8-2020

Enable Reliable and Secure Data Transmission in Resource-Constrained Emerging Networks

Xiaonan Zhang
Clemson University, zxn0509@gmail.com

Enable Reliable and Secure Data Transmission in Resource-constrained Emerging Networks

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Computer Engineering

by
Xiaonan Zhang
August 2020

Accepted by:
Dr. Linke Guo, Committee Chair
Dr. Daniel Noneaker
Dr. Harlan Russell
Dr. Long Cheng

Abstract

The increasing deployment of wireless devices has connected humans and objects all around the world, benefiting our daily life and the entire society in many aspects. Achieving those connectivity motivates the emergence of different types of paradigms, such as cellular networks, large-scale Internet of Things (IoT), cognitive networks, etc. Among these networks, enabling reliable and secure data transmission requires various resources including spectrum, energy, and computational capability. However, these resources are usually limited in many scenarios, especially when the number of devices is considerably large, bringing catastrophic consequences to data transmission. For example, given the fact that most of IoT devices have limited computational abilities and inadequate security protocols, data transmission is vulnerable to various attacks such as eavesdropping and replay attacks, for which traditional security approaches are unable to address. On the other hand, in the cellular network, the ever-increasing data traffic has exacerbated the depletion of spectrum along with the energy consumption. As a result, mobile users experience significant congestion and delays when they request data from the cellular service provider, especially in many crowded areas.

In this dissertation, we target on reliable and secure data transmission in resource-constrained emerging networks. The first two works investigate new security challenges in the current heterogeneous IoT environment, and then provide certain countermeasures for reliable data communication. To be specific, we identify a new physical-layer attack, the signal emulation attack, in the heterogeneous environment, such as smart home IoT. To defend against the attack, we propose two defense strategies with the help of a commonly found wireless device. In addition, to enable secure data transmission in large-scale IoT network, e.g., the industrial IoT, we apply the amply-and-forward cooperative communication to increase the secrecy capacity by incentivizing relay IoT devices. Besides security concerns in IoT network, we seek data traffic alleviation approaches to achieve reliable and energy-efficient data transmission for a group of users in the cellular network. The concept of mobile participation is introduced to assist data offloading from the base station to users in the group by leveraging the mobility of users and the social features among a group of users. Following with that, we deploy device-to-device data offloading within the group to achieve the energy efficiency at the user side while adapting to their increasing traffic demands. In the end, we consider a perpendicular topic - dynamic spectrum access (DSA) - to alleviate the spectrum scarcity issue in cognitive radio network, where the spectrum resource is limited to users. Specifically, we focus on the security concerns and further propose two physical-layer schemes to prevent spectrum misuse in DSA in both additive white Gaussian noise and fading environments.

To my beloved parents.

For their endless love, support, and encouragement

Acknowledgments

First of all, I would like to give my sincere appreciation to my advisor, Prof. Linke Guo, for giving me opportunity to do research and providing invaluable guidance, encouragement, and the greatest support with my years' study. Dr. Guo has not only helped me on my research during the past few years with his knowledge and insight, but also with thoughtfulness and patience on my personal growth. His dynamism, optimism, vision and sincerity have deeply inspired me. It was a great privilege and honor to work and study under his guidance.

I would like to thank Professor Daniel Noneaker, Professor Harlan Russell, and Professor Long Cheng for serving on my supervisory committee and for their strongest supports in my work and academic career.

I would also like to thank Dr. Yuguang Fang, Dr. Hongxin Hu, Dr. Zhanpeng Jin, Dr. Mark L. Fowler, Dr. Yu Chen, Dr. Xiaohua Li, and Dr. Ming Li for their timely help and suggestions on my research and my academic career.

I would not be a sane graduate student without a group of great friends. I would like to extend my thanks to all my colleagues in the lab for providing me a warm, family-like environment and for their collaboration and insightful advice. I specially thank Dr. Gaoqiang Zhuo, Dr. Qi Jia, Dr. Zekun Yang, Dr. Jian Zheng, Dr. Jing Zhang, Pei Huang, Sihan Yu, Ronghua Xu, Ning Chen, Weihang Tan, Antian Wang, Yu Xuan, Xiner Lu for many valuable discussions and all the good memories.

Specially, I would like to give express my gratitude to my advisor Linke Guo and his wife Wenjun Chen, who not only constantly encouraged me and helped me in many ways, but also shared their view of life with me.

Finally, I owe a special debt of gratitude to my beloved parents for their love and sacrifices for educating and preparing me for my future. It is them who have been always supporting me and have be accompanying with me to share my success, failure, joys, and tears. Without their constant and unwavering love, I would never imagine what I have achieved.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Research Overview

Our daily lives and even our society are greatly benefited from the emerging wireless networks such as Internet of Things (IoT) and the cellular network. Different from traditional networks, there are several new features in the emerging networks, including large quantities of data, an increasing number of users and devices, heterogeneous environment, etc. However, due to the fact that resources such as energy, spectrum, and computational capabilities are constrained, the deployment of the emerging networks faces lots of challenges. For example, although the exploding popularity of mobile devices enables people to enjoy benefits brought by various interesting mobile apps, such as social networking, mobile video services, and location-based services, the ever-increasing data traffic has exacerbated the depletion of licensed wireless spectrum bands along with the energy consumption in the cellular network. As a result, users experience severe congestion when they request data from the cellular provider. Not only by mobile devices such as mobile phones, but abundant data is also being continuously generated by ever-growing IoT devices like sensors, decision-making devices, and other miscellaneous electronic measuring apparatuses that are indiscriminately connected to the internet. These devices facilitate the evolution of the IoT, which forms a new networking paradigm that connects humans and the physical world through ubiquitous sensing, computing, and communications. The exponentially increasing number of those IoT devices also results in severe spectrum shortage specifically in the already crowded ISM band, resulting in several interferences as well. Besides, compared with mobile phones, IoT devices have very limited computational abilities and inadequate security protocols. As a result, data communication in IoT networks is more vulnerable to various attacks due to the open nature of the wireless environment, such as eavesdropping and replay attacks. In this dissertation, we strive to solve the mentioned issues around achieving reliable and secure data transmission in the emerging networks by carrying out feasible solutions.

1.2 Research Challenges

This subsection outlines the major reliability and security issues during data transmission that ought to be addressed in the emerging networks.

First of all, depending on different requirements on wireless transmission, dedicated wireless protocols have been adopted on various types of IoT, resulting in a heterogeneous environment. To alleviate interference among heterogeneous IoT devices and further improve the spectrum utilization efficiency, recent advances in Cross-Technology Communication (CTC) enable direct communication across those wireless protocols. However, this new methodology incurs serious security concerns on heterogeneous IoT devices. Data transmission becomes more vulnerable to various attacks such as eavesdropping and replay attacks. Even worse, with limited computational capabilities, traditional crypto approaches cannot work to defend against the above attacks.

Second, the information sensed, collected, and transmitted by IoT devices can be easily intercepted by adversaries, which becomes a serious concern in most IoT applications requiring sensitive data. The above problem becomes more serious in the large-scale IoT environment, such as the industrial IoT. In practice, cooperative communication approaches can effectively improve the security level for wireless communication under the presence of eavesdroppers with unbounded computational ability. How to motivate the participation of relay nodes to ensure reliable and secure data transmission becomes a huge challenge.

Third, mobile data offloading is a promising paradigm to alleviate data traffic by utilizing complementary and revolutionary networking techniques (e.g., small cell, WiFi offloading, and opportunistic communication) to deliver mobile data originally from the cellular network. However, the current approaches cannot fully address the issue in terms of user demand and offloaded traffic. As a result, mobile users still experience severe congestion when a large number of users request data. How to enable data delivery from the base station to a group of users becomes a big challenge and should be well addressed.

The last but not the least, Dynamic spectrum access (DSA) has been envisioned to become the key to enabler to solve worldwide spectrum shortage. However, the open nature of the wireless medium brings severe threats to the DSA system resulting from unauthorized access. Specifically, an unauthorized secondary user (SU) utilizes the licensed spectrum by faking/replaying the spectrum permit, which will not only introduce severe interference to authorized SUs but also disable the DSA system due to the lack of stability and incentives. Even worse, in practical DSA systems, pervasive fading channels would also cause wireless signal attenuation. Therefore, ensuring reliable communication between authorized secondary users while preventing spectrum misuse becomes a key challenge.

1.3 Scope and Organization of the Dissertation

The dissertation contributes to the scheme designs to achieve reliable and secure data transmission for several key research problems in the emerging networks given limited resources. The rest of the dissertation is organized as follows.

Cross-Technology Communication (CTC) tackles the interoperability issue in the heterogeneous IoT environment by enabling direct communication among devices across different wireless technologies. It can greatly avoid repeated data transmission among different protocols, enhance the spectrum efficiency in the already-crowded ISM band, and reduce the cost of gateway deployment. However, this new paradigm poses significant challenges. For example, an attacker can take advantage of CTC to launch attacks to IoT devices with a different protocol without being identified because of the protocol differences. Even worse, the low-computational capabilities of IoT devices hinder the deployment of computational-intensive cryptographic approaches at higher layers for detection. In Chapter 2, we identify a new physical-layer attack, cross-technology signal emulation attack, where a WiFi device can eavesdrop a ZigBee packet on the fly, and further manipulate the ZigBee IoT device by emulating a ZigBee signal. To defend against this attack, we propose two defense strategies with the help of a commonly found WiFi router.

In Chapter 3, we target on security enhancement in large-scale IoT network. On the one hand, over 60% of IoT applications are required to achieve low power consumption, long battery life, high data rate, and wide coverage simultaneously. However, none of the existing wireless technologies can satisfy the above requirement simultaneously. On the other hand, the disclosure of sensitive information, including machinery data, patients' health data, or financial files, collected by many IoT applications is unacceptable. Unfortunately, data communication is de facto vulnerable to the eavesdropping attack due to the heterogeneous wireless environment in the large-scale IoT system. Cooperative communication is a perfect fit to tackle the above challenges with its advantages on wide coverage, energy efficiency, and high interference mitigation capability. In addition, it introduces the inherent randomness of wireless channels, which could prevent eavesdroppers from intercepting the transmitted message. In Chapter 3, we apply the amplify-and-forward (AF) cooperative communication to increase the secrecy capacity of IoT systems by incentivizing relay IoT devices.

Facing the challenges that mobile users still experience severe congestion when a large number of users request data from the base station with the consideration of mobile data offloading, we take a step further to reconsider the human-enabled approach for mobile offloading, which takes human social behaviors and human activities into consideration. Intuitively, users with similar social interests often group together in certain crowded areas such as football stadiums and theme parks, which potentially results in similar content requests. The above phenomenon leads us to consider how to avoid repeated requests/retrievals in order to reduce the number of accesses to the service provider. As for human activities, an observation is that users in crowded areas either walk around or go to their interested attractions. Therefore, in Chapter 4, we introduce the concept of mobile participation to assist data offloading by leveraging the mobility of users and the social features among a group of users. A mobile caching user, who pre-caches a certain amount of contents, will roam around congested areas to participate in data dissemination in order to satisfy users' requests, which is expected to benefit both himself and users in the crowd simultaneously. To motivate such human-enabled mobile participation for data offloading, a Stackelberg game is deployed with joint considerations on social effect and delay effect.

As an extension work in Chapter 4, the data dissemination among the users within the group is well studied in Chapter 5 to achieve energy efficiency. The explosively increasing data traffic leads to a significant increase in energy consumption and thus puts an adverse effect on the environment. Having the offloaded data, similar social interests among users motivates them Device-to-Device (D2D) communication for further data dissemination within the group, which would greatly relieve the traffic burden at base stations and thus free energy consumption. However, energy consumption in D2D communication becomes one of the most critical challenges for deployment. Frequently transceiving data between battery-powered mobile devices could quickly drain their energy. Meanwhile, arbitrarily caching data in their buffer will bring trouble due to limited buffer size. Even worse, the stability of the entire network suffers from break-off users. In Chapter 4, we leverage users' social preference to reduce energy consumption on mobile devices and keep the stability of the entire system while satisfying users' traffic demands.

Dynamic System Access (DSA) has received considerable attention recently due to its ability to alleviate the spectrum scarcity issue. However, the unauthorized secondary user can utilize the licensed spectrum by faking/replaying the spectrum permit, which not only introduces severe interference to authorized SU but also disables the DSA system due to the lack of stability and incentives. In Chapter 6, we propose a secure and optimized unauthorized SU detection scheme. Our scheme achieves accurate and efficient permit detection. Meanwhile, unauthorized SU is effectively prevented from faking/replaying the spectrum permit, which improves the security of the DSA system.

As an extension work of Chapter 6, we consider the fading effects when designing an unauthorized secondary user detection scheme in Chapter 7. In practical DSA systems, due to the atmospheric ducting, ionospheric reflection and refraction, and the reflection from terrestrial objects, the communication between authorized second users is via a wireless multipath channel, which would suffer the wireless signal from an arbitrary time dispersion, attenuation, and phase shift, known as fading. In Chapter 7, we devise an authorized secondary user authentication scheme that is robustness to fading effects and further unleash its great potential for future wireless systems.

Finally, Chapter 8 concludes this dissertation and discusses some future research work.

Chapter 2

Signal Emulation Attack and Defense for Smart Home IoT

2.1 Chapter Overview

The proliferation of the Internet of Things (IoT) enables ubiquitous connections among various wireless devices, such as wearable health monitors, security locks, fitness trackers, etc., for bettering our daily life [9,161]. According to a recent market report [40], it is expected the number of IoT devices will reach to a total of 41.6 billion by 2025. Among different wireless technologies being used, ZigBee is one of the dominant protocols used for smart home applications. Many household appliances have equipped with ZigBee chips for receiving commands from a multi-protocol gateway (ZigBee communication) and further being managed by users' mobile devices (WiFi communication). However, the wireless transmission between the gateway and ZigBee devices can be easily overheard by eavesdroppers, in the sense that the smart home IoT devices have the potential of being hacked in the wireless environment. Considering the dramatic growth of IoT used in home areas and the critical functionalities that IoT has involved, the loss could be immense. For example, attackers can turn on the cooling on smart thermostats during winter, unlock the smart garage door, and even turn off security camera for break-in, by transmitting the eavesdropped ZigBee signal directly without using the authorized gateway. Even worse, as our experimental results demonstrate, existing upper-layer cryptographic approaches do not work, and thus the attacker can completely bypass the upper-level security detection at ZigBee receivers.

Besides ZigBee, WiFi and Bluetooth protocols also play important roles in smart home applications. They all occupy the Industrial, Scientific, and Medical (ISM) 2.4 GHz band, generating a heterogeneous environment [45,109,115,165]. To tackle the interoperability issue, Cross-Technology Communication (CTC) serves as a feasible solution by enabling direct communication among devices across different wireless technologies [35, 74, 119]. It can greatly avoid repeated data transmission among different protocols, enhance the spectrum efficiency in the already-crowded ISM band, and reduce the cost of gateway deployment. However, this new paradigm poses significant security challenges. One of them is: an attacker can take advantages of CTC to launch attacks to IoT devices with a different protocol without being identified. Even worse, the low-computational capabilities of IoT devices hinders the deployment of computational-intensive cryptographic approaches at higher layers for detection. Taking WiFi to ZigBee CTC as an example, with a much higher transmission power and mobility, WiFi devices can generate a stronger signal with a greater transmission range than ZigBee devices. As a result, WiFi devices can successfully attack ZigBee devices from a further distance without being found, making the attack more practical and powerful. Given the increasing deployment of IoT devices, it is critical to detect this type of attack and design effective countermeasures.

In this chapter, we identify a new attack named as **Signal Emulation Attack** in the practical smart home scenario, where a WiFi attacker first eavesdrops on the control message by listening to the communication between ZigBee devices and their gateway. Then, it embeds the control message into its WiFi signal to manipulate the functionality of ZigBee devices. The emulated signal can pass the demodulation process at the ZigBee receiver, and thus it is infeasible to be detected. To protect the ZigBee devices, this work proposes two defense strategies with the help of an auxiliary anchor, i.e., a WiFi router. We list our contribution as follows,

- We are the first to identify a new physical-layer attack, the signal emulation attack, in the heterogeneous environment.

- The proposed passive defense strategy prevents the WiFi attacker from emulating a perfect ZigBee signal by leveraging the noise generated by the anchor.

- We also propose a proactive defense strategy to protect ZigBee receiver with the help of the anchor, which can determine whether the signal is coming from a valid ZigBee source in a real-time manner.

- We perform extensive experiments to validate threats of the signal emulation attack and further demonstrate the effectiveness of two defense strategies.
- We design a real-world prototype to enable the smartphone to perform the signal emulation attack, while defense strategies are thoroughly evaluated in practical scenarios.

The rest of this chapter is organized as follows.The related works are discussed in Section 2.2. Section 2.3 illustrates the motivation of signal emulation attack, together with the introduction of a threat model. Section 2.4 gives some background information about the ZigBee receiver and the WiFi transmitter, based on which we demonstrate the details of the signal emulation attack in Section 2.5. As the countermeasures, passive and proactive strategies are proposed in Section 2.6 and Section 2.7, respectively. We give our experimental confirmation of the signal emulation attack as well as evaluation of two defense strategies in Section 2.8, followed by the conclusion in Section 2.9.

2.2 Related Work

2.2.1 Solutions to PHY Security Problems

Physical-layer security problems mostly focus on how to prevent attacks (e.g., eavesdropping and interception) during the communication. Corresponding defense strategies can be categorized into two groups. One is to theoretically discuss the secrecy capacity, which exploits the property of the wireless channel for secure communication [54, 178]. Many transmission strategies, such as cooperative transmission [201], artificial noise [124], and secure beamforming [121], are proposed to enhance the security capacity in the physical layer. The other group is to embed the private permit into the message to prevent it from being replayed, such as RF fingerprinting in [26, 83, 166] and authentication signal embedding in [97, 98, 105, 106, 142, 163, 185, 193]. However, the above methods cannot prevent the signal from being eavesdropped and emulated.

2.2.2 Cross-Technology Communication

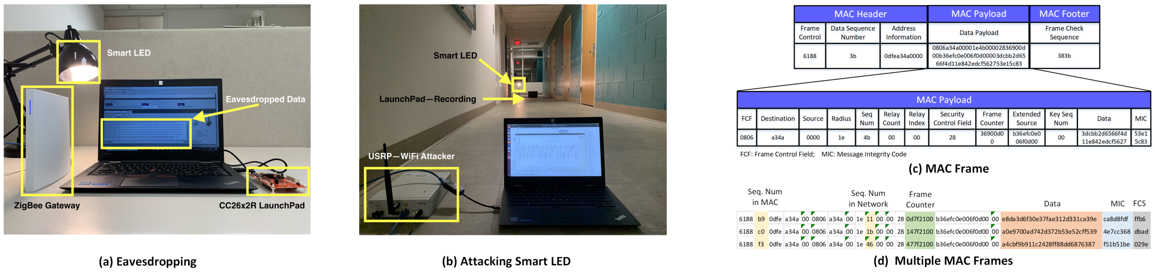
Cross-Technology Communication (CTC) is envisioned to serve as an effective approach to alleviate the cross-technology interference by allowing direct communication between devices with different protocols [32,194,197,198]. B^2W^2 [35] enables the high throughput and long distance concurrent N-way CTC between BLE and WiFi by leveraging channel state information. In FreeBee [102], Esense [32] and GSense [195], the communication between WiFi and ZigBee devices is enabled by using RSS to measure the WiFi signal. Different from the above packet-level CTCs, Li *et. al* in [119] propose a physical-level emulation technique. Their objective is to increase the throughput in CTC. From security perspective, Chen *et. al* discuss potential jamming attacks and sniffing attack in [33]. Different from these works, we consider the emulation technique as a powerful attacking method and further make the emulation attack complete and more practical to real life.

2.2.3 RF Fingerprinting

Most radio fingerprinting methods identify a device by considering various PHY layer classification approaches. Based on [26], RF features are broadly classified into: (1) channel-specific ones, e.g., channel impulse response, that characterize the wireless channel. They have been successfully adopted in robust location distinction [118,141]; (2) Transmitter-specific ones that are independent of the channel, e.g., artifacts of individual wireless frames [26], unique features in the radio turn-on transients [46], and joint time-frequency Gaborand Gabor-Wigner Transform features [149]; and (3) Hardware properties like TCP and ICMP time stamp in [103]. All the above work apply radio fingerprint techniques to distinguishing different wireless devices whiles our proactive defense strategy is to differentiate signals generated based on different protocols. In other words, our strategy still works even if the ZigBee device is changed to a new (unknown to the classifier) one.

2.3 Motivation

From the attackers' perspective, when performing attacks to ZigBee devices, one of the major difficulties is the short attacking range (approx. 10m). Due to the limited transmission power, attackers can even be identified within the line-of-sight (LoS) range. In what follows, we conduct an experiment to demonstrate the limitation of attacking ZigBe devices using the ZigBee protocol, and further discuss the feasibility and severeness of the WiFi-enabled emulation attack.



(a) Eavesdropping

(b) Attacking Smart LED

MAC Header			MAC Payload	MAC Footer
Frame Control	Data Sequence Number	Address Information	Data Payload	Frame Check Sequence
6188	3b	0dfea34a0000	0806a34a00001e4b00002836900d 00b36efc0e006f0d00003dcbb2d65 66f4d11e842edcf562753e15c83	383b

MAC Payload												
FCF	Destination	Source	Radius	Seq Num	Relay Count	Relay Index	Security Control Field	Frame Counter	Extended Source	Key Seq Num	Data	MIC
0806	a34a	0000	1e	4b	00	00	28	36900d0 0	b36efc0e0 06f0d00	00	3dcbb2d6566f4d 11e842edcf5627	53e1 5c83

FCF: Frame Control Field; MIC: Message Integrity Code

(c) MAC Frame

	Seq. Num in MAC								Seq. Num in Network				Frame Counter			Data	MIC	FCS
6188	b9	0dfe	a34a	00	0806	a34a	00	1e	11	00	00	28	0d7f2100	b36efc0e006f0d00	00	e8da3d6f30e37fae312d331ca39e	ca8d8fdf	ffb6
6188	c0	0dfe	a34a	00	0806	a34a	00	1e	1b	00	00	28	147f2100	b36efc0e006f0d00	00	a0e9700ad742d372b53e52cff539	4e7cc368	dbad
6188	f3	0dfe	a34a	00	0806	a34a	00	1e	46	00	00	28	477f2100	b36efc0e006f0d00	00	a4cbf9b911c2428ff88dd6876387	f51b51be	029e

(d) Multiple MAC Frames

Figure 2.1: Experiment on the Vulnerability of ZigBee devices

2.3.1 Experimental Results and Observations

2.3.1.1 Experiment Settings

As shown in Fig.2.1a, we use a Commercial off-the-shelf (COTS) Sylvania ZigBee LED [14] light bulb as an end IoT device, and we also let a gateway send “`TURNING ON`” and “`TURNING OFF`” commands to LED. The LaunchPad CC26x2R [92] (ZigBee attacker) is deployed to eavesdrop on the communication between the gateway and LED. The command messages are stored and re-sent using both the LaunchPad and USRP (WiFi attacker) as shown in Fig. 2.1b, where the USRP sends an emulated signal based on the eavesdropped ZigBee signal. Given the experimental results, we analyze the advantages of using WiFi for launching the attack.

2.3.1.2 Payload Analysis

We use WireShark [8] to analyze the packets sent by the gateway in Fig.2.1c. To launch the attack, we use the LaunchPad to send the eavesdropped ZigBee packet for attacking the smart LED. Although the commands change over time, the ciphertext form of “`TURNING ON`” shown in the “Data” field can still be re-used on the LaunchPad for turning on the LED as shown in Fig.2.1d. In our case, the receiver LED does not verify the sequence numbers and frame counters, making it already vulnerable to the replay attack. However, even if the protocol enforces the verification to defend, this type of attack is still possible because of the potential key leakage issue during the initialization process [99,133,155] especially when there is a new device added into the network [51]. Many cracking tools [7] can be used to steal the keys and finally decrypt the received commands. Therefore, even if ZigBee devices are using symmetric upper-layer encryption schemes, such as AES-CCM, this type of attacker still can change the sequence number and/or frame counters in the decrypted message and then re-encrypt as a new message, achieving the successful replay attack to

ZigBee devices.

2.3.1.3 Attacking Performance Analysis

From the perspective ZigBee devices, given the above vulnerability, they may suffer even more serious attacks in the heterogeneous environment consisting of malicious WiFi attackers.

- **Attacking range**: Adopting IEEE802.15.4 protocols, the transmission power of ZigBee attackers is relatively low at 5dBm, while a common smartphone WiFi transmission power is 6-7 times more than that, making the attacking range greatly improved.
- **Attacker detection**: The low transmission power of ZigBee attackers prevents them from performing the attack at Non Line-of-Sight (NLoS) locations. Thus, they are at a higher risk of being detected. However, the WiFi attacker can stay at NLoS locations to attack ZigBee devices without being found.
- **Device ubiquity**: Compared to WiFi devices that pervasively exist in people's daily life, devices with ZigBee protocol are always fixed at certain places, which reduces the feasibility for attacks.

From the attacker's viewpoint, to verify the feasibility and benefits brought by WiFi protocol, we extend the above experiment by using a USRP to attack LED using both ZigBee signal and WiFi emulated signal (detail will be presented later). We also deploy a LaunchPad next to LED to record received packets.

As shown in Table.2.1, both the symbol-error-rate (SER) and packet-error-rate (PER) will increase in the LoS scenario for both ZigBee and WiFi attackers, resulting in a significant drop in attack success rate. When both attackers are closer to the LED, their SER and PER remain similar. However, the WiFi attacker has higher attacking success rate as the distance increases to 15m and 20m. In addition, due to the NLoS propagation feature of the WiFi signal, the WiFi attacker can also launch the attack when hiding outside of the house. According to the above discussion, WiFi attackers are more powerful than ZigBee attackers in terms of 1) longer attacking range; 2) NLoS capability; 3) ubiquity of devices. Given these advantages, the resulting consequences would be immense if no prevention mechanism is deployed.

Table 2.1: Symbol/Packet Level Performance (LoS)

Distance	5m	10m	15m	20m
SER (WiFi)	0.55%	0.4%	0.52%	1.23%
PER (WiFi)	0.75%	1.8%	4.1%	4.8%
SER (ZigBee)	0.51%	0.44%	1.34%	2.31%
PER (ZigBee)	1.1%	1.7%	6%	15.2 %

2.3.2 Threat Model

Motivated by the above observation, we focus on a physical-layer signal emulation attack on ZigBee devices. Instead of launching the attack using ZigBee devices, we consider a WiFi attacker for longer attacking range and higher success rate, for which it can hide somewhere (50m away) without being found. Specifically, the entire signal emulation attack consists of the following steps.

Step 1: Signal Eavesdropping. The WiFi attacker moves close to ZigBee devices to eavesdrop on the communication between ZigBee devices and their authorized gateway.

Step 2: Signal Emulation. The WiFi attacker "translates" the eavesdropped ZigBee signals into its "own language" for attacking.

Step 3: Device Attacking. By ensuring the channel is not occupied by ZigBee devices, the WiFi attacker sends emulated signal via its RF component for attacking purpose.

With this being said, the WiFi attacker will follow the IEEE 802.11g standard for physical (PHY) and media access control layer (MAC) when launching the attack. We assume it will be able to eavesdrop on the overlapped frequency band between WiFi and ZigBee within a close proximity. The WiFi attacker can also store the historical knowledge of ZigBee signals, such as eavesdropping time, location, and amplitude. Given previously discussed advantages, the WiFi attacker can be any device with a WiFi radio, which can send signals with a higher power (approx. 8dB higher than ZigBee) at any place within the transmission range. Meanwhile, we limit the WiFi capabilities from the following aspects: due to protocol differences, 1) WiFi attackers are unable to generate a WiFi signal that is completely the same with the eavesdropped ZigBee signal; and 2) WiFi attackers are unable to simply replay and amplify the eavesdropped ZigBee signal.

As for ZigBee devices, they follow the IEEE 802.15.4 standard. Mostly, they are fixed at specific locations, such as kitchen, bedroom, and garage, where they communicate with gateways as usual. In particular, they are unable to detect the existence of WiFi attackers. Most importantly, we assume they cannot distinguish the sources of received signals and can only execute the command as long as the signal passes its security check (in the case where cryptographic keys have been compromised).

2.4 Preliminaries

Before stepping into the detailed design of signal emulation attack, we first analyze its feasibility by reconsidering the ZigBee transmitter/receiver and WiFi transmitter.

2.4.1 ZigBee Transmitter and Receiver

ZigBee devices work in the unlicensed 2.4 to 2.4835 GHz ISM bands where 16 channels are allocated. Each channel occupies 2 MHz bandwidth with 5 MHz spaced apart. They apply Direct Sequence Spread Spectrum (DSSS) to improve interference/noise resilience. At the transmitter, each original ZigBee symbol (4 bits) is mapped to a 32-chip sequence by being multiplied by a pseudo-random noise spreading code. Offset Quadrature Phase Shift Keying (OQPSK) is deployed as the modulation scheme, which maps every 2 DSSS chips to one of the 4 complex symbols. At the receiver, after OQPSK decoding, the ZigBee receiver calculates the Hamming distance between received 32-chip sequence and all the 16 predefined 32-chip sequences as shown in Fig.2.2, where each predefined one corresponds to one ZigBee symbol. The predefined chip sequence having the minimum Hamming distance is chosen as the candidate. Meanwhile, the ZigBee receiver sets a threshold. If the minimum Hamming distance is smaller than the threshold, the received chip sequence is decoded to the ZigBee symbol that the candidate represents. Otherwise, the received chip sequence is discarded.

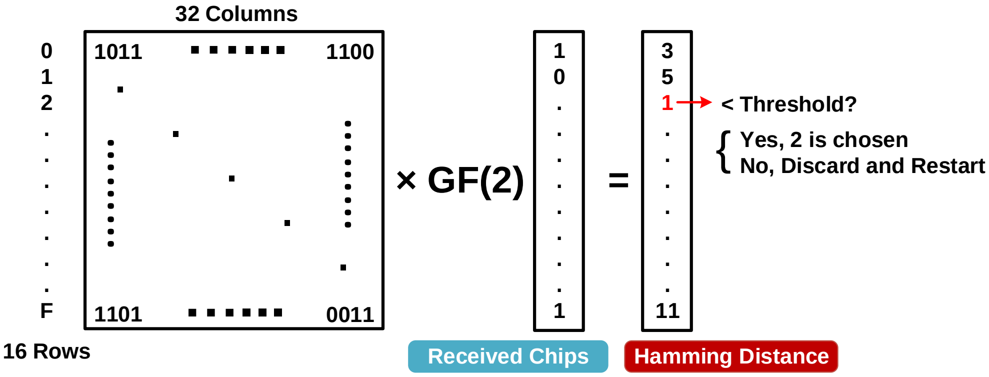


Figure 2.2: DSSS Demodulation

2.4.2 WiFi Transmitter

WiFi devices have a higher transmission power and longer transmission range compared to ZigBee devices. They also work in the 2.4GHz ISM band with 20 MHz bandwidth for each channel, which results in the potential spectrum overlapping between the WiFi and ZigBee signals. One example is that the ZigBee signal occupied on channel 17 (2434 – 2436MHz) is completely overlapped with that of the WiFi signal centered on the 2442 MHz (2432 – 2452MHz). However, WiFi transmitters deploy complete different PHY techniques compared to ZigBee transmitter. In our chapter, we mainly consider the following three differences.

2.4.2.1 Modulation scheme.

WiFi transmitter deploys 64-Quadrature Amplitude Modulation (QAM) followed by the Orthogonal Frequency Division Multiplexing (OFDM). Specifically, after preprocessing (scrambling, encoding, and interleaving), every 6 data bits are mapped to one of the 64 complex symbols on QAM constellation. Every 48 complex symbols together with 4 pilot symbols and 12 null symbols, representing the signal on 64 subcarriers (each occupies 312.5 kHz bandwidth) respectively, form an OFDM symbol [63] in frequency domain. The 64-point Inverse Fast Fourier Transform (IFFT) is then employed, changing the OFDM symbol from the frequency domain to the time domain.

2.4.2.2 Cyclic Prefix (CP)

After IFFT, a guard interval (CP), which is the repetition of the last 16 complex data, is added to the beginning, forming a complete WiFi symbol with 80 complex data. The CP together with OFDM helps WiFi signals combat multi-path effect by inhibiting inter-symbol interference (ISI) between adjacent OFDM symbols. ZigBee transmitter does not have CP process.

2.4.2.3 Repetitive Short Training Sequences (STSs)

WiFi receiver calculates the carrier frequency offset (CFO) from the center frequency via auto correlation among 10 repetitive STSs. Each STS contains 16 raw WiFi symbol. However, those repetitive STSs do not exist in the ZigBee signals.

In practice, the WiFi device can overhear the ZigBee signal due to spectrum overlapping. However, it cannot generate a signal that is completely the same as the ZigBee signal. Fortunately, the DSSS demodulation allows a few errors in received signals at the ZigBee receiver, which gives attackers opportunities to control ZigBee devices. Based on the above discussion, we list the main challenges in launching signal emulation attack, 1) how to generate a WiFi signal that is similar enough to the actual ZigBee signal? and 2) how to guarantee that the emulated signal can pass the DSSS demodulation and be decoded correctly?

2.5 Signal Emulation Attack

To answer the above questions, we detail our design in the signal emulation attack in this section.

2.5.1 Attack Overview

The signal emulation attack is shown in Fig.2.3. The WiFi attacker first eavesdrops on the signal from the communication between two ZigBee devices. Then, it generates a signal that is similar to the eavesdropped one. As a result, the emulated signal passes the DSSS demodulation process and the ZigBee device executes the command from the WiFi attacker.

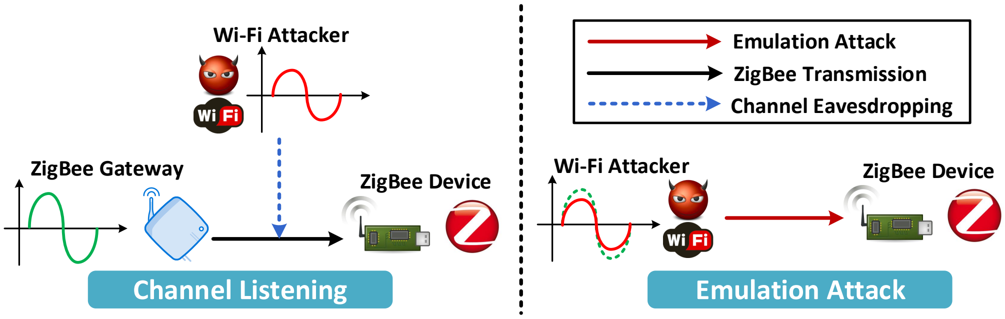


Figure 2.3: Cross-Technology Signal Emulation Attack

2.5.2 ZigBee Signal Eavesdropping

2.5.2.1 Overview

To launch the emulation attack, the WiFi attacker needs to know the ZigBee transmitter's signal. Locating close to ZigBee devices, the attacker passively senses the channel and records the received ZigBee signal. However, with a 20 MHz sensing bandwidth, the WiFi attacker also senses the signals from other sources, especially the environmental WiFi signals. Therefore, the difficulty becomes how to recognize and further capture the ZigBee signal from the received ones.

2.5.2.2 Short-Distance Eavesdropping

We first conduct an experiment to explain why the WiFi attacker has to eavesdrop on the ZigBee signal from a short distance to ZigBee devices. Two USRPs operating at the Channel 11 (centered at 2405MHz) play roles of the ZigBee transmitter and receiver, respectively. Their distance is set to 0.5m, 1m and 1.5m and 2m, respectively. The ZigBee transmitter randomly sends two signals each time. The real component amplitude of the received signals is shown in Fig.2.4, where the amplitude of the ZigBee signal decreases with the increase of the distance. When the transmitter is 2m away from the receiver, the ZigBee signal is overwhelmed by the noise. However, the ZigBee signal can still be decoded by the ZigBee receiver due to the error tolerance of DSSS. For the WiFi attacker, unfortunately, with completely different PHY layer techniques, it cannot extract the ZigBee signal from the noise. Therefore, the WiFi attacker has to locate in the close proximity to ZigBee devices to eavesdrop on the ZigBee signal.

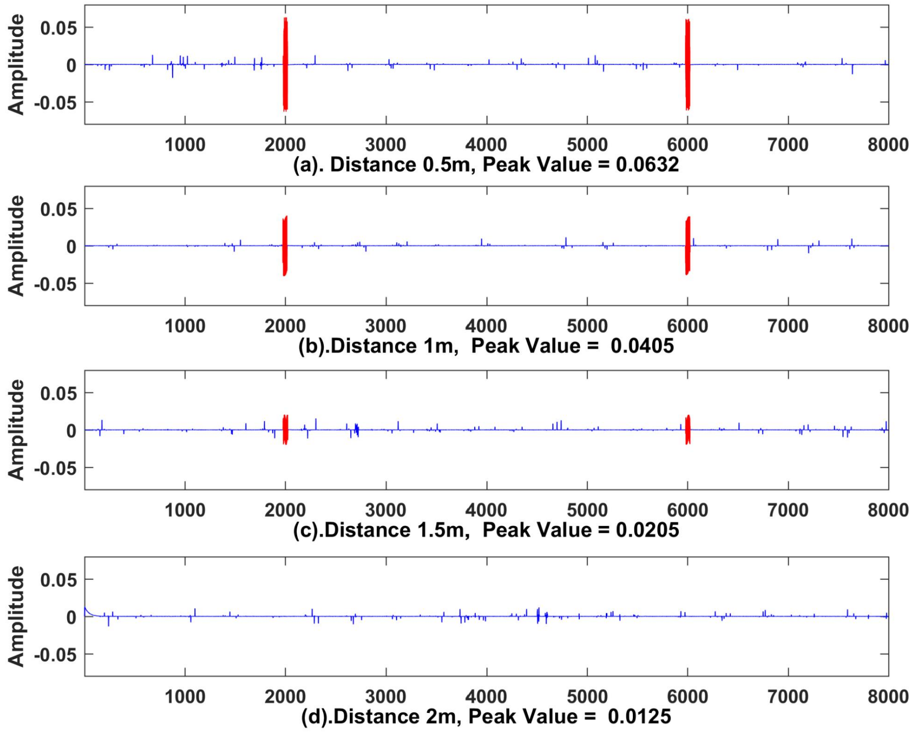


Figure 2.4: Received signal at ZigBee receiver

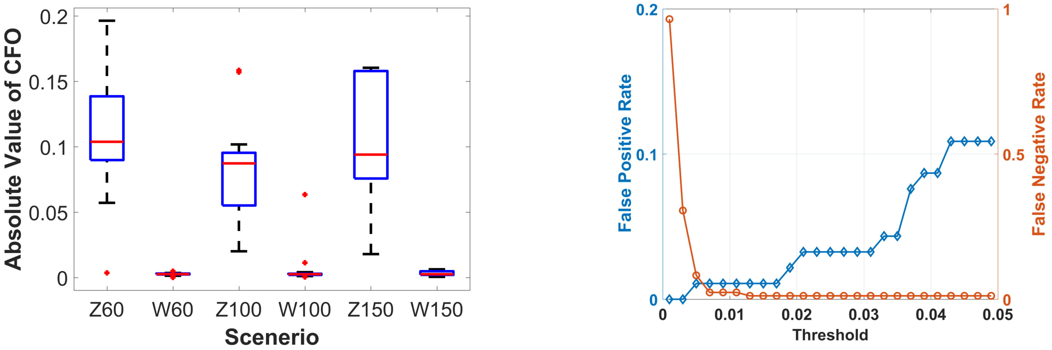
2.5.2.3 ZigBee Signal Distinguish and Extraction

WiFi attacker distinguishes the ZigBee signal from the view of WiFi frame structure. After detecting a sufficiently high amplitude, WiFi attacker temporarily stores the received signal and calculates the CFO as,

$$f_o = \frac{1}{16} \arg \sum_{n=0}^{N_{STS}-1-16} t[n]t^*[n+16], \tag{2.1}$$

where $t[n]$ denotes the n-th STS sample and $N_{STS} = 160$ represents total STS samples. t^* is the complex conjugate of the t. If f_o is above a given threshold, the received signal is supposed to be the ZigBee signal. WiFi attacker stores it for the further emulation. Otherwise, WiFi attacker assumes it as a WiFi signal and begins to decode it.

We conduct an experiment to verify the above method. Two USRPs send WiFi and ZigBee signals alternately while another USRP plays the role of the WiFi receiver. The distance between the transmitters and receiver is 0.6m, 1.5m and 2m. Each transmitter sends signals 100 times on each location. We illustrate the CFO performance in Fig.2.5a. The CFO of WiFi signal centralizes at 0 whereas the CFO of ZigBee signal is far larger (e.g., Z60 denotes ZigBee signal at 60cm and W100 denotes WiFi signal at 100cm). Fig.2.5b shows the eavesdropping accuracy. The false positive rate represents that the received normal WiFi signal is mistakenly considered to be from the ZigBee transmitter whereas the false negative rate denotes that the received ZigBee signal is regarded as from another WiFi device. As we can see, when the WiFi attacker sets its decision threshold for CFO to around 0.001, it can effectively eavesdrop on ZigBee signal while the WiFi signal receiving is not affected.



(a) CFO

(b) Accuracy

Figure 2.5: Eavesdropping Performance at WiFi attacker

Note that WiFi attacker can effectively extract the ZigBee signal without buffer overflow and extra cost as explained in the following. (1), Because WiFi attacker locates near to ZigBee devices, most RF samples with high amplitudes should come from either WiFi or ZigBee devices instead of other devices equipped with different wireless protocols. (2), Since users' operations to smart home ZigBee devices usually has the daily routines, WiFi attacker eavesdrops the ZigBee signal during a fixed period. Hence, WiFi attacker does not have to store the received signal all the time. (3), CFO calculation is the necessary step when decoding signals, there is no extra computational cost at the WiFi attacker.

2.5.3 ZigBee Signal Emulation

The objective of the ZigBee signal emulation is to generate a WiFi signal that is similar to the eavesdropped ZigBee signal. As shown in Fig.2.6, the attacker processes the eavesdropped signal in a reverse direction to obtain the corresponding WiFi data bits, which are sent to ZigBee devices when launching the attack. We ponder the problem step by step by comparing the difference between the ZigBee and WiFi transmitters.

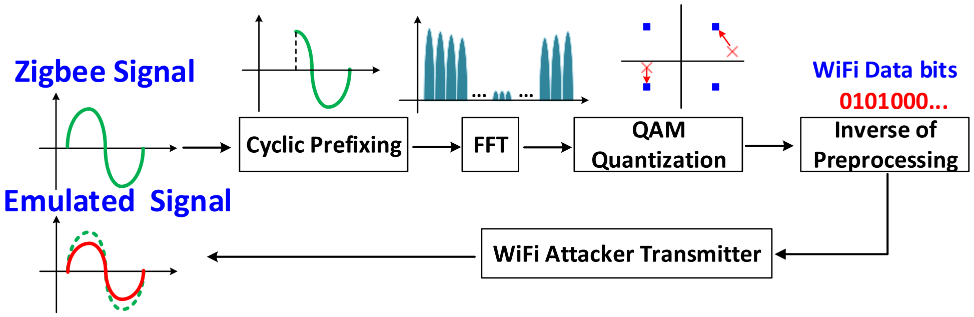


Figure 2.6: ZigBee Waveform Emulation

2.5.3.1 Cyclic Prefix Manipulation

Each WiFi symbol consists of 80 complex data, including 16 cyclic prefix data followed by the 64 effective data. However, the ZigBee signal does not have such a characteristic. Hence, given 80 eavesdropped data, the attacker inevitably discards the first 16 data and chooses the rest 64 data as the emulation objective. We assume every 64 data to be emulated constructs a sample. Meanwhile, we denote $z(n, s)$, where $n = 1, 2, \cdots, N$ and $s = 1, 2, \cdots, S$, as the n-th data in the s-th sample. We further assume there are S samples in the eavesdropped ZigBee signal and $N = 64$.

2.5.3.2 Frequency Subcarrier Selection

To get the corresponding WiFi data bits for each raw sample, a 64-point FFT is applied,

$$Z(k, s) = \sum\nolimits_{n=1}^{N} z(n, s) e^{-j\frac{2\pi}{N}nk}, k = 1, 2, \cdots, K, \tag{2.2}$$

where the FFT point $Z(k, s)$ denotes the component on the subcarrier k in the s-th raw sample in the frequency domain and $K = 64$. Since each WiFi symbol occupies 20MHz bandwidth with 64 subcarriers whereas the spectrum with 2MHz bandwidth is occupied by the ZigBee signal, only 7 subcarriers ($\frac{2}{20} \times 64$) of the WiFi signal are overlapped with the ZigBee Signal. The WiFi attacker emulates the eavesdropped signal by manipulating the components on 7 subcarriers. The question becomes how to locate those subcarriers.

Since the signal on the non-overlapped subcarriers is mostly the noise whereas that on the overlapped channels is more powerful. Hence, we deploy a folding process to locate them by considering the energy of the FFT points $E(k, s)$,

$$E(k, s) = Z(k, s)\overline{Z(k, s)}, \tag{2.3}$$

where $\overline{Z(k, s)}$ indicates the conjugate of $Z(k, s)$. The energy $E(k, s)$ forms a two-dimension matrix, where the elements in the kth row indicate the energy of each raw sample on the subcarrier k whereas those in the sth column signify the energy on each subcarrier in the raw sample s. Thus, a histogram $ES(k)$ of $E(k, s)$ is built according to the following equation,

$$ES(k) = \sum\nolimits_{s=1}^{S} E(k, s), k = 1, 2, \cdots, K, \tag{2.4}$$

where $ES(k)$ is the total energy of all the samples on the subcarrier k. We sort $ES(k)$ using the merge-sort algorithm [39] to identify the location of 8 most powerful subcarriers. The reason to choose 8 subcarriers instead of 7 is to ensure that the spectrum occupied by the emulated signal completely overlaps that occupied by the ZigBee signal. Here, subcarrier $29 - 36$ are chosen.

2.5.3.3 64-QAM Quantization Optimization

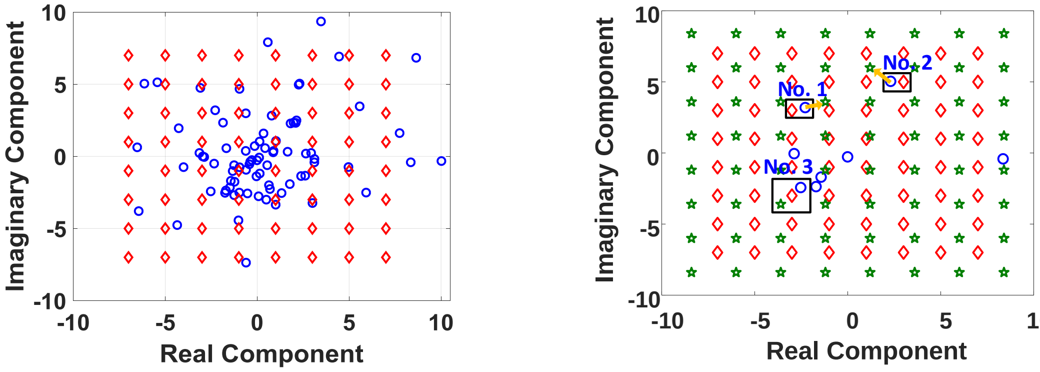
WiFi and ZigBee signals have different constellation structures. An example is shown in Fig. 2.7a, where blue circles and red diamonds represent FFT points of the eavesdropped signal and the 64-QAM constellation, respectively. To get WiFi data bits, the WiFi attacker quantizes FFT points to 64-QAM points. Such quantization results in irreversible distortion. WiFi attacker attempts to minimize the quantization distortion.

Based on the Parseval's theorem view [39], minimizing the signal distortion in the time-domain under energy metric is equivalent to minimizing the total deviation of frequency components after quantization. Hence, our principle is to choose the closest 64-QAM constellation point to each of the FFT points in term of Euclidean distance. Without considering constellation scale, the real and imaginary components of the 64-QAM points, Q_{Re} and Q_{Im}, are chosen from the set {-7, -5, -3, -1, +1, +3, +5, +7}, respectively. To minimize quantization errors, a scalar α is introduced. We have the following optimization problem,

$$\begin{aligned} \min_{\alpha} \quad & \sum_{k=SS}^{SE} \left(Z_{Re}(k,s) - \alpha Q_{Re}(m)\right)^2 + \left(Z_{Im}(k,s) - \alpha Q_{Im}(m)\right)^2 \\ & \alpha > 0, \end{aligned} \tag{2.5}$$

where $Z_{Re}(k,s)$ and $Z_{Im}(k,s)$ represent real and imaginary components of the FFT point $Z(k,s)$ respectively. SS and SE denote the start and end locations of the chosen FFT points, respectively. Let $j = \sqrt{-1}$. We have $Z(k,s) = Z_{Re}(k,s) + jZ_{Im}(k,s)$. In particular, $\alpha(Q_{Re}(m) + jQ_{Im}(m))$ indicates the 64-QAM point that is the nearest to the FFT point $Z(k,s)$. The optimization problem (2.5) aims to find the optimal scalar α such that the total quantization error between the chosen FFT points and their nearest QAM points is minimized. However, we cannot solve the problem directly since different $Q_{Re}(m)$ and $Q_{Im}(m)$ are chosen for the same FFT point $Z(k,s)$ given different scalar αs. For example, we choose 3 FFT points from Fig.2.7a and mark them as No. 1, 2, and 3 as shown in Fig. 2.7b. The scalar for the red-diamond 64-QAM constellation is $\alpha = 1$ while that of the green-pentagram 64-QAM constellation is $\alpha = 1.2$. In Fig.2.7b, the basic QAM point $Q_{Re}(m)$ and $Q_{Im}(m)$ for No.3 FFT point does not change, which is $-3-3j$. However, for No.1 FFT point, it is changed from $-3+3j$ to $-1+3j$ while from $3+5j$ to $1+5j$ for No.2 FFT point.

The above result indicates that an optimal scaler definitely exists that results in the least quantization error. We propose a quick algorithm to find the optimal scalar. As shown in Algorithm 1, we define a unit quantization (Line $7-14$) as the process that quantizes the FFT points to the



(a) Constellation Comparison

(b) Quantization Errors

Figure 2.7: 64-QAM Quantization Optimization

Algorithm 1: Quantization Error Minimization

```
Input: initial start and end of the scalar range $\alpha_S$ and $\alpha_E$
        basic 64 QAM constellation points $Q_{Re}(m)$ and $Q_{Im}(m)$, $m = 1, 2, \cdots, 64$
        chosen FFT points from ZigBee signal samples $Z(k, s), k = SS, SS + 1, \cdots, SE, s = 1, 2, \cdots, S$
its increasing gap $\delta = 1$
        error threshold $\eta = 10^{-5}$
Output: $\alpha^*$
1  $\hat{e} = 0$, $\overline{e} = 10^5$;
2  while $|\hat{e} - \overline{e}| > \eta$ do
3      $M = \alpha_E - \alpha_S/\delta$ ;
4      $\hat{e} = \overline{e}$ ;
5      for $i = 0; i < M$ do
6          $\alpha_i = \alpha_S + i * \delta$; $e_i = 0$ ;
7          for $i = 1$; $i \leq 8 * S$ do
8              for $m = 1$; $m \leq 64$ do
9                  $D(i, m) = (Z_{Re}(k, s) - \alpha_i Q_{Re}(m))^2 + (Z_{Im}(k, s) - \alpha_i Q_{Im}(m))^2$
10             end
11             $E(i) = \min_{0 \leq m \leq 64} D(i, m)$;
12             $k = \arg_{0 \leq i \leq 64} E(i)$;
13             $e_i = e_i + E(k)$
14         end
15     end
16     $\overline{e} = \min_{0 \leq i \leq M} e_i$;    $k = \arg_{0 \leq i \leq M} \overline{e}$;
17     $\alpha_S = \alpha_k - \delta/2$;    $\alpha_E = \alpha_k + \delta/2$;    $\delta = \delta/10$ ;
18 end
19 $\alpha^* = \alpha_k$ ;
20 return $\alpha^*$;
```

64-QAM points given a scalar and calculates the corresponding quantization error. Our key idea is that: instead of processing each unit quantization given a fixed scalar range $[\alpha_S, \alpha_E]$ with a fixed gap δ, we attempt to minimize the number of unit quantization process with a variable range and gap. As shown in Step 17, we shrink the optimal scalar range and decrease the gap simultaneously. Since the quantization error is a convex function of the scalar, the global optimal scalar is unique [25]. After each unit quantization, a current optimal scalar is found given a scalar range and gap. The global optimal scalar must be around the current one. Hence, after a few iterations, we can get a global optimal scalar.

Next, we demonstrate how the proposed algorithm speeds up the quantization process. Denote the number of the iterations as I_{num}. To ease description, we apply the symbol $'$ on the upper right to represent the initial values while the symbol $*$ to denote the values with the global optimal scalar. Without our algorithm, the unit quantization is processed $\frac{\alpha'_S - \alpha'_E}{\delta^*}$ times to minimize the quantization error by choosing the optimal scalar. Our algorithm reduces the times to $\frac{\alpha'_S - \alpha'_E}{\delta'} + 10I_{num}$, where $\delta^* = \delta' 10^{-I_{num}}$ as shown in Step 12. In the case with more iterations, our algorithm decreases the number of unit quantization processes by about $10^{I_{num}}$ times.

After 64-QAM quantization, WiFi data bits are obtained from the inverse process of the interleaver, convolution encoding, and scrambler as in [119]. Those bits are stored in the cache. The

WiFi attacker launches the attack by sending them to ZigBee devices.

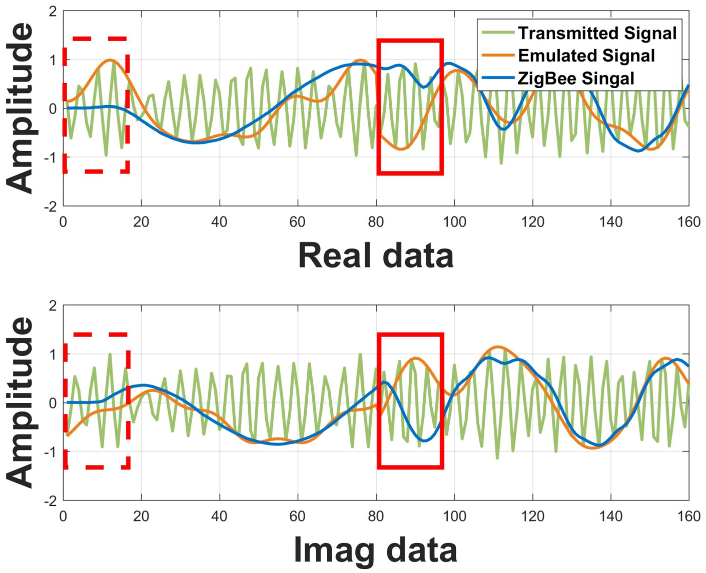


Figure 2.8: Eavesdropped Signal Vs. Emulated Signal

Fig.2.8 compares the ZigBee and emulated signals in a general case where ZigBee devices and WiFi attackers are centered in different frequencies, e.g., ZigBee on 2.405GHz and WiFi on 2.410GHz. The blue lines are the waveform of the ZigBee signal and the orange line represents the emulated signal. Those two waveforms are very similar except those in the red rectangle due to cyclic prefix rules. To achieve the goal of attacking the ZigBee receiver at its operation frequency, the WiFi attacker allocates the subcarriers $13-20$ to the emulated signal, which are 16 subcarriers' ahead from the central subcarrier locations $29-36$. Hence, the waveform of the transmitted signal is shown as the green lines in Fig.2.8.

2.6 Passive Defense Strategy

2.6.1 Motivation

The intuition behind our passive defense strategy is that *"Quantitative Changes lead to Qualitative Changes"*. By making trouble to the eavesdropping process, we mislead the WiFi attacker to generate the imperfect emulated signal, which cannot pass the detection at the ZigBee receiver. The proposed approach makes use of an auxiliary WiFi transmitter, for which we refer as an anchor.

As shown in Fig. 2.9, locating near the ZigBee transmitter, the anchor transmits the AWGN noise when the ZigBee device transmits the signal. We assume that the it follows the Gaussian distribution $n_z \sim \mathcal{CN}(0, \sigma^2)$ with the mean 0 and the variance σ^2. The signal received at both the ZigBee receiver and the WiFi attacker becomes,

$$z'(n, s) = z(n, s) + n_z(n, s). \tag{2.6}$$

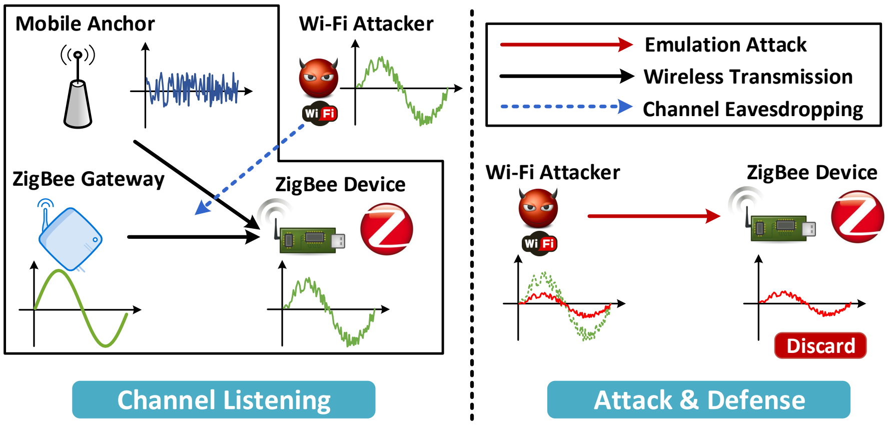


Figure 2.9: Passive Defense Model

2.6.2 Noise Effect to the WiFi Attacker

In the DSSS demodulation, ZigBee devices set a threshold to the number of error chips between the received chip sequence and the predefined ones. In other words, ZigBee devices tolerate a few error chips for each received chip sequence. Therefore, even if the ZigBee receiver receives a signal with a slightly smaller signal-to-noise ratio (SNR), it still can find one predefined chip sequence and is decoded to the ZigBee symbol that the predefined one represents. However, different from the regular decoding process, the noise concealed in the eavesdropped signal would propagate to the signal emulation process at the WiFi attacker, resulting in larger quantization distortion.

