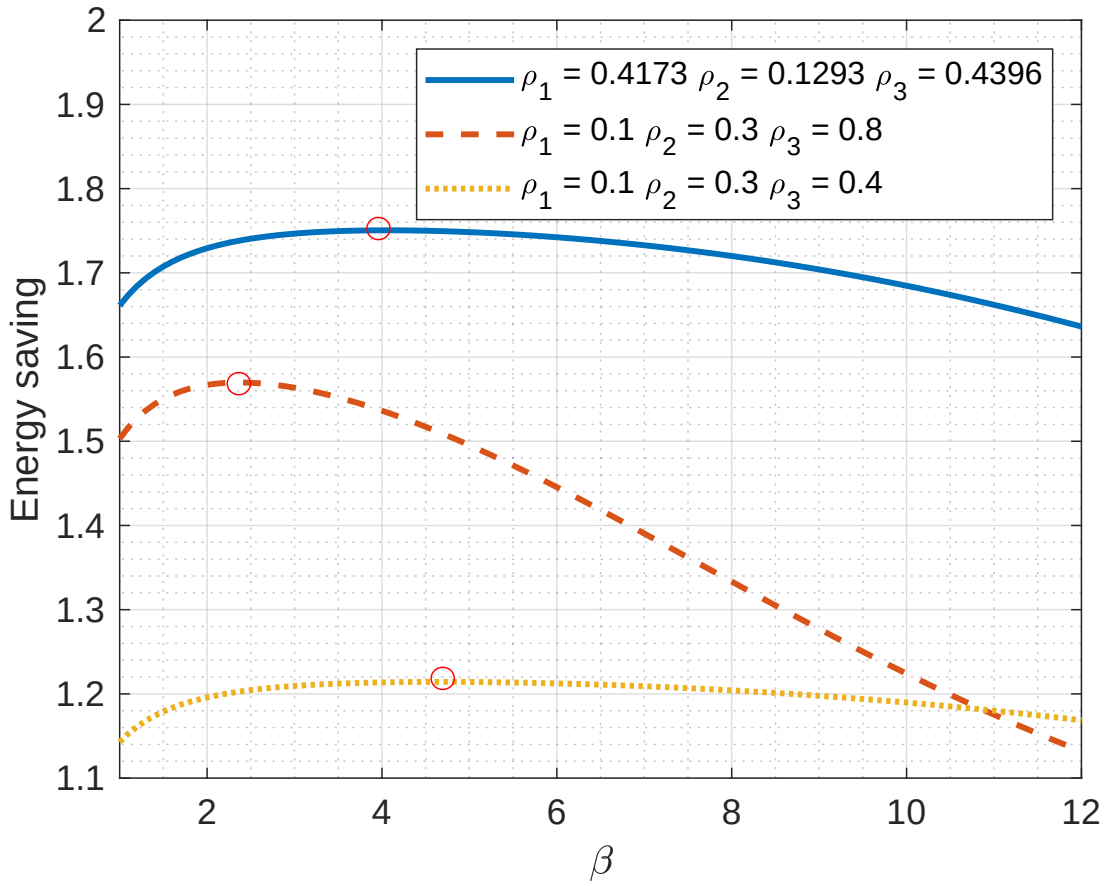

Figure 3.5: Illustration of the energy saving at β^*.

are guaranteed to get their highest utility. In this scheme, more than 50% of the energy consumption will be saved.

CHAPTER IV

PHYSICAL LAYER SECURITY

In this chapter, we will add the physical layer security into this network. We assume that the protocol layer security scheme is not adopted in this network. So we want to use the interference between the D2D communication area to protect each other.

4.1 Attack Model

In this section, we will introduce the attackers in the network. We assume that the eavesdroppers are distributed as a Poisson Point Process (PPP) Φ_e of intensity λ_e. And these eavesdroppers are curious about all the transmitted data in this network. But one attacker can only listen to one channel in a time slot. These eavesdropper are only passively listening to the data channel and never send massage. However, the locations of all the eavesdropper are known. We define the most dangerous attacker of a D2D relay user as the eavesdropper who is the closest to the transmitter. Though the closest attacker might not eavesdrop corresponding D2D relay user, this relay user still takes the best action based on this attacker. To achieve the fairness for all the data receivers in the D2D communication area, we makes all the data receivers on the edge of the D2D communication area have the same SINR. To achieve this goal, the relay users has to adjust their transmitting power. At the same time, the relay user will provide the highest security throughput to the data receivers. As shown in Fig .4.1, the D2D relay user cause interference to the data receiver and the eavesdropper at the same time. We assume that the D2D relays are distributed

