

Subband PUEA Detection and Mitigation in OFDM-Based Cognitive Radio Networks

Ahmed Alahmadi, Zhaoxi Fang, Tianlong Song, and Tongtong Li, *Senior Member, IEEE*

Abstract—This paper considers malicious user detection and energy harvesting in orthogonal frequency division multiplexing-based cognitive radio networks under primary user emulation attack (PUEA). The digital TV (DTV) model adopted is the second generation terrestrial digital television standard (DVB-T2). In this paper, first, we propose an efficient advanced encryption standard (AES)-based DTV scheme, where the existing reference sequence used to generate the P2 pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm to facilitate accurate 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. Second, we come up with an effective communication scheme for the secondary users (SUs) under PUEA by exploiting the energy harvesting techniques. Optimal power splitting is considered for sum-rate maximization. As the optimal solution relies on multidimensional exhaustive search, we propose an effective suboptimal solution with much lower computational complexity. It is observed that the sum-rate of the SU network can be improved significantly with the energy harvesting technique. Third, we evaluate the worst case PUEA interference in terms of minimizing the sum-rate for the SUs. We show that for practical systems, as channel state information 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.

Index Terms—Cognitive radio networks, primary user emulation attack, energy harvesting, wireless security.

I. INTRODUCTION

COGNITIVE radio (CR) networking [1], [2] 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 (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) [3], [4], where a malicious user (MU) emulates the signal characteristics of the primary user, thereby causing the SUs to erroneously identify the attacker as the primary user. The quality-of-service (QoS) for the secondary users can be severely degraded by the presence of PUEA in CR networks [5].

To detect and defend against PUEA, several schemes have been proposed in literature [6]–[11]. In [6], a localization-based transmitter verification scheme was proposed. In [7] and [8], the authors proposed a received signal strength (RSS) 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 [9], 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 [10] 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 [11], 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 (DoA) 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.

On a parallel avenue, energy harvesting from ambient radio frequency signals has gained considerable attention in both industrial and academic fields [12]–[22]. The concept of simultaneous wireless information transfer and energy harvesting was first proposed in [12], where the fundamental trade-off between information receiving and power transfer was studied from an information theory perspective. In literature [13]–[15], 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

Manuscript received December 21, 2014; revised April 24, 2015 and June 17, 2015; accepted June 17, 2015. Date of publication June 29, 2015; date of current version August 6, 2015. This work was supported in part by the U.S. National Science Foundation under Grant CNS-1117831, Grant CNS-1217206, and Grant ECCS-1232109, and in part by the Natural Science Foundation of China under Grant 61401400. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. T. Charles Clancy.

A. Alahmadi is with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824 USA, and also with the Department of Electrical Engineering, Taibah University, Medina 30001, Saudi Arabia (e-mail: alahmadi@msu.edu).

Z. Fang is with the Department of Communication Engineering, Zhejiang Wanli University, Ningbo 100044, China (e-mail: zfang@msu.edu).

T. Song and T. Li are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: songtia6@msu.edu; tongli@msu.edu).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TIFS.2015.2450673

the RF band at the receiver. The received RF signal is splitted 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.

Recently, energy harvesting has been widely discussed in Orthogonal Frequency Division Multiplexing (OFDM) systems [16], wireless relay networks [17], and cognitive radio networks [18]–[22]. For example, the authors in [18] 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 [19], 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 [18]–[22]. 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 [23] and [24], we investigated full band PUEA detection in single-carrier transmission systems, where the primary user's signal is processed in the entire spectrum. In this paper, motivated by the prevalence of the OFDM-based digital TV (DTV) standard, we consider sub-band malicious user detection and energy harvesting assisted SU transmission in an OFDM-based CR network under PUEA. Here, the CR network consists of primary users (DTV transmitters), 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 Advanced Encryption Standard (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. If all the subcarriers are occupied by the primary user, the SUs harvest energy from the received RF signals of both the primary user and the malicious user. Otherwise, secondary users harvest energy and transmit their own signals over the white spaces according to the proposed energy harvesting scheme. Numerical results are presented to demonstrate the effectiveness of the PUEA detection approach, and the advantages of the energy harvesting scheme in comparison with its non-energy harvesting counterpart.

The main contributions of this paper can be summarized as:

- We propose an AES-based DTV scheme which can facilitate simple and accurate PUEA detection. 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.

- 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.
- 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 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.

The rest of the paper is organized as follows. Section II describes the system model of the proposed OFDM-based cognitive radio networks. Section III investigates the AES-based PUEA detection scheme. Section IV presents the secondary users energy harvesting and performance optimization schemes. Section V discusses the worst jamming interference in PUEA. Section VI provides the simulation results, and Section VII concludes the paper.