As in (2.6), the signal eavesdropped by the WiFi attacker is a noised ZigBee signal $z'(n, s)$. After the FFT operation, the output is,

$$Z'(k, s) = Z(k, s) + N_Z(k, s), \tag{2.7}$$

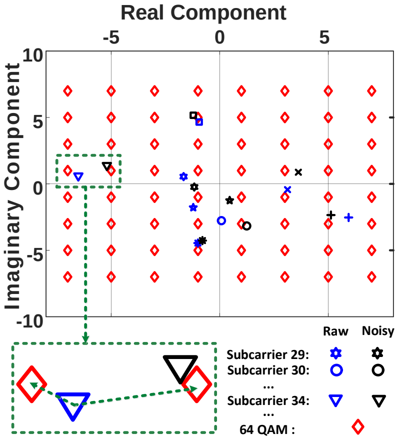
where $N_Z(k,s)$ is the FFT points of the AWGN in the frequency domain. The WiFi attacker quantizes the FFT points $Z'(k,s)$ to the QAM points based on Algorithm 1. Denote the QAM point corresponding to the FFT point $Z'(k,s)$ as $Q'(k,s)$. After quantization, the square error $e'(k,s)$ between the QAM point and the FFT point of raw signal is,

$$e'(k,s) = \left(Z_{Re}(k,s) - \alpha Q'_{Re}(m)\right)^2 + \left(Z_{Im}(k,s) - \alpha Q'_{Im}(m)\right)^2$$

However, if the anchor does not emit AWGN noise, the square error $e(k,s)$ for the FFT point $Z(k,s)$ is,

$$e(k,s) = \left(Z_{Re}(k,s) - \alpha Q_{Re}(m)\right)^2 + \left(Z_{Im}(k,s) - \alpha Q_{Im}(m)\right)^2 \tag{2.8}$$

The noise sent by the anchor tempts the WiFi attacker to quantize the FFT point $Z'(k,s)$ to a different QAM point $Q'(k,s)$. The new QAM point is farther to the FFT point $Z(k,s)$ of the ZigBee signal without the added noise, resulting in larger distortion in the emulated signal. To make it more clear, we pick up the noisy FFT points with the variance σ_F^2 in the first sample, $s = 1$ and draw them in Fig. 2.10 where the optimal scalar is $\alpha = 1$. σ_F^2 is the variance in the frequency domain. For the AWGN, variances in the time domain σ^2 and frequency domain σ_F^2 form a linear relationship. The blue marks in Fig. 2.10 denote the FFT points without the anchor whereas the black marks represent the FFT points with the added AWGN. We take the FFT point $k = 34$ as an example, which is amplified at lower left. When there is no added noise, the FFT point is quantized to the QAM point $-7 + j$ whereas the quantized QAM point becomes $-5 + j$ affected by the noise, which deviates the FFT point. Such a false quantization results in higher quantization error. The table in 2.10 further demonstrates our idea: the quantization error becomes larger when the anchor transmits the AWGN together with the ZigBee transmitter.



Subcarrier	$Q(k,s)$	$e(k,s)$	$Q'(k,s)$	$e'(k,s)$
29	$-1+j$	0.6466	$-1-j$	2.8371
30	$-1-3j$	1.2294	$1-3j$	0.8794
31	$-1-5j$	0.2995	$-1-5j$	0.2995
32	$3-j$	0.3377	$3+j$	2.0649
33	$5-3j$	1.0989	$5-3j$	1.0989
34	$-7+j$	0.3899	$-5+j$	2.4421
35	$-1-j$	0.6528	$1-j$	5.5319
36	$-1+5j$	0.1200	$-1+5j$	0.1199

Figure 2.10: Constellation Performance under AWGN Effect

Based on the Parseval's theorem [175], the energy in the time-domain is equalized to that in frequency-domain. Hence, the larger quantization error in the frequency domain results in the larger signal distortion. When the ZigBee device receives such a distorted signal, the chip error exceeds the threshold in DSSS. It discards the received signal. Therefore, the passive defense strategy prevents the WiFi attacker from controlling the ZigBee devices.

2.7 Proactive Defense Strategy

The major shortage in the previous passive defense strategy is that the added noise level cannot be too high. Otherwise, the ZigBee receiver cannot decode the valid information from the ZigBee transmitter neither. Besides, with the strong computation capability, the WiFi attacker can launch the signal emulation attack via the exhaustive search on its constellation and periodically checking the current state of the ZigBee receiver. Hence, new defense strategies are needed.

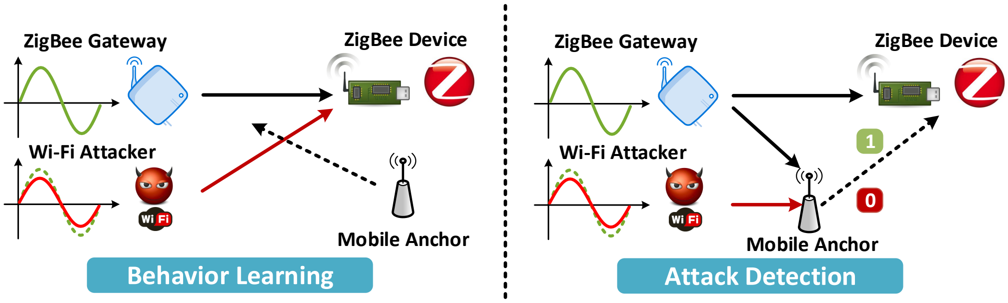
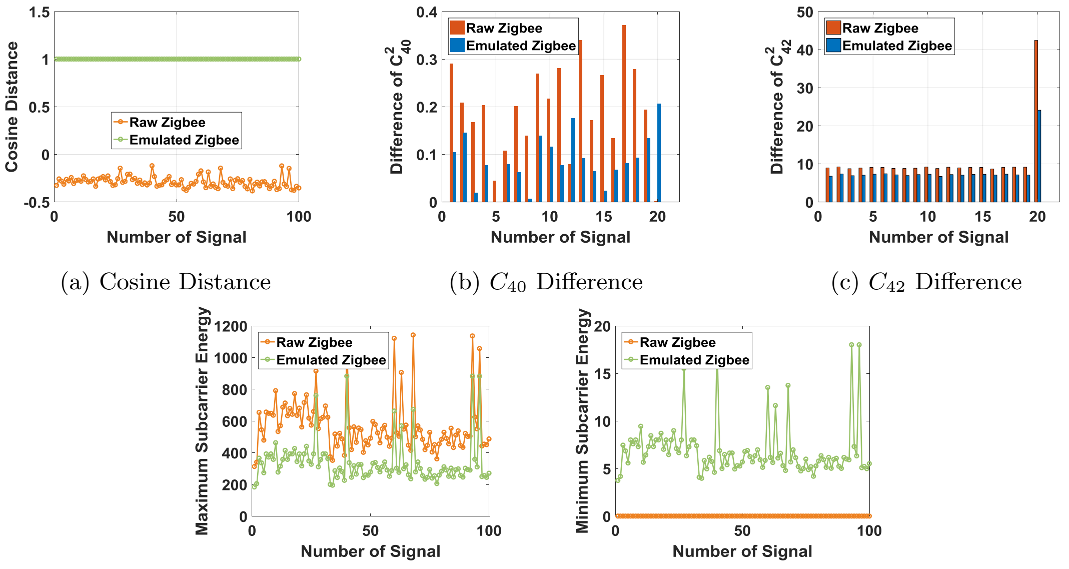


Figure 2.11: Proactive Defense Strategy

2.7.1 Motivation

As shown in Fig.2.11, the goal of this proactive defense strategy is to distinguish whether the received signal is from the WiFi attacker or the ZigBee transmitter in a real-time manner. To achieve it, the anchor will first proactively learn the behavior of both the WiFi attacker and the ZigBee transmitter from previously received signals. When the new signal is detected, the anchor classifies the signal source based on the historic learning knowledge.

Note that our proactive approach is different from radio frequency fingerprinting techniques [26, 46, 118, 141], which leverage the uniqueness in the transmitted signal to localize or identify the specific source based on the analog properties, particularly the presence of analog components in the radio transmission chain. However, our proactive scheme does not differentiate devices but instead, we use features to find differences between protocols. Besides, our used metric will only be evaluated within each signal (e.g., cosine difference) compared to RF fingerprinting-based approaches applying metrics for comparison of two same-protocol signals.



(a) Cosine Distance

(b) C_{40} Difference

(c) C_{42} Difference

(d) Maximum Energy

(e) Minimum Energy

Figure 2.12: Time-domain and Frequency-domain Features

2.7.2 Feature Extraction

To identify the differences between the ZigBee signal and emulated signal, the anchor extracts unique features from received signals on both the time and frequency domain.

2.7.2.1 Time Domain Feature

The cyclic prefix is obtained by prepending a copy of the last 16 complex data from the end to its beginning for the emulated ZigBee sample. With this being said, a circular signal structure appears, i.e., the first 16 data and last 16 data should be the same in each emulated sample. However, the ZigBee signal does not have such property. Therefore, the anchor can check whether the signal has such a circular structure. In particular, the anchor sends the received signal into the folding process after signal alignment. Because there are 80 complex data in each emulated sample, the anchor chooses 80 as the length of each column instead of 64. Denote the folding matrix as $\mathbf{F}$, and its element $F(n, s)$ is the n-th complex data in the s-th signal sample. To be consistent with the previous discussion, there are in total of S signal samples. Theoretically, if the signal comes from the WiFi attacker, the n-th row vector is the same with the $(n + 64)$-th row vector in the folding matrix, $i = 1, 2, \cdots, 16$. The cosine distance, which finds the angle between two vectors, is applied to measure the similarity between two row vectors. The value of the cosine distance is close to 1 if the two vectors are similar. To consider the similarity between the first 16 row vectors and the last 16 corresponding ones, we calculated the averaged cosine distance D_F as follows,

$$D_F = \frac{1}{16}\sum_{n=1}^{16} \frac{\sum_{s=1}^{S} F(n,s)F^*(n+64,s)}{\sqrt{\sum_{s=1}^{S} F^2(n,s)}\sqrt{\sum_{s=1}^{S} F^2(n+64,s)}} \tag{2.9}$$

In addition, we simulate the cosine distance of both the eavesdropped signal and the emulated signal as illustrated in Fig. 2.12a (Fig. 12a-12e are in next page), from which we see that the first 16 row vectors of the emulated signal and their related vectors in the end are almost the same. Different from this, the corresponding vectors of the ZigBee signal are negatively correlated.

2.7.2.2 Frequency Domain Features

The largest difference between the eavesdropped and the emulated signal is the constellation difference as shown in Fig.2.7a. Since the emulated signal is a WiFi signal, its constellation has a squared structure. However, the constellation of the eavesdropped signal does not have such a performance. Therefore, the constellation structure of the received signal is considered for detection.

The 64-QAM constellation has constant normalized fourth-order stimulants C_{40}, C_{41} and C_{42} [162]. Given received signal data $z(n,s)$, the anchor estimates them as follows,

$$\widetilde{C}_{40} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N} z^4(n,s) - 3\widetilde{C}_{20}^2$$

$$\widetilde{C}_{41} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N} z^3(n,s)z^*(n,s) - 3\widetilde{C}_{20}\widetilde{C}_{21}$$

$$\widetilde{C}_{42} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N} |z^4(n,s)| - |\widetilde{C}_{20}|^2 - 2\widetilde{C}_{21}^2 \tag{2.10}$$

In addition, the second-order moments $\widetilde{C}_{20}$ and $\widetilde{C}_{21}$ are estimated,

$$\widetilde{C}_{20} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N} z^2(n,s), \quad \widetilde{C}_{21} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N} |z(n,s)|^2.$$

Finally, the normalized second-order moments and fourth-order stimulants are given as,

$$\widehat{C}_{2q} = \widetilde{C}_{2q}/\widetilde{C}_{21}^2, q = 0, 1, \quad \widehat{C}_{4q} = \widetilde{C}_{4q}/\widetilde{C}_{21}^2, q = 0, 1, 2 \tag{2.11}$$

Their theoretical values are $C_{21} = 1$, $C_{20} = 0$, $C_{40} = C_{42} = -0.6190$ for the 64-QAM constellation.

By comparing the difference between the estimated second-order/fourth-order stimulants and their theoretical values, the anchor can roughly estimate the signal source. If the difference is small, the signal is from the attacker. Otherwise, it is from a ZigBee device. We deploy $(\widetilde{C}_{20} - C_{20})^2$, $(|\widehat{C}_{40}| - |C_{40}|)^2$ and $(\widetilde{C}_{42} - C_{42})^2$ to represent the above features. The reason for the absolute value of C_{40} is to avoid the effect brought by the signal phase rotation in transmission [162]. Their performance is shown in Fig. 2.12b, and Fig. 2.12c, respectively, where the difference between the second-order/fourth-order stimulants and their theoretical values in the emulated signal is smaller than that in the eavesdropped signal.

Besides the features related to stimulants, we consider the energy of the points in the constellations. By investigating Fig. 2.7a again, we see that the quantization process amplifies the FFT points with the smallest energy and shrinks the FFT points with the largest energy, resulting in their energy changes. We show the comparison of the maximum and minimum energy between the eavesdropped signal and the emulated signal in Fig.2.12d and Fig.2.12e, respectively, all of which validate our idea. Therefore, the maximum and minimum energy of the points after FFT operation from the received signal are chosen as the features.

2.7.3 Data Collection

In the training process, the anchor collects the data from both the WiFi attacker and the ZigBee transmitter based on the following process. As long as it is receiving the signal, the anchor first checks whether the state of the ZigBee receiver changes. If it is not changed, the anchor regards the signal as the emulated signal; otherwise, the anchor inquiries the ZigBee transmitter on whether it has transmitted signal. If it did not send any signal, the anchor likewise regards the signal as the emulated signal. If the ZigBee transmitter sends the signal, the anchor marks it as the signal source.

2.7.4 Signal Classification

The anchor deploys the binary logistic regression model [44,135] to distinguish whether the currently received signal is either from the WiFi attacker ('1') or the ZigBee transmitter ('0') by calculating the corresponding probability $P(Y=1|x)$ and $P(Y=0|x)$ after extracting the features,

$$P(Y=1|x) = \frac{exp(\hat{w}\cdot x + \hat{b})}{1 + exp(\hat{w}\cdot x + \hat{b})}, \quad P(Y=0|x) = \frac{1}{1 + exp(\hat{w}\cdot x + \hat{b})}$$

where x is a feature vector consisting of all the features described above. It denotes the feature extracted from the current received signal. If $P(Y=1|x)$ is larger than $P(Y=0|x)$, the anchor decides the signal is from the WiFi attacker; otherwise, the signal is from the ZigBee transmitter.

In particular, $\hat{w} \in \mathbf{R}^n$ and $\hat{b}$ are the estimated parameters learned from the training data set $T = \{(x_1, y_1), (x_2, y_2), \cdots, (x_T, y_T)\}$. They are obtained by maximizing logarithm likelihood $L(w, b)$,

$$L(w,b) = \sum\nolimits_{i=1}^{T} [y_i(w\cdot x_i) - \log(1 + exp(w\cdot x_i))]. \tag{2.12}$$

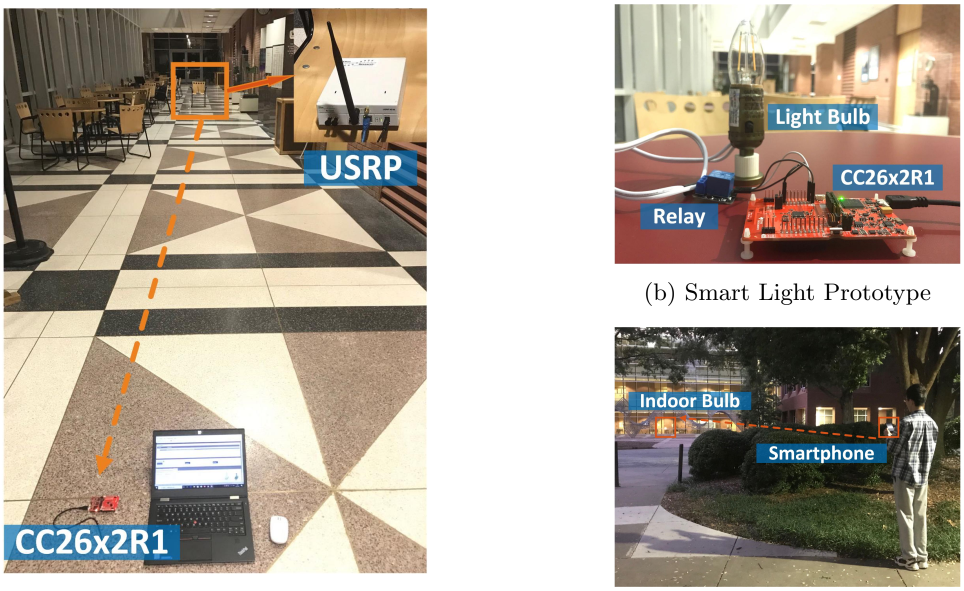
2.8 Performance Evaluation

2.8.1 Experiment Settings

We implement the emulation attack and its defense strategies on the USRP testbed and the Prototype testbed respectively to thoroughly evaluate their performance.

In the USRP testbed, the USRP-N210 is deployed as a WiFi attacker, attempting to control the ZigBee device CC26x2R Wireless MCU LaunchPad as shown in Fig. 2.13a. Both of them are centered at 2.405GHz. The distance between them is set to 5m, 10m, 15m, and 20m, respectively. USRP testbed gives freedom to choose parameters (e.g., transmission power, central frequency, payload length, etc.) for each step in the entire design, which can better simulate different environments.

As assumed in the motivation, we claim the signal emulation attack is severe due to the ubiquity of WiFi devices, where arbitrary devices with WiFi RF can launch the attack. Hence, we also implement experiments on a Prototype testbed, where the Nexus 5 smartphone (centered on 2.412GHz) attempts to control a smart light prototype (centered on 2.412GHz) in both LoS and NLoS as shown in Fig.2.13c. Nexus 5 whose radio chip is BCM4339 supports the widely used Nexmon framework which realizes modifications on the WiFi part [5] from a lower level. In Nexmon,



(a) USRP Testbed

(b) Smart Light Prototype

(c) Prototype Testbed

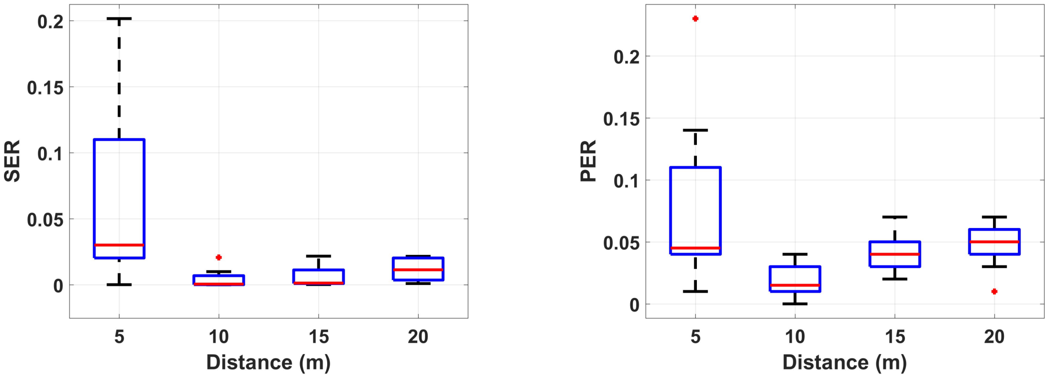
Figure 2.13: Experiment Settings and Prototype

we only change the WiFi packet length in order to fit the length of the ZigBee's "TURNING ON" command. To be specific, the length of a WiFi packet normally is around 1500 bytes. If the data is greater than that, it will be divided into several packets. Hence, we use Nexmon to ensure that a larger packet can be transmitted instead of being divided into several packets. In the smart light prototype in Fig.2.13b, the CC26x2R turns on the common light bulb by triggering a high level to the I/O output D100 as soon as detecting the "`TURNING ON`" command. Because the bulb needs a 110V voltage whereas the maximum supply voltage is 5V on CC26x2R, an extra relay is introduced playing the role of the switch. During the experiment, there are human activities such as walking, WiFi and Bluetooth signal transmission at the same time.

2.8.2 Signal Emulation Attack Performance

2.8.2.1 USRP Testbed

The attacker USRP sends 100 fixed-length emulated signals to ZigBee device CC26x2R 10 times given each distance. Symbol error rate (SER) denotes the number of symbols that are mistakenly decoded plus the number of symbols that are not received divided by the number of total symbols. Packet error rate (PER) represents the number of emulated signal packet being received with error over the number of total packets. The packet error happens if at least one symbol in it is detected with error. It means that the ZigBee device is not controlled by WiFi attacker. As can be seen in Fig.2.14, both the SER and PER are small even if the distance between them is long, e.g., 15m and 20m, which demonstrates that WiFi attacker can control the ZigBee device from a longer distance.



(a) SER

(b) PER

Figure 2.14: Signal Emulation Attack Performance

2.8.2.2 Prototype Testbed

The smartphone continuously sends “10000” as the “`TURNING ON`” commands from different locations. A USRP is deployed next to the bulb to help analyze the received signal. The result is illustrated in Table. 2.2. As the distance increases, both the SER and PER decrease. However, even the distance between the smartphone and the light bulb is beyond 20m, the PER is still very small. In other words, the smartphone can successfully control the ZigBee device from a longer distance, which demonstrates the effectiveness of our signal emulation attack.

Table 2.2: Prototype Signal Emulation Attack Performance

Distance	5m	10m	15m	20m	25m
SER	0.94%	3.26%	10.88%	15.93%	14.25%
PER	0.026%	0.082%	0.25%	0.36%	0.32%

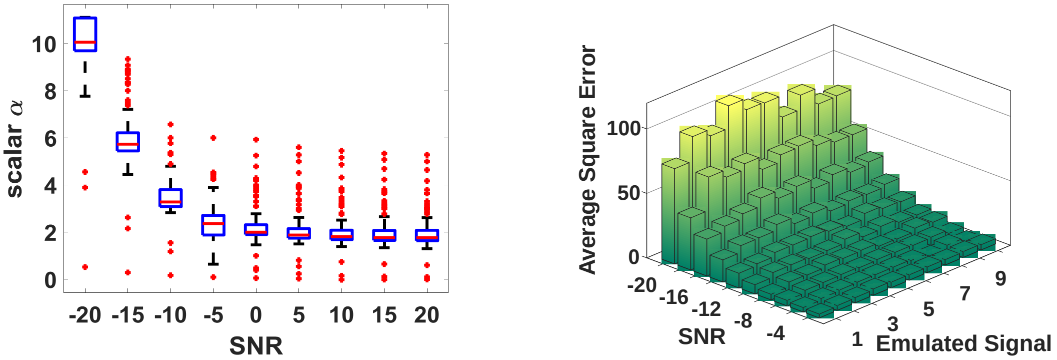
2.8.3 Passive Defense Strategy

To evaluate the passive defense strategy, we deploy another USRP in both testbeds to perform as the anchor, which transmits the AWGN with the ZigBee signal simultaneously during the eavesdropping phase. The signal-to-noise ratio is set from −20dB to 30dB. During the attacking process, we mainly consider the LoS case in USRP testbed and both the LoS and NLoS cases in Prototype testbed.

2.8.3.1 USRP Testbed

At the above locations, the WiFi attacker transmits 100 emulated noised signal 10 times. We show the effectiveness of the passive defense strategy from the following aspects.

Effect on the Quantization. We illustrate scalar α and the average square error corresponding with it in Fig.2.15a and Fig. 2.15b. When the SNR is under 0dB, a large scalar α is generated and results in a high average square error. This is because the noise with a high power brings a negative effect to the constellation quantization of the eavesdropped signal. Each FFT point of the eavesdropped signal is quantized to the 64-QAM point that is far away from itself.



(a) α Vs. SNR

(b) Average Square Error

Figure 2.15: Quantization Performance

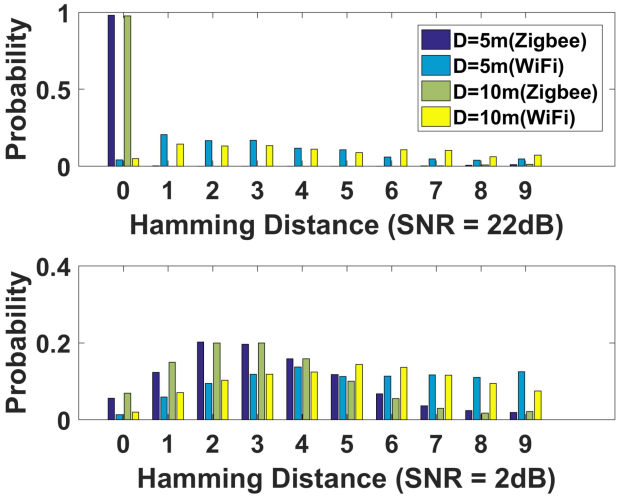
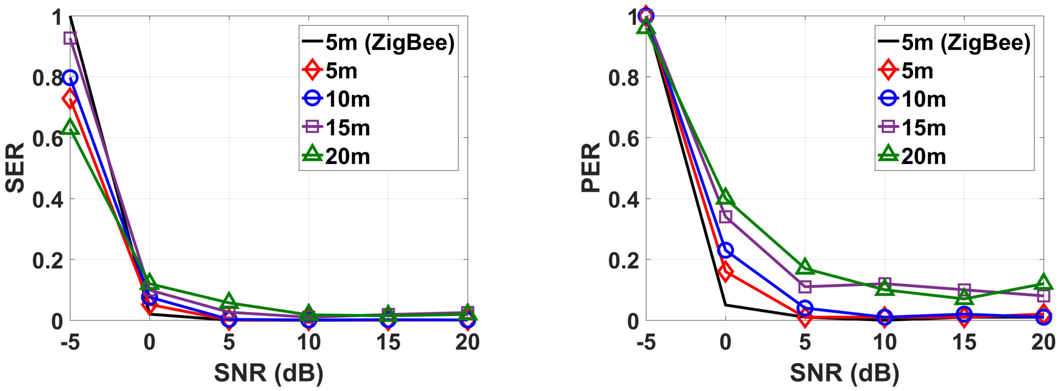


Figure 2.16: Hamming Distance Performance

Effect on Hamming Distance. In Fig.2.16, we illustrate the Hamming distance distribution for both the received ZigBee signal and emulated signal when the anchor generates the AWGN with the high SNR (22dB) and low SNR (2dB). The threshold of Hamming distance is set to 10. When the SNR is 22dB, most Hamming distance of ZigBee signal is around 0 and 1 whereas that of emulated signal is distributed among $2-9$. The ZigBee receiver decodes all the chips correctly. As the distance increases, the Hamming distance of the emulated signal becomes larger. Due to noise tolerance, the ZigBee receiver still decodes the emulated signal to correct symbols. However, when the SNR is 2dB, many chips are incorrectly decoded. The ZigBee receiver cannot recognize the emulated signal. WiFi attacker cannot control the ZigBee devices.

Effect on SER and PER. We evaluate the SER and PER from the receivers' perspective. As we can see in Fig.2.17, the SER and PER of both the ZigBee and emulated signal are very high when the SNR is below 0dB. The receiver decodes neither of them. When the SNR is above 5dB, the SER and PER of them approach to 0. The ZigBee receiver decodes both of them. When the SNR is between 0dB and 5dB, both SER and PER of ZigBee signal approach to 0 while the PER of the emulated signal is high, especially when the distance is larger. The receiver only decodes the ZigBee signal. The above analysis demonstrates that our passive defense strategy can effectively protect the ZigBee device from being attacked by WiFi attackers, particularly those who attempt to control the ZigBee device from a longer distance.



(a) CC26x2R SER

(b) CC26x2R PER

Figure 2.17: Effects on Error Rate

2.8.3.2 Prototype Testbed

The smartphone attempts to control the bulb from locations $L1$ to $L7$ in the building whose floor map is shown in Fig.2.18. Specifically, WiFi attacker locates at $L1$, $L2$ and $L4$ attacks the bulb in LoS. When the smartphone is at $L3$, $L5$, $L6$ or $L7$, it attempts to turn on the bulb without being found (NLOS). The SNR increases from -2dB to 30dB during the eavesdropping phase.

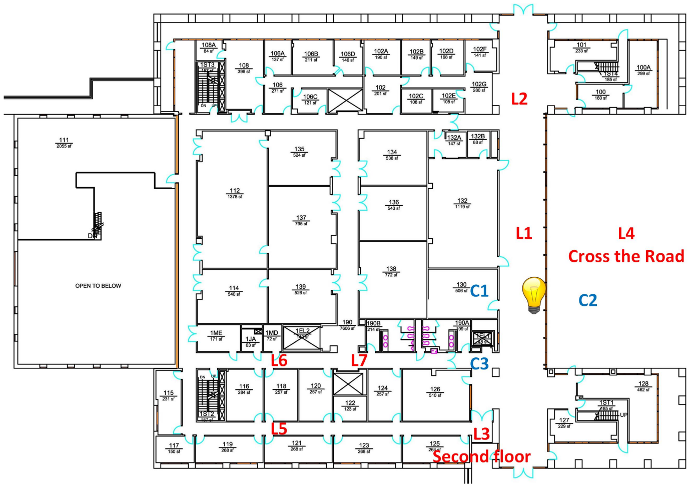


Figure 2.18: Building Map 1

The success rate of turning on the bulb is illustrated in Fig. 2.19. When the SNR is low, e.g., -2dB and 2dB, WiFi attacker only turns on the bulb in LoS case. As the SNR increases, indicating the added AWGN is decreasing, the success rate also increases. When it increases to

26dB and 30dB, the noise variance is so small that it cannot bring any trouble to the WiFi attacker. WiFi attacker turns on the prototype at all the marked locations, including many NLoS locations. The above observation also echos the effectiveness of our signal emulation attack in both LoS and NLoS case.

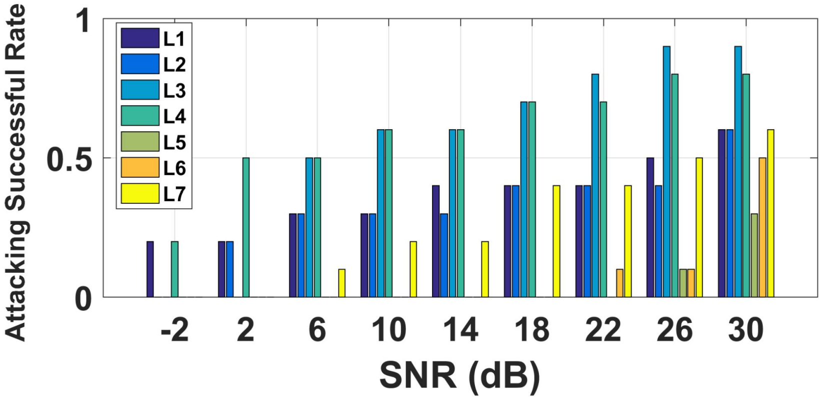
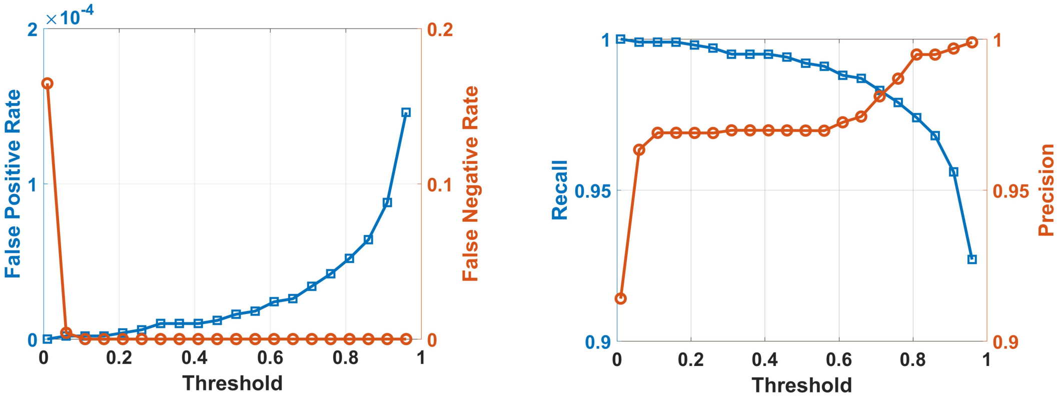


Figure 2.19: Defensive Performance on Prototype

2.8.4 Proactive Defense Strategy

In our proactive strategy, a USRP, as the anchor, is put next to ZigBee devices to help distinguish the signal source. Note that we consider the normalized maximum energy and minimized energy instead of extracting them directly.



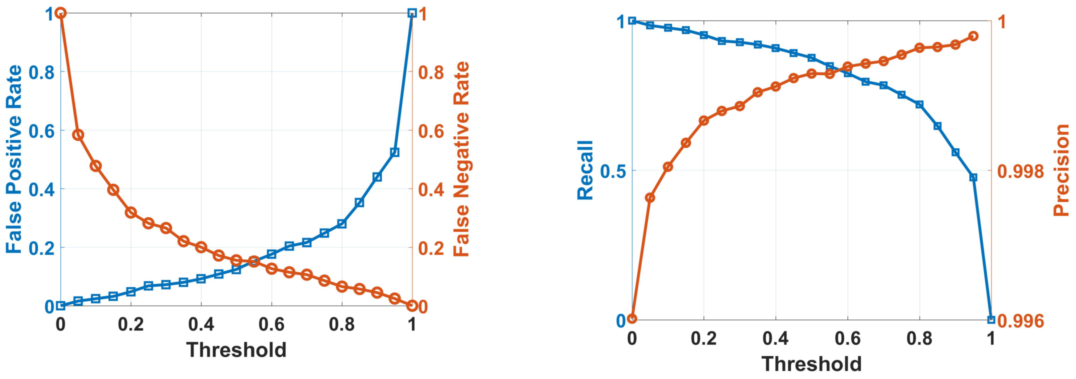
(a) ROC Curve

(b) Recall and Precision

Figure 2.20: Detection Performance in USRP Testbed

2.8.4.1 USRP Testbed

We randomly generate 1000 ZigBee signal, which are eavesdropped by the WiFi attacker. Then, it generates the corresponding emulated signal. The original ZigBee signal and the emulated ones are sent to the ZigBee device respectively. Half of the received emulated signal is put into the training set and the others are to be classified. The operation of the ZigBee signal is the same. The experimental results are shown as a Receiver Operating Characteristic (ROC) curve in Fig.2.20a. The false positive rate represents that the emulated signal is mistakenly considered to be from the ZigBee transmitter whereas the false negative rate denotes that the ZigBee signal is regarded as from the WiFi attacker. In the LoS case, both the false positive rate and false negative rate approach to 0 due to the existence of the powerful anchor. In addition, we demonstrate the recall and precision performance in Fig.2.20b. The recall value represents the capability of identifying the WiFi attacker whereas the precision value denotes the capability of recognizing the ZigBee transmitter from the received signal. When the detection threshold is set to around 0.7, both the recall and precision value are near to 1, in the sense that the anchor effectively identifies both the WiFi attacker and ZigBee transmitter.



(a) ROC Curve

(b) Recall and Precision

Figure 2.21: Detection Performance in Prototype Testbed

2.8.4.2 Prototype Testbed

The WiFi attacker attempts to control the bulb from the LoS locations $L1$ and $L2$ together with NLoS locations $C1$, $C2$ and $C3$. The USRP receives 500 emulated signals and ZigBee original signal, respectively. Half of both received signals are put into the training set and the others are going to be classified. As we can see from Fig.2.21, when the detection threshold is set to 0.5, both false positive and negative rates approach to 0.2 while the precision is near to 0. The anchor can effectively identify the received signal source.

2.8.5 Results from Field Experiments

2.8.5.1 Experiment Settings

To further verify the effectiveness of emulation attack and defense strategies, we conduct field experiments in a larger space, where the end-to-end distance is more than two times of the previous building. Due to the complicated floor plan as given in Fig. 2.22, we can carry out more experiments in the extreme NLoS case.

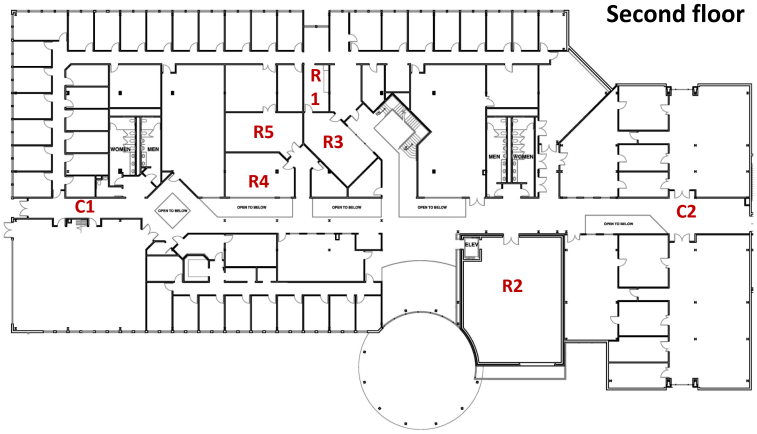


Figure 2.22: Building Map 2 – Second Floor

Specifically, we test the results on emulation attack to the commodity Sylvania ZigBee LED. The launchpad CC26x2R is always placed close to LED to show the symbol/packet level performance. A USRP is placed at location C1 on the second floor. For the LoS case, we move LED from USRP location to the end of the hallway $C2$. The distance from $C1$ to $C2$ is 80m. For the NLoS, we place the LED in room R1, R2, R3, and the end of the hallway on the first floor C2$'$. The distance between R2 and C1 is around 60m. The emulation signal has to pass through other rooms, e.g., R3, R4, R5, before being received at R1. The USRP sends the "`TURNING ON`" command that includes 49 ZigBee symbols 500 times to turn on the LED. As an attacker, the USRP sends the emulated command with the gain value 20dB, which indicates the amplification factor in hardware before sending the signal out [6]. As a ZigBee transmitter, the USRP transmits the received ZigBee command with the gain value 12dB. Since the maximum power of WiFi transmission on the smartphone (e.g., Samsung Galaxy series) is 13dBm whereas that on ZigBee devices is 5dBm, gain value settings are to ensure the maximum power ratio between WiFi and ZigBee.

2.8.5.2 Signal Emulation Attack Performance

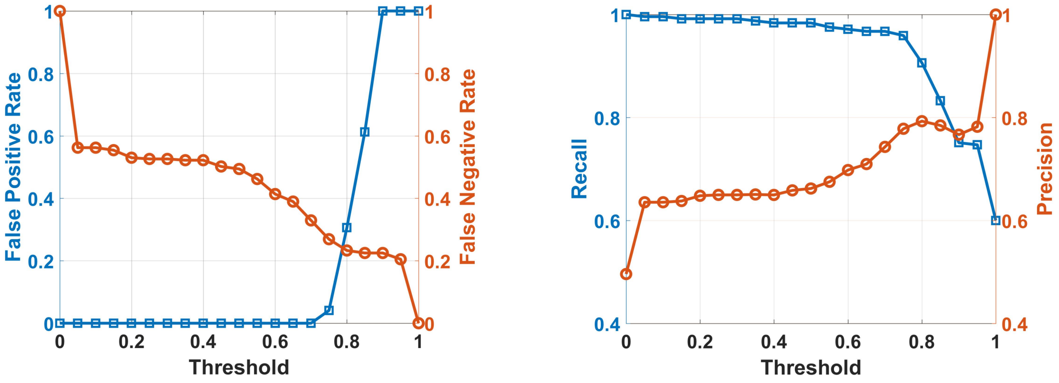
In the field experiment, the LED is turned on after receiving either emulated or ZigBee "TURNING ON" command in LoS case. In NLoS case, the LED is on for the above four locations only when the USRP sends emulated signals. The signal performance on CC26x2R gives similar results. As in Table.2.3, when the USRP sends the emulated command, the signals received by CC26x2R have a lower SER. The received packet is supposed to be incorrect if one of the symbols is not correctly received. Hence, the PER is relatively high. However, it is much smaller than that when the USRP sends the ZigBee. Even worse, being placed at R2, the CC26xR even cannot receive the ZigBee signal. The above results validate our intuition that ZigBee devices are more easily controlled by WiFi devices from NLoS locations.

Table 2.3: Symbol/Packet Level Performance

Location	C2	C2′	R1	R2	R3
SER (WiFi)	16.09%	9.15%	34.25%	23.09%	11.78%
PER (WiFi)	44.60%	44.30%	62.70%	57.60%	36.50%
SER (ZigBee)	16.07%	6.06%	53.81%	N/A	11.12%
PER (ZigBee)	44.30%	19.10%	83.20%	N/A	32.90%

2.8.5.3 Proactive Defense Strategy

To distinguish the signal source, a USRP is deployed next to the Smart LED. Similarly, it receives 500 emulated signals and original ZigBee signals (including both LoS and NLoS), respectively. The result is shown in Fig.2.23. When the detection threshold is lower than 0.8, the anchor would not ignore the emulated signal, but it is possible that the anchor mistakenly regards the ZigBee source as WiFi attacker. When the detection threshold is set above 0.8, the distinguishing result is reversed. When the threshold is set to around 0.8, the anchor gets a balance between the false positive rate and the false negative rate. Shown in Fig.2.23b, the recall and precision value approaches to 0.8 simultaneously when the threshold is set between 0.8 and 0.9, in the sense that the anchor can effectively identify both the ZigBee receiver and WiFi attacker.



(a) ROC Curve

(b) Recall and Precision

Figure 2.23: Detection Performance in Field Experiments

2.9 Chapter Summary

In this chapter, we identify a new physical-layer based attack, cross-technology signal emulation attack, where the WiFi attacker controls the ZigBee device by emulating the eavesdropped ZigBee signal. To combat this attack, we introduce an anchor to safeguard the ZigBee communication. In the passive defense strategy, the anchor transmits the AWGN to prevent the WiFi attacker from successfully emulating the perfect ZigBee signal. Whereas in the proactive defense strategy, the anchor receives the signal and identifies the signal source in real time. We implement our design on real-world testbeds and the commodity smart LED together with our self-designed prototype. Extensive experiments are performed, demonstrating both the feasibility of signal emulation attack and the effectiveness of the defense strategies.

Chapter 3

Incentivizing Relay Participation for Securing Internet of Things Communication

3.1 Chapter Overview

Internet of Things (IoT) is expected to enable ubiquitous connectivity and information exchange among billions of everyday necessities. Although the use of such smart connected objects has become a reality in our daily activities, serious concerns are raised as follows. On the one hand, over 60% of IoT applications are required to achieve low power consumption, long battery life, high data rate, and wide coverage simultaneously [114]. Although the newly proposed NB-IoT and LoRa protocols would be able to address some of the above requirements, the low data rate (approx. 50-250 kbps) becomes the main bottleneck to hinder their widely deployment in many applications. For some existing wireless technologies, such as Bluetooth Low Energy (BLE) and 802.15.4/ZigBee, the low power feature limits the communication range, and thus they are unable to be deployed in industrial applications, such as environmental sensing and machinery weakness monitoring. On the other hand, the disclosure of sensitive information collected by many IoT applications is unacceptable, such as machinery data, patients' health data, financial files, etc. Unfortunately, data communication is *de facto* vulnerable to the eavesdropping attack due to the heterogeneous wireless environment in the IoT system [179, 182].

Cooperative communication is a perfect fit to tackle the above challenges with its advantages on wide coverage, energy efficiency, and high interference mitigation capability. While being thoroughly investigated in the Wireless Sensor Network (WSN), it could play a more significant role in the IoT system on enhancing the reliability and security. Specifically, the cooperative communication will introduce inherent randomness of wireless channels, which could prevent eavesdroppers from intercepting the transmitted message. However, the major challenge that deters the deployment of cooperative communication on improving the security level is the limited battery life of wireless sensors. In this chapter, we propose a novel cooperative IoT system consisting of multiple relay IoT nodes to enhance the reliability and security, where the shortage of device energy is conquered by leveraging energy harvesting techniques on IoT devices. In particular, many Commercial off-the-shelf (COTS) IoT nodes are able to collect energy from renewable resources in ambient environments, such as vibration, solar and, wind energy [100]. In our proposed system, the newly introduced relay IoT node mainly plays two roles: 1) forwarding the data from each source node to the destination node to ensure the reliable communication; 2) preventing data information from being intercepted by the eavesdroppers to secure the IoT communication. Although the proposed paradigm enlightens a new methodology for reliable IoT communication, how to incentivize relay IoT nodes to help the data forwarding becomes a challenging issue, because each relay IoT node has to consume its own harvested energy for relaying. Therefore, we propose a game-theoretical solution to motivate the participation of relay IoT nodes with joint consideration on both channel state information (CSI) and energy consumption. We highlight our contributions as follows,

- We propose a novel cooperative IoT system to ensure the reliability and security of data communication specifically for IoT applications.
- Leveraging energy harvesting techniques, relay IoT nodes can help improve the secrecy capacity by participating in the cooperative communication continuously.
- To demonstrate the practicality, two two-stage Stackelberg games under both the wiretap-link CSI unknown and known cases are formulated between the source and relay IoT nodes.
- Simulations and the experiments using real-world dataset show the feasibility of the proposed scheme.

The rest of this chapter is organized as follows. We briefly review related work in Section 3.2. Detailed description of the system model and the Stackelberg game formulation are given in Section 3.3. In Section 3.4, we introduce the proposed Stackelberg game in the wiretap-link CSI unknown case in detail. An extension to the wiretap link CSI known case, which is more complex, is discussed in Section 3.5. In Section 3.6, complexity is analyzed and performance evaluation is demonstrated for both cases, followed with a conclusion in Section 3.7.

3.2 Related Work

3.2.1 Cooperative Communication in IoT

Cooperative communication aims at improving energy efficiency, overall throughput, power control, and resource allocation in wireless networks [81, 160]. It has been widely deployed in many IoT applications. Omar *et al.* in [139] use cooperative communications in a smart metering system to relay data in a multi-hop fashion to far-off aggregation points. The experimental results verify cooperative communication can increase network range, prolong network lifetime, and reduce energy consumption. It is also deployed in cluster-based industrial IoT network to optimize both energy efficiency and QoS in [159, 160]. In the context of large-scale IoT, Bader *et al.* in [18] use blind cooperative transmission in conjunction with multi-hop networking to minimize underlying protocol overhead and therefore allows for scalability. However, securing cooperative IoT system receives less attention.

3.2.2 Physical-layer Security

Physical-layer security mechanism exploits the property of the wireless channel for secure communication [53,177]. It has shown great potential in providing information-theoretically unbreakable secrecy [182]. Many transmission strategies, such as cooperative transmission [201], artificial noise [124], and secure beamforming [120], are proposed to enhance physical layer security. Among all those strategies, cooperative communication is of great significance to the IoT communication due to its low power and wide coverage requirements. A comprehensive overview of physical layer security in wireless cooperative relay networks is provided in [152]. The performance of secure transmission is improved by employing multiple cooperative relays in [201, 202]. Specifically, Xu *et* *al.* in [182] prove that the proper use of relay transmission enhances the secrecy throughput and extends the secure coverage range for IoT communications. However, without proper benefits, relay IoT nodes will not participate in the cooperative communication.

3.2.3 Stackelberg Game

Stackelberg game [48] models and analyzes the interactions among independent decision makers, which has been applied in a broad field of wireless communications and networks [90]. Particularly, A single-leader single-follower Stackelberg game is proposed in [52] for physical layer security and energy efficiency enhancement. However, it does not support multiple relay nodes case. A single-leader multiple-followers Stackelberg game is deployed to coordinate multiple relays for physical-layer security improvement in [53], where the fairness among relay nodes is considered. However, due to the different CSIs on the wiretap link between the eavesdropper and each relay node, each relay node contributes differently to physical layer security. The EWS-based algorithm in [53] is also not a proper method for physical-layer security enhancement.

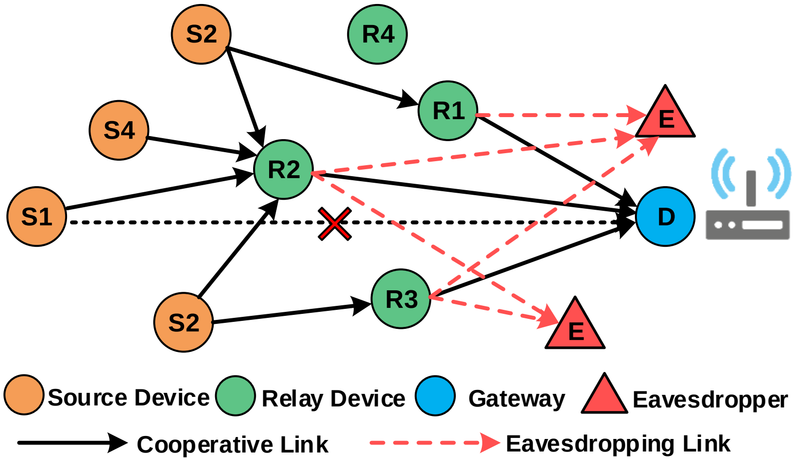


Figure 3.1: System Model

3.3 System Overview

3.3.1 System Model

An industrial IoT application shown in Fig.3.1 describes our system model. Assume K energy constrained source nodes $\mathcal{S} = \{S_1, S_2, \cdots, S_K\}$ to transmit data to a distant destination node D (e.g., IoT gateway) through orthogonal channels in the presence of an eavesdropper E near the destination node D. Nodes D and E are out of the transmission range of the source nodes. To enable data transmission and prevent them from being intercepted, an amplified-and-forward (AF) cooperative protocol is employed with the help of N mobile relay IoT nodes $\mathcal{R} = \{R_1, R_2, \cdots, R_N\}$. Each R_i can collect extra energy from the ambient environment when it does not work for $\mathcal{S}$. Besides, all the nodes including the eavesdropper are assumed to know the existence of the relay nodes and the cooperative protocol, which is a common assumption in the physical-layer security protocols [52]. Since the eavesdropper cannot receive data information from $\mathcal{S}$, it monitors the data transmission from R_i to D and attempts to interpret the data.

3.3.2 Cooperative IoT System

We consider a flat Rayleigh fading channel in the proposed cooperative IoT system. The fading amplitude between S_k and R_i is denoted $h_{S_k i}$, whereas that between R_i and D is represented by h_{id}. Meanwhile, we denote the fading amplitude between R_i and E as h_{ie}. Without loss of generality, n_{ki}, n_{id} and n_{ie} are the corresponding additive white Gaussian noise (AWGN) with the same distribution $\mathcal{CN}(0, \sigma^2)$, where σ^2 is one-sided power spectral density. Similar to [53], we assume that source nodes can get global CSI of the main links, and the local information can be obtained by the relay nodes. Generally, data transmission is divided into two steps:

Step 1: S_k broadcasts its encoded signal s_k ($E\left(|s_k|^2\right) = 1$) with the power P_{S_k}. The signal received at R_i is,

$$y_{S_k i} = \sqrt{P_{S_k}} h_{S_k i} s_k + n_{ki}. \tag{3.1}$$

Step 2: R_i normalizes and amplifies the received signal $y_{S_k i}$ with the power P_{iS_k} and sends to D. Then, D receives,

$$y_{S_k id} = \sqrt{P_{iS_k}} h_{id} \frac{y_{S_k i}}{|y_{S_k i}|} + n_{id}, \tag{3.2}$$

where the power P_{iS_k} consists of two parts: the power provided by the relay IoT node itself and harvested from the ambient environments. Similarly, S_k' signal forwarded by R_i can also be received by E, where

$$y_{ie} = \sqrt{P_{iS_k}} h_{ie} \frac{y_{S_k i}}{|y_{S_k i}|} + n_{ie}. \tag{3.3}$$

Substitute (3.1) into (3.2), the signal-to-noise radio (SNR) $\Gamma_{S_k id}$ on the main link (S_k-R_i-D) becomes,

$$\Gamma_{S_k id}(P_{iS_k}) = \frac{P_{S_k} P_{iS_k} \gamma_{S_k i} \gamma_{id}}{1 + P_{S_k} \gamma_{S_k i} + P_{iS_k} \gamma_{id}}, \tag{3.4}$$

where $\gamma_{S_k i} = |h_{S_k i}|^2/\sigma^2$ and $\gamma_{id} = |h_{id}|^2/\sigma^2$.

Similarly, based on (3.1) and (3.3), the SNR $\Gamma_{S_k ie}$ on the wiretap link (S_k-R_i-E) related to the relay node R_i is,

$$\Gamma_{S_k ie}(P_{iS_k}) = \frac{P_{S_k} P_{iS_k} \gamma_{S_k i} \gamma_{ie}}{1 + P_{S_k} \gamma_{S_k i} + P_{iS_k} \gamma_{ie}}, \tag{3.5}$$

in which $\gamma_{ie} = |h_{ie}|^2/\sigma^2$, $i = 1, 2, \cdots, N$.

To maximize the receiving SNR, we deploy Maximum Radio Combination (MRC) at both D and E, representing the theoretically optimal combiner over fading channels [63]. As a result, the corresponding channel capacities on the main link and wiretap link are,

$$C_{d_k}(\mathbf{P}_{\mathbf{r_k}}) = W \log_2(1 + \sum\nolimits_{i=1}^{N} \Gamma_{S_k id}) \tag{3.6}$$

and

$$C_{e_k}(\mathbf{P}_{\mathbf{r_k}}) = W \log_2(1 + \sum\nolimits_{i=1}^{N} \Gamma_{S_k ie}) \tag{3.7}$$

respectively, where $\mathbf{P}_{\mathbf{r_k}} = \{P_{1S_k}, P_{2S_k}, \cdots, P_{NS_k}\}$ denotes the power each relay node consumes to forward the signal.

DEFINITION 1. *(Secrecy Capacity) The secrecy capacity [76] related to S_k, defined as the difference between the capacity of the main link (S_k-$\mathcal{R}$-D) and that of the wiretap link (S_k-$\mathcal{R}$-E), is written as,*

$$C_{sec,k}(\mathbf{P}_{\mathbf{r_k}}) = \max\{C_d(\mathbf{P}_{\mathbf{r_k}}) - C_e(\mathbf{P}_{\mathbf{r_k}}), 0\} \tag{3.8}$$

It represents the maximum transmission rate of the main link that the eavesdropper is unable to decode any information.

Therefore, in order to enhance the IoT system security, it is necessary to maximize the secrecy capacity of S_k with the help of multiple relay IoT nodes given the source node power P_{S_k} and the CSI of both the main link and the wiretap link,

$$\max_{\mathbf{P_{r_k}}} C_{sec,k}(\mathbf{P_{r_k}}) \tag{3.9}$$

$$s.t. \quad 0 \leq \sum_{k=1}^{K} P_{iS_k} \leq P_{i,max}, i = 1, 2, \cdots, N. \tag{3.10}$$

where $P_{i,max}$ is the maximized power the relay node R_i can use to forward the data.

3.3.3 Stackelberg Game Formulation

To incentivize the relay participation, we propose a game-theoretical approach to choosing proper relay IoT nodes for data forwarding. In contrast to treating source nodes equally from relay IoT nodes' perspectives, S_i intends to select the most beneficial R_i because R_i has different performance on enhancing the secrecy capacity due to the different CSIs and available power. To maximize the benefits of both the source nodes and the relay nodes, we formulate their interactions as a two-stage multi-buyer multi-seller Stackelberg game. Particularly, we discuss the Stackelberg game under the wiretap-link CSI unknown and know cases, named as the CUS game and the CKS game, respectively.

3.3.3.1 CSI-Unknown Model (CUS Game)

Assuming the eavesdropper only listens without transmitting, the CSI on the wiretap link $h_ie, i = 1, 2, \cdots, N$, is unknown. The source node S_k cannot select qualified relay IoT nodes and purchases power to enhance the secrecy performance. Motivated by [53], we replace the capacity on the wiretap link with its supremum $\overline{C_e^{sup}}$, which can be obtained based on a period of monitoring. We define the multi-buyers multi-sellers Stackelberg game as,

DEFINITION 2. *(CUS Game)*

- ***Stage I (Unit Pricing)*** *Each relay IoT node $R_i \in \mathcal{R}$ sells a unit price q_i^* of its power to maximize its benefit U_i,*

$$q_i^* = \arg\max \sum_{i \in \mathcal{N}} (q_i - c_i) P_{iS_k}, i = 1, 2, \cdots, N \tag{3.11}$$

- ***Stage II (Power Purchased)*** *Each $S_k \in \mathcal{S}$ buys an amount of power P_{iS_k} from R_i, $R_i \in \mathcal{N}$ to maximize its utility given the power and secrecy capacity constraints.*

$$\mathbf{P_{r_k}}^* = \arg\max U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q}), k = 1, 2, \cdots, K \tag{3.12}$$

In the CUS game, each R_i sells the power to $\mathcal{S}$ with the unit price q_i to maximize its utility,

$$U_i(P_{iS_1}, P_{iS_2}, \cdots, P_{iS_K}, q_i) = (q_i - c_i) \sum\nolimits_{k=1}^{K} P_{iS_k} \tag{3.13}$$

with its current power constraint (3.10). c_i denotes its own cost. The unit price of each relay node composes a price vector $\mathbf{q} = \{q_1, q_2, \cdots, q_N\}$. As for each S_k, when $R_i, i \in \mathcal{N}$ helps forward the data, it gets the utility,

$$U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q}) = \alpha(C_{d_k}(\mathbf{P_{r_k}}) - \overline{C_e^{sup}}) - \sum\nolimits_{i=1}^{N} q_i P_{iS_k} \tag{3.14}$$

where α denotes the gain per unit of secrecy capacity.

3.3.3.2 CSI-known Model (CKS Game)

In an IoT system, a receiving node can play as a legitimate destination node for some data transmission while still performing as an eavesdropper for others. Therefore, the CSI on the wiretap link can be obtained, and we extend the above CUS game to the CKS game. At this time, the utility of each source node becomes,

$$U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q}) = \alpha C_{sec,k}(\mathbf{P_{r_k}}) - \sum\nolimits_{i=1}^{N} q_i P_{iS_k} \tag{3.15}$$

In addition, a secrecy capacity constraint is added to ensure data transmission security,

$$C_{sec,k}(\mathbf{P_{r_k}}) > C_0 \tag{3.16}$$

The Stackelberg game formulation and utility with power constraint for each relay node keeps unchanged.