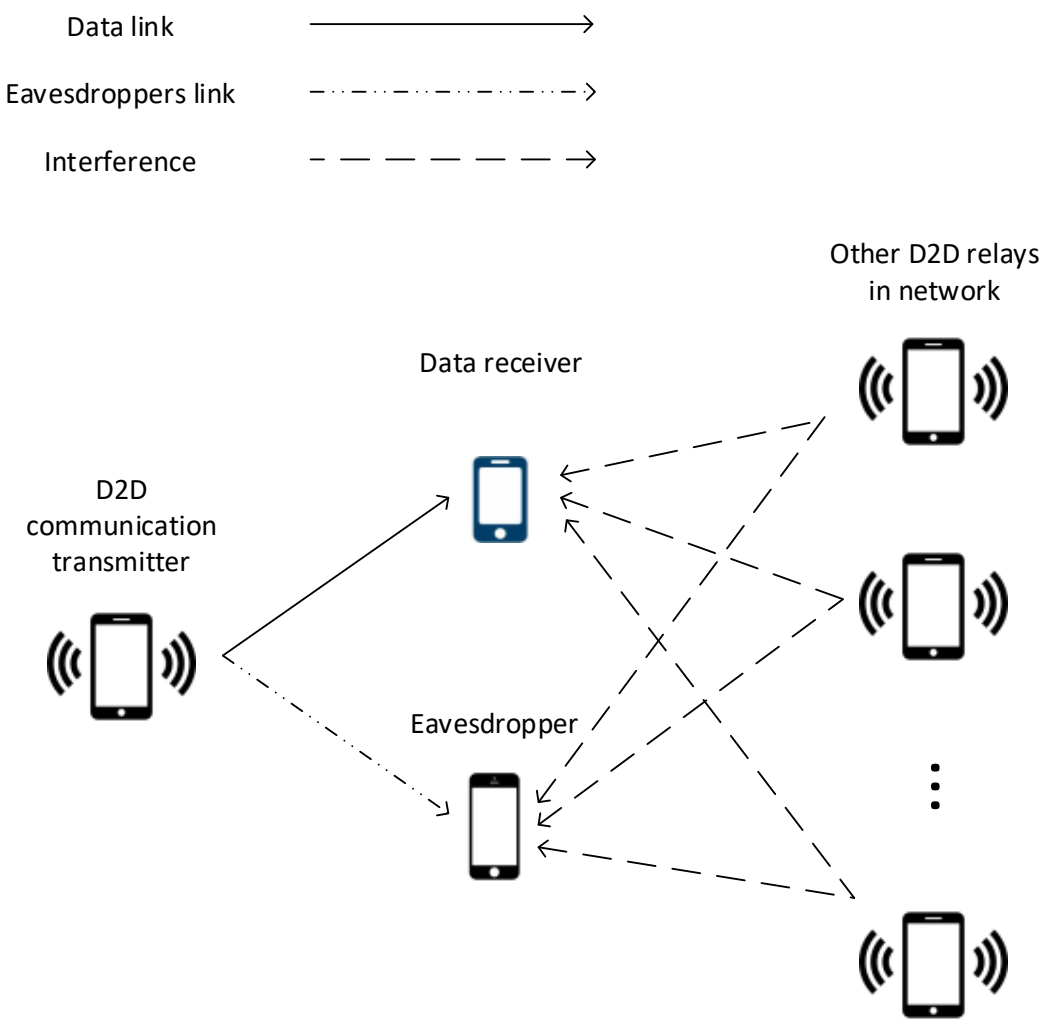

Figure 4.1: Studied attack model

as a homogeneous PPP which is denoted as Φ_d of intensity λ_d. We assume that the D2D link use different spectrum with the cellular link, so there is no interference from the base station for the D2D users. However, because the D2D cells are using the same spectrum, there will be interference between the D2D users. We assume the Rayleigh fading channel is used in the D2D cells. And the DR_i locate at the origin of the coordinate. The interference

of DR_i^j is denoted as:

$$I_i = \sum_{d \neq j, x_d \in \Phi_d} p_d h_d ||x_d||^{-\alpha}, \tag{4.1}$$

where p_d is the average transmitting power of D2D relays except R_j. h_d is the fading factor following an exponential distribution $h \sim \exp(1)$. x_d is the location of D2D relay. α is the path loss exponent. So the signal-to-noise-and-interference-ratio(SINR) of DR_i^j is denoted as:

$$\phi_i = \frac{p_j h_j ||x_j||^{-\alpha}}{\sigma + I_i} \tag{4.2}$$

where ϕ_i is the SINR of DR_i, σ is the Guassian noise. x_j is the location of D2D relay R_j. We assume that the signal to noise and interference ratio for all the data receivers is same because of fairness.

In this thesis, we assume that the transmitting link is exposed to the eavesdroppers. Therefor, Wyner's encoding is adopted in this work. We define the transmitting rate as R_t which satisfy that if the receiving rate of DR_i^j is higher than r_t, it is able to decode the message successfully:

$$\log_2(1 + \phi_i) \geq r_t. \tag{4.3}$$

Then we define the security rate r_s. If the receiving rate of the eavesdropper is lower than the redundancy rate $r_t - r_s$, it is unable to decode the message:

$$\log_2(1 + \phi_e) < r_t - r_s, \tag{4.4}$$

Where ϕ_e is denoted as:

$$\phi_e = \frac{p_j h_j ||x_j - x_e||^{-\alpha}}{\sigma + I_e}, \tag{4.5}$$

$$I_e = \sum_{x_d \neq x_j, x_d \in \Phi_d} p_d h_d ||x_d - x_e||^{-\alpha}, \tag{4.6}$$

where x_e is the location of the eavesdropper. If the DR_i^j is able to decode the message and the eavesdropper failed to leak the message, we define this link is a secured data link.

To achieve this goal, we should make the SINR of the data requester higher than a certain value and make the SINR of eavesdropper lower than a threshold. These two threshold are denoted as: T_u and T_e respectively. On the other hand, we define the probability that the SINR of data requester i is higher T_u as $\mathbb{P}(\phi_i \geq T_u)$. The probability that the SINR of eavesdropper is lower than T_e is defined as $\mathbb{P}(\phi_e < T_e)$. The probability of secure data link is denoted as: $\mathbb{P}(\phi_i \geq T_u)\mathbb{P}(\phi_e < T_e)$.

4.2 Analyze of Success Connection Probability

In this subsection we will discuss the connection probability of DR_i^j. For DR_i^j, it receives interference from other D2D relays. We define the probability of the success data link as: $\mathcal{P}_{data}$. To make the calculation easily, we locate the data receiver at the center of the coordinate.

$$\begin{aligned}
\mathcal{P}_{data} &= \mathbb{P}(\phi_i \geq T_u) \\
&= \mathbb{P}(\frac{p_j h_j ||x_j||^{-\alpha}}{\sigma + I_i} \geq T_u) \\
&= \mathbb{P}(h_i \geq \frac{T_u(\sigma + I_i)}{p_j ||x_j||^{-\alpha}}) \\
&= \mathbb{E}_{I_i}(\exp(-\frac{T_u(\sigma + I_i)}{p_j ||x_j||^{-\alpha}})) \\
&= \exp(-\frac{T_u \sigma ||x_j||^{\alpha}}{p_j}) \mathbb{E}_{I_i}(\exp(-\frac{T_u I_i ||x_j||^{\alpha}}{p_j}))
\end{aligned} \tag{4.7}$$

According to Eq.(4.1), the interference consists of all the interference from all the other D2D relay in this big cell. To simplify the equation, we use Laplace transform on the

interferences. The Laplace transform of the interference is defined as:

$$\begin{aligned}
\mathcal{L}_{I_i}(s) &= \mathbb{E}[\exp(-s \sum_{d\neq j, x_d\in\Phi_d} p_d h_d ||x_d||^{-\alpha})] \\
&= \mathbb{E}_{\Phi_d,h_d}[\prod_{d\neq j, x_d\in\Phi_d} \exp(-s p_d h_d ||x_d||^{-\alpha})] \\
&= \mathbb{E}_{\Phi_d}[\prod_{d\neq j, x_d\in\Phi_d} \mathbb{E}_{h_d}[\exp(-s p_d h_d ||x_d||^{-\alpha})]] \\
&\overset{(a)}{=} \exp(-\lambda_d \int_{\mathbb{R}^2} (1 - \mathbb{E}_{h_d}[\exp(-s p_{-j} h_d ||x_d||^{-\alpha})]) dx_d) \\
&\overset{(b)}{=} \exp(-\lambda_d \int_{\mathbb{R}^2} \frac{1}{1 + s^{-1} p_{-j}^{-1} ||x_d||^{\alpha}} dx_d) \\
&\overset{(c)}{=} \exp(-\lambda_d 2\pi \int_{l=0}^{\infty} \frac{l}{1 + s^{-1} p_{-j}^{-1} l^{\alpha}} dl) \\
&\overset{(d)}{=} \exp(-\lambda_d \pi (s p_{-j})^{\delta} \Gamma(1-\delta)\Gamma(1+\delta)) \\
&\overset{(e)}{=} \exp(-\frac{\pi \lambda_d p_{-j}^{\delta} s^{\delta}}{\mathrm{sinc}(\delta)})
\end{aligned} \tag{4.8}$$

