

SECURE AND EFFICIENT SPECTRUM SHARING AND QOS ANALYSIS IN
OFDM-BASED HETEROGENEOUS WIRELESS NETWORKS

By

Ahmed S. Alahmadi

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Electrical Engineering — Doctor of Philosophy

2016

ABSTRACT

SECURE AND EFFICIENT SPECTRUM SHARING AND QOS ANALYSIS IN OFDM-BASED HETEROGENEOUS WIRELESS NETWORKS

By

Ahmed S. Alahmadi

The Internet of Things (IoT), which networks versatile devices for information exchange, remote sensing, monitoring and control, is finding promising applications in nearly every field. However, due to its high density and enormous spectrum requirement, the practical development of IoT technology seems to be not available until the release of the large millimeter wave (mmWave) band (30GHz-300GHz). Compared to existing lower band systems (such as 3G, 4G), mmWave band signals generally require line of sight (LOS) path and suffer from severe fading effects, leading to much smaller coverage area. For network design and management, this implies that: (i) MmWave band alone could not support the IoT networks, but has to be integrated with the existing lower band systems through secure and effective spectrum sharing, especially in the lower frequency bands; and (ii) The IoT networks will have very high density node distribution, which is a significant challenge in network design, especially with the scarce energy budget of IoT applications.

Motivated by these observations, in this dissertation, we consider three problems: (1) How to achieve secure and effective spectrum sharing? (2) How to accommodate the energy limited IoT devices? (3) How to evaluate the Quality of Service (QoS) in the high density IoT networks? We aim to develop innovative techniques for the design, evaluation and management of future IoT networks under both benign and hostile environments. The main contributions of this dissertation are outlined as follows.

First, we develop a secure and efficient *spectrum sharing* scheme in single-carrier wireless networks. Cognitive radio (CR) is a key enabling technology for spectrum sharing, where the unoccupied spectrum is identified for secondary users (SUs), without interfering with the

primary user (PU). A serious security threat to the CR networks is referred to as primary user emulation attack (PUEA), in which a malicious user (MU) emulates the signal characteristics of the PU, thereby causing the SUs to erroneously identify the attacker as the PU. Here, we consider full-band PUEA detection and propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the DTV transmitter and used as the sync bits of the DTV data frames. For PU detection, we investigate the cross-correlation between the received sequence and reference sequence. The MU detection can be performed by investigating the auto-correlation of the received sequence.

We further develop a secure and efficient spectrum sharing scheme in multi-carrier wireless networks. We consider sub-band malicious user detection and propose a secure AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm. The resulted sequence is exploited for accurate detection of the authorized PU and the MU.

Second, we develop an *energy efficient* transmission scheme in CR networks using energy harvesting. We propose a transmitting scheme for the SUs such that each SU can perform information reception and energy harvesting simultaneously. We perform sum-rate optimization for the SUs under PUEA. It is observed that the sum-rate of the SU network can be improved significantly with the energy harvesting technique. Potentially, the proposed scheme can be applied directly to the energy-constrained IoT networks.

Finally, we investigate *QoS performance analysis methodologies*, which can provide insightful feedbacks to IoT network design and planning. Taking the spatial randomness of the IoT network into consideration, we investigate coverage probability (CP) and blocking probability (BP) in relay-assisted OFDMA networks using stochastic geometry. More specifically, we model the inter-cell interference from the neighboring cells at each typical node, and derive the CP in the downlink transmissions. Based on their data rate requirements, we classify the incoming users into different classes, and calculate the BP using the multi-dimensional loss model.

Copyright by
AHMED S. ALAHMADI
2016

This dissertation is dedicated to my beloved family...

ACKNOWLEDGMENTS

I would like to take this opportunity to express my sincere appreciation for all the support and encouragement that have led to the completion of this dissertation. I am greatly indebted to my advisor, Prof. Tongtong Li, for her continuous support, help, patience, and encouragement throughout my PhD studies at Michigan State University.

I would also like to thank Prof. Hassan Khalil, Prof. Eric Torng, and Prof. Mi Zhang for serving on my committee. I am deeply grateful to them for their valuable comments and insightful discussions.

Special thanks go to my past and present colleagues in the Broadband Access and Wireless Communication (BAWC) lab: Zhaoxi Fang, Mai Abdelhakim, Tianlong Song, Zhe Wang, Yuan Liang, Run Tian, and Yu Zheng for making my stay at Michigan State University more enjoyable, and for their insightful and helpful academic inputs.

I am greatly grateful to my family and friends for their tremendous support and encouragement. My profound gratitude is to my mother for her endless love, prayers, and support.

I could not be more grateful to my beloved wife and my sweet daughter. This dissertation would not have been accomplished without their love, care, patience, and support. Thank you all for making this dream a reality.

TABLE OF CONTENTS

LIST OF TABLES	x
LIST OF FIGURES	xi
KEY TO ABBREVIATIONS	xiii
Chapter 1 Introduction	1
1.1 Overview	1
1.1.1 Motivations and Problem Identification	1
1.1.2 Research Overview	2
1.2 Revisit of the Existing Work	4
1.2.1 Primary User Emulation Attack	4
1.2.2 Energy Harvesting and Reliable Information Transfer	7
1.2.3 QoS Performance Measure in IoT Networks	9
1.3 Summary of Dissertation Contributions	10
Chapter 2 Full-band PUEA Detection and Mitigation	15
2.1 Introduction	16
2.2 The Proposed AES-assisted DTV Approach	18
2.2.1 A Brief Review of the Terrestrial DTV System	18
2.2.2 AES-assisted DTV Transmitter	19
2.2.3 AES-assisted DTV Receiver	21
2.2.3.1 Detection of the Primary User	22
2.2.3.2 Detection of the Malicious User	23
2.2.4 Further Discussions	25
2.3 Analytical Evaluation of the Proposed AES-assisted DTV Approach	27
2.3.1 Analytical Evaluation of Primary User Detection	27
2.3.2 Analytical Evaluation of Malicious User Detection	31
2.3.2.1 False Alarm Rate and Miss Detection Probability for Malicious User Detection	31
2.3.2.2 The Optimal Thresholds for Malicious User Detection	38
2.4 Security and Feasibility of the Proposed AES-assisted DTV Approach	40
2.4.1 A Brief Overview of the AES Algorithm	40
2.4.2 Security of the AES-assisted DTV	42
2.4.3 Feasibility	43
2.5 Simulation Results	44
2.6 Summary	47
Chapter 3 Sub-band PUEA Detection and Mitigation	49
3.1 Introduction	49

3.2	System Model	51
3.3	AES-based PUEA Detection Scheme	54
3.3.1	Primary User Transmitter Design	54
3.3.2	Secondary User Coordinator Receiver Design	55
3.3.2.1	Primary User Detection	56
3.3.2.2	Malicious User Detection	57
3.3.3	False Alarm Rate and Miss Detection Probability	59
3.3.4	Detection Performance Versus Sample Size	60
3.4	Simulation Results	61
3.5	Summary	62
Chapter 4	Energy Harvesting and Reliable Information Transfer	64
4.1	Introduction	65
4.2	The Proposed Energy Harvesting Scheme	66
4.3	Energy Harvesting and Performance Optimization	68
4.3.1	Secondary Users Energy Harvesting and Information Recovery	68
4.3.1.1	Achievable Transmission Rate for SU1	69
4.3.1.2	Achievable Transmission Rate for SU2	71
4.3.2	Sum-rate Optimization	72
4.3.3	Suboptimal Solution	74
4.3.3.1	Sum-rate Lower Bound	74
4.3.3.2	Suboptimal Solutions	77
4.4	Discussions on Worst Jamming Interference in PUEA	78
4.5	Simulation Results	81
4.6	Summary	84
Chapter 5	Blocking Probability Analysis for Relay-assisted OFDMA Net-works	86
5.1	Introduction	86
5.2	System Model	89
5.2.1	Network Model	89
5.2.2	Transmission Protocol Design	90
5.2.3	Channel Model	92
5.3	Interference Modeling and Achievable Rate Analysis	92
5.3.1	Interference Model	92
5.3.2	Coverage Probability	94
5.3.2.1	Coverage Probability of Direct Transmission	94
5.3.2.2	Coverage Probability of 2-hop Transmission	95
5.3.3	Achievable Transmission Rate	96
5.4	Blocking Probability Analysis	97
5.4.1	Resource Allocation and Traffic Modeling	98
5.4.2	Blocking Probability Calculation	100
5.5	Simulation Results	102
5.6	Summary	104

Chapter 6	Conclusions and Future Work	106
6.1	Conclusions	106
6.2	Future Work	108
APPENDIX		110
BIBLIOGRAPHY		114

LIST OF TABLES

Table 4.1:	System Parameters	82
Table 5.1:	Simulation Parameters	102

LIST OF FIGURES

Figure 1.1:	A possible scenario for the attackers to avoid PUEA detection approaches based on the location and/or the energy level of the received signal. For example, MU1 can produce the same DOA and comparable received power level as the primary user, while MU2 can produce comparable received power level as the primary user.	6
Figure 2.1:	8-VSB signal frame structure.	19
Figure 2.2:	Generation of the reference signal.	20
Figure 2.3:	AES encryption.	41
Figure 2.4:	Normalized cross-correlation between the reference signal and noisy versions of malicious user's signal. Note that the cross-correlation values are in the order of 10^{-4} , which is close to 0.	42
Figure 2.5:	Normalized cross-correlation between the reference signal and noisy versions of the primary user's signal. Here, $\sigma_s^2 = 1$	43
Figure 2.6:	Example 1: The false alarm rate and miss detection probability for primary user detection.	45
Figure 2.7:	Example 2: The optimal thresholds for malicious user detection for $\delta = 10^{-3}$. Here, $P_0 = 0.25$	46
Figure 2.8:	Example 3: The overall false alarm rate and the overall miss detection probability for malicious user detection. Here, $P_0 = 0.25$ and $\delta = 10^{-3}$	47
Figure 3.1:	The proposed cognitive radio network architecture.	51
Figure 3.2:	The DVB-T2 frame structure.	52
Figure 3.3:	Generation of the proposed reference signal $\mathbf{s}$	55
Figure 3.4:	The false alarm rate (FAR) and miss detection probability (MDP) versus SNR for primary user detection.	61
Figure 3.5:	The false alarm rate (FAR) and miss detection probability (MDP) versus SNR for malicious user detection.	62

Figure 4.1:	The proposed energy harvesting scheme.	67
Figure 4.2:	The achievable sum-rate comparison of the proposed OFDM-based energy harvesting scheme and that of its non-energy harvesting counterpart versus different PU and MU transmit power levels.	83
Figure 4.3:	The optimal and suboptimal power splitting ratios versus PU transmit power.	84
Figure 5.1:	The proposed relay-assisted network architecture.	89
Figure 5.2:	The proposed 2-hop routing topology.	90
Figure 5.3:	Example 1: The system blocking probability P_B versus r_{BS} . Here, $r_{BS,Opt} = 225.36$ m.	103
Figure 5.4:	Example 2: Class distribution and class blocking probability versus M_j using $r_{BS,Opt} = 225.36$ m.	104

KEY TO ABBREVIATIONS

IoT	Internet of Things
mmWave	Millimeter Wave
CR	Cognitive Radio
DSA	Dynamic Spectrum Access
PU	Primary User
SU	Secondary User
SUC	Secondary User Coordinator
MU	Malicious User
PUEA	Primary User Emulation Attack
LFSR	Linear Feedback Shift Register
AES	Advanced Encryption Standard
BPSK	Binary Phase Shift Keying
RSS	Received Signal Strength
LOS	Line of Sight
DOA	Direction of Arrival
8-VSB	Eight Level Vestigial Sideband
DVB-T2	Second Generation Terrestrial DTV Standard
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
TDMA	Time Division Multiple Access
CSI	Channel State Information
SNR	Signal to Noise Ratio
SINR	Signal to Interference plus Noise Ratio
QoS	Quality of Service
BP	Blocking Probability
PPP	Poisson Point Process

Chapter 1

Introduction

In this chapter, we provide a brief overview of the IoT technology and highlight its fundamental challenges, which motivate us to develop innovative techniques to address them. These techniques are summarized in the main contributions of this dissertation, which include full-band PUEA detection and mitigation, sub-band PUEA detection and mitigation, energy harvesting and reliable information transfer, and blocking probability analysis for relay-assisted OFDMA networks.

1.1 Overview

1.1.1 Motivations and Problem Identification

The Internet of Things (IoT), which networks versatile devices for information exchange, remote sensing, monitoring and control, is finding promising applications in nearly every field. However, due to its high density and enormous spectrum requirement, the practical development of IoT technology seems to be not available until the release of the large millimeter wave (mmWave) band (30GHz-300GHz). Compared to existing lower band systems (such as 3G, 4G), mmWave band signals generally require line of sight (LOS) path and suffer from severe fading effects, leading to much smaller coverage area. For network design and management, this implies that: (i) MmWave band alone could not support the IoT networks,

but has to be integrated with the existing lower band systems through secure and effective spectrum sharing, especially in the lower frequency bands; and (ii) The IoT networks will have very high density node distribution, which is a significant challenge in network design, especially with the scarce energy budget and the low cost requirements of IoT applications.

Motivated by these observations, in this dissertation, we consider three problems: (1) How to achieve secure and effective spectrum sharing? (2) How to accommodate the energy limited IoT devices? (3) How to evaluate the Quality of Service (QoS) in the high density IoT networks? We aim to develop innovative techniques for the design, evaluation and management of future IoT networks under both benign and hostile environments. These techniques are highlighted in the following subsection.

1.1.2 Research Overview

In this subsection, we provide an overview of the proposed techniques that can be applied to the design, performance evaluation and enhancement of IoT networks. These techniques include:

- **Developing Secure and Efficient Spectrum Sharing Scheme in the HDTV Bands** Cognitive radio (CR) is a key enabling technology for spectrum sharing, where the unoccupied spectrum is identified for secondary users (SUs), without interfering with the primary user (PU). A serious security threat to the CR networks is referred to as primary user emulation attack (PUEA), in which a malicious user (MU) emulates the signal characteristics of the PU, thereby causing the SUs to erroneously identify the attacker as the PU. Here, we start with *single-carrier* transmission, where the signal is processed in the entire spectrum and hence allows full-band detection. We con-

sider full-band PUEA detection and propose a reliable Advanced Encryption Standard (AES)-assisted digital TV (DTV) scheme, where an AES-encrypted reference signal is generated at the DTV transmitter and used as the sync bits of the DTV data frames. For primary user detection, we investigate the cross-correlation between the received sequence and reference sequence. The malicious user detection can be performed by investigating the auto-correlation of the received sequence.

We further develop a secure and efficient spectrum sharing scheme in *multi-carrier* wireless networks. Motivated by the prevalence of the orthogonal frequency division multiplexing (OFDM)-based systems, we consider sub-band malicious user detection and propose a secure AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm, and the resulted sequence is exploited for accurate detection of the authorized PU and the MU.

Based on the discussions above, potentially, the proposed schemes can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

- **Developing Energy Efficient Schemes** We propose an energy efficient transmission scheme in CR networks using energy harvesting, where each SU can perform information reception and energy harvesting simultaneously. We perform sum-rate optimization for the SUs under PUEA. It is observed that the sum-rate of the SU network can be improved significantly with the energy harvesting technique. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

- **Developing Innovative Performance Analysis Methodologies** Taking the spatial randomness of the IoT network into consideration, we investigate blocking probability in relay-assisted orthogonal frequency division multiple access (OFDMA) networks using stochastic geometry. More specifically, we model the inter-cell interference from the neighboring cells at each typical node, and derive the coverage probability in the downlink transmissions. Based on their data rate requirements, we classify the incoming users into different classes, and calculate the BP using the multi-dimensional loss model. We show that the BP can be reduced by exploiting relay-assisted transmissions.

1.2 Revisit of the Existing Work

1.2.1 Primary User Emulation Attack

Along with the ever-increasing demand in high-speed wireless communications, spectrum scarcity has become a serious challenge to the emerging wireless technologies. In licensed networks, the primary users operate in their allocated licensed bands. It is observed that the licensed bands are generally underutilized and their occupation fluctuates temporally and geographically in the range of 15% to 85% [1]. Cognitive radio networks [2–4] provide a promising solution to the spectrum scarcity and underutilization problems [5].

CR networks are based on dynamic spectrum access (DSA), where the secondary users are allowed to share the spectrum with the primary users. The spectrum sharing is made under the condition that the secondary users do not interfere with the primary system’s traffic. The CRs identify the unused bands (white spaces) through spectrum sensing [4], then utilize the idle bands for data transmissions. The spectrum sensing function is continuously performed. If a primary signal is detected in the band that a CR operates in, then the CR must evacuate

that band and operate in another white space [6].

The CR system is vulnerable to malicious attacks that could disrupt its operation. A well-known malicious attack is the primary user emulation attack [7–9]. In PUEA, malicious users mimic the primary signal over the idle frequency band(s) such that the authorized secondary users cannot use the corresponding white space(s). This leads to low spectrum utilization and inefficient cognitive network operation.

PUEA has attracted considerable research attention in literature. In [10], an analytical model for the probability of successful PUEA based on the energy detection was proposed, where the received signal power is modeled as a log-normally distributed random variable. In this approach, a lower bound on the probability of a successful PUEA is obtained using Markov inequality. In [11], a nonparametric Bayesian approach, called DECLOAK, was investigated to identify PUEA. The idea of this approach is to use some of the transmitted signal parameters as a fingerprint to identify the actual primary users, and hence the attackers.

Several other methods have been proposed to detect and defend against PUEA. In [12], a transmitter verification scheme (localization-based defense) was proposed to detect PUEA. In [13] and [14], the authors proposed a received signal strength (RSS)-based defense technique to defend against PUEA, where the attackers can be identified by comparing the received signal power of the primary user and the suspect attacker. A Wald’s sequential probability ratio test (WSPRT) was presented to detect PUEA based on the received signal power in [15]. A similar strategy was used to detect PUEA in fading wireless environments in [16]. In [17], a cooperative secondary user model was proposed for primary user detection in the presence of PUEA. In this approach, the decision whether the primary user is present or absent is based on the energy detection method. In [18], the authors proposed compressive sensing

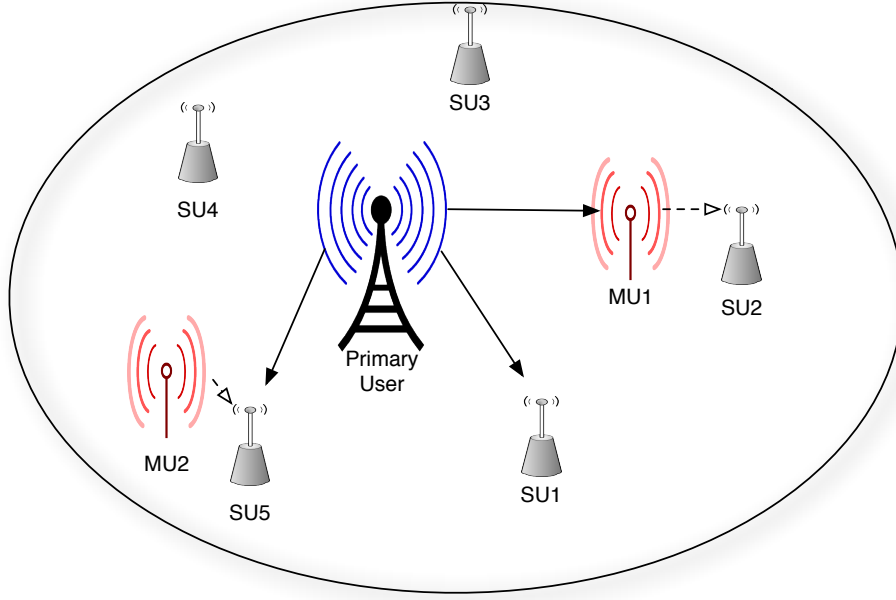


Figure 1.1: A possible scenario for the attackers to avoid PUEA detection approaches based on the location and/or the energy level of the received signal. For example, MU1 can produce the same DOA and comparable received power level as the primary user, while MU2 can produce comparable received power level as the primary user.

based approach to distinguish whether the signals transmitted are from the primary users or malicious users. In mobile CR networks, the authors in [19] proposed a method to detect PUEA on mobile primary users by exploiting the correlations between radio frequency (RF) signals and acoustic information to verify the existence of malicious wireless microphones. Recently, in [20], location reliability and malicious intention were explored to detect primary user and malicious user in mobile CR networks.

In most of these existing approaches, the detection of PUEA is mainly based on the power level and/or the direction of arrival (DOA) of the received signal. The basic idea is that: given the locations of the primary TV stations, the secondary user can distinguish the actual primary signal from the malicious user's signal by comparing the power level and/or the DOA of the received signal with that of the authorized primary user's signal. The major limitation with such approaches is that: they would fail when a malicious user

is at a location where it produces the same DOA and/or comparable received power level as that of the actual primary transmitter, as shown in Figure 1.1 (see the positions of MU1 and MU2).

1.2.2 Energy Harvesting and Reliable Information Transfer

Along with the emerging energy-constrained IoT network, which basically relies on transceivers with limited power capabilities, wireless energy transfer has attracted more research interest in recent years [21–35]. In literature, there are three main wireless power transfer techniques, namely, *magnetic inductive coupling*, *magnetic resonance coupling*, and *RF energy harvesting*. In this dissertation, we focus on the RF energy harvesting techniques.

Magnetic inductive coupling is based on the magnetic induction principle, where a varying current at the primary/transmitter coil generates a varying magnetic field, which then can be captured by a secondary/receiver coil and converted the magnetic field back to electricity. The power transfer efficiency depends on physical separation between the two coils and their quality factor. In [21], it was shown that, for distances range from 2 cm to 8 cm, the efficiency of the magnetic inductive coupling varies roughly from 65% to 5%, respectively.

Magnetic resonance coupling is similar to the inductive coupling, but with an addition of a capacitance on both the primary and secondary coils, which they are then referred to as resonators. To achieve high power transfer efficiency, the two resonators should work on the same frequency [22]. The authors in [23] were able to achieve power transfer efficiency from 30% to above 90% with distances vary from 2.25 m to 0.75 m, respectively, using magnetic resonance coupling method.

Energy harvesting from ambient RF signals has gained considerable attention in both industrial and academic fields. The concept of simultaneous wireless information transfer

and energy harvesting was first proposed in [24], where the fundamental trade-off between information receiving and power transfer was studied from an information theory perspective. In literature [25, 26], there have been two representative receiver architectures for energy harvesting: power-splitting and time-switching. In the power-splitting based approach, a power splitter is employed at the RF band at the receiver. The received RF signal is split into two parts: one for energy harvesting and the other for information processing. In the time-switching approach, the received signal is divided into two parts in the time domain. The power transfer efficiency of energy harvesting techniques depends mainly on the received signal strength. In [27], it was shown that an efficiency of 0.4%, 18.2% and above 50% can be achieved with RF energy transfer with input power -40dBm , -5dBm , and 20dBm , respectively. More details on efficiency performance of wireless energy transfer techniques can be found in [28].

Recently, energy harvesting has been widely discussed in OFDM-based systems [29], wireless relay networks [30], and cognitive radio networks [31–35]. For example, the authors in [31] investigated the optimal transmission and energy harvesting policy to maximize the secondary network throughput in a cognitive radio network, where the secondary users opportunistically access the spectrum or harvest energy from the ambient RF signals from primary users. In [32], the authors studied the channel access problem in CR networks in which a secondary user can choose to access the channel for data transmission or energy harvesting. To obtain the channel access, they presented an optimization formulation based on Markov decision process.

Generally, PUEA was not considered in these works [31–35]. However, PUEA is essentially jamming interference for the SUs, and potentially the performance of SUs can be improved significantly by exploiting PUEA as an extra energy resource. In addition to the

jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

1.2.3 QoS Performance Measure in IoT Networks

In designing and analyzing wireless networks, blocking probability has been used as a very important metric in evaluating the QoS of the network. Blocking probability is the probability that an arriving user is denied of service due to insufficient network resources. In literature, blocking probability has been investigated for the OFDMA networks from different perspectives. To provide more reliable services for users with low received signal strength, relay stations are often deployed along with the base stations to extend the coverage area and improve the QoS. As a result, blocking probability has been studied in both single-hop and multi-hop networks.

Some representative work on blocking probability for the single-hop OFDMA networks can be found in [36–38]. In [36], the authors tried to model the subcarrier-allocation system using the batch-arrival model $M^X/M/c/c$. This model is not sufficiently accurate due to the assumption that the subcarriers are allocated in bulks but released one by one. Therefore, in [37], a more realistic model known as multi-class Erlang loss model was proposed. Motivated by the fact that power should be considered in addition to subcarriers as a system resource, a more general model was proposed in [38], where both the power and the subcarriers are regarded as the system resources.

Blocking probability for multi-hop OFDMA networks is attracting more research attention along with the emerging high density IoT networks. For example, in [39], the authors proposed a system model to evaluate the blocking probability for the relay-based OFDMA cellular networks. In their model, each cell consists of a base station, located at the center of

the cell, and is surrounded by six relay stations with deterministic (known) locations. However, as pointed out in [40], results based on such highly idealized models generally may not be very accurate. On the other hand, it was also shown in [40] that modeling the locations of the base/relay stations stochastically according to a Poisson point process (PPP) depicts the reality and can achieve more reliable and accurate results compared to its idealized counterparts. More closely, stochastic geometry has been widely applied in modeling wireless networks in recent years [41–44]. For instance, in [41], stochastic geometry was used to analyze relay-aided two-hop networks. In [42], it was used to analyze multi-hop transmission in ad-hoc networks. However, no work has been done in literature to investigate blocking probability in relay-assisted OFDMA networks using stochastic geometry. Moreover, a very challenging problem in calculating the blocking probability is to obtain *the distribution of the group size of the subcarriers that an arriving user needs* to fulfill its data rate. In most of the existing work [36–38], this distribution is assumed to be known, usually assumed to be uniform. This may not be accurate, especially for large group sizes, which actually have very low request probability.

1.3 Summary of Dissertation Contributions

The main contributions of this dissertation are summarized in the following.