3.4 Utility Maximization in CUS Game

In the proposed CUS game, we deploy the backward induction [58] to find the optimal power strategies that no source node deviates based on the unit price each relay node charges. For each relay node in Stage I, we are interested in the pricing strategy that maximizes its benefit given the source nodes' optimal strategies of in Stage II, which yields the concept of power equilibrium,

DEFINITION 3. *(Power Equilibrium) For any price p_i given in Stage I, the power equilibrium (PE) in Stage II is a strategy profile $P^*_{iS_k}$ such that S_k cannot improve its utility by unilaterally changing the power purchased from R_i, i.e.,*

$$P^*_{iS_k} = \arg\max_{\mathbf{P_{r_k}}} U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q}), i = 1, 2, \cdots, N \tag{3.17}$$

3.4.1 Stage II: Power Equilibrium

Since source nodes transmit the data on the orthogonal channels and are equally treated by each relay node, we consider the power equilibrium for an S_k. Based on (3.4), (3.6) and (3.14), its utility becomes,

$$\begin{aligned} U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q}) = \alpha W \log_2(1 + \textstyle\sum_{i=1}^{N} \frac{P_{S_k} P_{iS_k} \gamma_{S_k i} \gamma_{id}}{1+P_{S_k}\gamma_{S_k i} + P_{iS_k}\gamma_{id}}) \\ -\overline{C_e^{sup}} - \textstyle\sum_{i=1}^{N} q_i P_{iS_k} \\ = \alpha W \log_2(1 + \sum_{i=1}^{N} \tfrac{A_{ki} P_{iS_k}}{B_{ki} + P_{iS_k}}) - \overline{C_e^{sup}} - \sum_{i=1}^{N} q_i P_{iS_k} \end{aligned} \tag{3.18}$$

where $A_{ki} = P_{S_k}\gamma_{S_k i}$ and $B_{ki} = 1 + P_{S_k}\gamma_{S_k i}/\gamma_{id}$. The constant $\overline{C_e^{sup}}$ transforms the utility maximization problem on the secrecy capacity to that on the channel capacity on the main link. Such transformation is an approximation to the original problem. Only when the supreme secrecy capacity equals to the channel capacity on the wiretap link are the two utility maximization problems equal [90].

Using the utility function (3.18), by setting the derivative $\partial U_{S_k}(\mathbf{P_{r_k}}, \mathbf{q})/P_{iS_k} = 0$ as the first-order condition and solving the equation set, we get the optimal power strategies,

$$P^*_{iS_k} = \sqrt{\frac{A_{ki}B_{ki}}{q_i}\frac{Y_k + \sqrt{Y_k^2 + 4X_k\frac{\alpha W}{In2}}}{2X_k}} - B_{ki} \tag{3.19}$$

where $X_k = 1 + \sum_{i=1}^{N} A_{ki}$ and $Y_k = \sum_{i=1}^{N} \sqrt{q_i A_{ki} B_{ki}}$. Meanwhile, since the utility function (3.18) is joint concave in $\{P_{iS_k}\}_1^N$, $P_{iS_k}^*$ is the power equilibrium purchased from R_i given its unit price p_i.

3.4.2 Stage I: Optimal Pricing

Different to the scenario in [58], CUS game is played between multiple source nodes and relay nodes. From (3.13), we see that the utility of each relay IoT node depends on the power sold to all the source nodes. To obtain the optimal price of R_i, we set the derivative $\partial U_{S_k i}/\partial q_i = 0$ and obtain,

$$q_i = I_i(\mathbf{q}) = c_i - \frac{\sum_{k=1}^{K} P_{iS_k}^*}{\partial \sum_{k=1}^{K} P_{iS_k}^* / \partial q_i} \tag{3.20}$$

Denote $\mathbf{I}(\mathbf{q}) = \{I_1(\mathbf{q}), I_2(\mathbf{q}), \cdots, I_N(\mathbf{q})\}$. We have,

Theorem 1. *The optimal price is obtained by continuously updating the price of each relay node as follows,*

$$\mathbf{q} = \mathbf{I}(\mathbf{q}). \tag{3.21}$$

Proof: To prove the convergence, we show that $\mathbf{I}(\mathbf{q})$ is a standard function [186], which means that $\mathbf{I}(\mathbf{q})$ needs to satisfy positivity, scalability, and monotonicity.

Positivity: $\mathbf{I}(\mathbf{q}) > 0$. From (3.19), for each relay node,

$$\frac{\partial \sum_{k=1}^{K} P_{iS_k}^*}{\partial q_i} = -\frac{1}{2q_i} \sum_{k=1}^{K} \left(\sqrt{\frac{A_{ki} B_{ki}}{q_i} \frac{Y_k + \sqrt{Y_k^2 + 4X_k \frac{\alpha W}{In2}}}{2X_k}} \right) \times \left(1 - \frac{\sqrt{q_i A_{ki} B_{ki}}}{\sqrt{Y_k^2 + 4X_k \frac{\alpha W}{In2}}} \right) < 0$$

Hence, $I_i(\mathbf{q})$ in (3.20) is positive under the condition that both c_i and $\sum_{k=1}^{K} P_{iS_k}^*$ are larger than 0.

Scalability: We show that for all $\vartheta > 1$, $\vartheta \mathbf{I}(\mathbf{q}) > \mathbf{I}(\vartheta \mathbf{q})$.

$$\vartheta \mathbf{I}(\mathbf{q}) - \mathbf{I}(\vartheta \mathbf{q}) = (\vartheta - 1)c_i + \vartheta \left(\frac{\sum_{k=1}^{K} P_{iS_k}^*(\vartheta \mathbf{q})}{\partial \sum_{k=1}^{K} P_{iS_k}^*(\vartheta \mathbf{q})/\partial q_i} - \frac{\sum_{k=1}^{K} P_{iS_k}^*(\mathbf{q})}{\partial \sum_{k=1}^{K} P_{iS_k}^*(\mathbf{q})/\partial q_i} \right) > 0 \tag{3.22}$$

where the key is to see whether the second part in (3.22) is positive. Denote $Z_i(W) = \frac{\sum_{k=1}^{K} P_{iS_k}^*(\mathbf{q})}{\partial \sum_{k=1}^{K} P_{iS_k}^*(\mathbf{q})/\partial q_i}$. Based on (3.19),

$$P_{iS_k}^*(\vartheta \mathbf{q}) = \sqrt{\frac{A_{ki} B_{ki}}{\vartheta q_i} \frac{\sqrt{\vartheta} Y_k + \sqrt{\vartheta Y_k^2 + 4X_k \frac{\alpha W}{In2}}}{2X_k}} - B_{ki} = \sqrt{\frac{A_{ki} B_{ki}}{q_i} \frac{Y_k + \sqrt{Y_k^2 + 4X_k \frac{\alpha W}{\vartheta In2}}}{2X_k}} - B_{ki} \tag{3.23}$$

Instead of $\mathbf{q}$, ϑ puts an effect to W in (3.23). Hence,

$$\frac{\sum_{k=1}^{K} P_{iS_k}^{*}(\vartheta\mathbf{q})}{\partial \sum_{k=1}^{K} P_{iS_k}^{*}(\vartheta\mathbf{q})/\partial q_i} = Z_i(W/\vartheta) \tag{3.24}$$

The scalability problem becomes to see whether $Z_i(W/\vartheta) - Z_i(W)$ is positive, where $Z_i(W)$ equals to

$$\frac{-2q_i \sum_{k=1}^{K} \left(\sqrt{\frac{A_{ki}B_{ki}}{q_i}} \frac{Y_k + \sqrt{Y_k^2 + 4X_k \frac{\alpha W}{In2}}}{2X_k} - B_{ki} \right)}{\sum_{k=1}^{K} \left(1 - \frac{\sqrt{q_i A_{ki} B_{ki}}}{\sqrt{Y_k^2 + 4X_k \frac{\alpha W}{In2}}} \right) \left(\sqrt{\frac{A_{ki}B_{ki}}{q_i}} \frac{Y_k + \sqrt{Y_k^2 + 4X_k \frac{\alpha W}{In2}}}{2X_k} \right)} \tag{3.25}$$

Through deduction, we conclude that $Z_i(W)$ in (3.25) is monotonic decreasing. $Z_i(W/\vartheta) > Z_i(W/\vartheta)$ for $i = 1, 2, \cdots, N$, the scalability of $\mathbf{I}(\mathbf{q})$ is proved.

Monotonicity: If $\mathbf{q} \geq \mathbf{q}^{'}, \mathbf{I}(\mathbf{q}) \geq \mathbf{I}(\mathbf{q}^{'})$. $\mathbf{q} \geq \mathbf{q}^{'}$ denotes that there at least exists an R_i such that $q_i \geq q_i^{'}$. For any $j \neq i$,

$$I_i(q_i, \mathbf{q_{-i}}) \geq I_i(q_i^{'}, \mathbf{q_{-i}}) \tag{3.26}$$

and

$$I_j(q_i, \mathbf{q_{-i}}) \geq I_j(q_i^{'}, \mathbf{q_{-i}}) \tag{3.27}$$

where $\mathbf{q_{-i}}$ denotes the price of other relay nodes except R_i. From (3.26) and (3.27), we see that the problem becomes to show that $\partial I_i(\mathbf{q})/\partial q_i \geq 0$ and $\partial I_j(\mathbf{q})/\partial q_i \geq 0$. We conclude that above inequalities are satisfied after deduction process. Therefore, monotonicity property is proved. □

Based on the above discussion, we describe the utility maximization process for both the source and relay nodes in Algorithm 2, which is convergent according to Theorem 1.

```
Algorithm 2: Utility Maximization in CUS Game
Input: convergence threshold $\xi$
Output: $\mathbf{P^*_{r_k}}, \mathbf{q}^*$
Set the initial price $q_{i(0)} = c_i, i = 1, 2, \cdots, N$;
Set the initial power $P_{iS_k} = 0, i = 1, 2, \cdots, N, k = 1, 2, \cdots, K$;
while $\mathbf{1}^T |\mathbf{q}_{(n+1)} - \mathbf{q}_{(n)}| \leq \xi$ do
    Compute $P_{iS_k}$ based on (3.19) for $k = 1, 2, \cdots, K, i = 1, 2, \cdots, N$;
    Update $\mathbf{q_{(n+1)}}$ according to (3.21);
end
Compute $P_{iS_k}$ given $\mathbf{q}_{(n)}$;
return $\mathbf{q}^* = \mathbf{q}_{(n)}$, $\mathbf{P^*_{r_k}} = \mathbf{P_{r_k}}$;
```

3.5 Utility Maximization in CKS GAME

In this section, we consider the CKS game. According to (3.8), instead of being a constant, the capacity of the wiretap link is affected by the power P_{iS_k}. Therefore, the algorithm applied in CUS game cannot be used here to get the optimal strategies for the source and relay nodes.

3.5.1 Relay Selection

Since relay nodes have different local CSIs and ask for different unit prices for helping the same source node, each source node has its own preference on the relay nodes.

Denote $\theta_i = |h_{id}|^2/|h_{ie}|^2 = \gamma_{id}/\gamma_{ie}$ as the ratio of the power gain between the R_i-D and R_i-E links. When the secrecy capacity is positive, $C_{sec,k}$ in (3.8) is rewritten as,

$$C_{sec,k} = W\log_2(1+\sum_{i=1}^{N}\frac{P_{S_k}P_{iS_k}\gamma_{S_k i}\theta_i\gamma_{ie}}{1+P_{S_k}\gamma_{S_k i}+P_{iS_k}\theta_i\gamma_{ie}}) - W\log_2(1+\sum_{i=1}^{N}\frac{P_{S_k}P_{iS_k}\gamma_{S_k i}\gamma_{ie}}{1+P_{S_k}\gamma_{S_k i}+P_{iS_k}\gamma_{ie}}) \tag{3.28}$$

By setting the $C_{sec,k}$'s derivative with respect to θ_i,

$$\frac{\partial C_{sec,k}}{\partial \theta_i} = \frac{W}{\ln 2}\frac{1}{(1+\sum_{i=1}^{N}\frac{P_{S_k}P_{iS_k}\gamma_{S_k i}\theta_i\gamma_{ie}}{1+P_{S_k}\gamma_{S_k i}+P_{iS_k}\theta_i\gamma_{ie}})} \times \frac{P_{S_k}P_{iS_k}\gamma_{S_k i}\gamma_{ie}(1+P_{S_k}\gamma_{S_k i})}{(1+P_{S_k}\gamma_{S_k i}+P_{iS_k}\theta_i\gamma_{ie})^2} > 0. \tag{3.29}$$

We see $C_{sec,k}$ is increasing with θ_i and $C_{sec,k} = 0$ only if $\theta_i = 1, i = 1, 2, \cdots, N$. Thus, to secure the data transmission, relay IoT nodes with a higher power gain on the wiretap link will be discarded. The remaining relay IoT nodes forms a new set $\mathcal{L} = \{R_1, R_2, \cdots R_L\}$.

3.5.2 Stage II: Power Equilibrium

Similar to that in CUS game, the source node S_k is considered. Its secrecy capacity is ensured to be positive with selected feasible relay IoT nodes. Given their unit price $\mathbf{q}$, the utility maximization problem (3.15) in State II becomes,

$$\begin{aligned} &\max_{\mathbf{P_{r_k}}} \alpha C_{sec,k}(\mathbf{P_{r_k}}) - \textstyle\sum_{i=1}^{L} q_i P_{iS_k} \\ \text{s.t.}\quad & 0 \le P_{iS_k} \le P_{i,max}/K, i = 1, 2, \cdots, L && (3.30) \\ & C_{sec,k}(\mathbf{P_{r_k}}) > C_0 && (3.31) \end{aligned}$$

Motivated by [171], we combine the penalty function method and the differential convex programming (DC programming) to maximize (3.30), which is equivalent to,

$$\min_{\mathbf{P}_{\mathbf{r_k}}} \sum_{i=1}^{L} q_i P_{iS_k} - \alpha C_{sec}(\mathbf{P}_{\mathbf{r_k}}) \tag{3.32}$$

3.5.2.1 Obtaining Exact Penalty

To simplify the minimization, penalty function method [20] is deployed to merge the constraint (3.31) into the objective function, which transforms the original problem to,

$$\begin{aligned} \min_{\mathbf{P}_{\mathbf{r_k}}} \quad & \sum_{i=1}^{N} q_i P_{iS_k} - \alpha C_{sec}(\mathbf{P}_{\mathbf{r_k}}) + \beta_m C^+(\mathbf{P}_{\mathbf{r_k}}) \\ & 0 \le P_{iS_k} \le P_{i,max}/K, i = 1, 2, \cdots, L \end{aligned} \tag{3.33}$$

where the penalty function $C^+(\mathbf{P}_{\mathbf{r_k}})$ is constructed as,

$$C^+(\mathbf{P}_{\mathbf{r_k}}) = \max\{-C_{sec}(\mathbf{P}_{\mathbf{r_k}}) + C_0, 0\} \tag{3.34}$$

where β_m is a suitable penalty factor. Based on [171], there exists $\beta > 0$ such that for every $\beta_m > \beta$ the problem in (3.32) is equivalent to the penalty problem in (3.33), which can be solved given β_m using DC programming. Since a larger β_m may increase the difficulty to solve the penalty problem, we start β_m with a small value and scale it up by a scaling factor $d > 1$ to make the problems (3.32) and (3.33) equivalent. The algorithm to obtain the exact penalty factor is as follows.

```
Algorithm 3: Obtaining Exact Penalty
Input: Pricing $\mathbf{q}$, convergence threshold $\epsilon$, the index of update $m$, and the maximum allowed
       number of $m$, $M_\epsilon$
Output: $\mathbf{P}_{\mathbf{r_k}}(\mathbf{q})$
Choose an initial value $\beta_0$, set $m = 0$ and $C^+(\mathbf{P}_{\mathbf{r_k}})^{(\beta_0)} = R_0$;
while $\beta_m C^+(\mathbf{P}_{\mathbf{r_k}})^{(\beta_m)} < \epsilon$ or $n > N_\xi$ do
    Given $\beta_m$, using DC Programing algorithm to solve (3.33) to otain the optimal ${\mathbf{P}_{\mathbf{r_k}}}^{(\beta_m)}$;
    Calculate $\beta_m C^+(\mathbf{P}_{\mathbf{r_k}})^{(\beta_m)}$;
    $\beta_{m+1} = d\beta_m$;
    $m = m + 1$;
end
return $\mathbf{P}_{\mathbf{r_k}}(\mathbf{q}) = {\mathbf{P}_{\mathbf{r_k}}}^{(\beta_m)}$;
```

Theorem 2. *Algorithm 3 is convergent.*

Proof: Assume (3.33) is solvable. Then $\mathbf{P_{r_k}}^{(\beta_m)}$ and $\mathbf{P_{r_k}}^{(\beta_{m+1})}$ are the optimal solutions of (3.33) given β_m and β_{m+1}, respectively. We have:

$$\sum_{i=1}^{L} q_i P_{iS_k}^{(\beta_m)} - \alpha C_{sec}(\mathbf{P_{r_k}})^{(\beta_m)} + \beta_m C^{+}(\mathbf{P_{r_k}})^{(\beta_m)} \leq$$
$$\sum_{i=1}^{L} q_i P_{iS_k}^{(\beta_{m+1})} - \alpha C_{sec}(\mathbf{P_{r_k}})^{(\beta_{m+1})} + \beta_m C^{+}(\mathbf{P_{r_k}})^{(\beta_{m+1})},$$

and

$$\sum_{i=1}^{L} q_i P_{iS_k}^{(\beta_{m+1})} - \alpha C_{sec}(\mathbf{P_{r_k}})^{(\beta_{m+1})} + \beta_{m+1} C^{+}(\mathbf{P_{r_k}})^{(\beta_{m+1})}$$
$$\leq \sum_{i=1}^{L} q_i P_{iS_k}^{(\beta_m)} - \alpha C_{sec}(\mathbf{P_{r_k}})^{(\beta_m)} + \beta_{m+1} C^{+}(\mathbf{P_{r_k}})^{(\beta_m)}$$

respectively. By adding the above two inequalities, we get,

$$C^{+}(\mathbf{P_{r_k}})^{(\beta_{m+1})} \leq C^{+}(\mathbf{P_{r_k}})^{(\beta_m)} \tag{3.35}$$

Since $C^{+}(\mathbf{P_{r_k}})$ is decreasing, Algorithm 3 is convergent. □

3.5.2.2 Solving Penalty Problem

Given the penalty factor β_m, we introduce an auxiliary variable $t \in \mathbb{R}$ and reformulate as,

$$\begin{aligned}
&\min_{\mathbf{P_{r_k}}} U'_{S_k}(\mathbf{P_{r_k}}) = \sum_{i=1}^{N} q_i P_{iS_k} - \alpha C_{sec,k}(\mathbf{P_{r_k}}) + \beta_m(t + C_{e_k}(\mathbf{P_{r_k}}))\\
&\text{s.t.} - C_{d_k}(\mathbf{P_{r_k}}) + C_0 \leq t\\
&\quad - C_{e_k}(\mathbf{P_{r_k}}) \leq t\\
&\quad 0 \leq P_{iS_k} \leq P_{i,max}/K, i = 1, 2, \cdots, L
\end{aligned}$$

For convenience, we denote the feasible set as

$$\mathcal{S} = \{(\mathbf{P_{r_k}}, t) : -C_{d_k}(\mathbf{P_{r_k}}) + C_0 \leq t, -C_{e_k}(\mathbf{P_{r_k}}) \leq t, \mathbf{P_{r_k}} \in \mathcal{S}, t \in R\} \tag{3.36}$$

By dividing the objective function into two convex functions,

$$U'_{S_k}(\mathbf{P_{r_k}}, t) = U_{S1}(\mathbf{P_{r_k}}, t) - U_{S2}(\mathbf{P_{r_k}}) \tag{3.37}$$

where

$$U_{S1}(\mathbf{P_{r_k}}, t) = \sum_{i=1}^{N} q_i P_{iS_k} - \alpha C_{d_k}(\mathbf{P_{r_k}}) + \beta_m t \tag{3.38}$$

and

$$U_{S2}(\mathbf{P_{r_k}}) = -(\beta_m + \alpha) C_{e_k}(\mathbf{P_{r_k}}) \tag{3.39}$$

The problem in (3.33) is a standard DC programming problem now. We solve it iteratively with a sequential convex program,

$$\min_{(\mathbf{P_{r_k}}, t) \in \mathcal{S}} U_{S1}(\mathbf{P_{r_k}}, t) - U_{S2}(\mathbf{P_{{r_k}(n)}}) - < \nabla U_{S2}(\mathbf{P_{{r_k}(n)}}), \mathbf{P_{r_k}} - \mathbf{P_{{r_k}(n)}} > \tag{3.40}$$

In particular, $\nabla U_{S2}(\mathbf{P_{r_k}}) = \left(\frac{\partial U_{S2}}{\partial P_{r1}}, \frac{\partial U_{S2}}{\partial P_{r2}}, \cdots, \frac{\partial U_{S2}}{\partial P_{rN}} \right)$ in (3.40) represents the gradient with respect to $\mathbf{P_{r_k}}$, where

$$\frac{\partial U_{S2}}{\partial P_{iS_k}} = -\frac{W(\beta_m + \alpha)}{\ln 2} \frac{\frac{\gamma_{S_k i} \gamma_{ie} P_{S_k} (1 + \gamma_{S_k i} P_{S_k})}{(1 + \gamma_{S_k i} P_{S_k} + \gamma_{ie} P_{iS_k})^2}}{\left(1 + \sum_{i=1}^{i=L} \frac{P_{S_k} P_{iS_k} \gamma_{S_k i} \gamma_{ie}}{1 + P_{S_k} \gamma_{S_k i} + P_{iS_k} \gamma_{ie}}\right)^2} \tag{3.41}$$

We propose Algorithm 4 to minimize the objective function in (3.40). According to [143], the $U'_{S_k}(\mathbf{P_{{r_k}(n+1)}})$ obtained is decreasing, and thus Algorithm 4 is convergent.

```
Algorithm 4: DC Programing Algorithm
    Input: $P_{S_k}$, $\beta_m$, convergence threshold $\xi, N_\xi$
    Output: $\mathbf{P_{r_k}}^{(\beta_m)}$
    Set the initial value $\mathbf{P_{{r_k}(n)}} = \mathbf{c}$ and $n = 0$;
    Compute $U'_{S_k}(\mathbf{P_{{r_k}(0)}})$ ;
    while $|U'_{S_k}(\mathbf{P_{{r_k}(n+1)}}) - U'_{S_k}(\mathbf{P_{{r_k}(n)}})| \leq \xi$ or $n > N_\xi$ do
        Based on $U'_{S_k}(\mathbf{P_{{r_k}(n)}})$, solving (3.40) to obtain $\mathbf{P_{{r_k}(n+1)}}$ using convex programming;
        Calculate $U'_{S_k}(\mathbf{P_{{r_k}(n+1)}})$;
        $n = n + 1$;
    end
    return $\mathbf{P_{r_k}}^{(\beta_m)} = \mathbf{P_{{r_k}(n)}}$;
```

Since both Algorithm 3 and Algorithm 4 are convergent, the power equilibrium for each source node is obtained given the price of relay nodes.

3.5.3 Stage I: Optimal Pricing

Similar to that in the CUS game, we update the price of each relay node as in (3.20). In practice, each selected relay node R_i listens to the instantaneous feedback information about $P^*_{iS_k}$ and $\partial P^*_{iS_k}/\partial p_i$ from the source node. In addition, it is natural for each relay node to regulate the unit price of its power as $q_i = c_i$, because a lower price q_i will result in a negative utility U_i while a higher price q_i would be at the risk of being excluded by the source node at the beginning.

3.6 Performance Analysis and Evaluation

In this section, we analyze the complexity for both the CUS and CKS game and evaluate their performance by both the simulations and experiments using real-world dataset.

3.6.1 Complexity Analysis

3.6.1.1 CUS Game (CUSG)

The problem of obtaining the strategies for both the source nodes and relay IoT nodes can be divided into two subproblems iteratively. First, for the utility maximization of source nodes, the optimal power is easily obtained according to Algorithm 2. Second, for the utility maximization of relay IoT nodes, the key to the price update is to calculate the partial derivative with respect to the unit price. Even if there are multiple relay IoT nodes, the source node updates the price for relay IoT nodes at one time and does not have to interact with each relay IoT node individually [90]. Hence, the expense of the communication between the source and relay IoT nodes is largely reduced.

3.6.1.2 CKS Game (CKSG)

The problem of obtaining the strategies for both the source and relay nodes is divided into three subproblems hierarchically. From Algorithm 3, Algorithm 4, and the Eq (3.20), the computational complexity of the proposed utility maximization method heavily depends on the DC programming and the derivatives with respect to the unit price of each relay IoT node. Since the convex subproblem in DC programming can be solved by many standard convex optimization methods, the utility maximization problem for the source node given the unit price can be easily solved.

3.6.2 Performance Evaluation Settings

To demonstrate the feasibility of our proposed game-theoretical approaches, we conduct both simulations and experiments using real-world datasets under both wiretap-link CSI known and unknown cases. In the wiretap-link CSI known case, we mainly consider the secrecy capacity performance, while the price, the power, and utilities of the source/relay nodes are focused in the wiretap-link CSI unknown case.

3.6.2.1 Simulation Setting

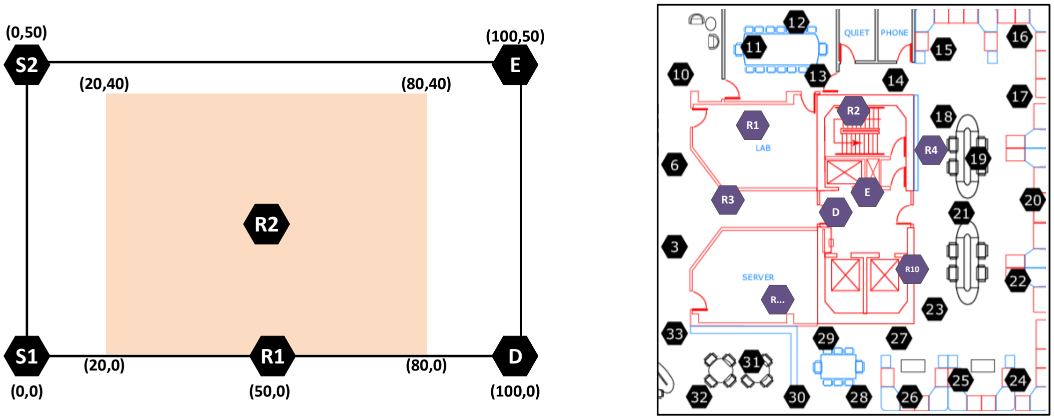
We mainly consider the following three cases, Single-Source Single-Relay (SSSR), Single-Source Multiple-Relay (SSMR), and Multiple-Source Multiple-Relay (MSMR), where we choose 2 nodes in the multiple source/relay cases. Note that these can be easily extended into the scenario with more than two source/relay nodes. The simulation settings are give in Fig. 3.3a and Tab. 3.2.

Simulation Parameter	Values
maximum power of the source node	10mW
maximum power of the relay IoT node	100mW
variance of the noise σ^2	10^{-8}
path loss of the static Rayleigh channel	2
transmission bandwidth W	1 (Normalization)
gain per unit of secrecy capacity α	0.01
unit cost of transmission power c_i	0.01
secrecy capacity constraint in CKSG	0.01bit/s/Hz
supreme secrecy capacity in CUSG	1bit/s/Hz

Figure 3.2: System Parameters in Simulation

3.6.2.2 Experiment Setting

We use the data from 54 sensors deployed in the Intel Berkeley Research lab [1] as shown in Fig. 3.3b. These sensors collect timestamped topology information, along with humidity, temperature, light and voltage values once every 31 seconds. We consider one of the circles surrounded by 26 nodes (No.3, No.6, and No.10-33). In addition, we assume there is a destination node located at the center of the circle $(10m, 15m)$. An eavesdropper $(12m, 18m)$ near the destination node attempts to intercept the sensed data information from all the source nodes.



(a) Location in CKSG

(b) Location in Dataset

Figure 3.3: System Settings

3.6.3 Security Performance in CKSG

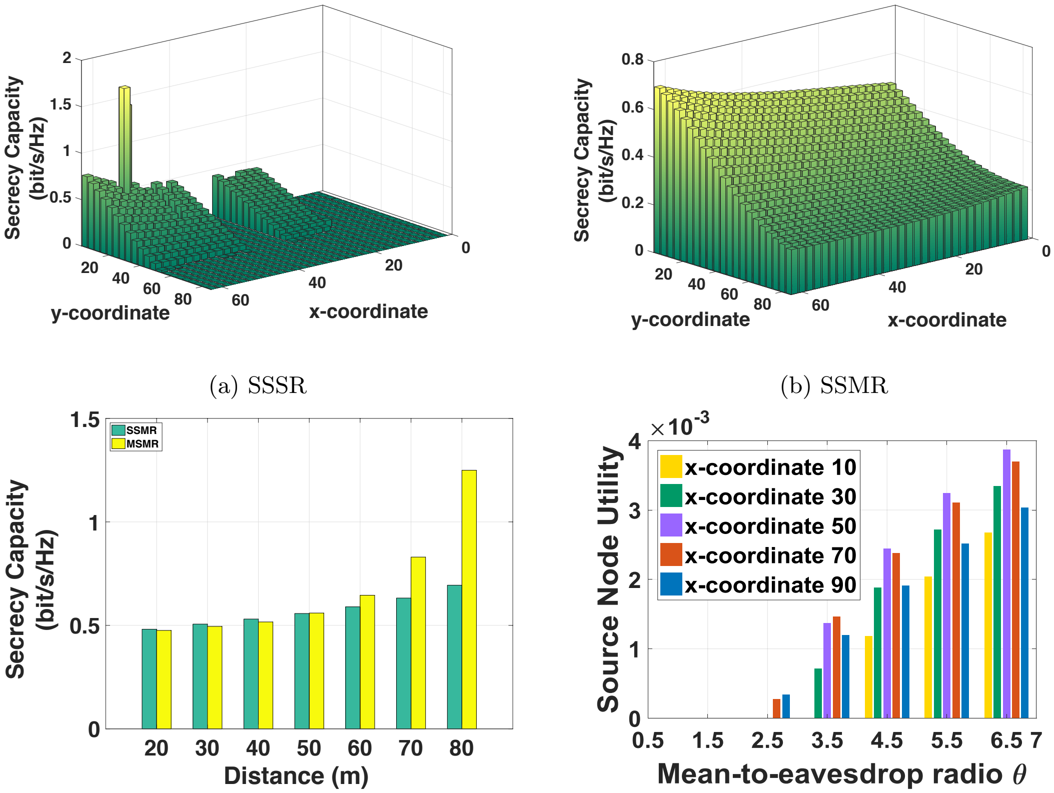
The secrecy capacity performance in the CKSG simulation is demonstrated in Fig.3.4, where ‘x-coordinate’ and ‘y-coordinate’ in Fig.3.4a and Fig. 3.4b denote the location of relay nodes. The ‘Distance’ represents the horizontal location difference between the source node S_1 and relay nodes. For SSSR scenario, S_1 is fixed and R_2 is moving in the red area in Fig.3.3a. For SSMR scenario, a new relay IoT node R_1 is introduced, which is fixed at the location $(50m, 0m)$. Extending to MSMR scenario, the source node S_2 is added and fixed at the location $(0m, 50m)$.

3.6.3.1 Effect of Multiple Relay Nodes

The location of R_2 has a strong effect on the secrecy capacity as shown in Fig.3.4a and Fig.3.4b. Particularly, when R_2 is near the destination node, the secrecy capacity is largely improved. This is because the power gain ratio between the relay-destination link and the relay-eavesdropper link increases as R_2 moves to the destination node. Besides, the comparison between Fig.3.4a and Fig.3.4b demonstrates that the introduction of R_1 increases the total secrecy capacity. Since R_1 close to the destination node D instead of the eavesdropper E, it can help forward the data from S_1 while preventing it from being intercepted by the eavesdropper. The security performance is improved.

3.6.3.2 Effect of Multiple Source Nodes

Fig.3.4c compares the secrecy capacity performance under the SSMR and MSMR scenarios, which shows that bringing in extra source nodes deteriorates the security performance. When the relay node R_2 moves from the source node to the destination node, the total secrecy capacity MSMR is first smaller then surpasses that in SSMR. This is because the power gain on the S_2-R_1-D link is less than that on the S_2-R_1-E link. When R_2 gets over to the $(50m, 0m)$, the power gain on the S_2-R_1-D link is larger than that on the S_2-R_1-E link. The total secrecy capacity begins to increase.



(a) SSSR

(b) SSMR

(c) MSMR

(d) Utility Vs. Power Gain (SSMR)

Figure 3.4: Security Performance in CKSG

3.6.3.3 Main-to-Eavesdropper Link Ratio Effect

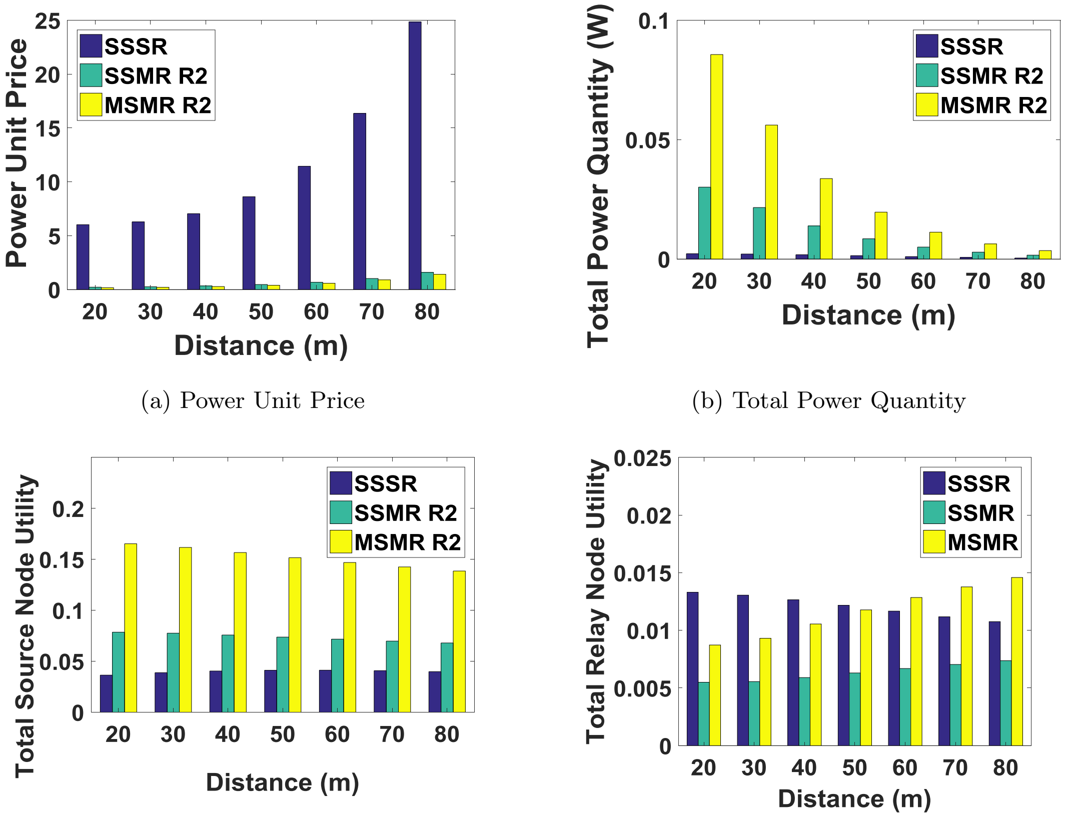
We draw the relationship between the utility of the source node and the power gain ratio in SSMR scenario in Fig.3.4d, where y-coordinate of the relay node R_2 is assumed to be 0. In Fig.3.4d, the power gain ratio θ brings a positive effect to the source node utility. When $\theta \leq 1$, the utility of the source node keeps 0, which shows that the relay selection in the CKS game is infeasible. In addition, the source node' utility is still 0 even if $\theta > 1$. Since the source node has to purchase the power from each relay node, it has to get a larger secrecy capacity in order to ensure its utility. In contrast to that in Fig.3.4b, the source node's utility gets maximized when R_2 is in the middle of the source and destination node. When R_2 is near to the destination node, it uses less power to forward the data. To get more benefits, R_2 requests a higher unit price, which decreases the utility of the source node. When R_2 is near the source node, it has to use more power for transmission. According to Eq.(3.15), the source node's utility is thus decreased.

3.6.4 Utility Performance in CUSG

In this subsection, we demonstrate the utility performance for both the source and relays nodes in CUSG. In particular, we keep the location of S_1, D and E while changing the location of S_2 and R_1 to $(0m, 25m)$ and $(50m, 25m)$, respectively, in both SSMR and MSMR scenarios. Meanwhile, we suppose R_1 in SSSR scenario and R_2 in other scenarios are moving from $(20m, 25m)$ to $(80m, 25m)$ in a straight line to see the changes on the price, power and utility of both source and relay nodes.

3.6.4.1 Effect of Multiple Relay Nodes

Fig.3.5 compares the performance in all ways between SSSR and SSMR scenarios. Particularly, we show the effect brought by the moving relay node R_2 in SSMR scenarios. Specifically, due to competition, introducing a new relay IoT node lowers the power unit price obviously as shown in Fig.3.5a. In the SSSR scenario, the source node purchases a smaller amount of power from the relay IoT node since the power is too expensive. Whereas in the SSMR and MSMR scenarios, the low power unit price stimulates the source nodes to purchase more power. Meanwhile, owing to the energy harvesting, the relay IoT nodes can use their power to forward the data from the source nodes as much as possible as shown in Fig.3.5b. As a result, the power unit price and power quantity co-determine the utility of the source and relay nodes shown in Fig.3.5c and Fig.3.5d, where the introduction of the relay nodes increases the utility of source nodes and brings a slightly negative effect on other relay IoT nodes.



(a) Power Unit Price

(b) Total Power Quantity

(c) Total Source Node Utility

(d) Total Relay Node Utility

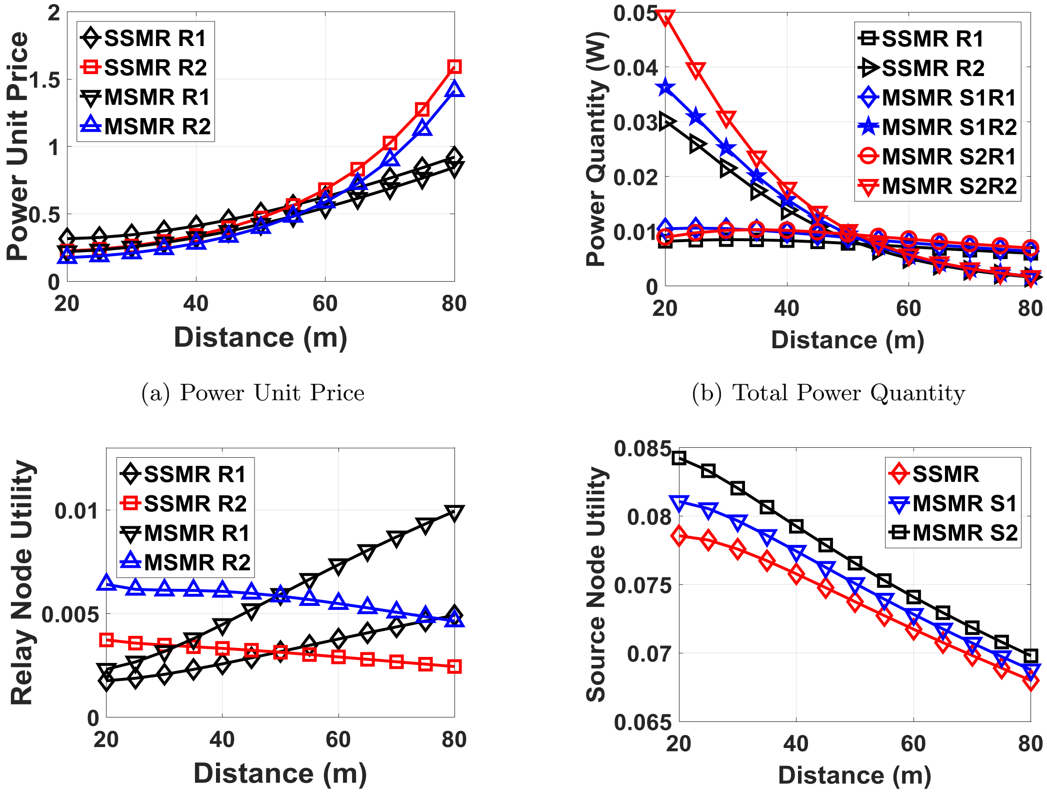
Figure 3.5: Comparison between SSSR and SSMR in CUSG

3.6.4.2 Mutual Effect among Relay Nodes

We mainly consider the SSMR scenarios, where R_1 is fixed at $(50m, 25m)$ and R_2 is moving. When R_2 is close to S_1, it uses more power to forward the S_1's data. Thus, a low power unit price is enough to get a high utility for R_2. Since S_1 buys less power from R_1, R_1 has to increase its unit price to maximize its utility. However, as R_2 is moving far away from S_1, it sells less power to S_1. R_2 has to increase the power unit price. Seeing that R_2 increases its unit price, R_1 also increases its own price as shown in Fig.3.6a. As a result, both R_1' power unit price and the power quantity sold to S_1 change even if it does not move as reflected in Fig.3.6a and Fig.3.6b. Obviously, the utility of R_2 is increasing when it is close to S_1 while becoming less as it is moving to D as shown in Fig.3.6c. Given less power and more unit price, the utility of the source node decreases as demonstrated in Fig.3.6d.

3.6.4.3 Effect of Multiple Source Nodes

The performance in all ways between SSMR and MSMR scenarios is compared in Fig.3.6, where Fig.3.6a and 3.6b show the changes of power unit price and quantity when introducing a new source node S_2. Suppose each relay node has enough harvested energy to forward the source nodes' data. Compared to the distance to S_1, R_2 is always close to S_2. R_2 sells more power to S_2 than to S_1. As R_2 continues moving, such distance difference becomes less. The power sold to S_1 and S_2 is almost the same. That is why the power quantity sold to S_1 and S_2 is similar for R_1. With more source nodes, the competition between relay IoT nodes becomes more fierce. Both relay nodes would like to sell more power to source nodes, which benefits source nodes' utilities. As shown in Fig.3.6d, the utility of each source node is more in MSMR scenario compared to that in SSMR scenario. Since each relay node sells more power with almost the same unit price, they get more utilities as shown in Fig.3.6c.



(a) Power Unit Price

(b) Total Power Quantity

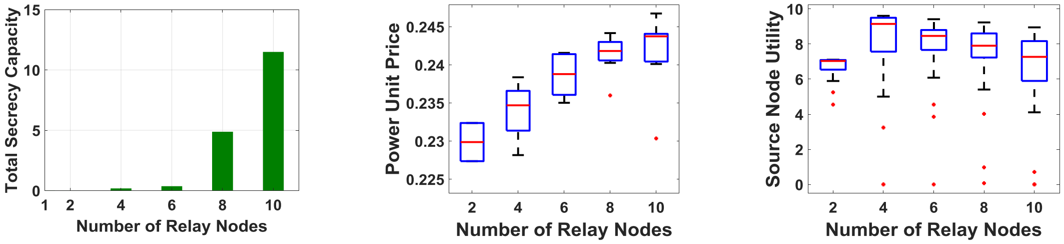
(c) Total Relay Node Utility

(d) Total Source Node Utility

Figure 3.6: Comparison between SSMR and MSMR in CUSG

3.6.5 Real-world Experimental Results

To show the performance of CKSG and CUSG, we conduct the experiment using real-world dataset as shown in Fig.3.7. We first verify the effect brought by multiple relay IoT nodes in CKSG. The total secrecy capacity of all the 26 participating source nodes is illustrated in Fig.3.7a. Obviously, the introduction of more relay nodes indeed improves the security performance when the wire-tap link CSI is known. Note that we assume at most 10 relay IoT nodes help forward data. With more relay nodes, the interference among them would deteriorate the data transmission. In CUSG, the competition among relay nodes increases the power unit price as given in Fig.3.7b. As power unit price becomes larger, the source nodes will not purchase more power. Thus, the average source node utility is increasing and then decreasing as more relay IoT nodes help forward the data as shown in Fig.3.7c.



(a) Secrecy Capacity in CKSG (b) Power Unit Price (CUSG) (c) Source Node Utility (CUSG)

Figure 3.7: Experimental Results

3.7 Chapter Summary

In this chapter, we design a cooperative IoT system for ensuring the communication security. To benefit the relays in forwarding the data for defending the eavesdropping attack, we propose two Stackelberg games, namely CUS game and CKS game, working under the wiretap-link CSI unknown and known cases, respectively. Our simulation and experiment results show that the game-theoretical approach will improve the utility of source nodes and defend against the eavesdropping attack, and thus enhances the security for IoT systems.

Chapter 4

Motivating Human-enabled Mobile Participation for Data Offloading

4.1 Chapter Overview

The soaring popularity of mobile devices enables people to communicate with their social ties at any time and from anywhere. People use mobile apps to create and exchange a huge amount of data with their social interactions in cyberspace. Reports warn that monthly global mobile data traffic will surpass 48.3 EB per month by 2021 [37]. Although cellular network operators exploit their efforts to provide better services in terms of higher data rate and lower costs, users are still facing poor performance in their daily life, especially in some crowded areas, such as football stadiums, theme parks, and airports. However, the above crowded areas are the places that highly need reliable wireless communication, e.g., broadcasting evacuation information for safety purpose. As a promising solution, mobile data offloading takes advantages of small cell, Wi-Fi, and opportunistic communication to pro-actively reduce the data traffic targeted for cellular networks [89]. Unfortunately, although various types of mobile offloading schemes have been proposed in both academia and industry, we are still lacking effective methods. For example, utilizing small cells is not an effective method due to the scarcity of licensed spectrum bandwidths. Even worse, deploying more small cells will incur significant costs. Regarding Wi-Fi offloading, the service provider has access to much larger free spectrum to cater the Wi-Fi deployment. However, Wi-Fi offloading cannot provide guaranteed QoS, and Wi-Fi-enabled devices may experience increased battery drainage since it has to operate on two different radio interfaces [11]. To perform mobile offloading, opportunistic communication has been identified as another approach, which increases communication chances by utilizing the potential social connections among users and thus is beneficial to deliver contents. In particular, some works [61, 87] apply social-based approaches to help data dissemination among social ties or users with similar social profiles. Apparently, the opportunistic communication is not reliable for data delivery in an ad hoc mode because there is lack of incentives for source users to coordinate the data dissemination. Clearly, mobile offloading has not been well developed nor widely applied.

Facing these challenges and existing solutions, we take a step further to reconsider the human-enabled approach for mobile offloading, which takes human social behaviors and human activities into consideration. Intuitively, users with similar social interests often group together at certain location [158], which potentially results in similar content requests. For example, users gathered in specific attractions in the Disneyland may request the similar contents related to those attractions. When they request similar contents, network congestion would be caused due to limited bandwidth. Such congestion potentially prevents users from getting their requested contents. The above phenomenon leads us to consider how to avoid repeated requests/retrievals in order to reduce the number of accesses to the service provider (SP). A possible solution is to leverage users' similar social attributes to design a human-enabled data offloading scheme. In sociology [134], homophily phenomenon describes that people with more similar attributes contact more frequently than complete strangers. The interactions between users with more contacts bring more **social effect**, which captures the advantages of word-of-mouth communication [29]. Specifically, users typically form their opinions about the quality of the contents based on the information they obtain from other users. Thus, when a user demands more contents, his social friends would also request more contents due to the similarity of their interests. Meanwhile, users with identical attributes could share their contents with each other using free device-to-device (D2D) communication. As for human activities, an observation is that users in crowded areas either walk around or go to their interested attractions. Hence, we can take advantage of the mobility of users to alleviate the congestion.

In this work, we propose a **human-enabled mobile participation** approach in data offloading by introducing a mobile caching user (MCU), who bridges the gap between the SP and users when the above congestion happens. Qur approach is mainly divided into two steps. In the first step, we consider the data offloading between the MCU and the representing users (RUs) with similar content requests in crowded areas. Specifically, an MCU pre-caches a number of large volume contents in advance. After receiving congestion information (e.g., congestion area, requested contents, .etc) from the SP, the MCU chooses a specific crowded area where requested contents are similar with his own interests and is near to his current location, physically moves to the RUs in the chosen area and transfers the contents to them. In the second step, the RUs with obtained contents further disseminate content copies via D2D communication to other users opportunistically, who have the identical content requests with them. We mainly consider the first step, where delay-tolerant scenario and delay-sensitive scenario are discussed. In the delay-tolerant scenario, RUs would like to wait until they download the requested contents. Whereas in the delay-sensitive scenario, RUs are urgent to get the requested contents. They will be more dissatisfied with the increasing of the waiting time. Compared to traditional data offloading approaches, the proposed approach is significantly cheaper than the small cell build-out. Moreover, by physically moving to the crowd, the MCU makes data transmission more reliable and flexible than either Wi-Fi or pure D2D communication.

To motivate above human-enabled mobile participation, we design an incentive mechanism. While participating in human-enabled data offloading, the MCU spends a few time in moving and consumes his own resources such as battery and storage. Hence, he would not be interested in it unless he receives a satisfying revenue. As for RUs, they not only get the originally requested contents, but also harvest additional contents they may be interested in due to the similarity of their interests with other RUs, which largely improves their satisfactions. Since RUs request similar contents and pay for them individually, it is reasonable to assume that RUs are selfish and rational. Hence, each RU only wants to maximize his own satisfaction. To increase the MCU's total revenue and provide RUs' satisfaction, we will thoroughly investigate RUs‘ content requests, social effect, delay effect, and unit payment strategy for both the MCU and RUs in the proposed incentive mechanism.

Our Contributions: We highlight our major contributions as follows,

- We propose a new data offloading scheme that takes advantages of both homophily phenomenon and mobile participation to greatly reduce the congestion in crowded areas where users with similar interests are normally grouped together.

- Specifically, we consider two system models: the delay-tolerant model and the delay-sensitive model. In both models, by considering RUs' interactions, we formulate the communication between the MCU and RUs as a two-stage Stackelberg game. In Stage I, the MCU chooses a unit payment to maximize his total revenue. In Stage II, each RU chooses a requested content level given the unit payment to maximize his satisfaction on the received contents.

- For the delay-tolerant scenario, the interactions between RUs bring social effect. We first give an assumption under which we show the existence and uniqueness of the Nash equilibrium in Stage II. Then, we present an effective algorithm to compute the unique Stackelberg equilibrium in Stage I, at which the revenue of the MCU is maximized, and none of the RUs continue requesting contents by unilaterally deviating from his current strategy
- For the delay-sensitive scenario, the interactions between RUs not only bring social effect but also delay effect. We extend the Stakelberg game to the delay-sensitive model. To alleviate the serious delay effect, we propose two improved delay-sensitive models by further taking advantages of users' mobility, where the first one considers the queueing delay and the other introduces multiple MCUs.

The rest of this chapter is organized as follows: In Section 4.2, we briefly review the existing data offloading approaches, economical incentives for performing data offloading and the social effect due to similar interests between RUs based on their social relationship. In Section 4.3, we explain our motivations of leveraging the homophily phenomenon and the mobile participation. Following with that, a detailed description of our proposed data offloading system models is given in Section 4.4, which are formulated as two-stage Stackelberg games respectively. In Section 4.5, we study the proposed Stackelberg game in the delay-tolerant scenario. To better adapt to the practical situation, we extend the Stackelberg game to the delay-sensitive scenario in Section 4.6. In Section 4.7, the performance of our data offloading approach is evaluated, followed by a conclusion in Section 4.8.

4.2 Related Work

4.2.1 Mobile Data Offloading

Mobile data offloading [11] is a promising way to alleviate traffic congestion and reduce the energy and bandwidth consumption. For example, Liang *et al.* in [180] offload their applications and data from mobile devices to the cloud to improve users' experience in terms of longer battery lifetime, larger data storage, faster processing speed and more powerful security services. Zhang *et al.* in [196] offload mobile users' applications to nearby mobile resource-rich devices (i.e., cloudlets) in an intermittently connected system to reduce energy consumption and improve performance. In this chapter, we generally discuss the mobile offloading for cellular networks, which is classified into two categories [78]. Infrastructure-based mobile data offloading [16] refers to deploying small cell base stations and Wi-Fi hotspots for mobile users [79, 134]. The connection between mobile users and the base station is proposed to achieve flow level load balancing under spatially heterogeneous traffic distributions in [19, 108] . However, the lack of cost-effective backhaul associations for base station often impairs their performance in terms of offloading mobile traffic. The second category is the ad-hoc-based mobile traffic offloading, which refers to applying short range communication as the underlay to offload mobile traffic [61, 87, 125, 164, 200].

4.2.2 Economic Incentives for Data Offloading

The above works mainly focus on the technical perspective adoption of data offloading without considering economic incentives. The incentive issue is significant for the case where Wi-Fi or small cell is privately owned by third-party entities, who are expected to be reluctant to admit non-registered users' traffic without proper incentives [60]. The incentive framework for the so-called user-initiated data offloading is considered in [86, 140], where users initiate the offloading process and offer necessary incentives in order to obtain their contents. Gao *et.al.* in [60] consider the network-initiated data offloading, where cellular networks initiate the offloading process, and hence the network operators are responsible for incentivizing Wi-Fi.

4.2.3 Attribute-based Social Effect

The above works do not consider homophily phenomenon [134]. Reingen *et al.* in [148] conduct a survey of the members of a sorority in which they measure brand preference congruity as a function of whether they live in the sorority house. They find that those who live together as a group have more congruent brand preferences than those who do not. Presumably, living together provides more opportunities for interaction and communication. Taking a further step, they note that information obtained from social tie connections will influence in decision making in [28].

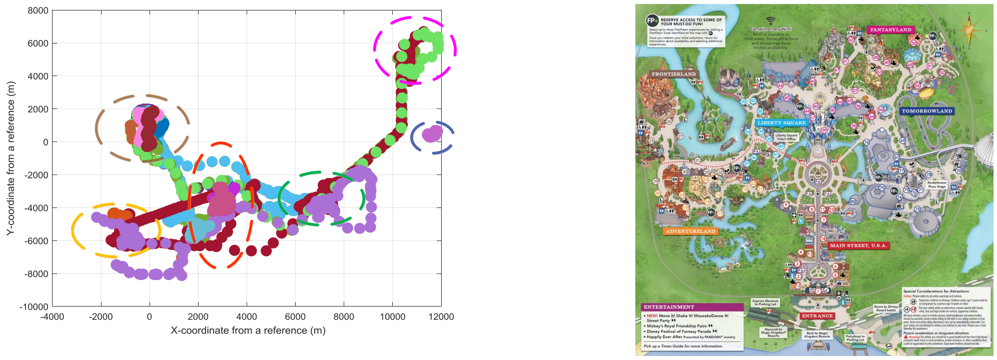
The above observations and inference are deployed in several works. In [68, 70, 71], different privacy-preserving authentication schemes for mobile health networks are designed from a social perspective view. Users in online social networks apply their attributes to find matched friends and establish social relationships with strangers in [69]. Gong *et al.* in [65] study users' behaviors by jointly considering congestion effect in the physical wireless domain and social effect based on users' social relationship. In [34, 64], a social group utility maximization framework, which captures the impact of mobile users' diverse social ties, is studied. Considering the social effect brought by social ties among users, different pricing strategies of a monopolist have been studied in [30]. In our previous work [190], the social effect brought by users' similar social attributes is deployed to assist data offloading. However, the introduction of the MCU brings severe delay effect, which negatively affects the data offloading performance. To alleviate delay effect, we take the queue and multi-leader Stackelberg game into consideration now, which differentiates our chapter with [65]. We focus on incentive mechanisms to motivate human-enabled mobile participation for data offloading under both social effect and severe delay effect.

4.3 Motivations and Preliminaries

4.3.1 Social Enabled Data Offloading

Given a pair of strangers, one cannot push another to help recommend/forward his contents if they do not have any pre-established relationship. However, comparing with complete strangers, people may intend to help the one that shares some similarities in terms of attributes, e.g., language, nationality, affiliation, etc. As discussed in [107], it is a well-accepted nature of human interaction that people like to interact with those who are similar to themselves, which is often termed the "like me" principle. In [72, 73], the authors conduct an experiment based on the trace file collected during the INFOCOM 2006 [154], which analyzes the relationship between the contact rate and the number of identical attributes. The result shows that the contact rate in terms of the number of contacts between two users increases with the increment of identical attributes, which further validates the "like-me" principle. Therefore, a potential social tie can be set up based on the attribute similarity. Furthermore, Reingen *et al.* in [28] find that information obtained from strong tie connections are more influential in decision making than weak tie connections at a micro level (information flows within dyads or small groups). Motivated by it, content dissemination would be more efficient given the assumption that more attribute similarities exist between users. In addition, users who share similar interests intend to form a group and they can forward messages to others in the group more efficiently according to [85]. Hence, we infer that the social-enabled content dissemination would be much more efficient if users apply attribute similarity to form the attribute-similar group.

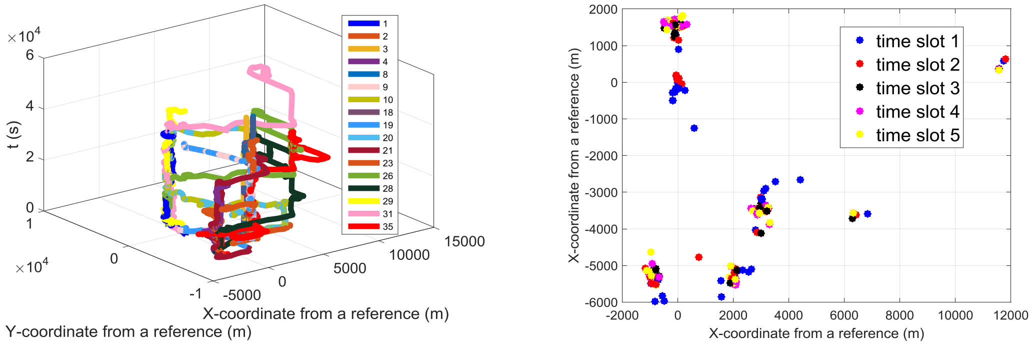
Motivated by the above discussions, we consider human's similar social attributes. In the scenarios where users group together based on their similar social attributes, such as interests, their requested contents have a higher probability to be similar even identical due to their influence on each other. Hence, we could select RUs to request contents and further disseminate them to other users via D2D communication. Thus, users can obtain more interested contents and their satisfactions are improved.