II. SYSTEM MODEL

A. The Proposed CR Network Architecture

We consider an OFDM-based cognitive radio network under PUEA, as shown in Figure 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 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

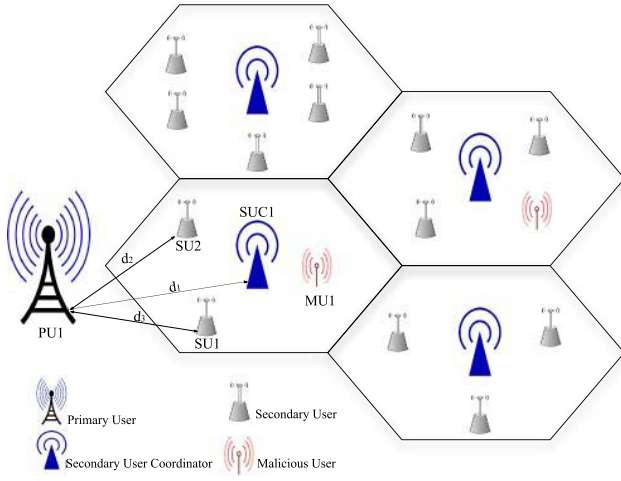


Fig. 1. The proposed cognitive radio network architecture.

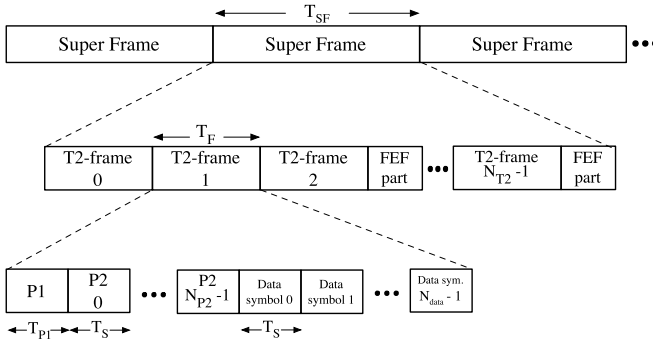


Fig. 2. The DVB-T2 frame structure.

case in most of the existing or future DTV systems [25]. 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 2 [26]. 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 [26]. In this paper, 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

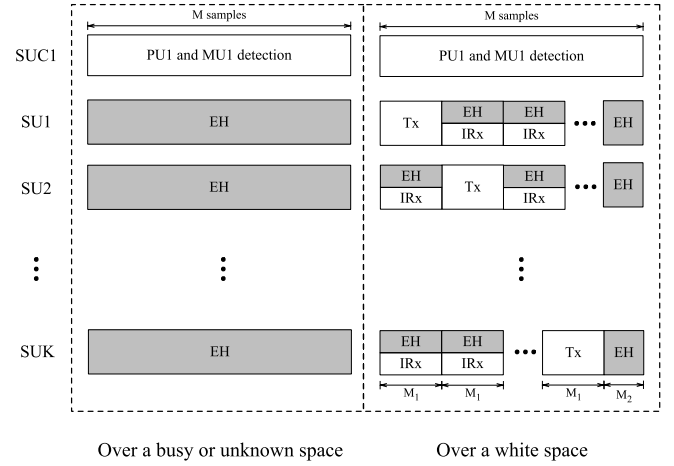


Fig. 3. The proposed energy harvesting scheme.

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 [27].

B. Energy Harvesting and Information Transfer Scheme

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.

Here, 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 efficient scheme for resource utilization between the secondary users, shown in Figure 3. In this scheme, we propose that SUC1 detects PU1 and MU1 using correlation

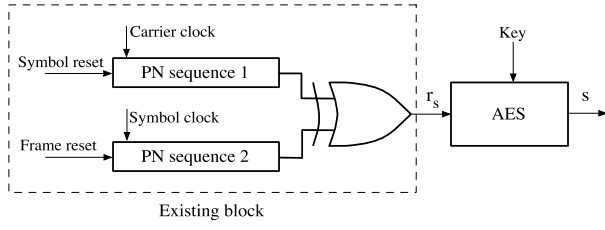


Fig. 4. Generation of the proposed reference signal s .

detectors after obtaining M samples of the received signal on the desired sub-channel (see Section III). 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 3. 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 [28]. 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.

III. 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.

A. Primary User Transmitter Design

The frequency indexes of P2 pilots are determined by:

$$\Omega = \{m \mid m \equiv 0 \pmod{3}, 0 \leq m \leq M_{\max}\}, \quad (1)$$

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 4 [26]. More details on the PN sequences generation can be found in [26].

In this paper, as illustrated in Figure 4, 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 s as follows:

$$s = E(\text{key}, \mathbf{r}_s), \quad (2)$$

where $E(\cdot, \cdot)$ denotes the AES encryption operation. It should be noted that the encrypted 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 [29], [30]. 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.

B. 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 III-C), 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 1, can be modeled as:

$$\mathbf{r}_k = \alpha_k \sqrt{l_{d1} P_{s,k}} |h_k| \mathbf{s}_k + \beta_k \mathbf{m}_k + \mathbf{n}_k, \quad (3)$$

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.

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:

$$\mathbf{R}_{r,s,k} = \frac{\langle \mathbf{r}_k, \mathbf{s}_k \rangle}{M} = \alpha_k \sqrt{l_{d1} P_{s,k}} |h_k|, \quad (4)$$

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.,

$$\hat{\mathbf{r}}_{rs,k} \triangleq \frac{1}{M} \sum_{i=1}^M \mathbf{r}_{k,i} \cdot \mathbf{s}_{k,i}^*, \quad (5)$$

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 (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.