In the calculation of (a), the probability generation function of PPP is used: $\mathbb{E}[\prod_{x\in\Phi} f(x)] = \exp(-\lambda \int_{\mathbb{R}_2} (1 - f(x)) dx)$. And p_{-j} is denoted as:

$$p_{-j} = \frac{\sum_{d\neq j, x_d\in\Phi_d} p_d ||x_d||^{-\alpha}}{\sum_{d\neq j, x_d\in\Phi_d} ||x_d||^{-\alpha}} \tag{4.9}$$

where $||x_d||$ is the distance from DR_i to the D2D relay RU_d. The calculation of (b) is:

$$\begin{aligned}
1 - \mathbb{E}_{h_d}[\exp(-s p_{-j} h_d ||x_d||^{-\alpha})] &= 1 - \int_{h_d=0}^{\infty} e^{-s p_{-j} h_d ||x_d||^{-\alpha}} e^{-h_d} dh_d \\
&= 1 - \int_{h_d=0}^{\infty} e^{-(\epsilon+1) h_d} dh_d \\
&= 1 - \frac{1}{-\epsilon - 1}(-1) \\
&= \frac{1}{1 + \epsilon^{-1}}
\end{aligned} \tag{4.10}$$

where we replace $s p_{-j} ||x_d||^{-\alpha}$ by ϵ. In (c), the equation transfer form orthogonal coordination to polar coordination. In (d), the gamma function is used:$\Gamma(\alpha) = \int_0^{\infty} l^{\alpha-1} e^{-l} dl$ [16]. And $\delta = \frac{2}{\alpha}$ In (e), the properties of Gamma function are used:$\Gamma(\delta)\Gamma(1-\delta) = \frac{\pi}{\sin(\pi\delta)}$, $\Gamma(1+\delta) = \delta\Gamma(\delta)$

$$\begin{aligned}
\exp(-\lambda_d \pi (s p_{-j})^{\delta} \Gamma(1-\delta)\Gamma(1+\delta)) &= \exp(-\lambda_d \pi (s p_{-j})^{\delta} \Gamma(1-\delta)\Gamma(\delta)\delta) \\
&= \exp(-\lambda_d \pi (s p_{-j})^{\delta} \frac{\pi}{\sin(\pi\delta)} \delta)
\end{aligned} \tag{4.11}$$

Then we put (4.8) into (4.7), we will have:

$$\begin{aligned}\mathbb{P}_{data} &= \exp(-\frac{T_u\sigma||x_j||^\alpha}{p_j})\mathcal{L}_{I_i}(\frac{T_u||x_j||^\alpha}{p_j}) \\ &= \exp(-\frac{T_u\sigma||x_j||^\alpha}{p_j} - \frac{\pi\lambda_d p_{-j}^\delta T_u^\delta||x_j||^2}{\text{sinc}(\delta)p_j^\delta})\end{aligned} \tag{4.12}$$

In this equation, we can find that when we increase the transmitting power of RU_j, the success rate will increase. When we increase the intensity of the D2D communication area λ_d and the transmitting power of other relay RU_d, the success rate of transmitting link between RU_j and DR_i will decrease.

Because the distribution of the DR_i follows PPP, so the upper bounds of the probability of successful data link could be denoted as [16]:

$$\begin{aligned}\mathcal{P}_{data} &= \mathbb{E}[\sum_{x_j\in\Phi_d}\mathbb{P}_{data}] \\ &\overset{(f)}{=} \lambda_d\int_{\mathbb{R}^2}\mathbb{P}_{data}dx_j \\ &= \lambda_d 2\pi\int_{l=0}^{\infty}\exp(-\frac{T_u\sigma l^\alpha}{p_j} - \frac{\pi\lambda_d p_{-j}^\delta T_u^\delta l^2}{\text{sinc}(\delta)p_j^\delta})ldl \\ &= \lambda_d\pi\int_{l=0}^{\infty}\exp(-\frac{T_u\sigma l^\alpha}{p_j} - \frac{\pi\lambda_d p_{-j}^\delta T_u^\delta l^2}{\text{sinc}(\delta)p_j^\delta})dl^2 \\ &= \lambda_d\pi\exp(-al^\alpha - \frac{b\pi p_{-j}^\delta l^2}{p_j^\delta})(\frac{1}{-al^{\alpha-2}\frac{\alpha}{2} - \frac{b\pi p_{-j}^\delta}{p_j^\delta}})|_0^\infty \\ &= \frac{\text{sinc}\delta}{[1+\frac{p_{-j}^\delta}{p_j^\delta}]T_u^\delta}\end{aligned} \tag{4.13}$$

where $a = \frac{T_u\sigma}{p_j}$ and $b = \frac{T_u^\delta}{\text{sinc}(\delta)}$. In (f), the Campbell-Mecke Theorem is used: $\mathbb{E}[\sum_{x\in\Phi}f(x)] = \lambda\int_{\mathbb{R}_d}f(x)dx$. Because the value of sincδ is always smaller than 1. So when T_u is lager than 1, this equation is always right.

4.3 Analysis of Security Probability

In this subsection, we will analyze the security probability of the data link between RU_j and DR_i. In other words, if the SINR of the eavesdroppers are lower than T_e, we say the

data link is secured. The probability is denoted as:

$$\begin{aligned}
\mathcal{P}_{sec} &= \mathbb{E}_{\Phi_e}[\prod \mathbb{P}(\phi_e \leq T_e)] \\
&= \mathbb{E}_{\Phi_e}[\prod_{x_e \in \Phi_e} \mathbb{P}(\frac{p_j h_j ||x_j - x_e||^{-\alpha}}{\sigma + I_e} \leq T_e)] \\
&= \mathbb{E}_{\Phi_e}[\prod_{x_e \in \Phi_e} \mathbb{P}(h_i \leq \frac{T_e(\sigma + I_e)}{p_j ||x_j - x_e||^{-\alpha}})] \\
&= \mathbb{E}_{\Phi_e}[\prod_{x_e \in \Phi_e} (1 - \exp(-\frac{T_e(\sigma + I_e)}{p_j ||x_j - x_e||^{-\alpha}}))] \\
&= \mathbb{E}_{\Phi_e}[\prod_{x_e \in \Phi_e} (1 - \exp(-T_e\sigma ||x_j - x_e||^{\alpha} p_j^{-1}) \exp(-T_e I_i ||x_j - x_e||^{\alpha} p_j^{-1}))] \\
&= \mathbb{E}_{\Phi_e}[\prod_{x_e \in \Phi_e} (1 - \exp(-T_e\sigma ||x_j - x_e||^{\alpha} p_j^{-1}) \mathcal{L}_{I_e}(T_e p_j^{-1} ||x_j - x_e||^{\alpha}) \\
&= \exp(-\lambda_e \int_{\mathbb{R}^2} (\exp(-T_e\sigma ||x_j - x_e||^{\alpha} p_j^{-1}) \mathcal{L}_{I_e}(T_e p_j^{-1} ||x_j - x_e||^{\alpha})) dx_e) \\
&= \exp(-\lambda_e \int_{\mathbb{R}^2} (\exp(-T_e\sigma ||x_j - x_e||^{\alpha} p_j^{-1} - \frac{\pi \lambda_d \bar{p}_{de}^{\delta} T_e^{\delta} ||x_j - x_e||^2}{\mathrm{sinc}(\delta) p_j^{\delta}})) dx_e)
\end{aligned} \tag{4.14}$$