In Chapter 2, we develop a secure and efficient spectrum sharing scheme in single-carrier wireless networks. We consider full-band PUEA detection in single-carrier ATSC 1.0 DTV system, where the primary user’s signal is processed in the entire spectrum. We propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared

secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve full-band identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The proposed scheme combats primary user emulation attacks, and enables more robust system operation and efficient spectrum sharing. The effectiveness of the proposed approach is demonstrated through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

In Chapter 3, we further develop a secure and efficient spectrum sharing scheme in multi-carrier wireless networks. Unlike single-carrier transmission schemes, which allow only full-band PUEA detection, multi-carrier schemes provide potential flexibility in performing sub-band PUEA detection in CR networks. Motivated by this fact and the prevalence of the OFDM-based DTV standard, we consider sub-band malicious user detection in OFDM-based CR network under PUEA. Here, the CR network consists of primary users, secondary user coordinators (SUCs), secondary users, and malicious users. The SUCs are designed to perform spectrum sensing and sub-band PUEA detection, and then coordinate the SUs for collision-free transmission over the white spaces. We propose a robust and efficient AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm, and the resulted sequence is exploited for accurate detection of the authorized primary user and the malicious user.

Along with the OFDM-based transceiver structure and pilot symbol allocation scheme in the DVB-T2 standard, we can detect the presence of PUEA over each 3-subcarrier sub-band. However, the proposed approach can be used to detect PUEA over each single subcarrier if

the preamble symbols in the DVB-T2 standard can be adjusted to cover every subcarrier. The performance of the proposed PUEA detection approach is evaluated through false alarm rate and miss detection probability. Our analysis indicates that the proposed approach can detect PUEA with high accuracy. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

In Chapter 4, we develop an energy efficient transmission scheme in CR networks using energy harvesting. Here, the main contribution is twofold. First, we come up with an effective communication scheme for the secondary users under PUEA by exploiting the energy harvesting techniques. Using PUEA as an extra power resource, we present a transmitting scheme for the SUs such that each SU can perform information reception and energy harvesting simultaneously. We perform sum-rate (downlink transmission rate plus uplink transmission rate) optimization for the SUs under PUEA. As the optimal solution is based on multi-dimensional exhaustive search, we further propose a suboptimal scheme with closed-form solution. Our simulations demonstrate that the performance of the suboptimal scheme is very close to that of the optimal solution. Moreover, as expected, significant performance improvement can be observed when comparing with non-energy harvesting systems. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

Second, we evaluate the worst-case PUEA interference in terms of minimizing the sum-rate for the secondary users. We prove that for the secondary users, equal power interference from the malicious user is the worst interference for weak jamming (i.e., when the received signal power is much larger than the received jamming power), and nearly the worst interference for strong jamming (i.e., when the received jamming power is much larger than

the received signal power and the noise power), while the channel state information (CSI) assisted interference is the worst-case interference for strong jamming in the high signal-to-noise ratio (SNR) region. Moreover, we show that the resulted sum-rate performance gap between equal power interference and CSI-assisted interference is small. These results indicate that for practical systems, due to the absence of CSI information, the worst jamming for the SUs is when the malicious user performs equal power allocation over all the white space subcarriers.

In Chapter 5, taking the spatial randomness of the IoT network into consideration, we investigate coverage probability and blocking probability in relay-assisted OFDMA networks using stochastic geometry. In OFDMA networks, users are assigned different number of resource elements (subcarriers) to meet their rate requirements. Therefore, the incoming users can be classified into different classes based on their subcarrier requirements. A very challenging problem in calculating the blocking probability is to obtain the distribution of the group size of the subcarriers that an arriving user needs to fulfill its data rate. In most of the existing work [36–38], this distribution is assumed to be known, usually assumed to be uniform. This may not be accurate, especially for large group sizes, which actually have very low request probability.

Here, we derive the distribution of user required subcarrier group size and then obtain the user blocking probability based on that. More specifically, first, we model the inter-cell interference from the neighboring cells at a typical node. Second, we derive the coverage probability (i.e., the probability of successful transmission) in the downlink transmissions, including both the direct and relay-based transmissions. Third, we classify the incoming users into different classes based on their subcarrier requirements. The system under consideration can be modeled using multi-dimensional Markov chains. Finally, we calculate the

blocking probability using the multi-dimensional loss model. It is shown that the blocking probability can be reduced by exploiting relay-assisted transmissions.

In Chapter 6, we summarize the conclusions and provide some outlines for future work.

Chapter 2

Full-band PUEA Detection and Mitigation

In this chapter, we consider full-band PUEA detection in cognitive radio networks operating in the white spaces of the DTV band. We propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve full-band identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. It should be noted that the AES-encrypted reference signal is also used for synchronization purposes at the authorized receivers, in the same way as the conventional synchronization sequence. We analyze the effectiveness of the proposed approach through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy under primary user emulation attacks. It should be emphasized that the proposed scheme requires no changes in hardware or system structure except of a plug-in AES chip. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing

lower band systems.

2.1 Introduction

Cognitive radio networks [2–4] have received considerable research attention recently because of their ability to alleviate the spectrum scarcity problem due to the rapid growth in the wireless communication devices. The basic idea of the CR networks is to allow the unlicensed users to share the frequency spectrum with the licensed users under the condition that they must not cause harmful interference to the primary users. The spectrum sharing is performed through spectrum sensing, where the CRs sense the spectrum to identify the unused bands (white spaces) for data transmission. If a primary signal is detected in the band that a CR operates in, then the CR must evacuate that band and operate in another white space. A serious security threat to the CR networks is known as primary user emulation attack [7–9], where the malicious users emulate the primary signal over the idle frequency band(s) such that the secondary users cannot use the corresponding white space(s).

Several approaches have been proposed to detect and defend against PUEA [12–15]. In [12], a localization-based transmitter verification scheme was proposed to detect PUEA. In [13] and [14], the authors proposed a RSS-based technique to defend against PUEA, where the attackers can be identified by comparing the received signal power of the primary user and the suspect attacker. A Wald’s sequential probability ratio test was presented to detect PUEA based on the received signal power in [15]. In these existing approaches, the detection of PUEA is mainly based on the power level and/or DOA of the received signal. The basic idea is that: given the locations of the primary TV stations, the secondary user can distinguish the actual primary signal from the malicious user’s signal by comparing the

power level and DOA of the received signal with that of the authorized primary user's signal. The major limitation with such approaches is that: they would fail when a malicious user is at a location where it produces the same DOA and comparable received power level as that of the actual primary transmitter.

In this chapter, we propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The proposed approach can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip, which has been commercialized and widely available [45–47]. It should be noted that the AES-encrypted reference signal is also used for synchronization purposes at the authorized receivers, in the same way as the conventional synchronization sequence.

The proposed scheme combats primary user emulation attacks, and enables more robust system operation and efficient spectrum sharing. The effectiveness of the proposed approach is demonstrated through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

2.2 The Proposed AES-assisted DTV Approach

In this section, we present the proposed AES-assisted DTV scheme for robust and reliable primary and secondary system operations. We first introduce the current terrestrial digital TV system. Then, we discuss the transmitter and the receiver designs of the proposed AES-assisted DTV scheme. Furthermore, we analyze the detection problem of the proposed approach using correlation-based methods. Finally, we discuss some possible concerns with the proposed AES-assisted DTV scheme, and provide some practical solutions.

2.2.1 A Brief Review of the Terrestrial DTV System

DTV is the advanced technology for enhancing the quality and performance of the analog television broadcasting. Several great benefits can be gained by the adoption of the DTV systems such as better picture and sound quality, less transmission power, and spectrum efficiency, where up to six channels can broadcast simultaneously over the same frequency band that is used by one analog channel [48]. Many countries have switched from the analog TV broadcasting to the digital TV by adopting one of the four widely used DTV broadcasting standards: Advanced Television System Committee (ATSC), Digital Video Broadcasting-Terrestrial (DVB-T), Terrestrial Integrated Services Digital Broadcasting (ISDB-T), and Digital Terrestrial Multimedia Broadcasting (DTMB). In the United States, the Federal Communications Commission (FCC) has adopted the ATSC standard as the official DTV terrestrial broadcasts. In 1996, the U.S. government allowed the TV companies to broadcast digital signals along with the analog broadcasting. By 2009, the FCC has announced that digital TV broadcasting is mandatory in the U.S.

In the ATSC standard, eight-level vestigial sideband (8-VSB) modulation is used for

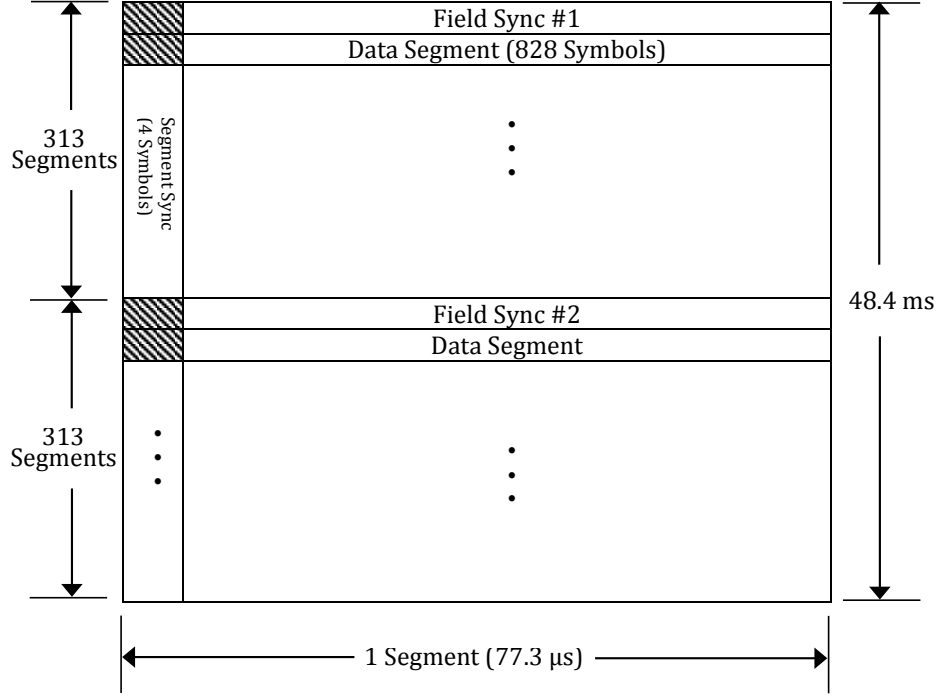


Figure 2.1: 8-VSB signal frame structure.

transmitting digital signals after they are partitioned into frames [49]. The frame structure of the 8-VSB signal is illustrated in Figure 2.1. Each frame has two data fields, and each data field has 313 data segments. The first data segment of each data field is used for frame synchronization and channel estimation at the receiver [49], [50]. The remaining 624 segments are used for data transmission. Each data segment contains 832 symbols, including 4 symbols used for segment synchronization. The segment synchronization bits are identical for all data segments. Each segment lasts $77.3 \mu s$, hence the overall time duration for one frame, which has 626 segments, is $626 * 77.3 \mu s = 48.4 ms$ [49].

2.2.2 AES-assisted DTV Transmitter

The DTV transmitter obtains the reference signal through two steps: first, generating a pseudo-random binary sequence (PRBS), then encrypting the sequence with the AES algo-

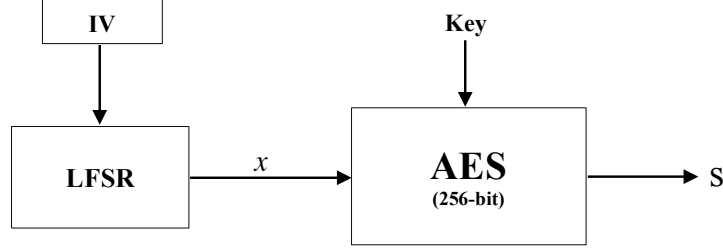


Figure 2.2: Generation of the reference signal.

rithm. More specifically, a pseudo-random binary sequence is first generated using a *Linear Feedback Shift Register* (LFSR)¹ with a secure *initialization vector* (IV). Maximum-length LFSR sequences can be achieved by tapping the LFSRs according to primitive polynomials. The maximum sequence length that can be achieved with a primitive polynomial of degree m is $2^m - 1$. Without loss of generality, a maximum-length sequence is assumed throughout this chapter.

Once the maximum-length sequence is generated, it is used as an input to the AES encryption algorithm, as illustrated in Figure 2.2. We propose that a 256-bit secret key be used for the AES encryption so that the maximum possible security is achieved. Security analysis will be provided in Section 2.4.

Denote the pseudo-random binary sequence by x , then the output of the AES algorithm is used as the reference signal, which can be expressed as:

$$\mathbf{s} = E(k, x), \quad (2.1)$$

where k is the encryption/decryption key, and $E(\cdot, \cdot)$ denotes the AES encryption operation. The transmitter then places the reference signal $\mathbf{s}$ in the sync bits of the DTV data segments.

The secret key can be generated and distributed to the DTV transmitter and receiver

¹Any other pseudo-random generators can be used as well.

from a trusted third party in addition to the DTV and the CR user. The third party serves as the authentication center for both the primary user and the CR user, and can carry out key distribution. To prevent impersonation attack, the key should be time varying [51].

2.2.3 AES-assisted DTV Receiver

The receiver regenerates the encrypted reference signal, with the secret key and IV that are shared between the transmitter and the receiver. A correlation detector is employed, where for primary user detection, the receiver evaluates the cross-correlation between the received signal $\mathbf{r}$ and the regenerated reference signal $\mathbf{s}$; for malicious user detection, the receiver further evaluates the auto-correlation of the received signal $\mathbf{r}$. The cross-correlation of two random variables $\mathbf{x}$ and $\mathbf{y}$ is defined as:

$$\mathbf{R}_{\mathbf{xy}} = \langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{E}\{\mathbf{xy}^*\}. \quad (2.2)$$

Under PUEA, the received signal can be modeled as:

$$\mathbf{r} = \alpha \mathbf{s} + \beta \mathbf{m} + \mathbf{n}, \quad (2.3)$$

where $\mathbf{s}$ is the reference signal, $\mathbf{m}$ is the malicious signal, $\mathbf{n}$ is the noise, α and β are binary indicators for the presence of the primary user and malicious user, respectively. More specifically, $\alpha = 0$ or 1 means the primary user is absent or present, respectively; and $\beta = 0$ or 1 means the malicious user is absent or present, respectively.

2.2.3.1 Detection of the Primary User

To detect the presence of the primary user, the receiver evaluates the cross-correlation between the received signal $\mathbf{r}$ and the reference signal $\mathbf{s}$, i.e.,

$$\begin{aligned}\mathbf{R}_{rs} &= \langle \mathbf{r}, \mathbf{s} \rangle = \alpha \langle \mathbf{s}, \mathbf{s} \rangle + \beta \langle \mathbf{m}, \mathbf{s} \rangle + \langle \mathbf{n}, \mathbf{s} \rangle \\ &= \alpha \sigma_s^2,\end{aligned}\tag{2.4}$$

where σ_s^2 is the primary user's signal power, and $\mathbf{s}$, $\mathbf{m}$, $\mathbf{n}$ are assumed to be independent with each other and are of zero mean. Depending on the value of α in (2.4), the receiver decides whether the primary user is present or absent.

Assuming that the signals are ergodic, then the ensemble average can be approximated by the time average. Here, we use the time average to estimate the cross-correlation. The estimated cross-correlation $\hat{\mathbf{R}}_{rs}$ is given by:

$$\hat{\mathbf{R}}_{rs} \triangleq \sum_{i=1}^N \frac{\mathbf{r}_i \cdot \mathbf{s}_i^*}{N},\tag{2.5}$$

where N is the reference signal's length, $\mathbf{s}_i$ and $\mathbf{r}_i$ denote the i th symbol of the reference and received signal, respectively.

To detect the presence of the primary user, the receiver compares the cross-correlation between the reference signal and the received signal to a predefined threshold λ . We have two cases:

1. If the cross-correlation is greater than or equal to λ , that is:

$$\hat{\mathbf{R}}_{rs} \geq \lambda,\tag{2.6}$$

then the receiver concludes that the primary user is present, i.e., $\alpha = 1$.

2. If the cross-correlation is less than λ , that is:

$$\hat{\mathbf{R}}_{rs} < \lambda, \quad (2.7)$$

then the receiver concludes that the primary user is absent, i.e., $\alpha = 0$.

This detection problem can be modeled as a binary hypothesis test problem with the following two hypotheses:

H_0 : the primary user is absent ($\hat{\mathbf{R}}_{rs} < \lambda$)

H_1 : the primary user is present ($\hat{\mathbf{R}}_{rs} \geq \lambda$)

As can be seen from (2.4), the cross-correlation between the reference signal and the received signal is equal to 0 or σ_s^2 , in case when the primary user is absent or present, respectively. Following the minimum distance rule, we choose $\lambda = \sigma_s^2/2$ as the threshold for primary user detection.

2.2.3.2 Detection of the Malicious User

For malicious user detection, the receiver further evaluates the auto-correlation of the received signal $\mathbf{r}$, i.e.,

$$\begin{aligned} \mathbf{R}_{rr} &= \langle \mathbf{r}, \mathbf{r} \rangle = \alpha^2 \langle \mathbf{s}, \mathbf{s} \rangle + \beta^2 \langle \mathbf{m}, \mathbf{m} \rangle + \langle \mathbf{n}, \mathbf{n} \rangle \\ &= \alpha^2 \sigma_s^2 + \beta^2 \sigma_m^2 + \sigma_n^2, \end{aligned} \quad (2.8)$$

where σ_m^2 and σ_n^2 denote the malicious user's signal power and the noise power, respectively.

Based on the value of α , β can be determined accordingly through (2.8). We have the

following cases:

$$\mathbf{R}_{rr} = \begin{cases} \sigma_s^2 + \sigma_m^2 + \sigma_n^2, & \alpha = 1, \beta = 1 \\ \sigma_s^2 + \sigma_n^2, & \alpha = 1, \beta = 0 \\ \sigma_m^2 + \sigma_n^2, & \alpha = 0, \beta = 1 \\ \sigma_n^2, & \alpha = 0, \beta = 0 \end{cases} \quad (2.9)$$

Assuming ergodic signals, we can use the time average to estimate the auto-correlation as follows:

$$\hat{\mathbf{R}}_{rr} \triangleq \sum_{i=1}^N \frac{\mathbf{r}_i \cdot \mathbf{r}_i^*}{N}. \quad (2.10)$$

Here, we can model the detection problem using four hypotheses, denoted by $H_{\alpha\beta}$, where $\alpha, \beta \in \{0, 1\}$:

H_{00} : the malicious user is absent given that $\alpha = 0$

H_{01} : the malicious user is present given that $\alpha = 0$

H_{10} : the malicious user is absent given that $\alpha = 1$

H_{11} : the malicious user is present given that $\alpha = 1$

In practical scenarios, however, we only have an estimated value of α , denoted as $\hat{\alpha}$. We estimate β after we obtain $\hat{\alpha}$. To do this, the receiver compares the auto-correlation of the received signal to two predefined thresholds λ_0 and λ_1 based on the previously detected $\hat{\alpha}$. More specifically, the receiver compares the auto-correlation of the received signal to λ_0

when $\hat{\alpha} = 0$, and to λ_1 when $\hat{\alpha} = 1$. That is:

$$\left\{ \begin{array}{l} \hat{H}_{00} : \hat{\mathbf{R}}_{rr} < \lambda_0, \text{ given that } \hat{\alpha} = 0, (\hat{\beta} = 0) \\ \hat{H}_{01} : \hat{\mathbf{R}}_{rr} \geq \lambda_0, \text{ given that } \hat{\alpha} = 0, (\hat{\beta} = 1) \\ \hat{H}_{10} : \hat{\mathbf{R}}_{rr} < \lambda_1, \text{ given that } \hat{\alpha} = 1, (\hat{\beta} = 0) \\ \hat{H}_{11} : \hat{\mathbf{R}}_{rr} \geq \lambda_1, \text{ given that } \hat{\alpha} = 1, (\hat{\beta} = 1) \end{array} \right. \quad (2.11)$$

The performance of the detection process for the primary user and malicious user is evaluated through the *false alarm rates* and the *miss detection probabilities*, as will be discussed in Section 2.3.

2.2.4 Further Discussions

The nature of the CR networks operation, which is based on the coexistence of primary users and secondary users, makes it vulnerable to hostile attacks such as PUEA. Several approaches have been proposed to detect PUEA, which can be categorized into two classes: (i) energy level and DOA based approaches [12–17], and (ii) user authentication approaches [52, 53]. In Chapter 1, we revisited some energy level based approaches, and discussed their major limitations. That is, they would fail when a malicious user is at a location where it produces the same DOA and/or comparable received power level as that of the actual primary transmitter, as shown in Figure 1.1.

The primary user and secondary user detection approaches proposed in this chapter can effectively overcome this drawback.

Some other user authentication based techniques have also been proposed such as in [52, 53]. In [52], a public key cryptography mechanism is used between primary users and

secondary users, such that the secondary users can identify the primary users accurately based on their public keys. A possible concern with this scheme is that public key based approaches generally have high computational complexity. In [53], a two-stage primary user authentication method was proposed: (i) generate the authentication tag for the primary user using a one-way hash chain, and (ii) embed the tag in the primary user's signal through constellation shift. Since the authentication tag is superimposed over the primary user transmitted symbols, it introduces some distortions to the primary user signals, and is sensitive to noise. Comparing with the existing user authentication based approaches, our approach is more efficient and has higher detection accuracy.

Although user authentication approaches are generally more reliable under various attack scenarios and generally have no assumptions on the primary user's transmission power or location, they can only be applied to detect the presence of the primary user and the malicious user but not the white spaces in the spectrum.

A more effective and practical solution for this problem would be to combine the proposed approach with the energy level detection approaches. In this case, both the primary user and malicious user, as well as the white spaces, can be accurately identified.

To completely resolve this problem, the primary user needs to use multi-carrier system such as OFDM, where each subcarrier operates in a particular sub-band in the allocated frequency spectrum. With this, it is possible to detect the primary user and malicious user in each sub-band using the proposed scheme, which we will consider in Chapter 3.

2.3 Analytical Evaluation of the Proposed AES-assisted DTV Approach

In this section, we analyze the detection performance of the the proposed AES-assisted DTV approach. First, we evaluate the system performance for primary user detection. Then, we analyze the effectiveness of the proposed AES-assisted DTV scheme in detecting malicious nodes.

2.3.1 Analytical Evaluation of Primary User Detection

We assume that the detection of the primary user has a false alarm rate P_f and a miss detection probability P_m , respectively. The false alarm rate P_f is the conditional probability that the primary user is considered to be present, when it is actually absent, i.e.,

$$P_f = Pr(H_1|H_0). \quad (2.12)$$

The miss detection probability P_m is the conditional probability that the primary is considered to be absent, when it is present, i.e.,

$$P_m = Pr(H_0|H_1). \quad (2.13)$$

As can be seen from (2.5), $\hat{\mathbf{R}}_{rs}$ is the averaged summation of N random variables. Since N is large, then based on the central limit theorem, $\hat{\mathbf{R}}_{rs}$ can be modeled as a Gaussian random variable. More specifically, under H_0 , $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_0, \sigma_0^2)$, and under H_1 , $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_1, \sigma_1^2)$, where μ_0 , σ_0 , and μ_1 , σ_1 can be derived as follows.

Under H_0 , the received signal is represented as $\mathbf{r}_i = \beta \mathbf{m}_i + \mathbf{n}_i$, where $\mathbf{m}_i$ is the i th malicious symbol, and $\mathbf{n}_i \sim \mathcal{N}(0, \sigma_n^2)$. Then, the mean μ_0 can be obtained as:

$$\begin{aligned}
\mu_0 &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\beta \mathbf{m}_i + \mathbf{n}_i) \mathbf{s}_i^* \right\} \\
&= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\beta \mathbf{m}_i \mathbf{s}_i^* + \mathbf{n}_i \mathbf{s}_i^*) \right\} \\
&= \frac{1}{N} \left[\sum_{i=1}^N (\beta \mathbb{E}\{\mathbf{m}_i\} \mathbb{E}\{\mathbf{s}_i^*\} + \mathbb{E}\{\mathbf{n}_i\} \mathbb{E}\{\mathbf{s}_i^*\}) \right] \\
&= 0.
\end{aligned} \tag{2.14}$$

The variance σ_0^2 can be obtained as:

$$\begin{aligned}
\sigma_0^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rs}|^2 \right\} - |\mu_0|^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N (\beta \mathbf{m}_i + \mathbf{n}_i) \mathbf{s}_i^* \sum_{j=1}^N (\beta \mathbf{m}_j + \mathbf{n}_j)^* \mathbf{s}_j \right\} \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N \sum_{j=1}^N (\beta^2 \mathbf{m}_i \mathbf{m}_j^* \mathbf{s}_j \mathbf{s}_i^* + \mathbf{n}_i \mathbf{n}_j^* \mathbf{s}_j \mathbf{s}_i^*) \right\} \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N (\beta^2 \mathbb{E}\{|\mathbf{m}_i|^2\} \mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\} \mathbb{E}\{|\mathbf{s}_i|^2\}) \right] \\
&= \frac{1}{N} \left[\beta^2 \sigma_s^2 \sigma_m^2 + \sigma_s^2 \sigma_n^2 \right].
\end{aligned} \tag{2.15}$$

Similarly, under H_1 , the received signal is represented as $\mathbf{r}_i = \mathbf{s}_i + \beta \mathbf{m}_i + \mathbf{n}_i$, and the

mean μ_1 can be obtained as follows:

$$\begin{aligned}
\mu_1 &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i + \beta \mathbf{m}_i + \mathbf{n}_i) \mathbf{s}_i^* \right\} \\
&= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i \mathbf{s}_i^* + \beta \mathbf{m}_i \mathbf{s}_i^* + \mathbf{n}_i \mathbf{s}_i^*) \right\} \\
&= \frac{1}{N} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^2\} + \beta \mathbb{E}\{\mathbf{m}_i\} \mathbb{E}\{\mathbf{s}_i^*\} + \mathbb{E}\{\mathbf{n}_i\} \mathbb{E}\{\mathbf{s}_i^*\}) \right] \\
&= \sigma_s^2,
\end{aligned} \tag{2.16}$$

and σ_1^2 can be obtained as:

$$\begin{aligned}
\sigma_1^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rs}|^2 \right\} - |\mu_1|^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i + \beta \mathbf{m}_i + \mathbf{n}_i) \mathbf{s}_i^* \sum_{j=1}^N (\mathbf{s}_j + \beta \mathbf{m}_j + \mathbf{n}_j)^* \mathbf{s}_j \right\} - (\sigma_s^2)^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N \sum_{j=1}^N (\mathbf{s}_i \mathbf{s}_i^* \mathbf{s}_j \mathbf{s}_j^* + \beta^2 \mathbf{m}_i \mathbf{m}_j^* \mathbf{s}_j \mathbf{s}_i^* + \mathbf{n}_i \mathbf{n}_j^* \mathbf{s}_j \mathbf{s}_i^*) \right\} - (\sigma_s^2)^2 \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^4\} + \beta^2 \mathbb{E}\{|\mathbf{m}_i|^2\} \mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\} \mathbb{E}\{|\mathbf{s}_i|^2\}) \right. \\
&\quad \left. + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \mathbb{E}\{|\mathbf{s}_i|^2\} \mathbb{E}\{|\mathbf{s}_j|^2\} \right] - (\sigma_s^2)^2 \\
&= \frac{1}{N^2} \left[N(\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2 \sigma_m^2 \sigma_s^2 + \sigma_n^2 \sigma_s^2) + N(N-1)(\sigma_s^2)^2 \right] - (\sigma_s^2)^2 \\
&= \frac{1}{N} \left[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2 \sigma_m^2 \sigma_s^2 + \sigma_n^2 \sigma_s^2 - (\sigma_s^2)^2 \right],
\end{aligned} \tag{2.17}$$

where we assume that $\mathbb{E}\{|\mathbf{s}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{s}}|^4\} \forall i$.