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:

$$\mathbf{R}_{rr,k} = \frac{\langle \mathbf{r}_k, \mathbf{r}_k \rangle}{M} = \alpha_k l_{d1} P_{s,k} |h_k|^2 + \beta_k \sigma_{m,k}^2 + \sigma_n^2. \quad (6)$$

Based on the estimated value of α_k , β_k can be determined accordingly through (6). We have the following cases:

$$\mathbf{R}_{rr,k} = \begin{cases} l_{d1} P_{s,k} |h_k|^2 + \sigma_{m,k}^2 + \sigma_n^2, & \alpha_k = 1, \beta_k = 1 \\ l_{d1} P_{s,k} |h_k|^2 + \sigma_n^2, & \alpha_k = 1, \beta_k = 0 \\ \sigma_{m,k}^2 + \sigma_n^2, & \alpha_k = 0, \beta_k = 1 \\ \sigma_n^2, & \alpha_k = 0, \beta_k = 0 \end{cases} \quad (7)$$

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

$$\hat{\mathbf{R}}_{rr,k} \triangleq \frac{1}{M} \sum_{i=1}^M \mathbf{r}_{k,i} \cdot \mathbf{r}_{k,i}^*. \quad (8)$$

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.

C. 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.,

$$P_{f,k} = Pr(H_1|H_0), \quad (9)$$

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.,

$$P_{m,k} = Pr(H_0|H_1). \quad (10)$$

Note that the cross-correlation $\hat{\mathbf{r}}_{rs,k}$, defined in (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 [31]. 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:

$$P_{f,k} = Pr\{\hat{\mathbf{r}}_{rs,k} \geq T_k | H_0\} = Q\left(\frac{T_k - \mu_0}{\sigma_0}\right), \quad (11)$$

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

$$P_{m,k} = Pr\{\hat{\mathbf{r}}_{rs,k} < T_k | H_1\} = 1 - Q\left(\frac{T_k - \mu_1}{\sigma_1}\right). \quad (12)$$

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:

$$\tilde{P}_{f,k} = P_0 Q\left(\frac{T_{k,0} - \mu_{00}}{\sigma_{00}}\right) + (1 - P_0) Q\left(\frac{T_{k,1} - \mu_{10}}{\sigma_{10}}\right), \quad (13)$$

and

$$\tilde{P}_{m,k} = 1 - P_0 Q\left(\frac{T_{k,0} - \mu_{01}}{\sigma_{01}}\right) + (P_0 - 1) Q\left(\frac{T_{k,1} - \mu_{11}}{\sigma_{11}}\right), \quad (14)$$

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

D. 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 (11) and (12), we have:

$$P_{f,k} = Q(c\sqrt{M}), \quad (15)$$

and

$$P_{m,k} = 1 - Q(-c\sqrt{M}), \quad (16)$$

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

Discussions: Following (15) and (16), under reasonably high signal-to-noise ratio (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 $\lim_{M \rightarrow \infty} P_{f,k} = 0$.

IV. 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.

A. 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 3. 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 $M_1 = M/2$.

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:

$$\mathbf{r}_{2,n} = \alpha_n \sqrt{l_{d2}P_{s,n}} g_{2,n} \tilde{\mathbf{s}}_n + \gamma_{1,n} \sqrt{l_{d4}P_{1,n}} f_{1,n} \tilde{\mathbf{s}}_{1,n} + \beta_n \tilde{\mathbf{m}}_{2,n} + \tilde{\mathbf{n}}_{a,n}, \quad (17)$$

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, $\alpha_n, \beta_n, \gamma_{1,n}$ 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 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 (17), the total harvested power at SU2 can be obtained as:

$$P_{EH,2} = \eta \rho_2 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \gamma_{1,n} l_{d4} P_{1,n} |f_{1,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2) + N \sigma_a^2 \right], \quad (18)$$

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:

$$\tilde{\mathbf{r}}_{2,n} = \sqrt{(1 - \rho_2) l_{d4} P_{1,n}} f_{1,n} \tilde{\mathbf{s}}_{1,n} + \sqrt{1 - \rho_2} (\beta_n \tilde{\mathbf{m}}_{2,n} + \tilde{\mathbf{n}}_{a,n}) + \tilde{\mathbf{n}}_{b,n}, \quad n \in \mathcal{A}, \quad (19)$$

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

From (19), the achievable rate for the link from SU1 to SU2 is given by:

$$R_1 = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2) (\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right). \quad (20)$$

Remark 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 (18). The same argument applies to the next subsection.