(a) Potential location in Real Trace

(b) Disney Map

Figure 4.1: Potential Location of the MCU



(a) Potential Location vs. Time

(b) Locations in Different Time Slot

Figure 4.2: Time Changes vs. Potential Location

4.3.2 Mobile Participation

We conduct an experiment analyzing human mobility traces using the real data trace file [151] in order to show the feasibility of mobile participation. The human traces are obtained every 30 seconds from 40 volunteers who spent their Thanksgiving and Christmas holidays in Disney World, Florida, US. We describe all the locations the volunteers have gone to as shown in Fig.4.1a, in which we circle the locations that are visited most. By comparing it with the real Disney World map [2] in Fig.4.1b, we find that those circled locations are exactly the crowded attraction areas, where users with similar interests get together and request similar contents. For example, at the Rock 'n' Roller Coaster Starring Aerosmith attraction, many young visitors who enjoy the trilling feelings group together and they are more interested in exciting contents. In addition, we draw 17 volunteers' mobile traces as time changes in Fig.4.2a, which verifies the mobility of volunteers. Meanwhile, we illustrate volunteers' locations in different time-slots in Fig.4.2b,where we see that volunteers are distributed in all crowded attraction areas in each time-slot. Inferring from the observations in Fig.4.1 and Fig.4.2, we conclude that: 1). volunteers move as time changes; 2), there always exist volunteers in each attraction in each time-slot. Therefore, leveraging mobile participation is feasible to achieve content delivery and dissemination.

4.4 System Model and Problem formulation

4.4.1 Overview

To assist the description, we continue the example in Disney World as shown in Fig. 4.3, where the yellow area is denoted as the Rock 'n' Roller Coaster Starring Aerosmith attraction. It is divided into two time-slots. In time-slot 1, no congestion exists in the yellow area. David downloads numbers of contents and continues to visit other attractions. In time-slot 2, an increasing number of users with similar interests group together and request for contents related to the attraction, which results in severe congestion. As a result, users cannot get the requested contents from the SP. The SP asks David for help via transmitting him the short message related to the congestion information. Since David is interested in the same attraction and can obtain extra revenue, he moves back to disseminate the contents after checking the distance availability between himself and the chosen attraction. He first announces the unit payment for the requested contents. Each RU chooses a requested content quantity to maximize his satisfaction based on the unit payment and other RU's choices, which is submitted to David. David maximizes the total revenue and computes the corresponding unit payment which is returned to RUs. Such communication between David and RUs is processed iteratively until David and RUs reach an agreement, in which David gets the maximized revenue and RUs satisfy the content obtaining experience. Finally, RUs disseminate their contents to other users in the crowd via D2D communication.

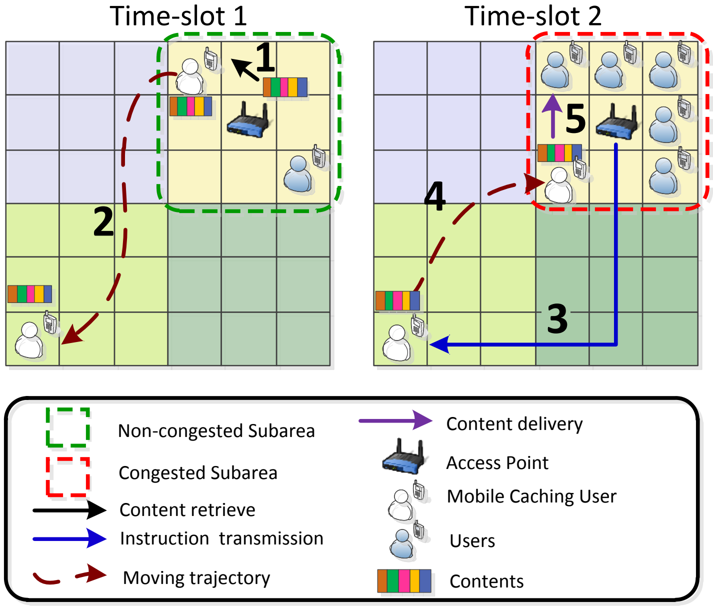


Figure 4.3: System Model of Mobile Participation

4.4.2 System Model

Depending on RUs' sensitiveness to the waiting time for the requested contents, two models are considered: **delay-tolerant model** and **delay-sensitive model**.

4.4.2.1 Delay-Tolerant Model

In the delay-tolerant model, RUs do not care their waiting time. Assume a set of RUs $\mathcal{N} = \{1, 2, \cdots, i, \cdots N\}$ group together and cannot get their requested contents from the SP directly, where N denotes the total number of RUs. Their corresponding requested content level profile is represented as $\mathbf{x} = \{x_1, x_2, \cdots, x_i, \cdots, x_N\}^T \in [0, \infty)^N$, which quantifies the contents they request from the MCU. Let $x_i \in [0, \infty)$ denote the requested content level of the RU i and $\mathbf{x}_{-i}$ denote the requested content levels of other RUs except for the RU i. According to [30], the RU i's satisfaction consists of the following two parts: 1), internal characteristics, represented by the maximum internal demand rate $a_i > 0$ and the internal demand elasticity factor $b_i > 0$. The internal demand rate represents the maximum satisfaction that each RU gets given unit content level whereas the elasticity factor measures the sensitivity of the RU's satisfaction to changes in content levels [31]. 2), external characteristics, represented by social effect that RU j brings to RU i, quantified by $g_{ij} > 0$, $\forall j \in \mathcal{N}$ and $j \neq i$. Since utility is a terminology in game theory and economics to represent the satisfaction experienced by the consumer of a good [176], the satisfaction of each RU is quantified by utility hereinafter. Given the unit payment p the MCU charges RUs, the utility of RU i is quantified as,

$$u_i(x_i, \mathbf{x}_{-i}, p) = a_i x_i - \frac{1}{2} b_i x_i^2 + \sum\nolimits_{j \neq i} g_{ij} x_i x_j - p x_i, \forall i \tag{4.1}$$

The quadratic form in (4.1) not only allows for tractable analysis but also serves a good second-order approximation for a broad class of concave utility functions [30].

Given RUs' requested content levels, the total revenue of the MCU is,

$$R\left(\mathbf{x}, p\right) = \sum\nolimits_{i \in \mathcal{N}} (p - c) x_i \tag{4.2}$$

where c is the unit cost the MCU spends when transmitting contents to RUs, including energy and move consumption.

4.4.2.2 Intuitive Delay-Sensitive Model

Due to the difference of RUs' requested contents, the MCU moves to RUs and delivers contents to them one by one. As a result, each RU has to wait for the content transmission from the MCU when multiple RUs request contents. If they are urgent to obtain the requested contents, their utilities would be lowered due to long waiting time.

Assume RUs do not know the transmission order of the MCU in advance. Each RU would consider the worst case that he is the last one to receive the contents. To clearly show the time delay effect, we assume the transmission rates between the MCU and RUs are normalized and the same. The utility of the RU i in the delay-sensitive model is,

$$\overline{u}_i\left(\overline{x}_i, \overline{\mathbf{x}}_{-i}, \overline{p}\right) = a_i\overline{x}_i - \frac{1}{2}b_i{\overline{x}_i}^2 + \sum\nolimits_{j\in\mathcal{N}} g_{ij}\overline{x}_i\overline{x}_j - \frac{1}{2}d\left(\sum\nolimits_{j\in\mathcal{N}}\overline{x}_j\right)^2 - \overline{px}_i, \forall i \tag{4.3}$$

where d is the delay effect coefficient determined by the SP. Compared (4.3) with (4.1), the social relationship between RUs brings not only positive social effect but also severe delay effect in the intuitive delay-sensitive model.

The total revenue of the MCU keeps unchanged,

$$\overline{R}\left(\overline{\mathbf{x}}, \overline{p}\right) = \sum\nolimits_{i\in\mathcal{N}}\left(\overline{p} - c\right)\overline{x}_i. \tag{4.4}$$

4.4.2.3 Queue Delay-Sensitive Model

The potential assumption in the above intuitive delay-sensitive model is that the MCU begins transmission after the SP receives content requests from all RUs. If the SP can predict the potential congestion effect at some locations, it could arrange the MCU to move to these locations in advance instead of asking the MCU for help after congestion effect appears. Because the SP keeps the historical data monitoring records, the above assumption is easily satisfied. Thus, when an RU broadcasts a content request, the MCU could transmit the content to him on time. Simultaneously, the content requests from other RUs continuously arrive at the MCU. Content transmission from the MCU to RUs forms a First In First Out (FIFO) queue model in Fig. 4.4. The notations are listed in Table. 4.1.

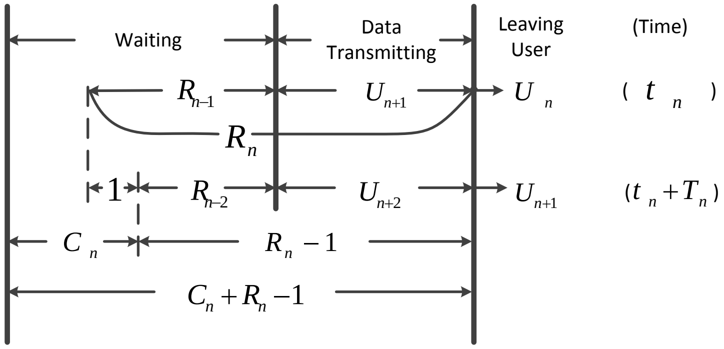


Figure 4.4: $M/G/1$ Queue in Delay-Sensitive Model

In the queue delay-sensitive model, we assume the levels of newly arrival requested contents

Table 4.1: Notations in $M/G/1$ Queue

Symbols	Meaning
R_n	the remaining requested content levels in the queue after the content delivery to user n
T_n	the content transmission period for user n
C_n	the content requests newly coming to the queue while user $n+1$ is receving the requested contents
t_n	the time at which the content transmission for user n is finished
$t_n + T_n$	the time at which the content transmission for user $n+1$ is finished

C_n in a finite interval of length t follows the Poisson distribution with mean arrival rate λ: $P\{C_n = j|T_n = t\} = \frac{(\lambda t)^j}{j!}e^{-\lambda t}$. The Poisson process is a viable model when contents originate from a large population of independent RUs. Due to the similar interests of RUs at the same location, most of their requested content levels distribute in the same interval. Given unit content transmission speed, the content transmission time is modeled to follow the Gaussian distribution with mean $\mu \gg 0$ and variance σ^2. Assume the traffic intensity $\rho = \lambda/\mu < 1$ for stability. Based on Pollaczek-Khinchin (P-K) formula [17], the expected RU waiting time W_q for each RU is,

$$W_q = \frac{\rho^2 + \lambda^2\sigma^2}{2\lambda(1-\rho)} \tag{4.5}$$

Considering the waiting time, each RU's utility becomes,

$$\hat{u}_i\left(\hat{x}_i, \hat{\mathbf{x}}_{-i}, \hat{p}\right) = a_i\hat{x}_i - \frac{1}{2}b_i\hat{x}_i^2 + \sum\nolimits_{j\in\mathcal{N}} g_{ij}\hat{x}_i\hat{x}_j - k\frac{\rho^2 + \lambda^2\sigma^2}{2\lambda(1-\rho)} - \hat{p}\hat{x}_i, \forall i \tag{4.6}$$

where k is the congestion coefficient. According to the historical records, the SP can predict the traffic mean arrival rate λ. One observation is that contents related to each attraction are time-invariant. Thus, the SP could also evaluate the current traffic intensity ρ. Since different RUs request contents when congestion effect happens, the variance σ^2 is unknown. Point estimation [43] is applied to estimate σ^2,

$$\hat{\sigma^2} = \frac{1}{N-1}\sum\nolimits_{j\in\mathcal{N}}\left(\hat{x}_j - \frac{1}{N}\sum\nolimits_{m\in\mathcal{N}}\hat{x}_m\right)^2 \tag{4.7}$$

Substitute (4.7) into (4.6), the utility becomes,

$$\hat{u}_i\left(\hat{x}_i, \hat{\mathbf{x}}_{-i}, \hat{p}\right) = a_i\hat{x}_i - \frac{1}{2}b_i\hat{x}_i^2 + \sum_{j\in\mathcal{N}} g_{ij}\hat{x}_i\hat{x}_j - k\frac{\rho^2}{2\lambda(1-\rho)} - k\frac{\lambda}{2(1-\rho)}\frac{1}{N-1}\sum_{j\in\mathcal{N}}\left(\hat{x}_j - \frac{1}{N}\sum_{m\in\mathcal{N}}\hat{x}_m\right)^2 - \hat{p}\hat{x}_i, \forall i \tag{4.8}$$

The total revenue of the MCU is the same as that in the intuitive delay-sensitive model.

4.4.2.4 Multi-leader Delay-Sensitive Model

Another observation in the intuitive delay-sensitive model is that only a single MCU satisfies RUs' content requests. If multiple MCUs cooperatively transmit contents to RUs simultaneously, the waiting time for each RU is reduced. Therefore, we extend to the case where multiple MCUs assist content transmission.

Assume there are M MCUs denoted by $\mathcal{M} = \{m_1, m_2, \cdots, m_M\}$. Each RU is assigned to the nearest MCU. Denote $I_{i,m} = 0, 1, i \in \mathcal{N}, m \in \mathcal{M}$ as the connection indicator between RU i and MCU m. In particular, $I_{i,m} = 1$ implicits MCU m transmits contents to RU i. Otherwise, there is no connection between them. Meanwhile, each RU is restricted to connect one MCU whereas each MCU serves multiple RUs, $\sum_{m\in\mathcal{M}} I_{i,m} = 1$. All the $I_{i,m}$ compose a indicator matrix $\mathbf{I}$. Given the locations of both RUs and MCUs, the indicator matrix is known. Denote the number of RUs served by the MCU $m_i, i = 1, 2, \cdots, M$ as n_{m_i}. To ease the description, we put the RUs served by the same MCU together and reorder the RU set as $\mathcal{N} = \{x_1, \cdots, x_{n_{m_1}}, x_{n_{m_1}+1}, \cdots, x_{n_{m_1}+n_{m_2}}, \cdots, x_N\}$ with $\sum_{m_i\in\mathcal{M}} n_{m_i} = N$.

Because the introduction of multiple MCUs divides RUs into smaller piles whereas the $M/G/1$ queue model adapts to the case with a large number of RUs better. Taking the indicator matrix $\mathbf{I}$ into consideration, we model the utilities based on the intuitive delay-sensitive model instead of the queue model. The utility of each RU is,

$$\tilde{u}_i\left(\tilde{x}_i, \tilde{\mathbf{x}}_{-i}, \tilde{\mathbf{p}}\right) = a_i\tilde{x}_i - \frac{1}{2}b_i\tilde{x}_i^2 + \sum\nolimits_{j\in\mathcal{N}} g_{ij}\tilde{x}_i\tilde{x}_j - \frac{1}{2}\tilde{d}\sum_{m=1}^{M} I_{i,m}\left(\sum\nolimits_{j\in\mathcal{N}} I_{j,m}\tilde{x}_j\right)^2 - \sum_{m=1}^{M}\tilde{p}_m\tilde{x}_i, \forall i \tag{4.9}$$

where $\tilde{\mathbf{p}} = \{p_1\mathbf{1}_{n_{m_1}}^T, p_2\mathbf{1}_{n_{m_2}}^T, \cdots, p_M\mathbf{1}_{n_{m_M}}^T\}^T$ is the unit payment vector corresponding to each RU. Specifically, $\mathbf{1}_{n_{m_i}}$ represents $n_{m_i} \times 1$ vector with 1s, and $\tilde{p}_m$ is the unit payment at the MCU m. Since MCUs serve different RU piles, their unit payments are different.

Accordingly, the revenue of each MCU is,

$$\tilde{R}_m\left(\tilde{\mathbf{x}}, \tilde{p}_m\right) = \sum\nolimits_{i \in \mathcal{N}} \left(\tilde{p}_m - c\right) I_{i,m} \tilde{x}_i, \forall m \in \mathcal{M} \tag{4.10}$$

Because all MCUs cooperate to offload data, they aim to achieve the maximum total revenue,

$$\tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right) = \sum\nolimits_{m \in \mathcal{M}} \sum\nolimits_{i \in \mathcal{N}} \left(\tilde{p}_m - c\right) I_{i,m} \tilde{x}_i. \tag{4.11}$$

4.5 Utility Maximization in Delay-tolerant Model

4.5.1 Overview

In game theory, Stackelberg game [58] is a tool to model the scenario where a hierarchy of actions exists between two types of players: one is the leader, and the other is the follower. The leader makes its move first. After the leader chooses a strategy, the follower always chooses the best response strategy that maximizes its utility. Knowing this reaction from the follower, the leader strategically chooses a strategy to maximize its utility. This optimal strategy of the leader, together with the corresponding best response strategy of the follower, constitutes a Stackelberg equilibrium. At a Stackelberg equilibrium, no follower has an incentive to adjust its strategy unilaterally.

The communication between the MCU and RUs in the delay-tolerant scenario can be formulated as such a two-stage Stackelberg game, named as Utility Maximization game in delay-tolerant (UMDT).

Stage I (Unit Payment) The MCU chooses a unit payment p^* to maximize the total revenue R,

$$p^* = \arg \max_{p \in [0,\infty)} \sum\nolimits_{i \in \mathcal{N}} x_i (p - c)$$

Stage II (Requested Content Level) Each RU $i \in \mathcal{N}$ chooses a requested content level x_i to maximize the utility $u_i\left(x_i, \mathbf{x}_{-i}, p\right)$ given the unit payment p and the requested content levels of others $\mathbf{x}_{-i}$,

$$x_i^* = \arg \max_{x_i \in [0,\infty)} u_i\left(x_i, \mathbf{x}_{-i}, p\right), \forall i$$

In the UMDT game, the MCU is the leader with the unit payment p^* as the strategy and RUs are the followers. The strategy of RU i is the requested content level x_i^*, $\forall i$. Due to each

RU is selfish, the game in Stage II is considered as a non-cooperative game, which we call Request Level Determination (RLD) game. Given the UMDT formulation, we are interested in the following questions:

- Q1: For a given unit payment p, is there a profile of stable strategies in the RLD game such that no RU can increase the utility by unilaterally changing his current strategy?
- Q2: If the answer to Q1 is affirmative, is the stable strategy profile unique? When it is unique, RUs will be guaranteed to select the strategies in the same stable strategy profile.
- Q3: How can the MCU select the value of p to maximize the total revenue?

The stable strategy profile in Q1 corresponds to the concept of Nash equilibrium [58].

DEFINITION 4. *Nash equilibrium: A profile of strategies* $\mathbf{x}^*$ *is a Nash equilibrium of the RLD game if for any mobile RU i*

$$u_i(x_i^*, \mathbf{x}_{-i}^*, p) \geq u_i(x_i, \mathbf{x}_{-i}^*, p) \tag{4.12}$$

for any $x_i \geq 0$*, where* u_i *is defined in (4.1).*

The existence (Q1) and uniqueness (Q2) of a stable Nash equilibrium strategy profile not only ensure that no RU has an incentive to make a change unilaterally but also allow the MCU to predict the behaviors of RUs and thus to select the optimal unit payment. The answer to Q3 depends heavily on those to Q1 and Q2. Stackelberg equilibrium, which is the final solution to the UMDT game, consists of the optimal solution computed in Q3 and the corresponding strategies at the Nash equilibrium in the RLD game.

4.5.2 RU Utility Maximization

Backward reduction methods [58] are deployed to maximize the utilities of both RUs and MCUs. We answer above Q1 and Q2 first, followed by an algorithm to find the RUs' best response strategies in the RLD game.

DEFINITION 5. *Best Response Strategy: Given* p *and* $\mathbf{x}_{-i}$*, a strategy is RU i's best response strategy, denoted by* $\beta_i(\mathbf{x}_{-i})$*, if it maximizes the utility function* $u_i(x_i, \mathbf{x}_{-i}, p)$ *in (4.1), over all* $x_i \geq 0$*.*

Based on the definition of Nash equilibrium, every RU plays his best response strategy at a Nash equilibrium. By setting the derivative $\frac{\partial u_i(x_i,\mathbf{x_{-i}},p_i)}{\partial x_i}=0$ as the first order condition in (4.1), we obtain the RU i's best response strategy,

$$\beta_i\left(\mathbf{x}_{-i}\right)=\max\left\{0,\frac{a_i-p}{b_i}+\sum\nolimits_{j\neq i}\frac{g_{ij}}{b_i}x_j\right\},\forall i \tag{4.13}$$

in which the max operation is to ensure RU i's strategy non-negative. Each RU's best response strategy consists of two parts: internal demand $(a_i-p)/b_i$ which is independent of other RUs, and external demand $\sum_{j\neq i}\frac{g_{ij}}{b_i}x_j$ indicating the social effect other RUs bring to the RU i. The coefficient g_{ij}/b_i represents the marginal increase of RU i's requested content level when RU j's requested content level increases. It implies that the increase of other RUs' strategies has a positive impact on the RU i's strategy.

4.5.2.1 Existence and Uniqueness of RUs' Best Response Strategies — the Answers to Q1 and Q2

Since each RU has a great incentive to unboundedly increase the requested content levels provided other RUs' request levels are sufficiently large, the Nash equilibrium cannot be ensured to exist. To circumvent such situation, we give a general assumption under which a Nash equilibrium exists.

***Assumption* 1.** $\sum_{j\neq i}\frac{g_{ij}}{b_i}<1,\forall i.$

The Assumption 1 is a sufficient condition for the existence of RUs‘ best response strategies. Assume that the maximum requested content level among all the other RUs is $x_j^{'}$. Under the Assumption 1, the external demand is $\sum_{j\neq i}\frac{g_{ij}}{b_i}x_j\leq\sum_{j\neq i}\frac{g_{ij}}{b_i}x_j^{'}<x_j^{'}$. It implies that the social effect experienced by an RU from others is limited to the largest effect this RU can experience from an individual of the other RUs.

Theorem 3. *Under Assumption 1, the RLD game in Stage II always admits a Nash equilibrium for RUs.*

To prove Theorem 3, the main idea is to show that our RLD game with unbounded content levels is equivalent to a game with bounded content levels that admits a Nash equilibrium. We prove it in the following.

Proof: In the RLD game $\mathcal{G} = \left\{\mathcal{N}, \{u_i\}_{i\in\mathcal{N}}, [0,\infty]^N\right\}$, we denote $\mathbf{x}^*$ as a strategy profile and x_i^* as the largest requested content level in it, i.e., $x_i^* > x_j^*, \forall j \neq i$. Based on (4.13), when $x_i^* > 0$,

$$x_i^* = \frac{a_i - p}{b_i} + \sum\nolimits_{j\neq i} \frac{g_{ij}}{b_i} x_j^* \leq \frac{|a_i - p|}{b_i} + \sum\nolimits_{j\neq i} \frac{g_{ij}}{b_i} x_i^*$$

from which we get $x_i^* \leq |a_i - p| / (b_i - \sum_{j\neq i} g_{ij}) \leq \tilde{x}$. $\tilde{x}$ is any number that satisfies $\tilde{x} \geq \max_{i\in\mathcal{N}} |a_i - p| / (b_i - \sum_{j\neq i} g_{ij})$. Since x_i^* is the largest content level, all the content levels in game $\mathcal{G}$ are bounded, i.e., $x_j^* \in [0, \tilde{x}], j \in \mathcal{N}$. Therefore, our game $\mathcal{G}$ is equivalent to a new game $\tilde{\mathcal{G}} = \left\{\mathcal{N}, \{u_i\}_{i\in\mathcal{N}}, [0,\tilde{x}]^N\right\}$ that has the same Nash equilbium stategy profile.

Taking the game $\tilde{\mathcal{G}}$ into consideration, the strategy space $[0,\tilde{x}]^N$ is compact and convex. The utility function $u_i(x_i, \mathbf{x_{-i}}, p)$ is continuous in x_i and $\mathbf{x}_{-i}$. The second-order derivative of RU i's utility function $\frac{\partial^2 u_i(x_i,\mathbf{x_{-i}},p)}{\partial^2 x_i} = -b_i$ is negative. Therefore, it is a concave game and admits a Nash equilibrium [50, 153]. Hence, the Nash equilibrium for our RLD game $\mathcal{G}$ exists. □

Theorem 4. *Under Assumption 1, the RLD game in Stage II has a unique best response strategy.*

According to [153], to prove Theorem 4, we try to demonstrate that the RLD game is a concave game.

Proof: The Jacobian matrix $\nabla\mathbf{u}(\mathbf{x})$ of RUs' utility profile $\mathbf{u}(\mathbf{x}) \triangleq \{u_1(\mathbf{x}), u_2(\mathbf{x}), \cdots, u_N(\mathbf{x})\}$ is given by $\nabla\mathbf{u}(\mathbf{x}) = -(\mathbf{\Lambda} - \mathbf{G})$,

where $\mathbf{\Lambda} = \mathrm{diag}(b_1, b_2, \cdots, b_N)$ and $\mathbf{G} = \begin{bmatrix} 0 & g_{12} & \cdots & g_{1N} \\ g_{21} & 0 & \cdots & g_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N1} & g_{N2} & \cdots & 0 \end{bmatrix}$. The ij-th element in $\mathbf{G}$, denoted by g_{ij}, represents the social effect that RU j brings to RU i, $j \neq i$. According to Assumption 1,

$$[\mathbf{\Lambda} - \mathbf{G}]_{ii} > \sum_{j\neq i} \left|[\mathbf{\Lambda} - \mathbf{G}]_{ij}\right|, \forall i$$

where $[\mathbf{\Lambda} - \mathbf{G}]_{ij}$ denotes the element in the ith row and jth column in the matrix $[\mathbf{\Lambda} - \mathbf{G}]$. Hence, $[\mathbf{\Lambda} - \mathbf{G}]$ is strictly diagonal dominant. Assume social effect between RUs is symmetric, $g_{ij} = g_{ji}, \forall i, j \in \mathcal{N}$, $[\mathbf{\Lambda} - \mathbf{G}]^T$ is also strictly diagonal dominant. Therefore, $\nabla\mathbf{u}(\mathbf{x}) + \nabla\mathbf{u}^T(\mathbf{x}) = -[\mathbf{\Lambda} - \mathbf{G}] - [\mathbf{\Lambda} - \mathbf{G}]^T$ is strictly diagonal dominant and symmetric. According to [82], a symmetric matrix that is strictly diagonally dominant with real nonnegative diagonal elements is positive definite. Thus,

$-\left[\mathbf{\Lambda}-\mathbf{G}\right]-\left[\mathbf{\Lambda}-\mathbf{G}\right]^T$ is negative definite since the elements in it are negative. $\nabla\mathbf{u}(\mathbf{x})$ is diagonally strictly concave [153]. The RLD game has a unique Nash equilibrium. □

4.5.2.2 Calculation of RUs' Best Response Strategies

We propose an algorithm to calculate RUs' best response strategies as shown in Algorithm 5.

```
Algorithm 5: Calculate the RUs' Best Response Strategies
   Input: precision threshold $\epsilon$
   Output: $\mathbf{x}^*$
1  $x_i^{(0)} \leftarrow 0, \forall i \in \mathcal{N}$; $n \leftarrow 1$;
2  for $j = 1; j \leq N$ do
3      $x_i^{(n)} = \max\left\{0, \frac{a_i - p}{b_i} + \sum_{j \neq i} \frac{g_{ij}}{b_i} x_j^{(n-1)}\right\}$;
4  end
5  if $||\mathbf{x}^{(n)} - \mathbf{x}^{(n-1)}|| < \epsilon$ then
6      $\mathbf{x}^* = \mathbf{x}^{(n)}$;
7      break;
8  else
9      $n = n + 1$;
10     go back to 2;
11 end
12 return $\mathbf{x}^*$;
```

Theorem 5. *Algorithm 5 calculates the Nash equilibrium in the RLD game.*

To prove Theorem 5, the key is to prove that the best response strategy for each user is converged.

Proof: Let $\Delta x_i^{(n)} \triangleq x_i^{(n)} - x_i^*, \forall i$. According to step 3 in Algorithm 5,

$$|\Delta x_i^{(n)}| \leq \left|\sum_{j \neq i} \frac{g_{ij}}{b_i} \Delta x_j^{(n-1)}\right| \leq \sum_{j \neq i} \frac{g_{ij}}{b_i} \left|\Delta x_j^{(n-1)}\right|, \forall i \tag{4.14}$$

Denote $||\Delta x_i^{(n)}||_\infty$ as the l_∞-norm of vector $(\Delta x_1^{(n)}, \Delta x_2^{(n)}, \cdots, \Delta x_N^{(n)})$, $||\Delta x_i^{(n)}||_\infty = \max\limits_{i \in \mathcal{N}}(\Delta x_1^{(n)}, \Delta x_2^{(n)}, \cdots, \Delta x_N^{(n)})$. According to (12), $||\Delta x_i^{(n)}||_\infty \leq \max\limits_{i \in \mathcal{N}} \sum_{j \neq i} \frac{g_{ij}}{b_i} \left|\Delta x_j^{(n-1)}\right| \leq \left(\max\limits_{i \in \mathcal{N}} \sum_{j \neq i} \frac{g_{ij}}{b_i}\right) ||\Delta x_i^{(n-1)}||_\infty$. Since $\max\limits_{i \in \mathcal{N}} \sum_{j \neq i} \frac{g_{ij}}{b_i} < 1$, $||\Delta x_i^{(n)}||_\infty \leq ||\Delta x_i^{(n-1)}||_\infty$. It implies that Algorithm 5 results in a contraction mapping of $||\Delta x_i^{(n-1)}||_\infty$ and thus converges to the Nash equilibrium. □

To ease the description, we express the best response strategies in a matrix format.

***Lemma* 1.** *Denote $\mathcal{S}$ as the set of RUs with positive strategies and $\mathcal{N}-\mathcal{S}$ as the set of other RUs: $\mathcal{S}=\{i|x_i^*>0\}$ and $\mathcal{N}-\mathcal{S}=\{i|x_i^*=0\}$, the best response strategies are:*

$$\mathbf{x}_{\mathcal{S}}^* = \left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}\left(\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}\right) \tag{4.15}$$

$$\mathbf{x}_{\mathcal{N}-\mathcal{S}}^* = \mathbf{0}_{\mathcal{N}-\mathcal{S}} \tag{4.16}$$

where $\mathbf{x}_{\mathcal{S}}^* = \{x_i^*|i\in\mathcal{S}\}$, $\mathbf{x}_{\mathcal{N}-\mathcal{S}}^* = \{x_i^*|i\in\mathcal{N}-\mathcal{S}\}$ and $\mathbf{a}_{\mathcal{S}} = \{a_i|i\in\mathcal{S}\}$. The matrices $\mathbf{\Lambda}_{\mathcal{S}}, \mathbf{G}_{\mathcal{S}}$ are $|\mathcal{S}|\times|\mathcal{S}|$ matrices with elements in $\mathbf{\Lambda}, \mathbf{G}$ with indices in $\mathcal{S}\times\mathcal{S}$, respectively. The vectors $\mathbf{1}_{\mathcal{S}}$ and $\mathbf{0}_{\mathcal{N}-\mathcal{S}}$ are $|\mathcal{S}|\times 1$ and $|\mathcal{N}-\mathcal{S}|\times 1$ vectors with 1s and 0s, respectively.

To prove Lemma 1, the important part is to show that $\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}$ is invertible.

Proof: According to (4.13) and Algorithm 5,

$$x_i^* = \frac{a_i - p}{b_i} + \sum_{j\neq i}\frac{g_{ij}}{b_i}x_j^*, i, j \in \mathcal{S} \tag{4.17}$$

The matrix format of (4.17) is,

$$\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)\mathbf{x}_{\mathcal{S}}^* = \left(\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}\right) \tag{4.18}$$

Because $\mathbf{\Lambda}_{\mathcal{S}}$ is a positive diagonal matrix, it is invertible. Denote any eigenvalue and the corresponding eigenvector of $\mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}$ as λ and μ, respectively. Mathematically, $\left(\mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}\right)\mu = \lambda\mu$. Assume μ_i is the largest element in absolute value, $|\mu_i| \geq |\mu_j|, \forall j\neq i$,

$$\begin{aligned} |\lambda\mu_i| = \left|\sum_{j\in\mathcal{N}}\left[\mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}\right]_{ij}\mu_j\right| &\leq \sum_{j\in\mathcal{N}}\left|\left[\mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}\right]_{ij}\right||\mu_j| \\ &\leq |\mu_i|\sum_{j\in\mathcal{N}}\tfrac{|g_{ij}|}{b_i} < |\mu_i| \end{aligned} \tag{4.19}$$

From (4.19), the absolute values of all eigenvalues of $\mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}$ are less than 1. Since the eigenvalue values of the matrix $\mathbf{I} - \mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}$ are equaled to $1-\lambda$, the matrix $\mathbf{I} - \mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}_{\mathcal{S}}$ does not have 0 eigenvalues. Thus, $\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}} = \mathbf{\Lambda}_{\mathcal{S}}\left(\mathbf{I} - \mathbf{\Lambda}_{\mathcal{S}}^{-1}\mathbf{G}\right)$ is invertible and $\mathbf{x}_{\mathcal{S}}{}^* = \left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}\left(\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}\right)$. □

4.5.2.3 Discussion on social effect

Proposition 1. *For the RLD game, when $a_i = a > p$ and the social effect is symmetric, $g_{ij} = g_{ji}, \forall i \neq j$, the social relationship between RUs brings a positive effect to Nash equilibrium.*

To prove Proposition 1, the main idea is to show that the total requested content level at the Nash equilibrium increases when g_{ij} increases. In addition, the performance under asymmetric social effect will be shown to be similar with that under symmetric social effect.

Proof: From (4.17), we find that RUs' strategies at the Nash equilibrium is a continuous function of the matrix G_S. Thus, we can find a matrix $G_S^{'}$, in which $g_{ij}^{'} \geq g_{ij}, g_{ij}^{'} \in G_S^{'}, g_{ij} \in G_S$ and at least one strictly inequality exists, such that RUs with positive strategies $\mathbf{x}_{\mathcal{S}}^{*'}$ at the Nash equilibrium under $G_S^{'}$ are also in the set $\mathcal{S}$. According to (4.18),

$$\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)\mathbf{x}_{\mathcal{S}}^{*} = \left(\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}\right) \tag{4.20}$$

$$\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}^{'}\right)\mathbf{x}_{\mathcal{S}}^{*'} = \left(\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}\right) \tag{4.21}$$

Subtract (4.20) from (4.21),

$$\mathbf{x}_{\mathcal{S}}^{*'} - \mathbf{x}_{\mathcal{S}}^{*} = \left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}\Delta\mathbf{G}_{\mathcal{S}}\mathbf{x}_{\mathcal{S}}^{*'} \tag{4.22}$$

where $\Delta\mathbf{G}_{\mathcal{S}} = \mathbf{G}_{\mathcal{S}}^{'} - \mathbf{G}_{\mathcal{S}}$. Thus, the total difference between $\mathbf{x}_{\mathcal{S}}^{*'}$ and $\mathbf{x}_{\mathcal{S}}^{*}$ is

$$\mathbf{1}_{\mathcal{S}}^{T}\left(\mathbf{x}_{\mathcal{S}}^{*'} - \mathbf{x}_{\mathcal{S}}^{*}\right) = \mathbf{1}_{\mathcal{S}}^{T}\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}\Delta\mathbf{G}_{\mathcal{S}}\mathbf{x}_{\mathcal{S}}^{*'} \tag{4.23}$$

According to $\mathbf{x}_{\mathcal{S}}^{*} = \left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}(a-p)\mathbf{1}_{\mathcal{S}}$ in (4.15), it follows that,

$$\mathbf{1}_{\mathcal{S}}^{T}\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1} = \left(\left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1}\mathbf{1}_{\mathcal{S}}\right)^{T} = \frac{1}{a-p}\mathbf{x}_{\mathcal{S}}^{*T} \tag{4.24}$$

Substitute (4.24) into (4.23), we get the total difference as,

$$\mathbf{1}_{\mathcal{S}}^{T}\left(\mathbf{x}_{\mathcal{S}}^{*'} - \mathbf{x}_{\mathcal{S}}^{*}\right) = \frac{1}{a-p}\mathbf{x}_{\mathcal{S}}^{*T}\Delta\mathbf{G}_{\mathcal{S}}\mathbf{x}_{\mathcal{S}}^{*'} \tag{4.25}$$

Because $a > p$, $\mathbf{x}_{\mathcal{S}}^{*'}, \mathbf{x}_{\mathcal{S}}^{*} \succ 0$ and $\Delta\mathbf{G}_{\mathcal{S}} \succeq 0$, the total difference between $\mathbf{x}_{\mathcal{S}}^{*'}$ and $\mathbf{x}_{\mathcal{S}}^{*}$, $\mathbf{1}_{\mathcal{S}}^{T}\left(\mathbf{x}_{\mathcal{S}}^{*'} - \mathbf{x}_{\mathcal{S}}^{*}\right) > 0$, which implies that the total requested content levels at the Nash equilibrium increase when g_{ij} increases. The Proposition 1 verifies that the social effect between RUs with similar social attributes makes RUs get more interested contents. □

4.5.3 The MCU Revenue Maximization

According to the above analysis, the MCU, as a leader, knows there exists the unique Nash equilibrium for the RUs given any unit payment. Hence, he can maximize the total revenue by choosing the optimal unit payment.

4.5.3.1 The Impact of Unit payment

We first take the case with two RUs as an example. Without loss of generality, assume $a_1 > a_2$. Intuitively, in (4.13), both RU 1 and RU 2 have positive strategies when the unit payment p is in a low price regime. Their strategies are,

$$\begin{cases} x_1 = \dfrac{a_1 - p}{b_1} + \dfrac{g_{12}}{b_1} x_2 & \text{(4.26a)} \\ x_2 = \dfrac{a_2 - p}{b_2} + \dfrac{g_{21}}{b_2} x_1 & \text{(4.26b)} \end{cases}$$

By solving above equations, we get the value of x_1 and x_2,

$$x_1 = \frac{(a_1 - p)b_2 + (a_2 - p)g_{12}}{b_1 b_2 - g_{12} g_{21}} \tag{4.27}$$

$$x_2 = \frac{(a_2 - p)b_1 + (a_1 - p)g_{21}}{b_1 b_2 - g_{12} g_{21}} \tag{4.28}$$

which show that the strategies of both RU 1 and RU 2 decrease as p increases. Based on the Assumption 1, $x_1 > x_2$. Thus, when increasing p, the strategy of RU 2, x_2, first decreases to 0. Denote the unit payment as p_{th} at which RU 2's best response strategy is decreased to 0. According to (4.28), $p_{th} = \frac{a_2 b_1 + a_1 g_{21}}{b_1 + g_{21}}$. Continuing to increase p, the strategy of RU 1 then decreases to 0. Therefore, we have the Proposition 2.

Proposition 2. *In RLD game, the impact that p brings to the two RUs' best response strategies $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$ is as follows*

- *When we set p in a low regime: $0 \leq p < p_{th}$, the best response strategies of two RUs are listed in (4.27) and (4.28);*
- *When we set p in a medium regime: $p_{th} \leq p < a_1$, $x_1 = \frac{a_1 - p}{b_1}$ and $x_2 = 0$;*
- *When we set p in a high regime; $p \geq a_1$, RUs will not pick up their strategies: $x_1 = x_2 = 0$.*

Based on the Assumption 1, $p_{th} = \frac{a_2 b_1 + a_1 g_{21}}{b_1 + g_{21}} > a_2$. It implies that RU 2 would like to take part in the game ($x_2 \in 0$) although the unit payment he has to pay is larger than the internal effect. This gives the credits to the social effect that RU 1 brings to, which verifies that social effect brings benefits in our scheme.

Next, we extend our discussion on the impact of p to a general case where more RUs request contents.

Proposition 3. *In RLD game, the impact that p brings to the RUs' best response strategies $\mathbf{x}^*$ is as follows*

- *When we set p in a low regime $0 \leq p \leq \max\limits_{i \in \mathcal{M}} a_i$: there is a set of prices $p_0 \triangleq 0 < p_1 < p_2 < \cdots < p_M < p_{M+1} \triangleq \max\limits_{i \in \mathcal{N}} a_i$. For each $k \in \{0, 1, 2, \cdots, M\}$, there is a set $S_k \subseteq \mathcal{N}$ such that for any $p \in [p_k, p_{k+1}]$ such that $x_i^* = \left[\left(\mathbf{\Lambda}_{S_k} - \mathbf{G}_{S_k} \right)^{-1} \left(\mathbf{a}_{S_k} - p \mathbf{1}_{S_k} \right) \right]_i, \forall i \in S_k$ and $x_i^* = 0, \forall i \notin S_k$*
- *When we set p in a high regime $p \geq \max\limits_{i \in \mathcal{N}} a_i$, $x_i^* = 0, \forall i$*

We prove Proposition 3 in the following. It shows that each RU' best response strategy is a piecewise linear function of the price, which motivates us to propose the Algorithm 6 to calculate the MCU's optimal revenue.

Proof: For any unit payment $p \in [0, \max_{i \in \mathcal{N}} a_i]$, the requested content levels of the set of RUs $\mathcal{S}$ with positive strategies are given in (4.15). Meanwhile, according to (4.13), RU i's the requested content level $x_i^* = \frac{a_i - p}{b_i} + \sum_{j \neq i} \frac{g_{ij}}{b_i} x_j^*$ is continuous in p and RU j's requested content level x_j^*, $j \neq i$. When the unit payment p increases a small amount to $p^{'}$, the set of RUs with positive strategies at the Nash equilibrium does not change and their strategies are still given by (4.15) except that p is replaced by $p^{'}$. Hence, the set of RUs with positive strategies is the same at any unit payment in a continuous unit payment interval. However, when the unit payment p increases a large amount to p'', some RUs' strategies decrease to 0 and thus they would not request any contents as shown in above two-RU example. Therefore, the interval of the unit payment is piecewise.

Assuming RU i has a maximized strategy $x_i^* > 0$ when $p \geq \max\limits_{i \in \mathcal{N}}$. According to (4.13), $x_i^* = \frac{a_i - p}{b_i} + \sum_{j \neq i} \frac{g_{ij}}{b_i} x_j^* \leq \sum_{j \neq i} \frac{g_{ij}}{b_i} x_j^* \leq \sum_{j \neq i} \frac{g_{ij}}{b_i} x_i^* < x_i^*$, which is a contradiction. Therefore, $x_i^* = 0, \forall i$ when $p \geq \max\limits_{i \in \mathcal{N}}$. □

4.5.3.2 Calculation of the MCU's Optimal Revenue — the Answer to Q3

Based on the Lemma 1, the piecewise unit payment p is linear with the total best response strategies $\mathbf{1}^T \mathbf{x}^*$ at the Nash equilibrium. Hence, the total revenue of the MCU $(p - c)\mathbf{1}^T \mathbf{x}^*$ is a quadratic function with the unit payment p according to (4.2). Given above characteristics, we propose the Algorithm 6. Inspired by PROPOSITION 3, we first determine the unit payment interval in which the set of RUs with positive strategies does not change when the unit payment increases or decreases. Within each determined unit payment interval, we calculate the optimal unit payment to maximize the total revenue of the MCU. Finally, by comparing total revenues in each interval, we obtain the final unit payment, which makes largest total revenue for the MCU. The final unit payment, together with the corresponding RUs' requested content levels, composes the Stackelberg equilibrium.

Specifically, the Algorithm 6 is initialized by calculating the RUs' best response strategies when the unit payment $p = 0$, as shown in Step 1. From Step 3 to Step 7, it finds the set $\mathcal{S}$ composed of RUs with positive strategies, which serves the initial conditions in the following steps. As the unit payment p increases from 0 to $\max\limits_{i \in \mathcal{N}} a_i$, it iteratively finds the critical unit payment at which the set $\mathcal{S}$ changes as illustrated from Step 10 to Step 22. Because the change of the set means either adding or dropping an eligible RU, the process of finding the critical unit payment can be divided into the following three parts:

- Step 10 to Step 15 investigates the critical unit payment in the set $\mathcal{S}$, which makes at least one RU's positive strategy decreases to 0. Since RU i is in the set $\mathcal{S}$, according to (4.15), his positive strategy x_i is,

$$x_i = \left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}} (\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}) > 0 \tag{4.29}$$

where $\left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}}$ denotes a $1 \times |\mathcal{S}|$ vector with elements in the ith row of the matrix $(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}$ and the columns with indices in $\mathcal{S}$. If $\left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}} \mathbf{1}_{\mathcal{S}} > 0$, the RU i's positive strategy decreases as p increases. Assuming when the unit payment increases to $\hat{p}_i$,

Algorithm 6: Calculate the MCU's Optimal Revenue

```
Input: none
Output: $p^*$, $\mathbf{x}^*$,$r^*$
calculate the Nash equilibrium $\mathbf{x}^{*'}$ using Algorithm 5 when the unit payment is 0;
$\underline{p} \leftarrow 0$; $p^* \leftarrow 0$; $r^* \leftarrow 0$; $\mathcal{S} \leftarrow \emptyset$;
for $i = 1, i \leq N$ do
    if $x_i^{*'} > 0$ then
        $\mathcal{S} \leftarrow \mathcal{S} \bigcup \{i\}$ ;
    end
end
while $\underline{p} \leq \max\limits_{i \in \mathcal{N}} a_i$ and $\mathcal{S} \neq \emptyset$ do
    $\mathcal{S}_1 \leftarrow \emptyset$; $\mathcal{S}_2 \leftarrow \emptyset$;
    foreach $i \in \mathcal{S}$ do
        if $\left[(\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1}\right]_i \mathbf{1}_\mathcal{S} > 0$ then
            $\mathcal{S}_1 \leftarrow \mathcal{S}_1 \bigcup \{i\}$;
            $\hat{p}_i \leftarrow \frac{\left[(\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1}\right]_i \mathbf{a}_\mathcal{S}}{\left[(\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1}\right]_i \mathbf{1}_\mathcal{S}}$;
        end
    end
    foreach $i \in \mathcal{N} - \mathcal{S}$ do
        if $[\mathbf{G}]_{i,\mathcal{S}} (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{1}_\mathcal{S} < -1$ then
            $\mathcal{S}_2 \leftarrow \mathcal{S}_2 \bigcup \{i\}$;
            $\hat{p}_i \leftarrow \frac{[\mathbf{G}]_{i,\mathcal{S}} (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{a}_\mathcal{S} + a_i}{[\mathbf{G}]_{i,\mathcal{S}} (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{1}_\mathcal{S} + 1}$;
        end
    end
    $\overline{p} = \min\limits_{i \in \mathcal{S}_1 \cup \mathcal{S}_2} \hat{p}_i$;
    $k = \arg_{i \in \mathcal{S}_1 \cup \mathcal{S}_2} \overline{p}$;
    $p^{'} = \frac{\mathbf{1}_\mathcal{S}^T (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{a}_\mathcal{S} + c \mathbf{1}_\mathcal{S}^T (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{1}_\mathcal{S}}{2 \mathbf{1}_\mathcal{S}^T (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} \mathbf{1}_\mathcal{S}}$;
    if $p^{'} \in \left[\underline{p}, \overline{p}\right]$ then
        $\widetilde{p} = p^{'}$;
    else if $p^{'} < \underline{p}$ then
        $\widetilde{p} = \underline{p}$;
    else
        $\widetilde{p} = \overline{p}$;
    end
    $\widetilde{r} = (\widetilde{p} - c) \mathbf{1}_\mathcal{S}^T (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} (\mathbf{a}_\mathcal{S} - \widetilde{p} \mathbf{1}_\mathcal{S})$;
    if $\widetilde{r} > r^*$ then
        $p^* \leftarrow \widetilde{p}$;$r^* \leftarrow \widetilde{r}$; $\mathbf{x}_\mathcal{S}^* = (\mathbf{\Lambda}_\mathcal{S} - \mathbf{G}_\mathcal{S})^{-1} (\mathbf{a}_\mathcal{S} - p^* \mathbf{1}_\mathcal{S})$; $\mathbf{x}_{\mathcal{N}-\mathcal{S}}^* = \mathbf{0}_{\mathcal{N}-\mathcal{S}}$, $\mathbf{x}^* = \mathbf{x}_\mathcal{S}^* \bigcup \mathbf{x}_{\mathbf{N-S}}^*$;
    end
    $\underline{p} \leftarrow \widetilde{p}$;
    if $k \in \mathcal{S}$ then
        $\mathcal{S} = \mathcal{S} \backslash \{k\}$;
    else
        $\mathcal{S} = \mathcal{S} \cup \{k\}$;
    end
end
return $p^*, \mathbf{x}^*, r^*$
```

the RU i's positive strategy x_i decreases to 0. We have,

$$\left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}} \mathbf{a}_{\mathcal{S}} = \hat{p}_i \left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}} \mathbf{1}_{\mathcal{S}}$$

$$\hat{p}_i = \frac{\left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{i,\mathcal{S}} \mathbf{a}_{\mathcal{S}}}{[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}]_{i,\mathcal{S}} \mathbf{1}_{\mathcal{S}}} \tag{4.30}$$

- Step 16 to 21 investigates the critical unit payment in the set $\mathcal{N} - \mathcal{S}$, which makes at least one RU's strategy become positive When RU i is in the set $\mathcal{N} - \mathcal{S}$, $x_i = 0 > \frac{a_i - p}{b_i} + \sum\limits_{j \neq i} \frac{g_{ij}}{b_i} x_j$. If $x_j > 0$, $x_j = \left[(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1}\right]_{j,\mathcal{S}} (\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}})$. Denote $\mathbf{G}_{i,S}$ as a $1 \times |\mathcal{S}|$ vector composed of the element of the ith row of the matrix $\mathbf{G}$ with column indices in $\mathcal{S}$,

$$\begin{aligned} x_i = 0 > \tfrac{a_i - p}{b_i} + \tfrac{1}{b_i} [\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} (\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}) \\ = \tfrac{1}{b_i} [\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{a}_{\mathcal{S}} + \tfrac{a_i}{b_i} - \tfrac{p}{b_i} \left([\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{1}_{\mathcal{S}} + 1 \right) \end{aligned}$$

  If $[\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{1}_{\mathcal{S}} < -1$, $\frac{a_i - p}{b_i} + \frac{1}{b_i} [\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} (\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}})$ increases as p decreases. It becomes positive when the unit payment decreases to,

$$\hat{p}_i = \frac{[\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{a}_{\mathcal{S}} + a_i}{[\mathbf{G}]_{i,S} (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{1}_{\mathcal{S}} + 1} \tag{4.31}$$

- By comparing both the critical unit payments in set $\mathcal{S}$ and $\mathcal{N} - \mathcal{S}$, we choose the minimized one as the final critical unit payment as illustrated in Step 22.

From Step 24 to Step 31, we calculate the unit payment $\widetilde{p} \in \left[\underline{p}, \overline{p}\right]$ such that the MCU's revenue $R(\mathbf{x}, p)$ is maximized, in which $R(\mathbf{x}, p) = R(\mathbf{x}_{\mathcal{S}}, p) = \sum\limits_{i \in \mathcal{S}} x_i (p - c) = (p{-}c) \mathbf{1}_{\mathcal{S}}^T (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} (\mathbf{a}_{\mathcal{S}} - p\mathbf{1}_{\mathcal{S}}), p \in \left[\underline{p}, \overline{p}\right]$. By setting the first order derivative of $R(\mathbf{x}, p)$ to 0, we find the potential optimal unit payment $p^{'}$ in the interval $\left[\underline{p}, \overline{p}\right]$.

$$p^{'} = \frac{\mathbf{1}_{\mathcal{S}}^T (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{a}_{\mathcal{S}} + c\mathbf{1}_{\mathcal{S}}^T (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{1}_{\mathcal{S}}}{2\mathbf{1}_{\mathcal{S}}^T (\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}})^{-1} \mathbf{1}_{\mathcal{S}}} \tag{4.32}$$

if $p^{'} \in \left[\underline{p}, \overline{p}\right]$, the optimal unit revenue $\widetilde{p} = p^{'}$. Otherwise, the optimal unit payment is $\widetilde{p} = \underline{p}$ if

$p^{'} <= \underline{p}$, or $\widetilde{p} = \overline{p}$ if $p^{'} <= \overline{p}$. The local optimal revenue $r^{'}$ is,

$$r^{'} = (\widetilde{p} - c)\mathbf{1}_{\mathcal{S}}^{T} \left(\mathbf{\Lambda}_{\mathcal{S}} - \mathbf{G}_{\mathcal{S}}\right)^{-1} \left(\mathbf{a}_{\mathcal{S}} - \widetilde{p}\mathbf{1}_{\mathcal{S}}\right), \widetilde{p} \in \left[\underline{p}, \overline{p}\right] \tag{4.33}$$

Meanwhile, the set $\mathcal{S}$ is updated as shown from Step 37 to Step 41 by adding or deleting the RU k found in Step 23. The renewed set $\mathcal{S}$ is deployed to continue finding another local optimal unit payment.

Finally, by comparing the local optimal revenues in each unit payment interval, we find the global optimal revenue r^* and its corresponding unit payment p^* as illustrated in Step 32 to Step 35. The related RUs' best response strategies $\mathbf{x}^*$ are calculated.

4.6 Utility Maximization in delay-sensitive Model

In this section, we model the delay-sensitive cases as three two-stage Stackelberg games to maximize the utilities of RUs and MCUs, respectively. Specifically, the delay effect considered in the intuitive delay-sensitive model is essentially a specific form of the congestion effect studied in [65]. Therefore, we mainly discuss the other two delay-sensitive models.

4.6.1 Intuitive Delay-Sensitive Model

Refering to [64], the RU i's best response strategy is,

$$\beta_i\left(\overline{\mathbf{x}}_{-i}\right) = \max\left\{0, \frac{a_i - \overline{p}}{b_i + d} + \sum\nolimits_{j \neq i} \frac{g_{ij} - d}{b_i + d} x_j\right\}, \forall i \tag{4.34}$$

By comparing (4.13) and (4.34), each RU suffers both positive social effect and negative delay effect brought by other RUs. When $g_{ij} < d$, the RU j even brings negative external effect to the RU i. Otherwise, the RU j puts positive external effect. Under the assumption $\sum\limits_{j \neq i} \frac{|g_{ij} - d|}{(b_i + d)} < 1, \forall i$, the utility maximization is obtained according to Algorithm 3 in [64].

4.6.2 Queueing Delay-Sensitive Model

By setting the derivative $\frac{\partial \hat{u}_i(\hat{x}_i,\hat{\mathbf{x}}_{-\mathbf{i}},\hat{p})}{\partial \hat{x}_i} = 0$ in (4.8), the RU i's best response strategy is obtained as,

$$\beta_i\left(\hat{\mathbf{x}}_{-i}\right) = \max\left\{0, \frac{a_i - \hat{p}}{b_i + \hat{d}} + \sum_{j\neq i, j\in\mathcal{N}} \frac{g_{ij} - \frac{\hat{d}}{N-1}}{b_i + \hat{d}} x_j\right\} \tag{4.35}$$

where $\hat{d} = \frac{k\lambda}{N(1-\rho)}$ is assumed as a system parameter estimated by the SP. Comparing (4.34) and (4.35), given $\hat{d} = d$, the delay effect in the queueing delay-sensitive model is relieved from d to $\frac{d}{N-1}$, which theoretically proves that our queue model lowers the delay effect. Meanwhile, the content mean arrival rate λ brings a negative effect to RUs' utilities. It is because larger λ increases the queue length given the fixed average content transmission time and thus puts RUs to the longer waiting time. Similarly, the traffic intensity ρ puts a negative delay effect to RUs' utilities.

Since each RU's utility in (4.35) is similar to that in (4.13) and the MCU's utility keeps unchanged, we could simply apply the Algorithm 6 to obtaining the best strategies for both RUs and MCU under the following assumption:

***Assumption* 2.** $\sum_{j\neq i} \frac{|g_{ij} - \frac{\hat{d}}{N-1}|}{(b_i + \hat{d})} < 1, \forall i.$

4.6.3 Multi-leader Delay-Sensitive Model

Due to the participation of multiple MCUs, the previous single-leader Stackelberg game is extended to a multi-leader two-stage Stackelberg game as follows:

Stage I (Unit Payment) Each MCU announces its unit payment $\tilde{p}_m$ to maximize their total revenues,

$$\tilde{\mathbf{p}}* = \arg \max_{\tilde{p}\in[0,\infty)^M} \tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right)$$

Stage II (Requested Content Level) Each RU $i \in \mathcal{N}$ strategies the required content level $\tilde{x}_i$ to maximize his own utility given the price $\tilde{\mathbf{p}}$ and the requested content levels of others $\tilde{\mathbf{x}}_{-i}$,

$$\tilde{x}_i^* = \arg \max_{\tilde{x}_i\in[0,\infty)} \tilde{u}_i\left(\tilde{x}_i, \tilde{\mathbf{x}}_{-i}, \tilde{\mathbf{p}}\right), \forall i.$$

4.6.3.1 Utility Maximization for RUs

Similar with (4.13), the best response strategy for RU i is:

$$\beta_i\left(\tilde{\mathbf{x}}_{-i}, \tilde{\mathbf{p}}\right) = \max\left\{0, \frac{a_i - \sum\limits_{m=1}^{M} I_{i,m}\tilde{p}_m}{b_i + \tilde{d}} + \sum_{j\neq i, j\in\mathcal{N}} \frac{g_{ij} - \tilde{d}\sum\limits_{m=1}^{M} I_{i,m}I_{j,m}}{b_i + \tilde{d}} x_j\right\}$$

Formula (4.36) shows that the introduction of multiple MCUs reduces each RU's delay effect by serving them locally whereas does not affect their global positive social effect. With known indicator matrix, (4.36) is similar with (4.3). Therefore, if we have the following assumption, the existence and uniqueness can be proved referring to the previous proof.

***Assumption* 3.** $\sum_{j\neq i} \frac{|g_{ij} - \tilde{d}\sum\limits_{m=1}^{M} I_{i,m}I_{j,m}|}{(b_i+\tilde{d})} < 1, \forall i$

Meanwhile, under the Assumption 3, the best response strategies for all RUs given the unit payment vector are

$$\tilde{\mathbf{x}}_{\mathcal{S}}^{*} = \left(\tilde{\mathbf{\Lambda}}_{\mathcal{S}} - \tilde{\mathbf{G}}_{\mathcal{S}}\right)^{-1}\left(\mathbf{a}_{\mathcal{S}} - \tilde{\mathbf{p}}_{\mathcal{S}}\right) \tag{4.36}$$

$$\tilde{\mathbf{x}}_{\mathcal{N}-\mathcal{S}}^{*} = \mathbf{0}_{\mathcal{N}-\mathcal{S}} \tag{4.37}$$

The corresponding matrices $\tilde{\mathbf{\Lambda}} = \text{diag}(b_1 + \tilde{d}, b_2 + \tilde{d}, \cdots, b_N + \tilde{d})$ and $\tilde{\mathbf{G}} = \mathbf{G} - \mathbf{D}$, where $D = \tilde{d}\begin{bmatrix} 0 & \sum\limits_{m\in\mathcal{M}} I_{1,m}I_{2,m} & \cdots & \sum\limits_{m\in\mathcal{M}} I_{1,m}I_{N,m} \\ \sum\limits_{m\in\mathcal{M}} I_{2,m}I_{1,m} & 0 & \cdots & \sum\limits_{m\in\mathcal{M}} I_{2,m}I_{N,m} \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{m\in\mathcal{M}} I_{N,m}I_{1,m} & \sum\limits_{m\in\mathcal{M}} I_{N,m}I_{2,m} & \cdots & 0 \end{bmatrix}$. The implication for $\mathcal{S}$ has been explained previously.