Following (2.12), the false alarm rate P_f can be obtained as:

$$\begin{aligned}
P_f &= P_r\{\hat{\mathbf{R}}_{rs} \geq \lambda | H_0\} \\
&= \frac{1}{\sqrt{2\pi}\sigma_0} \int_{\lambda}^{\infty} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}} dx \\
&= Q\left(\frac{\lambda-\mu_0}{\sigma_0}\right).
\end{aligned} \tag{2.18}$$

Similarly, following (2.13), the miss detection probability P_m can be obtained as:

$$\begin{aligned}
P_m &= P_r\{\hat{\mathbf{R}}_{rs} < \lambda | H_1\} \\
&= \frac{1}{\sqrt{2\pi}\sigma_1} \int_{-\infty}^{\lambda} e^{-\frac{(x-\mu_1)^2}{2\sigma_1^2}} dx \\
&= 1 - Q\left(\frac{\lambda-\mu_1}{\sigma_1}\right).
\end{aligned} \tag{2.19}$$

Remark 2.1 As will be shown later in Section 2.5, when $\lambda = \sigma_s^2/2$, both P_f and P_m are essentially zero, and independent of the SNR values. The underlying argument is that the detection of the primary user is based on $\mathbf{R}_{rs} = \alpha\sigma_s^2$ (see (2.4)), which is independent of both σ_m^2 and σ_n^2 .

2.3.2 Analytical Evaluation of Malicious User Detection

2.3.2.1 False Alarm Rate and Miss Detection Probability for Malicious User Detection

Define $\tilde{P}_{f,0}$ and $\tilde{P}_{f,1}$ as the false alarm rate when $\hat{\alpha} = 0$ or $\hat{\alpha} = 1$, respectively,

$$\tilde{P}_{f,0} = Pr(\hat{H}_{01}|\hat{H}_{00}), \quad (2.20)$$

$$\tilde{P}_{f,1} = Pr(\hat{H}_{11}|\hat{H}_{10}). \quad (2.21)$$

The overall false alarm rate is given by:

$$\tilde{P}_f = \hat{P}_0 \tilde{P}_{f,0} + (1 - \hat{P}_0) \tilde{P}_{f,1}, \quad (2.22)$$

where $\hat{P}_0$ is the probability that $\hat{\alpha} = 0$, i.e.,

$$\hat{P}_0 = (1 - P_f)P(\alpha = 0) + P_m P(\alpha = 1). \quad (2.23)$$

As will be shown in Section 2.4, with the avalanche effect of the AES algorithm, the cross-correlation between the reference signal and the received signal is always around σ_s^2 or 0, depending on whether the primary user is present or absent, respectively. That is, P_f and P_m are negligible, as will be demonstrated later in Section 2.5. Therefore, in the following, we assume that $\hat{\alpha} = \alpha$, and we do not distinguish between $\hat{H}_{\hat{\alpha}\beta}$ and $H_{\alpha\beta}$; it follows that $\hat{P}_0 = P_0 = P(\alpha = 0)$. Hence, the overall false alarm rate is given by:

$$\tilde{P}_f = P_0 \tilde{P}_{f,0} + (1 - P_0) \tilde{P}_{f,1}. \quad (2.24)$$

Similarly, the miss detection probabilities can be defined as $\tilde{P}_{m,0}$ and $\tilde{P}_{m,1}$, when the primary user is absent and present, respectively, i.e.,

$$\tilde{P}_{m,0} = Pr(H_{00}|H_{01}). \quad (2.25)$$

$$\tilde{P}_{m,1} = Pr(H_{10}|H_{11}). \quad (2.26)$$

The overall malicious node miss detection probability is defined as:

$$\tilde{P}_m = P_0\tilde{P}_{m,0} + (1 - P_0)\tilde{P}_{m,1}. \quad (2.27)$$

Since $\hat{\mathbf{R}}_{rr}$ is the averaged summation of a large number of random variables, then based on the central limit theorem, $\hat{\mathbf{R}}_{rr}$ can be modeled as a Gaussian random variable. Hence, we have:

$$\left\{ \begin{array}{ll} \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{00}, \sigma_{00}^2), & H_{00} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{01}, \sigma_{01}^2), & H_{01} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{10}, \sigma_{10}^2), & H_{10} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{11}, \sigma_{11}^2), & H_{11} \end{array} \right. \quad (2.28)$$

where μ_{00} , σ_{00} , μ_{01} , σ_{01} , μ_{10} , σ_{10} , and μ_{11} , σ_{11} can be derived as follows.

Under H_{00} , both the primary user and malicious user are absent, resulting in $\mathbf{r}_i = \mathbf{n}_i$. It

follows that:

$$\begin{aligned}
\mu_{00} &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N \mathbf{n}_i \mathbf{n}_i^* \right\} \\
&= \frac{1}{N} \sum_{i=1}^N \mathbb{E}\{|\mathbf{n}_i|^2\} \\
&= \sigma_n^2,
\end{aligned} \tag{2.29}$$

and σ_{00}^2 can be obtained as:

$$\begin{aligned}
\sigma_{00}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{00}|^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N \sum_{j=1}^N \mathbf{n}_i \mathbf{n}_i^* \mathbf{n}_j^* \mathbf{n}_j \right\} - (\sigma_n^2)^2 \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N \mathbb{E}\{|\mathbf{n}_i|^4\} + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \mathbb{E}\{|\mathbf{n}_i|^2\} \mathbb{E}\{|\mathbf{n}_j|^2\} \right] - (\sigma_n^2)^2 \\
&= \frac{1}{N^2} \left[N \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + N(N-1)(\sigma_n^2)^2 \right] - (\sigma_n^2)^2 \\
&= \frac{1}{N} \left[\mathbb{E}\{|\tilde{\mathbf{n}}|^4\} - (\sigma_n^2)^2 \right],
\end{aligned} \tag{2.30}$$

where we assume that $\mathbb{E}\{|\mathbf{n}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} \forall i$. Similarly, under H_{01} , the received signal is

represented as $\mathbf{r}_i = \mathbf{m}_i + \mathbf{n}_i$, and the mean μ_{01} can be obtained as follows:

$$\begin{aligned}
\mu_{01} &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{m}_i + \mathbf{n}_i)(\mathbf{m}_i + \mathbf{n}_i)^* \right\} \\
&= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{m}_i \mathbf{m}_i^* + \mathbf{n}_i \mathbf{n}_i^*) \right\} \\
&= \frac{1}{N} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{m}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}) \right] \\
&= \sigma_m^2 + \sigma_n^2.
\end{aligned} \tag{2.31}$$

The variance σ_{01}^2 can be obtained as:

$$\begin{aligned}
\sigma_{01}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{01}|^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{m}_i + \mathbf{n}_i)(\mathbf{m}_i + \mathbf{n}_i)^* \sum_{j=1}^N (\mathbf{m}_j + \mathbf{n}_j)^*(\mathbf{m}_j + \mathbf{n}_j) \right\} - (\sigma_m^2 + \sigma_n^2)^2 \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{m}_i|^4\} + \mathbb{E}\{|\mathbf{n}_i|^4\} + 4\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{2\text{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\}) \right. \\
&\quad \left. + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + 2\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} \right] - (\sigma_m^2 + \sigma_n^2)^2 \\
&= \frac{1}{N} \left[\mathbb{E}\{|\tilde{\mathbf{m}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_m^2\sigma_n^2 - (\sigma_m^2)^2 - (\sigma_n^2)^2 \right],
\end{aligned} \tag{2.32}$$

where we assume that $\mathbb{E}\{|\mathbf{m}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{m}}|^4\}$ and $\mathbb{E}\{2\text{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\} = \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} \forall i$.

Under H_{10} , the received signal is expressed as $\mathbf{r}_i = \mathbf{s}_i + \mathbf{n}_i$, and the mean μ_{10} can be

obtained as follows:

$$\begin{aligned}
\mu_{10} &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i + \mathbf{n}_i)(\mathbf{s}_i + \mathbf{n}_i)^* \right\} \\
&= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i \mathbf{s}_i^* + \mathbf{n}_i \mathbf{n}_i^*) \right\} \\
&= \frac{1}{N} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}) \right] \\
&= \sigma_s^2 + \sigma_n^2,
\end{aligned} \tag{2.33}$$

and σ_{10}^2 can be obtained as:

$$\begin{aligned}
\sigma_{10}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{10}|^2 \\
&= \frac{1}{N^2} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i + \mathbf{n}_i)(\mathbf{s}_i + \mathbf{n}_i)^* \sum_{j=1}^N (\mathbf{s}_j + \mathbf{n}_j)^*(\mathbf{s}_j + \mathbf{n}_j) \right\} - (\sigma_s^2 + \sigma_n^2)^2 \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^4\} + \mathbb{E}\{|\mathbf{n}_i|^4\} + 4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{2\text{Re}\{(\mathbf{s}_i)^2(\mathbf{n}_i^*)^2\}\}) \right. \\
&\quad \left. + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{s}_j|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + 2\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} \right] - (\sigma_s^2 + \sigma_n^2)^2 \\
&= \frac{1}{N} \left[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_s^2\sigma_n^2 - (\sigma_s^2)^2 - (\sigma_n^2)^2 \right].
\end{aligned} \tag{2.34}$$

Similarly, under H_{11} , the received signal is represented as $\mathbf{r}_i = \mathbf{s}_i + \mathbf{m}_i + \mathbf{n}_i$, and the mean

μ_{11} can be obtained as follows:

$$\begin{aligned}
\mu_{11} &= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i + \mathbf{m}_i + \mathbf{n}_i)(\mathbf{s}_i + \mathbf{m}_i + \mathbf{n}_i)^* \right\} \\
&= \frac{1}{N} \mathbb{E} \left\{ \sum_{i=1}^N (\mathbf{s}_i \mathbf{s}_i^* + \mathbf{m}_i \mathbf{m}_i^* + \mathbf{n}_i \mathbf{n}_i^*) \right\} \\
&= \frac{1}{N} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{m}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}) \right] \\
&= \sigma_s^2 + \sigma_m^2 + \sigma_n^2.
\end{aligned} \tag{2.35}$$

The variance σ_{11}^2 can be obtained as:

$$\begin{aligned}
\sigma_{11}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{11}|^2 \\
&= \frac{1}{N^2} \left[\sum_{i=1}^N (\mathbb{E}\{|\mathbf{s}_i|^4\} + \mathbb{E}\{|\mathbf{m}_i|^4\} + \mathbb{E}\{|\mathbf{n}_i|^4\} + 4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{m}_i|^2\} + 4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} \right. \\
&\quad + 4\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{2\text{Re}\{(\mathbf{s}_i)^2(\mathbf{m}_i^*)^2\}\} + \mathbb{E}\{2\text{Re}\{(\mathbf{s}_i)^2(\mathbf{n}_i^*)^2\}\} \\
&\quad + \mathbb{E}\{2\text{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\}) + \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{s}_j|^2\} + \mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\} \\
&\quad + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\} + \mathbb{E}\{|\mathbf{s}_j|^2\}\mathbb{E}\{|\mathbf{m}_i|^2\} + \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} \\
&\quad + \mathbb{E}\{|\mathbf{s}_j|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + \mathbb{E}\{|\mathbf{m}_j|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} \left. \right] - |\mu_{11}|^2 \\
&= \frac{1}{N} \left[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{m}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{m}}^*)^2\}\} + \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\} \right. \\
&\quad + \mathbb{E}\{2\text{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_s^2\sigma_m^2 + 2\sigma_s^2\sigma_n^2 + 2\sigma_m^2\sigma_n^2 - (\sigma_s^2)^2 - (\sigma_m^2)^2 - (\sigma_n^2)^2 \left. \right]. \tag{2.36}
\end{aligned}$$

Following the discussions above, we have:

$$\begin{aligned}\tilde{P}_{f,0} &= P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_0 | H_{00}\} \\ &= Q\left(\frac{\lambda_0 - \mu_{00}}{\sigma_{00}}\right),\end{aligned}\tag{2.37}$$

and

$$\begin{aligned}\tilde{P}_{f,1} &= P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_1 | H_{10}\} \\ &= Q\left(\frac{\lambda_1 - \mu_{10}}{\sigma_{10}}\right).\end{aligned}\tag{2.38}$$

Similarly, we have:

$$\begin{aligned}\tilde{P}_{m,0} &= P_r\{\hat{\mathbf{R}}_{rr} < \lambda_0 | H_{01}\} \\ &= 1 - Q\left(\frac{\lambda_0 - \mu_{01}}{\sigma_{01}}\right),\end{aligned}\tag{2.39}$$

and

$$\begin{aligned}\tilde{P}_{m,1} &= P_r\{\hat{\mathbf{R}}_{rr} < \lambda_1 | H_{11}\} \\ &= 1 - Q\left(\frac{\lambda_1 - \mu_{11}}{\sigma_{11}}\right).\end{aligned}\tag{2.40}$$

The overall false alarm rate $\tilde{P}_f$ and miss detection probability $\tilde{P}_m$ can be calculated following (2.24), (2.27). That is:

$$\tilde{P}_f = P_0 Q\left(\frac{\lambda_0 - \mu_{00}}{\sigma_{00}}\right) + (1 - P_0) Q\left(\frac{\lambda_1 - \mu_{10}}{\sigma_{10}}\right),\tag{2.41}$$

and

$$\tilde{P}_m = 1 - P_0 Q\left(\frac{\lambda_0 - \mu_{01}}{\sigma_{01}}\right) + (P_0 - 1) Q\left(\frac{\lambda_1 - \mu_{11}}{\sigma_{11}}\right). \quad (2.42)$$

2.3.2.2 The Optimal Thresholds for Malicious User Detection

In this subsection, we seek to obtain the optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$ that minimize the overall miss detection probability of the malicious node detection problem, while maintaining the false alarm rates below a certain threshold δ . This problem can be formulated as follows:

$$\begin{aligned} & \min \tilde{P}_m \\ & \text{subject to } \tilde{P}_{f,0} \leq \delta, \text{ and } \tilde{P}_{f,1} \leq \delta. \end{aligned} \quad (2.43)$$

It is noted that the problem formulation above is equivalent to:

$$\begin{aligned} & \min \tilde{P}_{m,0} \\ & \text{subject to } \tilde{P}_{f,0} \leq \delta, \end{aligned} \quad (2.44)$$

and

$$\begin{aligned} & \min \tilde{P}_{m,1} \\ & \text{subject to } \tilde{P}_{f,1} \leq \delta. \end{aligned} \quad (2.45)$$

Thus, we request:

$$\tilde{P}_{f,0} = Q\left(\frac{\lambda_0 - \mu_{00}}{\sigma_{00}}\right) \leq \delta, \quad (2.46)$$

and

$$\tilde{P}_{f,1} = Q\left(\frac{\lambda_1 - \mu_{10}}{\sigma_{10}}\right) \leq \delta, \quad (2.47)$$

which implies that:

$$\lambda_0 \geq \sigma_{00}Q^{-1}(\delta) + \mu_{00}, \quad (2.48)$$

and

$$\lambda_1 \geq \sigma_{10}Q^{-1}(\delta) + \mu_{10}. \quad (2.49)$$

Note that in order to minimize the overall miss detection probability $\tilde{P}_m$, λ_0 in (2.48), and λ_1 in (2.49) should be as small as possible. Hence, we set the thresholds to:

$$\lambda_{0,opt} = \sigma_{00}Q^{-1}(\delta) + \mu_{00}, \quad (2.50)$$

and

$$\lambda_{1,opt} = \sigma_{10}Q^{-1}(\delta) + \mu_{10}. \quad (2.51)$$

By substituting $\lambda_{0,opt}$ and $\lambda_{1,opt}$ in (2.42), we obtain the overall miss detection probability as:

$$\begin{aligned} \tilde{P}_m &= 1 - P_0 Q\left(\frac{\sigma_{00}Q^{-1}(\delta) + \mu_{00} - \mu_{01}}{\sigma_{01}}\right) \\ &\quad + (P_0 - 1) Q\left(\frac{\sigma_{10}Q^{-1}(\delta) + \mu_{10} - \mu_{11}}{\sigma_{11}}\right). \end{aligned} \quad (2.52)$$

Proposition 2.1 For malicious user detection, to minimize the overall miss detection probability $\tilde{P}_m$ subject to the false alarm rate constraints $\tilde{P}_{f,0} \leq \delta$ and $\tilde{P}_{f,1} \leq \delta$, which also ensures that $\tilde{P}_f \leq \delta$, we need to choose $\lambda_{0,opt} = \sigma_{00}Q^{-1}(\delta) + \mu_{00}$, and $\lambda_{1,opt} = \sigma_{10}Q^{-1}(\delta) + \mu_{10}$.

2.4 Security and Feasibility of the Proposed AES-assisted DTV Approach

This section is devoted to discuss the security and feasibility of the proposed AES-assisted DTV scheme. We begin by providing a general overview of the AES algorithm. We then discuss and investigate the security and practicability of the AES-assisted DTV scheme.

2.4.1 A Brief Overview of the AES Algorithm

Advanced Encryption Standard is the current National Institute of Standards and Technology (NIST) data encryption standard, it has been adopted by the U.S. Department of Commerce in 2001 after going through a long evaluation period. It has been chosen because of its security (resistance against all known attacks), simplicity, availability in different key sizes, and efficiency in hardware and software implementations [54]. AES is a symmetric-key cipher, in which a *single key* is used for both encryption and decryption. The key is shared between the communication parties, and kept private. Figure 2.3 shows the general structure of the AES encryption algorithm. It mainly consists of four stages that are applied to the input data, which is arranged in 4×4 array of bytes. The four stages are repeated, and the number of repetitions depends on the key length (128, 192, or 256 bits). The four stages of AES are:

1. SubBytes Stage

In this stage, each byte in the 4×4 array is simply mapped to another byte based on a lookup table called the S-box. The security reason for creating the S-box is to thwart all the known cryptanalytic attacks [51].

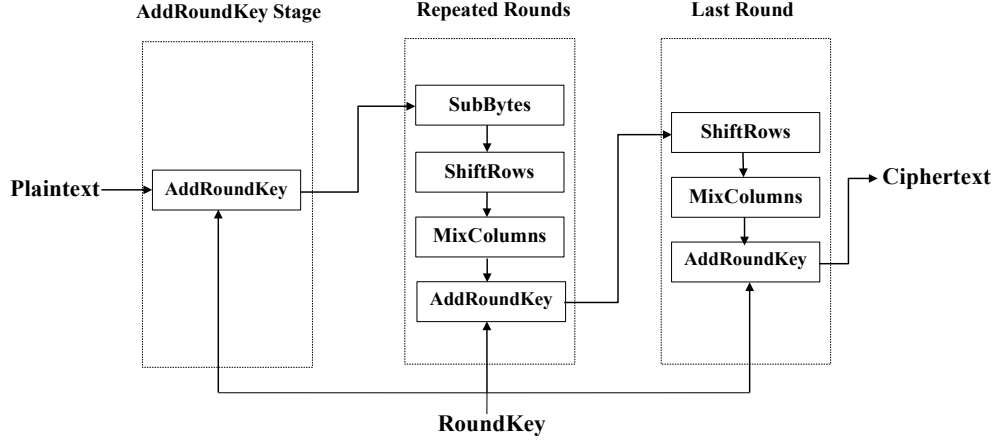


Figure 2.3: AES encryption.

2. ShiftRows Stage

Here, each row in the 4×4 data array, except the first row, is shifted to the left by a number of bytes. In particular, the second row is shifted to the left by 1 byte, while the third and fourth are shifted by 2 bytes and 3 bytes, respectively. The ShiftRows stage provides diffusion in the cipher so that the output of the AES algorithm (i.e. the ciphertext) carries no statistical relationship to the input (i.e. the plaintext) [51].

3. MixColumns

In this stage, each byte in a column is replaced by a combination of the four bytes within the same column. The MixColumns operation also provides diffusion property [51].

4. AddRoundKey

In this stage, each byte in the array is added to the RoundKey array using bit-wise XOR function. The AddRoundKey stage is used to impact every bit within the array [51].

2.4.2 Security of the AES-assisted DTV

As stated earlier, AES has been proven to be secure under all known attacks, in the sense that it is computationally infeasible to break AES in real time. In our case, this means that it is computationally infeasible for malicious users to regenerate the reference signal. Moreover, the AES algorithm has a very important security feature known as the *avalanche effect*, which means that a small change in the plaintext or the key yields a large change in the ciphertext [51]. Actually, even if one bit is changed in the plaintext, the ciphertext will be changed by approximately 50%. Therefore, it is impossible to recover the plaintext given the ciphertext only.

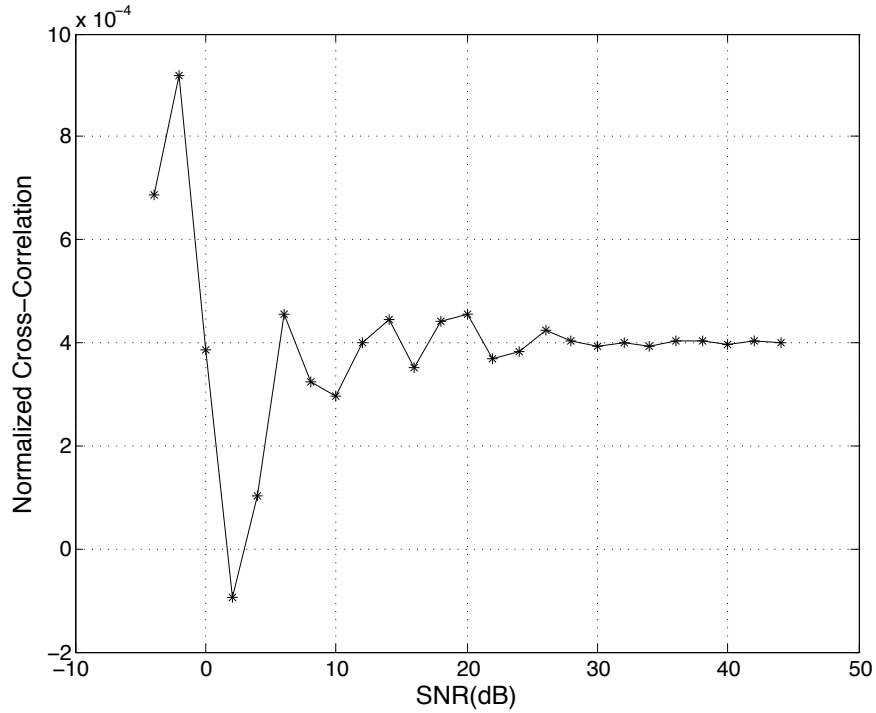


Figure 2.4: Normalized cross-correlation between the reference signal and noisy versions of malicious user's signal. Note that the cross-correlation values are in the order of 10^{-4} , which is close to 0.

To illustrate the security of the AES-assisted DTV based on the avalanche effect, the cross-correlation between the reference signal and malicious signal under different SNR values

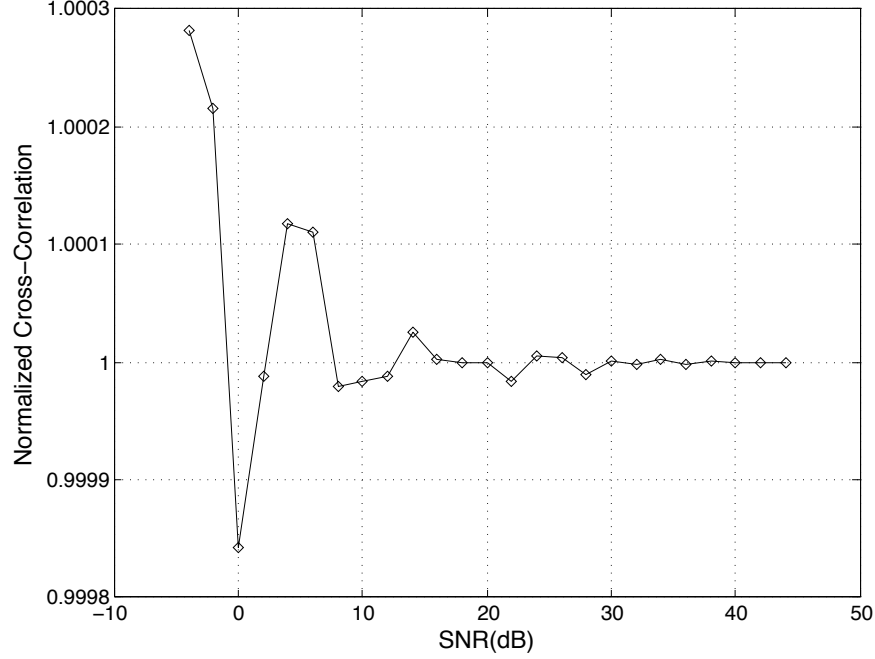


Figure 2.5: Normalized cross-correlation between the reference signal and noisy versions of the primary user's signal. Here, $\sigma_s^2 = 1$.

is obtained, as shown in Figure 2.4. It can be seen that the cross-correlation values are around μ_0 in (2.14), which implies that the malicious signal and the reference signal are uncorrelated. On the other hand, the cross-correlation between the reference signal and noisy versions of the primary signal is shown to be very high (around μ_1 in (2.16)), under all SNR values, as depicted in Figure 2.5. It should be appreciated that in the DTV system, the minimum SNR is 28.3 dB [49].