To simplify the equation, we move the eavesdropper to the origin of the coordinate, then change the equation to the polar coordinate.

$$\mathcal{P}_{sec} = \exp(-\lambda_e 2\pi \int_{l_e=0}^{\infty} \exp(-\frac{T_e\sigma l_e^{\alpha}}{p_j} - \frac{\pi \lambda_d \bar{p}_{de}^{\delta} T_e^{\delta} l_e^2}{\mathrm{sinc}(\delta) p_j^{\delta}}) l_e dl_e), \tag{4.15}$$

where l equals $||x_j - x_e||$. Then we transfer the security probability to:

$$\begin{aligned}
\mathcal{P}_{sec} &= \exp(-\lambda_e 2\pi \int_{l_e=0}^{\infty} \exp(-a' l_e^{\alpha} - \frac{b' \pi \bar{p}_{de}^{\delta} l_e^2}{p_j^{\delta}}) l_e dl_e) \\
&= \exp(-\lambda_e \pi \int_{0}^{\infty} \exp(-a' l_e^{\alpha} - \frac{b' \pi \bar{p}_{de}^{\delta} l_e^2}{p_j^{\delta}}) dl_e^2) \\
&= \exp(-\lambda_e \pi \exp(-a' l_e^{\alpha} - \frac{b' \pi \bar{p}_{de}^{\delta} l_e^2}{p_j^{\delta}}) (\frac{1}{-a' l_e^{\alpha - 2} \frac{\alpha}{2} - \frac{b' \pi \bar{p}_{de}^{\delta}}{p_j^{\delta}}}) |_0^{\infty} \\
&= \exp(-\frac{\lambda_e p_j^{\delta}}{b' \bar{p}_{de}^{\delta}})
\end{aligned} \tag{4.16}$$

where $a' = \frac{T_e \sigma}{p_j}$, $b' = \frac{T_e^{\delta} \lambda_d}{\mathrm{sinc}(\delta)}$, and $\bar{p}_{de} = \frac{\sum_{d \neq j, x_d \in \Phi_d} p_d ||x_d - x_e||^{-\alpha}}{\sum_{d \neq j, x_d \in \Phi_d} ||x_d - x_e||^{-\alpha}}$. Where x_e is the location of the eavesdroppers.

4.4 Problem Formulation

In this subsection, we will discuss the throughput of the D2D data link. The throughput of a certain link is denoted as:

$$TP = r_t \mathcal{P}_{data} \mathcal{P}_{sec}. \tag{4.17}$$

where r_t is the transmitting rate. r_t is denoted as:

$$r_t = W \log_2(1 + \phi_i), \tag{4.18}$$

where W is the bandwidth of the channel. (4.17) could be transfered to be a optimize question which is denoted as:

$$\mathbf{P}1 : \max : TP_i = r_t \exp(-\frac{\pi \lambda_d p_{-j}^{\delta} T_u^{\delta} ||x_j||^2}{\mathrm{sinc}(\delta) p_j^{\delta}}) \exp(-\frac{\lambda_e \mathrm{sinc}(\delta) p_j^{\delta}}{\lambda_d T_e^{\delta} \bar{p}_{de}^{\delta}}) \tag{4.19}$$

As we mentioned before, all the data receivers in the edge of the D2D communication area have the same SINR. And these users have the lowest SINR in the D2D communication area. So in this work, we will provide the highest security throughout to these data receivers by adjusting transmitting power of the relay user. We assume that the noise is very small compared with the interference. The ϕ_i could be denoted as:

$$\begin{aligned} \phi_i &= \frac{p_j h_j ||x_j||^{-\alpha}}{\sum_{d \neq j, x_d \in \Phi_d} p_d h_d ||x_d||^{-\alpha}} \\ &= \frac{p_j h_j ||x_j||^{-\alpha}}{p_{-j} \sum_{d \neq j, x_d \in \Phi_d} h_d ||x_d||^{-\alpha}} \end{aligned} \tag{4.20}$$

Similarly, the ϕ_e could be denoted as:

$$\phi_e = \frac{p_j h_j ||x_j - x_e||^{-\alpha}}{\bar{p}_{de} \sum_{d \neq j, x_d \in \Phi_d} h_d ||x_d - x_e||^{-\alpha}} \tag{4.21}$$

We denote $\frac{h_j ||x_j||^{-\alpha}}{\sum_{d \neq j, x_d \in \Phi_d} h_d ||x_d||^{-\alpha}}$ as ξ_j. $\frac{h_j ||x_j - x_e||^{-\alpha}}{\sum_{d \neq j, x_d \in \Phi_d} h_d ||x_d - x_e||^{-\alpha}}$ is denoted as ξ_e. Based on the value of ϕ_i, the optimal p_j could be derived as:

$$p_j^* = p_{-j} \frac{\phi_i^*}{\xi_j}. \tag{4.22}$$

We assume that in this network, all the D2D relay users make $\phi_e = \omega\phi_i$ to make sure the SINR of the eavesdropper won't be high. According to (4.20), we can transform (4.19) into:

$$\mathbf{P}2 : \max : TP_i = r_t \exp(-\frac{\pi\lambda_d\xi_i^\delta T_u^\delta ||x_j||^2}{\mathrm{sinc}(\delta)\phi_i^\delta}) \exp(-\frac{\lambda_e \mathrm{sinc}(\delta)\phi_i^\delta \omega^\delta}{\lambda_d T_e^\delta \xi_e^\delta}) \tag{4.23}$$

To provide the highest through put for the data receivers, the optimal ϕ_i^* should be derived. The optimal ϕ_i^* is denoted as:

$$\phi_i^* \Rightarrow \arg\max TP_i \tag{4.24}$$

To calculate ϕ_i^*, we calculate the first derivative of the (4.24) as:

$$\phi_i^* \Rightarrow \arg\frac{\partial TP_i}{\partial \phi_i} = 0 \tag{4.25}$$