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:

$$\mathbf{r}_{1,n} = \alpha_n \sqrt{l_{d3} P_{s,n}} g_{1,n} \tilde{\mathbf{s}}_n + \gamma_{2,n} \sqrt{l_{d4} P_{2,n}} f_{2,n} \tilde{\mathbf{s}}_{2,n} + \beta_n \tilde{\mathbf{m}}_{1,n} + \tilde{\mathbf{n}}_{a,n}, \quad (21)$$

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 (21), the total harvested power at SU1 can be obtained as:

$$P_{EH,1} = \eta \rho_1 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \gamma_{2,n} l_{d4} P_{2,n} |f_{2,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right]. \quad (22)$$

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:

$$\tilde{\mathbf{r}}_{1,n} = \sqrt{(1 - \rho_1) l_{d4} P_{2,n}} f_{2,n} \tilde{\mathbf{s}}_{2,n} + \sqrt{1 - \rho_1} (\beta_n \tilde{\mathbf{m}}_{1,n} + \tilde{\mathbf{n}}_{a,n}) + \tilde{\mathbf{n}}_{b,n}, \quad n \in \mathcal{A}, \quad (23)$$

where $\tilde{\mathbf{n}}_{b,n} \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I})$ is the AWGN noise in the baseband. From (23), the achievable rate for the uplink transmission is given by:

$$R_2 = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_1) l_{d4} P_{2,n} |f_{2,n}|^2}{(1 - \rho_1) (\beta_n \tilde{\sigma}_{1,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right). \quad (24)$$

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:

$$\tilde{P}_{EH,1} = \eta (M - 2M_1) \times \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right], \quad (25)$$

and

$$\tilde{P}_{EH,2} = \eta (M - 2M_1) \times \left[\sum_{n=1}^N (\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2) + N \sigma_a^2 \right]. \quad (26)$$

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

B. Sum-Rate Optimization

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

From (20) and (24), the sum-rate maximization problem can be expressed as:

$$\begin{aligned} \max_{\rho_1, \rho_2, M_1, \mathbf{P}_1, \mathbf{P}_2} \quad & R_{sum} = R_1 + R_2 \\ \text{s.t.} \quad & 0 \leq \rho_1 \leq 1, \\ & 0 \leq \rho_2 \leq 1, \\ & 0 \leq M_1 \leq \frac{M}{2}, \\ & \sum_{n \in \mathcal{A}} P_{1,n} \leq P_{SU1} + \frac{P_{EH,1} + \tilde{P}_{EH,1}}{M_1}, \\ & \sum_{n \in \mathcal{A}} P_{2,n} \leq P_{SU2} + \frac{P_{EH,2} + \tilde{P}_{EH,2}}{M_1}, \end{aligned} \quad (27)$$

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 (27) 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 (18) and (22) are both linear functions of \mathbf{P}_1 and \mathbf{P}_2 . Hence, the constraints in (27) become linear constraints. Based on these observations, it can be seen that the problem in (27) 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 [32]. Hence, the sum-rate maximization problem in (27) 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 (27), 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 (27). 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.

C. Suboptimal Solution

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

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.,

$$P_{1,n} = \frac{1}{|\mathcal{A}|} \left[P_{SU1} + \frac{P_{EH,1}}{M_1} \right], \quad (28)$$

and

$$P_{2,n} = \frac{1}{|\mathcal{A}|} \left[P_{SU2} + \frac{P_{EH,2}}{M_1} \right]. \quad (29)$$

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

$$\begin{aligned} R_1 &= \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2)(\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right) \\ &> \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2)(\beta_n \tilde{\sigma}_{2,m,n}^2 + \sigma_a^2) + \sigma_b^2} \right) \\ &\geq \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2) l_{d4} P_{1,n} |f_{1,n}|^2}{(1 - \rho_2) \tilde{\sigma}_{2,m}^2 + \sigma_b^2} \right), \end{aligned} \quad (30)$$

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:

$$R_2 \geq \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_1) l_{d4} P_{2,n} |f_{2,n}|^2}{(1 - \rho_1) \tilde{\sigma}_{1,m}^2 + \sigma_b^2} \right), \quad (31)$$

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 (22) can be lower bounded by:

$$P_{EH,1} > P_{EH,1}^{LB} = \eta \rho_1 M_1 \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right]. \quad (32)$$

From (28) and (32), the allocated power $P_{1,n}$ is lower bounded by:

$$P_{1,n} > c_1 \rho_1 + \zeta_1, \quad (33)$$

where

$$c_1 = \frac{\eta \left[\sum_{n=1}^N (\alpha_n l_{d3} P_{s,n} |g_{1,n}|^2 + \beta_n \tilde{\sigma}_{1,m,n}^2) + N \sigma_a^2 \right]}{|\mathcal{A}|}, \quad (34)$$

and

$$\zeta_1 = \frac{P_{SU1}}{|\mathcal{A}|}. \quad (35)$$

From (33), the rate R_1 in (31) can be further bounded by:

$$R_1 > R_1^{LB} = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_2)(c_1 \rho_1 + \zeta_1) l_{d4} |f_{1,n}|^2}{(1 - \rho_2) \tilde{\sigma}_{2,m}^2 + \sigma_b^2} \right). \quad (36)$$