These results show that the AES-assisted DTV scheme is secure under PUEA, as malicious users cannot regenerate the reference signal in real time.

2.4.3 Feasibility

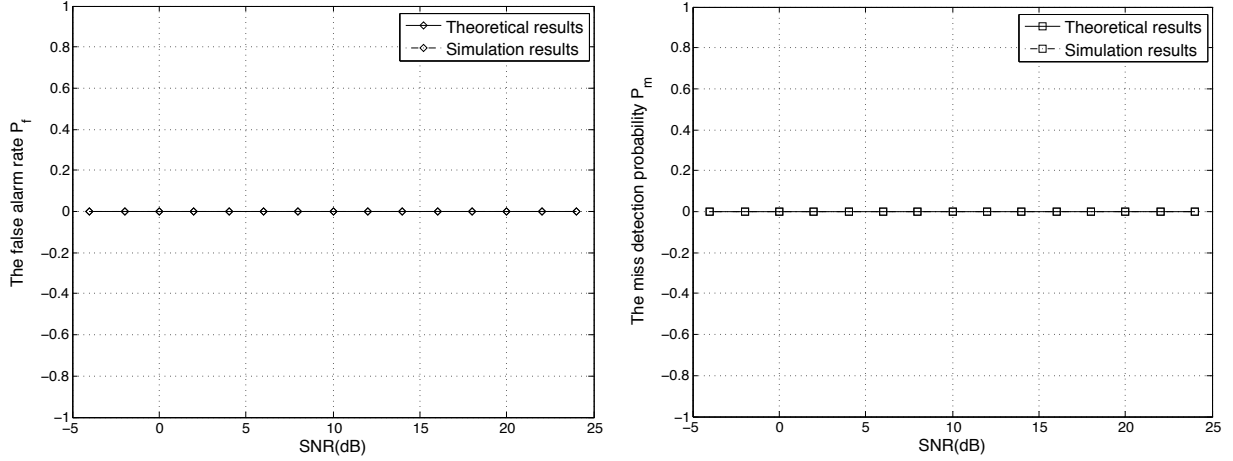
Here, we show that it is practical to generate the required sync bits within the frame time duration shown in Figure 2.1.

The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data [55]. High-throughput (3.84 Gbps and higher) AES chips can be found in [46, 47]. In [56], an experiment was performed to measure the AES algorithm performance, where several file sizes from 100KB to 50MB were encrypted using a laptop with 2.99 GHz CPU and 2 GB RAM. Based on the results of the experiment, when the AES operates in the cipher feedback (CFB) mode, 554bytes can be encrypted using 256-bit AES algorithm in $77.3 \mu s$. Therefore, even the 2.99GHz CPU can generate the required AES reference signal within the frame time duration. Note that the TV stations generally have powerful processing units, hence it is not a problem to generate the required secure sync bits within the frame duration. With 3.84 Gbps encryption speed, for example, 39KB can be encrypted in $77.3 \mu s$, which is more than adequate.

2.5 Simulation Results

In this section, we demonstrate the effectiveness of the AES-assisted DTV scheme through simulation examples. First, we illustrate the impact of the noise level on the optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$. Then, we evaluate the false alarm rates and miss detection probabilities for both primary user and malicious user detection. In the simulations, we assume that $\mathbf{s}_i$, $\mathbf{m}_i$, and $\mathbf{n}_i$ are i.i.d. sequences, and are of zero mean. We further assume that the primary user is absent with probability $P_0 = 0.25$. The primary user's signal power is assumed to be normalized to $\sigma_s^2 = 1$. For malicious user detection, we set the false alarm constraint $\delta = 10^{-3}$.

Example 1: False alarm rate and miss detection probability for primary user detection. Using $\lambda = \sigma_s^2/2$, we obtain the false alarm rate and miss detection probability



(a) The false alarm rate P_f , the two curves are identical. (b) The miss detection probability P_m , the two curves are identical.

Figure 2.6: Example 1: The false alarm rate and miss detection probability for primary user detection.

numerically and compare them with the theoretical results. The false alarm rate is illustrated in Figure 2.6(a). It is noted that the theoretical false alarm rate P_f in (2.18) depends on β , since σ_0^2 is a function of β . However, based on (2.15) and the avalanche effect of the AES algorithm, this dependency becomes negligible when N is large. This can be seen from Figure 2.6(a) as the theoretical calculations match perfectly with the numerical simulations.

The probability of miss detection is shown in Figure 2.6(b). It also can be seen that the theoretical calculations and numerical simulations are matched perfectly. It is clear that the proposed AES-assisted DTV approach achieves *zero* false alarm rate and miss detection probability under a large range of SNR values.

Example 2: The optimal thresholds for malicious user detection. In this example, we demonstrate the optimal thresholds that minimize the miss detection probabilities under a predefined constraint on the false alarm rates for malicious user detection.

Figure 2.7 shows the two optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$ versus SNR for $\delta = 10^{-3}$. We observe that the two curves decrease as the SNR increases, which can be verified with

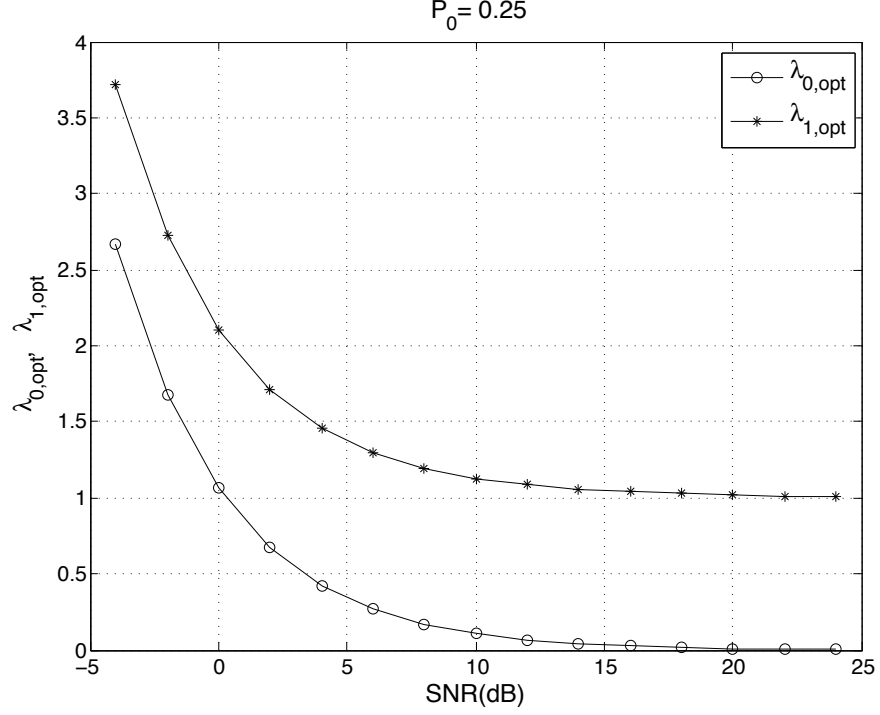


Figure 2.7: Example 2: The optimal thresholds for malicious user detection for $\delta = 10^{-3}$. Here, $P_0 = 0.25$.

(2.50) and (2.51).

Example 3: False alarm rate and miss detection probability for malicious user detection. In this example, we obtain the overall false alarm rate and miss detection probability numerically and compare them with the theoretical results. Figure 2.8(a) shows the overall false alarm rate $\tilde{P}_f$ for $\delta = 10^{-3}$. It is noted that the theoretical calculations and numerical simulations are almost equal, and the predefined false alarm constraint δ is satisfied.

The overall miss detection probability $\tilde{P}_m$ is illustrated in Figure 2.8(b). It is shown that the proposed approach achieves *zero* overall miss detection probability under a large range of SNR values.

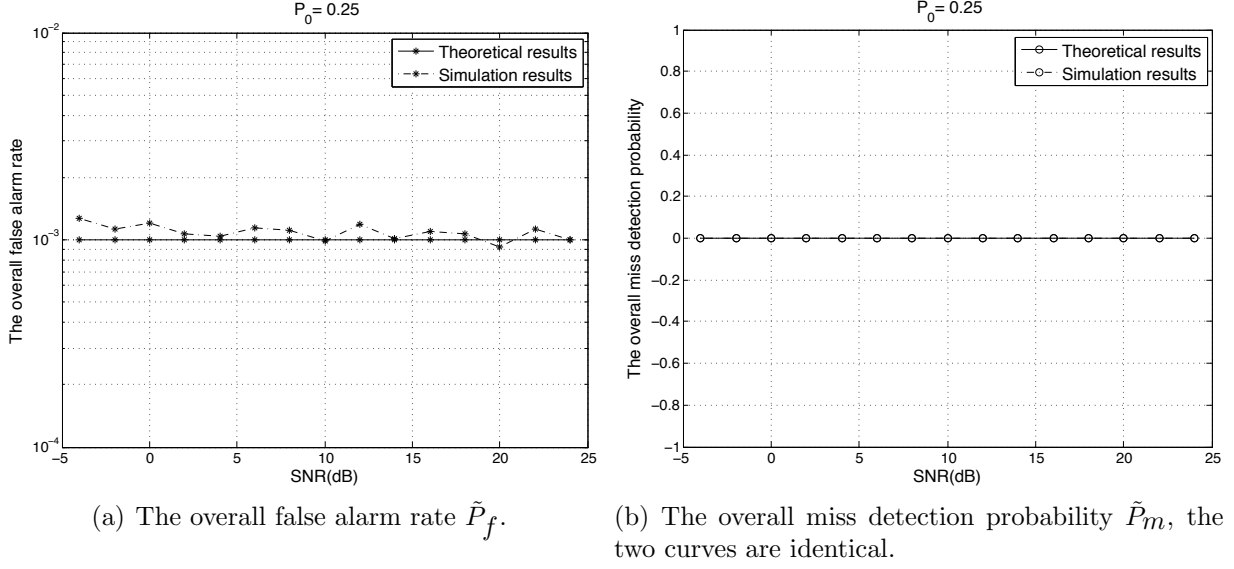


Figure 2.8: Example 3: The overall false alarm rate and the overall miss detection probability for malicious user detection. Here, $P_0 = 0.25$ and $\delta = 10^{-3}$.

2.6 Summary

In this chapter, first, we presented the proposed AES-assisted DTV scheme for robust primary and secondary system operations under primary user emulation attacks. In the proposed scheme, an AES-encrypted reference signal is generated at the DTV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate full-band identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. Second, we analyzed the detection performance of the proposed AES-assisted DTV approach. Third, we discussed the security and feasibility of the proposed AES-assisted DTV approach. Through simulation examples, it was shown that the proposed AES-assisted DTV scheme can achieve very low false alarm rates and miss detection probabilities when detecting the

primary user and malicious user. That is, with the proposed AES-assisted DTV scheme, primary user emulation attacks can be effectively combated. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

Chapter 3

Sub-band PUEA Detection and Mitigation

In this chapter, we consider sub-band PUEA detection in the OFDM-based cognitive radio networks. The DTV model adopted is the second generation terrestrial digital television standard (DVB-T2). We propose an efficient AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm for accurate sub-band primary user and malicious user detection. With the proposed scheme, we can detect PUEA accurately over all subcarriers or subbands where the P2 symbols present. Numerical results show that with the AES-based DTV scheme, both the primary user and malicious user can be detected accurately under primary user emulation attacks. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

3.1 Introduction

Cognitive radio networking [2–4] is a promising technique to solve the spectrum scarcity problem and has attracted a lot of research interest in recent years. The basic idea of the CR networks is to identify the unoccupied licensed spectrum for secondary users, without

interfering with the primary user. A serious security threat to the CR networks is referred to as primary user emulation attack [7–9], where a malicious user emulates the signal characteristics of the primary user, thereby causing the SUs to erroneously identify the attacker as the primary user. The QoS for the secondary users can be severely degraded by the presence of PUEA in CR networks [57].

To detect and defend against PUEA, several schemes have been proposed in literature. In [12], a localization-based transmitter verification scheme was proposed. In [13] and [14], the authors proposed a RSS-based based technique to defend against PUEA, where the attackers can be identified by comparing the received signal power levels of the primary user and the suspected attacker. In [18], the authors proposed compressive sensing based approach to distinguish whether the signals transmitted are from the primary users or malicious users. In mobile CR networks, the authors in [19] proposed a method to detect PUEA on mobile primary users by exploiting the correlations between radio frequency signals and acoustic information to verify the existence of malicious wireless microphones. Recently, in [20], location reliability and malicious intention were explored to detect primary user and malicious user in mobile CR networks. In most of these approaches, the detection of PUEA is based on the assumption that: when the signal is from the primary user, the received signal strength at the secondary users is higher than that from a malicious user. As a result, the secondary user can distinguish the primary signal from the malicious signal by examining the power level and the direction of arrival of the received signal. The major limitation with this kind of approaches is that: they may fail when a malicious user is at a location where it produces the same DOA and comparable RSS as that of the actual primary transmitter.

In this chapter, motivated by the prevalence of the OFDM-based DTV standard, we consider sub-band malicious user detection in OFDM-based CR network under PUEA. Here,

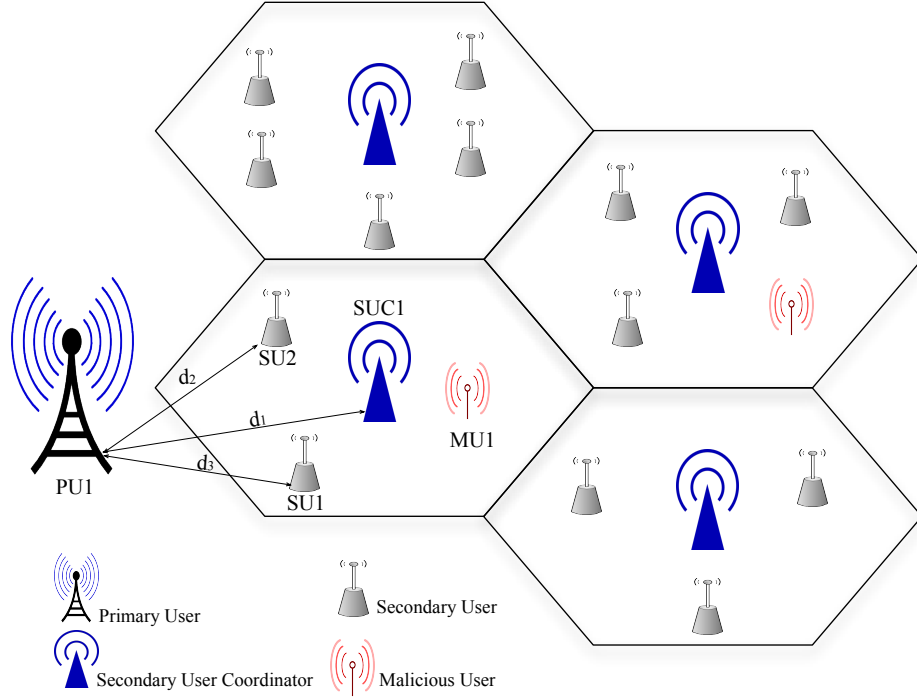


Figure 3.1: The proposed cognitive radio network architecture.

the CR network consists of primary users, secondary user coordinators (SUCs), secondary users, and malicious users. The SUCs are designed to perform spectrum sensing and PUEA detection, and then coordinate the SUs for collision-free transmission over the white spaces. We propose a robust and efficient AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm, and the resulted sequence is exploited for accurate detection of the authorized primary user and the malicious user.

3.2 System Model

We consider an OFDM-based cognitive radio network under PUEA, as shown in Figure 3.1. In this model, we assume that the network is divided into hexagonally shaped areas (cells), each of which consists of a secondary user coordinator located at the center of the

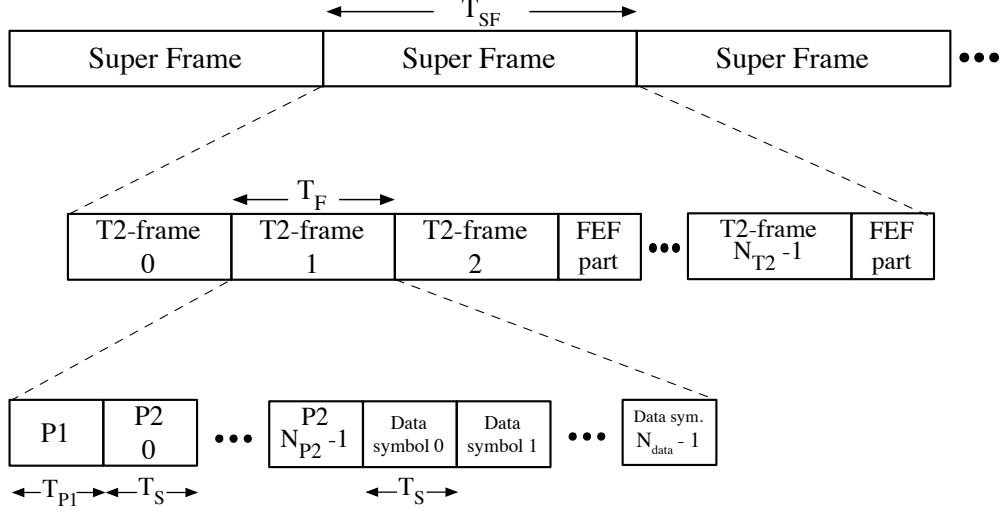


Figure 3.2: The DVB-T2 frame structure.

cell, a set of secondary users, and some malicious users. Furthermore, the network includes powerful primary users (DTV transmitters) distributed uniformly throughout the network. The primary users are assumed to be using OFDM scheme for data transmission, which is the case in most of the existing or future DTV systems [58]. Here, we consider the second generation terrestrial digital television standard (DVB-T2) system as an example due to its prevalence and efficiency.

The frame structure of the DVB-T2 standard is shown in Figure 3.2 [59]. It consists of super frames, which are partitioned into T2-frames and supplementary future extension frames (FEF). Each T2-frame has three kinds of OFDM symbols: P1 preamble symbol used for characterizing the basic transmission parameters, P2 preamble symbol(s) used for carrying signaling information, and data symbols for payload. Furthermore, each symbol has different pilot symbols used for frame synchronization, frequency synchronization, and channel estimation [59]. Here, we propose to use the P2 pilots for the detection of the primary user and malicious user for two reasons. First, they are the only pilots whose frequency locations are independent of the FFT size (1K, 2K, 4K, 8K, 16K, 32K) and the

operational modes (SISO, MIMO) except in 32K SISO mode. Second, they have the largest number among all the pilot symbols, which can be exploited to achieve effective detection of the authorized primary user and the malicious user.

We would like to point out that with the OFDM structure used in DVB-T2, the proposed scheme can accurately detect the presence of the malicious user over all the subcarriers where the P2 pilots present. Note that the P2 pilots present on subcarriers whose indexes are integer multiples of 3, which implies that we can detect the presence of the malicious users over each 3-subcarrier sub-band. However, the proposed approach can be used to detect PUEA over each single subcarrier if we can spread the preamble P2 symbols in the DVB-T2 standard to cover every subcarrier, instead of putting multiple P2 symbols over each selected subcarrier.

The deployment of the secondary user coordinators in the proposed network architecture can provide efficient spectrum sharing between the primary user and the secondary users, and also among the secondary users. More specifically, the secondary user coordinator can detect idle spectral spaces in the frequency spectrum, and assign these spaces to the secondary users within the cell. With a secure reference signal shared between the primary user and the secondary user coordinator, the secondary user coordinator can also detect the existence of the malicious user. It should also be emphasized that when a secondary user coordinator is involved, only the secondary user coordinator needs to perform primary user and malicious user detection. Hence, it can reduce the burden of each individual secondary user, which generally relies on transceivers with limited capabilities [60].

3.3 AES-based PUEA Detection Scheme

In this section, we present the AES-based PUEA detection scheme for reliable and effective CR network operation. We start by discussing the primary DTV transmitter design, where the existing reference sequence used to generate the P2 pilots is encrypted using the AES algorithm. Then, we investigate the SUC receiver design for accurate detection of the primary user and malicious user. Moreover, we evaluate the detection performance through false alarm rate and miss detection probability, and discuss the effect of the sample size on the detection measures.

3.3.1 Primary User Transmitter Design

The frequency indexes of P2 pilots are determined by:

$$\Omega = \{m \mid m \equiv 0 \pmod{3}, 0 \leq m \leq M_{\max}\}, \quad (3.1)$$

where $M_{\max}$ is the maximum frequency index for the P2 symbol. The P2 pilots are generated based on the reference sequence $\mathbf{r}_s$, which is obtained by performing the XOR (exclusive-OR) function to two pseudo-random sequences, as shown in Figure 3.3 [59]. More details on the PN sequences generation can be found in [59].

As illustrated in Figure 3.3, we propose that the existing reference sequence $\mathbf{r}_s$ is further encrypted using the AES algorithm with a secret key to obtain the proposed reference signal $\mathbf{s}$ as follows:

$$\mathbf{s} = E(\text{key}, \mathbf{r}_s), \quad (3.2)$$

where $E(\cdot, \cdot)$ denotes the AES encryption operation. It should be noted that the encrypted

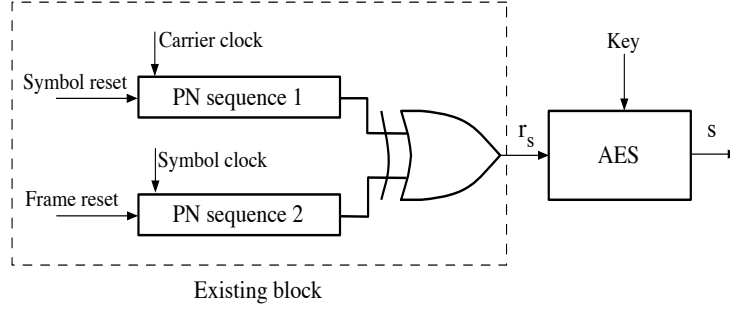


Figure 3.3: Generation of the proposed reference signal $\mathbf{s}$.

pilot symbols are still used as the conventional pilots for synchronization purposes.

The secret key can be generated and distributed to the DTV transmitter and receiver from a trusted 3rd party in addition to the DTV and the SUCs. The 3rd party serves as the authentication center for both the primary user and the CR user, and can carry out key distribution. To prevent impersonation and replay attacks, the key should be time varying [51, 61]. In the cognitive radio network, authentication and authorization are needed before key distribution, to ensure that only authorized users would receive the key, and to enforce user accountability and prevent misuse of privileges.

3.3.2 Secondary User Coordinator Receiver Design

The SUC receiver regenerates the encrypted reference signal with the secret key shared between the primary transmitter and the receiver. A correlation detector is employed, where for primary user detection, the receiver evaluates the cross-correlation between the received signal and the regenerated reference signal; for malicious user detection, the receiver further evaluates the auto-correlation of the received signal. To perform primary user and malicious user detection, the SUC receiver needs to collect a sufficient amount of the received samples, M samples (see Section 3.3.3), on the desired subcarrier before calculating the cross-correlation and the auto-correlation.

For any $k \in \Omega = \{0, 3, 6, \dots, M_{\max}\}$, the received $M \times 1$ vector on subcarrier k at SUC1, shown in Figure 3.1, can be modeled as:

$$\mathbf{r}_k = \alpha_k \sqrt{l_{d1} P_{s,k}} |h_k| \mathbf{s}_k + \beta_k \mathbf{m}_k + \mathbf{n}_k, \quad (3.3)$$

where $\mathbf{s}_k$, $P_{s,k}$, l_{d1} , and $h_k \sim \mathcal{CN}(0, 1)$ are the transmitted binary phase shift keying (BPSK) symbol vector (BPSK is adopted here because it is used in the DVB-T2 standard), the allocated transmit power, the path loss attenuation factor, and the Rayleigh fading coefficient on subcarrier k between PU1 and SUC1, respectively. $\mathbf{m}_k$ is the MU1 BPSK symbol vector, $\mathbf{n}_k \sim \mathcal{N}(0, \sigma_n^2 \mathbf{I})$ is the noise, α_k and β_k are binary indicators for the presence of the primary user and malicious user on $k \in \Omega$ subcarrier, respectively.

3.3.2.1 Primary User Detection

To detect the presence of the primary user on subcarrier k , where $k \in \Omega$, the SUC receiver evaluates the cross-correlation between the received vector and the regenerated reference vector. The normalized cross-correlation can be represented as:

$$\mathbf{R}_{rs,k} = \frac{\langle \mathbf{r}_k, \mathbf{s}_k \rangle}{M} = \alpha_k \sqrt{l_{d1} P_{s,k}} |h_k|, \quad (3.4)$$

where we assume that the channel is time-invariant during the observed period, and the channel gain is available at the SUC receiver, and $\mathbf{s}_k$, $\mathbf{m}_k$, $\mathbf{n}_k$ are independent with each other and are of zero mean.

Depending on the value of α_k , the SUC receiver decides whether the primary user is present or absent on subcarrier k , and then passes the information detection to the SUs within the cell.

Assuming that the signals are ergodic, then the ensemble average can be approximated by the time average. Here, we use the time average to estimate the cross-correlation, i.e.,

$$\hat{\mathbf{R}}_{rs,k} \triangleq \frac{1}{M} \sum_{i=1}^M \mathbf{r}_{k,i} \cdot \mathbf{s}_{k,i}^*, \quad (3.5)$$

where M is the sample size, $\mathbf{s}_{k,i}$ and $\mathbf{r}_{k,i}$ denote the i th entries in the reference and received vectors on subcarrier $k \in \Omega$, respectively.

To detect the presence of the primary user, the receiver compares the cross-correlation between the reference signal and the received signal with a predefined threshold T_k . We have two cases: (i) if $\hat{\mathbf{R}}_{rs,k} \geq T_k$, then we determine that the primary user is present, and (ii) if $\hat{\mathbf{R}}_{rs,k} < T_k$, then we determine that the primary user is absent. The detection problem can be modeled as a binary hypothesis test problem as follows:

H_0 : the primary user is absent on subcarrier k ($\alpha_k = 0$)

H_1 : the primary user is present on subcarrier k ($\alpha_k = 1$)

As can be seen from (3.4), the normalized cross-correlation between the reference signal and the received signal is equal to 0 or $\sqrt{l_{d1}P_{s,k}}|h_k|$, in case when the primary user is absent or present, respectively. Following the *minimum distance rule*, we choose $T_k = (\sqrt{l_{d1}P_{s,k}}|h_k|)/2$ as the threshold for primary user detection.