Then we want to verify that $\mathbf{P}2$ is a quasi convex function. (4.23) could be simplify to be $W\log_2(1+\phi_i)\exp(-\frac{c_1}{\phi_i^\delta})\exp(-c_2\phi_i^\delta)$, because the log function is a convex function, so we just need to justify that $\exp(\frac{c_1}{\phi_i^\delta})\exp(-c_2\phi_i^\delta)$ is a quasi convex function. Then we replace ϕ_i^δ as $x > 0$ since $\phi_i > 0$. And $c_1 > 0$, $c_2 > 0$.

$$\frac{\partial e^{-\frac{c_1}{x}} e^{-c_2 x}}{\partial x} = e^{-\frac{c_1}{x} - c_2 x}(\frac{c_1}{x^2} - c_2), \tag{4.26}$$

So there are only one solution for $\frac{c_1}{x^2} - c_2 = 0$, and $x = \sqrt{\frac{c_1}{c_2}}$. So $c_i\phi_i^\delta \exp(-c_2\phi_i^\delta)$ is convex as well. (4.23) is a convex function. Because $\mathbf{P}2$ is a convex function, to simplify the calculation, we transfer the (4.23) to the form :

$$\mathbf{P}3 : \max : \ln(TP_i) = \ln(r_t) - \frac{\pi\lambda_d\xi_i^\delta ||x_j||^2}{b\phi_i^\delta} - \frac{\lambda_e\phi_i^\delta\omega^\delta}{b'\xi_e^\delta} \tag{4.27}$$

The optimal result of $\mathbf{P}3$ is denoted as:

$$\phi_i^* \Rightarrow \arg\max \ln(TP_i) \tag{4.28}$$

We take the first derivative of **P3**:

$$\begin{aligned}\frac{\partial \ln(TP_i)}{\partial \phi_i} &= \frac{\partial \ln(W \log_2(1+\phi_i))}{\partial \phi_i} - \frac{\partial \pi \lambda_d \xi_i^\delta ||x_j||^2 / b\phi_i}{\partial \phi_i} - \frac{\partial(\lambda_e \phi_i^\delta \omega^\delta)/(b'\xi_e^\delta)}{\partial \phi_i} \\ &= \frac{1}{W^2 \log_2(1+\phi_i)(1+\phi_i)\ln(2)} + \frac{\pi \lambda_d \xi_i^\delta ||x_j||^2}{b\phi_i^2} - \frac{\delta \lambda_e \phi_i^{\delta-1} \omega^\delta}{b'\xi_e^\delta}\end{aligned} \tag{4.29}$$

To calculate the value of ϕ_i^*, we let $\frac{\partial \ln(TP_i)}{\partial \phi_i} = 0$. Then we have:

$$\phi_i^* \Rightarrow \arg \frac{\partial \ln(TP_i)}{\partial \phi_i} = 0 \tag{4.30}$$

According to the value of ϕ_i^*, we could calculate the value of p_j^* as:

$$p_j^* = p_{-j} \frac{\phi_i^*}{\xi_j} \forall RU_j \tag{4.31}$$

4.5 Simulation Results

In this section, we provide some simulation result to validate the proposed scheme. There are some normalized parameters:

Table 4.1: Parameter Settings

Simulation Parameters	
parameters	values
λ_u	6
λ_e	3
λ_d	6
T_u	0.25
T_e	0.5
α	3
ω	0.5
W	10MHz

In the simulation, we assume the location of the eavesdropper is known. We assume there are 6 D2D relay users and the eavesdroppers EU_1 is the eavesdropper that is most dangerous for the transmitter RU_j. Then we calculate the success data link probability and

the security probability for RU_j. In the Fig. 4.2, we can see that there is always a maximum

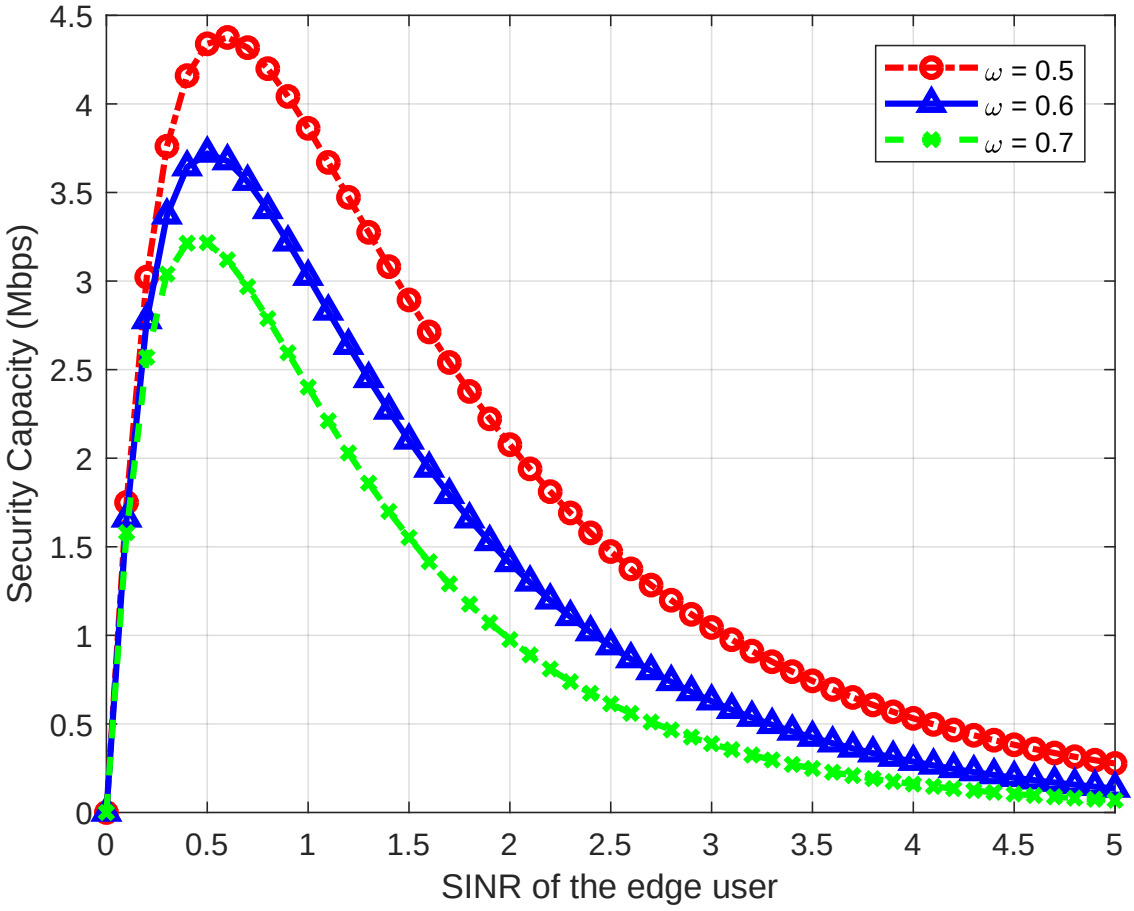

Figure 4.2: Security capacity of the edge user

value for the security capacity of the data receiver. When the value of ω gets higher, which means the SINR of eavesdropper to the SINR of data receiver ratio get higher. In this situation, when the SINR of the data receiver gets high, the security capacity will drop.