Similarly, we have:

$$R_2 > R_2^{LB} = \frac{M_1}{M} \sum_{n \in \mathcal{A}} \log_2 \left(\frac{(1 - \rho_1)(c_2 \rho_2 + \zeta_2) l_{d4} |f_{2,n}|^2}{(1 - \rho_1) \tilde{\sigma}_{1,m}^2 + \sigma_b^2} \right), \quad (37)$$

where

$$c_2 = \frac{\eta \left[\sum_{n=1}^N (\alpha_n l_{d2} P_{s,n} |g_{2,n}|^2 + \beta_n \tilde{\sigma}_{2,m,n}^2) + N \sigma_a^2 \right]}{|\mathcal{A}|}, \quad (38)$$

and

$$\zeta_2 = \frac{P_{SU2}}{|\mathcal{A}|}. \quad (39)$$

2) *Suboptimal Solutions*: Instead of maximizing the sum-rate in (27), we maximize the sum-rate lower bound, which can be formulated as:

$$\begin{aligned} \max_{\rho_1, \rho_2} & R_1^{LB} + R_2^{LB} \\ \text{s.t.} & 0 \leq \rho_1 \leq 1, \\ & 0 \leq \rho_2 \leq 1, \end{aligned} \quad (40)$$

which is equivalent to:

$$\begin{aligned} \max_{\rho_1, \rho_2} & \frac{(1 - \rho_2)(c_1 \rho_1 + \zeta_1)}{(1 - \rho_2) \tilde{\sigma}_{2,m}^2 + \sigma_b^2} \frac{(1 - \rho_1)(c_2 \rho_2 + \zeta_2)}{(1 - \rho_1) \tilde{\sigma}_{1,m}^2 + \sigma_b^2} \\ \text{s.t.} & 0 \leq \rho_1 \leq 1, \\ & 0 \leq \rho_2 \leq 1. \end{aligned} \quad (41)$$

The optimal power splitting ratios for (41) can be obtained as:

$$\rho_1^* = \left[\frac{\tilde{\sigma}_{1,m}^2 + \sigma_b^2 - \sigma_b \sqrt{\sigma_b^2 + (1 + \zeta_1/c_1) \tilde{\sigma}_{1,m}^2}}{\tilde{\sigma}_{1,m}^2} \right]^+, \quad (42)$$

and

$$\rho_2^* = \left[\frac{\tilde{\sigma}_{2,m}^2 + \sigma_b^2 - \sigma_b \sqrt{\sigma_b^2 + (1 + \zeta_2/c_2) \tilde{\sigma}_{2,m}^2}}{\tilde{\sigma}_{2,m}^2} \right]^+, \quad (43)$$

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.

V. 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:

$$\begin{aligned} \min_{\sigma_{MU,n}^2} R_1 &= \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\ \text{s.t. } \sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 &= \sigma_{MU}^2, \end{aligned} \quad (44)$$

where $H_n = \sqrt{l_d} f_{1,n}$ and $\sigma^2 = \sigma_a^2 + \sigma_b^2$. $\sigma_{MU,n}^2 = \beta_n \sigma_{MU}^2$ 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:

$$\begin{aligned} R_1 &= \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\ &\simeq \sum_{n \in \mathcal{A}} \log_2 \left(\frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \right) \\ &= \log_2 \prod_{n \in \mathcal{A}} \left(\frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \right) \end{aligned} \quad (45)$$

Hence, minimizing the sum-rate is equivalent to

$$\max_{\sigma_{MU,n}^2} \prod_{n \in \mathcal{A}} (|H_{2,m,n}|^2 \sigma_{MU,n}^2) \quad (46)$$

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:

$$\begin{aligned} R_1 &= \sum_{n \in \mathcal{A}} \log_2 \left(1 + \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2 + \sigma^2} \right) \\ &\simeq \log_2(e) \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2}, \end{aligned} \quad (47)$$

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:

$$\begin{aligned} \min_{\sigma_{MU,n}^2} \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^2} \\ \text{s.t. } \sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 &= \sigma_{MU}^2, \end{aligned} \quad (48)$$

which is given by:

$$\sigma_{MU,n}^2 = \frac{|H_n| \sqrt{P_{1,n}} / |H_{2,m,n}|}{\sum_{k \in \mathcal{A}} |H_k| \sqrt{P_{1,k}} / |H_{2,m,k}|} \sigma_{MU}^2, \quad \forall n \in \mathcal{A}. \quad (49)$$

In fact, from (48), 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:

$$\sum_{n \in \mathcal{A}} \sigma_{MU,n}^2 \sum_{n \in \mathcal{A}} \frac{a_n}{\sigma_{MU,n}^2} \geq \left(\sum_n \sqrt{a_n} \right)^2, \quad (50)$$

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 (49).

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:

$$\begin{aligned} \Delta R_1 &\simeq \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^{2*}} - \sum_{n \in \mathcal{A}} \frac{|H_n|^2 P_{1,n}}{|H_{2,m,n}|^2 \sigma_{MU,n}^{2'}} \\ &= \frac{1}{\sigma_{MU}^2} \left[|\mathcal{A}| \sum_{n \in \mathcal{A}} |H_n|^2 P_{1,n} / |H_{2,m,n}|^2 \right. \\ &\quad \left. - \left(\sum_{n \in \mathcal{A}} |H_n| \sqrt{P_{1,n}} / |H_{2,m,n}| \right)^2 \right], \end{aligned} \quad (51)$$

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.

VI. SIMULATION RESULTS

In this section, we evaluate the effectiveness of the proposed AES-based DTV scheme and the energy harvesting scheme using simulation examples. First, we evaluate the detection performance for the primary user and malicious user through false alarm rates and miss detection probabilities. Then, we calculate the achievable sum-rate 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. The simulation parameters are listed in Table I.