3.3.2.2 Malicious User Detection

For malicious user detection, the SUC receiver further evaluates the auto-correlation of the received vector $\mathbf{r}_k$, where the normalized auto-correlation can be represented as:

$$\mathbf{R}_{rr,k} = \frac{\langle \mathbf{r}_k, \mathbf{r}_k \rangle}{M} = \alpha_k l_{d1} P_{s,k} |h_k|^2 + \beta_k \sigma_{m,k}^2 + \sigma_n^2. \quad (3.6)$$

Based on the estimated value of α_k , β_k can be determined accordingly through (3.6). We have the following cases:

$$\mathbf{R}_{rr,k} = \begin{cases} l_{d1}P_{s,k}|h_k|^2 + \sigma_{m,k}^2 + \sigma_n^2, & \alpha_k = 1, \beta_k = 1 \\ l_{d1}P_{s,k}|h_k|^2 + \sigma_n^2, & \alpha_k = 1, \beta_k = 0 \\ \sigma_{m,k}^2 + \sigma_n^2, & \alpha_k = 0, \beta_k = 1 \\ \sigma_n^2, & \alpha_k = 0, \beta_k = 0 \end{cases} \quad (3.7)$$

Assuming ergodic signals, we can use the time average to estimate the auto-correlation as follows:

$$\hat{\mathbf{R}}_{rr,k} \triangleq \frac{1}{M} \sum_{i=1}^M \mathbf{r}_{k,i} \cdot \mathbf{r}_{k,i}^*. \quad (3.8)$$

Threshold based detection method can be developed accordingly. Here, we can model the detection problem using four hypotheses, denoted by $H_{\alpha_k\beta_k}$, where $\alpha_k, \beta_k \in \{0, 1\}$:

H_{00} : the malicious user is absent given that $\alpha_k = 0$ ($\hat{\mathbf{R}}_{rr,k} < T_{k,0}$)

H_{01} : the malicious user is present given that $\alpha_k = 0$ ($\hat{\mathbf{R}}_{rr,k} \geq T_{k,0}$)

H_{10} : the malicious user is absent given that $\alpha_k = 1$ ($\hat{\mathbf{R}}_{rr,k} < T_{k,1}$)

H_{11} : the malicious user is present given that $\alpha_k = 1$ ($\hat{\mathbf{R}}_{rr,k} \geq T_{k,1}$)

The performance of the detection process for the primary user and malicious user is evaluated through the false alarm rates (FARs) and the miss detection probabilities (MDPs), as will be discussed in the following subsection.

3.3.3 False Alarm Rate and Miss Detection Probability

Denote the false alarm rate for primary user detection on subcarrier k , where $k \in \Omega$, by $P_{f,k}$, and the miss detection probability by $P_{m,k}$. The false alarm rate is defined as the conditional probability that the primary user is considered to be present, when it is actually absent, i.e.,

$$P_{f,k} = Pr(H_1|H_0), \quad (3.9)$$

whereas the miss detection probability is defined as the conditional probability that the primary is considered to be absent, when it is present, i.e.,

$$P_{m,k} = Pr(H_0|H_1). \quad (3.10)$$

Note that the cross-correlation $\hat{\mathbf{R}}_{rs,k}$, defined in (3.5), is the sample mean of independent random variables of size M . According to the central limit theorem (CLT), as long as M is sufficiently large (i.e., $M \geq 30$), this sample mean approximately follows the Gaussian distribution [62]. More specifically, under H_0 , $\hat{\mathbf{R}}_{rs,k} \sim \mathcal{N}(\mu_0, \sigma_0^2)$ with mean $\mu_0 = 0$ and variance $\sigma_0^2 = \frac{1}{M} [\beta_k \sigma_{m,k}^2 + \sigma_n^2]$. Similarly, under H_1 , $\hat{\mathbf{R}}_{rs,k} \sim \mathcal{N}(\mu_1, \sigma_1^2)$ with mean $\mu_1 = \sqrt{l_{d1} P_{s,k}} |h_k|$ and variance $\sigma_1^2 = \frac{1}{M} [l_{d1} P_{s,k} |h_k|^2 \mathbb{E}\{|\tilde{\mathbf{s}}_k|^4\} + \beta_k \sigma_{m,k}^2 + \sigma_n^2 - l_{d1} P_{s,k} |h_k|^2]$, where $\mathbb{E}\{|\mathbf{s}_{k,i}|^4\} = \mathbb{E}\{|\tilde{\mathbf{s}}_k|^4\} \forall i$. The false alarm rate $P_{f,k}$ can be obtained as:

$$P_{f,k} = Pr\{\hat{\mathbf{R}}_{rs,k} \geq T_k | H_0\} = Q\left(\frac{T_k - \mu_0}{\sigma_0}\right), \quad (3.11)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{u^2}{2}} du$ denotes the tail probability of the standard normal distribu-

tion. The miss detection probability $P_{m,k}$ can be obtained as:

$$P_{m,k} = P_r\{\hat{\mathbf{R}}_{rs,k} < T_k | H_1\} = 1 - Q\left(\frac{T_k - \mu_1}{\sigma_1}\right). \quad (3.12)$$

Similarly, for malicious user detection, denote the false alarm rate by $\tilde{P}_{f,k}$ and the miss detection probability by $\tilde{P}_{m,k}$, which can be obtained as:

$$\tilde{P}_{f,k} = P_0 Q\left(\frac{T_{k,0} - \mu_{00}}{\sigma_{00}}\right) + (1 - P_0) Q\left(\frac{T_{k,1} - \mu_{10}}{\sigma_{10}}\right), \quad (3.13)$$

and

$$\tilde{P}_{m,k} = 1 - P_0 Q\left(\frac{T_{k,0} - \mu_{01}}{\sigma_{01}}\right) + (P_0 - 1) Q\left(\frac{T_{k,1} - \mu_{11}}{\sigma_{11}}\right), \quad (3.14)$$

where $P_0 = P_r(\alpha_k = 0)$, and μ_{00} , σ_{00} , μ_{01} , σ_{01} , μ_{10} , σ_{10} , μ_{11} , σ_{11} , and the optimal values for $T_{k,0}$ and $T_{k,1}$ can be found in the appendix.

3.3.4 Detection Performance Versus Sample Size

In this subsection, we discuss the influence of the sample size M on the the false alarm rate and miss detection probability.

Substituting by $(\sqrt{l_{d1} P_{s,k}} |h_k|)/2$ for T_k in (3.11) and (3.12), we have:

$$P_{f,k} = Q(c\sqrt{M}), \quad (3.15)$$

and

$$P_{m,k} = 1 - Q(-c\sqrt{M}), \quad (3.16)$$

where $c = (\sqrt{l_{d1} P_{s,k}} |h_k|) / (2\sqrt{\beta_k \sigma_{m,k}^2 + \sigma_n^2})$.

Discussions: Following (3.15) and (3.16), under reasonably high SNR level, both the false alarm rate $P_{f,k}$ and the miss detection $P_{m,k}$ decrease as the sample size increases. More specifically, $\lim_{M \rightarrow \infty} P_{m,k} = 0$ and $\lim_{M \rightarrow \infty} P_{f,k} = 0$.

3.4 Simulation Results

In this section, we demonstrate the performance of the proposed AES-based DTV scheme through the evaluation of the false alarm rate and miss detection probability for primary user and malicious user detection. In the following, we assume that $\mathbf{s}_k$, $\mathbf{m}_k$, $\mathbf{n}_k$ are independent with each other and are of zero mean. Furthermore, the path loss attenuation factor is given by $l_{d1} = d_1^{-\gamma}$, where $\gamma = 2$ is the path loss exponent and $d_1 = 500m$ is the distances between PU1 and SUC1, shown in Figure 3.1.

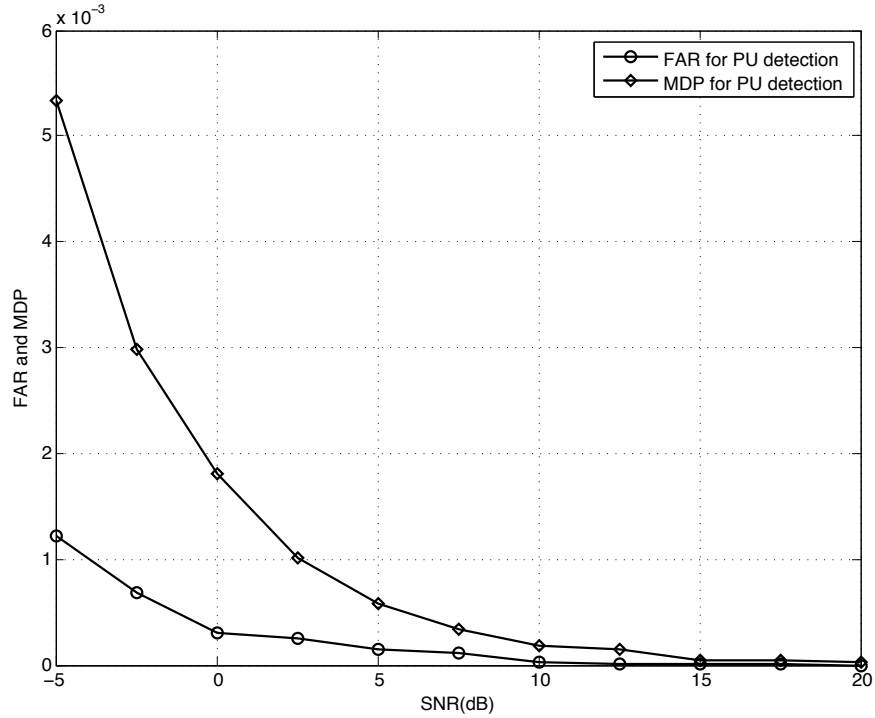


Figure 3.4: The false alarm rate (FAR) and miss detection probability (MDP) versus SNR for primary user detection.

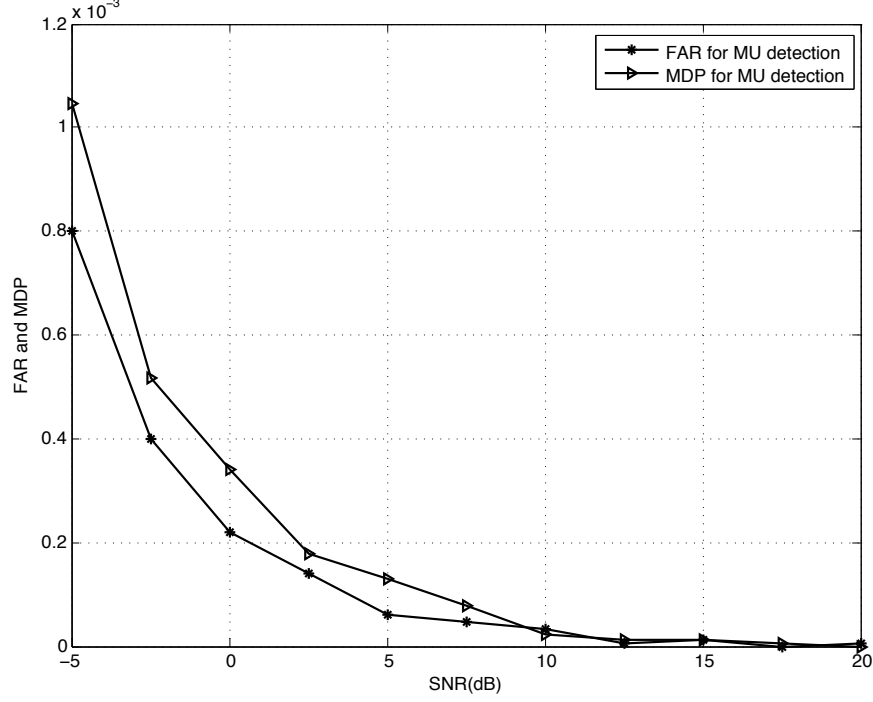


Figure 3.5: The false alarm rate (FAR) and miss detection probability (MDP) versus SNR for malicious user detection.

Using the sample size $M = 100$, we obtain the false alarm rate and miss detection probability for both primary user detection and malicious user detection. Figure 3.4 shows the false alarm rate and miss detection for primary user detection versus SNR, while the false alarm rate and miss detection for malicious user detection are depicted in Figure 3.5. It can be seen that the proposed AES-based DTV scheme can achieve very low false alarm rates and miss detection probabilities even under very low SNR values when detecting the primary user and malicious user.

3.5 Summary

In this chapter, we studied the PUEA problem in the OFDM-based CR networks, and proposed a reliable and efficient AES-based DTV scheme. In the proposed approach, the

existing reference sequence in the DTV system is encrypted using the AES algorithm for accurate sub-band detection of the authorized primary user, as well as malicious user, in the allocated frequency spectrum. It was shown that, with the AES-based DTV scheme, both the primary user and the malicious user can be detected accurately under primary user emulation attacks. The proposed approach is practically feasible in the sense that it can effectively detect primary user and malicious user with no change in hardware or system structure except of a plug-in AES chip. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

Chapter 4

Energy Harvesting and Reliable Information Transfer

This chapter aims to study simultaneous wireless information transfer and energy harvesting in OFDM-based CR networks under PUEA. Here, first, we propose an effective communication scheme for the secondary users under PUEA by exploiting the energy harvesting techniques. Optimal power splitting is considered for sum-rate maximization. As the optimal solution relies on multi-dimensional exhaustive search, we propose an effective suboptimal solution with much lower computational complexity. It is observed that the sum-rate of the secondary user network can be improved significantly with the energy harvesting technique. Then, we evaluate the worst-case PUEA interference in terms of minimizing the sum-rate for the secondary users. We show that for practical systems, as CSI among the SUs is not available to the malicious user, the worst jamming for the SUs is when the malicious user performs equal power allocation over all the white space subcarriers. Simulation results are provided to illustrate the proposed approaches. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

4.1 Introduction

Along with the emerging energy-constrained IoT network, which basically relies on transceivers with limited power capabilities, energy harvesting from ambient RF signals has attracted more research attention in recent years [24–35]. The concept of simultaneous wireless information transfer and energy harvesting was first proposed in [24], where the fundamental trade-off between information receiving and power transfer was studied from an information theory perspective. In literature [25, 26], there have been two representative receiver architectures for energy harvesting: power-splitting and time-switching. In the power-splitting based approach, a power splitter is employed at the RF band at the receiver. The received RF signal is split into two parts: one for energy harvesting and the other for information processing. In the time-switching approach, the received signal is divided into two parts in the time domain. The power transfer efficiency of energy harvesting techniques depends mainly on the received signal strength. In [27], it was shown that an efficiency of 0.4%, 18.2% and above 50% can be achieved with RF energy transfer with input power -40dBm , -5dBm , and 20dBm , respectively. More details on efficiency performance of wireless energy transfer techniques can be found in [28].

Recently, energy harvesting has been widely discussed in OFDM-based systems [29], wireless relay networks [30], and cognitive radio networks [31–35]. For example, the authors in [31] investigated the optimal transmission and energy harvesting policy to maximize the secondary network throughput in a cognitive radio network, where the secondary users opportunistically access the spectrum or harvest energy from the ambient RF signals from primary users. In [32], the authors studied the channel access problem in CR networks in which a secondary user can choose to access the channel for data transmission or energy har-

vesting. To obtain the channel access, they presented an optimization formulation based on Markov decision process. Generally, PUEA was not considered in these works [31–35]. However, PUEA is essentially jamming interference for the SUs, and potentially the performance of SUs can be improved significantly by exploiting PUEA as an extra energy resource. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

In Chapter 3, we investigated sub-band PUEA detection by proposing a robust AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm, and the resulted sequence is exploited for accurate sub-band detection of the authorized primary user and the malicious user. The SUCs were designed to perform spectrum sensing and PUEA detection, and then coordinate the SUs for collision-free transmission over the white spaces.

In this chapter, we propose an energy harvesting scheme as follows. When the detection of the primary user and the malicious user is done at the SUC, the SUC will coordinate the transmissions and spectrum sharing of the SUs based on the detection results. If there are no white spaces detected (i.e., the PU is occupying all the allocated spectrum), then secondary users perform energy harvesting from the received PU and MU signals. Otherwise (i.e., if there exist some white spaces), secondary users harvest energy and transmit their own signals simultaneously over the assigned time slots and frequency bands.

4.2 The Proposed Energy Harvesting Scheme

We consider a typical cell, which consists of a primary user, a secondary user coordinator, a malicious user, and a multiple (K) of secondary users, and propose a reliable and effi-

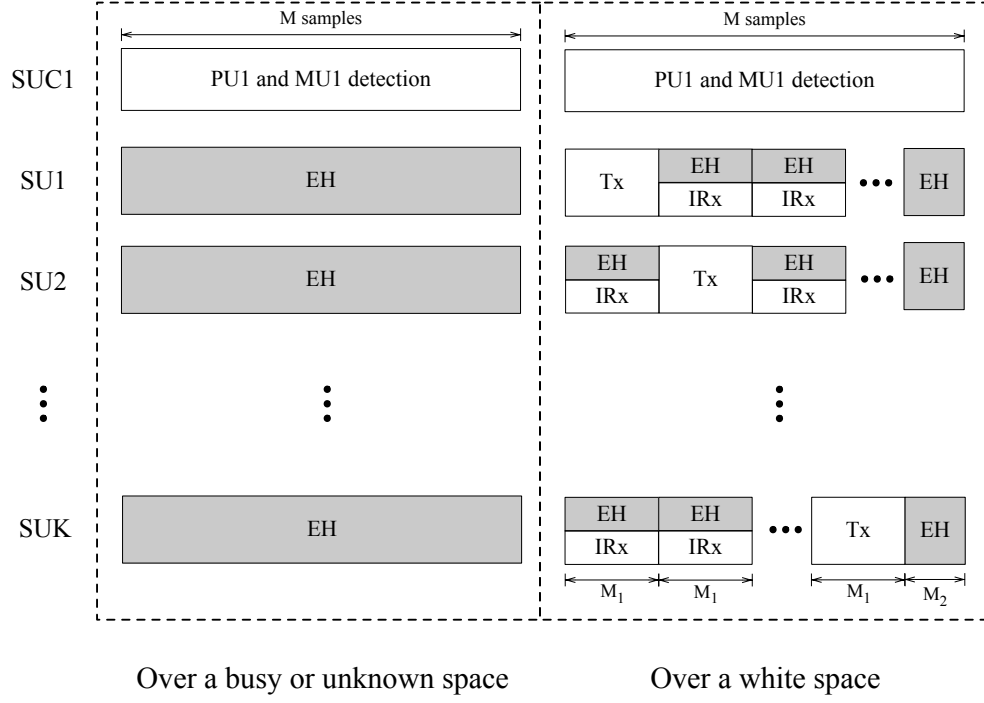


Figure 4.1: The proposed energy harvesting scheme.

cient scheme for resource utilization between the secondary users, shown in Figure 4.1. In this scheme, we propose that SUC1 detects PU1 and MU1 using correlation detectors after obtaining M samples of the received signal on the desired sub-channel (see Section 3.3). During the initial detection period, all the SUs harvest energy from all the subcarriers. The detection result is then used by SUC1 to coordinate transmissions among the SUs. Assuming there exist some white spaces, then the SUs share these white spaces using a collision-free multiple access scheme. Without loss of generality, here, we choose Time Division Multiplexing (TDM), as shown in Figure 4.1. More specifically, for the first $M_1 = \lfloor M/K \rfloor$ samples, SU1 transmits its signal, while the remaining SUs process information and harvest energy from the received signals with a power splitting receiver [63]. For the next M_1 samples, SU2 transmits with its inherent power and the harvested power, while the remaining SUs perform information recovery and energy harvesting, and so on. For the remaining $M_2 = M - KM_1$

samples, we propose that all the SUs harvest energy from the received signals, including both the primary user's signal and the malicious user's signal. Note that when the allocated channel bandwidth is fully utilized by the primary user, the harvested power, by the secondary users, can be stored in internal and/or external batteries for later usages.

4.3 Energy Harvesting and Performance Optimization

In this section, we discuss a secondary users energy harvesting and information exchange technique to improve the system performance of the OFDM-based CR networks under PUEA. To illustrate the proposed approaches, we discuss the optimal transceiver design for maximizing the sum-rate between two secondary users under jamming.

4.3.1 Secondary Users Energy Harvesting and Information Recovery

As mentioned earlier, if the primary user is present on all the subcarriers, then SUs only harvest energy from the received signals since they are prohibited from transmitting as long as the primary user is transmitting. On the other hand, if there exist some idle spectral spaces, then SUs process information and harvest energy simultaneously from the received RF signals, based on the proposed method shown in Figure 4.1. Here, we consider two-way communication between SU1 and SU2. First, we investigate the downlink transmission, where for the first M_1 samples, SU1 transmits to SU2, meanwhile SU2 performs information recovery and energy harvesting from the received signals with a power splitting receiver. Then, for the next M_1 samples, we consider the uplink transmission similarly as the downlink transmission case, except that the transmission this time is from SU2 to SU1. For the

remaining $M_2 = M - 2M_1$ samples, both SU1 and SU2 harvest energy from the received signals, including both the primary user's signal and the malicious user's signal. In the case that the SUs have sufficient power, for maximal transmission rate, we choose $M_1 = M/2$.

4.3.1.1 Achievable Transmission Rate for SU1

Consider an OFDM system with N subcarriers. Then, the downlink transmission corresponding to the *first* received M_1 samples on subcarrier $n \in \mathcal{N}_{sc} = \{1, 2, \dots, N\}$, at SU2, can be modeled as:

$$\mathbf{r}_{2,n} = \alpha_n \sqrt{l_{d2} P_{s,n}} g_{2,n} \tilde{\mathbf{s}}_n + \gamma_{1,n} \sqrt{l_{d4} P_{1,n}} f_{1,n} \tilde{\mathbf{s}}_{1,n} + \beta_n \tilde{\mathbf{m}}_{2,n} + \tilde{\mathbf{n}}_{a,n}, \quad (4.1)$$

where $P_{s,n}$ is the PU1's transmit power, and l_{d2} , $g_{2,n} \sim \mathcal{CN}(0, 1)$, $\tilde{\mathbf{s}}_n$ denote the path loss attenuation factor from PU1 to SU2, the Rayleigh fading coefficient between PU1 and SU2, and the PU1's transmitted symbol $M_1 \times 1$ vector on the n th subcarrier, respectively; l_{d4} , $P_{1,n}$, $f_{1,n} \sim \mathcal{CN}(0, 1)$, and $\tilde{\mathbf{s}}_{1,n}$ denote the path loss attenuation factor from SU1 to SU2, SU1's transmit power, the Rayleigh fading coefficient between SU1 and SU2, and SU1's transmitted symbol vector on the n th subcarrier, respectively; $\tilde{\mathbf{m}}_{2,n}$ is the received jamming symbol vector from MU1, $\tilde{\mathbf{n}}_{a,n} \sim \mathcal{CN}(0, \sigma_a^2 \mathbf{I})$ is the noise, α_n , β_n , $\gamma_{1,n}$ are binary indicators for the presence of the primary user, malicious user, and SU1 on the n th subcarrier, respectively. Note that $\gamma_{1,n} = 1$, for $n \in \mathcal{A}_1$ and $\gamma_{1,n} = 0$, for $n \notin \mathcal{A}_1$, where $\mathcal{A}_1$ is the set of white space subcarriers assigned to SU1. Let $\mathcal{A} = \{k | \alpha_k = 0, k \in \Omega\}$ be the set of all idle subcarriers. Without loss of generality, since SU1 and SU2 share the white spaces using time division multiple access (TDMA), we assume that $\mathcal{A}_1 = \mathcal{A}$.

The received signal, at SU2, is split into two parts: one for energy harvesting and the

other for information decoding. Let $\rho_2 \in [0, 1]$ denote the power splitting ratio at SU2, that is, $\sqrt{\rho_2} \mathbf{r}_{2,n}$ is used for energy harvesting. Then, from (4.1), the total harvested power at SU2 can be obtained as:

$$P_{EH,2} = \eta \rho_2 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \gamma_{1,n} l_{d4} P_{1,n} |f_{1,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2) + N \sigma_a^2 \right], \quad (4.2)$$

where $0 < \eta < 1$ is the energy conversion efficiency.

The other part of the received signal, i.e. $\sqrt{1 - \rho_2} \mathbf{r}_{2,n}$, is then used for information detection. The baseband signal can be expressed as:

$$\tilde{\mathbf{r}}_{2,n} = \sqrt{(1 - \rho_2) l_{d4} P_{1,n} f_{1,n}} \tilde{\mathbf{s}}_{1,n} + \sqrt{1 - \rho_2} (\beta_n \tilde{\mathbf{m}}_{2,n} + \tilde{\mathbf{n}}_{a,n}) + \tilde{\mathbf{n}}_{b,n}, \quad n \in \mathcal{A}, \quad (4.3)$$

where $\tilde{\mathbf{n}}_{b,n} \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I})$ is the noise in the baseband. Note that there is no primary user signal in the white spaces.

From (4.3), the achievable rate for the link from SU1 to SU2 is given by:

$$R_1 = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2) (\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right). \quad (4.4)$$

Remark 4.1 *We would like to point out that, theoretically, we should harvest all the energy (i.e., choose $\rho_2 = 1$) over the band occupied by the PU, use energy harvesting (i.e., choose $\rho_2 = 0$) for information recovery over jamming-free white spaces, and perform power splitting only over the white spaces which are contaminated by the malicious user. However, in practical systems, one receive antenna is used for all the subcarriers. As a result, the same power splitting ratio has to be applied for all the bands, as shown in (4.2). The same argument applies to the next subsection.*

4.3.1.2 Achievable Transmission Rate for SU2

The uplink transmission from SU2 to SU1 corresponding to the *next* received M_1 samples on subcarrier $n \in \mathcal{N}_{sc} = \{1, 2, \dots, N\}$, at SU1, can be modeled as:

$$\mathbf{r}_{1,n} = \alpha_n \sqrt{l_{d3} P_{s,n}} g_{1,n} \tilde{\mathbf{s}}_n + \gamma_{2,n} \sqrt{l_{d4} P_{2,n}} f_{2,n} \tilde{\mathbf{s}}_{2,n} + \beta_n \tilde{\mathbf{m}}_{1,n} + \tilde{\mathbf{n}}_{a,n}, \quad (4.5)$$

where $P_{s,n}$ is the PU1's transmit power, and l_{d3} , $g_{1,n} \sim \mathcal{CN}(0, 1)$, $\tilde{\mathbf{s}}_n$ denote the path loss attenuation factor from PU1 to SU1, the Rayleigh fading coefficient between PU1 and SU1, and PU1's transmitted symbol $M_1 \times 1$ vector on the n th subcarrier, respectively; $P_{2,n}$, $f_{2,n} \sim \mathcal{CN}(0, 1)$, and $\tilde{\mathbf{s}}_{2,n}$ denote SU2's transmit power, the Rayleigh fading coefficient between SU2 and SU1, and SU2's transmitted symbol vector on the n th subcarrier, respectively; $\tilde{\mathbf{m}}_{1,n}$ is the received jamming symbol vector from MU1, α_n , β_n , $\gamma_{2,n}$ are binary indicators for the presence of the primary user, malicious user, and SU2 on the n th subcarrier, respectively. Note that $\gamma_{2,n} = 1$, for $n \in \mathcal{A}_2$ and $\gamma_{2,n} = 0$, for $n \notin \mathcal{A}_2$, where $\mathcal{A}_2$ is the set of white space subcarriers assigned to SU2. Here, since SU1 and SU2 share the white spaces using TDMA, we assume that $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$.