Fig. 4.3 is the probability of successful data link. In this can see that when the transmitting power of the transmitter growth, the probability improve as well. When we set a

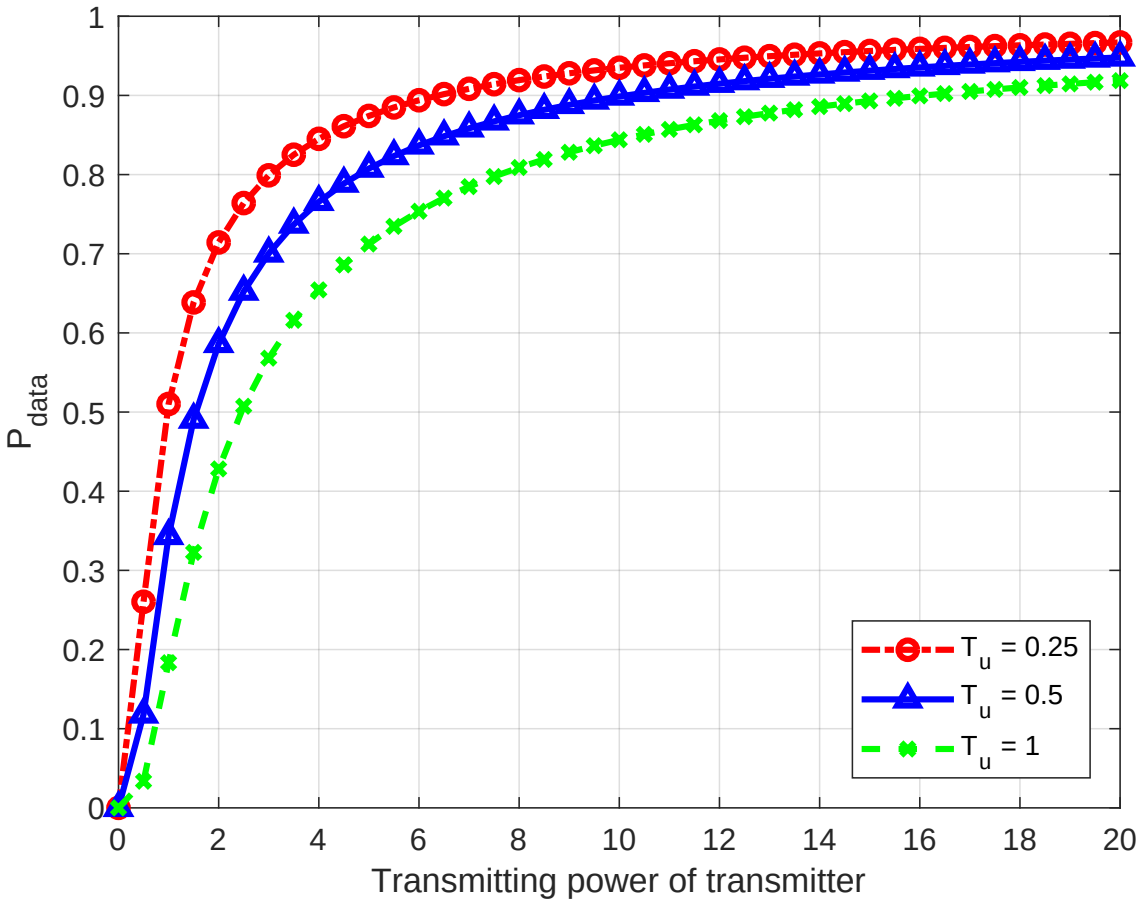

Figure 4.3: Success data link probability with different T_u

higher threshold of the data link, the probability drops because it is harder for the data receiver to decode the message.

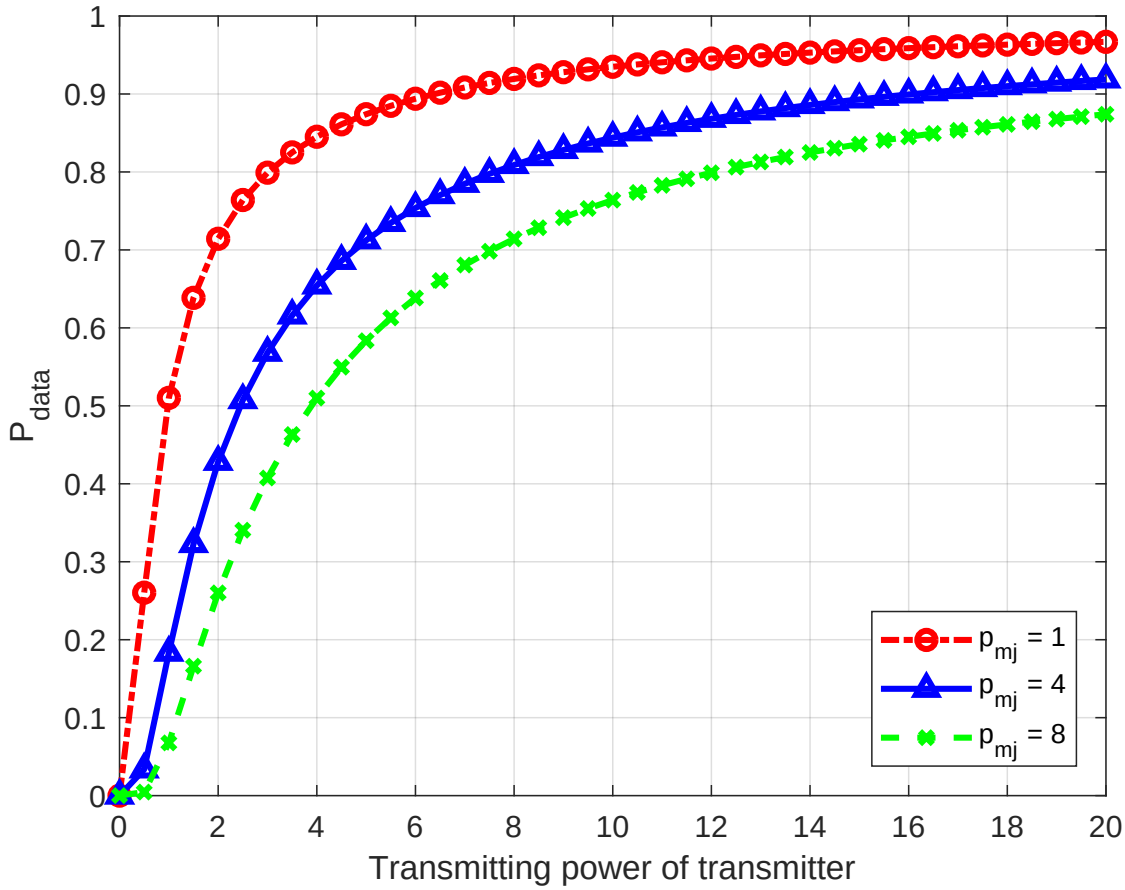

Figure 4.4: Success data link probability with different P_{-j}

In the Fig. 4.4, we change the average transmitting power of other D2D relay users. We find that when the transmitting power of other relays are bigger, the success probability gets lower. Because the data receiver get higher interference.