4.6.3.2 Utility Maximization for MCUs

Due to the globally positive social effect and locally negative delay effect, we cannot simply deploy the Algorithm 6 to solve the Stackelberg game for each pile of RUs. However, owing to the existence and uniqueness of all RUs' best response strategies $\tilde{\mathbf{x}}^{*}$, MCUs can correctly predict the behaviors of all RUs given the unit price $\tilde{\mathbf{p}}$, which gives them opportunities to maximize their total revenues.

To ease the description, we consider the case where all RUs receive their requested data $\tilde{\mathbf{x}}_{\mathcal{S}}^* = \tilde{\mathbf{x}}^*$. The case in which some RUs receive no contents can be easily extended. With the known indicator matrix, (4.11) is rewritten as,

$$\tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right) = \left(\tilde{\mathbf{p}} - c\mathbf{1}_N\right)^T \tilde{\mathbf{x}}^* \tag{4.38}$$

Substitute (4.36) into (4.38), we have,

$$\begin{aligned} \tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right) &= \left(\tilde{\mathbf{p}} - c\mathbf{1}_N\right)^T \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1} \left(\mathbf{a} - \tilde{\mathbf{p}}\right) \\ &= -\tilde{\mathbf{p}}^T \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1} \tilde{\mathbf{p}} + \tilde{\mathbf{p}}^T \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1} \mathbf{a} + c\mathbf{1}_N^T \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1} \tilde{\mathbf{p}} - c\mathbf{1}_N^T \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1} \mathbf{a} \end{aligned} \tag{4.39}$$

We ignore the last term in (4.39) since it has nothing to do with $\tilde{\mathbf{p}}$ in the following. To obtain the strategies for each MCU, we have the total utilities maximization problem as,

$$\begin{aligned} \max_{\tilde{p}_1, \cdots, \tilde{p}_M} \quad & \tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right)' = -\tilde{\mathbf{p}}^T \mathbf{A} \tilde{\mathbf{p}} + \tilde{\mathbf{p}}^T \mathbf{A} \mathbf{a} + c\mathbf{1}_N^T \mathbf{A} \tilde{\mathbf{p}} \\ \text{s.t.} \quad & 0 \le \tilde{p}_m \le \max_{i \in \mathcal{N}} a_i, \forall m \end{aligned} \tag{4.40}$$

where $\mathbf{A} = \left(\tilde{\mathbf{\Lambda}} - \tilde{\mathbf{G}}\right)^{-1}$. The constraints in (4.40) is to restrict each MCU's unit payment. Otherwise, RUs would not receive any contents from MCUs as shown in (4.36) and (4.37). Since $\tilde{\mathbf{p}}$ is piecewise, we divide the matrix $\mathbf{A}$ into blocks,

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1M} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{M1} & \mathbf{A}_{M2} & \cdots & \mathbf{A}_{MM} \end{bmatrix} \tag{4.41}$$

where

$$\mathbf{A}_{uv} = \begin{bmatrix} a_{\sum\limits_{u=1}^{i-1} n_{m_u}+1, \sum\limits_{v=1}^{j-1} n_{m_v}+1} & \cdots & a_{\sum\limits_{u=1}^{i-1} n_{m_u}+1, \sum\limits_{v=1}^{j} n_{m_v}} \\ \vdots & \ddots & \vdots \\ a_{\sum\limits_{u=1}^{i} n_{m_u}, \sum\limits_{v=1}^{j-1} n_{m_v}+1} & \cdots & a_{\sum\limits_{u=1}^{i} n_{m_u}, \sum\limits_{v=1}^{j} n_{m_v}} \end{bmatrix}$$

$\mathbf{a} = \{a_1, \cdots, a_{n_{m_1}}, a_{n_{m_1}+1}, \cdots, a_{n_{m_1}+n_{m_2}}, \cdots, a_N\}^T = \{\mathbf{a}_1'^T, \mathbf{a}_2'^T, \cdots, \mathbf{a}_M'^T\}^T$ is rewritten, where

$\mathbf{a}_i^{'} = \{a_{\sum n_{m_{i-1}}+1}, \cdots, a_{\sum n_{m_i}}\}^T$. Substituting (4.41) into (4.40),

$$\begin{aligned}\tilde{R}\left(\tilde{\mathbf{x}}, \tilde{\mathbf{p}}\right)^{'} &= \sum_{i=1}^{M}\sum_{j=1}^{M} \tilde{p}_i \tilde{p}_j \mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{1}_{n_{m_j}} + \sum_{i=1}^{M} \tilde{p}_i \sum_{j=1}^{M} \left((\mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{1}_{n_{m_j}})^T + \mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{a}_j^{'} \right) \\ &= \tilde{\mathbf{p}}^{'T} \mathbf{A}^{'} \tilde{\mathbf{p}}^{'} + \sum_{i=1}^{M} \tilde{p}_i \sum_{j=1}^{M} \left((\mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{1}_{n_{m_j}})^T + \mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{a}_j^{'} \right)\end{aligned}$$

where $\tilde{\mathbf{p}}^{'} = [\tilde{p}_1, \tilde{p}_2, \cdots, \tilde{p}_M]$ and $\mathbf{A}^{'}$ is a new matrix with the ij_{th} element $\mathbf{1}_{n_{m_i}}^T \mathbf{A}_{ij} \mathbf{1}_{n_{m_j}}$. According to [82] and [25], the total utilities maximization is a convex optimization problem as long as $\mathbf{A}^{'} + \mathbf{A}^{'T}$ is positive semidefinite. Therefore, we can use convex toolbox cvx [66] to obtain the strategies of MCUs under the positive semidefinite assumption.

4.7 Performance Evaluation

In this section, we evaluate the performance of the data offloading approaches in both the delay-tolerant scenario and the delay-sensitive scenario.

4.7.1 Simulation Settings

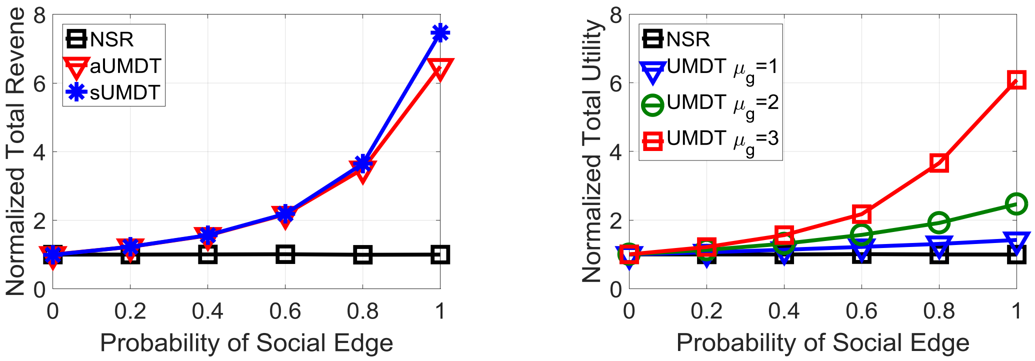
We consider a scenario with $N = 10$ RUs served by MCUs. Their internal characteristics follow a Gaussian distribution, where $a_i \sim \mathcal{N}(\mu_a, 2)$ and $b_i \sim \mathcal{N}(\mu_b, 2), \forall i$. To show the social effect brought by RUs' social relationship, we deploy the Erdős-Rényi (ER) graph [49] model, in which a social edge between RUs exists with probability P_S in a group. If a social edge indeed exists, it is assumed to follow a normal distribution $\mathcal{N}(\mu_g, 2)$. To ensure the assumptions proposed in the chapter, we set $\mu_a = \mu_b = 30$. In addition, the MCU's unit cost when delivering contents to RUs is constant, $c = 5$.

4.7.2 Simulation Results

In our simulations, we mainly compare the performance of the following cases: (1) No relationship case (NSR), in which there are no interactions between RUs, $g_{ij} = 0, i, j \in \mathcal{N}$, $d = \hat{d} = \tilde{d} = 0$. (2) Delay-tolerant case (UMDT), in which the social effect exists among RUs due to their similar social attributes $g_{ij} \neq 0, \exists i, j \in \mathcal{N}$, $d = \hat{d} = \tilde{d} = 0$. (3) Intuitive Delay-sensitive case (iUMDS). (4) Queue Delay-sensitive case (qUMDS), and (5) Multi-leader Delay-sensitive case (mUMDS). Note that we normalize most simulation performance based on the NSR case, which means the performance value is divided by the corresponding value in the NSR case. In what follows, we show the impacts to which the social effect and delay effect will bring respectively.

4.7.2.1 The Impact of the Probability of Social Edge

To investigate the impact of social effect, we first consider the UMDT case in Fig.4.5. Since two RUs in a social relationship could have different interests, we want to find whether such an asymmetry impacts RUs' utilities. Fig.4.5a shows that it does not play an important role on RUs. Therefore, we choose the asymmetric social relationship in the followings as $g_{ij} \neq g_{ji}$ to be close to reality. Fig.4.5a also tells us that the probability of the social relationship between RUs has a large impact. This is because the probability implies the contact opportunities between RUs, which would bring more social effects. Fig.4.5b further demonstrates the above observation, which shows that the total utility of RUs increases as the increasing of the probability of social relationship. Hence, our motivation is verified that the homophily phenomenon truly brings positive social effects to data offloading scheme.



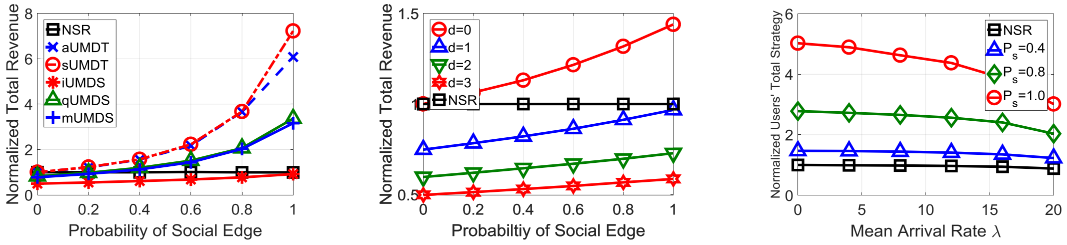
(a) Asymmetry Effect

(b) Social Effect

Figure 4.5: UMDT Case

4.7.2.2 The Impact of Delay Effect

In iUMDS case, we consider the intuitive delay effect. From Fig.4.6b, we find that such delay effect puts a serious negative impact on the MCU's total revenue. Specifically, when the delay effect is large, it could even cancel out the benefits brought by the social effect. When RUs are eager to obtain their requested contents, they have to wait for a long time. Thus, they would not request more contents even if the unit payment is low. The low unit payment and few contents decrease the total revenue of the MCU.



(a) Total Levels vs. Number of RUs

(b) Intuitive Delay Effect

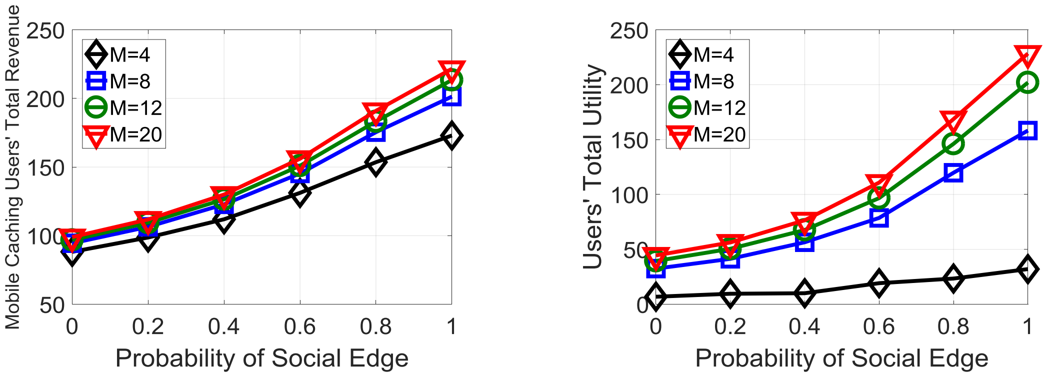
(c) Queue Effect

Figure 4.6: Delay Effect

4.7.2.3 The Benefits brought by Improved Models

In order to show the benefits in the qUMDS and mUMDS cases, we compare the MCU's total revenue as shown in Fig. 4.6a. The worst situation is considered that the intuitive delay effect cancels the benefits brought by social effect completely, where $\mu_g = d = 3$. Fig. 4.6a demonstrates that the introduction of the queue and multiple MCUs indeed helps increase the total revenue.

qUMDS Case. We discuss the impact of the mean arrival rate shown in Fig. 4.6c. It impacts RUs' content levels negatively. Higher mean arrival rate indicates that more content requests come to the MCU while it is delivering contents, which would increase the content queue length. RUs have to wait for a longer time to obtain their contents and thus dissatisfy with the content transmission. Therefore, their requested content levels would decrease.

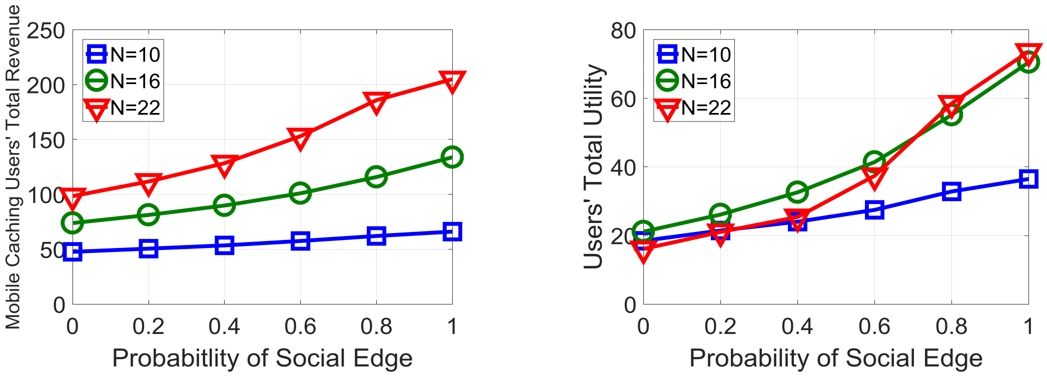


(a) Total Revenue

(b) Total Utility

Figure 4.7: Effect from MCUs

mUMDS Case. In Fig. 4.7, we draw the impacts to both MCUs and RUs' utilities brought by the number of MCUs. Assume there are $N = 25$ RUs requesting contents. As can be seen from Fig.4.7a and Fig.4.7b, more MCUs not only increase the utilities of RUs but also improve the total revenue of themselves. Fig.4.8 shows an interesting phenomenon. Given the number of MCUs, each RU's waiting time will increase as the number of RUs becomes large, and thus their own utilities reduce. In the worst case, the total utilities of a larger number of RUs are lower than those of a smaller number of RUs as shown in Fig.4.8b. However, since the number of RUs is large, the total avenue obtained from them can still be as high as shown in Fig. 4.8a. Both Fig. 4.7 and Fig. 4.8 demonstrate the effectiveness of our proposed multiple MCU delay sensitive model.



(a) Total Revenue

(b) Total Utility

Figure 4.8: Effect from RUs

4.8 Chapter Summary

In this chapter, we propose a data offloading approach by leveraging human's social behavior and human activities. To motivate the participation of MCUs, a two-stage Stackelberg game is deployed considering the interactions between RUs. In the delay-tolerant scenario, the interactions bring social effect owing to RUs' similar social attributes. We prove that the Stackelberg game has a unique Nash equilibrium and design an effective algorithm to compute the RUs' best response strategies. This enables the MCU to maximize the revenue. In the delay-sensitive scenario, by further taking advantages of RUs' mobility, we propose two improved approaches to lower RUs' delay effect due to their long waiting time, which introduces queue and extends the single-leader Stackelberg game to the multi-leader scheme, respectively. Based on the simulation results, we have shown the feasibility and effectiveness of our proposed approaches.

Chapter 5

Social-aware Energy-efficient Data Offloading with Strong Stability

5.1 Chapter Overview

With the rapid growth of the popularity of mobile devices and Internet services, people enjoy more benefits than ever before. For example, communicating with friends and watching videos at any time and anywhere become a reality. However, such operations generate a huge amount of data traffic. According to the report from the Cisco, global mobile data traffic will increase sevenfold between 2016 and 2021, reaching 48.3 EB per month by 2021 [37]. On the one hand, the explosively increasing data traffic burdens mobile operators with large operational expenditure [199]. On the other hand, it leads to a significant increase in energy consumption and thus puts an adverse effect to the environment [188]. As shown in [59], the amount of CO_2 emissions from the cellular networks will be 345 million tons by 2020. As a result, it is critical to investigate effective solutions to reduce energy consumption while adapting to the ever-increasing data traffic demands.

Mobile data offloading is a promising paradigm to address the above challenge by utilizing complementary and revolutionary networking approaches (e.g., small cell, WiFi offloading, and opportunistic communication) to deliver mobile data originally planned for cellular networks [199]. Instead of requesting data from base stations, users either access data from other users or offload data to other requested users with the help of the Device-to-Device (D2D) communication. Hence, energy consumption at base stations is largely reduced. Taking a step further, incorporating mobile users' social behaviors into consideration facilities the above idea in real life. Specifically, users with similar social interests often group together in a region, which potentially results in similar content requests. For example, users gathered in specific attractions, such as Disneyland, may request similar contents related to those attractions. Such a characteristic is also reflected in social networks, where socially-related data shared among social ties are similar or even identical (e.g., similar photo updates on Facebook). The above observation leads us to consider whether we can avoid duplicated requests/retrievals in order to reduce the number of accesses to the cellular network. Having the offloaded data, similar social interests among users will motivate them using D2D communication for further data dissemination [15], which would greatly relieve the traffic burden at base stations and thus free energy consumption.

However, energy consumption in D2D communication becomes one of the most critical challenges for the deployment. Frequently transceiving data between battery-powered mobile devices could quickly drain their energy [174, 187]. Meanwhile, arbitrarily caching data in their buffer will bring trouble due to limited buffer size. Even worse, the stability of the entire network suffers from break-off users [110, 168]. In our chapter, we leverage users' social preference to reduce energy consumption on mobile devices, and keep the stability of the entire system while satisfying users' traffic demands. Specifically, we mainly focus on the following problems:

- **Whether to cache or offload data?** It relies on the current caching queue size and the underlying wireless environment. When the channel condition is poor, transmitting the same amount of data results in higher energy consumption. Rather than forwarding the data to the next hop, the user keeps them in a queue and waits for a better channel condition. However, the cumulative queuing data may surpass the buffer size and further affect network stability. Therefore, each user has to make a decision on whether to forward the data or queue it for energy saving purpose.

- **How much data to be cached or offloaded?** Since the energy and the queue size are limited, each user sets different preferences over caching and offloading data for others, which is addressed by allocating different queue sizes and data transmission rates according to their social interests to offloaded data.

- **Who will cache and offload data?** In a wireless environment, the same data can be cached at different users and one user can cache for multiple data. If more users help cache and offload data, the overall system-wide energy consumption is reduced by decreasing the transmission ranges between users. However, these users inevitably increase energy consumption at their own sides. Hence, users who cache and offload data should be selected.

- **How does social preference work?** Users have different interests in different kinds of data. They could affect the data offloading according to their preferences. For example, when the channel condition is poor, they assign a larger buffer size for the interested data. Thus, the energy consumption is decreased. Based on their preferences, users can flexibly allocate buffer size to data, which will guarantee network stability.

Obviously, energy consumption, channel condition, and network capacity in social-aware data offloading are tightly coupled. To answer those questions, we present a cross-layer optimization framework. An offline energy optimization problem $P1$ is formulated aiming at minimizing the time-averaged value of energy consumption at all users by jointly considering the correlation between random channel conditions, users' social preferences, network capacity and transmission scheduling, which turns out to be a time-coupling stochastic Mixed-Integer Non-Linear Programming (MINLP) problem. Previous approaches applying Dynamic Programming (DP) always suffer from the "curse of dimensionality" problem [22]. Besides, solutions using DP require detailed statistical information on system random variables, which are difficult to obtain in practice. Therefore, based on deploying Lyapunov optimization theory [137], we reformulate an equivalent problem $P2$ and propose an online energy approximation problem $P3$. Different with the offline energy optimization requiring the knowledge of the network statistics, the online energy approximation problem $P3$ does not require any statistic knowledge of the random process. However, $P3$ is still a MINLP which is NP-hard and needs to be solved in each time slot. By introducing a virtual queue, we decompose P3 into three subproblems: link scheduling and power allocation ($S1$), content allocation ($S2$), and routing ($S3$). Three algorithms are developed to solve them based on the current network states only respectively. Finally, we demonstrate the network stability by proving all the queues are finite (Theorem 1). Meanwhile, we prove that the proposed algorithm leads to an upper and lower bound (Theorem 2 and Theorem 3) to the original problem, where $\phi^*_{P3} - \frac{B}{V} \leq \phi^*_{P1} \leq \phi^*_{P3}$. ϕ^*_{P1} and ϕ^*_{P3} are the optimal results of $P1$ and $P3$, respectively. B is a constant and V represents the weight on how much we emphasize on the energy consumption minimization in $P3$. As we can see, $\frac{B}{V}$ goes to

0 as V increases, in which the minimized time-averaged expected energy is obtained in $P1$.

The rest of this chapter is organized as follows: Section 5.2 briefly reviews the existing D2D enabled data offloading schemes and studies the effect brought by social characteristics, together with Lyapunov optimization techniques applied in wireless networks. In Section 5.3, we introduce our system architecture and network model. The formulation of an offline energy minimization optimization problem is given in Section 5.4. In Section 5.5, based on Lyapunov optimization theory, we formulate an online finite-queue-aware energy minimization problem and design a decomposition based approximation algorithm to solve it. We prove that the proposed approximation algorithm guarantees network strong stability, and derive both a lower and upper bound on the optimal result of the offline optimization problem in Section 5.6, followed by the simulation results. Finally, we conclude our work in Section 5.7.

5.2 Related Work

5.2.1 D2D Enabled Data Offloading

In D2D enabled data offloading framework, some users are chosen as helpers/relays [80, 96, 183, 192] to receive the data via cellular networks. Then, those users further propagate the data among all the users through D2D communications. It is further classified into two categories: in-band offloading and out-of-band offloading [147], where the direct communication between users occupies the licensed cellular spectrum and unlicensed spectrum (e.g., WiFi-Direct, Bluetooth) respectively. In-band offloading may improve the resource utilization by reusing the spectrum for the users that are physically in close proximity to communicate with each other at a high rate and low power consumption. The developments in the 3GPP LTE Standard (Rel-12) have proposed integrating direct in-band communication capabilities into the future cellular architecture [123]. Li *et al.* in [116] study the realistic bound of an offloading strategy exploiting LTE-D2D in a large-scale scenario. Their simulation results confirm that augmenting the number of users in the cell largely benefits to offloading, increasing its efficiency. In that case, D2D transmissions account for up to 50% of the traffic, which shows the feasibility of in-band offloading.

Since direct transmissions take place in the same band as the cellular transmissions, in-band offloading provides additional flexibility to the network but raises issues on mutual interference and resource allocation. Thus, previous works mainly focus on interference management and transmission coordination problems. In [145], the radio resource allocation is optimized to help decrease the mutual interference between D2D communications and the primary cellular network. Xu *et al.* propose a reverse iterative combinatorial auction mechanism to allocate spectrum resources between cellular users and D2D pairs [181]. Doppler *et al.* in [47] limit the maximum transmission power of D2D peers to alleviate the interference. With the explosive increase of data traffic, power allocation puts an effect on not only the interference management but also device battery. However, how to improve energy efficiency at mobile users receives little attention in D2D enabled data offloading. Meanwhile, social-characteristics, which play an important role in other offloading schemes [77,173], are not considered.

5.2.2 Social-enabled Data Offloading

The “like-me” principle [107] describes a well-accepted nature of human interaction that people like to interact with those who are similar to themselves. An experiment analyzing the relationship between the contact rate and the number of identical attributes is conducted in [72,73] based on the trace file collected during the INFOCOM 2006 [154]. Its result shows that the contact rate in terms of the number of contacts between two users increases with the increment of identical attributes, which further validates the “like-me” principle. In addition to that, Hsu *et al.* in [85] show that users who share similar interests intend to form a group and they forward messages to others in the group more efficiently. From the above phenomena, in the scenario where users with attribute similarities form the attribute-similar group, we infer that the content dissemination is much more efficient when the social characteristics are considered. As in our previous work [190, 191], users are more satisfied with the data offloading process when we take into consideration the social effect brought by users’ similar attributes.

The deployment of the above social characteristics has been addressed in data offloading. Li *et al.* in [117] demonstrate that we can leverage the social behaviors to assist D2D communication in order to enhance the achievable system performance. In [77], social participation and interaction are exploited to help select the target users in order to minimize the mobile data traffic over the cellular network. Zhang *et al.* and Wang *et al.* exploit social network characteristics for assisting the ad hoc peer discovery in [189] and [172], respectively. Social characteristics are also applied to resource allocation in D2D communication. In [172], a two-step coalition game is formulated to achieve optimal spectrum allocation by deploying social times in human-formed social networks. Although the social characteristics are utilized to improve the energy efficiency in [88], they do not consider the randomness in D2D communication, e.g., channel condition and cellular users. However, such randomness would result in serious changes in the network. In our chapter, we investigate how to minimize the energy consumption at mobile users (D2D users) while satisfying their traffic demands and network stability under the varying channel condition.

5.2.3 Lyapunov Optimization Method

Lyapunov optimization theory has been adopted to investigate stochastic optimization problems in communication and queuing systems [93,110,136–138,168,184]. However, the queues are not guaranteed to be finite in [110,168,184], which destroys the network stability. Although finite queue sizes are maintained in [136,138,184], some packets are dropped as a cost in opportunistic scheduling scheme. Hence, network utility is lowered. Based on Lyapunov optimization framework, the authors in [110] address social preference of users and apply back-pressure based transmission scheduling to achieve guaranteed utility optimality. Li *et al.* in [111] employ Lyapunov optimization theory to develop online crowdsourcing algorithms. Liao *et al.* in [122] propose an online finite-queue-aware energy cost minimization problem with the help of Lyapunov optimization theory. The above two works guarantee both network stability and utility. However, they do not consider the social characteristics among nodes. Besides, the work [122] deploys a fixed modulation scheme whereas the simulation results in [112] demonstrate the effectiveness on the users' utility using an adaptive modulation scheme. Motivated by the above work, we try to minimize the energy consumption in D2D data offloading by taking social characteristics and adaptive modulation into accounts based on Lyapunov optimization theory in our chapter.

5.3 System Models

5.3.1 System Architecture

We take data dissemination in the Disney World as an example, where users with similar social interests group together in the same place, e.g., Rock 'n' Roller Coaster Starring Aerosmith attraction. They request the same contents, e.g., videos related to the attraction, whereas WiFi is not accessible. As shown in Fig.5.1, instead of getting the requested contents from the base station

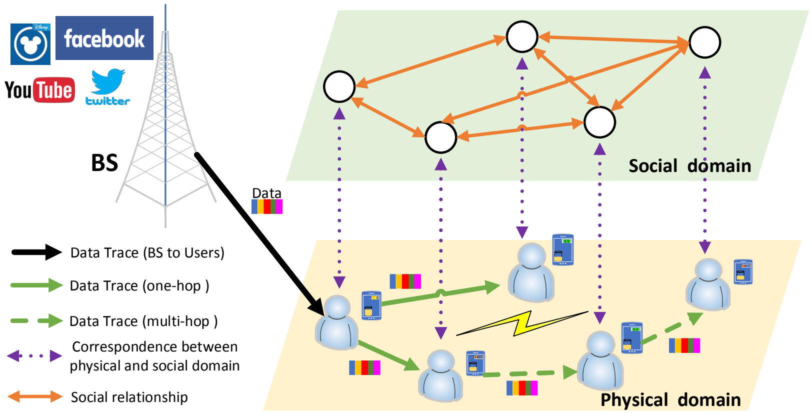


Figure 5.1: System Model

(BS) directly, D2D offloading is deployed to satisfy users' requests. Specifically, users with the largest cache are chosen as the **representative users** to get the contents from the BS, which are further transmitted among the crowd via D2D communication. To reuse the network resource, all the D2D communications occur on the fixed spectrum bands, whi ch introduces possible interference between different D2D communications and hence would affect the achievable communication rate. In order to prevent interference and improve the energy efficiency at mobile users, the cellular network takes charge of the whole process including network management, link scheduling and resource allocation taking advantage of the social relationships among users.

5.3.2 Network Model

As described in Fig. 5.1, a set of users $\mathcal{U} = \{1, 2, \cdots, U\}$ with the common interests request new contents from the service provider. We represent the above contents using a set $\mathcal{L} = \{1, 2, \cdots, L\}$. Since these users are in close proximity, they get the requested contents either from the BS via cellular communication or from others having common interests via D2D communication. Each content l is further denoted as a tuple $\{f^l_{ij}(t), i, j\}$, indicating the amount of content l offloaded from the caching user i to the requesting user j in time slot t. Because users have different communication interfaces and locate at different positions, they occupy different spectrum bands. Let $\mathcal{M}_i$ denote the set of available spectrum bands the user i has. $\mathcal{M}_i$ might be different from $\mathcal{M}_j$, i.e., $\mathcal{M}_i \neq \mathcal{M}_j$ for $i \neq j$, $i, j \in \mathcal{U}$. All the available spectrum bands compose a spectrum set $\mathcal{M} = \{1, 2, \cdots, M\}$ and $\mathcal{M}_i \subset \mathcal{M}$ for each user i. In addition, we assume the bandwidth of band m is an i.i.d. random process denoted by $\{W^m(t)\}_{t=0}^{\infty}$, which is observed at the beginning of each time slot.

Table 5.1 summarizes the main notations for ease of reference, where t denotes in the time slot t.

Table 5.1: Notation Table

$\mathcal{U}$	user set
$\mathcal{L}$	content set
$\mathcal{C}$	modulation order set
$P_{ij}^{m}(t)$	power of transmission from user i to user j on band m
$P_{i}^{rev}(t)$	receiving power at user i
$e_i(t)$	total energy consumption at user i
Δt	duration for one time slot
$Q_i^l(t)$	data queue for content l at user i
$Y_{ij}(t)$	virtual link-layer queue from user i to user j
$\rho_i^l(t)$	user i's interest in content l
p_i^l	buffer size for data queue $Q_i^l(t)$
$f_{ij}^l(t)$	amount of content l offloaded from user i to user j
$c_{ij}^l(t)$	content l's maximum transmission rate from user i to user j on band m
c_{ij}^{max}	content l's maximum transmission rate from user i to user j
$s_{ij}^m(t)$	Binary Var: band m is assigned for transmission from user i to user j
$s_{ij}^{mc}(t)$	Binary Var: band m is assigned for transmission from user i to user j with modulation order 2^c
$v_l(t)$	amount of content l, maximum: v^{max}
v^{max}	maximum amount of content received from BS
λ	parameter determined by system controller
V	weight on importance on energy minimization

5.3.3 Network rate stable and strongly stable

We first introduce definitions and theorems of Lyapunov optimization [137]. We denote those theorems as lemmas used for scheme design and analysis later.

DEFINITION 6. *The time average of a random process* $a(t)$*, denoted by* $\overline{a}$*, is* $\overline{a} = lim_{T\rightarrow\infty}\sum_{t=0}^{T}\frac{1}{T}\mathbb{E}\left[a(t)\right]$.

□

DEFINITION 7. *A discrete time process* $a(t)$ *is rate stable if* $lim_{t\rightarrow\infty}sup\frac{a(t)}{t} = 0$ *with probability 1, and strongly stable if* $lim_{T\rightarrow\infty}sup\frac{1}{T}\sum_{t=0}^{T}\mathbb{E}\left[a(t)\right] < \infty$. □

Lemma 2. Queue Rate Stability [137]

Let $Q(t)$ *denote the queue length of a single-user discrete time queuing system, whose initial state* $Q(0)$ *is a non-negative real-valued random variable, and future states are driven by stochastic arrival and transmission processes* $a(t)$ *and* $b(t)$ *according to the following dynamic equation:*

$$Q(t+1) = \max\left\{Q(t) - b(t), 0\right\} + a(t), t \in \{0, 1, 2, \cdots\}$$

Then $Q(t)$ *is rate stable if and only if* $\overline{a} \leq \overline{b}$. □

Lemma 3. Necessity for Queue Strong Stability [137]

If a queue $Q(t)$ *is strongly stable, and there is a finite constant* c *such that either* $a(t) + b^{-}(t) \leq c$ *with probability* 1 *for all* t*, where* $b^{-}(t) \overset{\Delta}{=} -\min\left\{b(t), 0\right\}^{1}$*, or* $b(t) - a(t) \leq c$ *with probability* 1 *for all* t*, then* $Q(t)$ *is rate stable, i.e.,* $\overline{a} \leq \overline{b}$.

Besides, we say that a network is rate stable or strongly stable if all queues in this network are rate stable or strong stable as described above. □

5.4 Energy Consumption Optimization

In this section, we investigate the energy consumption optimization problem given cross-layer constraints in D2D data offloading.

5.4.1 Energy Consumption

For each offloading user, he consumes the energy when he either transmits the contents or receives the requested contents. Denote the energy consumed at user i as $E_i(t), i \in \mathcal{U}$, in time slot t,

$$E_i(t) = \sum_{j\in\mathcal{U}, j\neq i}\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} P_{ij}^{m}(t)s_{ij}^{m}(t)\Delta t + P_i^{rev}s_{ji}^{m}(t)\Delta t, \tag{5.1}$$

[1] Based on [137], the value of $a(t)$ is assumed to be non-negative. For most physical queuing systems, $b(t)$ assumed to be non-negative, although it is sometimes convenient to allow $b(t)$ to take negative values.

where the user i consumes the power $P_{ij}^m(t)$ to transmit the contents to the user j using band m. P_i^{rev}, a constant, denotes the power the user i spends receiving the contents. We suppose Δt to be the time duration in each time slot, and $s_{ij}^m(t)$ is a binary transmission indicator where $s_{ij}^m(t) = 1$ means that user i transmits to user j on band m in time slot t. Otherwise, $s_{ij}^m(t) = 0$.

5.4.2 Interference Constraints

To mitigate the interference and improve the throughput when different users offload contents simultaneously, we investigate the constraints from the physical layer.

Based on a widely applied model [55,63,84], the power propagation gain from user i to user j, denoted by g_{ij}, is,

$$g_{ij} = d(i,j)^{-\gamma}, \tag{5.2}$$

where $d(i,j)$ is the Euclidean distance between user i and j and γ represents the path loss exponent. Here we assume that the coherence bandwidth of each band is larger than the bandwidth itself so that each band is flat. Meanwhile, the coherence time of the channel is larger than the duration of a time slot so that the fading remains constant in each time slot. In addition, users are assumed to be in the same location during content transmission.

Given the propagation gain in (5.2), according to [63], the signal-to-interference-plus-noise ratio (SINR) of the signal received at j from i on band m becomes,

$$SINR_{ij}^m(t) = \frac{g_{ij} P_{ij}^m(t)}{\eta_j W^m(t) + \sum_{k \neq i, v \neq j} g_{kj} P_{kv}^m(t)}, \tag{5.3}$$

in which we denote η_j as the thermal noise power density at user j. $W^m(t), m \in \mathcal{M}$ represents the bandwidth of the current spectrum being occupied. We simulate the changes of the current channel condition by changing $W^m(t)$. As in [75, 113], the content transmission is successful only if the received SINR at user j satisfies,

$$SINR_{ij}^m(t) \geq \Gamma, \tag{5.4}$$

where Γ is a threshold that depends on the current modulation scheme and the target bit error rate (BER) P_b [63]. To adapt the current channel condition, we deploy an adaptive M-order quadratic amplitude modulation (M-QAM) scheme, where the modulation order O is chosen from a order set

$\mathcal{C} = \{2^1, 2^2, \cdots, 2^C\}$. Hence, we have different possible thresholds as,

$$\Gamma_{\log_2 O} = -\frac{(O-1)\ln(5P_b)}{1.5}, O = 2^1, 2^2, \cdots, 2^C. \tag{5.5}$$

Suppose that ideal Nyquist data pulse is applied on modulation. The spectrum efficiency of M-QAM is $\log_2 O$ bps/Hz [63]. Let $\Gamma_{C+1} = \infty$. When $\Gamma_{\log_2 O} \leq SINR_{ij}^m(t) \leq \Gamma_{\log_2 O+1}$, the achievable data rate from user i to user j on band m is,

$$c_{ij}^m(t) = W^m(t) \log_2 O(t). \tag{5.6}$$

5.4.3 Network Layer Constraints

It is an efficient way to improve the energy efficiency by considering the channel condition changes. Instead of offloading the contents to other users when the channel condition is poor, each user would like to keep the contents until that channel condition becomes better. Hence, each user maintains a content queue $Q_i^l(t), i \in \mathcal{U}, l \in \mathcal{L}$ for his received content at the network layer. For every queue Q_i^l at each user, it is updated in the following,

$$Q_i^l(t+1) = \max\left\{Q_i^l(t) - \sum_{j\in\mathcal{U}, j\neq i} f_{ij}^l(t), 0\right\} + (\sum_{\{j|i\neq j\}} f_{ji}^l(t) + v_l(t)\mathbf{1_{i=s_l}}). \tag{5.7}$$

If $Q_i^l(t) = 0$, the user i is not on the offloading path for the content l in the current time slot. In (5.7), the binary variable $\mathbf{1}_{i\in s_l}(i \in \mathcal{U})$ indicates whether the user i is the representative user who receives the content l from the BS. We use $v_l(t)$ to denote its amount in the unit of the number of bits, $v_l(t) \leq v^{max}$, where the constant v^{max} denotes the maximum amount of content received from base station. Note that we suppose the value of $v_l(t)$ is known at the beginning of each time slot. Because there is no incoming data from other users at the source user of session l, we have the following constraint,

$$\sum_{\{j\neq i|i\}} f_{ji}^l(t) = 0, \forall i = s_l, l \in \mathcal{L}. \tag{5.8}$$

5.4.4 Social Preference in Queue

We define a rational number $\rho_i^l \in [0,1]$ to denote user i's social interests on content l. The more interesting to the contents, the larger ρ_i^l is. Our social preference in queue is reflected on the maximum queue size to the contents. To be specific, $p_i^l = F(\rho_i^l), i \in \mathcal{U}$ denotes the maximum queue size user i provides for by-passing content $l \in \mathcal{L}$. $F(\cdot)$ is a positive function that differentiates the queue size allocated to contents with different social preferences ρ_i^l of user i. We suppose $F(\cdot)$ is an increasing function with users' social preference ρ_i^l. It means users would like to provide larger queues for caching their interested contents. Specifically, we denote $p_i^l = (1+\alpha\rho_i^l)p_{s_l}^l$, where $p_{s_l}^l$ is the maximum queue size user s_l provides for content l from base station and α is the weight to strengthen the social preference's effect to the maximum buffer size. The reason for 1 is to ensure that user still participates the data offloading process even he is not interested in the content. Otherwise, in the worst case that no user is interested in the contents, they all keep the contents to themselves and thus data offloading is stopped. In addition, we assume $\alpha = 1$.

5.4.5 Link Scheduling Constraints

In this subsection, we illustrate the power allocation and link scheduling on content dissemination. Since each user is unable to transmit to or receive from multiple users on the same band, given the binary transmission indicator $s_{ij}^m(t)$ mentioned above, we have,

$$\sum_{j \in \mathcal{U}, j \neq i} s_{ij}^m(t) \leq 1, \text{and} \sum_{i \in \mathcal{U}, i \neq j} s_{ij}^m(t) \leq 1. \tag{5.9}$$

Besides, due to "self-interference" at the physical layer, a user cannot use the same frequency band for both transmission and receiving at the same time. Hence,

$$\sum_{i \in \mathcal{U}, i \neq j} s_{ij}^m(t) + \sum_{q \in \mathcal{U}, q \neq j} s_{jq}^m(t) \leq 1. \tag{5.10}$$

Meanwhile, we suppose that each user is equipped with a single radio, in the case that he cannot occupy more spectrum bands in each time slot. Taking (5.9) and (5.10) into consideration, one of the constraints in the link scheduling finally becomes,

$$\sum_{m \in \mathcal{M}_i \cap \mathcal{M}_j} \sum_{i \neq j} s_{ij}^m(t) + \sum_{n \in \mathcal{M}_j \cap \mathcal{M}_q} \sum_{q \neq j} s_{jq}^n(t) \leq 1. \tag{5.11}$$

In addition to the above constraints at a certain user, there are also power constraints due to potential interferences among different users. Denote $s_{ij}^{mc}(t)$ as a binary indicator that describes whether the content transmission from user i to user j on band m satisfies $\Gamma_c \leq SINR_{ij}^m(t) \leq \Gamma_{c+1}(1 \leq c \leq C)$, where $c = \log_2 O$,

$$\sum_{c=1}^{C} s_{ij}^{mc}(t) \leq 1. \tag{5.12}$$

Moreover, since each available transmission's SINR must be above one of the thresholds in $\{\Gamma_1, \Gamma_2, \cdots, \Gamma_C\}$, we get,

$$s_{ij}^m(t) = \sum_{c=1}^{C} s_{ij}^{mc}(t). \tag{5.13}$$

Considering (5.3) and (5.4), under an adaptive M-QAM schemes, the constraint on the power P_{ij}^m is,

$$g_{ij} P_{ij}^m(t) \geq \left(\sum_{c=1}^{C} s_{ij}^{mc}(t) \Gamma_c \right) \left(\eta_j W^m(t) + \sum\nolimits_{k \neq i, v \neq j} g_{kj} P_{kv}^m(t) \right), \tag{5.14}$$

The other constraint on the transmission power P_{ij}^m is,

$$0 \leq P_{ij}^m(t) \leq P_i^{max}, \forall i, j \in \mathcal{U}, m \in \mathcal{M}_i \cap \mathcal{M}_j, \tag{5.15}$$

where P_i^{max} is the maximum transmission power of user i.

Besides, the amount of contents transmitted from user i to user j on band m in each time slot cannot exceed the achievable data rate multiplied by the duration of the time slot,

$$\sum_{l \in \mathcal{L}} f_{ij}^l(t) \leq \sum_{m \in \mathcal{M}_i \cap \mathcal{M}_j} c_{ij}^m(t) s_{ij}^m(t) \Delta t. \tag{5.16}$$

5.4.6 Offline Energy Consumption Minimization

In offline energy consumption minimization, we aim to minimize the **time-averaged expected** energy consumption given the interference and link scheduling constraints while guaranteeing the strong stability of the network. We formulate offline energy consumption minimization problem,

$$\begin{array}{lrl} \textbf{P1:} & \textbf{minimize} & \lim\limits_{T \to \infty} \frac{1}{T} \sum\limits_{t=0}^{T-1} \sum\limits_{i \in \mathcal{U}} \mathbb{E}[E_i(t)] \\ \textbf{s.t.} & \text{Constraints} & (5.8), (5.11), (5.13)\text{-}(5.16) \\ & \mathbf{Q}(t) & \text{is strongly stable.} \end{array} \tag{5.17}$$

In (5.17), $\mathbf{Q}(t) = \left\{Q_i^l(t), \forall i \in \mathcal{U}, l \in \mathcal{L}\right\}$. We denote the optimal result of P1 by ϕ_{P1}^*. Without the constraint (5.17), P1 is a time-coupling stochastic MINLP problem, which is already expensive to solve. Previous approaches usually solve such problems based on Dynamic Programming [22] and suffer from the "curse of dimensionality" problem. They also require detailed statistical information on the random variables in the problem, which may be difficult to obtain in practice. In addition, the constraint (5.17) makes P1 an even more complicated problem. Hence, we reformulate this problem into an online energy consumption optimization problem using Lyapunov optimization theory to break the time-coupling in P1 and find a feasible solution based on the current network condition.

5.5 Online Energy Consumption Minimization

In this section, Lyapunov optimization theory is applied to design a *drift-plus-penalty* online energy consumption minimization problem P3 without requiring any prior knowledge of the network parameters while guaranteeing the network stability. The solution to P3 depends on the current channel conditions and the current queue backlogs.

5.5.1 Equivalent Offline Optimization Problem

Before moving forward, we reformulate the offline optimization problem P1 into a new one denoted as P2 to help ensure the strong stability of the network. We will show it later. Generally, two changes have been made as follows.

To adapt to the Lyapunov optimization framework , the objective function in P1 is replaced by:

$$\overline{E} = \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \left(\sum_{i\in\mathcal{U}} \mathbb{E}[E_i(t)] - \lambda \sum_{i\in\mathcal{U}} \sum_{l\in\mathcal{L}} v_l(t) \mathbf{1}_{i=s_l} \right), \tag{5.18}$$

in which λ is a parameter determined by the system controller.

Besides, we add another constraint in the following,

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}\left[\sum_{l\in\mathcal{L}} f_{ij}^l(t)\right] \leq \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}\left[\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^m(t) s_{ij}^m(t) \Delta t\right], \tag{5.19}$$

which is obtained by summing the inequality (5.16), taking expectation and limitation of both sides.

The complete formulation of P2 is as follows,

$$\begin{array}{lll} \textbf{P2:} & & \textbf{minimize} \quad \overline{E} \\ \textbf{s.t.} & \text{Constraints} & (5.8), (5.11), (5.13)\text{-}(5.17), (5.19)\ . \end{array}$$

We denote the optimal result of P2 by ϕ^*_{P2}.

Since λ and $v_l(t)$ in (5.18) are neither related to the constraints (5.8), (5.11), (5.13)-(5.16) nor the energy consumption, the new adding item $\lambda \sum\limits_{i\in\mathcal{U}} \sum\limits_{l\in\mathcal{L}} v_l(t)\mathbf{1}_{i=s_l}$ does not affect the optimal solution to P1. Meanwhile, if the constraint (5.16) is satisfied, the constraint (5.19) is satisfied spontaneously. Therefore, we say that the new proposed optimization problem P2 is equivalent to the problem P1. The same with P1, P2 is also a time-coupling stochastic MINLP problem which requires the prior knowledge of the network parameters. Besides, the requirement of the network stability (5.17) further increases its difficulty. In the following, we formulate a drift-plus-penalty problem P3 based on P2.

5.5.2 Modeling Virtual Queues

To satisfy the constraint (5.19), we first introduce a virtual queue $Y_{ij}(t)$ complying with the following queue law,

$$Y_{ij}(t+1) = \max\{Y_{ij}(t) - \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t, 0\} + \sum_{l\in\mathcal{L}} f^l_{ij}(t). \tag{5.20}$$

It is understood as the link-layer queue for the link from user i to his neighbor user j, describing the total amount of contents stored at user i to be transmitted to the user j at the beginning of the time slot t. Since each user transmits to at most one neighbor on one band in each time slot, the following inequality is satisfied,

$$\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t - \sum_{l\in\mathcal{L}} f^l_{ij}(t) \le c^{max}_{ij}\Delta t. \tag{5.21}$$

Therefore, according to Lemma 3, if we guarantee the strong stability of the queue $Y_{ij}(t)$, we ensure the rate stability, i.e., constraint (5.16).

5.5.3 Online Finite-queue-aware Energy Minimization

In this subsection, we formulate an online finite-queue-aware energy consumption minimization problem. A new queue $\mathbf{\Theta}(t) = \{\mathbf{Q}(t), \mathbf{Y}(t)\}$ is introduced which is composed of the network-layer queue $\mathbf{Q}(t) = \left\{Q_i^l(t), \forall i \in \mathcal{U}, l \in \mathcal{L}\right\}$ and the link-layer queue $\mathbf{Y}(t) = \{Y_{ij}(t), \forall i, j \in \mathcal{U}\}$. Suppose $\mathbf{Q}(0) = \mathbf{0}$ and $\mathbf{Y}(0) = \mathbf{0}$, we define a Lyapunov function for $\mathbf{\Theta}(t)$,

$$L\left(\mathbf{\Theta}(t)\right) = L\left(\mathbf{Q}(t)\right) + L\left(\mathbf{Y}(t)\right) \triangleq \frac{1}{2}\left[\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p_{s_l}^l}{p_i^l}Q_i^l(t)^2 + \sum_{i\in\mathcal{U}}\sum_{j\neq i}Y_{ij}(t)^2\right], \tag{5.22}$$

where $\frac{1}{p_i^l}Q_i^l(t)^2$ can be roughly understood as the buffer occupancy ratio of content l at user i. We multiply it by $p_{s_l}^l$ is to eliminate the parameters' effect on $L\left(\mathbf{Q}(t)\right)$ (We will prove that $p_{s_l}^l = \lambda V + v^{max}$).

In (5.22), $L\left(\mathbf{\Theta}(t)\right)$ being small implies that all queue backlogs are small, while $L\left(\mathbf{\Theta}(t)\right)$ being large implies that at least one queue backlog is large. Since all queue backlogs change with time, a key idea to push queue backlogs towards a lower congestion state is to make the queue backlogs change as small as possible. Hence, we define the one-slot conditional Lyapunov drift as,

$$\Delta\left(\mathbf{\Theta}(t)\right) \triangleq \mathbb{E}\left[L\left(\mathbf{\Theta}(t+1)\right) - L\left(\mathbf{\Theta}(t)\right)|\mathbf{Q}(t)\right], \tag{5.23}$$

where the expectation $\mathbb{E}(\cdot)$ is with respect to the random channel condition and depends on the control policy in reaction to these channel conditions. However, a lower queue congestion state cannot ensure limited energy consumption at users. We revise the conditional Lyapunov drift to the following drift-plus-penalty expression,

$$\Delta\left(\mathbf{\Theta}(t)\right) + V\mathbb{E}\left[\sum_{i\in\mathcal{U}}E_i(t) - \lambda\sum_{i\in\mathcal{U}}\sum_{l\in\mathcal{L}}v_l(t)\mathbf{1}_{i=s_l}|\mathbf{\Theta}(t)\right], \tag{5.24}$$

in which V is a positive control parameter to represent a weight on how much we emphasize on the energy consumption minimization. According to the drift-plus-penalty framework in Lyapunov optimization [137], an upper bound for (5.24) should be minimized in each time slot to achieve network stability while improving energy efficiency at users with the observation of the queue states $\mathbf{\Theta}(t)$, and the channel condition $c_{ij}^m(t)$ and $W^m(t)$. Specifically, the upper bound on $L\left(\mathbf{\Theta}(t+1)\right) -$

$L\left(\boldsymbol{\Theta}(t)\right)$ in (5.23) is:

$$
\begin{aligned}
&L\left(\boldsymbol{\Theta}(t+1)\right) - L\left(\boldsymbol{\Theta}(t)\right) = \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}\left(Q^l_i(t+1)^2 - Q^l_i(t)^2\right) + \frac{1}{2}\sum_{i\in\mathcal{U}}\sum_{j\neq i}\left(Y_{ij}(t+1)^2 - Y_{ij}(t)^2\right) \\
&= \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}\left[\left(\max\{Q^l_i(t) - \sum_{j\in\mathcal{U},j\neq i} f^l_{ij}(t),0\} + (\sum_{\{j|i\neq j\}} f^l_{ji}(t) + v_l(t)\mathbf{1_{i=S_l}})\right)^2 - Q^l_i(t)^2\right] \\
&+ \frac{1}{2}\sum_{i\in\mathcal{U}}\sum_{j\neq i}\left[\left(\max\{Y_{ij}(t) - \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t,0\} + \sum_{l\in\mathcal{L}} f^l_{ij}(t)\right)^2 - Y_{ij}(t)^2\right] \\
&\leq \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}\left[(\sum_{\{j|i\neq j\}} f^l_{ji}(t) + v_l(t)\mathbf{1_{i=S_l}})^2 + (\sum_{j\in\mathcal{U},i\neq j} f^l_{ij}(t))^2\right] + \\
&\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}Q^l_i(t)\left[\sum_{\{j|i\neq j\}} f^l_{ji}(t) + v_l(t)\mathbf{1_{i=S_l}} - \sum_{j\in\mathcal{U},j\neq i} f^l_{ij}(t)\right] + \frac{1}{2}\sum_{i\in\mathcal{U}}\sum_{j\neq i}\left(\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t\right)^2 + \\
&\frac{1}{2}\sum_{i\in\mathcal{U}}\sum_{j\neq i}\left(\sum_{l\in\mathcal{L}} f^l_{ij}(t)\right)^2 + \sum_{i\in\mathcal{U}}\sum_{j\neq i}Y_{ij}(t)\left(\sum_{l\in\mathcal{L}} f^l_{ij}(t) - \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t\right) \\
&\leq \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}(\max_{j\in\mathcal{U},j\neq i} c^{max}_{ij}\Delta t)^2 + \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}(\max_{\{j|i\neq j\}} c^{max}_{ji}\Delta t + v^{max}_l)^2 + \sum_{i\in\mathcal{U}}\sum_{j\neq i}\left(c^{max}_{ij}\Delta t\right)^2 + \\
&\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}Q^l_i(t)\left[\sum_{\{j|i\neq j\}} f^l_{ji}(t) + v_l(t)\mathbf{1_{i=S_l}} - \sum_{j\in\mathcal{U},j\neq i} f^l_{ij}(t)\right] + \sum_{i\in\mathcal{U}}\sum_{j\neq i}Y_{ij}(t)\left(\sum_{l\in\mathcal{L}} f^l_{ij}(t) - \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t\right) \\
&= B + \sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}Q^l_i(t)\left[\sum_{\{j|i\neq j\}} f^l_{ji}(t) + v_l(t)\mathbf{1_{i=S_l}} - \sum_{j\in\mathcal{U},j\neq i} f^l_{ij}(t)\right] + \\
&\sum_{i\in\mathcal{U}}\sum_{j\neq i}Y_{ij}(t)\left(\sum_{l\in\mathcal{L}} f^l_{ij}(t) - \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t\right)
\end{aligned}
\tag{5.25}
$$

where $B = \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}\left(\max_{j\in\mathcal{U},j\neq i} c^{max}_{ij}\Delta t\right)^2 + \frac{1}{2}\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p^l_{s_l}}{p^l_i}\left(\max_{\{j|i\neq j\}} c^{max}_{ji}\Delta t + v^{max}_l\right)^2 + \sum_{i\in\mathcal{U}}\sum_{j\neq i}\left(c^{max}_{ij}\Delta t\right)^2$. $c^{max}_{ij} = W^{max}\log_2 O^{max}$ denotes the maximum capacity on the link from user i to user j. W^{max} is the maximized transmission bandwidth and O^{max} is the maximized modulation order. In the first inequality, we use the fact that $(\max\{Q-b,0\}+a)^2 \leq Q^2+a^2+b^2+2Q(a-b)$ for any $Q \geq 0$, $b \geq 0$, and $a \geq 0$.

According to (5.16), we have $\sum_{j\in\mathcal{U},j\neq i} f^l_{ij}(t) \leq \sum_{j\in\mathcal{U},j\neq i}\sum_{l\in\mathcal{L}} f^l_{ij}(t) \leq \sum_{j\in\mathcal{U},j\neq i}\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c^m_{ij}(t)s^m_{ij}(t)\Delta t$. Since one user can transmit to at most one neighbor on at most one band in each time slot, we get

$\sum\limits_{j\in\mathcal{U},j\neq i} f_{ij}^{l}(t) \leq \max\limits_{j\in\mathcal{U},j\neq i} c_{ij}^{max}\Delta t$. The above explains the second inequality. Substitute (5.25) into (5.23) and (5.24), we have,

$$\Delta\left(\boldsymbol{\Theta}(t)\right) + V\mathbb{E}\left[\sum_{i\in\mathcal{U}} E_i(t) - \lambda\sum_{i\in\mathcal{U}}\sum_{l\in\mathcal{L}} v_l(t)\mathbf{1}_{i=s_l}|\boldsymbol{\Theta}(t)\right] \leq B + \psi_1(t) + \psi_2(t) + \psi_3(t), \tag{5.26}$$

where:

$\psi_1(t)$: related to link scheduling variables $s_{ij}^{mc}(t)$ and transmission power $P_{ij}^{m}(t)$,

$$\psi_1(t) = \mathbb{E}\left[\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p_{s_l}^{l}}{p_i^{l}}Q_i^{l}(t)v_l(t)\mathbf{1}_{\mathbf{i=s_l}}|\mathbf{Q}(t)\right] + \mathbb{E}\left[\sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i}(Y_{ij}(t)\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^{m}(t)s_{ij}^{m}(t)\Delta t)|\mathbf{Y}(t)\right]$$
$$+V\mathbb{E}\left[\sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i}\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} P_{ij}^{m}(t)s_{ij}^{m}(t)\Delta t|\boldsymbol{\Theta}(t)\right]. \tag{5.27}$$

$\psi_2(t)$: related to amount of the contents obtained from the BS $v_l(t)$,

$$\psi_2(t) = \mathbb{E}\left[\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}(\frac{p_{s_l}^{l}}{p_i^{l}}Q_i^{l}(t) - \lambda V)v_l(t)\mathbf{1}_{\mathbf{i=s_l}}|\mathbf{Q}(t)\right]. \tag{5.28}$$

$\psi_3(t)$: related to the amount of contents transmitted between users $f_{ij}^{l}(t)$,

$$\psi_3(t) = \mathbb{E}\left\{\sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p_{s_l}^{l}}{p_i^{l}}Q_i^{l}(t)(\sum_{\{j|i\neq j\}} f_{ji}^{l}(t) - \sum_{j\neq i} f_{ij}^{l}(t))|\mathbf{Q}(t)\right\} + \mathbb{E}\left[\sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i}\left(Y_{ij}(t)\sum_{l\in\mathcal{L}} f_{ij}^{l}(t)\right)|\mathbf{Y}(t)\right]. \tag{5.29}$$

Because B is a constant, we minimize $\psi_1(t) + \psi_2(t) + \psi_3(t)$ instead of minimizing the right-hand-side of (5.26), where $\psi_1(t)$, $\psi_2(t)$ and $\psi_3(t)$ are conditional expectations. By using the concept of opportunistically minimizing an expectation, we minimize $\psi_1^{'}(t) + \psi_2^{'}(t) + \psi_3^{'}(t)$ instead, where,

$$\psi_1^{'}(t) = -\sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i} Y_{ij}(t)\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^{m}(t)s_{ij}^{m}(t)\Delta t + V\sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i}\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j}(P_{ij}^{m}(t)s_{ij}^{m}(t))\Delta t, \tag{5.30}$$

$$\psi_2^{'}(t) \quad = \sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}(\frac{p_{s_l}^{l}}{p_i^{l}}Q_i^{l}(t) - \lambda V)v_l(t)\mathbf{1}_{\mathbf{i=s_l}}, \tag{5.31}$$

and

$$\psi_3^{'}(t) = \sum_{l\in\mathcal{L}}\sum_{i\in\mathcal{U}}\frac{p_{s_l}^l}{p_i^l}Q_i^l(t)(\sum_{\{j|i\neq j\}} f_{ji}^l(t) - \sum_{j\neq i} f_{ij}^l(t)) + \sum_{i\in\mathcal{U}}\sum_{j\in\mathcal{U},j\neq i}(Y_{ij}(t)\sum_{l\in\mathcal{L}} f_{ij}^l(t)). \tag{5.32}$$

The final optimization problem P3 is,

$$\begin{aligned} \textbf{P3:} \qquad & \textbf{minimize} \quad \psi_1^{'}(t) + \psi_2^{'}(t) + \psi_3^{'}(t) \\ \textbf{s.t.} \qquad & \text{Constraints} \quad (5.8), (5.11), (5.13)\text{-}(5.16) \\ & \mathbf{Q}(t) \text{ and } \mathbf{Y}(t) \text{ are stable .} \end{aligned} \tag{5.33}$$

5.5.4 A Decomposition Based Approximation Algorithm

In this subsection, we decompose P3 into three subproblems and solve them individually to obtain a suboptimal and feasible solution.