The received signal, at SU1, is then split into two parts: one for energy harvesting and the other for information recovering. Let $\rho_1 \in [0, 1]$ denote the power splitting ratio at SU1, that is, $\sqrt{\rho_1} \mathbf{r}_{1,n}$ is used for energy harvesting. Then, from (4.5), the total harvested power at SU1 can be obtained as:

$$P_{EH,1} = \eta \rho_1 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \gamma_{2,n} l_{d4} P_{2,n} |f_{2,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right]. \quad (4.6)$$

The other part of the received signal, $\sqrt{1 - \rho_1} \mathbf{r}_{1,n}$, is then used for information detection.

The baseband signal can be expressed as:

$$\tilde{\mathbf{r}}_{1,n} = \sqrt{(1 - \rho_1)l_{d4}P_{2,n}f_{2,n}}\tilde{\mathbf{s}}_{2,n} + \sqrt{1 - \rho_1}(\beta_n\tilde{\mathbf{m}}_{1,n} + \tilde{\mathbf{n}}_{a,n}) + \tilde{\mathbf{n}}_{b,n}, \quad n \in \mathcal{A}, \quad (4.7)$$

where $\tilde{\mathbf{n}}_{b,n} \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I})$ is the noise in the baseband. From (4.7), the achievable rate for the uplink transmission is given by:

$$R_2 = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_1)l_{d4}P_{2,n}|f_{2,n}|^2}{(1 - \rho_1)(\beta_n\tilde{\sigma}_{1,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right). \quad (4.8)$$

Discussions: If $M_1 < M/2$, i.e., $M_2 = M - 2M_1 > 0$, then both SU1 and SU2 harvest energy from the received signals during the M_2 period. Therefore, the total harvested power at the SU1 and SU2 during the M_2 period can be obtained as:

$$\tilde{P}_{EH,1} = \eta(M - 2M_1) \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N\sigma_a^2 \right], \quad (4.9)$$

and

$$\tilde{P}_{EH,2} = \eta(M - 2M_1) \left[\sum_{n=1}^N (\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2) + N\sigma_a^2 \right]. \quad (4.10)$$

In the case that the SUs have sufficient power, then for maximal transmission rate, we choose $M_1 = M/2$.

4.3.2 Sum-rate Optimization

In this subsection, we investigate the optimal transceiver design that aims to maximize sum-rate between SU1 and SU2.

From (4.4) and (4.8), the sum-rate maximization problem can be expressed as:

$$\begin{aligned}
& \max_{\rho_1, \rho_2, M_1, \mathbf{P}_1, \mathbf{P}_2} R_{sum} = R_1 + R_2 \\
& \text{s.t.} \quad 0 \leq \rho_1 \leq 1, \\
& \quad 0 \leq \rho_2 \leq 1, \\
& \quad 0 \leq M_1 \leq \frac{M}{2}, \\
& \quad \sum_{n \in \mathcal{A}} P_{1,n} \leq P_{SU1} + \frac{P_{EH,1} + \tilde{P}_{EH,1}}{M_1}, \\
& \quad \sum_{n \in \mathcal{A}} P_{2,n} \leq P_{SU2} + \frac{P_{EH,2} + \tilde{P}_{EH,2}}{M_1},
\end{aligned} \tag{4.11}$$

where $\mathbf{P}_j = \{P_{j,n}, \forall n \in \mathcal{A}\}$, $j = 1, 2$, and P_{SU1} , P_{SU2} denote the inherent power supply of SU1 and SU2, respectively.

The optimization problem in (4.11) belongs to the class of non-convex optimization problems due to the presence of ρ_1 , ρ_2 , and M_1 . However, for fixed ρ_1 , ρ_2 , and M_1 , the harvested powers in (4.2) and (4.6) are both linear functions of $\mathbf{P}_1$ and $\mathbf{P}_2$. Hence, the constraints in (4.11) become linear constraints. Based on these observations, it can be seen that the problem in (4.11) turns out to be convex when ρ_1 , ρ_2 , and M_1 are fixed, and can be solved numerically using the standard algorithms for convex optimization [64]. Hence, the sum-rate maximization problem in (4.11) for the proposed scheme can be solved by three-dimensional exhaustive search over ρ_1 , ρ_2 , and M_1 .

Note that although exhaustive search over ρ_1 , ρ_2 , and M_1 along with the convex optimization techniques guarantees the globally optimal solution of (4.11), it requires high computational complexity. To reduce the complexity, we propose a suboptimal solution.

Discussions: The sum-rate optimization problem can be extended to the K -user case by

dividing the SUs into groups of two, then performing the same sum-rate optimization as in (4.11). If K is odd, then the SUs can be divided into $\frac{K-1}{2}$ pairs plus 1 SU. The sum-rate optimization for the last SU is actually much simpler. Therefore, the overall sum-rate for multiple users would be similar to that of the two-user case. Taking the large number of white spaces in cognitive radios, it would be beneficial to keep the number of pair groups small in each shared/assigned frequency band.

4.3.3 Suboptimal Solution

In this subsection, we first calculate the sum-rate lower bound, and then derive the suboptimal solution based on it.

4.3.3.1 Sum-rate Lower Bound

For maximal transmission rate, let M_1 be fixed as $M_1 = M/2$ and consider equal power allocation at the two SUs, i.e.,

$$P_{1,n} = \frac{1}{|\mathcal{A}|} \left[P_{SU1} + \frac{P_{EH,1}}{M_1} \right], \quad (4.12)$$

and

$$P_{2,n} = \frac{1}{|\mathcal{A}|} \left[P_{SU2} + \frac{P_{EH,2}}{M_1} \right]. \quad (4.13)$$

Then, the achievable rate for SU1 can be lower bounded by:

$$\begin{aligned}
R_1 &= \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2)(\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right) \\
&> \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2)(\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right) \\
&\geq \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2) \tilde{\sigma}_{2,m}^2 + \sigma_b^2} \right),
\end{aligned} \tag{4.14}$$

where $\tilde{\sigma}_{2,m}^2 = \frac{1}{|\mathcal{A}|} \sum_{n \in \mathcal{A}} \beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2$. In the inequality above, we have used the fact that $\prod_{n=1}^N x_n \leq \left(\frac{1}{N} \sum_{n=1}^N x_n \right)^N$.

Similarly, the achievable rate of SU2 is lower bounded by:

$$R_2 \geq \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_1) l_{d4} P_{2,n} |f_{2,n}|^2}{(1 - \rho_1) \tilde{\sigma}_{1,m}^2 + \sigma_b^2} \right), \tag{4.15}$$

where $\tilde{\sigma}_{1,m}^2 = \frac{1}{|\mathcal{A}|} \sum_{n \in \mathcal{A}} \beta_n \tilde{\sigma}_{1,m,n}^2 + \sigma_a^2$.

$P_{EH,1}$ in (4.6) can be lower bounded by:

$$P_{EH,1} > P_{EH,1}^{LB} = \eta \rho_1 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right]. \tag{4.16}$$

From (4.12) and (4.16), the allocated power $P_{1,n}$ is lower bounded by:

$$P_{1,n} > c_1 \rho_1 + \zeta_1, \tag{4.17}$$

where

$$c_1 = \frac{\eta \left[\sum_{n=1}^N \left(\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2 \right) + N \sigma_a^2 \right]}{|\mathcal{A}|}, \quad (4.18)$$

and

$$\zeta_1 = \frac{P_{SU1}}{|\mathcal{A}|}. \quad (4.19)$$

From (4.17), the rate R_1 in (4.14) can be further bounded by:

$$R_1 > R_1^{LB} = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2)(c_1 \rho_1 + \zeta_1) l_{d4} |f_{1,n}|^2}{(1 - \rho_2) \tilde{\sigma}_{2,m}^2 + \sigma_b^2} \right). \quad (4.20)$$

Similarly, we have:

$$R_2 > R_2^{LB} = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_1)(c_2 \rho_2 + \zeta_2) l_{d4} |f_{2,n}|^2}{(1 - \rho_1) \tilde{\sigma}_{1,m}^2 + \sigma_b^2} \right), \quad (4.21)$$

where

$$c_2 = \frac{\eta \left[\sum_{n=1}^N \left(\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2 \right) + N \sigma_a^2 \right]}{|\mathcal{A}|}, \quad (4.22)$$

and

$$\zeta_2 = \frac{P_{SU2}}{|\mathcal{A}|}. \quad (4.23)$$

4.3.3.2 Suboptimal Solutions

Instead of maximizing the sum-rate in (4.11), we maximize the sum-rate lower bound, which can be formulated as:

$$\begin{aligned}
& \max_{\rho_1, \rho_2} R_1^{LB} + R_2^{LB} \\
& \text{s.t.} \quad 0 \leq \rho_1 \leq 1, \\
& \quad \quad 0 \leq \rho_2 \leq 1,
\end{aligned} \tag{4.24}$$

which is equivalent to:

$$\begin{aligned}
& \max_{\rho_1, \rho_2} \frac{(1 - \rho_2)(c_1\rho_1 + \zeta_1)}{(1 - \rho_2)\tilde{\sigma}_{2,m}^2 + \sigma_b^2} \frac{(1 - \rho_1)(c_2\rho_2 + \zeta_2)}{(1 - \rho_1)\tilde{\sigma}_{1,m}^2 + \sigma_b^2} \\
& \text{s.t.} \quad 0 \leq \rho_1 \leq 1, \\
& \quad \quad 0 \leq \rho_2 \leq 1.
\end{aligned} \tag{4.25}$$

The optimal power splitting ratios for (4.25) can be obtained as:

$$\rho_1^* = \left[\frac{\tilde{\sigma}_{1,m}^2 + \sigma_b^2 - \sigma_b \sqrt{\sigma_b^2 + (1 + \zeta_1/c_1)\tilde{\sigma}_{1,m}^2}}{\tilde{\sigma}_{1,m}^2} \right]^+, \tag{4.26}$$

and

$$\rho_2^* = \left[\frac{\tilde{\sigma}_{2,m}^2 + \sigma_b^2 - \sigma_b \sqrt{\sigma_b^2 + (1 + \zeta_2/c_2)\tilde{\sigma}_{2,m}^2}}{\tilde{\sigma}_{2,m}^2} \right]^+, \tag{4.27}$$

where $[x]^+ = \max(x, 0)$. The computational complexity of this suboptimal scheme is much lower than the optimal one, which requires three-dimensional exhaustive search together with convex optimization.

4.4 Discussions on Worst Jamming Interference in PUEA

In this section, we discuss the worst-case interference for the SUs, which aims to minimize the maximum sum-rate. We will show that for the secondary users, equal power interference from the malicious user is the worst interference for weak jamming, and nearly the worst interference for strong jamming, while the CSI-assisted interference is the worst-case interference for strong jamming in the high SNR region. To see this, consider the following optimal interference power allocation problem for sum-rate minimization for SU1:

$$\begin{aligned} \min_{\sigma_{MU,n}^2} \quad & R_1 = \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\ \text{s.t.} \quad & \sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 = \sigma_{MU}^2, \end{aligned} \tag{4.28}$$

where $H_n = \sqrt{l_{d4}} f_{1,n}$ and $\sigma^2 = \sigma_a^2 + \sigma_b^2$. $\sigma_{MU,n}^2 = \beta_n \sigma_{MU,n}^2$ and $H_{2,m,n}$ denote the allocated jamming power at the MU1, and the frequency response of the n th subchannel from MU1 to SU2, respectively. Here, we have omitted the constant $\frac{M_1}{M}$ and assumed that there is no energy harvesting, i.e., $\rho_2 = 0$.

For weak interference, where $|H_{2,m,n}|^2 \sigma_{MU,n}^2 \ll |H_n|^2 P_{1,n}, \forall n$, and in the high SNR

region, we have:

$$\begin{aligned}
R_1 &= \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\
&\simeq \sum_{n \in \mathcal{A}} \log_2 \left(\frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \right) \\
&= \log_2 \prod_{n \in \mathcal{A}} \left(\frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \right)
\end{aligned} \tag{4.29}$$

Hence, minimizing the sum-rate is equivalent to

$$\max_{\sigma_{MU,n}^2} \prod_{n \in \mathcal{A}} \left(|H_{2,m,n}|^2 \sigma_{MU,n}^2 \right) \tag{4.30}$$

It can be shown that the optimal solution is $\sigma_{MU,n}^{2*} = \frac{\sigma_{MU}^2}{|\mathcal{A}|}, \forall n \in \mathcal{A}$, which implies that *equal power interference is the worst-case interference for weak interference*.

For strong interference, where $|H_{2,m,n}|^2 \sigma_{MU,n}^2 \gg |H_n|^2 P_{1,n}, \forall n$, and in the high SNR region, we have:

$$\begin{aligned}
R_1 &= \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\
&\simeq \log_2(e) \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2},
\end{aligned} \tag{4.31}$$

where we have used the approximation that $\log_2(1+x) \simeq x \log_2(e)$ for small x .

The optimal interference power can be determined by solving the following problem:

$$\begin{aligned} \min_{\sigma_{MU,n}^2} \quad & \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \\ \text{s.t.} \quad & \sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 = \sigma_{MU}^2, \end{aligned} \quad (4.32)$$

which is given by:

$$\sigma_{MU,n}^{2'} = \frac{|H_n| \sqrt{P_{1,n}} / |H_{2,m,n}|}{\sum_{k \in \mathcal{A}} |H_k| \sqrt{P_{1,k}} / |H_{2,m,k}|} \sigma_{MU}^2, \forall n \in \mathcal{A}. \quad (4.33)$$

In fact, from (4.32), let $a_n = \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2}$. Using the well known inequality: $\sum_n x_n \sum_n \frac{a_n}{x_n} \geq (\sum_n \sqrt{a_n})^2$, we have:

$$\sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 \sum_{n \in \mathcal{A}} \frac{a_n}{\sigma_{MU,n}^2} \geq \left(\sum_n \sqrt{a_n} \right)^2, \quad (4.34)$$

where the equality holds if and only if $\sigma_{MU,n}^2 = c \sqrt{a_n}$, where c is a constant to meet the constraint $\sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 = \sigma_{MU}^2$. We can then obtain the result in (4.33).

The result above shows that: under strong interference, the optimal strategy for the malicious user is to adjust its power level on each white space subcarrier based on the knowledge of channel, namely *CSI-assisted interference*.

However, it is not difficult to show that the performance gap between the equal power interference and CSI-assisted adaptive interference is small. The sum-rate performance gap

is:

$$\begin{aligned}\Delta R_1 &\simeq \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^{2*}} - \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^{2'}} \\ &= \frac{1}{\sigma_{MU}^2} \left[|\mathcal{A}| \sum_{n \in \mathcal{A}} |H_n|^2 P_{1,n} / |H_{2,m,n}|^2 - \left(\sum_{n \in \mathcal{A}} |H_n| \sqrt{P_{1,n} / |H_{2,m,n}|} \right)^2 \right],\end{aligned}\quad (4.35)$$

which is small for large σ_{MU}^2 under strong interference.

Discussions: From the derivations above, we can see that for practical systems, equal power allocation at the malicious user is nearly optimal in terms of sum-rate degradation. In other words, due to the absence of CSI information, the worst jamming for the SUs is when the malicious user performs equal power allocation over all the white space subcarriers.

4.5 Simulation Results

In this section, we evaluate the performance of the proposed energy harvesting scheme. In the simulation, the path loss attenuation factor is given by $l_d = d^{-\gamma}$, where γ is the path loss exponent and d represents the distances between the network nodes. Moreover, the primary user is assumed to be transmitting with equal power over 112 subcarriers from 128 total subcarriers. The remaining 16 subcarriers are white spaces used for secondary user transmissions. It is also assumed that the malicious user has perfect knowledge of the location of the white space subcarriers, and performs equal power allocation over all these white space subcarriers to achieve the worst interference. To mitigate the interference from the malicious user, each secondary user needs to increase its own transmit power so that the received signal power at the other secondary user is higher than the received jamming power. For this purpose, each secondary user harvests energy from both the PUEA signals

Table 4.1: System Parameters

Sample size M	100
Number of subcarriers N	128
Number of white space & interference subcarriers	16
Distance between PU1 and SCU1 (d1)	500 m
Distance between PU1 and SU1 (d3)	50 m
Distance between PU1 and SU2 (d2)	50 m
PU1 total transmit power (over 112 subcarriers)	20 – 50 dBm
SU1 total transmit power (over 16 subcarriers)	10 dBm
SU2 total transmit power (over 16 subcarriers)	10 dBm
MU1 total transmit power (over 16 subcarriers)	10, 20 dBm
Noise variance per subcarrier	–60 dBm
Path loss exponent γ	2
Energy conversion efficiency η	0.7

and the primary user signals. The complete simulation parameters are listed in Table 4.1.

To demonstrate the effectiveness of the energy harvesting, Figure 4.2 shows achievable sum-rate of the proposed energy harvesting scheme and the conventional non-energy harvesting OFDM system under different PU and MU transmit power levels. It can be seen that, without the energy harvesting scheme, the sum-rate is low and independent of the transmit power levels. This is attributed to the fact that secondary users are limited to their inherent power. In contrast, with the proposed scheme, the achievable sum-rate improves significantly, especially under high PU transmit power. It should be noted that when we consider the power distributed to each subcarrier, the MU transmit power levels given in Table 4.1 are comparable to the PU transmit power levels. This reflects the fact that the MU is emulating the PU signal. More specifically, let P_s and P_m denote the total transmit power (in dBm) for the primary user and malicious user, respectively. Then, the PU transmit power per subcarrier (in dBm) is $(P_s - 10\log_{10}(112))$ dBm, and the MU transmit power per subcarrier is $(P_m - 10\log_{10}(16))$ dBm. This means, in terms of individual subcarrier, P_s

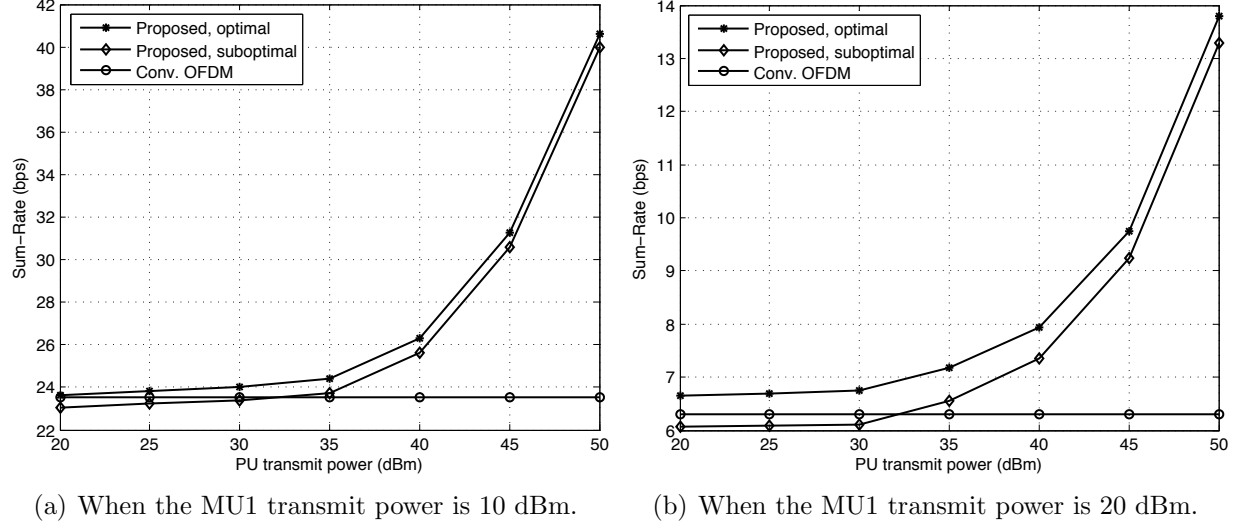


Figure 4.2: The achievable sum-rate comparison of the proposed OFDM-based energy harvesting scheme and that of its non-energy harvesting counterpart versus different PU and MU transmit power levels.

is equivalent to $P_m + 10\log_{10}(\frac{112}{16})$.

In the simulations, the power splitting ratios are calculated using both the optimal solution (through exhaustive search) and the suboptimal solution. More specifically, Figure 4.3 shows the optimal ρ_1^* and ρ_2^* for the proposed energy harvesting scheme versus PU transmit power. It can be seen that as the PU transmit power increases, the optimal and suboptimal power splitting ratios also increase. This indicates that there would be no benefit in harvesting energy for low received signal power. On the other hand, almost all the received signal is used for energy harvesting under high PU transmit power to enhance the uplink transmission. It is also observed that the performance of the suboptimal scheme is fairly close to the optimal one, but with much lower computational complexity.

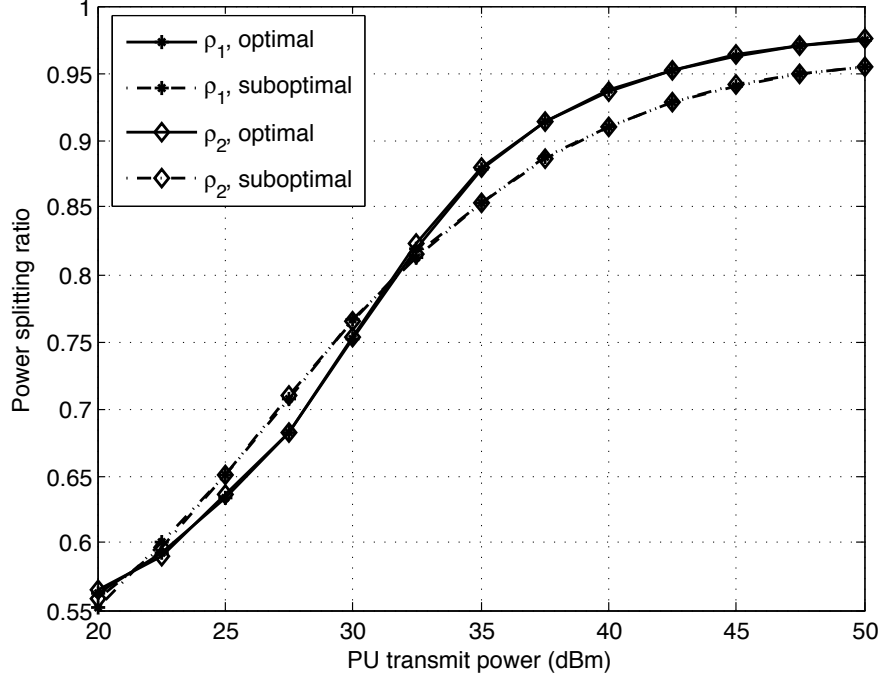


Figure 4.3: The optimal and suboptimal power splitting ratios versus PU transmit power.

4.6 Summary

In this chapter, we considered energy harvesting scheme for reliable and efficient OFDM-based CR network operation under PUEA. First, we proposed an effective communication scheme for the secondary users under PUEA by exploiting the energy harvesting techniques. Optimal power splitting was considered for sum-rate maximization. As the optimal solution relies on multi-dimensional exhaustive search, we proposed an effective suboptimal solution with much lower computational complexity. It was observed that the sum-rate of the secondary user network can be improved significantly with the energy harvesting technique. Second, we evaluated the worst-case PUEA interference in terms of minimizing the sum-rate for the secondary users. We showed that for practical systems, as CSI among the SUs is not available to the malicious user, the worst jamming for the SUs is when the malicious user performs equal power allocation over all the white space subcarriers. Simulation results were

provided to illustrate the proposed approaches. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

Chapter 5

Blocking Probability Analysis for Relay-assisted OFDMA Networks

Along with the emerging high density IoT networks, relay-assisted networks are attracting more research attention in recent years due to their abilities to extend the coverage area and improve the QoS. Blocking probability (BP) has been used as a very important metric in evaluating the QoS of the network. In this chapter, taking the spatial randomness of the IoT network into consideration, we investigate blocking probability in relay-assisted OFDMA networks using stochastic geometry. More specifically, first, we model the inter-cell interference from the neighboring cells at each typical node. Then, we derive the coverage probability in the downlink transmissions, including both the direct and relay-based transmissions. Finally, we classify the incoming users into different classes based on their data rate requirements, and calculate the blocking probability using the multi-dimensional loss model based on the Markov chains. We show that the blocking probability can be reduced by exploiting relay-assisted transmissions.

5.1 Introduction

In designing and analyzing wireless networks, blocking probability has been used as a very important metric in evaluating the QoS of the network. Blocking probability is the prob-

ability that an arriving user is denied of service due to insufficient network resources. In literature, blocking probability has been investigated for the OFDMA networks from different perspectives. To provide more reliable services for users with low received signal strength, relay stations are often deployed along with the base stations to extend the coverage area and improve the QoS. As a result, blocking probability has been studied in both single-hop and multi-hop networks.

Some representative work on blocking probability for the single-hop OFDMA networks can be found in [36–38]. In [36], the authors tried to model the subcarrier-allocation system using the batch-arrival model $M^X/M/c/c$. This model is not sufficiently accurate due to the assumption that the subcarriers are allocated in bulks but released one by one. Therefore, in [37], a more realistic model known as multi-class Erlang loss model was proposed. Motivated by the fact that power should be considered in addition to subcarriers as a system resource, a more general model was proposed in [38], where both the power and the subcarriers are regarded as the system resources.