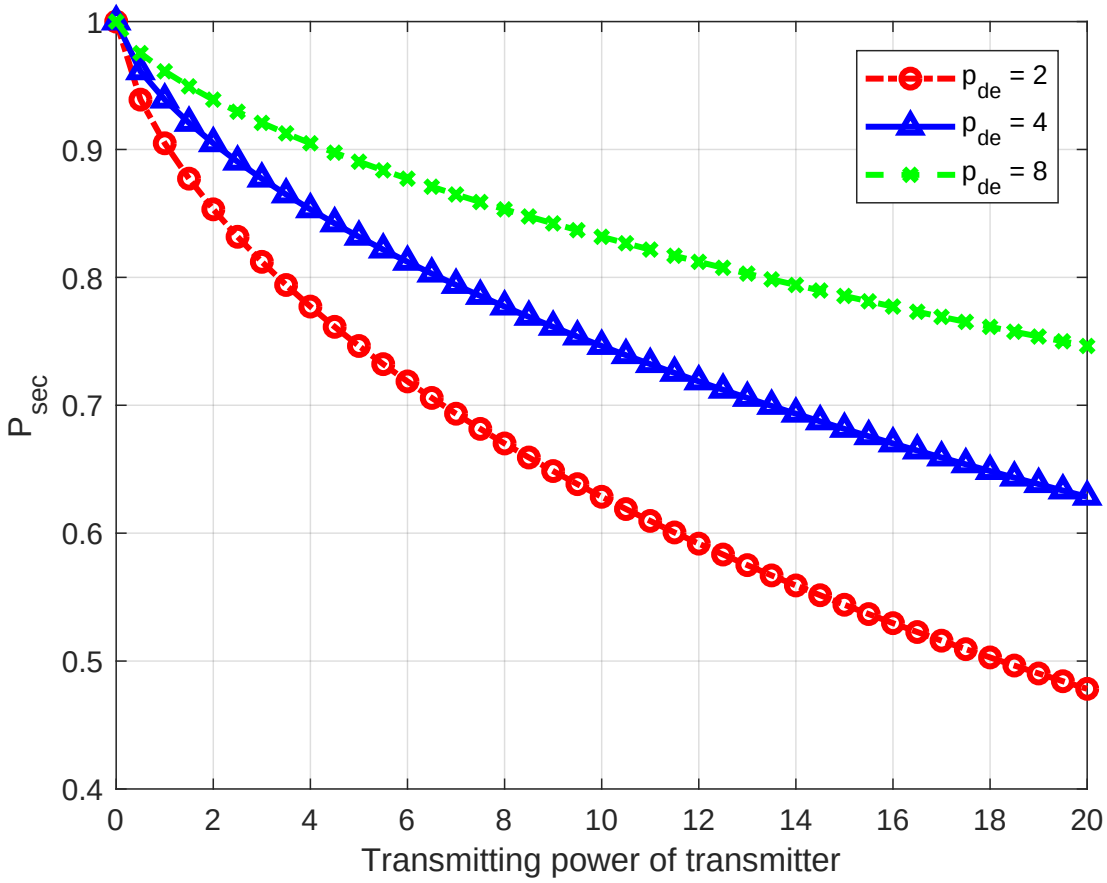

Figure 4.5: Security probability via transmitting power

In Fig. 4.5, we can see that when the transmitting power of the transmitter get higher, the security probability get lower. Because the eavesdropper could get a better SINR so that it can leak the message more easily. On the contrary, if the other D2D relay users improve their transmitting power, the SINR of the eavesdropper will have a lower SINR.