5.5.4.1 Link Schedule and Power Allocation

We minimize $\psi_1^{'}(t)$ as follows by finding the optimal link scheduling and power allocation policy, determined by the variables $s_{ij}^m(t)$ and $P_{ij}^m(t)$.

$$\begin{aligned} \textbf{S1:} \qquad & \textbf{minimize} \quad \psi_1^{'}(t) \\ \textbf{s.t.} \qquad & \text{Constraints} \quad (5.11), (5.13)\text{-}(5.15). \end{aligned} \tag{5.34}$$

S1 is a mixed integer quadratically constrained quadratic programming problem, which is also difficult to solve. We propose an iterative method in Algorithm 7. Generally, as shown in the while iteration (Line 3-11), we update power allocation profiles $P_{ij}^m(t)$ and link scheduling variables $s_{ij}^{mc}(t)$ for any $\forall i, j \in \mathcal{U}, m \in \mathcal{M}, 2^c \in \mathcal{C}$ iteratively until the objective function in S1 does not change or the maximum number of iterations is reached. We explain it in detail next.

- Fix $s_{ij}^{mc}(t)$. The main idea is to fix the values of $s_{ij}^{mc}(t)$ sequentially through a series of relaxed linear programming problems. To be specific, given $P_{ij}^m(t), \forall i, j \in \mathcal{U}, m \in \mathcal{M}$, S1 becomes a binary integer programming problem. As shown in Line 4-8, a greedy algorithm is proposed. We first relax all the 0-1 integer constraints on $s_{ij}^{mc}(t)$ to $0 \leq s_{ij}^{mc}(t) \leq 1$, transforming the problem to a linear programming problem. Line 5 solves the linear programming problem to obtain an optimal solution with each $s_{ij}^{mc}(t)$ between 0 and 1. Among them, the largest $s_{ij}^{mc}(t)$ is set to 1, denoted as $s_{i^*j^*}^{m^*c^*}(t) = 1$. Due to $\sum\limits_{m \in \mathcal{M}_i \cap \mathcal{M}_j} \sum\limits_{i \neq j} s_{ij}^{m}(t) + \sum\limits_{n \in \mathcal{M}_j \cap \mathcal{M}_q} \sum\limits_{q \neq j} s_{jq} \leq 1$ in the constraint (5.11), all the $s_{pj^*}^{nc}(t) = 0$ and $s_{j^*p}^{mc}(t) = 0$ for $n, m \in \mathcal{M}$, $2^c \in \mathcal{C}$ and $p, q \in \mathcal{U}$ are set to 0. The above is what Line 6 does. We remove those already fixed $s_{ij}^{mc}(t)$ from the objective functions and constraints as illustrated in Line 7. The process in Line 5-8 is repeated until all the $s_{ij}^{mc}(t)$ is obtained.

- Fix $P_{ij}^{m}(t)$. After obtaining the values of $s_{ij}^{mc}(t), \forall i, j \in \mathcal{U}, m \in \mathcal{M}$, S1 becomes a linear programming problem with constraints (5.14)-(5.15), which can be easily solved.

- Update $\psi_1^{'}(t)^{(n+1)}$ given all $P_{ij}^{m}(t)^{(n+1)}$ and $s_{ij}^{mc}(t)^{(n)}$.

As in Line 6, band m is allocated to one transmission link in time slot t, say, from user i^* to user j^*. All the other users who want to offload contents to user i^* and j^* or request contents from user i^* and j^* on band m are not allowed. Since we get a number of the $s_{ij}^{mc}(t)$ values in each "inside" while iteration, Line 6 simplifies the solving process for S1. In addition, due to the interference constraints, allowing many user pairs (e.g., user i to user j, user k to user v) to occupy the same band is impossible in order to ensure the successful transmission. Hence, the complexity of Algorithm 7 does not increase as the number of users increases. It does not suffer from the issue "curse of dimensionality". The complexity of Algorithm 7 is the same as the complexity of linear programming. Whereas previous approaches applying Dynamic Programming always suffers from the "curse of dimensionality" problem [22].

Algorithm 7: Link Scheduling and Power Allocation

```
   Input: $c_{ij}^{m}(t)$, $\mathbf{Y}(t)$, $V$, $\epsilon$, Num
   Output: $s_{ij}^{mc}(t)$, $P_{ij}^{m}(t)$ for $m \in \mathcal{M}$, $2^c \in \mathcal{C}$ and $i, j \in \mathcal{U}$
1  Choose an initial value for $\psi_1^{'}(t)^{(0)}$, $\psi_1^{'}(t)^{(1)}$ and $P_{ij}^{m}(t)^{(0)}$;
2  Set $n = 0$
3  while $|\psi_1^{'}(t)^{(n+1)} - \psi_1^{'}(t)^{(n)}| < \epsilon$ or $n + 1 > Num$ do
4      while there exists one $s_{ij}^{mc}(t)^{(n)}$ that is not fixed as 0 or 1 do
5          Solving $S1$ by relaxing all $s_{ij}^{mc}(t)^{(n)}$ as $0 \leq s_{ij}^{mc}(t)^{(n)} \leq 1$ for any $m \in \mathcal{M}$, $2^c \in \mathcal{C}$ and $i, j \in \mathcal{U}$ given
            $P_{ij}^{m}(t)^{(n)}$.
6          Set the largest $s_{ij}^{mc}(t)^{(n)}$ to 1. Denote as $s_{i^*j^*}^{m^*c^*}(t)^{(n)} = 1$ Based on (5.11), set $s_{pj^*}^{nc}(t)^{(n)} = 0$ and
            $s_{j^*p}^{mc}(t)^{(n)} = 0$ for any $n, m \in \mathcal{M}$, $2^c \in \mathcal{C}$ and $p, q \in \mathcal{U}$
7          Given already fixed $s_{ij}^{mc}(t)^{(n)}$ for $m \in \mathcal{M}$, $2^c \in \mathcal{C}$ and $i, j \in \mathcal{U}$, update $S1$.
8      end
9      Calculate $P_{ij}^{m}(t)^{(n+1)}$ by solving $S1$ given all $s_{ij}^{mc}(t)^{(n)}$.
10     Calculate $\psi_1^{'}(t)^{(n+1)}$ given all $P_{ij}^{m}(t)^{(n+1)}$ and $s_{ij}^{mc}(t)^{(n)}$.
11 end
```

5.5.4.2 Content Allocation

We minimize $\psi_2^{'}(t)$ by finding representative users together with the amount of the contents they obtain from the BS,

$$\begin{aligned} &\textbf{S2:} && \textbf{minimize} \quad \psi_2^{'}(t) \\ &\textbf{s.t.} && \text{Constraints} \quad 0 \leq v_l(t) \leq v^{max}. \end{aligned} \tag{5.35}$$

A search algorithm is developed to achieve the content allocation. To be specific, at the beginning of each time slot, given the queue backlogs $Q_i^l(t)$ for each content l, the user with the smallest queue backlog is chosen as the representative. When there are multiple users with the same smallest queue backlog, we randomly pick one of them as the representative user. Therefore, the amount of contents he can get is determined by,

$$v_l(t) = \begin{cases} v^{max} & \text{if} \quad Q_{s_l}^l(t) - \lambda V \leq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{5.36}$$

5.5.4.3 Routing

In this subsection, we minimize $\psi_3^{'}(t)$ by finding the optimal routing policy, i.e., determining the variables $f_{ij}^l(t)$. By reorganizing (5.32), we have,

$$\psi_3^{'}(t) = \sum_{l \in \mathcal{L}} \sum_{i \in \mathcal{U}} \sum_{j \in \mathcal{U}} \left(-\frac{p_{s_l}^l}{p_i^l} Q_i^l(t) + \frac{p_{s_l}^l}{p_j^l} Q_j^l(t) + Y_{ij}(t) \right) f_{ij}^l(t). \tag{5.37}$$

Hence, the optimization problem becomes,

$$\begin{aligned} &\textbf{S3:} && \textbf{minimize} \quad \psi_3^{'}(t) \\ &\textbf{s.t.} && \text{Constraints} \quad (5.8), \quad (5.16). \end{aligned} \tag{5.38}$$

The objective function of S3 can be viewed as a weighted sum of the variables $f_{ij}^l(t)$. Hence, we can determine $f_{ij}^l(t)$ at user i locally based on the current queue backlogs $\frac{p_{s_l}^l}{p_i^l} Q_i^l(t)$, $\frac{p_{s_l}^l}{p_j^l} Q_j^l(t)$ and $Y_{ij}^l(t)$. An algorithm is proposed described in Algorithm 8.

In Line 1, the variables $f_{ij}^l(t)$ ($\forall j = s_l, l \in \mathcal{L}$) are set to 0 according to constraint (5.8).

Line 2-9 and line 11 are to set the variables $f_{ij}^l(t)$ ($\forall i, j \in \mathcal{U}, l \in \mathcal{L}$). Specifically, the variables $f_{ij}^l(t)$ ($\forall j \in \mathcal{U}, l \in \mathcal{L}$) with non-negative coefficients are set to 0 in line 3-4. The variable $f_{ij}^l(t)$ with the smallest coefficient is found in Line 9. The value for $f_{ij}^l(t)$ is fixed in line 10-14. Because it is possible that $\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^m(t)s_{ij}^m(t)\Delta t$ is equal to 0 if $\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} s_{ij}^m(t) = 0$. In that case, the corresponding variable $f_{ij}^l(t)$ is set to 0. Otherwise, $f_{ij}^l(t)$ with the smallest coefficient is set to $\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^m(t)s_{ij}^m(t)\Delta t$. It means that the transmission link from user i to user j is fully utilized to deliver the requested contents. Note that if there are multiple variables $f_{ij}^l(t)$ with the same smallest coefficients, the user i randomly picks one of them and sets it to $\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{ij}^m(t)s_{ij}^m(t)\Delta t$.

Algorithm 8: Routing

```
   Input: $\mathbf{Q}(t)$, $\mathbf{Y}(t)$, $p_i^l$ for any $l \in \mathcal{L}$ and $i \in \mathcal{U}$
   Output: $f_{ij}^l(t)$ for any $l \in \mathcal{L}$ and $i, j \in \mathcal{U}$
1  Set $f_{js_l}^l(t) = 0$ for any $j \in \mathcal{U}$
2  foreach $l \in \mathcal{L}$ and $i, j \in \mathcal{U}$ do
3      if $\left(-\frac{p_{s_l}^l}{p_i^l}Q_i^l(t) + \frac{p_{s_l}^l}{p_j^l}Q_j^l(t) + Y_{ij}(t)\right) \geq 0$ then
4          $f_{ij}^l(t) = 0$
5      else
6          Calculate $coe_{ij}^l(t) = \left(-\frac{p_{s_l}^l}{p_i^l}Q_i^l(t) + \frac{p_{s_l}^l}{p_j^l}Q_j^l(t) + Y_{ij}(t)\right)$.
7      end
8  end
9  Find the smallest $coe_{ij}^l(t)$. Denote corresponding $f_{ij}^l(t)$ as $f_{i*j*}^{l*}(t)$
10 if $\sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} s_{i*j*}^m(t) = 0$ then
11     Set $f_{i*j*}^{l*}(t) = 0$
12 else
13     Set $f_{i*j*}^{l*}(t) = \sum_{m\in\mathcal{M}_i\cap\mathcal{M}_j} c_{i*j*}^m(t)s_{i*j*}^m(t)\Delta t$
14 end
15 Set other $f_{ij}^l(t) = 0$ for any $l \in \mathcal{L}$ and $i \in \mathcal{U}$
```

In each time slot, the online finite-queue-aware energy consumption minimization problem is solved after S1, S2 and S3 are solved respectively. The queues $\mathbf{Q}(t)$ and $\mathbf{Y}(t)$ are then updated according to (5.7) and (5.20), respectively. We denote the corresponding time-averaged expected total energy consumption by ϕ_{P3}^*.

5.6 Performance Analysis

In this section, we prove that the proposed approximation algorithm guarantees network strong stability. Following that, we derive both the lower and upper bounds on the optimal result of P1. Finally, we give some simulation results based on our proposed approach.

5.6.1 Network Strong Stability

Our proposed approach finds an approximation solution to P3 which satisfies the constraints (5.8), (5.11), (5.13)-(5.16). However, we do not consider the network strong stability, which is an important and challenging problem.

Theorem 6. *Our proposed approximation problem guarantees that the queues* $\mathbf{Q}(t)$ *and* $\mathbf{Y}(t)$ *are all strongly stable.* □

Proof: First, we demonstrate the strong stability of $\mathbf{Q}(t)$ by considering an arbitrary queue $Q^l_i(t)$. In particular, the induction method is deployed to prove that $Q^l_i(t) \leq p^l_i$, where $p^l_{s_l} = \lambda V + v^{max}$ and $p^l_i = (1 + \alpha\rho^l_i)p^l_{s_l}$.

When $t = 0$, we have $Q^l_i(0) = 0 \leq p^l_i$.

When $t = t'(t' \geq 0)$, we suppose $Q^l_i(t') \leq p^l_i$. We prove that $Q^l_i(t'+1) \leq p^l_i$ in the following.

Situation 1: $i = s_l$. The queuing law (5.7) becomes,

$$Q^l_{s_l}(t+1) = \max\{Q^l_{s_l}(t) - \sum_{j \in \mathcal{U}, j \neq i} f^l_{s_l j}(t), 0\} + v_l(t). \tag{5.39}$$

We consider two situations on the value of $v_l(t)$,

- Case 1: $Q^l_{s_l}(t) \leq \lambda V$. According to (5.36), $v_l(t) = v^{max}$. $Q^l_{s_l}(t'+1) \leq Q^l_{s_l}(t') + v^{max} \leq \lambda V + v^{max} = p^l_{s_l}$.
- Case 2: $Q^l_{s_l}(t) > \lambda V$. According to (5.36), $v_l(t) = 0$. $Q^l_{s_l}(t'+1) \leq Q^l_{s_l}(t') \leq \lambda V + v^{max} = p^l_{s_l}$,

Situation 2: $i \neq s_l$. The queuing law of $Q^l_i(t)$ is,

$$Q^l_i(t+1) = \max\left\{Q^l_i(t) - \sum\nolimits_{j \in \mathcal{U}, j \neq i} f^l_{ij}(t), 0\right\} + \sum\nolimits_{\{j | i \in \mathcal{U}, i \neq j\}} f^l_{ji}(t). \tag{5.40}$$

Since only one neighboring user can transmit to user i in time slot t, we denote him as user j. Considering the coefficient before $f^l_{ji}(t)$ in the objective function of S3, two situations are discussed:

- Case 1: $\frac{p^l_{s_l}}{p^l_i}Q^l_i(t) < \frac{p^l_{s_l}}{p^l_j}Q^l_j(t) - Y_{ji}(t)$. According to (5.40), $Q^l_i(t+1) \leq Q^l_i(t) + f^l_{ji}(t) \leq \frac{p^l_i}{p^l_j}Q^l_j(t) - \frac{p^l_i}{p^l_{s_l}}Y_{ji}(t) + f^l_{ji}(t) \leq \frac{p^l_i}{p^l_j}Q^l_j(t) \leq p^l_i$. The third inequality is satisfied due to the following reasons,

– $Y_{ji}(t) = 0$. Based on the solution to S1, $s_{ji}^{mc}(t) = 0$ and thus $f_{ji}^l(t) = 0$. The inequality holds.

– $Y_{ji}(t) \geq 1$. Since $f_{ji}^l(t) \leq \max\limits_{i \in \mathcal{U}, j \neq i} c_{ij}^{max} \Delta t$ and $\frac{p_i^l}{p_{s_l}^l} \geq 1$, we have $\frac{p_i^l}{p_{s_l}^l} Y_{ij}(t) \geq f_{ji}^l(t)$. The inequality is satisfied.

- Case 2: $\frac{p_{s_l}^l}{p_i^l} Q_i^l(t) \leq \frac{p_{s_l}^l}{p_j^l} Q_j^l(t) - Y_{ji}(t)$. Based on the solution to S3, $f_{ji}^l(t) = 0$. Following (5.40), we get $Q_i^l(t+1) \leq Q_i^l(t) \leq p_i^l$.

From the above proof, an arbitrary queue $Q_i^l(t)$ is finite in each time slot. With Definition 7, $\mathbf{Q}(t)$ is strongly stable.

Next, we prove the strong stability of $\mathbf{Y}(t)$ by considering an arbitrary queue $Y_{ij}(t)$. In particular,

$$Y_{ij}(t) \leq \max_{0 \leq k \leq t} \sum_{l \in \mathcal{L}} f_{ij}^l(k). \tag{5.41}$$

When $t = 0$, $Y_{ij}(0) = 0 \leq \max\limits_{0 \leq k \leq t} \sum_{l \in \mathcal{L}} f_{ij}^l(k)$.

When $t = t'(t' \geq 0)$, we suppose $Y_{ij}(t') \leq \max\limits_{0 \leq k \leq t} \sum_{l \in \mathcal{L}} f_{ij}^l(k)$. We prove that $Y_{ij}(t'+1) \leq \max\limits_{0 \leq k \leq t'+1} \sum_{l \in \mathcal{L}} f_{ij}^l(k)$ in the following.

- Case 1: $Y_{ij}(t) \leq \sum\limits_{m \in \mathcal{M}_i \cap \mathcal{M}_j} c_{ij}^m(t) s_{ij}^m(t) \Delta t$. Based on (5.20), $Y_{ij}(t+1) = \sum_{l \in \mathcal{L}} f_{ij}^l(t) \leq \max\limits_{0 \leq k \leq t+1} \sum_{l \in \mathcal{L}} f_{ij}^l(k)$.

- Case 2: $Y_{ij}(t) > \sum\limits_{m \in \mathcal{M}_i \cap \mathcal{M}_j} c_{ij}^m(t) s_{ij}^m(t) \Delta t$. Based on (5.20), $Y_{ij}(t+1) = Y_{ij}(t) - \sum\limits_{m \in \mathcal{M}_i \cap \mathcal{M}_j} c_{ij}^m(t) s_{ij}^m(t) \Delta t + \sum\limits_{l \in \mathcal{L}} f_{ij}^l(t)$. With inequality (5.16), $Y_{ij}(t+1) \leq Y_{ij}(t) \leq \max\limits_{0 \leq k \leq t} \sum_{l \in \mathcal{L}} f_{ij}^l(k) \leq \max\limits_{0 \leq k \leq t+1} \sum_{l \in \mathcal{L}} f_{ij}^l(k)$

Because $\sum_{l \in \mathcal{L}} f_{ij}^l(t) \leq c_{ij}^{max} \Delta t$, we have $Y_{ij}(t) \leq c_{ij}^{max} \Delta t$. Therefore, $\mathbf{Y}(t)$ is always finite and strongly stable. □

5.6.2 Lower and Upper Bounds for P1

In this subsection, we obtain both lower and upper bounds for the optimal results of P1, i.e., ϕ_{P1}^*.

Theorem 7. *The solution obtained from our proposed algorithm serves as a suboptimal solution to P1. And the corresponding time-averaged expected energy consumption holds an upper bound on the optimal result of P1, i.e.,* $\phi_{P1}^* \leq \phi_{P3}^*$. □

Proof: Our proposed algorithm finds a feasible solution to P3 in each time while satisfying all the constraints, e.g., (5.8), (5.11), (5.13)-(5.16) and (5.33). In addition, because (5.16) is satisfied and $\mathbf{Y}(t)$ is strongly stable as proved above, $\mathbf{Y}(t)$ is rate stable according to the Lemma 3. Hence, the constraint (5.19) holds as well. The solution in P3 is a feasible solution to P2. Because the problems P1 and P2 are equivalent, the solution in P3 is also a feasible solution to P1. The corresponding time-averaged expected energy consumption holds an upper bound on the optimal result of P2, i.e., $\phi^*_{P3} \geq \phi^*_{P1}$. □

Next, we find a lower bound on ϕ^*_{P1} as in Theorem 8.

Theorem 8. *The time-averaged expected energy consumption minimized by optimally solving P3, denoted by ϕ^*_{P3}, is within a constant gap $\frac{B}{V}$ from the time-averaged expected energy consumption achieved by P2, i.e., ϕ^*_{P1}. Specifically, we obtain,*

$$\phi^*_{P3} - \frac{B}{V} \leq \phi^*_{P1},$$

in which B and V are defined in previous sections. □

Proof: Please refer to Appendix A for the detailed proof. □

According to the Theorem 7 and the Theorem 8, we get a lower bound and an upper bound on the optimal result of P1, respectively, where,

$$\phi^*_{P3} - \frac{B}{V} \leq \phi^*_{P1} \leq \phi^*_{P3}. \tag{5.42}$$

Because B and V are independent, $\frac{B}{V}$ definitely goes to 0 as V increases. Thus, the gap between the upper and lower bound definitely becomes smaller. Thus, we could totally prove its sub-optimality theoretically.

5.6.3 Simulation Results

We evaluate the performance of our proposed approximation approaches in MATLAB on a computer with 4.0 GHz CPU and 32GB RAM. All the parameters are set in Table. 5.2. Specifically, users are located at $(375, 250)$, $(625, 250)$, $(300, 500)$, $(550, 500)$, $(800, 500)$, $(300, 750)$, $(550, 750)$, $(800, 750)$, $(375, 1000)$ and $(625, 1000)$ respectively as shown in Fig. 5.2.

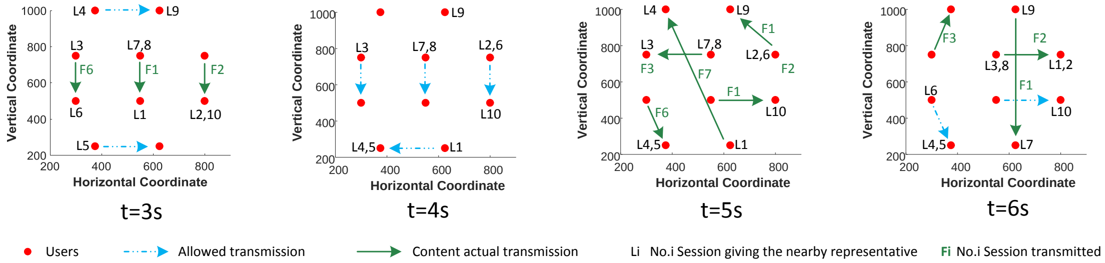


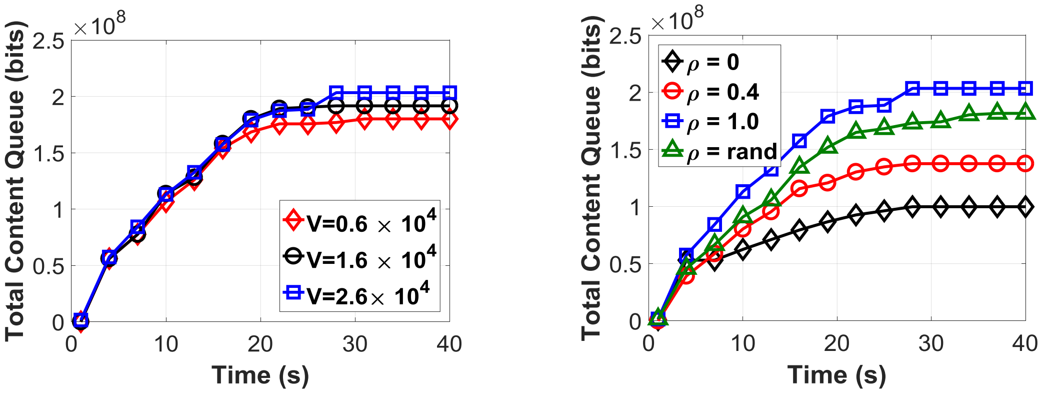
Figure 5.2: Dynamic Characteristics

Table 5.2: Simulation Settings

Parameter	Values
Area	$1000m \times 1000m$
Number of Users	10
Number of Time Slots	40
Duration in each time slot	1s
Bandwidth	$[1.2, 1.4, 1.6]\ MHz$
Modulation Strategy	$[2^3, 2^4, 2^5]$QAM
Bit Error Rate	10^{-3}
SINR Thresholds	$\{24.73, 52.98, 109.50\}$
Max. Transmission Power	2W
Noise Power Density	10^{-20}W/Hz
Path Loss	4
Weight V	4.6×10^4
User's Interest ρ	1

5.6.3.1 Content Queue Performance

Fig. 5.3 demonstrates the changes in content queue amount as time goes by. In each time slot, we sum up the content queue amount for each session at each user as the total one, which is dynamic and arrives at a stable state after a period of less than 30s. Such observation is consistent with the analysis in subsection 6.1. Thus, in the following simulations, we consider the time slots from 1 to 30 instead of 40. Besides, we check the effect on the content queue brought by the energy



(a) Energy Weight Controller V Effect

(b) User's Interest ρ Effect

Figure 5.3: Content Queue Performance

weight controller and the user's interest respectively. In Fig. 5.3a, the total content queue varies slightly under different energy weight controller. It is mainly because we factitiously initialize the content queue amount to be proportional to the energy weight controllers. On the other hand, the user's interest in the content session puts a positive effect on the content queue. If a user is more interested in each content, he would like to store contents and popularize them at the same time. Thus, he allows more contents to be kept in his queue. As can be seen in Fig. 5.3b, at the stable state, the total content queue is maximized when $\rho = 1.0$.

5.6.3.2 Dynamic Characteristics

The dynamic content queue in Fig. 5.3 introduces the dynamic performance to the whole system. Such dynamic characteristics are reflected on the representative user choice ($\mathbf{1_{i=S_l}}$) directly according to (5.36). As shown in Fig. 5.4, in each time slot, different representative users are chosen to receive different content sessions from the service provider. Meanwhile, the same content session is transmitted to different representative users in different time slots. As time goes by, the choice of different representative users becomes stable (from 25s to 31s), which indicates the stability of the entire system is reached.

Besides, we describe the dynamic content transmission choice from the time slot 3 to the time slot 6 in Fig. 5.2. The allowed and the actual content transmission pairs ($s_{ij}^m(t)$ and $f_{ij}^l(t)$) change in different time slots. In some time slots, e.g., the time slot 4, no contents are transmitted although a few transmission pairs are allowed. Whereas the contents are transmitted in all the

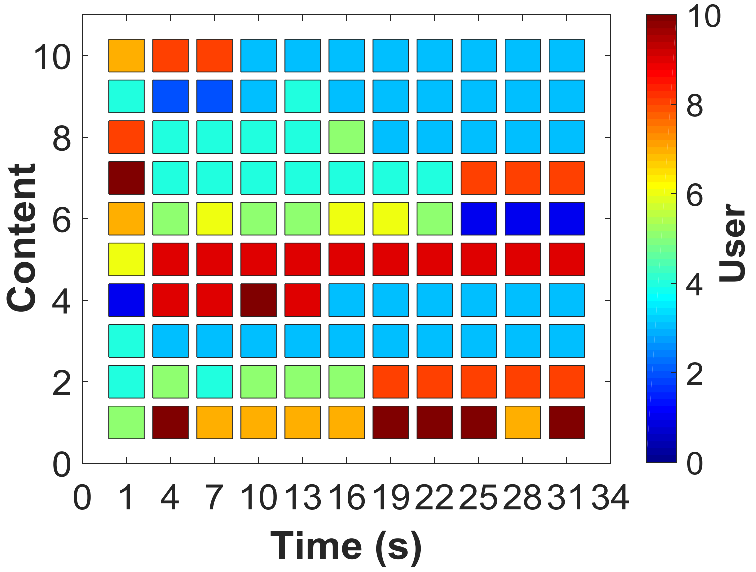


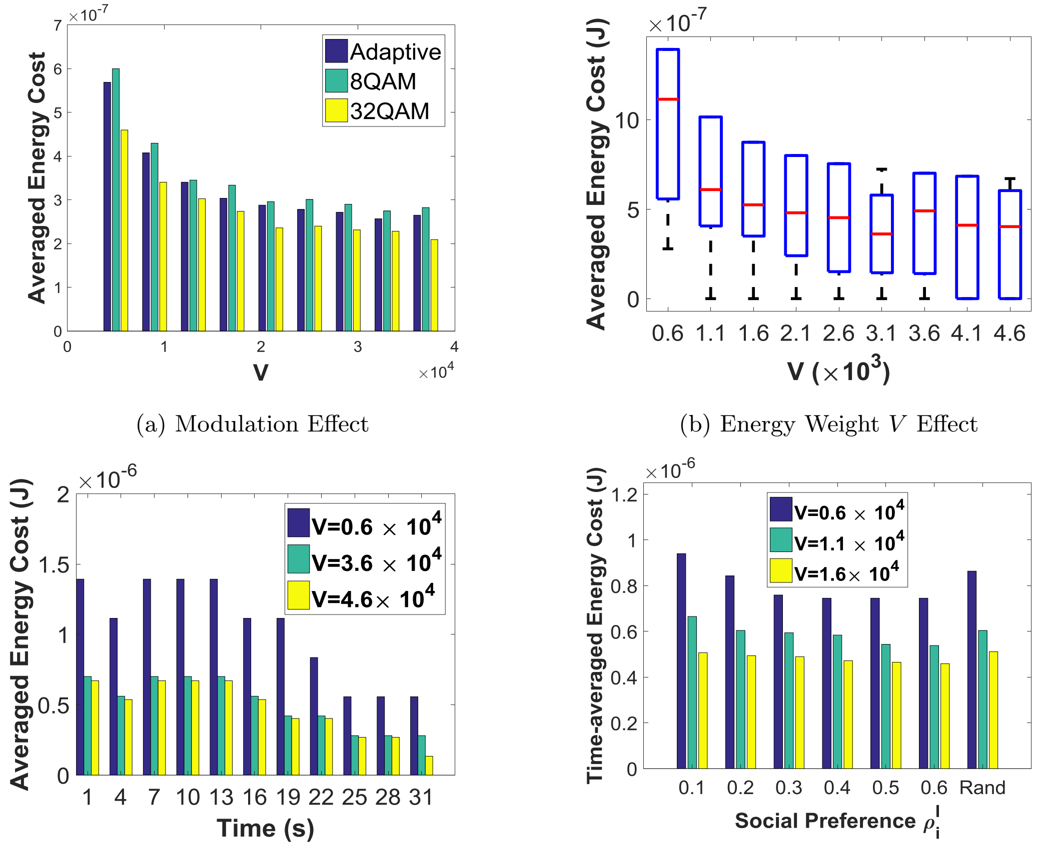
Figure 5.4: Representative Choice

allowed transmission pairs in some time slot, e.g., the time slot 5. Meanwhile, different content sessions are transmitted between different transmission pairs in different time slots. The dynamic content queue affects the offloading content amount as in **S3**, which puts an effect on both the content queue and the virtual queue like. The dynamic virtual queue affects the choice of the allowed transmission pairs as in **S2**. Thus, the system becomes dynamic but finally arrives at a stable state.

5.6.3.3 Energy Cost Performance

We consider the averaged energy cost for each user in each time in Fig.5.5. Fig. 5.5a shows the effect on the averaged energy cost brought by different modulation schemes. To achieve content successful transmission under random channel conditions, users have to choose different modulations schemes adaptively. Therefore, we see that the averaged energy cost under the adaptive M-QAM scheme is lower than that under 8QAM and higher than that under 32QAM.

Fig. 5.5b considers the averaged energy cost in time slot 2. As can be seen, the averaged energy cost decreases with the increase of the energy weight controller, which is consistent with our description previously. Fig. 5.5c shows the changes in the averaged energy cost as the time goes by, from which the average energy cost becomes almost the same after 20 time slots. The dynamic averaged energy cost performance is the same as that of the content queue amount. Besides, we demonstrate the time-averaged energy cost under users' social preferences in Fig.5.5d, where "Rand" means users have different interests in different contents. Users would like to cache their interested contents instead of disseminating them, especially in bad channel conditions. Therefore, we see that the time-averaged energy cost decreases with the increase of social preference.



(a) Modulation Effect

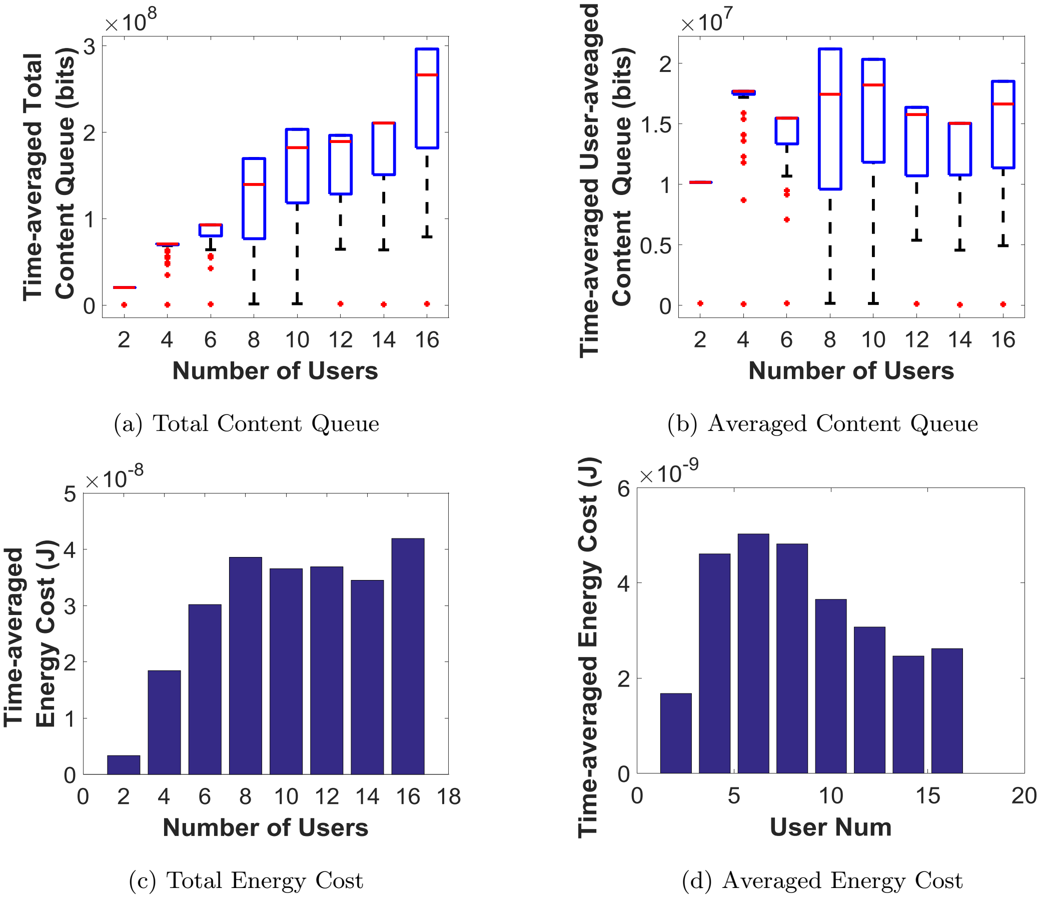
(b) Energy Weight V Effect

(c) Time Effect

(d) Social Effect

Figure 5.5: Energy Cost Performance

Meanwhile, as energy weight controller V increases, the difference of time-averaged energy cost between social preferences becomes smaller in Fig.5.5d. Social preference's effect on the energy cost results from its effect on the maximum queue size. When V becomes larger, keeping queue stability becomes less important. Users could cache more contents no matter how much they are interested in the contents. Hence, the total energy cost is lowered. Besides, social preference's effect on the energy cost becomes subtle. When V becomes smaller, users have to strictly guarantee their queue stability. They could not cache too much in their buffers. Therefore, they have to offload more contents to other users, which increases the energy cost. Meanwhile, due to the strict requirement to queue stability, users cache their most interested contents. Thus, their social preferences will greatly affect the energy cost.



(a) Total Content Queue

(b) Averaged Content Queue

(c) Total Energy Cost

(d) Averaged Energy Cost

Figure 5.6: User Number Effect

5.6.3.4 User Number Effect

Besides the above consideration, we compare the content queue and energy cost performance under a different number of users. Specifically, we consider the cases with 2, 4, 6, 8, 10, 12, 14 and 18 users respectively. The minimum distance among users in each case is set to 250m. In Fig.5.6a, we consider the time-averaged total content queues, where the content queue amount increases as the number of users increases. In Fig. 5.6b, we further average the content queue over the user number. The time-averaged user-averaged content queue jumps among the cases with different numbers,

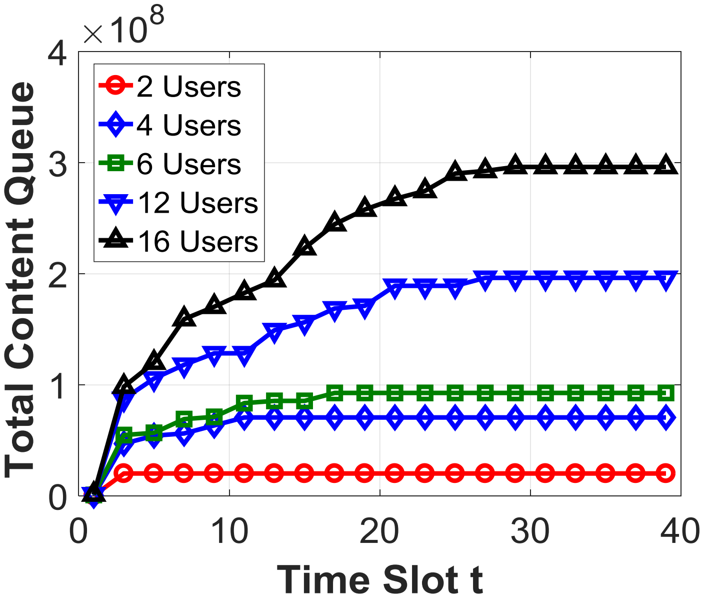


Figure 5.7: Reaching Steady State Speed

which indicates the introduction of more users does not affect the stability of the content queue. In addition to time-averaged total content queue performance, the time-averaged energy cost also increases with the introduction of more users whereas per-user time-averaged energy cost decreases, which are shown in Fig. 5.6c and 5.6d respectively.

Finally, we investigate our solution's speed to a steady network state. As shown in Fig.5.7, when a few users exist, they can reach a steady network state very soon. When the number of users increases, it takes a longer time to reach a steady state. Since users are always in a changing environment, the speed of reaching a network state does not affect users to offload or to access data as long as they do not reach the maximum queue size. Such observations further demonstrate that our proposed online optimization solution is not affected by the number of users, which means our solution does not suffer from the “curse of dimensionality”.

5.7 Chapter Summary

In this chapter, we propose a social-aware energy-efficient data offloading approach to reduce energy consumption and achieve green communication in the cellular network. By jointly considering storage capacity allocation, queuing and transmission scheduling, we design an offline energy consumption minimization problem, which is a time-coupling stochastic MINLP problem. By introducing a virtue queue and employing Lyapunov drift-plus-penalty theory, we reformulate the problem as an online finite-queue-aware energy consumption problem, which is decoupled and then decomposed into several separate subproblems in each time slot. The proposed method ensures the network with strong stability. Both lower and upper bounds on the optimal result of the original optimization problem are obtained. Based on the simulation results, we show the feasibility and efficiency of our approximation approach.

Chapter 6

Secure and Optimized Unauthorized Secondary User Detection in Dynamic Spectrum Access

6.1 Chapter Overview

The proliferation of mobile and interconnected devices has exacerbated the depletion of licensed wireless spectrum bands in the recent decades. Dynamic System Access (DSA) has received considerable attention recently due to its ability to alleviate the spectrum scarcity issue. In a DSA system, a spectrum operator, who regulates the licensed spectrum, authorizes the secondary user (SU) to opportunistically use the spectrum when it is not occupied by primary users. However, the open nature of the wireless medium makes the DSA system a potential target for unauthorized access. Specifically, by faking/replaying the spectrum permit (denoted as permit hereinafter), unauthorized SU can use any available spectrum bands and introduce severe interference to authorized SU who is currently using the designated spectrum bands. As a result, the authorized SU will lose interests on participating in DSA and thus the benefits brought by the DSA system are largely deteriorated.

Therefore, it is highly needed to devise an efficient and accurate unauthorized SU detection scheme to ensure the DSA system and further unleash its great potential for future wireless systems with cognitive capabilities.

Physical-layer authentication is an effective way to distinguish unauthorized SU from authorized SU without having to complete higher-layer processing [97, 98, 105, 106, 185]. Specifically, the authorized SU embeds an unforgeable permit into its data traffic using techniques related to the physical layer. A third party named as the verifier passively eavesdrops on the SU's transmission and tries to detect and verify the permit. Yang *et al.* [185] add cryptographic permit into OFDM symbols for detection. Permit is concealed via inter-symbol interference in [106]. These two schemes negatively impact normal data transmission. Jin *et al.* [98] embed the permit by using dynamic power control on transmitted signals. FEAT scheme in [105] embeds the authentication information into the transmitted waveform by inserting an intentional frequency offset. It takes a long time to detect the unauthorized SU in these two schemes, which gives the unauthorized SU opportunity to transmit its information without being detected. By concealing the permit into the cyclic prefix in [97], the fake/replayed permit can be detected, which is impractical due to the modification of the existing physical layer protocols. These identified weaknesses motivate us to design an accurate, efficient and implementable unauthorized SU detection scheme, which not only ensures the current DSA system but also becomes a crucial component adapted to future wireless systems [4].

In this chapter, we propose a novel unauthorized SU detection scheme based on hierarchical modulation [95], where permit symbols generated using a hash function and data symbols are synchronously aggregated before transmission. To overcome the intrusion to data transmission, the operator picks up a proper power allocation scalar between the permit and data transmission power, which allows the reliable transmission of both permit and data. Different from the traditional hierarchical modulation, the operator modulates the permit using rotation multiple layer modulation (RMLM), in which permit bits are first grouped, modulated, rotated and finally added together. By choosing proper rotation angles based on the current channel condition, which sensors in DSA obtain by performing channel estimation and then return to the operator, RMLM not only helps permit information to resist the noise but also prevents unauthorized SU faking/preventing the permit. The parameters related to the hash function, the power allocation scalar, the rotation angles in RMLM together with permit rotation angles are sent to the verifier through an authenticated and encrypted channel at the beginning of the spectrum authentication by the operator. At the verifier, MMSE-SIC (Minimum mean square error-Successive interference cancellation) is deployed to detect the permit information. Together with RMLM, our scheme can achieve permit reliable transmission with high transmission rate [165]. Since no extra knowledge is needed at the authorized SU receiver, our scheme does not change the existing physical-layer protocols. We highlight and list our **contributions** as follows:

- We propose a novel unauthorized SU detection scheme, which prevents unauthorized users from capturing the authorized SU's spectrum bands.
- We deploy an improved hierarchical modulation to embed permit information into data transmission. A proper power allocation scalar is chosen to reduce the permit's intrusiveness to normal data transmission.
- Based on the current channel condition, we optimize the permit RMLM and achieve high efficiency and accuracy in unauthorized SU detection.
- By combining the permit embedding at the SU transmitter and MMSE-SIC at the verifier, a satisfactory permit error performance is achieved.

The rest of this chapter is organized as follows: In Section 6.2, we briefly review the existing unauthorized SU detection schemes and study the literature of RMLM and MMSE-SIC. Then, we give a description of our system model and the proposed framework in Section 6.3. In Section 6.4, we elaborate the scheme from the following four parts: permit generation and encoding, permit modulation, permit embedding, and permit detection and verification. To show the security effectiveness of our proposed scheme, we analyze the resilience to emulation and replay attacks, as well as the comprising attack in Section 6.5. Both permit and data detection performance are thoroughly evaluated in Section 6.6, followed by the conclusion in Section 6.7.

6.2 Related Work

In this section, we review the prior works closely related to our proposed scheme.

6.2.1 Unauthorized SU Detection

Previous methods on safeguarding the DSA system is to deploy cryptographic schemes [12, 57, 126, 130] at the higher layers where messages carried by the waveform are detected for authentication. Different with those mechanisms, the physical layer-based authentication approaches enable a receiver to distinguish the authorized SU and the unauthorized SU without involving higher-layer processing. This fact brings obvious advantages on efficiency improvement. More importantly, the physical layer-based detection is indispensable in some cases. For example, in the heterogeneous coexistence environment, e.g., IEEE 802.22 and 802.11af systems coexisting in TV white space, incompatible system may not be able to decode each others' higher layer signals. Thus, the research on the physical layer-based detection approaches, such as RF fingerprinting in [26, 83, 166] and authentication signal embedding in [97, 98, 105, 106, 142, 163, 185], attract a lot of attentions.

6.2.2 Superposition coding (SC) and MMSE-SIC

Hierarchical modulation is considered as a practical implementation of SC [131] while RMLM is the extension of SC. Tse *et al.* [42,91,128,129,165] assume SC to be an alternative scheme for high throughput transmission. An interesting feature of SC is that the transmitted signal exhibits an approximately Gaussian distribution, which provides a more straightforward approach for achieving the so-called shaping gain [56,167,169] as demonstrated in [129]. Successive interference cancellation (SIC) is a physical-layer detection strategy at the receiver. As is described in [165], in SIC, one of the users, say user 1, is decoded treating user 2 as interference, but user 2 is decoded with the benefit of the signal of user 1 already removed. It has been proven that the transmission rate of users in the capacity region can be achieved by deploying SC at the transmitter and SIC at the receiver in [165]. Therefore, we apply SC and SIC to improve the accuracy and efficiency of both permit and data transmission.

6.3 System Model and Framework Overview

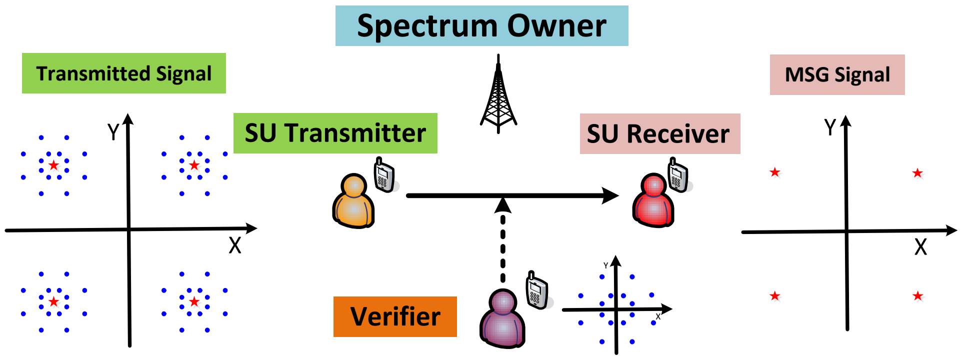


Figure 6.1: System Model of the Optimized Detection Scheme

6.3.1 System Model

As shown in Fig.6.1, our system model contains three entities.

- Spectrum Operator: It refers to a licensed spectrum owner or a spectrum-service provider that regulates spectrum sharing. A typical example is the SAS in 3.5GHz band [38]. When a SU requests an unoccupied spectrum, the spectrum operator allows the SU transmission by sending it the spectrum authorized information. To prevent unauthorized access, the spectrum operator recruits multiple verifiers in the specific area. Besides, the spectrum operator optimizes the permit embedding by picking up a proper allocation scalar and rotation angles in RMLM according to the known current channel condition (In 3.5GHz, it is sensed by Environmental Sensing Capability sensors (ESC) and reported to SAS), which are sent to the SU and its nearby verifier. Either according to a pre-determined random schedule or when the authorized SU in a particular area reports abnormal interference, the spectrum operator authorizes the SU and the verifier to begin permit detection process.

- Secondary Users (SU): A SU requests and pays for a given licensed spectrum at the desired location and time. As soon as receiving permit detection indication from the spectrum operator, the SU transmitter embeds the permit into its data and transmits the aggregated symbols. The SU receiver has no idea about the permit embedding and detects data information without any changes on the physical layer.

- Verifier: It extracts the permit information from the received signal and does not participate in normal data transmission. Even if the verifier detects data symbols, it cannot know the data information due to the lack of higher layer protocols. After authentication, the verifier reports its results to the spectrum operator who will then physically locate and further punish the illegitimate transmitters.

6.3.2 Attack Model

We define the attacker as the unauthorized SU who transmits without authentication either by accident or misconfiguration, or who illegally accesses the spectrum to avoid costs of spectrum occupation. Given the flexibility of today's cognitive radios, above operations can be done by controlling its transceiver to manipulate its physical-layer symbols. Without a valid permit, the attacker tries to compromise the spectrum by faking/replaying one. Meanwhile, we assume that the unauthorized SU is computationally bounded and cannot break the cryptographic primitives used to generate the permit. Finally, the unauthorized SU can compromise the verifier to report incorrect results to the spectrum operator.

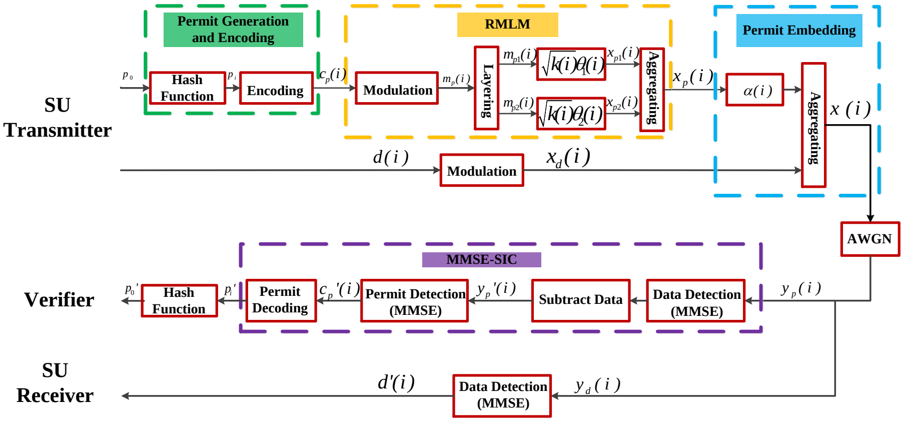


Figure 6.2: Framework of the Secure and Optimized Detection Scheme

6.3.3 Framework Overview

The framework of the proposed detection scheme is shown in Fig.6.2. The permit sequence p_i in time slot i is encoded as the coded bit sequence $c_p(i)$, which is then mapped into permit symbol sequence $x_p(i)$ using RMLM:

$$x_p(i) = \sqrt{k(i)}(m_{p1}(i)e^{j\theta_1(i)} + m_{p2}(i)e^{j\theta_2(i)}) \tag{6.1}$$

which is then added to the modulated data symbol sequence $x_d(i)$. Given the AWGN noise $n_d(i)$ with mean 0 and variance σ^2, the received signal $y(i)$ at the SU receiver is:

$$y_d(i) = x_d(i) + x_p(i)e^{j\alpha(i)} + n_d(i) \tag{6.2}$$

MMSE is used to detect the data bit sequence $d'(i)$ from $y_d(i)$.

The received signal $y_p(i)$ at the verifier is:

$$y_p(i) = x_d(i) + x_p(i)e^{j\alpha(i)} + n_p(i) \tag{6.3}$$

where $n_p(i)$ is the AWGN noise with the same mean and variance with $n_d(i)$. We apply MMSE-SIC to detect the permit p'_i. The verifier detects data symbols while treating permit symbols as interference at first. After subtracting detected data symbols, the remaining part is decoded as the permit p'_i using MMSE.

6.4 Optimized Unauthorized SU Detection Scheme

In this section, we elaborate the proposed unauthorized SU detection scheme. Mutual information (MI) between the transmitter and receiver is a measure of transmission rate on the premise of reliable communication [165]. Therefore, we choose the rotation angle in permit RMLM by maximizing MI to achieve the accurate and efficient permit detection. As for permit embedding, the power allocation scalar and the rotated angle for permit symbols are discussed step by step. Due to the same detection scheme optimization in each time slot, we ignore the time slot expression i in the following.

6.4.1 Permit Generation and Encoding

Before elaborating the scheme in detail, we make three assumptions to ensure the entire process, which is the same as those in [98]. First, the geographic region is divided into non-overlapping cells of equal size to avoid the inter-cell interference. In each cell, we assume that the idle spectrum is divided into non-overlapping channels to prevent the intra-cell interference. Finally, time is divided into slots of equal length. To ensure the correct detection for permit and data, all entities are assumed to be loosely synchronized to a global time server.

An efficient one-way hash chain is deployed by the operator to generate the unforgeable spectrum permits. Denote $h(x)$ as a cryptographic hash function on x and $h^{\eta}(x)$ as η successive operations on $h(\cdot)$ to x. An SU transmitter requests a spectrum usage by specifying a band index, an area index, and a time duration γ. Receiving the request, the spectrum operator transmits a random number p_{γ} to the SU transmitter securely. The SU transmitter recursively computes $p_i = h(p_{i+1})$, $i \in [1, \gamma - 1]$ as its permit in time slot i. The spectrum operator also generates $p_0 = h^{\gamma}(p_{\gamma})$ and sends it to the verifier.

To tolerate transmission errors resulted from the noise and reduce the hardware cost, the permit is encoded using repetition code $\mathcal{C}_m$ with system parameter m. Other encoding techniques, such as convolutional code and turbo code, can also be applied, which further improves the permit detection efficiency by paying the complexity cost.

6.4.2 Permit RMLM

Given the permit RMLM process in Fig.6.2, we first show an example of permit constellation assuming $\theta_1 = 0$ and $\theta_2 = \pi/6$ in Fig.6.3 after RMLM. We employ Quadrature Phase Shift Keying (QPSK) to modulate the permit bits. It is widely applied in many applications and standards such as IEEE 802.11b and IEEE 802.11g. General quadrature amplitude modulation is also supported. In Fig.6.3, the two bits in angle brackets represent permit bits in the first layer while those in parenthesis indicate permit bits in the rotated second layer. Every four bits correspond to one permit symbol.

6.4.2.1 Rotation Angle Effect

As shown in Fig.6.3, the choice of rotation angle affects the permit transmission reliability due to its effect on the minimum distance between permit symbols. In AWGN channel, increasing the minimum distance is an effective method to enhance the noise-resilient capability [63]. A worst case is $\theta_1 = 0$ and $\theta_2 = \pi/2$ under which the minimum distance becomes 0. The verifier cannot distinguish permit bits from the detected permit symbols. Therefore, how to choose a proper rotation

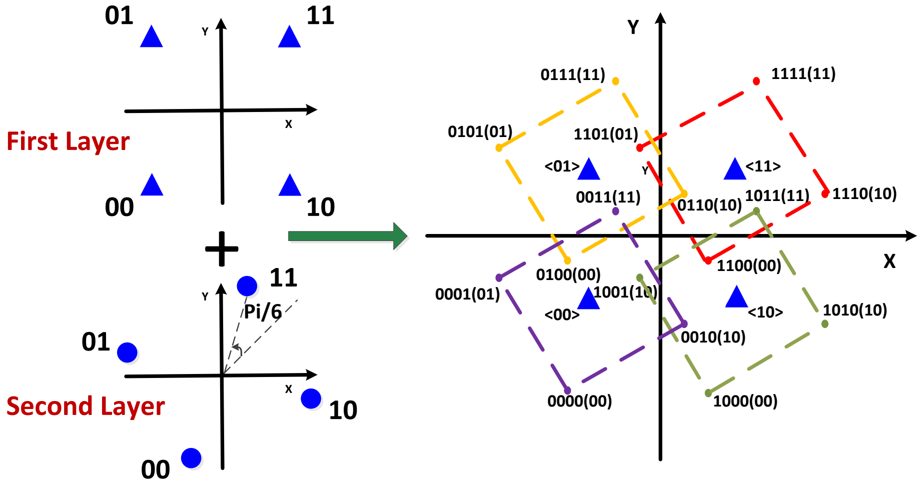


Figure 6.3: An Example for Permit Symbol Constellation

angle becomes the key part in permit RMLM. Since the repition code $\mathcal{C}_m$ encoding the permit has an strong error correcting capacity of $(m-1)/2$, we consider the permit transmission quality instead of its recoverability at the verifier in our scheme. According to [67], the input−output MI is an indicator of how much coded information can be pumped through a channel reliably given a certain input signaling. Therefore, we pick up the rotation angle by maximizing MI.

Assuming we have subtracted the data symbols at the verifier. Since choosing the proper rotation angle is the same in each time slot, we rewrite the permit at the SU transmitter and the verifier as $U = U_1 + U_2 e^{j\theta}$ and $V = U + N$, where U_1, $U_2 e^{j\theta}$, U represent $\sqrt{k(i)}m_{p1}(i)$, $\sqrt{k(i)}m_{p2}(i)e^{j\theta_2(i)}$ and $x_p(i)$ respectively. The noise $n_p(i)$ in (6.3) is denoted as N with zero mean and variance σ^2. Our goal is to find a proper θ by maximizing MI between V and U:

$$\begin{aligned} \max_{\theta} \quad & I(U;V) \\ \text{s.t.} \quad & 0 \leq \theta \leq 2\pi \end{aligned} \tag{6.4}$$

where $I(U;V) = \sum_{u \in U, v \in V} p(uv) \log_2 \frac{\sum_{u' \in U} p(v|u')p(u')}{p(u)}$ [42]. The joint distribution of the input u and output v, the probability distribution function (PDF) of u, and the PDF of v on the knowledge of u' are $p(uv)$, $p(u)$, and $p(v|u')$, respectively. When the probability of each elements in U is equal, the MI gets the maximum value [42]. It is written as:

$$I(U;V) = \log_2 M - \frac{1}{M} \sum_{\substack{u_m \in U \\ v \in V}} p(v|u_m) \log_2 \frac{\sum\limits_{u_j \in U} p(v|u_j)}{p(v|u_m)} \tag{6.5}$$

where $p(v|u_j) = \frac{1}{\pi\sigma^2}\exp(\frac{-|v-u_j|^2}{\sigma^2})$. M denotes maximum number of permit symbols after RMLM. Using QPSK modulation, $M = 16$.