Blocking probability for multi-hop OFDMA networks is attracting more research attention along with the emerging high density IoT networks. For example, in [39], the authors proposed a system model to evaluate the blocking probability for the relay-based OFDMA cellular networks. In their model, each cell consists of a base station, located at the center of the cell, and is surrounding by six relay stations with deterministic (known) locations. However, as pointed out in [40], results based on such highly idealized models generally may not be very accurate. On the other hand, it was also shown in [40] that modeling the locations of the base/relay stations stochastically according to a Poisson point process depicts the reality and can achieve more reliable and accurate results compared to its idealized counterparts. More closely, stochastic geometry has been widely applied in modeling wireless networks in

recent years [41–44]. For instance, in [41], stochastic geometry was used to analyze relay-aided two-hop networks. In [42], it was used to analyze multi-hop transmission in ad-hoc networks. However, to the best of our knowledge, no work has been done in literature to investigate blocking probability in relay-assisted OFDMA networks using stochastic geometry, which is the main contribution of this chapter.

In OFDMA networks, users are assigned different number of resource elements (subcarriers) to meet their rate requirements. Therefore, the incoming users can be classified into different classes based on their subcarrier requirements. A very challenging problem in calculating the blocking probability is to obtain *the distribution of the group size of the subcarriers that an arriving user needs* to fulfill its data rate. In most of the existing work [36–38], this distribution is assumed to be known, usually assumed to be uniform. This may not be accurate, especially for large group sizes, which actually have very low request probability.

In this work, we derive the distribution of user required subcarrier group size and then obtain the user blocking probability based on that. More specifically, first, we model the inter-cell interference from the neighboring cells at a typical node. Second, we derive the coverage probability (i.e., the probability of successful transmission) in the downlink transmissions, including both the direct and relay-based transmissions. Third, we classify the incoming users into different classes based on their subcarrier requirements. The system under consideration can be modeled using multi-dimensional Markov chains. Finally, we calculate the blocking probability using the multi-dimensional loss model.

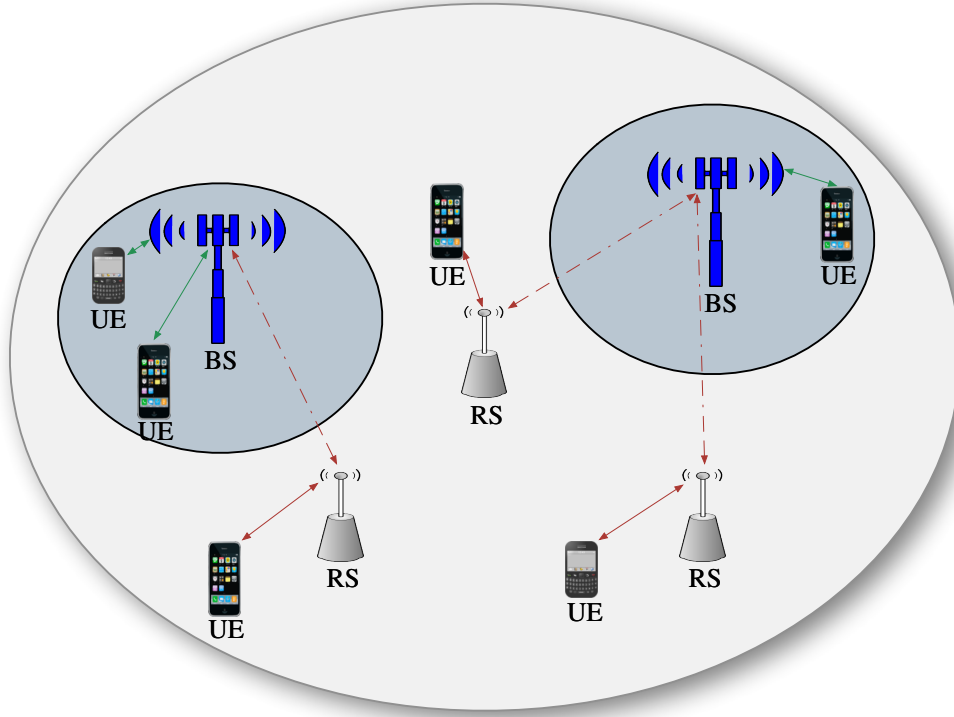


Figure 5.1: The proposed relay-assisted network architecture.

5.2 System Model

In this section, we present the relay-assisted system model for efficient OFDM-based networks.

5.2.1 Network Model

We consider a relay-assisted OFDM-based network, as shown in Figure 5.1. In this model, the network consists of base stations, relay stations, and end users, such as IoT devices. To account for the spatial randomness of the network, the locations of the base stations are modeled by a homogeneous Poisson point process $\Phi_B = \{X_i, i = 0, 1, 2, \dots\}$ in $\mathbb{R}^2$ with intensity λ_B , and the locations of the relay stations are modeled as another PPP $\Phi_R = \{Y_i\}$ with intensity λ_R , which is independent of Φ_B . It is further assumed that every user can

establish a connection with its geographically closest base station, either through a direct single-hop path, or through a multi-hop path with assistance from the relay stations. More specifically, based on their locations, the users can be divided into two groups S_D and S_R , where S_D denotes the set of all EUs that are located at a distance less than r_{BS} from their closest base station, and can communicate directly with the BS. On the other hand, S_R represents the set of the users that are located outside that circle of radius r_{BS} of the BS, and only connect to the BS indirectly through the relay stations, as shown in Figure 5.1. As will be discussed in Section 5.5, the optimal value of r_{BS} can be determined by minimizing the system blocking probability.

5.2.2 Transmission Protocol Design

Ideally, relays should lie on the line segment between the source and the destination to avoid the detour in routing. In addition, assuming that the source node and relay node use the same transmission power, then their intervals should be equal since the throughput of the path is bottlenecked by the hop with the longest distance. Motivated by this observation, we propose a routing protocol for relay-assisted transmission, as shown in Figure 5.2. More specifically, assume that a user EU_i is located at a distance $d_{BU} > r_{BS}$ from its base station,

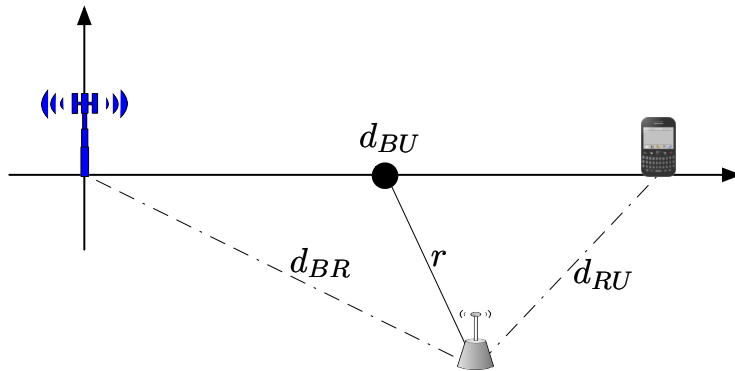


Figure 5.2: The proposed 2-hop routing topology.

i.e, $EU_i \in S_R$. Typically, EU_i should first send its data to the RS located in the middle point between the EU_i and the BS, and then the RS decodes the information and forwards it to the BS. However, since the locations of the RSs are random, it is not guaranteed that there will be a RS in the halfway point between transmitter and the receiver. Therefore, intuitively, EU_i should select its next hop to a RS that is located nearest to the optimal mid-point [65]. Let r denote the minimum distance between the optimal RS and any other arbitrary RS, then from the law of cosines, r can be expressed as:

$$r = \frac{1}{2} \sqrt{2(d_{BR}^2 + d_{RU}^2) - d_{BU}^2}, \quad (5.1)$$

where d_{BU} , d_{BR} and d_{RU} represent the distances between the BS to the user, the BS to the RS, and the RS to the user, respectively. Following the results in stochastic geometry [40], the probability density function (PDF) of the random variable r can be obtained as:

$$f_r(r) = 2\pi\lambda_R r e^{-\lambda_R \pi r^2}. \quad (5.2)$$

It should be emphasized that if $d_{BU} \leq r_{BS}$, user EU_i communicates directly with the base station, i.e, no hopping is required. This means, ideally, no relay stations should be deployed inside the circular areas of the BSs.

Here, all RSs are assumed to be half-duplex using decode-and-forward mechanism, which means that the 2-hop transmission is done through two different time slots (i.e., using TDD sharing mode). In the first time slot, BS/UE sends its information to the RS, then the RS decodes the information and forwards it to the UE/BS in the second slot. Moreover, a call will be dropped if it is wrongly decoded at the RSs.

5.2.3 Channel Model

We consider a propagation channel model, where the received power at a typical node of a transmitted signal at a distance d is $P_r(d) = \frac{P_t h}{l(d)}$, where P_t is the transmit power, $l(d)$ is the path-loss attenuation function of distance d , and h is the channel (power) gain. A simplified model for the path-loss is:

$$l(d) = \kappa_0 \cdot d^\alpha, \quad (5.3)$$

where α is the path-loss exponent, $\kappa_0 = (4\pi/v)^2$, and v is the electromagnetic wavelength. h is exponentially distributed random variable with unit mean, i.e., Rayleigh fading is considered.

5.3 Interference Modeling and Achievable Rate Analysis

In this section, we first analyze the inter-cell interference from the neighboring cells at a typical node. Then, we calculate the coverage probability in the downlink transmissions. After that, we obtain the achievable transmission rate.

5.3.1 Interference Model

In OFDMA networks, the total available spectrum is divided into a number of orthogonal subcarriers such that no two users belonging to the same cell share the same set of subcarriers. As a result, the intra-cell interference at a typical receiver can be avoided. However, inter-cell interference due to the neighboring cells should be investigated.

Consider a relay-assisted OFDM system with N subcarriers, each of bandwidth $\Delta f = \frac{B}{N}$,

where B is the system bandwidth. Define Φ_{T} as the set of active transmitters (BSs or RSs) occupying the same subcarrier k . Following the independent thinning property of the PPP [66], Φ_{T} can be modeled as a homogeneous PPP with intensity $p\lambda_{\text{B}}$, where p is the activity factor of the BS. Note that $p = 1$ is the worst case scenario where all the transmitters are active.

The signal-to-interference-plus-noise ratio (SINR) experienced by a typical node (RS or UE) at a distance d_0 from a transmitter $X_0 \in \Phi_{\text{T}}$ over subcarrier k can be expressed as:

$$\text{SINR}_k = \frac{P_{t,k} h_k l^{-1}(d_0)}{I_k + W}, \quad (5.4)$$

where

$$I_k = \sum_{i \in \Phi_{\text{T}} \setminus X_0} P_{t,k} h_{k,i} l^{-1}(d_i), \quad (5.5)$$

is the aggregate interference from all active transmitters over subcarrier k , except the serving transmitter X_0 . $W = \Delta f N_0$ is the total noise power over subcarrier k sub-band, and N_0 is the power spectral density of the noise. In an interference limited scenario, W is small compared to the interferences from all the active transmitters, and it can be ignored. The Laplace transform (LT) of the PDF of the random variable I_k evaluated at s can be obtained as [66]:

$$\begin{aligned} \mathcal{L}_{I_k}(s) &= \mathbb{E}\{e^{-sI_k}\} \\ &= \exp\left\{-2\pi p\lambda_{\text{B}}\left(\frac{s}{\kappa_0}\right)^{2/\alpha} \frac{\pi}{\alpha \sin(2\pi/\alpha)}\right\}, \end{aligned} \quad (5.6)$$

where it is assumed that $P_{t,k} = 1$. Hence, without loss of generality, we consider unit transmit power throughout this chapter. Also, for notational simplicity, we omit the subscript k used

to emphasize the explicit reference to a single subcarrier.

5.3.2 Coverage Probability

In this subsection, we study the probability of successful transmission (i.e., the coverage probability) in downlink transmission including both the direct and relay-based transmissions.

The coverage probability is defined as the probability that the receive SINR at a typical node is above a certain threshold γ , which is the same as the complementary cumulative distribution function (CCDF) of the SINR, i.e.,

$$P_c(\gamma) = \Pr\{\text{SINR} > \gamma\}. \quad (5.7)$$

5.3.2.1 Coverage Probability of Direct Transmission

Without loss of generality, we assume that the base station under consideration is located at the origin, as shown in Figure 5.2. Then, the coverage probability of the BS-UE link can be obtained as:

$$\begin{aligned} P_{c,BU}(\gamma_{BU} \mid d_{BU}) &= \Pr\{\text{SINR}_{BU} > \gamma_{BU}\} \\ &= \mathbb{E}_I \left\{ \Pr\left\{ \frac{hl^{-1}(d_{BU})}{I} > \gamma_{BU} \right\} \right\} \\ &= \mathbb{E}_I \left\{ \Pr\{h > \gamma_{BU} Il(d_{BU})\} \right\} \\ &= \mathcal{L}_I(\gamma_{BU} l(d_{BU})) \\ &= \exp\{-2\pi p \lambda_B (\gamma_{BU})^{2/\alpha} d_{BU}^2 \frac{\pi}{\alpha \sin(2\pi/\alpha)}\}, \end{aligned} \quad (5.8)$$

where we used the assumption that $h \sim \text{Exp}(1)$, $\mathcal{L}(\cdot)$ is the Laplace transform evaluated in (5.6).

5.3.2.2 Coverage Probability of 2-hop Transmission

As mentioned earlier, based on the distance between the user and its associated base station, in case where $d_{BU} > r_{BS}$, the user may attempt to connect to the BS with the help of the RS. Therefore, the coverage probability of the downlink transmission from the base station to the relay station (i.e., BS-RS link) can be expressed as:

$$\begin{aligned} P_{c,BR}(\gamma_{BR} \mid d_{BR}) &= \Pr\{\text{SINR}_{BR} > \gamma_{BR}\} \\ &= \exp\{-2\pi p \lambda_B (\gamma_{BR})^{2/\alpha} d_{BR}^2 \frac{\pi}{\alpha \sin(2\pi/\alpha)}\}. \end{aligned} \quad (5.9)$$

Once the data is decoded correctly at the RS, the RS further forwards it to the intended user. The coverage probability of the RS-EU link can be expressed as:

$$\begin{aligned} P_{c,RU}(\gamma_{RU} \mid d_{RU}) &= \Pr\{\text{SINR}_{RU} > \gamma_{RU}\} \\ &= \exp\{-2\pi p \lambda_B (\gamma_{RU})^{2/\alpha} d_{RU}^2 \frac{\pi}{\alpha \sin(2\pi/\alpha)}\}. \end{aligned} \quad (5.10)$$

Assuming the two links are independent, then the coverage probability of the 2-hop transmission can be obtained as:

$$\begin{aligned} P_{c,BRU}(\gamma_{BU}, \gamma_{RU} \mid d_{BR}, d_{RU}) &= \Pr\{\text{SINR}_{BU} > \gamma_{BU}\} \Pr\{\text{SINR}_{RU} > \gamma_{RU}\} \\ &= \exp\{-2\pi p \lambda_B (\tilde{\gamma})^{2/\alpha} \frac{\pi}{\alpha \sin(2\pi/\alpha)} \\ &\quad \times \left((\gamma_{BU})^{2/\alpha} d_{BR}^2 + (\gamma_{RU})^{2/\alpha} d_{RU}^2 \right)\}. \end{aligned} \quad (5.11)$$

Without loss of generality, let the required SINR thresholds for both links be the same, i.e., $\gamma_{BU} = \gamma_{RU} = \tilde{\gamma}$, then $P_{c,BRU}$ can be simplified to:

$$\begin{aligned} P_{c,BRU}(\tilde{\gamma} \mid d_{BU}, r) &= \exp\{-2\pi p \lambda_B(\tilde{\gamma})^{2/\alpha} \frac{\pi}{\alpha \sin(2\pi/\alpha)} (d_{BR}^2 + d_{RU}^2)\} \\ &= \exp\{-2\pi p \lambda_B(\tilde{\gamma})^{2/\alpha} \frac{\pi}{\alpha \sin(2\pi/\alpha)} (d_{BU}^2/2 + 2r^2)\}, \end{aligned} \quad (5.12)$$

which can be averaged over r to yield:

$$\begin{aligned} \bar{P}_{c,BRU}(\tilde{\gamma} \mid d_{BU}) &= \int_0^\infty P_{c,BRU}(\tilde{\gamma} \mid d_{BU}, r) f_r(r) dr \\ &= \frac{\lambda_R}{\beta + \lambda_R} e^{-\pi \beta d_{BU}^2/4}, \end{aligned} \quad (5.13)$$

where $\beta = 4p \lambda_B(\tilde{\gamma})^{2/\alpha} \frac{\pi}{\alpha \sin(2\pi/\alpha)}$.

Hence, the coverage probability of the relay-assisted system can be expressed as:

$$P_c = \begin{cases} P_{c,BU}(\gamma_{BU} \mid d_{BU}), & d_{BU} \leq r_{BS}, \\ \bar{P}_{c,BRU}(\tilde{\gamma} \mid d_{BU}), & d_{BU} > r_{BS}. \end{cases} \quad (5.14)$$

5.3.3 Achievable Transmission Rate

Here, we consider the successful achievable rate in the downlink relay-assisted networks.

According to Shannon-Hartley theorem, given $\text{SINR} = \gamma$, the maximum rate of information that can be reliably sent over a given link with unit bandwidth (i.e., spectral efficiency in bit/s/Hz) is $\log_2(1 + \gamma)$. As a result, the successful transmission per subcarrier at rate

$\log_2(1 + \gamma_{BU})$ for the BS-EU link can be obtained as:

$$\begin{aligned} R_{b,BU} &= \Delta f \log_2(1 + \gamma_{BU}) P_{c,BU}(\gamma_{BU} \mid d_{BU}) \\ &= \Delta f \log_2(1 + \gamma_{BU}) e^{-2\pi p \lambda_B (\gamma_{BU})^{2/\alpha} d_{BU}^2 \frac{\pi}{\alpha \sin(2\pi/\alpha)}}. \end{aligned} \quad (5.15)$$

Similarly, the achievable rate for the 2-hop transmission can be obtained as:

$$\begin{aligned} R_{b,BRU} &= \frac{1}{2} \Delta f \log_2(1 + \tilde{\gamma}) \bar{P}_{c,BRU}(\tilde{\gamma} \mid d_{BU}) \\ &= \frac{\lambda_R \Delta f}{2(\beta + \lambda_R)} \log_2(1 + \tilde{\gamma}) e^{-\pi \beta d_{BU}^2 / 4}. \end{aligned} \quad (5.16)$$

Note that the rate for the relay-based transmission is half that of the direct transmission because the data requires two time slots to reach the destination for the 2-hop transmission.

The achievable transmission rate for the relay-assisted system can be expressed as:

$$R_b = \begin{cases} R_{b,BU}, & d_{BU} \leq r_{BS}, \\ R_{b,BRU}, & d_{BU} > r_{BS}. \end{cases} \quad (5.17)$$

5.4 Blocking Probability Analysis

In this section, we investigate the blocking probability of the relay-assisted system. First, we model the traffic of the users and classify them into different classes based on their required subcarriers. We consider the queueing system to be multi-dimensional with multiple classes. Then, we calculate the blocking probability using the multi-dimensional loss model.

5.4.1 Resource Allocation and Traffic Modeling

In OFDMA networks, users are assigned different number of subcarriers to fulfill their rate requirements. In fact, even if all users request the same predefined rate R , due to the relative distances between the users and the base station, some users would experience poor SINR levels and hence would require more subcarriers to satisfy their transmission requirements. To see this, let R be the rate achieved using M subcarriers on the BS-UE link. Then, from (5.15), we have:

$$R = \Delta f \sum_{i=1}^M \log_2(1 + \gamma_{BU,i}) P_{c,BU}(\gamma_{BU,i} | d_{BU}). \quad (5.18)$$

Assume that the SINR targets are equal for all M subcarriers, then, M can be expressed as:

$$\begin{aligned} M &= \frac{R}{\Delta f \log_2(1 + \gamma_{BU}) P_{c,BU}(\gamma_{BU} | d_{BU})} \\ &= \frac{R}{\Delta f \log_2(1 + \gamma_{BU}) e^{-2\pi p \lambda_B (\gamma_{BU})^{2/\alpha} d_{BU}^2 \frac{\pi}{\alpha \sin(2\pi/\alpha)}}}. \end{aligned} \quad (5.19)$$

It is clear that, for given R and γ_{BU} , as the distance between the base station and the user increases, M also increases. That is, under the same data rate requirement R , users that are close to the base station need fewer subcarriers, while users that are far away need more subcarriers to compensate for the low RSS. This explains why cell-edge users consume more resources than the cell-center users.

Motivated by the observation above, we can classify the incoming users into different classes based on their subcarrier requirements, or alternatively based on their relative distances to the base station, as follows. First, let the entire distance range be divided into L non-overlapping consecutive intervals/classes, denoted by C_j , $j = 1, 2, \dots, L$. Thus, a user at a distance d_{BU} from its serving base station in the range $[d_{BU,j-1}, d_{BU,j})$ belongs to

class C_j . We refer to this user as class- j user. Second, each class will be allocated a certain number of subcarriers to satisfy its rate requirement. Without loss of generality, we assign M_j subcarriers to class C_j , where M_j is the mean number of subcarriers required to achieve the rate R for d_{BU} in the range $[d_{BU,j-1}, d_{BU,j})$.

Define $P(C_j \mid d_{BU} \leq r_{BS})$ as the probability that an arriving user belongs to class C_j and requires M_j subcarriers given that it is located within the base station coverage region, which can be obtained as:

$$\begin{aligned}
P(C_j \mid d_{BU} \leq r_{BS}) &= P(d_{0,j-1} \leq d_{BU} < d_{0,j} \mid d_{BU} \leq r_{BS}) \\
&= \frac{P(d_{0,j-1} \leq d_{BU} < d_{0,j}, d_{BU} \leq r_{BS})}{P(d_{BU} \leq r_{BS})} \\
&= \frac{\int_{\min(d_{0,j-1}, r_{BS})}^{\min(d_{0,j}, r_{BS})} f_{d_{BU}}(d_{BU}) dd_{BU}}{\int_0^{r_{BS}} f_{d_{BU}}(d_{BU}) dd_{BU}} \\
&= \frac{e^{-\lambda_B \pi \min(d_{0,j-1}^2, r_{BS}^2)} - e^{-\lambda_B \pi \min(d_{0,j}^2, r_{BS}^2)}}{1 - e^{-\lambda_B \pi r_{BS}^2}}, \tag{5.20}
\end{aligned}$$

where $f_{d_{BU}}(d_{BU}) = 2\pi\lambda_B d_{BU} e^{-\lambda_B \pi d_{BU}^2}$ is the PDF of the distance between a user and its nearest base station. $d_{0,j-1}$ and $d_{0,j}$, which can be calculated from (5.19), represent the distances between the user and the base station to achieve the rate R with M_{j-1} and M_j , respectively. $P(C_j \mid d_{BU} > r_{BS})$ can be calculated similarly.

Using the law of total probability, the probability that a new user belongs to class C_j

and requires M_j subcarriers can be obtained as:

$$P(C_j) = e^{-\lambda_B \pi \min(d_{0,j-1}^2, r_{BS}^2)} - e^{-\lambda_B \pi \min(d_{0,j}^2, r_{BS}^2)} \\ + e^{-\lambda_B \pi \max(d_{1,j-1}^2, r_{BS}^2)} - e^{-\lambda_B \pi \max(d_{1,j}^2, r_{BS}^2)}. \quad (5.21)$$

5.4.2 Blocking Probability Calculation

We assume that users arrive to the network according to a Poisson process with mean arrival rate λ , and depart with service rate μ , in which the service times (holding times) are independently and exponentially distributed with mean $\frac{1}{\mu}$.

As discussed earlier, based on the users rate requirements, each user is allocated, by the base station, a certain number of subcarriers from the total N subcarriers. That is, a class- j user would be assigned M_j subcarriers. If the available number of subcarriers is less than M_j , then this user will be blocked from accessing the network and may try later. Therefore, a blocking occurs when a user is denied of service due to the insufficient network resources. Since each user can request multiple subcarriers and release them simultaneously upon the completion of the service, then the relay-assisted system can be modeled using multi-dimensional Markov chains. More specifically, let λ_j denote the arrival rate of the users belonging to class C_j and requesting M_j subcarriers to meet their rate requirements. In this case, $\lambda_j = P(C_j)\lambda$, where $P(C_j)$ obtained in (5.21). Note that $\lambda = \sum_j \lambda_j$ for $j = 1, 2, \dots, L$.

The state space (i.e., the set of all allowable states) of the existing users in the system can be expressed as:

$$S = \{\mathbf{n} : \sum_{j=1}^L n_j M_j \leq N\}, \quad (5.22)$$

where $\mathbf{n} = (n_1, n_2, \dots, n_L)$ represents a state with n_1 users from class C_1 , n_2 users from class C_2 , and so on, that satisfies the inequality in (5.22).

The stationary distribution of $\mathbf{n}$ can be expressed in a product form as [67]:

$$\pi(\mathbf{n}) = \frac{1}{G(N, L)} \prod_{j=1}^L \frac{\rho_j^{n_j}}{n_j!}, \quad (5.23)$$

where

$$G(N, L) = \sum_{\mathbf{n} \in S} \prod_{j=1}^L \frac{\rho_j^{n_j}}{n_j!}, \quad \rho_j = \frac{\lambda_j}{\mu}. \quad (5.24)$$

Now, since the system has multiple classes and each class requires a certain number of subcarriers, then each class experiences different blocking probability. Let $P_{B,j}$ denote the class C_j blocking probability, which is the probability that a class- j user arrives and finds less than M_j subcarriers available in the system. $P_{B,j}$ can be obtained as:

$$P_{B,j} = \sum_{\mathbf{n} \in S_j} \pi(\mathbf{n}), \quad (5.25)$$

where $S_j = \{\mathbf{n} : N - M_j < \sum_{j=1}^L n_j M_j \leq N\}$ denotes the set of blocking states for class- j user.

The entire system blocking probability P_B can be obtained as:

$$P_B = \frac{1}{\rho} \sum_{j=1}^L \rho_j P_{B,j}, \quad (5.26)$$

where $\rho = \frac{\lambda}{\mu} = \sum_j \rho_j$ is the utilization factor.

Due to the large state space of the system, which is generally in the order of $\mathcal{O}(N^L)$, computing the blocking probability in (5.25) directly is computationally inefficient. Therefore, to

reduce the computational complexity, for numerical evaluation, we use a recursive algorithm, known as Kaufman-Roberts algorithm [68, 69], to calculate the blocking probability.