Example 1 (PUEA Detection Performance): In this example, we obtain the false alarm rates and miss detection probabilities for primary user and malicious user detection under different SNR values, as shown in Figure 5. It can be seen that the proposed scheme can achieve negligible false alarm rates and miss detection probabilities. This means that the proposed approach can detect the primary user and the malicious user with high accuracy, which implies that, potentially, the proposed scheme can significantly improve the performance of the SUs network in the CR networks under PUEA.

TABLE I
SYSTEM PARAMETERS

Sample size M	100
Number of subcarriers N	128
Number of white space & interference subcarriers	16
Distance between PU1 and SCU1 (d_1)	500 m
Distance between PU1 and SU1 (d_3)	50 m
Distance between PU1 and SU2 (d_2)	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

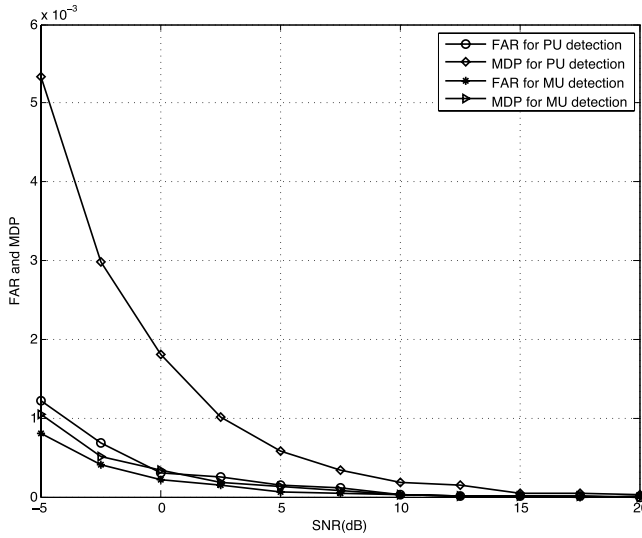


Fig. 5. Example 1: The false alarm rates (FARs) and miss detection probabilities (MDPs) versus SNR for primary user and malicious user detection.

Example 2 (Energy Harvesting Performance): Here, we demonstrate the advantages of the proposed energy harvesting scheme over the conventional non-energy harvesting OFDM systems. In the simulations, 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 and the primary user signals.

To demonstrate the effectiveness of the energy harvesting, Figure 6 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

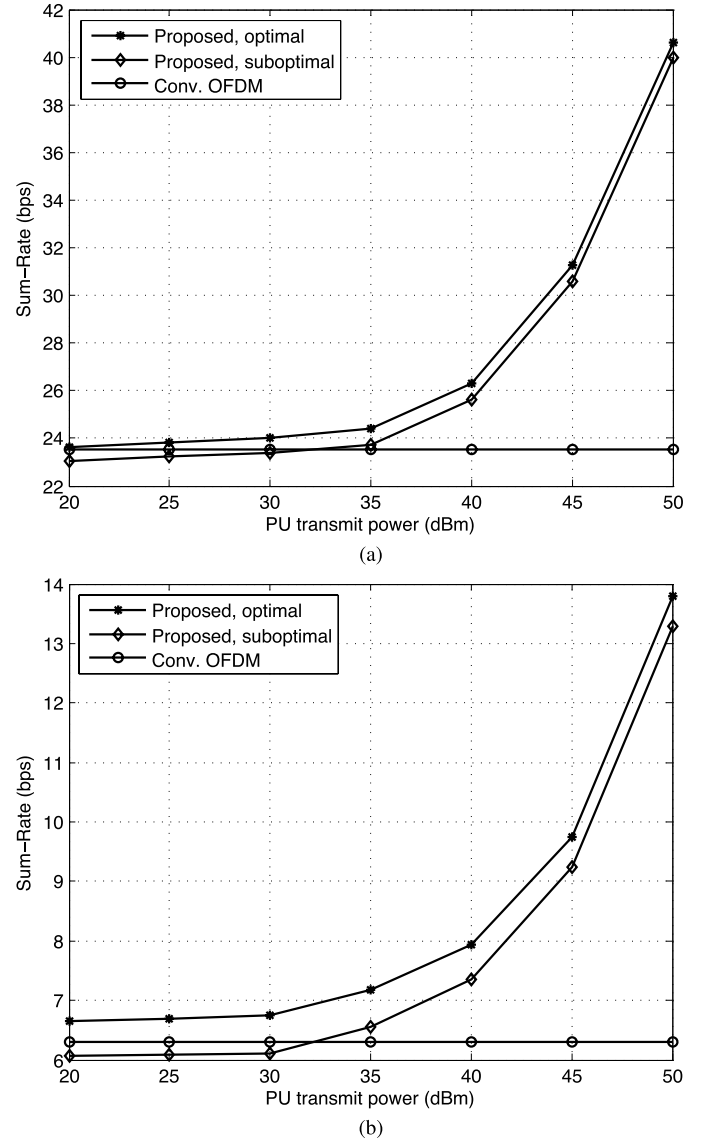


Fig. 6. Example 2: The achievable sum-rate comparison of the proposed OFDM-based energy harvesting scheme and that of its non-energy harvesting counterpart versus different PU and MU transmit power levels. (a) When the MU1 transmit power is 10 dBm. (b) When the MU1 transmit power is 20 dBm.