6.4.2.2 MI Optimization

Denote $d_{mj} = \frac{u_m - u_j}{\sigma}$ and $t = \frac{v - u_m}{\sigma}$. Due to the complex and continuity of the received signal V, rewrite $I(U;V)$ in (6.5) as:

$$I(U;V) = \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \int\limits_{-\infty}^{+\infty} \int\limits_{-\infty}^{+\infty} \exp\left(-|t|^2\right) \times \left\{ \log_2 \sum_{j=1}^{M} \exp\left(-2t \cdot d_{mj} - |d_mj|^2\right) \right\} dt \tag{6.6}$$

Assume $f_m(t) = \log_2 \sum_{j=1}^{M} \exp\left(-2t \cdot d_{mj} - |d_{mj}|^2\right)$, $I(U;V)$ is expressed by Gussian-Hermite numerical integration as:

$$I(U;V) = \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \int\limits_{-\infty}^{+\infty} \int\limits_{-\infty}^{+\infty} \exp\left(-|t|^2\right) f_m(t)\, dt = \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \sum_{p_1=1}^{P} W_{p_1} \sum_{p_2=1}^{P} W_{p_2} f(t_1, t_2) \tag{6.7}$$

where P, W_{p1}, W_{p2}, t_1 and t_2 are the parameters that can be found in [10].

The $I(U;V)$ in (6.7) is a function with variable θ concealed in $f_m(t)$. The MI maximization problem becomes:

$$\begin{aligned} \max_{\theta} \quad & \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \sum_{p_1=1}^{P} W_{p_1} \sum_{p_2=1}^{P} W_{p_2} f(t_1, t_2) \\ \text{s.t.} \quad & 0 \le \theta \le 2\pi \end{aligned} \tag{6.8}$$

We solve the above optimization problem by a numerical global research method [104], which can be implemented using the MATLAB Global Optimization Toolbox. This method is a gradient-based algorithm using multiple randomized starting points to find different local optimal values of a smooth nonlinear optimization problem [27].

6.4.2.3 Rotation Angle Chosen

We figure the relationship between the rotation angle and the MI in Fig.6.4 assuming the Signal-to-Noise Ratio $SNR = 20\text{dB}$ and $k = 0.25$. The opmital rotation angle is $\theta^* = \pi/4$ and the figure is about θ symmetric. In Fig.6.5, the permit constellations are plotted together when $\theta = \pi/6$ (red solid circle) and $\theta = \pi/3$ (blue hollow circle). Combining Fig.6.4 and Fig.6.5, we conclude that the permit constellations are totally different under different rotation angles even if their effects on MI are similar, e.g., $\theta = \pi/6, \pi/4, \pi/3$. Motivated by above observations, the spectrum operator is designed to choose a list of sequential rotation angles randomly based on the current channel condition, e,g., $\boldsymbol{\theta} = \{\pi/6, \pi/4, \pi/3, \pi/3, \pi/4, \cdots\}$ at 20dB, which are sent to the verifier and SU respectively.

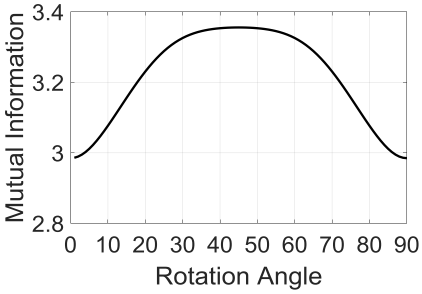


Figure 6.4: MI vs Rotation Angle

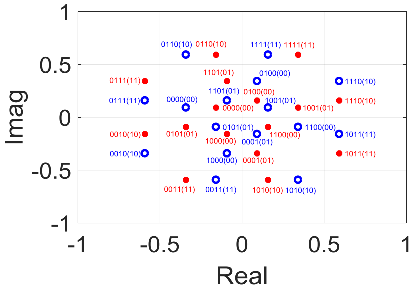


Figure 6.5: Permit Contellation after RMLM

6.4.3 Permit Embedding

6.4.3.1 Power Allocation

Although the permit symbols and data symbols can be transmitted simultaneously, the embedded permit symbols are actually the interference of data symbols, which brings negative impacts to the data transmission. To alleviate such negative impact, we introduce the power allocation scalar k. Assume the unit total power, the power of the permit and the data is k and $1 - k$ respectively. We will thoroughly investigate the power allocation via the experiment in Section V to choose a proper one under which the reliable transmission of both the permit and data is achieved.

6.4.3.2 RMLM Permit Symbol Rotation

The motivation to rotate RMLM symbols when embedded into data is to increase the data detection accuracy and further improve the permit detection performance. Specifically, we rotate RMLM permit symbols with an angle α when they are embedded to the data symbols in the first quadrant, such that the minimum distance between aggregated symbols and the vertical/horizontal axis is maximized. The aggregated symbols are then made symmetric along the vertical axis, the central point, and the horizontal axis to construct the constellation. Since QPSK and MMSE-SIC employed at the SU transmitter and the verifier respectively, the above minimum distance maximization effectively helps resist against the interference to the transmitted symbols brought by the noise. Data symbols are detected with better accuracy and thus an improved permit detection is achieved. Meanwhile, the data detection performance is also improved at the SU receiver.

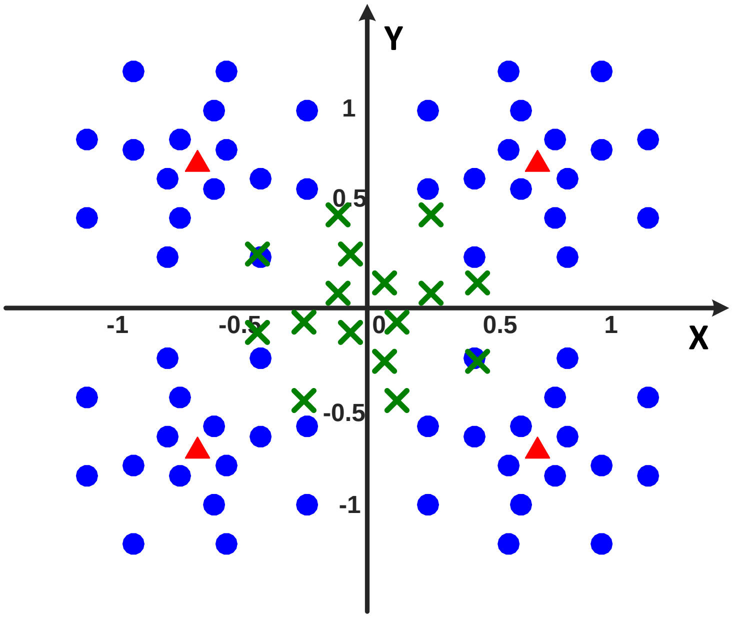


Figure 6.6: Constellation of the Transmitted Symbols

An constellation example of the transmitted symbols is shown in Fig.6.6 with $k = 0.25$, $\theta = \pi/6$, and $\alpha = 0$, in which x marks, red triangles and green blue dots represent the constellations of the original permit symbols, the original data symbols and the final transmitted symbols respectively. In practice, a permit can be transmitted via one or multiple data packets. Permit embedding starts after the preamble and header transmission until either permit bits are all sent or the data symbols all are used up [98]. In our scheme, each data symbol carries four permit bits due to two layers' aggregation in RMLM. More permit bits can be embedded by increasing the number of layers.

6.4.4 Permit Detection and Verification

6.4.4.1 Permit and Data Detection

MMSE-SIC is deployed to detect the permit at the receiver. With the received signal, the verifier first detects each QPSK data symbol sequentially by using MMSE. Specifically, the verifier suggests the QPSK constellation point nearest to the received signal as the transmitted data symbol, e.g., red triangular in Fig. 6.6. The detected data symbol is then subtracted from the received signal. At the same time, the verifier makes a re-symmetry for the remained signal according to the position of the detected data symbol. If it is in the second/three/four quadrant, the verifier finds the point that is symmetric with the remained signal about the vertical/central/horizontal axis as the received permit signal. Similar with the data detection, the verifier detects the permit symbols using MMSE. According to the mapping rules between permit symbols and permit bits, the verifier can easily get the transmitted permit bits, which is then decoded as either 0 or 1 by using the hard-decision strategy. Since each permit bit has been consecutively repeated m times, the majority rule is then applied to determine each permit bit. Note that the verifier reconstructs the permit constellation based on k, α, and θ, e.g., green cross ($\times$) in Fig. 6.6.

Permit transmission and detection are totally transparent to the SU receiver as if it does not know the existence of permit. The SU receiver still performs QPSK demodulation.

6.4.4.2 Permit Detection in Practice

In practice, the start of the permit detection is similar with that in [97,98]. The verifier keeps detecting the permit from physical-layer signals on the corresponding band in a specific duration. It first detects the preamble for synchronization and obtains the packet size from the header, followed by the permit detection. If the verifier misses the preamble of the current packet, it detects the permit from the upcoming packet.

6.4.4.3 Permit Verification

Denote the detected permit in time-slot i as p'_i. To verify the transmitter's identity, the verifier computes p'_0 by i successive operations of the same hash function h on p'_i, $p'_0 = h^i(p'_i)$. If $p'_0 \neq p_0$, verifier suggests this transmitter is an unauthorized SU. Otherwise, the specific band is assumed to be securely used by an authorized SU. All the detection results are finally reported to the spectrum operator who will take further measures according to the receiving results.

6.5 Security Analysis

By emulating an authorized SU transmitter, replaying an overheard permit, or compromising the verifier to report incorrect results to the spectrum operator, the unauthorized SU may access the spectrum illegally. Our proposed scheme is resilient to above attacks.

6.5.1 Emulation Attack

A successful emulation attack is achieved if an unauthorized SU provides a proof of the SU transmitter's identity to mislead the verifier to believe that the current spectrum is occupied. Specifically, the unauthorized SU launches an emulation attack if it derives a fake permit which is the same as that of the SU transmitter. However, such emulation attack is impossible in our scheme. The unauthorized SU does not have the computational ability to break the cryptographic primitives. Therefore, it cannot obtain the permit in the next time slot without the root of the hash chain. However, the unauthorized SU may occasionally create the same permit. Fortunately, the length of the permit generated using hash function is long enough, so we can ignore such case. Taking SHA-1 for example, which is one of the most widely used cryptographic hash functions, it generates 160-bit values. The maximized probability of generating the same permit is $1/(2^{160})$, which is negligible. Therefore, our scheme can successfully prevent the emulation attack.

6.5.2 Replay Attack

Although the unauthorized SU cannot derive a fake permit, it may eavesdrop on a SU transmission, extract its permit, and then attempt to use it for its data transmission. To prevent the unanthorized SU from extracting the permit, we provide three barriers. As mentioned in IV-B-3) part, the angles calculated based on the current channel condition are put into the roatation angle list randomly, which is sent to the SU transmitter and the verifier through an authenticated and encrypted channel. Both the SU transmitter and the verifier process the permit using the rotation angles sequentially and consistently. Therefore, the first barrier in our scheme is the channel estimation. With wrong channel estimation, it is difficult for the unauthorized SU to know the rotation angle range. Even though the unauthorized SU guesses the range successfully, the randomness of the chosen rotation angles sets up a new obstacle for the unauthorized SU to know the current rotation angle based on the previous knowledge. Meanwhile, as shown in Fig.6.5, the constellation patterns of the permit under different rotation angles are totally different. Hence, the unauthorized SU is almost impossible to guess the permit exactly without the rotation angle. Taking a step back, if the unauthorized SU luckily extracts the current permit, it cannot replay the permit in the next slot without the hash root. Therefore, a lion is in the way for the unauthorized SU to extract the current permit and further replay one to deceive the verifier.

6.5.3 Compromising Attack

By compromising the verifier to report the wrong detection results to the spectrum operator, the unauthorized SU can access the spectrum "legally". To solve such problem, the spectrum operator deploys a number of verifiers to patrol the potential transmission area. By receiving detection results from various verifiers and combining them using known consensus distributed algorithms [41], the probability of wrong spectrum occupation judgment is greatly lowered.

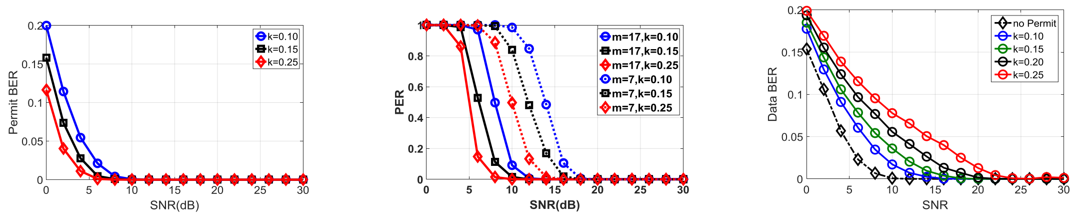
6.6 Performance Evaluation

In this section, we evaluate the performance of our secure and optimized detection scheme using both MATLAB simulations and the USRP experiment.

6.6.1 Evaluation Settings

In the evaluation, we use SHA-1 with 160-bit long as the hash function for the permit generation. 100 data packages with payload length of 2000 bytes each are transmitted in each time slot. As shown in Fig. 6.2, we assume the aggregated symbols are transmitted in an AWGN environment with the noise variance σ^2, the power of which is normalized. SNR is defined as

$SNR = \frac{1}{\sigma^2}$. We evaluate the permit detection performance based on permit bit-error-rate (BER) and permit error rate (PER). In particular, PER is approximated by the probability when all the 160 permit bits are correctly extracted. The data detection performance is measured using data bit-error-rate (data BER).



(a) Permit BER with $m = 17$

(b) PER

(c) Data BER

Figure 6.7: The Impact of Power Allocation Scalar k on Performance

6.6.2 Results in MATLAB Simulations

6.6.2.1 Permit BER Performance

In Fig.6.7a, the permit BER decreases to 0 when SNR is near 15dB with $m = 17$ and $k = 0.10$. By increasing k, the permit BER performance improves. In a very poor wireless channel, e.g., SNR = 5dB, our detection scheme obtains a satisfactory permit BER performance.

6.6.2.2 PER and Data BER Performance

PER Performance. Since the one-way hash function is used, we have to ensure the correctness of each permit with 160 permit bits. The relationship between the permit BER P_b and the PER P_p is calculated theoretically as:

$$P_p = 1-(\binom{m}{\lceil m/2\rceil}(1-P_b)^{\lceil m/2\rceil}P_b^{m-\lceil m/2\rceil}+\binom{m}{\lceil m/2+1\rceil}(1-P_b)^{\lceil m/2+1\rceil}P_b^{m-\lceil m/2+1\rceil}+\cdots+(1-P_b)^m)^{160} \tag{6.9}$$

In Fig.6.7b and Fig.8, we see that our scheme can achieve a very low PER. Taking the case with $m = 17$, $k = 0.25$ as an example, when SNR equals 2|4|6|8|10|12dB, the PER is 1.00|0.86|0.14|0.02|0.0009|0. We compare the PER performance between our proposed scheme and schemes in [98] as illustrated in Fig.6.11a. With the same repetition parameter $m = 17$ and similar power allocation scalar k, our scheme achieves a lower PER. Note that we evaluate the power allocation scalar in [98] by squaring its system parameter k. When $k = 0.4949$ and 0.4241 in [98], the power allocation scalar equals to 0.2499 and 0.1799.

The impact to Data detection. From Fig.6.7c and Fig.9, we see that the data can be correctly transmitted with SNR $>$ 15dB. This is consistent with the fact that accurate data transmissions are unlikely to occur in poor wireless channels. In addition, the data BER performance is compared between the case without permit transmission and the case with spectrum permits of different allocating power in Fig.6.7c, which shows that introducing permit brings 3dB SNR reduction. To further show the relationship between the permit and the data transmission, we joint consider the performance of PER and data BER as shown in Fig. 6.8 with $m = 7$. When SNR $=$ 12dB, the power allocation scalar k is equaled to $0.10, 0.15, 0.2, 0.25$ and 0.3, respectively. The setting of k in other SNRs is similar. Obviously, the closer the curves to the origin, the lower decoding errors for the permit as well as the data BER. From Fig. 6.8, we find that the permit brings a negligible negative impact to the data transmission even in poor wireless channels [62]. When SNR $>$ 15dB and $k > 0.20$, both PER and data BER approach to the origin.

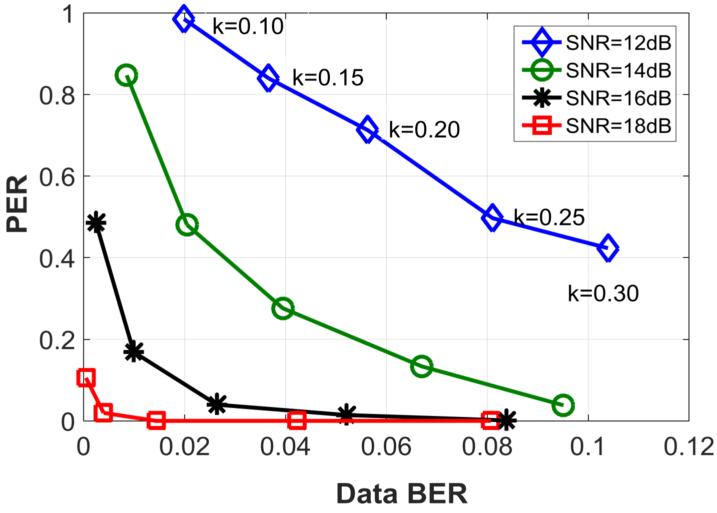
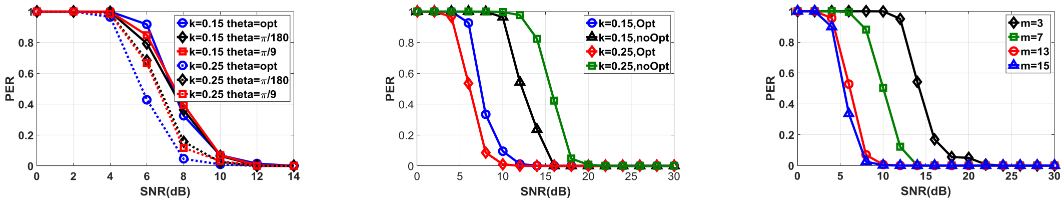


Figure 6.8: Trade off between PER and Data BER

Additionally, the performance of PER and data BER are affected by parameters and optimization variables related to our scheme. We discuss their influences as follows,

The Impact of Power Allocation Scalar. From Fig.6.7, we see that the power allocation scalar brings a positive effect on the PER whereas a negative effect on the data BER. It is because permit symbols are considered as the noise when data symbols are detected. Thus, permit symbols with higher power make data detection vulnerable to the noise. An interesting observation is that the performance of permit detection mainly depends on k although the detection of permit symbols depends on that of data symbols. It gives a credit to the repetition encoding for permit symbols and the optimization in permit embedding. The optimization in permit embedding ensures that parts of permit symbols can be accurately detected even if data symbols are incorrectly detected. Combing with hard-decision decoding strategy, the PER performance is further improved.

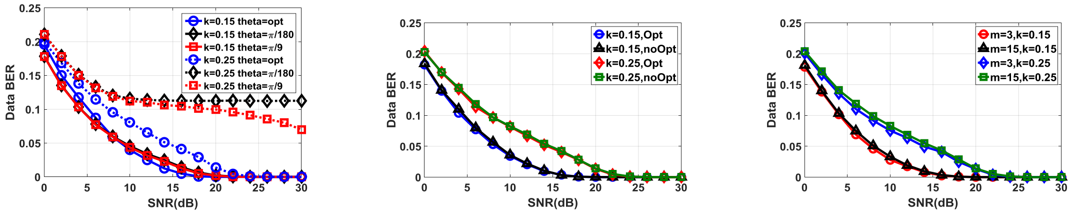


(a) Permit Modulation

(b) Permit Embedding

(c) Permit Detection with $k = 0.25$

Figure 6.9: PER vs. SNR



(a) Permit Modulation

(b) Permit Embedding

(c) Permit Detection with $k = 0.25$

Figure 6.10: Data BER vs. SNR

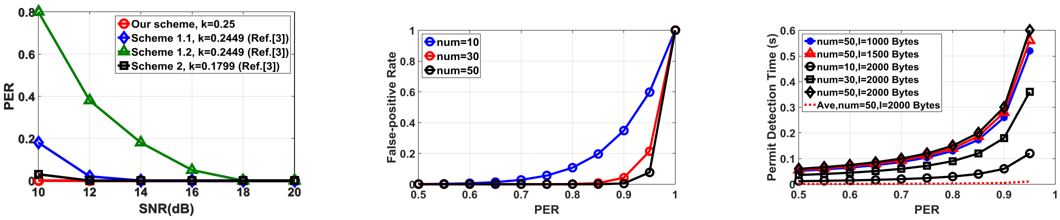
Permit Modulation Optimization. Fig.6.9a and Fig.6.10a illustrate the results of permit modulation optimization with $m = 13$. Both PER and data BER decrease with an optimized permit modulation, which satisfies our expectations. By optimizing the rotation angle θ of permit symbols in the second layer, we maximize the MI of permit symbols, which increases their resistance to the environmental noise. The permit symbols with an optimal constellation introduce less noise to data symbols. Therefore, the performance of data BER is improved.

Permit Embedding Optimization. The effect of permit embedding optimization is shown in Fig.6.9b and Fig.6.10b with $m = 13$, in which "Opt" means that we rotate permit symbols and make a symmetry for them when they are embedding into data symbols whereas “noOpt” means permit symbols are added on data symbols directly. The data detection mainly depends on k and the permit embedding optimization contributes to permit detection. This can be supported by comparing the “Opt” and “unOpt” cases with $m = 13$ and $k = 0.25$ in Fig.6.9b. Without optimization, the PER of the permit detection depends on k and data detection simultaneously. When k is large, the incorrect data detection brings negative impacts on permit detection. As illustrated in the impact of power allocation scalar, the permit embedding optimization alleviates the negative impact on permit detection. Thus, “Opt” case outperforms “unOpt” case.

Permit Detection. Fig.6.9c and Fig.6.10c describe the impact of parameter m Since repetition encoding is applied to permit symbols, it has nothing to do with data BER. Due to majority rules in the decoding, the detection performance can be easily improved by increasing m. However, it also brings more redundancy to permit transmission. In the simulations, we find that increasing m brings better PER performance by sacrificing efficiency with m lower than 13. However, when $m > 13$, the PER cannot reduce more even if continuing increasing m. This reminds us to choose a proper m which both improves the PER performance and increases the acceptable redundancy.

6.6.2.3 Detection Accuracy and Efficiency

False-positive and False-negative rates. Based on the PER results, we further analyze the false-positive rate as shown in Fig.6.11b with $m = 13$ and $k = 0.25$. The *num* in the figure implies the number of verification attempts for the permit. We can clearly see that the false-positive rate of our schemes is almost negligible even with a high PER. As for the false-negative rate, the probability that a fake permit is identified as authorized one is $(1 - P_p)/2^{160}$, which is too small to mislead the verifier. Hence, our proposed scheme can effectively defend both emulation or replay attack.



(a) Comparison with $m = 17$

(b) Accuracy

(c) Efficiency

Figure 6.11: Comparison, Accuracy and Efficiency

Detection Efficiency With the above false-positive rate, we compute permit detection time as follows. Denote l as the byte length of each data packet. Assuming the data is transmitted with a speed of 2 Mbit/s and repetition encoding parameter $m = 13$, Fig. 6.11c shows the impact of l and num on the permit detection time. Generally, the permit detection time increases with l. In particular, larger data packet means that the time gap between the transmission of two consecutive permits becomes longer, leading to longer permit detection time. With the same length of the data packet, the permit detection time increases with the number of the verification attempts. This is because the increment of the number of verification attempts will potentially increase the number of data packets, which results in longer permit detection time. No matter how many the number of verification attempts and data packet length are, the average detection time for each permit is the same, which is near to 10^{-3}s. Both permit detection time and average permit detection time demonstrate the high efficiency of our scheme.

6.6.3 Results in USRP Experiment

An experiment using USRP N210 [150] with GNU Radio is conducted in our lab. During the experiment, there are human activities such as walking. Since the phase ambiguity commonly exists in QPSK modulation in practice, differential QPSK, where the information bits are differentially coded, substitutes QPSK in our experiment [63].

The PER performance using USRP is shown in Fig.6.12. Both the power allocation scalar k and repetition encoding parameter m have a positive impact on the permit detection. However, the PER performance in the USRP experiment is worse than that in MATLAB simulations. Taking the case with $k = 0.25$ and $m = 7$ as an example, the PER is near to 0.3 when the SNR increases to 16dB in the USRP experiment, whereas the PER approaches to 0 when SNR is above 8dB in

MATLAB simulations. We infer that it is due to the imperfect time and frequency synchronization together with the phase recovery. Poor phase recovery mechanisms bring a serious impact on the permit detection. Even worse, when k is decreased to 0.15, the verifier cannot detect the permit. This is because the received permit power is further lowered due to the attenuation of transmission signals, which submerges the permit into the noise. Although the experimental results are not as good as those in MATLAB simulations, our scheme can achieve high detection accuracy in the good environment and outperforms Jin's work in [98] with proper parameters. In the case with $k = 0.3$ and $m = 7$, the PER is about 0.7|0.05|0.02|0.01 when SNR approaches to 12|14|16|18dB. This result demonstrates the effectiveness of our scheme.

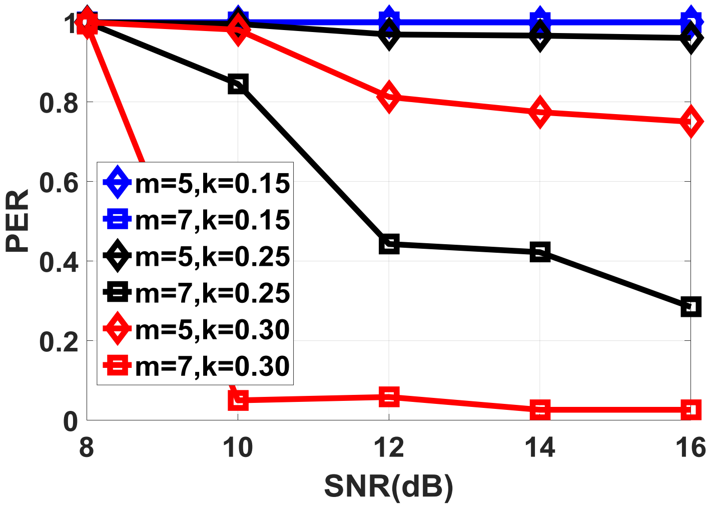


Figure 6.12: PER Performance using USRP

6.7 Chapter Summary

In this chapter, we present a secure and optimized unauthorized SU detection scheme. Through optimizing both permit modulation and permit embedding, our scheme achieves accurate and efficient permit detection. Meanwhile, unauthorized SU is effectively prevented from faking/replaying the spectrum permit, which improves the security of the DSA system. The detailed MATLAB simulations and USRP experiment results have proven above advantages of our proposed scheme.

Chapter 7

CREAM: Unauthorized Secondary User Detection in Fading Environments

7.1 Chapter Overview

The exploding growth and popularity of wireless devices and services have exacerbated the depletion of licensed wireless spectrum in recent decades [36,190]. Dynamic Spectrum Access (DSA) is a viable option to mitigate the above spectrum scarcity issue by allowing the spectrum sharing between primary users (PUs) and secondary users (SUs). In particular, Federal Communications Commission (FCC) regulates that the spectrum sharing framework in 3.5 GHz allows the Citizens Broadband Service Devices (CBSDs) to opportunistically use the spectrum when it is not occupied by or interfered with the incumbent users (authorized federal and grandfathered fixed satellite service users). To effectively regulate the spectrum access, the spectrum operator in DSA usually issues a unique and unforgeable spectrum permit (denoted as permit hereinafter) to an authorized SU (aSU), which acts as an authorization to allow the aSU to occupy the dedicated frequency channel in the specified area and time duration [98].

Although the DSA is envisioned as a promising approach, quite a few practical concerns prevent it from actually implementing. On the one hand, specifically to the wireless environment, due to the atmospheric ducting, ionospheric reflection/refraction, and the reflection from terrestrial objects, the message transmitted via a wireless multi-path channel suffers dispersion, attenuation, and phase shift, all of which are known as fading effects [132]. On the other hand, the open nature of the wireless medium provides opportunities for unauthorized SUs (uSUs) to occupy the spectrum by faking/replaying the permit, which would cause severe interference to aSUs allocated to the same spectrum. As a result, no user would participate in the DSA system for improving the spectrum usage efficiency. Therefore, it is highly needed to devise an aSU authentication scheme to ensure the security of the DSA system in fading environments to further unleash its great potential for future wireless systems.

In this chapter, we propose a spectrum misuse detection scheme in fading environments, **CREAM**, **C**onstellation **R**otation **E**mbedding for **A**uthenticating the authorized SUs based on superposition **M**odulation. Working under the Orthogonal Frequency-Division Multiplexing (OFDM) framework, CREAM conceals each aSU's permit into its message signal by superposing them into the power domain. To better adapt specific fading environments, CREAM constructs an optimization problem to find the optimal angle for constellation rotation and interleaving prior to superposition modulation. A third party verifier, close to the aSU transmitter, passively monitors the signal transmission. Having a pre-shared secret on the related parameters with the aSU, e.g., power allocation factor, rotation angles, and the permit root, the verifier detects the permit using maximum likelihood (ML) estimation, followed by the transmitter identification. In general, CREAM has the following **salient features** that make it ideal for uSU detection in fading environments:

- **Security:** Without the complete knowledge of modulation parameters, uSUs cannot fake or replay the current permit of aSUs. When uSUs occupy the spectrum directly, the changes in the received signal's will alert the verifier. In both cases, spectrum misuse can be easily detected.

- **Accuracy:** OFDM is robust against fading caused by the multi-path propagation. In addition to that, the optimized constellation rotation produces significant gains by increasing the dimensionality of the signal in fading environments. Therefore, CREAM effectively improves the performance for permit and message transmission and thus achieves low false-positive and false-negative rates for permit detection.

- **Efficiency:** Superposition modulation benefits the DSA system from achieving a high authentication rate [105]. Spectrum misuse can be detected in an extremely short time period. Meanwhile, the high authentication rate leaves little time for uSUs to fake or replay the permit.

- **Low-intrusion:** The closeness between the verifier and the aSU transmitter results in less path loss, which requires less power to achieve the reliable communication for the permit. Thus, the permit embedding exerts less intrusion to message transmission. Beyond that, the constellation rotation and interleaving for the message signals contribute to their transmission performance improvement in fading environments.

The rest of this chapter is organized as follows: In Section 7.2, we review the existing uSU detection schemes, along with a brief description of the fading environments and the techniques to defend against fading. Section 7.3 describes the system model and the proposed framework. The CREAM scheme is elaborated in Section 7.4 from the following three components: permit pre-processing, permit embedding, permit post-processing. Particularly, Section 7.5 optimizes the constellation rotation in permit embedding process. In Section 7.6, we analyze the theoretical performance for CREAM, followed by a thorough evaluation of the permit and message performance using MATLAB simulations in Section 7.7. Finally, Section 7.8 concludes the chapter.

7.2 Related Work

7.2.1 Unauthorized SU Detection

Methods for authenticating SUs can be classified into three categories. One is to utilize cryptographic schemes [13, 57, 126, 130] at the higher layers. However, involving higher-layer processing lowers the authentication efficiency due to high time consumption. Meanwhile, incompatible systems may not be able to decode each others' higher layer signals [105]. The transmitter-unique "intrinsic" characteristics of the waveform, such as RF fingerprinting and electromagnetic signature identification [26,83,166], can also be deployed to identify transmitters. However, according to [105], those methods are sensitive to environmental factors, e.g., temperature changes, interference, etc, which limits their efficacy in real-world scenarios.

Recent methods focus on "extrinsically" physical-layer authentication scheme, in which a unique unforgeable signal is embedded in the message signal and then extracted at the receiver [97, 98, 105, 106, 185]. Yang *et al.* [185] embed the permit by duplicating sub-carriers in OFDM to achieve the desired and detectable cyclo-stationary feature. Such operations not only decrease the message throughput but also introduce high computational overhead. In [106], P-DSA is proposed to conceal permit via controlled inter-symbol interference, which negatively impacts normal message transmission. FEAT scheme in [105] enables the verifier to perform blind parameter estimation on multiple parameters of the OFDM signal, giving rise to a high computation complexity. Jin *et al.* [97] conceal at most two permit bits by changing the cyclic prefix length in each symbol of a physical-layer frame, resulting in low authentication rate. By controlling the power of the transmitted signals in [98], the permit is embedded given power constraint imposed on the transmitter. However, the first two schemes in [98] are mainly designed for AWGN environments and are not robustness to fading effects. Although another scheme is proposed to adapt to fading environments by changing the message constellation, it has a low authentication rate together with the first two schemes. Hence, CREAM rotates and superposes the permit and message to achieve a secure and reliable aSU transmission in fading environments with a high authentication rate and a low-complexity implementation.

7.2.2 Fading Environments

The phenomenon of fading is the time variation of the channel strengths due to the small-scale fading resulted from multi-path and moving, as well as larger-scale effects such as path loss via distance attenuation and shadowing by obstacles, which causes the attenuation of the signal at the receiver [165]. Multi-path fading causes the magnitude attenuation and the phase shift of the signal due to the atmospheric ducting, ionospheric reflection and refraction, and reflection from terrestrial objects such as mountains and buildings [63]. Rayleigh fading [146] is a stochastic model to show the effect brought by multi-path fading in which the envelope of the channel response is Rayleigh distributed and the phase of the channel response is randomly distributed between 0 and 2π. It is quite reasonable for scattering mechanisms where there are many small reflectors.

Constellation rotation is considered as a practical implementation of signal space diversity (SSD) [127]. By increasing the diversity order [165], the rotated signal transmitted over the fading channel has exactly the same performance of the nonrotated one transmitted over an additive white Gaussian noise (AWGN) channel [24]. OFDM is a widely used modulation scheme in fading environments [144]. It is robust against the multi-path fading by separating a wideband signal into many smaller narrowband signals [156]. CREAM combines the constellation rotation and the OFDM to achieve the permit and message reliable transmission in fading environments.

7.3 System Model

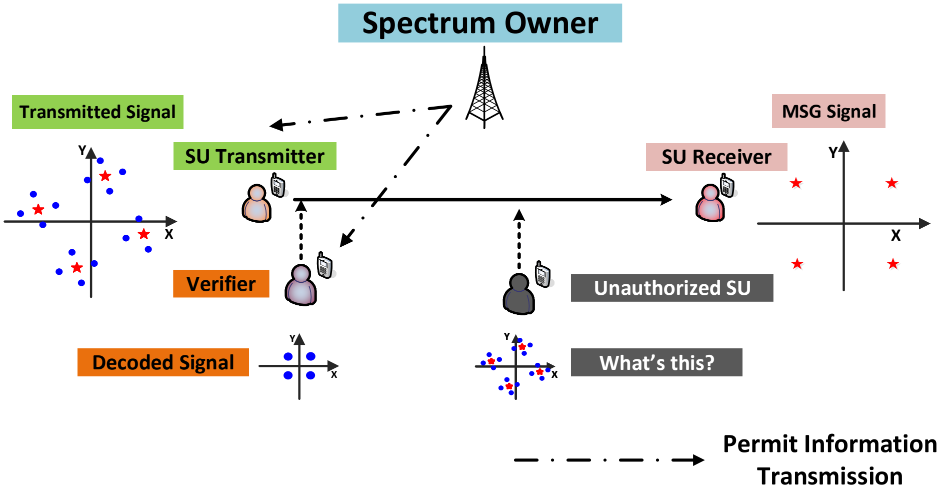


Figure 7.1: System Model

7.3.1 System Model

As shown in Fig.7.1, our system model contains three entities.

Spectrum Operator: Being an administrator and pivot in DSA system, it obtains the current channel estimation from dispersed sensors. For example, in 3.5GHz, Environmental Sensing Capability (ESC) is deployed to sense and then report the channel conditions. Receiving the spectrum request from each aSU, it chooses a proper allocation factor and constellation rotation angles based on the channel condition together with a permit root. These parameters are transmitted to the aSU and its nearby verifiers via an authenticated and encrypted channel respectively. When an aSU reports abnormal interference or when a pre-determined random schedule is required, it mandates the verifiers to begin uSU detection.

Secondary Users: They request and pay for a given licensed spectrum by submitting their locations and time periods. Meanwhile, they embed the unique spectrum permits into the message signals to demonstrate their legal identities using the received parameters from the spectrum operator.

Verifiers: They are employed by the spectrum operator to help identify their nearby SU transmitters. The authentication results are sent to the spectrum operator. They do not participate in the message transmission.

7.3.2 Adversary Model

We define the attacker as an uSU who accesses the spectrum either by accident or misconfiguration, or to avoid costs of spectrum occupation. The above operations can be done by controlling its transceiver to manipulate its physical-layer symbols. By occupying the channels allocated to aSUs directly or with a faked/replayed permit, the uSU brings severe interference to aSUs. Meanwhile, we assume that the uSU is computationally bounded and cannot break the cryptographic primitives used to generate the permit. Finally, it can compromise verifiers to report incorrect results to the spectrum operator.

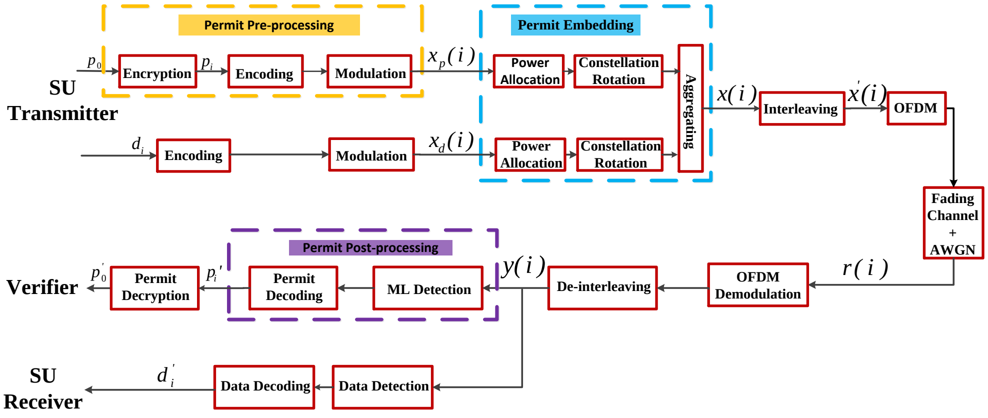


Figure 7.2: Framework

7.3.3 Framework Overview

The CREAM framework is shown in Fig.7.2, in which the superposed signal in time slot i is:

$$x(i) = \sqrt{P_p(i)}x_p(i)e^{j\theta_p(i)} + \sqrt{P_d(i)}x_d(i)e^{j\theta_d(i)} \tag{7.1}$$

where $x_p(i)$ and $x_d(i)$ are the permit and message symbols after encoding and modulation respectively. Their corresponding constellation rotation angles are $\theta_p(i)$ and $\theta_d(i)$ whereas $P_p(i)$ and $P_d(i)$

are their transmitted powers. Denote $x(i)$'s real and imaginary components as $x_R(i)$ and $x_I(i)$. After interleaving [101], it becomes:

$$x^{'}(i) = x_R(i) + jx_I(i-k) \tag{7.2}$$

which is remapped to OFDM symbols to be transmitted.

Denote $h(i)$ as the channel multi-path fading coefficient with expectation $E\{|h(i)|^2\} = 1$. At the verifier and the aSU receiver, the received signal is:

$$r(i) = h(i)x^{'}(i) + n(i) \tag{7.3}$$

where $n(i)$ is the equivalent AWGN noise with large-scale path loss absorbed into it. It has noise variances σ_p^2 and σ_d^2 at the verifier and the aSU receiver respectively. Assume perfect channel estimation, the received signal after OFDM demodulation and de-interleaving is:

$$y(i) = h(i)^*/|h(i)|r(i) = |h(i)|x(i) + \eta(i) \tag{7.4}$$

where $|h(i)|$ is the channel gain and the equivalent noise becomes $\eta(i) = h(i)^*/|h(i)|n(i)$. It has the same variance as the original noise $n(i)$. ML detection is deployed at both the verifier and the aSU receiver. Without loss of generality, we ignore index i in what follows.

7.4 CREAM Scheme

According shown in Fig. 7.2, CREAM is divided into three sequential parts *permit pre-processing*, *permit embedding*, and *permit post-embedding*, each of which will be discussed respectively as follows.

7.4.1 Permit Pre-processing

Similar to [98], the spectrum and the geographic region are divided into non-overlapping parts respectively. The time period is split into slots of equal length. All entities are assumed to be loosely synchronized to a global time server.

- Generation: An efficient one-way hash chain is used to generate the unforgeable spectrum permits. Let $f(x)$ denote a cryptographic hash function on x, and $f^{\eta}(x)$ means η successive operations on $f(\cdot)$ to x. Assuming an aSU requests a spectrum in a time period γ. The spectrum operator sends a random number p_{γ} to the aSU. The aSU recursively computes $p_i = f(p_{i+1})$, $i \in [1, \gamma - 1]$ as its permit in time slot i. Meanwhile, the spectrum operator transmits $p_0 = f^{\gamma}(p_{\gamma})$ to the verifier.

- Encoding: For simplicity, the permit is encoded using repetition code $\mathcal{C}_m$ to tolerate transmission errors resulted from the noise, in which each permit bit is repeated m times.
- Modulation: Quadrature Phase Shift Keying (QPSK), which has been widely applied in many applications and standards such as IEEE 802.11b and IEEE 802.11g, is chosen as the basic modulation scheme for both permit and message. General quadrature amplitude modulation is also supported.

7.4.2 Permit Embedding

As shown Fig.7.2, CREAM allocates the power to permit and message, followed by rotating their constellations with the optimized angles. Finally, the rotated permit and message are superposed with the Gray-mapping rule [156], in which constellation points with the minimum Euclidean distance have one-bit difference. A Grey-mapping constellation example after permit embedding is shown in Fig.7.3 with $\theta_d = \theta_p = \pi/6$ and $P_p = 0.1$, $P_d = 0.9$, where the first two bits represent message and the second bits in the bracket denote the permit.

In order to achieve low intrusion to the message, the permit and message power should satisfy:

$$P_p + P_d = 1, P_d > P_p > 0. \tag{7.5}$$

Fractional Transmit Power Allocation (FTPA) [21], as an effective power allocation method, is chosen in CREAM. In FTPA, the power of the permit is allocated as:

$$P_p = \frac{1}{(|h|/{\sigma_p}^2)^{-\alpha} + (|h|/{\sigma_d}^2)^{-\alpha}} (|h|/{\sigma_p}^2)^{-\alpha} \tag{7.6}$$

where $\alpha \in [0, 1]$ is the decay factor. The case of $\alpha = 0$ corresponds to equal transmit power allocation between the permit and message. When α is increased, the more power is allocated to the message. In CREAM, the spectrum operator thoroughly investigates the value of the decay factor via experiments such that the reliable transmission of both permit and message is ensured.

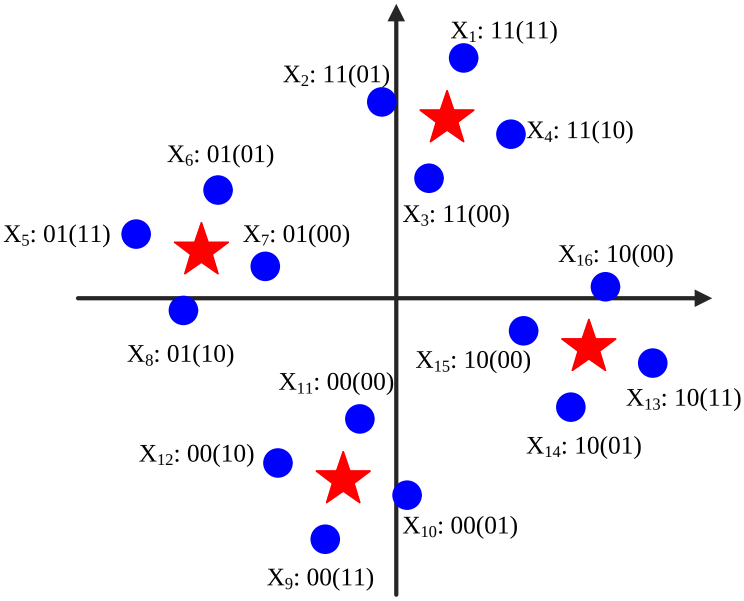


Figure 7.3: An Example of Superposed Constellation

7.4.3 Permit Post-processing

According to Eq (7.2), interleaving the real and imaginary components of the superposed symbol x makes them being transmitted in different time. Hence, when the duration between the transmission of real and imaginary components is larger than the coherent time of the fading channel [165], their transmissions suffer independent fading effect. Therefore, different to Eq (7.4), the received signal after de-interleaving can be rewritten as:

$$y_R = |h_R|x_R + \eta_R, \quad y_I = |h_I|x_I + \eta_I \tag{7.7}$$

where $|h_R|$ and $|h_I|$ are the channel gains of the signal x's real and imaginary components, respectively. To ease the description, we rewrite $|h_R|$ and $|h_I|$ as h_R and h_I. In the Rayleigh fading model, they are *i.i.d.* Rayleigh random variables with distribution as follows:

$$p(x) = 2x/\beta \times e^{-\frac{x^2}{\beta}}, \quad x = h_R, h_I \tag{7.8}$$

where $\beta = E(h_R^2) = E(h_I^2) = \frac{1}{2}$.

At the verifier, ML is deployed. According to Eq (7.7), the ML metric for detecting x_p is:

$$M(x) = \exp\left(-\frac{(y_R - h_R x_R)^2 + (y_I - h_I x_I)^2}{\sigma^2}\right) \tag{7.9}$$

The bit Likelihood ratio (LLR) for the permit is written as:

$$L(i) = \text{In}\sum\nolimits_{x\in A_i^0} M(x) - \text{In}\sum\nolimits_{x\in A_i^0} M(x), i = 3, 4 \tag{7.10}$$

where A_i^l is a set of x whose i bit is l, $l = 0, 1$. If $L(i) > 0$, the i bit in x is detected as 0. Otherwise, it is detected as 1. The majority rule is applied to decode each permit bit. Permit transmission and detection are totally transparent to the aSU receiver as if it does not know the permit existence. QPSK together with ML detection is utilized at the aSU receiver.

Denote the detected permit in time-slot i as p_i'. To verify the transmitter's identity, the verifier computes p_0' by i successive operations of the same hash function f on p_i', $p_0' = f^i(p_i')$. If $p_0' \neq p_0$, the verifier suggests the transmitter as an uSU. The detection results are finally reported to the spectrum operator who will physically locate and further punish the transmitter.

7.5 Optimized Constellation Rotation in CREAM

In this section, we thoroughly investigate the how to optimize constellation rotation for permit and message in a specific fading environment.

7.5.1 Motivation

Consider the case without constellation rotation, $\theta_p = \theta_d = 0$ in Eq (7.1). the superposed symbol becomes:

$$x = \sqrt{P_p}(x_{p,R} + x_{d,R}) + j\sqrt{P_d}(x_{p,I} + x_{p,I}). \tag{7.11}$$

in which the real/imaginary component of x is only composed of the corresponding real/imaginary component of the permit and message respectively. Suppose that a deep fade hits only one of the components of the superposed signal, e.g., real component. Then, only the imaginary components of the permit and message survive. The integrity of the permit and message symbol is negatively affected.

While we rotate the constellation of the permit and message with θ_p and θ_d respectively, the real component of x in Eq (7.1) becomes $\sqrt{P_p}(x_{p,R}\cos\theta_p - x_{p,I}\sin\theta_p) + \sqrt{P_d}(x_{d,R}\cos\theta_d - x_{d,I}\sin\theta_d)$, whereas the imaginary component changes to $\sqrt{P_p}(x_{p,R}\cos\theta_p - x_{p,I}\sin\theta_p) + \sqrt{P_d}(x_{d,R}\cos\theta_d - x_{d,I}\sin\theta_d)$. Each component now contains all the components of the permit and message after rotation. Thus, even if one component suffers from deep fading, the integrity of the permit and message is still retained. The information involved in real and imaginary components of the symbol can be reconstructed. Fig. 7.4 shows a simple example to further illustrate the advantages of the rotation. With constellation rotation, any two points achieve the maximum number of distinct components. In the case that one component is deep faded, e.g., imaginary component, the 'compressed' constellation in Fig.7.4b (empty circles) offers more protection against fading effect, since no components for any two points collapse together as would happen with Fig.7.4a.

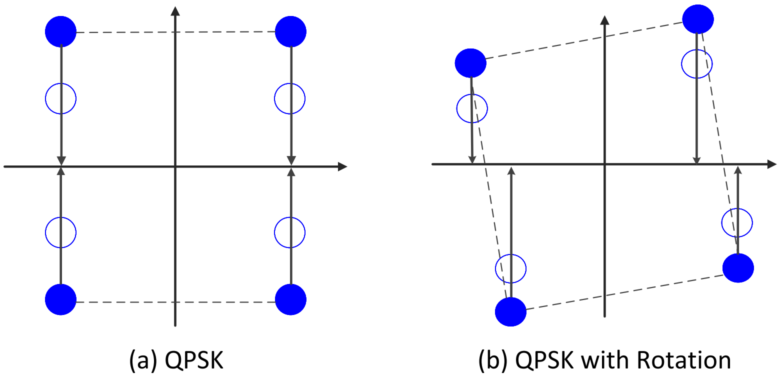


Figure 7.4: Comparison between QPSK and QPSK with Rotation

7.5.2 Constellation Rotation Optimization

To effectively defend against fading effects, the constellation rotation is usually optimized by maximizing the minimum product distance or minimizing error probabilities when ML detection is deployed. However, it is difficult to obtain an explicit expression for the exact error probabilities [165]. Therefore, CREAM employs a suboptimal method, which is to minimize the permit symbol error rate (PSER) upper bound.

$$P_e \leq \frac{1}{N} \sum\nolimits_{i=1}^{N} \sum\nolimits_{k=1, k\notin\Gamma_{(i)}}^{N} P(x_i \to x_k) \tag{7.12}$$

where N is the size of the superposed constellation. $P(x_i \rightarrow x_k)$ is the pairwise error probability (PER) of confusing x_i with x_k when x_i is transmitted. $\Gamma_{(i)}$ is the set involving symbols that do not constitute a valid PER for x_i after permit detection. For example, when x_1 is transmitted, the detected permit bits are always 11 if the detected signal belongs to the set $[x_1, x_5, x_9, x_{13}]$ as shown in Fig.7.3.

PER in Eq (7.12) is refined as $P(x_i \rightarrow x_k) = \int_0^\infty \int_0^\infty P(x_i \rightarrow x_k | h_R, h_I) p(h_R) p(h_I) dh_R dh_I$ given the probability density function of channel gain $p(h_R)$ and $p(h_I)$, where $P(x_i \rightarrow x_k | h_R, h_I)$ is calculated based on Eq (7.9) as:

$$
\begin{aligned}
& P(x_i \rightarrow x_k | h_R, h_I) = P\left((y_R - h_R x_{k,R})^2 + (y_I - h_I x_{k,I})^2 \leq (y_R - h_R x_{k,R})^2 + (y_I - h_I x_{k,I})^2 | x_i \text{ is sent}\right) \\
& = P\left(h_R(x_{i,R} - x_{x,R})\eta_R + h_I(x_{i,I} - x_{k,I})\eta_I \leq -\frac{1}{2}h_R^2(x_{i,R} - x_{k,R})^2 - \frac{1}{2}h_I^2(x_{i,I} - x_{k,I})^2\right) \\
& = \frac{1}{2}\text{erfc}\left(\frac{1}{2}\sqrt{\frac{1}{\sigma_p^2}}\sqrt{h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2}\right) \\
& \leq \frac{1}{2}\exp\left(-\frac{1}{4\sigma_p^2}\left(h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2\right)\right)
\end{aligned}
\tag{7.13}
$$

in which the third equation is derived because $h_R(x_{i,R} - x_{k,R})\eta_R + h_I(x_{i,I} - x_{k,I})\eta_I$ is a Gaussian random variable with zero mean and the variance $\Omega^2 = h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2$. The inequality is based on the rule $P(X \leq x) = \frac{1}{2}\text{erfc}(\sqrt{x^2/2\Omega^2})$ [94].

Since h_R and h_I are the Rayleigh channel gain, $p(h_R^2)$ and $p(h_I^2)$ submit to the exponential distribution where $p(x^2) = e^{-x^2}$ [170]. $P(x_i \rightarrow x_k)$ in Eq (7.12) is finally expressed as:

$$
\begin{aligned}
& P(x_i \rightarrow x_k) \leq \frac{1}{2}\int\limits_0^\infty \exp\left(-h_R^2\left(1 + \frac{1}{4\sigma_p}(x_{i,R} - x_{k,R})^2\right)\right) dh_R^2 \times \int\limits_0^\infty \exp\left(-h_I^2\left(1 + \frac{1}{4\sigma_p}(x_{i,I} - x_{k,I})^2\right)\right) dh_I^2 \\
& = \frac{1}{2\left(1 + \frac{(x_{i,R} - x_{k,R})^2}{4\sigma_p^2}\right)\left(1 + \frac{(x_{i,I} - x_{k,I})^2}{4\sigma_p^2}\right)}
\end{aligned}
\tag{7.14}
$$

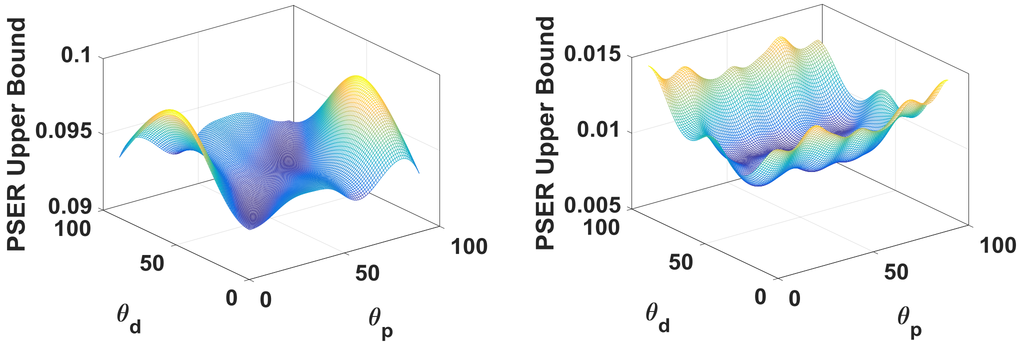
Based on Eq (7.14), the upper bound for PSER P_{upper} in Eq (7.12) is:

$$
P_e \leq \frac{1}{N}\sum_{i=1}^{N}\sum_{k=1, k \notin \Gamma_{(i)}^{N}}^{N} \frac{1}{2\left(1 + \frac{(x_{i,R} - x_{k,R})^2}{4\sigma_p^2}\right)\left(1 + \frac{(x_{i,I} - x_{k,I})^2}{4\sigma_p^2}\right)}
\tag{7.15}
$$

Since the constellation rotation angels θ_p and θ_d are concealed in x_i and x_k, the angles can be obtained by minimizing above PSER upper bound. The optimization problem in CREAM is as follows:

$$\begin{aligned} \min_{\theta_p,\theta_d} \quad & P_{upper} \\ \text{s.t.} \quad & 0 \le \theta_p, \theta_d \le 2\pi \end{aligned} \tag{7.16}$$

Based on Eq (7.15), P_{upper} mainly depends on the constellation pattern. In addition, different rotation angles may produce the same constellation pattern. Therefore, the PSER upper bound minimization is a non-convex problem. We deploy a numerical method by performing a global search with one-degree step.



(a) SNR = 10dB

(a) SNR = 20dB

Figure 7.5: PSER Upper Bound vs. SNR

Table 7.1: PSER Upper Bound when $SNR = 10dB$

Upper Bound	0.0092	0.0092	0.0092	0.0092	0.0092
θ_d	19	20	20	70	71
θ_p	23	24	25	65	67

Two examples are shown in Fig.7.5 with $P_p = 0.1$ and $P_d = 0.9$. Meanwhile, Table 7.1 illustrates the minimized PSER upper bound with corresponding rotation angles θ_p and θ_d when $SNR = 10dB$. From them, we see that 1) the PSER upper bound has different shapes under different channel conditions, which verifies that the constellation rotation angles vary with the current channel condition; 2) the PSER upper bound minimization problems have multiple solutions. Such characteristics make CREAM a powerful scheme to prevent the uSU from replaying the permit.

7.6 Scheme Analysis

In this section, we analyze the spectrum misuse detection efficiency, the computational complexity, and the security of CREAM.

7.6.1 High Detection Efficiency

Assume the permit is repetition coded with 1/7 rate ($m = 7$) and the message is convolutional coded using 1/2 rate. In IEEE 802.11a standard with 24Mbps message bit rate, the transmission rate for the permit bits is close to 7Mbps. FEAT [105] and SafeDSA [97] embedded one permit bit into each OFDM frame. The permit bit transmission rate is at most 1/4Mbps when there is only one OFDM symbol in each frame that includes 96 message bits. Compared with SafeDSA and FEAT, CREAM achieves a high authentication rate. For the uSUs who have not accessed the spectrum, CREAM leaves them little time to prepare the faked/replayed permit. For the uSUs who are occupying the spectrum, CREAM can detect them in a short time.

7.6.2 Low Computational Complexity

In CREAM, the transmission and reception of both permit and message use the basic physical-layer techniques. Although interleaving and de-interleaving are the most time-consumption operations, they only require a buffer to store the received signal without complex operations. Whereas in SafeDSA [97], the verifier needs to estimate the cyclic prefix length based on the message dependency test to detect each permit bit. Even worse, in FEAT [105], the verifier has to perform blind parameter estimation on multiple parameters of the OFDM signal. For complete blind estimation, the possible ranges of the parameters to be estimated need to be comprehensive, which covers all possible values and thus results in a high computation complexity.

7.6.3 High Resilience to Attack

Emulation Attack. A successful emulation attack is achieved if a uSU provides a proof of an aSU transmitter identity to mislead the verifier to believe that the current spectrum is not misused. Specifically, the uSU launches an emulation attack if it derives a faked permit which is the same as that of the aSU transmitter. Since the one-way hash chain is employed to generate the spectrum permits, the uSU does not have the computational ability to break the cryptographic primitives and therefore it cannot obtain the permit without the root of the hash chain. Unfortunately, the uSU may occasionally create the same permit. However, the probability of such situation is so small that we can ignore it. Taking SHA-1 with 160-bit length as an example, the probability of generating the same permit is $(1/2)^{160}$. Therefore, our scheme can successfully prevent the emulation attack [157].