Table 5.1: Simulation Parameters

Number of subcarriers N	256
Number of classes L	200
Predefined rate R	0.2 Mbps
Subcarrier bandwidth Δf	180 KHz
Base stations intensity λ_B	$1 \times 10^{-5}/\text{m}^2$
Relay stations intensity λ_R	$1 \times 10^{-5}/\text{m}^2$
Base station activity factor p	1
SINR thresholds $\gamma_{BU} = \tilde{\gamma}$	5 dB
Mean arrival rate λ	3
Mean service rate μ	1
Path loss exponent α	4

5.5 Simulation Results

In this section, we carry out the QoS performance analysis of relay-assisted system based on the proposed method for BP evaluation. More specifically, first, we obtain the optimal value of r_{BS} , denoted by $r_{BS,Opt}$, that minimizes the system blocking probability P_B . Then, using $r_{BS,Opt}$, we calculate the class distribution as well as the class blocking probability. The simulation parameters are listed in Table 5.1.

Example 1: The optimal base station range In this example, we obtain $r_{BS,Opt}$ that achieves minimum blocking probability P_B , as shown in Figure 5.3. It can be seen that for small values of r_{BS} , the blocking probability is relatively high since most of the users communicate with the base station indirectly through the relay stations. As r_{BS} starts increasing, more users will be located inside the base station coverage region and establish a direct connection with the base station, which reduces the blocking probability. When r_{BS}

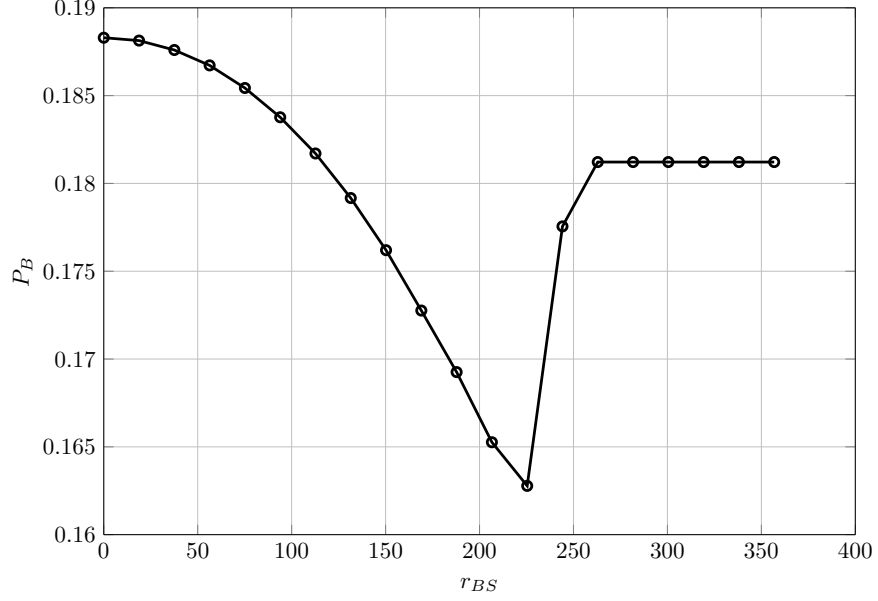


Figure 5.3: Example 1: The system blocking probability P_B versus r_{BS} . Here, $r_{BS,Opt} = 225.36$ m.

becomes larger, P_B starts increasing again, since the users that are far away would connect to the base station directly, but have low coverage probability. Thus, more network resources would be released for such users to meet their service requirements. It can also be observed that, when r_{BS} is very large, P_B stays constant. In this case, all users are located within the base station coverage area.

From the discussions above, it is concluded that deploying relay stations along with the base stations extend the coverage area and improve the QoS, i.e., reduce the blocking probability.

Example 2: Class distribution and class blocking probability Using $r_{BS,Opt}$ obtained in **Example 1**, first, we evaluate the distribution of the number of subcarriers that an arriving user requires to meet its rate requirement. Then, based on this distribution, we calculate the class blocking probability $P_{B,j}$, as depicted in Figure 5.4. It can be noted from Figure 5.4 that as the group size of the number of subcarriers increases, the class

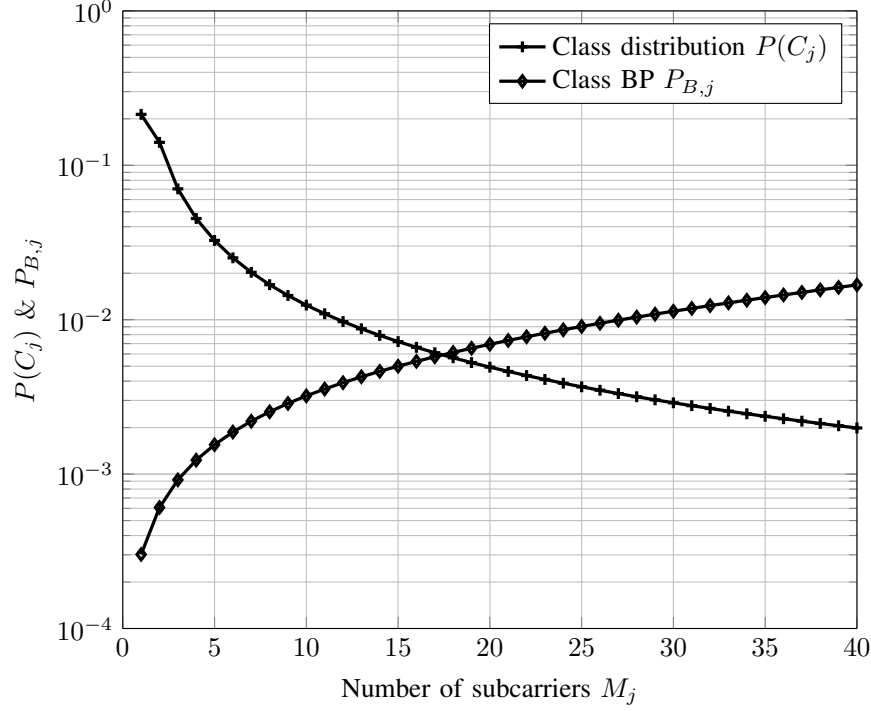


Figure 5.4: Example 2: Class distribution and class blocking probability versus M_j using $r_{BS,Opt} = 225.36$ m.

probability decreases. This is in contrast with most of the existing work, which assumes uniform distribution [36–38]. It can also be seen from Figure 5.4 that the class blocking probability $P_{B,j}$ is a monotonically decreasing function with the class sizes, since users that are requiring large number of subcarriers are more likely to be blocked than those that are requiring fewer subcarriers.

5.6 Summary

In this chapter, we studied blocking probability in relay-assisted OFDMA networks using stochastic geometry. First, we modeled the inter-cell interference from the neighboring cells at a typical node. Second, we derived the coverage probability in the downlink transmissions, including both the direct and relay-based transmissions. Third, we classified the incoming

users into different classes based on their subcarrier requirements, and calculated the system blocking probability. It was shown that, with the relay-assisted system, the blocking probability can be reduced and therefore the network performance can be improved.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

IoT is the next impetus in the development of new wireless networks. The main challenges here lie in effective spectrum sharing, high network density, and the scarce energy budget and the low cost requirements of IoT applications.

We tried to address these challenges from three aspects: (1) Secure and effective spectrum sharing in the lower frequency bands; (2) Energy efficient transmission for IoT devices through energy harvesting; and (3) QoS evaluation in the high density IoT networks. The main conclusions are summarized in the following.

First, we developed a secure and efficient spectrum sharing scheme in the HDTV bands. We started with single-carrier transmission, where the signal is processed in the entire spectrum and hence allows full-band detection. In Chapter 2, we considered full-band PUEA detection and proposed a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the DTV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve full-band identification of authorized PUs. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the MU can be detected accurately no matter the primary user is present or not. It was shown that with the AES-assisted DTV scheme, both the PU

and MU can be detected with high accuracy and low false alarm rate under PUEA.

We further developed a secure and efficient spectrum sharing scheme in multi-carrier wireless networks. In Chapter 3, we considered sub-band PUEA detection in the OFDM-based CR networks. We proposed an efficient AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm for accurate sub-band PU and MU detection. With the proposed scheme, we can detect PUEA accurately over all subcarriers or sub-bands where the P2 symbols present. Numerical results showed that with the AES-based DTV scheme, both the PU and MU can be detected accurately under PUEA. Potentially, the proposed scheme can be applied directly to future IoT networks for more efficient spectrum sharing with the existing lower band systems.

Then, in Chapter 4, we first proposed an effective communication scheme for the SUs under PUEA by exploiting the energy harvesting techniques. Optimal power splitting was considered for sum-rate maximization. It was observed that the sum-rate of the SU network can be improved significantly with the energy harvesting technique. Then, we evaluated the worst-case PUEA interference in terms of minimizing the sum-rate for the SUs. We showed that for practical systems, as CSI among the SUs is not available to the malicious user, the worst jamming for the SUs is when the MU performs equal power allocation over all the white space subcarriers. Simulation results were provided to illustrate the proposed approaches. In addition to the jamming scenario, energy harvesting can be applied in the benign environment as well to resolve the energy scarcity in the IoT networks.

Finally, in Chapter 5, taking the spatial randomness of the IoT network into consideration, we investigated coverage probability and blocking probability in relay-assisted OFDMA networks using stochastic geometry. More specifically, we modeled the inter-cell interference

from the neighboring cells at each typical node, and derived the coverage probability in the downlink transmissions, including both the direct and relay-based transmissions. Based on their data rate requirements, we classified the incoming users into different classes, and calculated the blocking probability using the multi-dimensional loss model. It was shown that the blocking probability can be reduced by exploiting relay-assisted transmissions.

6.2 Future Work

We propose the following directions for future research.

Security enhancement for IoT nodes under malicious attacks

In Chapters 2 and 3, we proposed secure and efficient spectrum sharing schemes that can enable IoT nodes to accurately identify the malicious attacks. For effective transmission, however, they can adopt different methodologies such as:

- *Avoid transmission on the white spaces jammed by malicious nodes.* For example, consider the case where the IoT nodes are OFDM-based transceivers, then they can shape their transmitted signal through proper precoding design to avoid communication over the jammed subcarriers. We plan to carry out more research on this by exploiting secure symbol-level coding, which can provide more design flexibility under hostile jamming. For time-varying attacks, the precoder should be adapted accordingly for transmission. This necessitates that jamming detection needs to be performed in real-time, which can generally be achieved by evaluating the time-varying power spectrum of the jamming signal.
- *Exploit techniques that are inherently jamming-resistant,* such as code division multiple access (CDMA) and frequency hopping (FH) techniques. Both CDMA and FH were

initially developed for secure military communications. CDMA is particularly efficient under narrow-band jamming [70], even if the malicious user hops from band to band. FH based systems are generally robust under wide-band jamming. Further research can be conducted to develop a secure subcarrier allocation scheme for secure and collision-free transmission between the secondary users. When the malicious jamming pattern is time-varying, i.e., the malicious user switches between wide-band and narrow-band jamming, the transmitter then needs to be adjusted to combat the cognitive hostile attacks.

Reliable IoT network design and performance evaluation under hostile environments

We will consider to develop new techniques to detect erroneous transmissions in multi-hop networks, and examine whether it is a node failure or link failure. We will evaluate the impacts of different nodes on the network, and aim to perform quantitative analysis on network throughput and reliability. We will also consider the development of more effective routing protocol design to enhance network performance and reliability.

QoS performance analysis for CR networks under PUEA

In Chapter 5, taking the spatial randomness of the IoT network into consideration, we investigated blocking probability in relay-assisted OFDMA networks using stochastic geometry. It was shown that the blocking probability can be reduced by exploiting relay-assisted transmissions. Motivated by this observation, we plan to study blocking probability in CR networks under PUEA for both single-hop and multi-hop transmission schemes.

APPENDIX

Appendix

Proof of Parameters used in Section

3.3.3

In this appendix, we calculate μ_{00} , σ_{00} , μ_{01} , σ_{01} , μ_{10} , σ_{10} , μ_{11} , σ_{11} , and the optimal values for $T_{k,0}$ and $T_{k,1}$.

Under H_{00} , both the primary user and malicious user are absent, resulting in $\mathbf{r}_{k,i} = \mathbf{n}_{k,i}$.

It follows that:

$$\begin{aligned}\mu_{00} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M \mathbf{n}_{k,i} \mathbf{n}_{k,i}^* \right\} \\ &= \sigma_n^2,\end{aligned}\tag{.1}$$

and σ_{00}^2 can be obtained as:

$$\begin{aligned}\sigma_{00}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{00}|^2 \\ &= \frac{1}{M} \left[\mathbb{E} \{ |\tilde{\mathbf{n}}_k|^4 \} - (\sigma_n^2)^2 \right],\end{aligned}\tag{.2}$$

where we assume that $\mathbb{E}\{|\mathbf{n}_{k,i}|^4\} = \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} \forall i$. Similarly, under H_{01} , the received signal is

represented as $\mathbf{r}_{k,i} = \mathbf{m}_{k,i} + \mathbf{n}_{k,i}$, and the mean μ_{01} can be obtained as follows:

$$\begin{aligned}\mu_{01} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M (\mathbf{m}_{k,i} + \mathbf{n}_{k,i})(\mathbf{m}_{k,i} + \mathbf{n}_{k,i})^* \right\} \\ &= \sigma_{m,k}^2 + \sigma_n^2.\end{aligned}\tag{.3}$$

The variance σ_{01}^2 can be obtained as:

$$\begin{aligned}\sigma_{01}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{01}|^2 \\ &= \frac{1}{M} \left[\mathbb{E}\{|\tilde{\mathbf{m}}_k|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}_k|^4\} + \mathbb{E}\{2\Re\{(\tilde{\mathbf{m}}_k)^2(\tilde{\mathbf{n}}_k^*)^2\}\} \right. \\ &\quad \left. + 2\sigma_{m,k}^2\sigma_n^2 - (\sigma_{m,k}^2)^2 - (\sigma_n^2)^2 \right],\end{aligned}\tag{.4}$$

where we assume that $\mathbb{E}\{|\mathbf{m}_{k,i}|^4\} = \mathbb{E}\{|\tilde{\mathbf{m}}|^4\}$, $\mathbb{E}\{|\mathbf{n}_{k,i}|^4\} = \mathbb{E}\{|\tilde{\mathbf{n}}|^4\}$, $\mathbb{E}\{2\Re\{(\mathbf{m}_{k,i})^2(\mathbf{n}_{k,i}^*)^2\}\} = \mathbb{E}\{2\Re\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\}$, $\forall i$.

Under H_{10} , the received signal is expressed as $\mathbf{r}_{k,i} = \sqrt{l_{d1}P_{s,k}}|h_k|\mathbf{s}_{k,i} + \mathbf{n}_{k,i}$, and the mean μ_{10} can be obtained as follows:

$$\begin{aligned}\mu_{10} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M (\tilde{C}_k \mathbf{s}_{k,i} + \mathbf{n}_{k,i})(\tilde{C}_k \mathbf{s}_{k,i} + \mathbf{n}_{k,i})^* \right\} \\ &= \tilde{C}_k^2 + \sigma_n^2,\end{aligned}\tag{.5}$$

where $\tilde{C}_k = \sqrt{l_{d1}P_{s,k}}|h_k|$. The variance σ_{10}^2 can be obtained as:

$$\begin{aligned}
\sigma_{10}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{10}|^2 \\
&= \frac{1}{M} \left[\tilde{C}_k^4 \mathbb{E}\{|\tilde{\mathbf{s}}_k|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}_k|^4\} + \mathbb{E}\{2\tilde{C}_k^2 \mathbb{R}\{(\tilde{\mathbf{s}}_k)^2(\tilde{\mathbf{n}}_k^*)^2\}\} \right. \\
&\quad \left. + 2\tilde{C}_k^2 \sigma_n^2 - \tilde{C}_k^4 - (\sigma_n^2)^2 \right]. \tag{.6}
\end{aligned}$$

Similarly, under H_{11} , the received signal is represented as $\mathbf{r}_{k,i} = \sqrt{l_{d1}P_{s,k}}|h_k|\mathbf{s}_{k,i} + \mathbf{m}_{k,i} + \mathbf{n}_{k,i}$, and the mean μ_{11} can be obtained as follows:

$$\mu_{11} = \tilde{C}_k^2 + \sigma_{m,k}^2 + \sigma_n^2, \tag{.7}$$

and σ_{11}^2 can be obtained as:

$$\begin{aligned}
\sigma_{11}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{11}|^2 \\
&= \frac{1}{M} \left[\tilde{C}_k^4 \mathbb{E}\{|\tilde{\mathbf{s}}_k|^4\} + \mathbb{E}\{|\tilde{\mathbf{m}}_k|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}_k|^4\} \right. \\
&\quad + 2\tilde{C}_k^2 \mathbb{E}\{\mathbb{R}\{(\tilde{\mathbf{s}}_k)^2(\tilde{\mathbf{m}}_k^*)^2\}\} + 2\tilde{C}_k^2 \mathbb{E}\{\mathbb{R}\{(\tilde{\mathbf{s}}_k)^2(\tilde{\mathbf{n}}_k^*)^2\}\} \\
&\quad + 2\mathbb{E}\{\mathbb{R}\{(\tilde{\mathbf{m}}_k)^2(\tilde{\mathbf{n}}_k^*)^2\}\} + 2\tilde{C}_k^2 \sigma_{m,k}^2 + 2\tilde{C}_k^2 \sigma_n^2 \\
&\quad \left. + 2\sigma_{m,k}^2 \sigma_n^2 - \tilde{C}_k^4 - (\sigma_{m,k}^2)^2 - (\sigma_n^2)^2 \right]. \tag{.8}
\end{aligned}$$

Similar to the threshold for primary user detection, following the minimum distance rule, we choose $T_{k,0} = (\sigma_{m,k}^2 + 2\sigma_n^2)/2$ and $T_{k,1} = (2l_{d1}P_{s,k}|h_k|^2 + \sigma_{m,k}^2 + 2\sigma_n^2)/2$ as the thresholds for malicious user detection.

BIBLIOGRAPHY

BIBLIOGRAPHY

- [1] Federal Communications Commission, “Spectrum policy task force report,” *ET Docket No. 02-135*, November 2002.
- [2] B. Wang and K. J. R. Liu, “Advances in cognitive radio networks: A survey,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5–23, Feb 2011.
- [3] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.
- [4] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006.
- [5] M. Thanu, “Detection of primary user emulation attacks in cognitive radio networks,” in *International Conference on Collaboration Technologies and Systems (CTS)*, May 2012, pp. 605–608.
- [6] Federal Communications Commission, “Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band,” *ET Docket No. 04-186 and 02-380*, September 2010.
- [7] R. Chen and J.-M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, Sept. 2006, pp. 110–119.
- [8] T. Clancy and N. Goergen, “Security in cognitive radio networks: Threats and mitigation,” in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. Conference on 3rd International*, May 2008, pp. 1–8.
- [9] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.
- [10] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE on Symposium*, 2008, pp. 1–6.

- [11] N. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1432–1445, 2012.
- [12] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
- [13] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2011, pp. 599–604.
- [14] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.
- [15] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *IEEE International Conference on Communications*, June 2009, pp. 1–5.
- [16] —, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, 2009.
- [17] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.
- [18] M. Dang, Z. Zhao, and H. Zhang, "Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks," in *International Conference on Wireless Communications & Signal Processing (WCSP)*, Oct 2013, pp. 1–5.
- [19] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting mobile primary user emulation attack in white space," in *Proceedings IEEE INFOCOM*, April 2011, pp. 36–40.
- [20] S. Jana, K. Zeng, W. Cheng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1497–1507, Sept 2013.

- [21] S. L. Ho, J. Wang, W. N. Fu, and M. Sun, "A comparative study between novel witricity and traditional inductive magnetic coupling in wireless charging," *IEEE Transactions on Magnetics*, vol. 47, no. 5, pp. 1522–1525, May 2011.
- [22] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless charging technologies: Fundamentals, standards, and network applications," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1413–1452, Secondquarter 2016.
- [23] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 317, no. 5834, pp. 83–86, 2007. [Online]. Available: <http://science.sciencemag.org/content/317/5834/83>
- [24] L. Varshney, "Transporting information and energy simultaneously," in *IEEE International Symposium on Information Theory*, July 2008, pp. 1612–1616.
- [25] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989–2001, May 2013.
- [26] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, November 2013.
- [27] C. Mikeka and H. Arai, *Design issues in radio frequency energy harvesting system*. INTECH Open Access Publisher, 2011.
- [28] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 757–789, Secondquarter 2015.
- [29] D. Ng, E. Lo, and R. Schober, "Energy-efficient resource allocation in multiuser OFDM systems with wireless information and power transfer," in *IEEE Wireless Communications and Networking Conference (WCNC)*, April 2013, pp. 3823–3828.
- [30] D. Li, C. Shen, and Z. Qiu, "Sum rate maximization and energy harvesting for two-way af relay systems with imperfect CSI," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2013, pp. 4958–4962.
- [31] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4788–4799, September 2013.

- [32] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Opportunistic channel access and RF energy harvesting in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2039–2052, November 2014.
- [33] A. Sultan, "Sensing and transmit energy optimization for an energy harvesting cognitive radio," *IEEE Wireless Communications Letters*, vol. 1, no. 5, pp. 500–503, 2012.
- [34] A. Shafie and A. Sultan, "Optimal random access for a cognitive radio terminal with energy harvesting capability," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1128–1131, June 2013.
- [35] S. Park, H. Kim, and D. Hong, "Cognitive radio networks with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1386–1397, March 2013.
- [36] J.-C. Chen and W.-S. E. Chen, "Call blocking probability and bandwidth utilization of OFDM subcarrier allocation in next-generation wireless networks," *IEEE Communications Letters*, vol. 10, no. 2, pp. 82–84, Feb 2006.
- [37] V. Pla, J. Martinez-Bauset, and V. Casares-Giner, "Comments on "call blocking probability and bandwidth utilization of OFDM subcarrier allocation in next-generation wireless networks",," *IEEE Communications Letters*, vol. 12, no. 5, pp. 349–349, May 2008.
- [38] C. Paik and Y. S. Suh, "Generalized queueing model for call blocking probability and resource utilization in OFDM wireless networks," *IEEE Communications Letters*, vol. 15, no. 7, pp. 767–769, July 2011.
- [39] M. Mehta, R. B. Jain, and A. Karandikar, "Analysis of blocking probability in a relay-based cellular OFDMA network," *Wireless Personal Communications*, vol. 84, no. 4, pp. 2467–2492, 2015.
- [40] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, November 2011.
- [41] W. Lu and M. D. Renzo, "Stochastic geometry modeling and system-level analysis & optimization of relay-aided downlink cellular networks," *IEEE Transactions on Communications*, vol. 63, no. 11, pp. 4063–4085, Nov 2015.

- [42] P. H. J. Nardelli, P. Cardieri, and M. Latva-aho, "Efficiency of wireless networks under different hopping strategies," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 15–20, January 2012.
- [43] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 996–1019, Third 2013.
- [44] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An aloha protocol for multihop mobile wireless networks," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 421–436, Feb 2006.
- [45] AT32UC3A3256S. [Online]. Available: <http://www.atmel.com/devices/at32uc3a3256s.aspx>
- [46] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbaughede, "A 3.84 Gbits/s AES crypto coprocessor with modes of operation in a 0.18- μm CMOS technology," in *Proceedings of the 15th ACM Great Lakes symposium on VLSI*. New York, NY, USA: ACM, 2005, pp. 60–63.
- [47] S.-Y. Lin and C.-T. Huang, "A high-throughput low-power AES cipher for network applications," in *Design Automation Conference*, 2007, pp. 595–600.
- [48] J. Adda and M. Ottaviani, "Digital television 1: The transition to digital television *," September 2004.
- [49] Advanced Television Systems Committee, "A/53: ATSC digital television standard, part 2," Tech. Rep., Dec. 2011.
- [50] V.-H. Pham, J.-Y. Chouinard, A. Semmar, X. Wang, and Y. Wu, "Enhanced ATSC DTV channel estimation," in *Canadian Conference on Electrical and Computer Engineering*, May 2009, pp. 772–776.
- [51] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Prentice Hall, Jan. 2010.
- [52] C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, 2007, pp. 1037–1041.

- [53] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013, pp. 2935–2939.
- [54] W. Burr, "Selecting the advanced encryption standard," *IEEE Security Privacy*, vol. 1, no. 2, pp. 43–52, Mar 2003.
- [55] T. Good and M. Benaissa, "AES as stream cipher on a small FPGA," in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE on International Symposium*, 2006, pp. 4 pp.–.
- [56] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," in *International Journal of Computer Trends and Technology*, Aug. 2011.
- [57] D. Das and S. Das, "Primary user emulation attack in cognitive radio networks: A survey," *IRACST–International Journal of Computer Networks and Wireless Communications ISSN*, pp. 2250–3501, 2013.
- [58] C. yen Ong, J. Song, C. Pan, and Y. Li, "Technology and standards of digital television terrestrial multimedia broadcasting [topics in wireless communications]," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 119–127, May 2010.
- [59] Digital Video Broadcasting, "Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)," *ETSI Std. EN 302 755 V1.3.1*, April 2012.
- [60] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 82–88, August 2012.
- [61] N. Haller, "The S/KEY one-time password system," in *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, February 1994.
- [62] P. S. Mann, *Introductory Statistics*, 7th ed. Wiley, February 2010.
- [63] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," in *IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 3982–3987.
- [64] Z.-Q. Luo and W. Yu, "An introduction to convex optimization for communications and signal processing," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1426–1438, Aug 2006.

- [65] Z. Lin, Y. Li, S. Wen, Y. Gao, X. Zhang, and D. Yang, "Stochastic geometry analysis of achievable transmission capacity for relay-assisted device-to-device networks," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 2251–2256.
- [66] F. Baccelli and B. Blaszczyzyn, *Stochastic Geometry and Wireless Networks: Volume I Theory (Foundations and Trends(r) in Networking)*. Now Publishers Inc, 2009.
- [67] R. R. Mazumdar, "Performance modeling, loss networks, and statistical multiplexing," *Synthesis Lectures on Communication Networks*, vol. 2, no. 1, pp. 1–151, 2009.
- [68] J. Kaufman, "Blocking in a shared resource environment," *IEEE Transactions on Communications*, vol. 29, no. 10, pp. 1474–1481, Oct 1981.
- [69] J. W. Roberts, "A service system with heterogeneous user requirements," in *Performance of Data Communications systems and their applications*, vol. 29, no. 10. Amsterdam, The Netherlands: North-Holland, 1981, pp. 423–431.
- [70] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, Jul 2007. [Online]. Available: <http://jwcn.eurasipjournals.com/content/2007/1/083589>