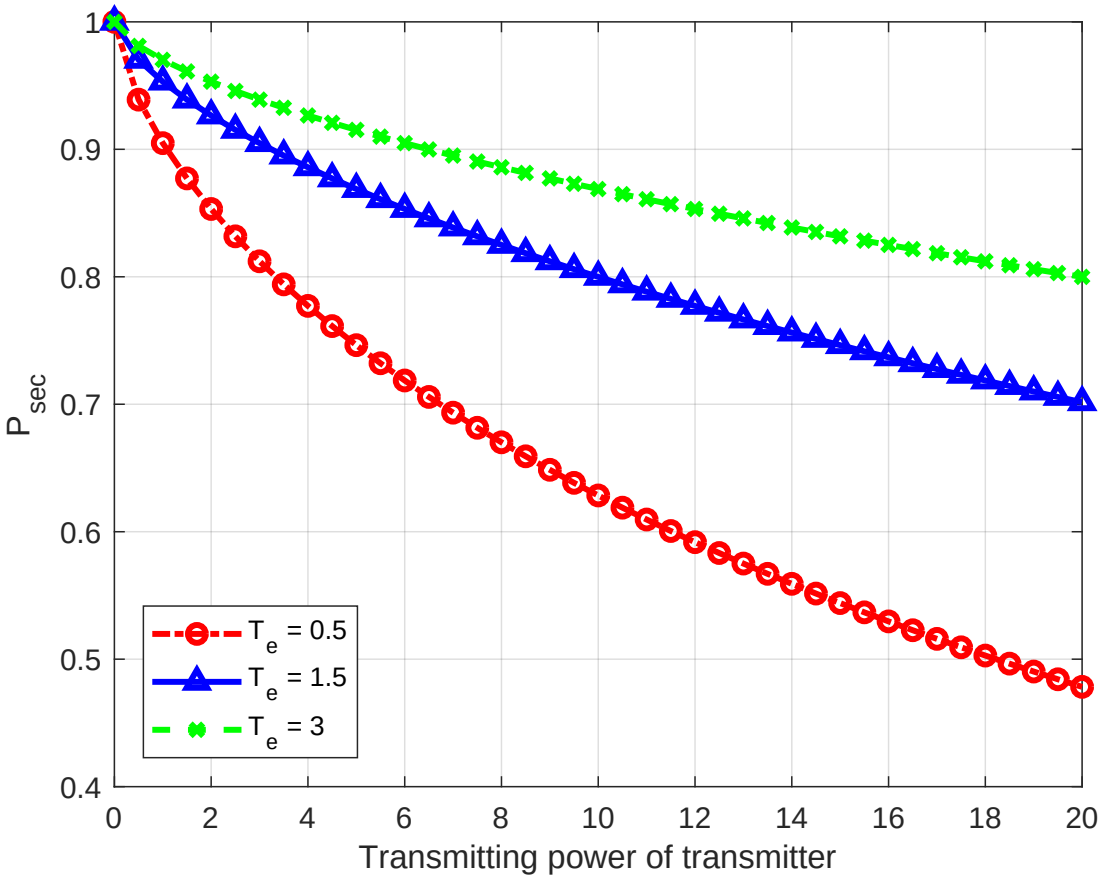

Figure 4.6: Security probability via transmitting power

In Fig. 4.6, we can find that when the value of T_e gets higher, the secured probability get higher because it is harder for the eavesdropper to leak the message.

4.6 Summary

In this chapter, we proposed a physical-layer security to equally protect the D2D users. In this scheme, the relay users will adjust their transmitting power to provide highest secured throughput for the receiver at the edge of the D2D transmitting area. Because all the relay users are send the different data, they do not need to spend extra energy to provide security

service. And the fairness of all data receivers are achieved since all the receivers at the edge of the D2D communication area have same SINR.

CHAPTER V

CONCLUSION AND FUTURE WORK

In this work, we proposed a data off-loading scheme based on game theoretical approach to achieve the maximum energy saving at a service provider. In the meanwhile, our proposed scheme provides the most incentive to D2D relay users. We proved that an optimal solution uniquely exists to the proposed scheme. We also proposed two algorithms to quickly approach to the optimal solution. The evaluation and simulation results demonstrated that our proposed D2D off-loading and rewarding scheme can benefit both of the service provider and the D2D relay user. In the future work, we will extend the schemes to other types of services in addition to multi-cast communications.

In the security part, we proposed a physical security scheme to protect D2D users. D2D transmitters manage their transmitting power to provide the highest SINR to the D2D receivers. The receivers are equally protected by all the other transmitters. In the meantime, the fairness of all the receivers are received, all the receivers have a common SINR in our scheme.

In the future work, we will improve our scheme to protect D2D users from the eavesdroppers whose locations are unknown. And more probability will be used as the distribution of the eavesdroppers so that the secured probability will be accurately derived.

BIBLIOGRAPHY

[1] F. Tong, Y. Wan, L. Zheng, J. Pan, and L. Cai, "A probabilistic distance-based modeling and analysis for cellular networks with underlaying device-to-device communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 451–463, Jan 2017.

[2] J. Wen, M. Sheng, X. Wang, J. Li, and H. Sun, "On the capacity of downlink multi-hop heterogeneous cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4092–4103, Aug 2014.

[3] Y. Shen, C. Jiang, T. Q. S. Quek, and Y. Ren, "Device-to-device-assisted communications in cellular networks: An energy efficient approach in downlink video sharing scenario," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1575–1587, Feb 2016.

[4] Q. Wu, G. Y. Li, W. Chen, and D. W. K. Ng, "Energy-efficient d2d overlaying communications with spectrum-power trading," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4404–4419, July 2017.

[5] D. H. Lee, K. W. Choi, W. S. Jeon, and D. G. Jeong, "Two-stage semi-distributed resource management for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1908–1920, April 2014.

[6] A. He, L. Wang, Y. Chen, K. K. Wong, and M. Elkashlan, "Spectral and energy efficiency of uplink d2d underlaid massive mimo cellular networks," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3780–3793, Sept 2017.

[7] Q. Wang, W. Wang, S. Jin, H. Zhu, and N. T. Zhang, "Quality-optimized joint source selection and power control for wireless multimedia d2d communication using stackelberg game," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3755–3769, Aug 2015.

[8] S. Wen, X. Zhu, Y. Lin, Z. Lin, X. Zhang, and D. Yang, "Achievable transmission capacity of relay-assisted device-to-device (d2d) communication underlay cellular networks," in *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, Sept 2013, pp. 1–5.

[9] R. Ma, Y. J. Chang, H. H. Chen, and C. Y. Chiu, "On relay selection schemes for relay-assisted d2d communications in lte-a systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8303–8314, Sept 2017.

[10] S. Xiao, X. Zhou, Y. Yuan-Wu, G. Y. Li, and W. Guo, "Energy-efficient relay placement and power allocation for two-hop d2d relay networks," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[11] Q. Sun, L. Tian, Y. Zhou, J. Shi, and X. Wang, "Energy efficient incentive resource allocation in d2d cooperative communications," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 2632–2637.

[12] D. Wasil, O. Nakhila, S. S. Bacanli, C. Zou, and D. Turgut, "Exposing vulnerabilities in mobile networks: A mobile data consumption attack," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, Oct 2017, pp. 550–554.

[13] R. Zhang, X. Cheng, and L. Yang, "Joint power and access control for physical layer security in d2d communications underlaying cellular networks," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[14] D. Fang, Y. Qian, and R. Q. Hu, "Interference management for physical layer security in heterogeneous networks," in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Nov 2017, pp. 133–138.

[15] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in d2d communications underlaying a cellular network," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2018.

[16] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in d2d-enabled cellular networks: A secrecy perspective," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 229–242, Jan 2015.

[17] Y. Chen, X. Ji, J. Yang, K. Huang, and M. Yi, "Physical layer security in d2d-enabled cellular networks: Artificial noise assisted," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–6.

[18] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[19] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[20] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5g of terrestrial mobile telecommunication," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 36–43, May 2014.

[21] Y. Benchaabene, N. Boujnah, and F. Zarai, "5g cellular: Survey on some challenging techniques," in *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, Dec 2017, pp. 348–353.

[22] Y. Huang, Y. Li, H. Ren, J. Lu, and W. Zhang, "Multi-panel mimo in 5g," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 56–61, MARCH 2018.

[23] P. Gandotra, R. K. Jha, and S. Jain, "Green communication in next generation cellular networks: A survey," *IEEE Access*, vol. 5, pp. 11 727–11 758, 2017.

[24] D. Nandi and A. Maitra, "Study of rain attenuation effects for 5g mm-wave cellular communication in tropical location," *IET Microwaves, Antennas Propagation*, vol. 12, no. 9, pp. 1504–1507, 2018.

[25] H. Wang, L. Dong, W. Wei, W. S. Zhao, K. Xu, and G. Wang, "The wsn monitoring system for large outdoor advertising boards based on zigbee and mems sensor," *IEEE Sensors Journal*, vol. 18, no. 3, pp. 1314–1323, Feb 2018.