Replay Attack. The uSU may eavesdrop an aSU transmission, extract its permit, and then attempt to use it for its message transmission. CREAM provides several barriers to prevent the replay attack. Since the constellation rotation angles are calculated based on the current channel condition, it is difficult for the uSU to extract the permit from the received signals with wrong channel estimation. In addition, the characteristics of the minimized PSER upper bound allows for using different rotation angles in the same channel condition. Therefore, even if the uSU eavesdrops the angles by monitoring the permit transmission in the current slot, it does not know the rotation angles in the next slot, which confuses it when extracting permit. In addition to that, since it cannot generate the next permit based on the current eavesdropped one without the root of the hash chain, it is impossible for the uSU to replay the future permits to deceive the verifier. Therefore, CREAM is resilient to replay attack.

Free-rider Attack. In free-rider attack, the uSU hides behind the aSU by sending message parallel without permits [185]. Since the messages of the uSU and the aSU are independent, the free-rider attack would increase the number of the constellation points, which can be easily found by the verifier.

Compromising Attack. By compromising the verifier to report the wrong detection results to the spectrum operator, the uSU can access the spectrum "legally". The low computational complexity allows the DSA to employ a number of verifiers to patrol the area near the aSU transmitter. By receiving detection results from various verifiers and combining them using known consensus distributed algorithms [41], the probability of wrong spectrum occupation judgment is greatly lowered.

7.7 Performance Evaluation

We evaluate the performance of CREAM in fading environments using MATLAB simulations. Specifically, three indoor environments are considered as listed in Table 7.2 and CREAM

Table 7.2: Fading Parameters

Parameter	Values
Moving speed	2.7km/h
1. Small office/ Home office	
Rms delay spread	50ns
Number of taps	5
2. Large office building	
Rms delay spread	100ns
Number of taps	10
3. Factory	
Rms delay spread	200ns
Number of taps	19

performance in fading environment 1 is mainly discussed. We show the performance in other two fading environments 2 and 3 by comparing with that in fading environment 1.

7.7.1 Simulation Settings

Adapting to indoor environments, we set parameters in CREAM with the help of IEEE802.11a standard, in which message transmission speeds as high as 54Mbps are possible. The main difference is that we consider CREAM performance in 3.5GHz band, particularly for small cell deployments [23] approved by FCC [3]. The system parameters are listed in Table 7.3 and Table 7.4 respectively.

Table 7.3: OFDM Parameters

Parameter	Values
Operation Frequence	3.5GHz
Sampling rate	20Mhz
IFFT/FFT sampling point	64
Subcarrier frequency spacing	0.3125MHz
Total Bandwidth	$16.25MHz$
OFDM Symbol Period	4μs
Guard interval	0.8μs
Number of message Subcarriers	48
Number of pilot Subcarriers	4

Table 7.4: System Parameters

Parameter	Values
message Encoding	1/2 Conv coding
Permit Encoding	$1/m$ repetition coding
Modulation	QPSK
Mapping	Grey mapping
Coded bits	96
message bits	48
Permit bits	$96/m$

As for other default simulation settings, CREAM uses the 160-bit SHA-1 function to construct the permit. Each frame has a constant message payload length of 100 OFDM symbols. Hence, $N_s = \lfloor \frac{100*96}{160m} \rfloor = \lfloor \frac{60}{m} \rfloor$ permit is transmitted in each frame. Moreover, we transmit 500 frames to average each point in MATLAB results. As for power settings, we assume the superposed symbols are transmitted using the unit power. The received signal-to-noise radio at the verifier SNR_p and the aSU receiver SNR_d are defined respectively as follows:

$$SNR_p = \frac{1}{\sigma_p^2}, SNR_d = \frac{1}{\sigma_d^2}, \quad SNR_\delta = SNR_p - SNR_d > 0$$

Since the aSU transmitter is further to the aSU receiver than the verifier as assumed previously, we denote SNR_δ as the received SNR difference. In the following simulations, $SNR_\delta = 10$dB. The default delay factor α is set to 1 to ensure the reliable communication for the message. The permit encoding rate m is set to 7.

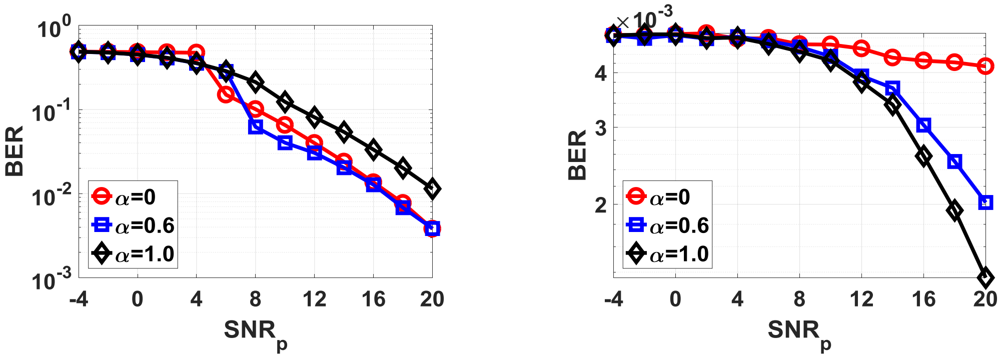
7.7.2 CREAM Performance

We first evaluate the permit bit-error-rate (BER) and message BER performance. Permit BER is a basic measurement on the permit transmission accuracy, whereas message BER reflects the permit's intrusion to message. Further, we calculate the permit error rate, which describes transmission error for a whole permit composed of 160 bits. False-positive rate is also considered to measure the negative effect CREAM possibly brings to the aSU's transmission. Several key parameters affect the CREAM performance, including the SNR difference between the verifier and the secondary user receiver SNR_δ, the power allocation factor α, the rotation angles θ_p and θ_d, etc, all of which will be discussed in the following.

Note that although the physical-layer authentication work in fading environments is mentioned in [97] and [105], they do not consider the detailed factors, e.g., the moving speed, the time delay, and the multi-path. Therefore, we cannot compare the CREAM performance with these works directly.

7.7.2.1 Impact Factor

The Impact of the Power Allocation. According to Eq (7.6), the power allocation between the permit and message depends on the decay factor α given SNRs. Fig.7.6a and Fig.7.6b show its impact on the permit BER and message BER respectively. By comparing these two figures, it seems that the decay factor puts an opposite effect on the permit and message transmission. When $\alpha = 0$, the power is allocated evenly. The permit is transmitted with the high power. However, it results in the loss of message power and brings serious intrusion to message. When the decay factor is near to 1, most power is allocated to the message transmission. The permit is easily affected by the fading effects and noise. Thus, permit BER has a poor performance. In practice, we have to ensure that the permit embedding brings the slightest negative impact on message transmission. Under this premise, we try to distribute more power to the permit.

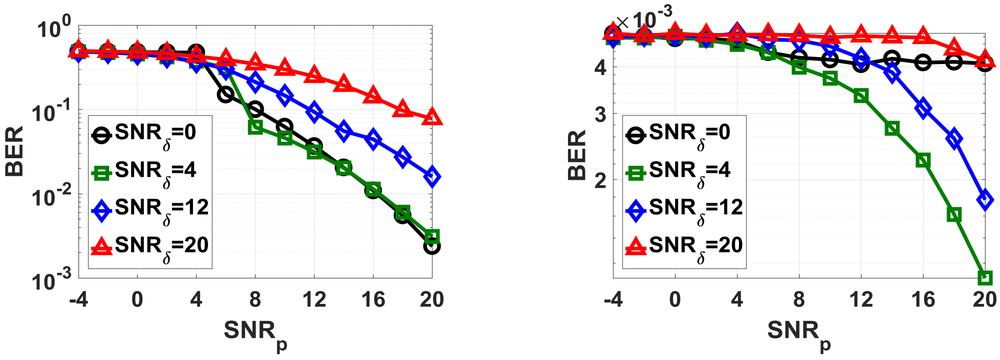


(a) Permit Bit Performance

(b) Message Bit Performance

Figure 7.6: Power Allocation Impact

The Impact of the Received SNR Difference. SNR difference between the verifier and the aSU receiver plays an important role in both permit and message performance as illustrated in Fig.7.7a and Fig. 7.7b. When they are near to each other, the message and permit transmission cannot be easily distinguished in the power domain. Hence, the message transmission is negatively affected by the permit. When they are far from each other and the permit is much closer to the aSU transmitter, a reliable permit transmission can be achieved with less power and thus more power is allocated to the message transmission to help it defend against the pass loss. However, when they are far apart and the aSU receiver is much further to the aSU transmitter, the message transmission would suffer larger pass loss and thus most power has to be allocated to the message, which affects the permit transmission negatively. As shown in Fig.7.7a and Fig. 7.7b, the message BER has a poor performance when $SNR_\delta = 0$dB and 20dB. The permit BER also performs poor at $SNR_\delta = 20$dB. When $SNR_\delta = 4$dB, both the permit and message can be transmitted accurately with a low BER.

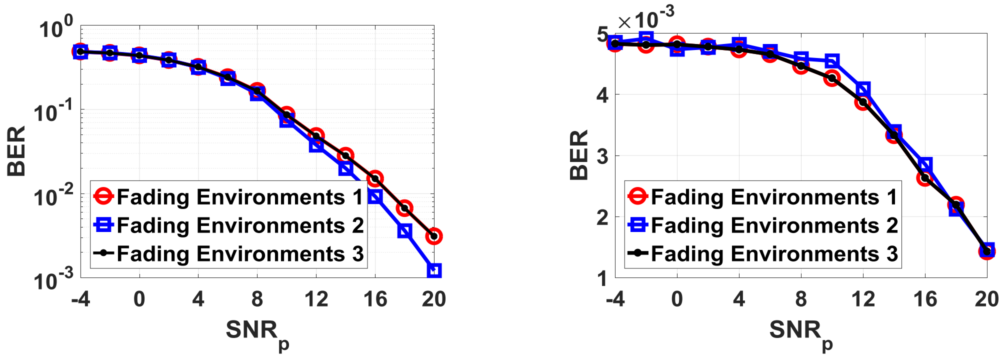


(a) Permit Bit Performance

(b) Message Bit Performance

Figure 7.7: SNR_δ Impact

Fading Environments. We simulate the permit BER and message BER under different fading environments in Fig.7.8a and Fig.7.8b, respectively. From them, we see that CREAM has a similar performance and performs well under three different fading environments. The difference is that permit transmission performs slightly better in large office building whereas message transmission has a better performance in small office/home office environments.

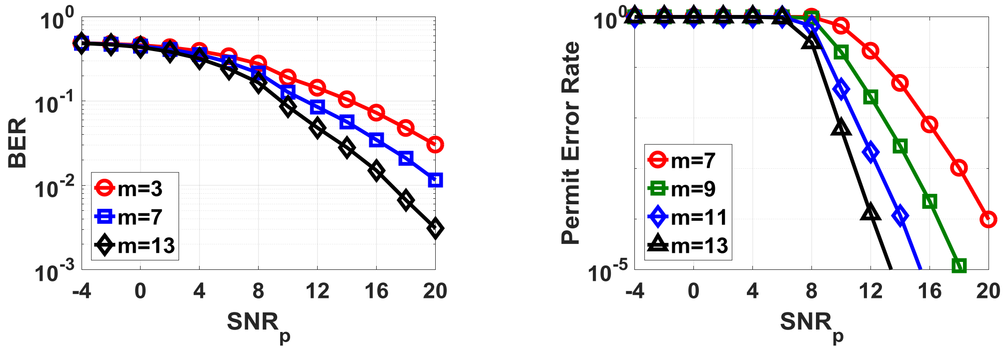


(a) Permit Bit Performance

(b) Message Bit Performance

Figure 7.8: Fading Environments Impact

The Impact of the Repetition Code Rate. Fig.7.9a describes the permit BER performance using different repetition encoding rates $1/m$. From it, we see that a low rate helps improve the permit BER performance. According to [63], a repetition code with parameter m has an error correcting capacity $\frac{m-1}{2}$. Hence, when m is large, the permit BER has a good performance. However, a low encoding rate decreases the permit transmission rate and brings a negative impact on the authentication rate. We will discuss it later. **The Impact of the Rotation Angles.** By



(a) Permit BER Performance

(b) Permit Performance

Figure 7.9: Repetition Encoding Impact

optimizing the rotation angles in Section V, we can get a minimized PSER upper bound. Fig.7.10 compares the permit BER performance under different rotation angles. From it, we conclude that optimized permit rotation angle indeed improves the permit BER performance. Specifically, when the $SNR_p \in [0\text{dB}, 10\text{dB}]$, it brings almost 3dB gain.

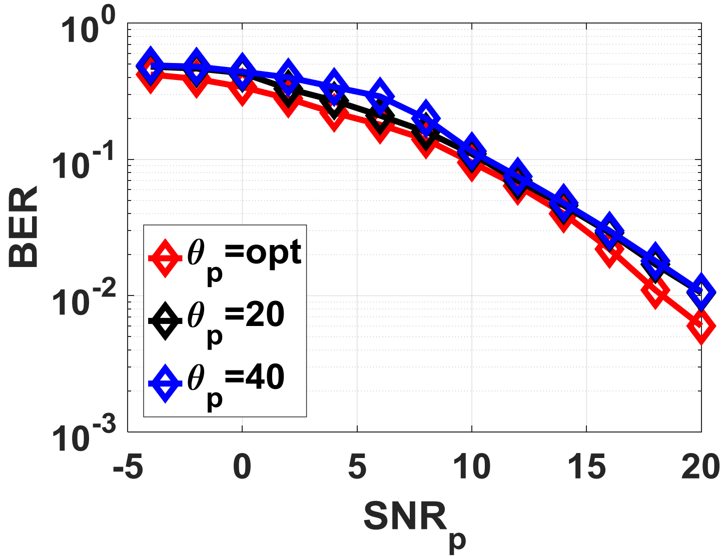


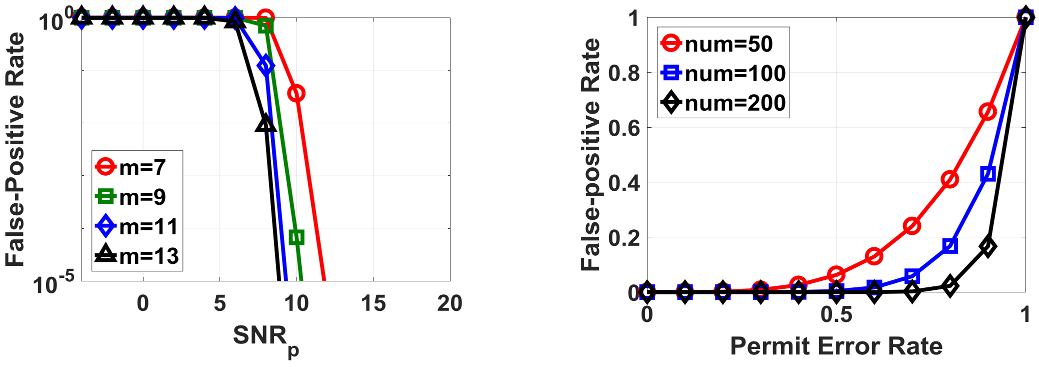
Figure 7.10: θ_p Impact

7.7.2.2 Detection Accuracy

Permit Error Rate. Since the one-way hash function is used to secure the authentication, CREAM has to ensure the correctness of each permit with 160 bits. Denote above permit BER as P_b. The permit length is $L = 160$, the permit error rate P_p can be calculated theoretically as follows:

$$P_p = 1-\left(\begin{pmatrix} m \\ \lceil m/2 \rceil \end{pmatrix}(1-P_b)^{\lceil m/2 \rceil} P_b^{m-\lceil m/2 \rceil} + \begin{pmatrix} m \\ \lceil m/2+1 \rceil \end{pmatrix}(1-P_b)^{\lceil m/2+1 \rceil} P_b^{m-\lceil m/2+1 \rceil} + \cdots + (1-P_b)^m\right)^L \tag{7.17}$$

From Fig. 7.9b, we see that the permit error rate has a good performance above $SNR_p = 8dB$. Based on [62], the channel SNR in $[10, 15)$, $[15, 25)$, and $[25, 40)$ indicates very poor, poor, and very good wireless channels. Hence, the whole permit transmission can realize in CREAM even in poor channel conditions.



(a) Repetition Encoding Impact

(b) Symbol Number Impact

Figure 7.11: False-positive Rate

False-positive Rate and False-negative Rate. As shown in Fig. 7.11a, the false-positive rate performs better above $SNR_p = 5$dB, which means the aSU is mistakenly recognized as the uSU with an extremely low possibility even in a poor channel. Comparing Fig.7.9b and Fig.7.11a, m puts a more important impact to the permit error rate than to the false-positive rate. With the same number of transmitted message bits in each frame, the number of permits is decreased due to low repetition rate. Therefore, we say that a large m lowers the permit transmission efficiency. Meanwhile, the number of OFDM symbols in each frame also affects the false-positive rate as shown in Fig.7.11b. With more OFDM symbols in each frame, each permit is transmitted more times. Since the verifier considers the transmitter as unauthorized when all the permits cannot be identified, the probability of identifying an incorrect aSU is lowered.

As for the false-negative rate, the probability that a uSU is identified as an aSU by successfully faking the 160-bit permit is $(1 - P_p)/2^{160}$. The probability is so small that the faking attack is considered as negligible.

7.7.2.3 Intrusiveness to message

Finally, we compare the message BER performance between the case without the permit and CREAM in Fig. 7.12. Suppose that the SNR difference $SNR_\delta = 12dB$. When $SNR_p \in [4dB, 14dB]$, the actually received SNR at the aSU receiver is in $[-8dB, 2dB]$. From Fig. 7.12, we conclude that CREAM almost brings no negative effect on message transmission. Instead, CREAM improves the message BER performance due to rotating the message constellation.

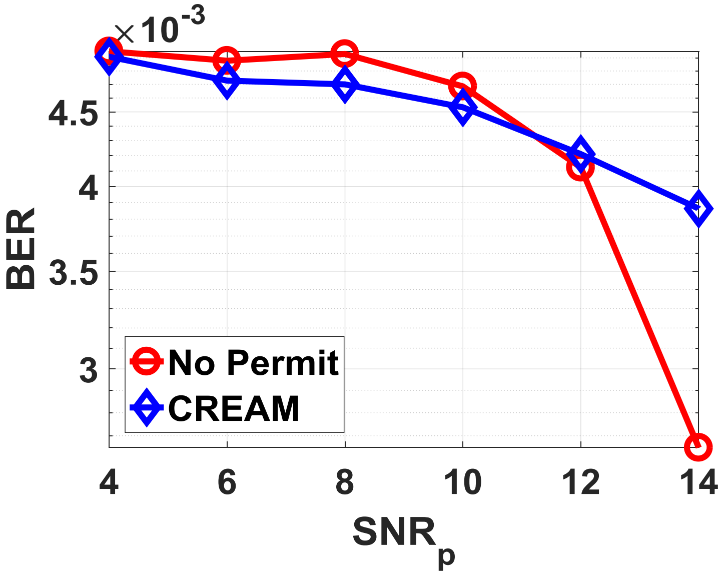


Figure 7.12: Comparison

7.8 Chapter Summary

In this chapter, we present a physical-layer unauthorized secondary user detection scheme referred to as CREAM. Combining the constellation rotation optimization, interleaving and superposition modulation in the OFDM framework, CREAM not only alleviates the negative effect of the aSU message transmission brought by fading, but also prevents the uSU from occupying the spectrum effectively. Detailed analysis and MATLAB simulation results have proven its accuracy, efficiency, security and low intrusion to message transmission.

Chapter 8

Conclusions and Discussion

This dissertation is along the line of designing schemes to ensure reliable and secure data transmission in emerging networks, especially in IoT network and cellular network. The common drawback in these emerging networks is the resource limitation due to the explosively increasing number of devices and data traffic they have generated, which devastates the data transmission in terms of reliability. Besides, most smart devices in IoT network are resource-constrained, for which they are vulnerable to various attacks. Although DSA is a promising way to alleviate the spectrum scarcity issue for both IoT network and cellular network, security concern arises. To address those problems, different schemes are designed in each chapter. Through simulations, real-world data evaluations, as well as practical experiments, we have demonstrated the effectiveness and efficiency of the proposed schemes, which validate our design objective, achieving reliable and secure data transmission in emerging networks given resource limitation.

As a matter of fact, IoT is transforming every corner of our daily life and plays a more and more important role. At the same time, there will be a larger number of smart devices equipped with various wireless protocols, resulting in severe wireless interference. As one of the future work, the potential attacks due to heterogeneous environment need to be future explored. For instance, following the line of signal emulation attack from WiFi to ZigBee devices, is it possible to launch the attacks from WiFi to BLE and from BLE to ZigBee in 2.4GHz band as well as from ZigBee to LoRa in 900MHz band? For the second future work, in the heterogeneous environment, the interference among different wireless protocols, named as the cross-technology interference (CTI), is usually treated as bad things. A plethora of work discusses how to alleviate and even eliminate it. CTI is small and a slight disturbance results in perceptible changes on it. Different from the traditional work, whether the above CTI feature can benefit us is a new direction. I will comprehensively investigate those features and attempt to apply them to human behavior detection and access authentication. In the end, with the application of machine learning or even deep learning in both wireless communication and networks, I would like to investigate it from the perspective of security. To be specific, adversarial attacks have been widely investigated in the image processing area, but they are scarcely addressed in the RF signal domain. The general idea for adversarial attacks to RF signal is to generate imperceptible perturbations to RF signal at the transmitter so as to mislead the DL classifier at the receiver. However, it is far more complex and difficult than that in the image domain. To be specific, RF adversarial examples suffer from complex channel proropogation/interference/noise during transmission, the effects of which will persist at the DL classifier and may change the classification results. As an emerging area, there are many open problems worth further investigation.

Bibliography

[1] Intel lab data. http://db.csail.mit.edu/labdata/labdata.html.

[2] Magic kingdom - disney world. http://www.wdwinfo.com/maps/magic-kingdom-map.pdf.

[3] Fcc. report and order and second further notice of proposed rulemaking. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-71A1.pdf, April 2015.

[4] Fcc claims us leadership in 5g with rules for millimeter wave spectrum. http://rethinkresearch.biz/articles/fcc-claims-us-leadership-in-5g-with-rules-for-millimeter-wave-spectrum/, July 2016.

[5] The c-based firmware patching framework for broadcom/cypress wifi chips that enables monitor mode, frame injection and much more. https://github.com/seemoo-lab/nexmon, 2017.

[6] Role of gain in usrp. http://lists.ettus.com/pipermail/usrp-users_lists.ettus.com/2017-May/053025.html, 2017.

[7] Ubiqua protocol analyzer. https://www.ubilogix.com/ubiqua/, 2019.

[8] Wireshark. https://www.wireshark.org/, 2019.

[9] Iot report how internet of things technology is now reaching mainstream companies and consumers. https://www.businessinsider.com/internet-of-things-report, 2020.

[10] Milton Abramowitz, Irene A Stegun, et al. Handbook of mathematical functions. *Applied mathematics series*, 55:62, 1966.

[11] Adnan Aijaz, Hamid Aghvami, and Mojdeh Amani. A survey on mobile data offloading: technical and business perspectives. *Wireless Communications, IEEE*, 20(2):104–112, 2013.

[12] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. *IEEE Transactions on Information Forensics and Security*, 9(5):772–781, May 2014.

[13] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong Li. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. *IEEE transactions on information forensics and security*, 9(5):772–781, 2014.

[14] Amazon. Sylvania dimmable led lamp, a19. https://www.amazon.com/SYLVANIA-SmartThings-Required-Assistant-Packaging/dp/B0197840KQ/ref=sr_1_5?ie=UTF8&qid=1529017285&sr=8-5&keywords=zigbee+bulb, 2018.

[15] Arash Asadi, Qing Wang, and Vincenzo Mancuso. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys & Tutorials*, 16(4):1801–1819, 2014.

[16] Imran Ashraf, Lester TW Ho, and Holger Claussen. Improving energy efficiency of femtocell base stations via user activity detection. In *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pages 1–5. IEEE, 2010.

[17] Søren Asmussen. *Applied probability and queues*, volume 51. Springer Science & Business Media, 2008.

[18] Ahmed Bader and Mohamed-Slim Alouini. Localized power control for multihop large-scale internet of things. *IEEE Internet of Things Journal*, 3(4):503–510, 2016.

[19] Aruna Balasubramanian, Ratul Mahajan, and Arun Venkataramani. Augmenting mobile 3g using wifi. In *Proceedings of the 8th international conference on Mobile systems, applications, and services*, pages 209–222. ACM, 2010.

[20] Mokhtar S Bazaraa, Hanif D Sherali, and Chitharanjan M Shetty. *Nonlinear programming: theory and algorithms*. John Wiley & Sons, 2013.

[21] Anass Benjebbour, Anxin Li, Yuya Saito, Yoshihisa Kishiyama, Atsushi Harada, and Takehiro Nakamura. System-level performance of downlink noma for future lte enhancements. In *Globecom Workshops (GC Wkshps), 2013 IEEE*, pages 66–70. IEEE, 2013.

[22] Dimitri P Bertsekas, Dimitri P Bertsekas, Dimitri P Bertsekas, and Dimitri P Bertsekas. *Dynamic programming and optimal control*, volume 1. Athena scientific Belmont, MA, 1995.

[23] Sudeep Bhattarai, Jung-Min Jerry Park, Bo Gao, Kaigui Bian, and William Lehr. An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research. *IEEE Transactions on Cognitive Communications and Networking*, 2(2):110–128, 2016.

[24] Joseph Boutros and Emanuele Viterbo. Signal space diversity: a power-and bandwidth-efficient diversity technique for the rayleigh fading channel. *IEEE Transactions on Information theory*, 44(4):1453–1467, 1998.

[25] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[26] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 116–127. ACM, 2008.

[27] Vladimir Brik, Vivek Shrivastava, Arunesh Mishra, and Suman Banerjee. Towards an architecture for efficient spectrum slicing. In *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*, pages 64–69. IEEE, 2007.

[28] Jacqueline Johnson Brown and Peter H Reingen. Social ties and word-of-mouth referral behavior. *Journal of Consumer research*, 14(3):350–362, 1987.

[29] Jo Brown, Amanda J Broderick, and Nick Lee. Word of mouth communication within online communities: Conceptualizing the online social network. *Journal of interactive marketing*, 21(3):2–20, 2007.

[30] Ozan Candogan, Kostas Bimpikis, and Asuman Ozdaglar. Optimal pricing in networks with externalities. *Operations Research*, 60(4):883–905, 2012.

[31] Karl E Case and Ray C Fair. *Principles of microeconomics*. Pearson Education, 2007.

[32] Kameswari Chebrolu and Ashutosh Dhekne. Esense: communication through energy sensing. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, pages 85–96. ACM, 2009.

[33] G. Chen and W. Dong. Jamcloak: Reactive jamming attack over cross-technology communication links. In *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, pages 34–43, Sep. 2018.

[34] Xu Chen, Xiaowen Gong, Lei Yang, and Junshan Zhang. A social group utility maximization framework with applications in database assisted spectrum access. In *INFOCOM, 2014 Proceedings IEEE*, pages 1959–1967. IEEE, 2014.

[35] Zicheng Chi, Yan Li, Hongyu Sun, Yao Yao, Zheng Lu, and Ting Zhu. B2w2: N-way concurrent communication for iot devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 245–258. ACM, 2016.

[36] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2015-2020 white paper. `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html`, Feb. 2016.

[37] VNI Cisco. Cisco visual networking index: Forecast and methodology 2016–2021.(2017), 2017.

[38] Federal Communications Commission et al. Report and order and second further notice of proposed rulemaking. *Amendment of the Commission's Rules with Regard to Commercial Operations in the*, pages 3550–3650, 2015.

[39] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. *Introduction to algorithms.* MIT press, 2009.

[40] International Data Corporation. The growth in connected iot devices is expected to generate 79.4zb of data in 2025, according to a new idc forecast. `https://www.idc.com/getdoc.jsp?containerId=prUS45213219`, Jun. 2019.

[41] George F Coulouris, Jean Dollimore, and Tim Kindberg. *Distributed systems: concepts and design.* pearson education, 2005.

[42] Thomas M Cover and Joy A Thomas. *Elements of information theory.* John Wiley & Sons, 2012.

[43] Harald Cramér. *Random variables and probability distributions*, volume 36. Cambridge University Press, 2004.

[44] Antonio Criminisi, Jamie Shotton, Ender Konukoglu, et al. Decision forests: A unified framework for classification, regression, density estimation, manifold learning and semi-supervised learning. *Foundations and Trends® in Computer Graphics and Vision*, 7(2–3):81–227, 2012.

[45] Daniele Croce, Natale Galioto, Domenico Garlisi, Fabrizio Giuliano, and Ilenia Tinnirello. An inter-technology communication scheme for wifi/zigbee coexisting networks. In *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*, pages 305–310. Junction Publishing, 2017.

[46] Boris Danev and Srdjan Capkun. Transient-based identification of wireless sensor nodes. In *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, pages 25–36. IEEE Computer Society, 2009.

[47] Klaus Doppler, Mika Rinne, Carl Wijting, Cássio B Ribeiro, and Klaus Hugl. Device-to-device communication as an underlay to lte-advanced networks. *IEEE Communications Magazine*, 47(12), 2009.

[48] Prajit K Dutta. *Strategies and games: theory and practice.* MIT press, 1999.

[49] Paul Erdos and A Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hungar. Acad. Sci*, 5:17–61, 1960.

[50] Ky Fan. Fixed-point and minimax theorems in locally convex topological linear spaces. *Proceedings of the National Academy of Sciences of the United States of America*, 38(2):121, 1952.

[51] Xueqi Fan, Fransisca Susan, William Long, and Shangyan Li. Security analysis of zigbee. `https://courses.csail.mit.edu/6.857/2017/project/17.pdf`, 2017.

[52] He Fang, Li Xu, and Kim-Kwang Raymond Choo. Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks. *Applied Mathematics and Computation*, 296:153–167, 2017.

[53] He Fang, Li Xu, and Xianbin Wang. Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme. *IEEE Transactions on Information Forensics and Security*, 2017.

[54] He Fang, Li Xu, and Xianbin Wang. Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme. *IEEE Transactions on Information Forensics and Security*, 13(1):197–209, 2018.

[55] Zhenhua Feng and Yaling Yang. Joint transport, routing and spectrum sharing optimization for wireless networks with frequency-agile radios. In *INFOCOM 2009, IEEE*, pages 1665–1673. IEEE, 2009.

[56] Robert FH Fischer. *Precoding and signal shaping for digital transmission.* John Wiley & Sons, 2005.

[57] Alexandros G Fragkiadakis, Elias Z Tragos, and Ioannis G Askoxylakis. A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 15(1):428–445, 2013.

[58] Drew Fudenberg and Jean Tirole. Game theory. Technical report, The MIT press, 1991.

[59] Pimmy Gandotra, Rakesh Kumar Jha, and Sanjeev Jain. Green communication in next generation cellular networks: a survey. *IEEE Access*, 5:11727–11758, 2017.

[60] Lin Gao, George Iosifidis, Jianwei Huang, and Leandros Tassiulas. Economics of mobile data offloading. In *Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on*, pages 351–356. IEEE, 2013.

[61] Wei Gao, Qinghua Li, and Guohong Cao. Forwarding redundancy in opportunistic mobile networks: Investigation and elimination. In *INFOCOM, 2014 Proceedings IEEE*, pages 2301–2309. IEEE, 2014.

[62] Jim Geier. How to: Define minimum snr values for signal coverage. *Viitattu*, 23:2012, 2008.

[63] Andrea Goldsmith. *Wireless communications.* Cambridge university press, 2005.

[64] Xiaowen Gong, Xu Chen, and Junshan Zhang. Social group utility maximization game with applications in mobile social networks. In *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on*, pages 1496–1500. IEEE, 2013.

[65] Xiaowen Gong, Lingjie Duan, and Xu Chen. When network effect meets congestion effect: Leveraging social services for wireless services. *Network*, 1(2):3, 2015.

[66] Michael Grant, Stephen Boyd, and Yinyu Ye. Cvx: Matlab software for disciplined convex programming, 2008.

[67] Dongning Guo, Shlomo Shamai, and Sergio Verdú. Mutual information and minimum mean-square error in gaussian channels. *IEEE Transactions on Information Theory*, 51(4):1261–1282, 2005.

[68] Linke Guo, Xinxin Liu, Yuguang Fang, and Xiaolin Li. User-centric private matching for ehealth networks-a social perspective. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 732–737. IEEE, 2012.

[69] Linke Guo, Chi Zhang, and Yuguang Fang. A trust-based privacy-preserving friend recommendation scheme for online social networks. *IEEE Transactions on Dependable and Secure Computing*, 12(4):413–427, 2015.

[70] Linke Guo, Chi Zhang, Jinyuan Sun, and Yuguang Fang. Paas: A privacy-preserving attribute-based authentication system for ehealth networks. In *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*, pages 224–233. IEEE, 2012.

[71] Linke Guo, Chi Zhang, Jinyuan Sun, and Yuguang Fang. A privacy-preserving attribute-based authentication system for mobile health networks. *IEEE Transactions on Mobile Computing*, 13(9):1927–1941, 2014.

[72] Linke Guo, Chi Zhang, Hao Yue, and Yuguang Fang. Psad: A privacy-preserving social-assisted content dissemination scheme in dtns. *IEEE Transactions on Mobile Computing*, 13(12):2903–2918, 2014.

[73] Linke Guo, Xiaoyan Zhu, Chi Zhang, and Yuguang Fang. Privacy-preserving attribute-based friend search in geosocial networks with untrusted servers. In *2013 IEEE Global Communications Conference (GLOBECOM)*, pages 629–634. IEEE, 2013.

[74] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Liangcheng Yu, and Omprakash Gnawali. Zigfi: Harnessing channel state information for cross-technology communication. In *Proceedings of ACM INFOCOM*, 2018.

[75] Piyush Gupta and Panganmala R Kumar. The capacity of wireless networks. *Information Theory, IEEE Transactions on*, 46(2):388–404, 2000.

[76] Biao Han, Jie Li, Jinshu Su, Minyi Guo, and Baokang Zhao. Secrecy capacity optimization via cooperative relaying and jamming for wanets. *IEEE Transactions on Parallel and Distributed Systems*, 26(4):1117–1128, 2015.

[77] Bo Han, Pan Hui, VS Anil Kumar, Madhav V Marathe, Jianhua Shao, and Aravind Srinivasan. Mobile data offloading through opportunistic communications and social participation. *Mobile Computing, IEEE Transactions on*, 11(5):821–834, 2012.

[78] Tao Han and Nayeem Ansari. Offloading mobile traffic via green content broker. *Internet of Things Journal, IEEE*, 1(2):161–170, 2014.

[79] Tao Han, Nayeem Ansari, Mingquan Wu, and Haoyong Yu. On accelerating content delivery in mobile networks. *Communications Surveys & Tutorials, IEEE*, 15(3):1314–1333, 2013.

[80] Zhiqiang He, Xiaonan Zhang, Yunqiang Bi, Weipeng Jiang, and Yue Rong. Optimal source and relay design for multiuser mimo af relay communication systems with direct links and imperfect channel information. *IEEE Transactions on Wireless Communications*, 15(3):2025–2038, 2015.

[81] Zhiqiang He, Xiaonan Zhang, Yunqiang Bi, Weipeng Jiang, and Yue Rong. Optimal source and relay design for multiuser mimo af relay communication systems with direct links and imperfect channel information. *IEEE Transactions on Wireless Communications*, 15(3):2025–2038, 2016.

[82] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[83] Weikun Hou, Xianbin Wang, and Jean-Yves Chouinard. Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates. In *2012 IEEE International Conference on Communications (ICC)*, pages 3559–3563. IEEE, 2012.

[84] Y Thomas Hou, Yi Shi, and Hanif D Sherali. Spectrum sharing for multi-hop networking with cognitive radios. *Selected Areas in Communications, IEEE Journal on*, 26(1):146–155, 2008.

[85] Wei-jen Hsu, Debojyoti Dutta, and Ahmed Helmy. Profile-cast: Behavior-aware mobile networking. In *2008 IEEE Wireless Communications and Networking Conference*, pages 3033–3038. IEEE, 2008.

[86] Sha Hua, Xuejun Zhuo, and Shivendra S Panwar. A truthful auction based incentive framework for femtocell access. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 2271–2276. IEEE, 2013.

[87] Pan Hui, Jon Crowcroft, and Eiko Yoneki. Bubble rap: Social-based forwarding in delay-tolerant networks. *Mobile Computing, IEEE Transactions on*, 10(11):1576–1589, 2011.

[88] De-Thu Huynh, Xiaofei Wang, Trung Q Duong, Nguyen-Son Vo, and Min Chen. Social-aware energy efficiency optimization for device-to-device communications in 5g networks. *Computer Communications*, 2018.

[89] iData Research. Small cells market and wifi offloading opportunities for mnos discussed in new 2015 research report.

[90] iData Research. Small cells market and wifi offloading opportunities for mnos discussed in new 2015 research report. *Mobile Computing, IEEE Transactions on*, 8(7):975–990, 2009.

[91] Hideki Imai and Shuji Hirakawa. A new multilevel coding method using error-correcting codes. *IEEE Transactions on Information Theory*, 23(3):371–377, 1977.

[92] Texas Instruments. Simplelink multi-standard cc26x2r wireless mcu launchpad development kit. `http://www.ti.com/tool/LAUNCHXL-CC26X2R1`, Jun. 2017.

[93] Juan José Jaramillo and R Srikant. Optimal scheduling for fair resource allocation in ad hoc networks with elastic and inelastic traffic. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.

[94] Edwin T Jaynes. *Probability theory: The logic of science*. Cambridge university press, 2003.

[95] Hong Jiang and Paul A Wilford. A hierarchical modulation for upgrading digital broadcast systems. *IEEE transactions on broadcasting*, 51(2):223–229, 2005.

[96] Weipeng Jiang, Zhiqiang He, Xiaonan Zhang, Yunqiang Bi, and Yue Rong. Joint transceiver design for amplify-and-forward multiuser mimo relay communication systems with source-destination links. *Journal of Communications*, 10(7), 2015.

[97] Xiaocong Jin, Jingchao Sun, Rui Zhang, and Yanchao Zhang. Safedsa: Safeguard dynamic spectrum access against fake secondary users. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 304–315. ACM, 2015.

[98] Xiaocong Jin, Jingchao Sun, Rui Zhang, Yanchao Zhang, and Chi Zhang. Specguard: Spectrum misuse detection in dynamic spectrum access systems. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 172–180. IEEE, 2015.

[99] P. Jokar, N. Arianpoo, and V. C. M. Leung. Spoofing prevention using received signal strength for zigbee-based home area networks. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 438–443, Oct 2013.

[100] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan. Wireless energy harvesting for the internet of things. *IEEE Communications Magazine*, 53(6):102–108, June 2015.

[101] Majid N Khormuji, Umar H Rizvi, Gerard JM Janssen, and S Ben Slimane. Rotation optimization for mpsk/mqam signal constellations over rayleigh fading channels. In *Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on*, pages 1–5. IEEE, 2006.

[102] Song Min Kim and Tian He. Freebee: Cross-technology communication via free side-channel. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pages 317–330. ACM, 2015.

[103] Tadayoshi Kohno, Andre Broido, and Kimberly C Claffy. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 2(2):93–108, 2005.

[104] Rajet Krishnan, Alexandre Graell i Amat, Thomas Eriksson, and Giulio Colavolpe. Constellation optimization in the presence of strong phase noise. *IEEE Transactions on Communications*, 61(12):5056–5066, 2013.

[105] Vireshwar Kumar, Jung-Min Park, and Kaigui Bian. Blind transmitter authentication for spectrum security and enforcement. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 787–798. ACM, 2014.

[106] Vireshwar Kumar, Jung-Min Park, T Charles Clancy, and Kaigui Bian. Phy-layer authentication by introducing controlled inter symbol interference. In *Communications and Network Security (CNS), 2013 IEEE Conference on*, pages 10–18. IEEE, 2013.

[107] Edward O Laumann. *Prestige and association in an urban community: An analysis of an urban stratification system.* Bobbs-Merrill Company, 1966.

[108] Kyunghan Lee, Joohyun Lee, Yung Yi, Injong Rhee, and Song Chong. Mobile data offloading: how much can wifi deliver? In *Proceedings of the 6th International COnference*, page 26. ACM, 2010.

[109] Feng Li, Jun Luo, Gaotao Shi, and Ying He. Art: Adaptive frequency-temporal co-existing of zigbee and wifi. *IEEE Transactions on Mobile Computing*, 16(3):662–674, 2017.

[110] Hongxing Li, Wei Huang, Chuan Wu, Zongpeng Li, and Francis CM Lau. Utility-maximizing data dissemination in socially selfish cognitive radio networks. In *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*, pages 212–221. IEEE, 2011.

[111] Ming Li and Pan Li. Crowdsourcing in cyber-physical systems: Stochastic optimization with strong stability. *IEEE Transactions on Emerging Topics in Computing*, 1(2):218–231, 2013.

[112] Ming Li, Pan Li, Xiaoxia Huang, Yuguang Fang, and Savo Glisic. Energy consumption optimization for multihop cognitive cellular networks. *IEEE Transactions on Mobile Computing*, 14(2):358–372, 2015.

[113] Pan Li, Chi Zhang, and Yuguang Fang. The capacity of wireless ad hoc networks using directional antennas. *Mobile Computing, IEEE Transactions on*, 10(10):1374–1387, 2011.

[114] Y. Li, K. Chi, H. Chen, Z. Wang, and Y. h. Zhu. Narrowband internet of things systems with opportunistic d2d communication. *IEEE Internet of Things Journal*, PP(99):1–1, 2017.

[115] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, pages 159–171. ACM, 2018.

[116] Yong Li, Zhaocheng Wang, Depeng Jin, and Sheng Chen. Optimal mobile content downloading in device-to-device communication underlaying cellular networks. *IEEE Transactions on Wireless Communications*, 13(7):3596–3608, 2014.

[117] Yong Li, Ting Wu, Pan Hui, Depeng Jin, and Sheng Chen. Social-aware d2d communications: Qualitative insights and quantitative analysis. *IEEE Communications Magazine*, 52(6):150–158, 2014.

[118] Zang Li, Wenyuan Xu, Rob Miller, and Wade Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM workshop on Wireless security*, pages 33–42. ACM, 2006.

[119] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 2–14. ACM, 2017.

[120] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi. Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach. *IEEE Transactions on Signal Processing*, 59(3):1202–1216, March 2011.

[121] Wei-Cheng Liao, Tsung-Hui Chang, Wing-Kin Ma, and Chong-Yung Chi. Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach. *IEEE Transactions on Signal Processing*, 59(3):1202–1216, 2011.

[122] Weixian Liao, Ming Li, Sergio Salinas, Pan Li, and Miao Pan. Optimal energy cost for strongly stable multi-hop green cellular networks. In *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on*, pages 62–72. IEEE, 2014.

[123] Xingqin Lin, Jeffrey Andrews, Amitabha Ghosh, and Rapeepat Ratasuk. An overview of 3gpp device-to-device proximity services. *IEEE Communications Magazine*, 52(4):40–48, 2014.

[124] Shuiyin Liu, Yi Hong, and Emanuele Viterbo. Practical secrecy using artificial noise. *IEEE Communications Letters*, 17(7):1483–1486, 2013.

[125] Xinxin Liu, Kaikai Liu, Linke Guo, Xiaolin Li, and Yuguang Fang. A game-theoretic approach for achieving k-anonymity in location based services. In *INFOCOM, 2013 Proceedings IEEE*, pages 2985–2993. IEEE, 2013.

[126] Yao Liu, Peng Ning, and Huaiyu Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 286–301. IEEE, 2010.

[127] Waslon Terllizzie Araújo Lopes and Marcelo Sampaio de Alencar. Performance of a rotated qpsk based system in a fading channel subject to estimation errors. In *Microwave and Optoelectronics Conference, 2001. IMOC 2001. Proceedings of the 2001 SBMO/IEEE MTT-S International*, volume 1, pages 27–30. IEEE, 2001.

[128] Xiao Ma and Li Ping. Coded modulation using superimposed binary codes. *IEEE Transactions on Information Theory*, 50(12):3331–3343, 2004.

[129] Xiao Ma and Li Ping. Power allocations for multilevel coding with sigma mapping. *Electron. Lett*, 40(10):609–611, 2004.

[130] Chetan N Mathur and KP Subbalakshmi. Digital signatures for centralized dsa networks. In *First IEEE Workshop on Cognitive Radio Networks*, pages 1037–1041, 2007.

[131] Hugo Méric, Jérôme Lacan, Fabrice Arnal, Guy Lesthievent, and Marie-Laure Boucheret. Combining adaptive coding and modulation with hierarchical modulation in satcom systems. *IEEE Transactions on Broadcasting*, 59(4):627–637, 2013.

[132] Md Sipon Miah, M Mahbubur Rahman, TK Godder, Bikash Chandra Singh, and M Tania Parvin. Performance comparison of awgn, flat fading and frequency selective fading channel for wireless communication system using 4qpsk. *International Journal of Computer and Information Technology*, 1(2):82–90, 2011.

[133] S. Michaels, K. Akkaya, and A. Selcuk Uluagac. Inducing data loss in zigbee networks via join/association handshake spoofing. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 401–405, Oct 2016.

[134] Subhasish Mitra, Subrata Chattopadhyay, and Suvra Sekhar Das. Deployment considerations for mobile data offloading in lte-femtocell networks. In *Signal Processing and Communications (SPCOM), 2014 International Conference on*, pages 1–6. IEEE, 2014.

[135] Nasser M Nasrabadi. Pattern recognition and machine learning. *Journal of electronic imaging*, 16(4):049901, 2007.

[136] Michael J Neely. Intelligent packet dropping for optimal energy-delay tradeoffs in wireless downlinks. *Automatic Control, IEEE Transactions on*, 54(3):565–579, 2009.

[137] Michael J Neely. Stochastic network optimization with application to communication and queueing systems. *Synthesis Lectures on Communication Networks*, 3(1):1–211, 2010.

[138] Michael J Neely. Opportunistic scheduling with worst case delay guarantees in single and multi-hop networks. In *INFOCOM, 2011 Proceedings IEEE*, pages 1728–1736. IEEE, 2011.

[139] Muhammad Shahmeer Omar, Syed Ahsan Raza Naqvi, Shahroze Humayun Kabir, and Syed Ali Hassan. An experimental evaluation of a cooperative communication-based smart metering data acquisition system. *IEEE Transactions on Industrial Informatics*, 13(1):399–408, 2017.

[140] Francesco Pantisano, Mehdi Bennis, Walid Saad, and Mérouane Debbah. Spectrum leasing as an incentive towards uplink macrocell and femtocell cooperation. *Selected Areas in Communications, IEEE Journal on*, 30(3):617–630, 2012.

[141] Neal Patwari and Sneha K Kasera. Robust location distinction using temporal link signatures. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 111–122. ACM, 2007.

[142] L Yu Paul, John S Baras, and Brian M Sadler. Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1):38–51, 2008.

[143] Anh Huy Phan, Hoang Duong Tuan, Ha Hoang Kha, and Ha H Nguyen. Beamforming optimization in multi-user amplify-and-forward wireless relay networks. *IEEE Transactions on Wireless Communications*, 11(4):1510–1520, 2012.

[144] Ramjee Prasad. *OFDM for wireless communications systems*. Artech House, 2004.

[145] Balaji Raghothaman, Eric Deng, Ravikumar Pragada, Gregory Sternberg, Tao Deng, and Kiran Vanganuru. Architecture and protocols for lte-based device to device communication. In *Computing, Networking and Communications (ICNC), 2013 International Conference on*, pages 895–899. IEEE, 2013.

[146] Theodore S Rappaport et al. *Wireless communications: principles and practice*, volume 2. Prentice Hall PTR New Jersey, 1996.

[147] Filippo Rebecchi, Marcelo Dias De Amorim, Vania Conan, Andrea Passarella, Raffaele Bruno, and Marco Conti. Data offloading techniques in cellular networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(2):580–603, 2015.

[148] Peter H Reingen, Brian L Foster, Jacqueline Johnson Brown, and Stephen B Seidman. Brand congruence in interpersonal relations: A social network analysis. *Journal of Consumer Research*, 11(3):771–783, 1984.

[149] Donald R Reising, Michael A Temple, and Mark E Oxley. Gabor-based rf-dna fingerprinting for classifying 802.16 e wimax mobile subscribers. In *2012 International Conference on Computing, Networking and Communications (ICNC)*, pages 7–13. IEEE, 2012.

[150] Ettus Research. Usrp n210. `https://www.ettus.com/product/details/UN210-KIT`.

[151] Injong Rhee, Minsu Shin, Seongik Hong, Kyunghan Lee, Seongjoon Kim, and Song Chong. CRAWDAD dataset ncsu/mobilitymodels (v. 2009-07-23). Downloaded from `http://crawdad.org/ncsu/mobilitymodels/20090723`, July 2009.

[152] Leonardo Jimenez Rodriguez, Nghi H Tran, Trung Q Duong, Tho Le-Ngoc, Maged Elkashlan, and Sachin Shetty. Physical layer security in wireless cooperative relay networks: State of the art and beyond. *IEEE Communications Magazine*, 53(12):32–39, 2015.

[153] J Ben Rosen. Existence and uniqueness of equilibrium points for concave n-person games. *Econometrica: Journal of the Econometric Society*, pages 520–534, 1965.

[154] James Scott, Richard Gass, Jon Crowcroft, Pan Hui, Christophe Diot, and Augustin Chaintreau. CRAWDAD dataset cambridge/haggle (v. 2009-05-29). Downloaded from `http://crawdad.org/cambridge/haggle/20090529`, May 2009.

[155] Y. Sharaf-Dabbagh and W. Saad. On the authentication of devices in the internet of things. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–3, June 2016.

[156] Bernard Sklar. *Digital communications*, volume 2. Prentice Hall Upper Saddle River, 2001.

[157] Nicolas Sklavos and Xinmiao Zhang. *Wireless security and cryptography: specifications and implementations.* CRC Press, 2007.

[158] Chaoming Song, Zehui Qu, Nicholas Blumm, and Albert-László Barabási. Limits of predictability in human mobility. *Science*, 327(5968):1018–1021, 2010.

[159] Liumeng Song, Kok Keong Chai, Yue Chen, Jonathan Loo, and John Schormans. Cooperative coalition selection for quality of service optimization in cluster-based capillary networks. *IEEE Systems Journal*, 2016.

[160] Liumeng Song, Kok Keong Chai, Yue Chen, John Schormans, Jonathan Loo, and Alexey Vinel. Qos-aware energy-efficient cooperative scheme for cluster-based iot systems. *IEEE Systems Journal*, 11(3):1447–1455, 2017.

[161] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017.

[162] Ananthram Swami and Brian M Sadler. Hierarchical digital modulation classification using cumulants. *IEEE Transactions on communications*, 48(3):416–429, 2000.

[163] Xi Tan, Kapil Borle, Wenliang Du, and Biao Chen. Cryptographic link signatures for spectrum usage authentication in cognitive radio. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 79–90. ACM, 2011.

[164] Sibel Tombaz, Zhihao Zheng, and Jens Zander. Energy efficiency assessment of wireless access networks utilizing indoor base stations. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, pages 3105–3110. IEEE, 2013.

[165] David Tse and Pramod Viswanath. *Fundamentals of wireless communication.* Cambridge university press, 2005.

[166] Oktay Ureten and Nur Serinken. Wireless security through rf fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1):27–33, 2007.

[167] Nedeljko Varnica, Xiao Ma, and Aleksandar Kavcic. Iteratively decodable codes for bridging the shaping gap in communication channels. In *Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on*, volume 1, pages 3–7. IEEE, 2002.

[168] VJ Venkataramanan, Xiaojun Lin, Lei Ying, and Sanjay Shakkottai. On scheduling for minimizing end-to-end buffer usage over multihop wireless networks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.

[169] Udo Wachsmann, Robert FH Fischer, and Johannes B Huber. Multilevel codes: theoretical concepts and practical design rules. *IEEE Transactions on Information Theory*, 45(5):1361–1391, 1999.

[170] Christian Walck. Handbook on statistical distributions for experimentalists. 2007.

[171] Dong Wang, Bo Bai, Wei Chen, and Zhu Han. Achieving high energy efficiency and physical-layer security in af relaying. *IEEE Transactions on Wireless Communications*, 15(1):740–752, 2016.

[172] Fang Wang, Yong Li, Zhaocheng Wang, and Zhixing Yang. Social-community-aware resource allocation for d2d communications underlaying cellular networks. *IEEE Transactions on Vehicular Technology*, 65(5):3628–3640, 2016.

[173] Tianyu Wang, Yue Sun, Lingyang Song, and Zhu Han. Social data offloading in d2d-enhanced cellular networks by network formation games. *IEEE Transactions on Wireless Communications*, 14(12):7004–7015, 2015.

[174] Zehua Wang, Hamed Shah-Mansouri, and Vincent WS Wong. How to download more data from neighbors? a metric for d2d data offloading opportunity. *IEEE Transactions on Mobile Computing*, 16(6):1658–1675, 2017.

[175] Eric W. Weisstein. "parseval's theorem." from mathworld–a wolfram web resource. `http://mathworld.wolfram.com/ParsevalsTheorem.html`.

[176] Wikipedia. `https://en.wikipedia.org/wiki/Utility`.

[177] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.

[178] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[179] X. Zhang, Q. Jia, and L. Guo. Secure and optimized unauthorized secondary user detection in dynamic spectrum access. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, October 2017.

[180] Liang Xiao, Caixia Xie, Tianhua Chen, Huaiyu Dai, and H Vincent Poor. A mobile offloading game against smart attacks. *IEEE Access*, 4:2281–2291, 2016.

[181] Chen Xu, Lingyang Song, Zhu Han, Qun Zhao, Xiaoli Wang, Xiang Cheng, and Bingli Jiao. Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach. *IEEE Journal on Selected Areas in Communications*, 31(9):348–358, 2013.

[182] Qian Xu, Pinyi Ren, Houbing Song, and Qinghe Du. Security enhancement for iot communications exposed to eavesdroppers with uncertain locations. *IEEE Access*, 4:2840–2853, 2016.

[183] Wenbo Xu, Xiaonan Zhang, Jing Zhai, and Jiaru Lin. On the achievable rate of mimo cognitive radio network with multiple secondary users. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2014.

[184] Dongyue Xue and Eylem Ekici. Guaranteed opportunistic scheduling in multi-hop cognitive radio networks. In *INFOCOM, 2011 Proceedings IEEE*, pages 2984–2992. IEEE, 2011.

[185] Lei Yang, Zengbin Zhang, Ben Y Zhao, Christopher Kruegel, and Haitao Zheng. Enforcing dynamic spectrum access with spectrum permits. In *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*, pages 195–204. ACM, 2012.

[186] Roy D. Yates. A framework for uplink power control in cellular radio systems. *IEEE Journal on selected areas in communications*, 13(7):1341–1347, 1995.

[187] Changyan Yi, Shiwei Huang, and Jun Cai. An incentive mechanism integrating joint power, channel and link management for social-aware d2d content sharing and proactive caching. *IEEE Transactions on Mobile Computing*, 17(4):789–802, 2018.

[188] Haoran Yu, Man Hon Cheung, George Iosifidis, Lin Gao, Leandros Tassiulas, and Jianwei Huang. Mobile data offloading for green wireless networks. *IEEE Wireless Communications*, 24(4):31–37, 2017.

[189] Bentao Zhang, Yong Li, Depeng Jin, Pan Hui, and Zhu Han. Social-aware peer discovery for d2d communications underlaying cellular networks. *IEEE Transactions on Wireless Communications*, 14(5):2426–2439, 2015.

[190] Xiaonan Zhang, Linke Guo, Ming Li, and Yuguang Fang. Social-enabled data offloading via mobile participation-a game-theoretical approach. In *Global Communications Conference (GLOBECOM), 2016 IEEE*, pages 1–6. IEEE, 2016.

[191] Xiaonan Zhang, Linke Guo, Ming Li, and Yuguang Fang. Motivating human-enabled mobile participation for data offloading. *IEEE Transactions on Mobile Computing*, 2017.

[192] Xiaonan Zhang, Pei Huang, Linke Guo, and Mo Sha. Incentivizing relay participation for securing iot communication. In *2019 Proceedings IEEE INFOCOM*, pages 1–9. IEEE, 2019.

[193] Xiaonan Zhang, Qi Jia, and Linke Guo. Secure and optimized unauthorized secondary user detection in dynamic spectrum access. In *Communications and Network Security (CNS), 2017 IEEE Conference on*, pages 1–9. IEEE, 2017.

[194] Xinyu Zhang and Kang G Shin. Cooperative carrier signaling: Harmonizing coexisting wpan and wlan devices. *IEEE/ACM Transactions on Networking (TON)*, 21(2):426–439, 2013.

[195] Xinyu Zhang and Kang G Shin. Gap sense: Lightweight coordination of heterogeneous wireless devices. In *INFOCOM, 2013 Proceedings IEEE*, pages 3094–3101. IEEE, 2013.

[196] Yang Zhang, Dusit Niyato, and Ping Wang. Offloading in mobile cloudlet systems with intermittent connectivity. *IEEE Transactions on Mobile Computing*, 14(12):2516–2529, 2015.

[197] Yifan Zhang and Qun Li. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In *INFOCOM, 2013 Proceedings IEEE*, pages 1366–1374. IEEE, 2013.

[198] Xiaolong Zheng, Yuan He, and Xiuzhen Guo. Stripcomm: Interference-resilient cross-technology communication in coexisting environments. In *IEEE Int. Conf. Comput. Commun.(INFOCOM)*, pages 15–19, 2018.

[199] Huan Zhou, Hui Wang, Xiuhua Li, and Victor CM Leung. A survey on mobile data offloading technologies. *IEEE Access*, 6:5101–5111, 2018.

[200] Ying Zhu, Bin Xu, Xinghua Shi, and Yu Wang. A survey of social-based routing in delay tolerant networks: positive and negative social effects. *Communications Surveys & Tutorials, IEEE*, 15(1):387–401, 2013.

[201] Yulong Zou, Xianbin Wang, and Weiming Shen. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, 31(10):2099–2111, 2013.

[202] Yulong Zou, Jia Zhu, Xianbin Wang, and Victor CM Leung. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, 29(1):42–48, 2015.