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

In the simulations, the power splitting ratios, ρ_1 and ρ_2 , are calculated using both the optimal solution (through exhaustive search) and the suboptimal solution. It is observed that the

performance of the suboptimal scheme is fairly close to the optimal one, but with much lower computational complexity.

VII. CONCLUSIONS

In this paper, we considered malicious user detection and energy harvesting for reliable and efficient OFDM-based CR network operation under PUEA. In the proposed scheme, the existing reference sequence used to generate the P2 pilots in the DVB-T2 standard is encrypted using the AES algorithm to facilitate accurate detection of the primary user and malicious user. The detection information is used by the SUC to coordinate collision-free transmissions among the SUs. Depending on the bandwidth availability, if no white spaces are available, then secondary users harvest energy from the received signals; otherwise, secondary users harvest energy and transmit their own signals according to the proposed energy harvesting scheme. It was shown that with the AES-based DTV scheme, the malicious user can be detected accurately over all subcarriers where the P2 symbols present. Moreover, with the energy harvesting scheme, the sum-rate of the secondary user network can be significantly improved.

APPENDIX

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:

$$\begin{aligned}\mu_{00} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M \mathbf{n}_{k,i} \mathbf{n}_{k,i}^* \right\} \\ &= \sigma_n^2,\end{aligned}\quad (52)$$

and σ_{00}^2 can be obtained as:

$$\begin{aligned}\sigma_{00}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{00}|^2 \\ &= \frac{1}{M} \left[\mathbb{E} \{ |\tilde{\mathbf{n}}_k|^4 \} - (\sigma_n^2)^2 \right],\end{aligned}\quad (53)$$

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:

$$\begin{aligned}\mu_{01} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M (\mathbf{m}_{k,i} + \mathbf{n}_{k,i})(\mathbf{m}_{k,i} + \mathbf{n}_{k,i})^* \right\} \\ &= \sigma_{m,k}^2 + \sigma_n^2.\end{aligned}\quad (54)$$

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

$$\begin{aligned}\sigma_{01}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{01}|^2 \\ &= \frac{1}{M} \left[\mathbb{E} \{ |\tilde{\mathbf{m}}_k|^4 \} + \mathbb{E} \{ |\tilde{\mathbf{n}}_k|^4 \} + \mathbb{E} \{ 2\mathbb{R} \{ (\tilde{\mathbf{m}}_k)^2 (\tilde{\mathbf{n}}_k^*)^2 \} \} \right. \\ &\quad \left. + 2\sigma_{m,k}^2 \sigma_n^2 - (\sigma_{m,k}^2)^2 - (\sigma_n^2)^2 \right],\end{aligned}\quad (55)$$

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

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:

$$\begin{aligned}\mu_{10} &= \frac{1}{M} \mathbb{E} \left\{ \sum_{i=1}^M (\tilde{C}_k \mathbf{s}_{k,i} + \mathbf{n}_{k,i})(\tilde{C}_k \mathbf{s}_{k,i} + \mathbf{n}_{k,i})^* \right\} \\ &= \tilde{C}_k^2 + \sigma_n^2,\end{aligned}\quad (56)$$

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

$$\begin{aligned}\sigma_{10}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr,k}|^2 \right\} - |\mu_{10}|^2 \\ &= \frac{1}{M} \left[\tilde{C}_k^4 \mathbb{E} \{ |\tilde{\mathbf{s}}_k|^4 \} + \mathbb{E} \{ |\tilde{\mathbf{n}}_k|^4 \} + \mathbb{E} \{ 2\tilde{C}_k^2 \mathbb{R} \{ (\tilde{\mathbf{s}}_k)^2 (\tilde{\mathbf{n}}_k^*)^2 \} \} \right. \\ &\quad \left. + 2\tilde{C}_k^2 \sigma_n^2 - \tilde{C}_k^4 - (\sigma_n^2)^2 \right].\end{aligned}\quad (57)$$

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:

$$\mu_{11} = \tilde{C}_k^2 + \sigma_{m,k}^2 + \sigma_n^2, \quad (58)$$

and σ_{11}^2 can be obtained as:

$$\begin{aligned}\sigma_{11}^2 &= \mathbb{E} \left\{ |\hat{\mathbf{R}}_{rr}|^2 \right\} - |\mu_{11}|^2 \\ &= \frac{1}{M} \left[\tilde{C}_k^4 \mathbb{E} \{ |\tilde{\mathbf{s}}_k|^4 \} + \mathbb{E} \{ |\tilde{\mathbf{m}}_k|^4 \} + \mathbb{E} \{ |\tilde{\mathbf{n}}_k|^4 \} \right. \\ &\quad + 2\tilde{C}_k^2 \mathbb{E} \{ \mathbb{R} \{ (\tilde{\mathbf{s}}_k)^2 (\tilde{\mathbf{m}}_k^*)^2 \} \} + 2\tilde{C}_k^2 \mathbb{E} \{ \mathbb{R} \{ (\tilde{\mathbf{s}}_k)^2 (\tilde{\mathbf{n}}_k^*)^2 \} \} \\ &\quad + 2\mathbb{E} \{ \mathbb{R} \{ (\tilde{\mathbf{m}}_k)^2 (\tilde{\mathbf{n}}_k^*)^2 \} \} + 2\tilde{C}_k^2 \sigma_{m,k}^2 + 2\tilde{C}_k^2 \sigma_n^2 \\ &\quad \left. + 2\sigma_{m,k}^2 \sigma_n^2 - \tilde{C}_k^4 - (\sigma_{m,k}^2)^2 - (\sigma_n^2)^2 \right].\end{aligned}\quad (59)$$

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.

REFERENCES

- [1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.
- [2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.
- [3] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. Conf. 3rd Int. Cognit. Radio Oriented Wireless Netw. Commun. (CrownCom)*, May 2008, pp. 1–8.
- [4] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, Jan. 2013.
- [5] D. Das and S. Das, "Primary user emulation attack in cognitive radio networks: A survey," *Int. J. Comput. Netw. Wireless Commun.*, pp. 2250–3501, 2013.
- [6] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
- [7] 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 *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2011, pp. 599–604.

- [8] 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 J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1850–1860, Nov. 2012.
- [9] M. Dang, Z. Zhao, and H. Zhang, "Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2013, pp. 1–5.
- [10] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting mobile primary user emulation attack in white space," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 36–40.
- [11] S. Jana, K. Zeng, W. Cheng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1497–1507, Sep. 2013.
- [12] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.
- [13] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.
- [14] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.
- [15] X. Lu, P. Wang, D. Niyato, D. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, May 2015.
- [16] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in multiuser OFDM systems with wireless information and power transfer," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 3823–3828.
- [17] D. Li, C. Shen, and Z. Qiu, "Sum rate maximization and energy harvesting for two-way af relay systems with imperfect CSI," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2013, pp. 4958–4962.
- [18] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788–4799, Sep. 2013.
- [19] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Opportunistic channel access and RF energy harvesting in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2039–2052, Nov. 2014.
- [20] A. Sultan, "Sensing and transmit energy optimization for an energy harvesting cognitive radio," *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 500–503, Oct. 2012.
- [21] A. E. Shafie and A. Sultan, "Optimal random access for a cognitive radio terminal with energy harvesting capability," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1128–1131, Jun. 2013.
- [22] S. Park, H. Kim, and D. Hong, "Cognitive radio networks with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1386–1397, Mar. 2013.
- [23] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 3229–3234.
- [24] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 772–781, May 2014.
- [25] C.-Y. Ong, J. Song, C. Pan, and Y. Li, "Technology and standards of digital television terrestrial multimedia broadcasting [Topics in Wireless Communications]," *IEEE Commun. Mag.*, vol. 48, no. 5, pp. 119–127, May 2010.
- [26] *Digital Video Broadcasting, Frame Structure Channel Coding and Modulation for a Second Generation Digital Terrestrial Television Broadcasting System (DVB-T2)*, ETSI Standard EN 302 755 V1.3.1, Apr. 2012.
- [27] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Commun.*, vol. 19, no. 4, pp. 82–88, Aug. 2012.
- [28] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 3982–3987.
- [29] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.
- [30] N. Haller, "The S/KEY one-time password system," in *Proc. Internet Soc. Symp. Netw. Distrib. Syst. Secur.*, Feb. 1994.
- [31] P. S. Mann, *Introductory Statistics*, 7th ed. Hoboken, NJ, USA: Wiley, Feb. 2010.
- [32] Z.-Q. Luo and W. Yu, "An introduction to convex optimization for communications and signal processing," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1426–1438, Aug. 2006.



Ahmed Alahmadi received the B.S. degree in electrical engineering from Taibah University, Madina, Saudi Arabia, in 2010, and the M.S. degree in electrical and computer engineering from Michigan State University, East Lansing, MI, USA, in 2014, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His research interests include wireless communications and networking, and wireless security.



Zhaoxi Fang received the B.Eng. degree in communication engineering and the Ph.D. degree in electrical engineering from Fudan University, Shanghai, China, in 2004 and 2009, respectively. In 2009, he joined the School of Electronic and Information Engineering, Zhejiang Wanli University, Ningbo, China, where he is currently an Associate Professor. From 2013 to 2014, he was a Post-Doctoral Research Associate with the Department of Electrical and Computer Engineering, Michigan State University. His research interests include cooperative communications, multipleinput multipleoutput communications, and energy-efficient communications.



Tianlong Song received the B.S. degree in communication engineering from the Beijing University of Chemical Technology, Beijing, China, in 2009, and the M.S. degree in information and communication engineering from Beihang University, Beijing, China, in 2012, respectively. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Michigan State University. His research interests lie in the areas of efficient and secure communications, antijamming techniques, and coding theory.



Tongtong Li (SM'08) received the Ph.D. degree in electrical engineering from Auburn University, in 2000. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, Michigan State University. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory, and statistical signal processing. She is currently serving as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING.