A Practical Underlay Spectrum Sharing Scheme for Cognitive Radio Networks

Pedram Kheirkhah Sangdeh, Hossein Pirayesh, Huacheng Zeng and Hongxiang Li
Department of Electrical and Computer Engineering, University of Louisville
Email: {pedram.kheirkhahsangdeh, hossein.pirayesh, huacheng.zeng, h.li}@louisville.edu

***Abstract*—As the proliferation of mobile devices has led to an ever-growing demand for wireless Internet services, the spectrum shortage issue becomes increasingly severe and spectrum sharing is regarded as a promising approach to addressing the spectrum shortage issue. In this paper, we propose a practical underlay spectrum sharing scheme for cognitive radio networks (CRNs) where the primary users are oblivious to the secondary users. The key components of our scheme are two MIMO-based interference cancellation (IC) techniques to handle cross-network interference on the secondary network side. The first one is a blind beamforming technique for secondary transmitters. This IC technique allows a secondary transmitter to nullify its generated interference for primary users without requiring channel state information (CSI). The second one is a blind interference cancellation (BIC) technique for secondary receivers. This IC technique enables a secondary receiver to decode its desired signal in the presence of strong unknown interference from primary transmitters. Based on these two MIMO-based IC techniques, we develop a MAC protocol for the secondary network to enable underlay spectrum sharing in CRNs. We have implemented the proposed underlay spectrum sharing scheme on a GNURadio-USRP2 wireless testbed. Experimental results show that the secondary users can achieve an average of 1 bit/s/Hz spectrum efficiency without degrading the performance of the primary users in a real-world office building environment.**

***Index Terms*—Cognitive radio networks, spectrum sharing, blind interference cancellation, beamforming, MIMO**

I. Introduction

The proliferation of mobile devices and the emergence of Internet of Things (IoT) applications have led to severe spectrum shortage issue for wireless networks (e.g., cellular and WiFi networks). Although there is an expectation that much spectrum in the millimeter band (30 GHz to 300 GHz) can be allocated for communication purposes, most of this spectrum is limited to short-range applications due to its rapid path loss. Moreover, millimeter wave is highly vulnerable to blockage and thus mainly considered for complementary use. Therefore, it is crucial to improve the utilization efficiency of sub-6 GHz golden spectrum bands to meet the ever-growing demand for wireless services.

In the context of cognitive radio networks (CRNs), depending on the knowledge and strategy that are needed for the secondary network to coexist with the primary network, the spectrum sharing approaches were divided into three classes: underlay, overlay and interweave [1]. Compared to the other two approaches, the underlay approach allows secondary users to concurrently use the spectrum with primary users without degrading the performance of primary users. It is therefore considered to be the most appealing spectrum sharing approach for CRNs. The key challenge in the underlay approach is the management of cross-network interference on the secondary network side. Specifically, the challenge lies in the following two tasks: (i) at a secondary transmitter, how to nullify its generated interference for its surrounding primary receivers; and (ii) at a secondary receiver, how to decode its desired signal in the presence of interference from primary transmitters. These two tasks become even more challenging in the scenarios where the secondary users have no knowledge of the primary users and where the primary users are unable or reluctant to cooperate with the secondary users.

While there is a large amount of work on underlay spectrum sharing for CRNs, most work is either focused on theoretical exploration or reliant on the assumption that global channel knowledge and clock synchronization are available at the secondary users (see, e.g., [2]–[11]). Very limited progress has been made so far in the development of practical schemes to enable underlay spectrum sharing for CRNs. Moreover, to the best of our knowledge, there is no underlay spectrum sharing solution that has been implemented and evaluated on testbeds in real-world wireless environments.

In this paper, we develop a practical MIMO-based underlay spectrum sharing scheme for CRNs and evaluate its performance using real-world implementation. We assume that the primary users are not cooperative with the secondary users. We also assume that secondary users have no knowledge about the cross-network interference from the primary users. The secondary users take full responsibility for cross-network interference cancellation. The key components of our scheme are two MIMO-based interference cancellation (IC) techniques. The first one is a blind beamforming technique for secondary transmitters; the second one is a blind interference cancellation (BIC) technique for secondary receivers. Based on these two IC techniques, we develop a MAC protocol to enable underlay spectrum sharing between uncoordinated secondary and primary networks. The main contributions of this paper are summarized as follows:

- We have designed a blind beamforming technique for a secondary transmitter, which can nullify cross-network interference for its surrounding primary users. In contrast to most existing beamforming techniques, which require CSI for the design of precoders, this blind beamforming technique does not require CSI for the design of precoders. Instead, it uses the overheard cross-network interference from the

primary users to infer the beamforming direction for the design of precoders. Our analytical results show that such a blind beamforming technique can completely nullify the cross-network interference for primary users if the noise is negligible and the channel coherence time is sufficiently large.

- We have designed a MIMO-based BIC technique for a secondary receiver, which can decode the desired signal in the presence of strong unknown cross-network interference from primary transmitters. The core of this BIC scheme is a spatial filter, which combines the desired signals in a constructive manner and combines interference in a destructive manner. This BIC technique can completely cancel cross-network interference and perfectly recover the desired signal in noise-negligible scenarios.
- Based on these two MIMO-based IC techniques, we have designed a new MAC protocol to enable underlay spectrum sharing between a primary network and a secondary network. The new MAC protocol is applied to the secondary network only; and there is no need for modification on the primary network. The two IC techniques and the MAC protocol constitute a holistic spectrum sharing scheme, which is amenable to practical implementation.
- We have built a prototype of the proposed spectrum sharing scheme on a GNURadio-USRP2 wireless testbed. Experimental results show that the secondary users can achieve an average of 1 bit/s/Hz spectrum efficiency without degrading the performance of the primary users in a real-world office building environment. Particularly, the proposed blind beamforming technique can achieve an average of 25.3 dB IC capability for a two-antenna secondary transmitter, and the proposed BIC technique can achieve an average of 32.8 dB IC capability for a two-antenna secondary receiver.

II. Problem Statement

We consider a CRN as shown in Fig. 1, which consists of two active primary users and two secondary users. The primary users conduct bidirectional communications in time-division duplex (TDD) mode. The traffic in the primary network are consistent and persistent in both directions, as illustrated in Fig. 2. The secondary users want to use the same spectrum for their own communications without harmfully affecting the primary users. To do so, the secondary transmitter performs beamforming operations to nullify its generated interference for the primary receiver, and the secondary receiver performs IC for its signal detection. Simply put, the secondary users take full responsibility for cross-network interference cancellation, and their data transmissions are transparent to the primary users.

In this CRN, there is no coordination between the primary and secondary users. The secondary users have no knowledge about cross-network interference characteristics. The primary users have one or multiple antennas, and the number of their antennas is denoted by M_{p}. The secondary users have multiple antennas, and the number of their antennas is denoted by M_{s}. In our study, we assume that the number of antennas on a secondary user is greater than that on a primary user (i.e., $M_{\mathrm{s}} > M_{\mathrm{p}}$). This assumption ensures that each secondary user has sufficient spatial degrees of freedom (DoFs) to tame the cross-network interference from/to primary users.

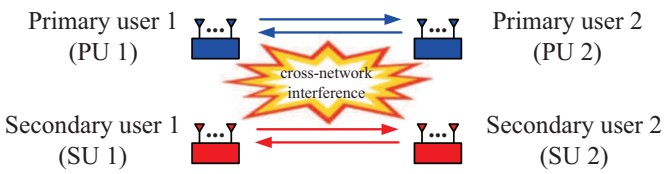


Fig. 1: A CRN consisting of two active primary users and two active secondary users.

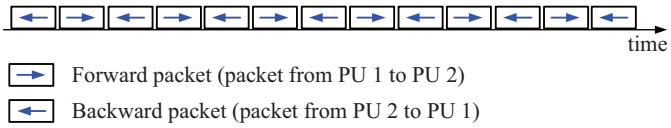


Fig. 2: Consistent and persistent traffic in the primary network.

Design Objectives: In such a CRN, our objectives are fourfold: (i) develop a blind beamforming technique for the secondary transmitter to nullify their generated interference for primary receivers; (ii) develop a MIMO-based BIC technique for the secondary receiver to decode its desired signal in the presence of interference from the primary transmitter; (iii) develop a holistic spectrum sharing scheme by leveraging these two IC techniques; and (iv) evaluate the IC techniques as well as the spectrum sharing scheme in real-world wireless environments.

Two Justifications: First, in this paper, we study a CRN that has only one pair of primary users and one pair of secondary users. Albeit simple, such a network serves as a fundamental building block for a large-scale CRN that have many primary and secondary users. Therefore, understanding this simple CRN is of great importance. Second, in our study, we assume that the secondary users have no knowledge about cross-network interference characteristics. Such a conservative assumption will lead to a more robust spectrum sharing scheme, which will be versatile for many application scenarios.

III. An Underlay Spectrum Sharing Scheme

In this section, we present an underlay spectrum sharing scheme for the secondary network so that it can use the same spectrum for communication without harmfully affecting the performance of the primary network. Our scheme consists of a lightweight MAC protocol and a new PHY design for the secondary users. In what follows, we first present the MAC protocol and then describe the new PHY design.

A. MAC Protocol for Secondary Network

Fig. 3 shows our MAC protocol in the time domain. It includes both forward communication (from SU 1 to SU 2) and backward communication (from SU 2 to SU 1) between the two secondary users. Since the two-way communications are

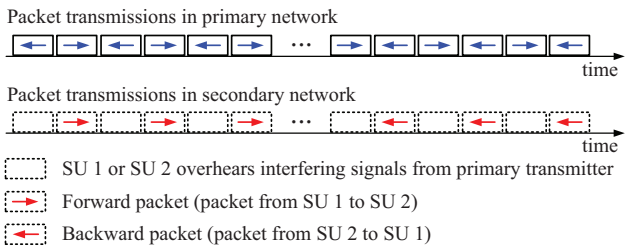
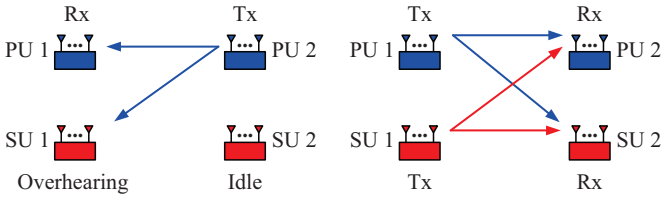


Fig. 3: A MAC protocol for underlay spectrum sharing in a CRN that has two primary users and two secondary users.



(a) Phase I: SU 1 overhears the interfering signals from PU 2.

(b) Phase II: SU 1 sends data to SU 2 using IC techniques.

Fig. 4: Illustration of our proposed spectrum sharing scheme.

symmetric, our presentation in the following will focus on the forward communication. The backward communication can be done in the same way.

The forward communication in the proposed MAC protocol comprises two phases: *overhearing (Phase I)* and *packet transmission (Phase II)*. In the time domain, Phase I aligns with the backward packet transmission in the primary network, and Phase II aligns with the forward packet transmission in the primary network, as illustrated in Fig. 3. We elaborate the operations in the two phases as follows:

- Phase I (*overhearing*): Fig. 4(a) shows the network behavior in this phase. Specifically, SU 1 overhears the cross-network interference from PU 2, and SU 2 remains idle.
- Phase II (*packet transmission*): Fig. 4(b) shows the network behavior in this phase. Specifically, SU 1 first constructs beamforming filters (a.k.a. precoding vectors or precoders) using the overheard interference in Phase I, and then transmits signals to SU 2 using the constructed beamforming filters. Meanwhile, SU 2 decodes the signals from SU 1 in the presence of interference from PU 1.

B. PHY Design for Secondary Users: An Overview

To support the proposed MAC protocol, we use the legacy 802.11 PHY for the secondary network, including the frame format, OFDM modulation, and channel coding schemes. However, 802.11 PHY is vulnerable to cross-network interference. Therefore, we need to modify the 802.11 PHY for the secondary users. The modified PHY should be resilient to cross-network interference on both transmitter and receiver sides. The design of such a PHY faces the following two challenges.

Challenge 1: Referring to Fig. 4(b), it is a nontrivial task for the secondary transmitter (SU 1) to nullify its generated interference at the primary receiver (PU 2). Note that we assume the secondary transmitter has no knowledge about the primary network, including the signal waveform, bandwidth, and frame format. The primary network may use OFDM, CDMA, or other types of modulation for its packet transmission. The lack of knowledge about the interfering signals from the primary users makes it challenging to nullify the interference at the secondary transmitter.

To address this challenge, we design a blind beamforming technique for the secondary transmitter (SU 1) to nullify its interference at the primary receiver. Our beamforming technique takes advantage of the overheard interfering signals in Phase I to construct precoding vectors for beamforming. Albeit without knowledge of interfering signals, our beamforming technique can completely nullify the interference at the primary receiver, provided that the noise is negligible and the channel coherence time is sufficiently large. Details of this beamforming technique are presented in Section IV.

Challenge 2: Again, referring to Fig. 4(b), it is a nontrivial task for the secondary receiver (SU 2) to decode its desired signal in the presence of cross-network interference from the primary transmitter. Note that the secondary receiver does not have the knowledge of the interference characteristics. This makes it challenging to cancel interference for signal detection.

To address this challenge, we design a MIMO-based BIC technique for the secondary receiver. The core of our BIC technique is a spatial filter, which can mitigate the interference from the primary transmitter and recover the desired signal. Details of this BIC technique are presented in Section V.

IV. Blind Beamforming

In this section, we study the beamforming operations at SU 1 in Fig. 4. In Phase I, SU 1 first overhears the interfering signals from the primary transmitter, and then uses the overheard interfering signals to construct spatial filters. Based on channel reciprocity, the constructed spatial filters are used as beamforming filters in Phase II to nullify interference for the primary receiver. These operations are performed on each subcarrier in the OFDM modulation. In what follows, we first present the derivation of beamforming filters and then offer performance analysis of the proposed beamforming technique.

Mathematical Formulation: Consider SU 1 in Fig. 4(a). It overhears interfering signals from PU 2. The overheard interfering signals are converted to the frequency domain through FFT operation. We assume that the channel from PU 2 to SU 1 is a block-fading channel in the time domain. That is, all the OFDM symbols in the backward transmissions experience the same channel. Denote $\mathbf{Y}(l,k)$ as the lth sample of overheard interfering signal on subcarrier k in Phase I. Then we have[1]

$$\mathbf{Y}(l,k) = \mathbf{H}_{\text{sp}}^{[1]}(k)\mathbf{X}_{\text{p}}^{[1]}(l,k) + \mathbf{W}(l,k), \quad (1)$$

[1]For the notation in this paper, superscripts "[1]" and "[2]" mean Phases I and II, respectively. Subscripts "s" and "p" mean the secondary and primary users, respectively.

where $\mathbf{H}_{\mathrm{sp}}^{[1]}(k) \in \mathbb{C}^{M_{\mathrm{s}} \times M_{\mathrm{p}}}$ is the matrix representation of the block-fading channel from PU 2 to SU 1 on subcarrier k, $\mathbf{X}_{\mathrm{p}}^{[1]}(l,k) \in \mathbb{C}^{M_{\mathrm{p}} \times 1}$ is the interfering signal transmitted by PU 2 on subcarrier k, and $\mathbf{W}(l,k) \in \mathbb{C}^{M_{\mathrm{s}} \times 1}$ is the noise vector at SU 1.

At SU 1, we seek a spatial filter that can combine the overheard interfering signals in a destructive manner. Denote $\mathbf{P}(k) \in \mathbb{C}^{M_{\mathrm{s}} \times 1}$ as the spatial filter on subcarrier k. Then, the combined received signal can be further written as: $\mathbf{P}(k)^* \mathbf{Y}(l,k)$, where $(\cdot)^*$ is conjugate transpose operator. Under the minimum mean square error (MMSE) criteria, the design of $\mathbf{P}(k)$ can be formulated as:

$$\min \ \ \mathbb{E}\big[\mathbf{P}(k)^* \mathbf{Y}(l,k) \mathbf{Y}(l,k)^* \mathbf{P}(k)\big], \quad \text{s.t. } \mathbf{P}(k)^* \mathbf{P}(k) = 1. \tag{2}$$

Optimal Spatial Filter: To solve the optimization problem in (2), we use Lagrangian method. We define the Lagrange function as:

$$\mathcal{L}(\mathbf{P}(k), \lambda) = \mathbb{E}\big[\mathbf{P}(k)^* \mathbf{Y}(l,k) \mathbf{Y}(l,k)^* \mathbf{P}(k)\big] - \lambda \big[\mathbf{P}(k)^* \mathbf{P}(k) - 1\big],$$

where λ is Lagrange multiplier.

By setting the partial derivatives of $\mathcal{L}(\mathbf{P}(k), \lambda)$ to zero, we have

$$\frac{\partial \mathcal{L}(\mathbf{P}(k), \lambda)}{\partial \mathbf{P}(k)} = \mathbf{P}(k)^* \Big(\mathbb{E}[\mathbf{Y}(l,k) \mathbf{Y}(l,k)^*] - \lambda \mathbf{I} \Big) = 0, \tag{3}$$

$$\frac{\partial \mathcal{L}(\mathbf{P}(k), \lambda)}{\partial \lambda} = \mathbf{P}(k)^* \mathbf{P}(k) - 1 = 0. \tag{4}$$

Based on the definition of eigendecomposition, it is easy to see that the solutions to equations (3) and (4) are the eigenvectors of $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$ and the corresponding values of λ are the eigenvalues of $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$. Note that $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$ has M_{s} eigenvectors each of which corresponds to a stationary point of the Lagrange function (extrema, local optima, and global optima). As λ is the penalty multiplier for the Lagrange function, the optimal spatial filter $\mathbf{P}(k)$ lies in the subspace spanned by the eigenvectors of $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$ that correspond to the minimum eigenvalue (λ).

For Hermitian matrix $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$, it may have multiple eigenvectors that corresponds to the minimum eigenvalue. Denote M_{e} as the number of its eigenvectors that correspond to the minimum eigenvalue. Then, we can write them as:

$$[\mathbf{U}_1, \mathbf{U}_2, \cdots, \mathbf{U}_{M_{\mathrm{e}}}] = \mathrm{mineigvectors}\Big(\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*] \Big), \tag{5}$$

where $mineigvectors(\cdot)$ represents the eigenvectors that corresponds to the minimum eigenvalue.

To estimate $\mathbb{E}[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*]$ in (5), we average the received interfering signal samples over the time domain. By doing so, we have

$$[\mathbf{U}_1, \mathbf{U}_2, \cdots, \mathbf{U}_{M_{\mathrm{e}}}] = mineigvectors\Big(\sum_{l=1}^{L_{\mathrm{p}}} \mathbf{Y}(l,k)\mathbf{Y}(l,k)^* \Big), \tag{6}$$

where L_{p} is the total number of the received interference samples. Based on (6), the optimal filter $\mathbf{P}(k)$ can be written as:

$$\mathbf{P}(k) = \sum_{m=1}^{M_{\mathrm{e}}} \alpha_m \mathbf{U}_m, \tag{7}$$

where α_m is a weight coefficient with $\sum_{m=1}^{M_{\mathrm{e}}} \alpha_m^2 = 1$.

Blind Beamforming Procedure: Now, we summarize the blind beamforming procedure as follows: In Phase I, SU 1 overhears interfering signals $\mathbf{Y}(l,k)$ from PU 2. Based on the overheard interfering signals, it constructs a spatial filter $\mathbf{P}(k)$ for subcarrier k using (6) and (7), where α_m can be any value that meets the norm constraint. In Phase II, we use $\overline{\mathbf{P}(k)}$ as the precoding vector for beamforming on subcarrier k, where $\overline{(\cdot)}$ is element-wise complex conjugate operator. The beamforming operation can be written as: $\overline{\mathbf{P}(k)} X_{\mathrm{s}}^{[2]}(l,k)$, where $X_{\mathrm{s}}^{[2]}(l,k)$ is the secondary transmit signal in Phase II.

For this beamforming technique, we have the following remarks.

Remark 1: It is evident to see that this beamforming technique does not require explicit CSI. Instead, it directly uses the overheard interfering signals to construct the precoding vectors. Therefore, we term this technique as "blind" beamforming.

Remark 2: In practice, the noises from SU 1's antennas are typically drawn from identical distributions. If that is the case, the number of eigenvectors in (6) that correspond to the minimum eigenvalue is $M_{\mathrm{e}} = M_{\mathrm{s}} - M_{\mathrm{p}}$ almost surely. Therefore, in (7), we have $(M_{\mathrm{s}} - M_{\mathrm{p}})$ free variables α_m that can be optimized to maximize the signal strength at the secondary receiver (SU 2).

Remark 3: This beamforming technique involves only one eigendecomposition for each subcarrier. It has a low computational complexity and is amenable to practical implementation.

IC Capability of This Beamforming Technique: For the performance of the proposed beamforming technique, we have the following lemma:

Lemma 1: The proposed beamforming technique can completely nullify interference for the primary receiver if (i) the forward and backward channels are reciprocal; and (ii) the noise is negligible.

We omit the proof to conserve the space.

Channel Reciprocity: To maintain the reciprocity of forward and backward channels in practical wireless systems, we can employ the relative calibration method in [12]. This relative calibration method is an internal and standalone calibration method that can be done at SU 1 without requiring involvement of other users. In our experiment, we implement this calibration method to preserve the channel reciprocity.

V. Blind Interference Cancellation

In this section, we shift our focus from the secondary transmitter (SU 1) to the secondary receiver (SU 2) in Phase II as shown in Fig. 4(b). We develop a BIC technique for the secondary receiver (SU 2) to decode its desired signals in the presence of interference from the primary transmitter (PU 1).

Mathematical Formulation: We employ legacy 802.11 frame for data transmission in the secondary network. Specifically, SU 1 sends frame-based signals to SU 2, which comprises a bulk of OFDM symbols. In each frame, the first four OFDM symbols carry reference signals and the remaining OFDM symbols carry payloads.

Consider the signal transmission in Phase II as shown in Fig. 4(b). Denote $X_{\rm s}^{[2]}(l,k)$ as the signal that SU 1 transmits on subcarrier k in OFDM symbol l. Denote $\mathbf{X}_{\rm p}^{[2]}(l,k)$ as the signal that PU 1 transmits on subcarrier k in OFDM symbol l. Denote $\mathbf{Y}(l,k)$ as the received signal vector at SU 2 on subcarrier k in OFDM symbol l. Then, we have

$$\mathbf{Y}(l,k) = \mathbf{H}_{\rm ss}^{[2]}(k)\overline{\mathbf{P}(k)}X_{\rm s}^{[2]}(l,k)+\mathbf{H}_{\rm sp}^{[2]}(k)\mathbf{X}_{\rm p}^{[2]}(l,k)+\mathbf{W}(l,k), \tag{8}$$

where $\mathbf{H}_{\rm ss}^{[2]}(k)$ is the block-fading channel between SU 2 and SU 1 on subcarrier k, $\mathbf{H}_{\rm sp}^{[2]}(k)$ is the block-fading channel between SU 2 and PU 1 on subcarrier k, and $\mathbf{W}(l,k)$ is the noise on subcarrier k in OFDM symbol l.

At SU 2, in order to decode the intended signal in the presence of interference, we use a linear spatial filter $\mathbf{G}(k)$ for all OFDM symbols on subcarrier k. Then, the decoded signal can be written as:

$$\hat{X}_{\rm s}^{[2]}(l,k) = \mathbf{G}(k)^*\mathbf{Y}(l,k). \tag{9}$$

While there exist many criteria for the design of $\mathbf{G}(k)$, our objective is to minimize the mean square error (MSE) between the decoded and original signals. Thus, the signal detection problem can be formulated as:

$$\min \quad \mathbb{E}\Big[\Big|\hat{X}_{\rm s}^{[2]}(l,k) - X_{\rm s}^{[2]}(l,k)\Big|^2\Big]. \tag{10}$$

Optimal Spatial Filter: To solve the optimization problem in (10), we use Lagrangian method again. We define the Lagrangian function as:

$$\mathcal{L}(\mathbf{G}(k)) = \mathbb{E}\Big[\Big|\hat{X}_{\rm s}^{[2]}(l,k) - X_{\rm s}^{[2]}(l,k)\Big|^2\Big]. \tag{11}$$

Based on (9), (11) can be rewritten as:

$$\mathcal{L}(\mathbf{G}(k)) = \mathbb{E}\Big[\Big|\mathbf{G}(k)^*\mathbf{Y}(l,k) - X_{\rm s}^{[2]}(l,k)\Big|^2\Big]. \tag{12}$$

Equation (12) is a quadratic function of $\mathbf{G}(k)$. To minimize MSE, we can take the gradient with respect to $\mathbf{G}(k)$. The optimal filter $\mathbf{G}(k)$ can be obtained by setting the gradient to zero, which we show as follows:

$$\mathbb{E}\big[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*\big]\mathbf{G}(k) - \mathbb{E}\big[\mathbf{Y}(l,k)X_{\rm s}^{[2]}(l,k)^*\big] = 0. \tag{13}$$

Based on (13), the optimal filter can be obtained by:

$$\mathbf{G}(k) = \mathbb{E}\big[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*\big]^\dagger\mathbb{E}\big[\mathbf{Y}(l,k)X_{\rm s}^{[2]}(l,k)^*\big]\ , \tag{14}$$

where $(\cdot)^\dagger$ is pseudo-inverse operator.

Equation (14) is the optimal design of $\mathbf{G}(k)$ in the sense of minimizing MSE. To calculate $\mathbb{E}\big[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*\big]$ and $\mathbb{E}\big[\mathbf{Y}(l,k)X_{\rm p}^{[2]}(l,k)^*\big]$ in (14), we can take advantage of the reference symbols in wireless systems (e.g., the preamble OFDM symbols in legacy 802.11 frame). Denote $\mathcal{Q}_k$ as the set of reference symbols in a frame that can be used for the design of spatial filter $\mathbf{G}(k)$. Then, we can approach the statistical expectations in (14) using the averaging operations as follows:

$$\mathbb{E}\big[\mathbf{Y}(l,k)\mathbf{Y}(l,k)^*\big] \approx \frac{1}{|\mathcal{Q}_k|}\sum_{(l,k')\in\mathcal{Q}_k}\mathbf{Y}(l,k')\mathbf{Y}(l,k')^*\ , \tag{15}$$

$$\mathbb{E}\big[\mathbf{Y}(l,k)X_{\rm s}^{[2]}(l,k)^*\big] \approx \frac{1}{|\mathcal{Q}_k|}\sum_{(l,k')\in\mathcal{Q}_k}\mathbf{Y}(l,k')X_{\rm s}^{[2]}(l,k')^*, \tag{16}$$

where $\mathcal{Q}_k$ will be further studied later.

With a bit abuse of notation, we replace the approximation sign in (15) and (16) with an equation sign for simplicity. Then, the spatial filter $\mathbf{G}(k)$ can be written as:

$$\mathbf{G}(k)=\Big[\sum_{(l,k')\in\mathcal{Q}_k}\mathbf{Y}(l,k')\mathbf{Y}(l,k')^*\Big]^\dagger\Big[\sum_{(l,k')\in\mathcal{Q}_k}\mathbf{Y}(l,k')X_{\rm s}^{[2]}(l,k')^*\Big]. \tag{17}$$

BIC Procedure: We now summarize our BIC procedure as follows: In Phase II, SU 2 needs to decode its desired signal in the presence of interference from PU 1. To do so, SU 2 first constructs a spatial filter for each of its subcarriers using (17), and then decodes its desired signal using (9).

For this BIC technique, we have the following remarks.

Remark 1: As shown in (17) and (9), this BIC technique does not require any knowledge of the interference characteristics, including waveform and bandwidth. Therefore, we term it as "blind" interference cancellation.

Remark 2: While this BIC technique does not require explicit CSI, it only requires reference signals at the secondary transmitter. In contrast to conventional signal detection schemes such as zero-forcing (ZF) and minimum mean square error (MMSE), this BIC technique does not require channel estimation.

Remark 3: The spatial filter in (17) not only cancels the interference but also equalizes the channel distortion for signal detection.

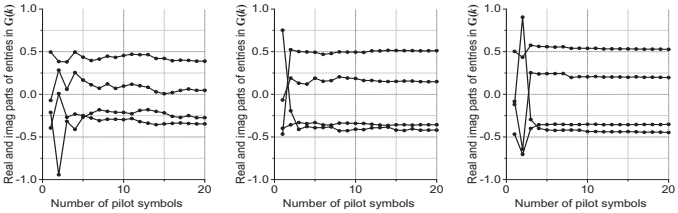
Remark 4: As shown in (17) and (9), this BIC technique involves matrix inversion and multiplication, where the dimension of the matrix is equal to the number of antennas on a secondary user. Its computational complexity is similar to the computational complexity of ZF detection scheme, which is already used in many real wireless systems. Therefore, we do not expect computational issue for this BIC technique.

IC Capability of This BIC Technique: For the performance of the proposed BIC technique, we have the following lemma:

Lemma 2: If the reference signals are sufficient and the noise is negligible, the BIC technique can perfectly recover the signals in the presence of cross-network interference (i.e., $\hat{X}_{\rm s}^{[2]}(k,l) = X_{\rm s}^{[2]}(k,l)$, $\forall k,l$) .

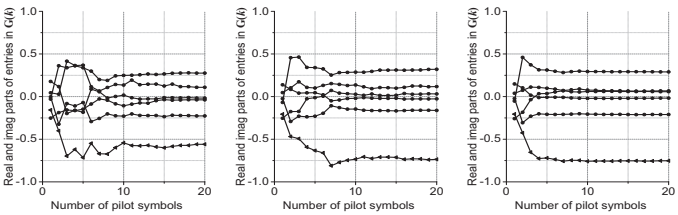
We omit the proof to conserve the space.

Reference Signals for Spatial Filter Design: Lemma 2 shows the superior performance of our BIC technique when the reference signals are sufficient. A question to ask is how many reference signals on each subcarrier are sufficient to reach convergence for the spatial filter. To answer this question,



(a) SNR=5dB case (b) SNR=15dB case (c) SNR=25dB case

Fig. 5: Convergence speed of spatial filter over the number of reference symbols in $(M_{\rm p}=1, M_{\rm s}=2)$ network.



(a) SNR=5dB case (b) SNR=15dB case (c) SNR=25dB case

Fig. 6: Convergence speed of spatial filter over the number of reference symbols in $(M_{\rm p}=2, M_{\rm s}=3)$ network.

we first use simulation to study the convergence speed of the spatial filter over the number of reference signals, and then propose a method to increase the number of reference signals for the spatial filter design.

As an instance, we have simulated the convergence speed of the spatial filter over the number of reference symbols for the secondary receiver. Fig. 5 and 6 present the simulation results in two network settings: $(M_{\rm p}=1, M_{\rm s}=2)$ and $(M_{\rm p}=2, M_{\rm s}=3)$. From the simulation results, we can see that the spatial filter converges at a pretty fast speed in these two network settings. Further, the spatial filter can achieve a good convergence with about 10 reference symbols.

In the secondary network, we use legacy 802.11 frame for data transmission from SU 1 to SU 2, which only has four reference symbols on each subcarrier (i.e., two L-STF OFDM symbols and two L-LTF OFDM symbols). So, the construction of spatial filter is in shortage of reference symbols. To address this issue, for each subcarrier, we not only use the reference symbols on that subcarrier but also the reference symbols on its neighboring subcarriers, as illustrated in Fig. 7. The rationale behind this operation lies in the fact that channel

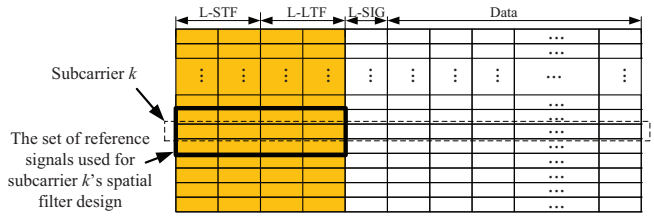
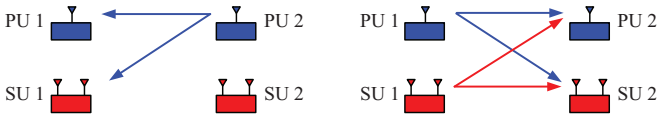


Fig. 7: Illustrating an example of $\mathcal{Q}(k)$ in legacy 802.11 frame.



(a) Transmission in phase I. (b) Transmission in phase II.

Fig. 8: Experimental setup for a cognitive radio network.

coefficients on neighboring subcarriers are highly correlated in real-world wireless environments. By leveraging the reference symbols on two neighboring subcarriers, we have 12 reference symbols for the construction of the spatial filter, which appear to be sufficient based on our simulation results in Fig. 5 and Fig. 6.

VI. Implementation

We consider a network in two time slots as shown in Fig. 8, where each primary user has one antenna and each secondary user has two antennas. We have implemented the proposed underlay spectrum sharing scheme in this network on a software-defined radio (SDR) wireless testbed consisting of GNU-Radio software package [13] and USRP N210 devices [14] to evaluate its performance in real-world wireless environments.

Prototype of The Primary Network: We have built a prototype of the two primary users on the wireless testbed. We have implemented two types of PHY for the primary network: LTE-based PHY and CDMA-based PHY. For the LTE-based PHY, we use 1024-point FFT operation for each OFDM symbol, which corresponds to 1024 subcarriers. Of the 1024 subcarriers, 600 are used for payloads. We set the sampling rate to 10 Msps. So, the bandwidth of the primary network in this case is about $10 \times 600/1024 \approx 5.8$ MHz. For the CDMA-based PHY, we use QPSK for data symbol transmission with a spreading factor of 64. We set the sampling rate to 5 Msps. The bandwidth of the primary network is about 5 MHz in this case. For both types of PHY, we set the carrier frequency to 2.48 GHz.

We have implemented the MAC protocol in Fig. 2 for the primary network. For ease of experimentation, we set the time duration of both forward and backward packet transmission to ten seconds. Due to the hardware limitations, we set the transition time between backward to forward packet transmissions to two seconds. Note that these time durations are used to ease our experimentation. In real wireless systems such as Wi-Fi, the time duration of a packet is about $100\,\mu$s and the transition time is about 16μs. With a smaller packet and shorter transition time, our spectrum sharing scheme will perform better in real-world wireless systems than in our testbed.

Prototype of the Secondary Network: We have built a prototype of the two secondary users in Fig. 8 on the wireless testbed. We have implemented legacy 802.11 PHY for the secondary network. We use the frame format in Fig. 7. Each OFDM symbol has 64 subcarriers, 48 of which are used for payloads and 4 of which are used as pilots. We set the sampling rate to 5 MHz. So, the bandwidth of the secondary

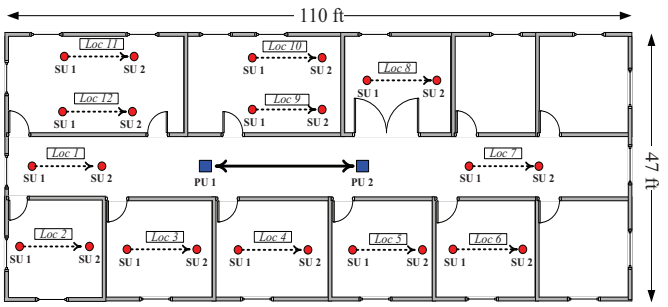


Fig. 9: Floor plan of primary and secondary users' locations.

TABLE I: EVM specification in IEEE 802.11ac standards [15].

EVM (dB)	(inf -5)	[-5 -10)	[-10 -13)	[-13 -16)	[-16 -19)	[-19 -22)	[-22 -25)	[-25 -27)	[-27 -30)	[-30 -32)	[-32 -inf)
Modulation	N/A	BPSK	QPSK	QPSK	16QAM	16QAM	64QAM	64QAM	64QAM	256QAM	256QAM
Coding rate	N/A	1/2	1/2	3/4	1/2	3/4	2/3	3/4	5/6	3/4	5/6
γ(EVM)	0	0.5	1	1.5	2	3	4	4.5	5	6	20/3

network is about $5 \times 52/64 \approx 4.1$ MHz. We set the carrier frequency to 2.48 GHz, which is the same as the primary network.

We have implemented the MAC protocol in Fig. 3 for the secondary network. The packet transmissions in the two networks are aligned in the time domain, as shown in Fig. 3. Since two-way communications in the secondary network are symmetric, we only consider the forward communication (from SU 1 to SU 2) in our experiment. The backward communication can be done in the same way and has the same performance.

We have implemented the proposed beamforming scheme on SU 1 and the proposed BIC scheme on SU 2 to handle the interference between the primary and secondary networks. In addition, we have implemented the internal calibration method [12] on the secondary user (SU 1 in Fig. 8) to maintain the relative channel reciprocity.

VII. Performance Evaluation

In this section, we evaluate the performance of the proposed underlay spectrum sharing scheme in an office building wireless environment.

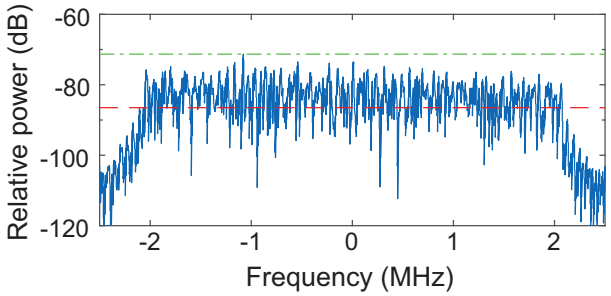
A. Experimental Setup and Performance Metrics

Experimental Setup: Fig. 9 shows the floor plan of our test scenarios. The two primary users are always placed at the spots marked "PU 1" and "PU 2." The two secondary users are placed at one of the 12 locations in Fig. 9. The distance between PU 1 and PU 2 is 10 m and the distance between SU 1 and SU 2 is 6 m. The transmit power of primary users is fixed to 15 dBm and the transmit power of secondary users is appropriately set to ensure that its generated interference at the primary receiver side is below the noise floor.

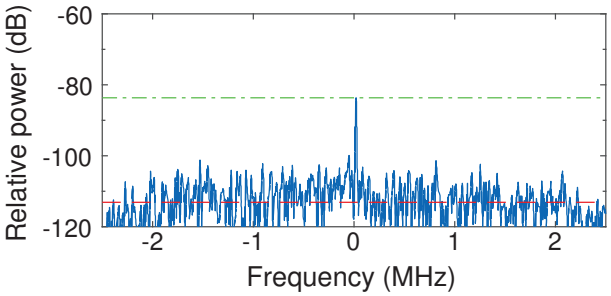
Performance Metrics: We evaluate the performance of the proposed underlay spectrum sharing scheme using the following four metrics: (i) Transmitter-side IC capability at SU 1: This IC capability is from SU 1's blind beamforming. It is defined as $\beta_{\text{tx}} = 10\log_{10}(P_1/P_2)$, where P_1 is the received interference power at PU 2 when SU 1 uses $[\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}]$ as the precoder and P_2 is the received interference power at PU 2 when SU 1 uses the precoder constructed by the blind beamforming technique. (ii) Receiver-side IC capability at SU 2: This IC capability is from SU 2's BIC. It is defined as $\beta_{\text{rx}} = -\text{EVM} - \max\{\text{SIR}_m\}$, where SIR_m is the signal to interference ratio (SIR) on SU 2's mth antenna and EVM will be defined shortly. (iii) Error vector magnitude (EVM) of the decoded signals at SU 2: EVM is widely used for evaluating the performance of a wireless receiver. It is defined as $\text{EVM} = 10\log_{10}\left(\mathbb{E}\big[|\hat{X}_{\text{s}}^{[2]}(l,k) - X_{\text{s}}^{[2]}(l,k)|^2\big]/\mathbb{E}\big[|X_{\text{s}}^{[2]}(l,k)|^2\big]\right)$. (iv) Throughput of the secondary network: The throughput is inferred based on the measured EVM at SU 2 and the modulation and coding scheme (MCS) specified in 802.11 standard [15], without taking into account communication overhead. It is calculated by

$$r = \frac{1}{2} \cdot \frac{48}{80} \cdot b \cdot \gamma(\text{EVM}), \tag{18}$$

where $1/2$ refers to the half-time use of the spectrum (see Fig. 3), 48 is the number of payload subcarriers, 80 is the number of samples in an OFDM symbol, b is the bandwidth (5 MHz), and $\gamma(\text{EVM})$ is the average number of bits carried by one subcarrier in an OFDM symbol and it is given in Table I.



(a) In the case when SU 1 uses $[\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}]$ as precoder.

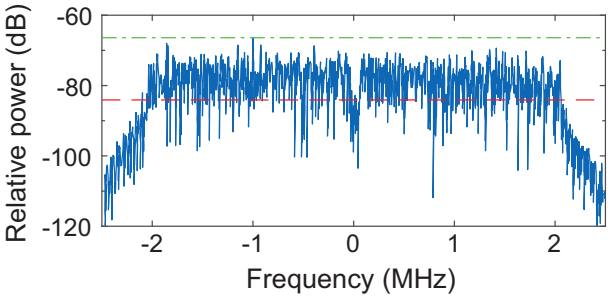


(b) In the case when SU 1 use our proposed blind beamforming.

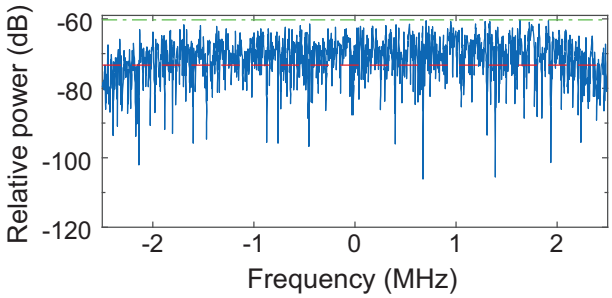
Fig. 10: Relative power spectral density of PU 2's received interference from SU 1.

B. A Case Study

We use a case study to demonstrate the performance of the proposed spectrum sharing scheme. In this case study, we place the secondary users at *Loc 1* in Fig. 9 and use CDMA-based PHY for the primary users.

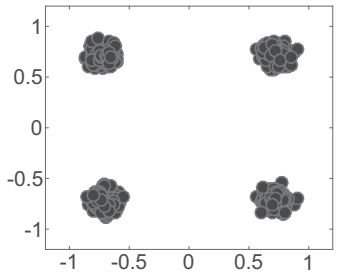


(a) Received signal from SU 1

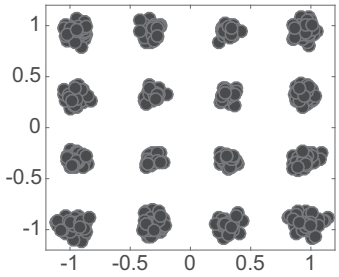


(b) Received interference from PU 1

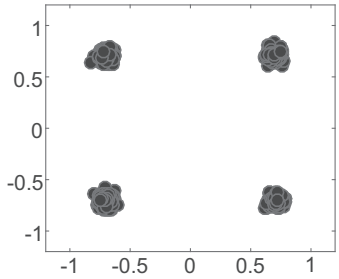
Fig. 11: Relative power spectral density of SU 2's received signal and interference on its first antenna.



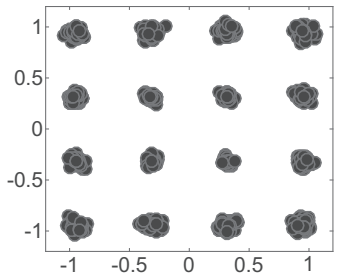
(a) Decoded QPSK signals at SU 2 in the proposed scheme



(b) Decoded 16QAM signals at SU 2 in the proposed scheme



(c) Decoded QPSK signals at SU 2 in interference-free case



(d) Decoded 16QAM signals at SU 2 in interference-free case

Fig. 12: Constellation diagram of the decoded signals at SU 2 in two cases: in presence of cross-network interference from PU 1 *versus* in an interference-free case (PU 1 is turned off).

Transmitter-Side IC Capability: We quantify the transmitter-side IC capability from the proposed beamforming technique at SU 1. To do so, we turn off the primary transmitter (PU 1) and measure the received interference power spectral density at the primary receiver (PU 2) in two cases: (i) using $[\frac{1}{\sqrt{2}} \ \frac{1}{\sqrt{2}}]$ as the precoder; and (ii) using our proposed beamforming precoder in (6) and (7) with $\alpha_1 = 1$. Fig. 10 presents our experimental results. We can see that in the first case, the average relative power of PU 2's received interference is about -87 dB; in the second case, the average relative power of PU 2's received interference is about -113 dB. The transmitter-side IC capability from the proposed beamforming technique is about $-87 - (-113) = 26$ dB in this case.

Note that, based on our observations, the average relative power of the noise at PU 2 in this case varies in the range of -120 dB to -110 dB. We therefore conclude that by using the blind beamforming technique, the interference from the secondary transmitter has negligible impact on the primary receiver.

Receiver-Side EVM, IC Capability, and Throughput: We now study the performance of the proposed BIC technique at the secondary receiver (SU 2) to see if it can successfully decode its desired signal in the presence of interference from the primary transmitter (PU 1).

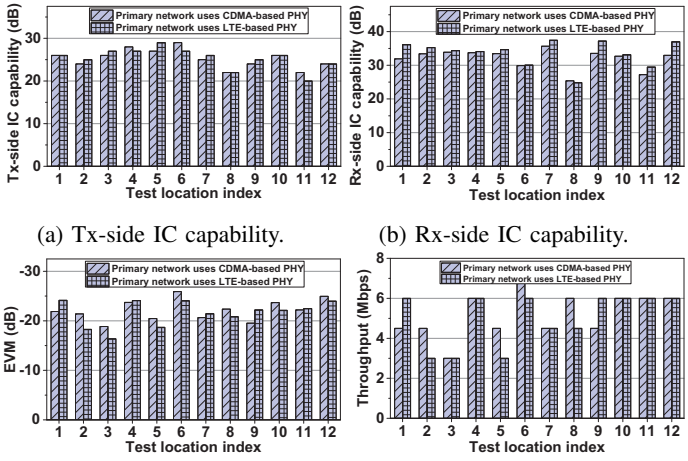
Firstly, we measure the SIR at SU 2's two antennas. For ease of explanation, we assume that the noise is negligible in this case. Fig. 11 shows our experimental results from SU 2's first antenna. We can see that the average relative power of its received signal and interference is -83 dB and -73 dB, respectively. This means that the SIR on SU 2's first antenna is -10 dB. Using the same method, we measured that the SIR on SU 2's second antenna is -12 dB.

Secondly, we measure the EVM of SU 2's decoded signals in the presence of interference. Fig. 12(a–b) present the constellation diagram of the decoded signal at SU 2 when blind beamforming is used at SU 1 and BIC is used at SU 2. It is evident that SU 2 can decode both QPSK and 16QAM signals from SU 1 in the presence of interference from PU 1. The measured EVM of the decoded signals at SU 2 is -21.9 dB when QPSK is used and -22.0 dB when 16QAM is used. As a performance benchmark, Fig. 12(c–d) present the experimental results when there is no interference from PU 1. Comparing Fig. 12(a–b) to Fig. 12(c–d), we can see that SU 2 can successfully decode its desired signals in the presence of unknown interference from PU 1.

Finally, we calculate SU 2's IC capability and throughput. Based on the measured SIR on SU 2's antennas and the measured EVM of its decoded signals, SU 2's IC capability is $-(-21.9) - \max\{-10, -12\} = 31.9$ dB in this case. Based on the formula in (18) and the measured EVM, the inferred throughput in this case is 4.5 Mbps. Note that the throughput calculation has taken into account the airtime overhead caused by blind beamforming (i.e., Phase I in the proposed MAC protocol).

C. Experimental Results at All Locations

We now present the experimental results in all 12 locations. **Transmitter-Side IC Capability:** Fig. 13(a) presents the transmitter-side IC capability of the two-antenna secondary



(a) Tx-side IC capability. (b) Rx-side IC capability.

(c) EVM of the decoded signals. (d) Secondary network throughput

Fig. 13: Performance evaluation of the secondary network at 12 different locations when primary network uses CDMA-based and LTE-based PHY.

transmitter. We can see that in all the locations, the secondary transmitter has more than 20 dB IC capability regardless of the PHY used in the primary network. On average over the 12 locations, the proposed blind beamforming technique achieves 25.3 dB IC capability for the secondary transmitter.

Receiver-Side IC Capability: Fig. 13(b) presents the receiver-side IC capability of the two-antenna secondary receiver. We can see that in all the locations, the secondary receiver has more than 25 dB IC capability regardless of the PHY used in the primary network, and achieves an average of 32.8 dB IC capability at the 12 test locations.

EVM: Fig. 13(c) presents the measured EVM of the decoded signals at the two-antenna secondary receiver in the face of interference from the primary transmitter. We can see that the measured EVM is less than -16.35 dB at all 12 test locations, no matter which PHY (LTE or CDMA) is used in the primary network. The average EVM at the 12 locations is -21.8 dB.

Throughput of Secondary Network: Fig. 13(d) presents the throughput of the secondary network using the legacy 802.11 PHY. We can see that the secondary network can achieve more than 3 Mbps in 5 MHz bandwidth in all 12 locations, without harmfully affecting the performance of the primary network. On average, the data rate at the 12 test locations is 5.1 Mbps in 5 MHz bandwidth. This means that our underlay spectrum sharing scheme can achieve an average of 1.02 bit/s/Hz spectrum efficiency for the secondary network.

VIII. Conclusion

In this paper, we proposed a practical underlay spectrum sharing scheme for the secondary users in CRNs. The key components of our scheme are two MIMO-based IC techniques. One is a blind beamforming technique for secondary transmitters and the other is a BIC technique for a secondary receiver. With these two IC techniques, the secondary network can tame the cross-network interference without requiring the knowledge of the primary network and without requiring coordination from the primary network. Based on these two IC techniques, we develop a lightweight MAC protocol to enable underlay spectrum sharing in CRNs. We have built a prototype of our underlay spectrum sharing scheme on a wireless testbed. Experimental results show that the secondary users can achieve an average of 1 bit/s/Hz spectrum efficiency without degrading the performance of the primary users in a real-world office building environment. This paper made a concrete step towards bridging the gap between theory and practice for the research of CRNs.

Acknowledgment

We would like to thank the anonymous reviewers for their valuable comments and feedback. This project was partially supported by the NSF under Grant CNS-1717840.

References

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[2] S. He, Y. Huang, H. Wang, S. Jin, and L. Yang, "Leakage-aware energy-efficient beamforming for heterogeneous multicell multiuser systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1268–1281, 2014.

[3] H. Pennanen, A. Tölli, and M. Latva-aho, "Multi-cell beamforming with decentralized coordination in cognitive and cellular networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 2, pp. 295–308, 2014.

[4] A. Tajer, N. Prasad, and X. Wang, "Robust linear precoder design for multi-cell downlink transmission," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 235–251, 2011.

[5] E. A. Gharavol, Y.-C. Liang, and K. Mouthaan, "Robust downlink beamforming in multiuser MISO cognitive radio networks with imperfect channel-state information," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 2852–2860, 2010.

[6] L. Zhang, Y. Xin, and Y.-C. Liang, "Weighted sum rate optimization for cognitive radio MIMO broadcast channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, 2009.

[7] E. Yaacoub and Z. Dawy, "Enhancing the performance of OFDMA underlay cognitive radio networks via secondary pattern nulling and primary beam steering," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1476–1481, 2011.

[8] A. Manolakos, Y. Noam, K. Dimou, and A. J. Goldsmith, "Blind null-space tracking for MIMO underlay cognitive radio networks," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 1223–1229, 2012.

[9] Y. Noam and A. J. Goldsmith, "Blind null-space learning for MIMO underlay cognitive radio with primary user interference adaptation," *IEEE Transactions on Wireless Communications*, vol. 12, no. 4, pp. 1722–1734, 2013.

[10] V.-D. Nguyen, C. T. Nguyen, H. V. Nguyen, and O.-S. Shin, "Joint beamforming and antenna selection for sum rate maximization in cognitive radio networks," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1369–1372, 2017.

[11] S. Kusaladharma and C. Tellambura, "Secondary user interference characterization for spatially random underlay networks with massive MIMO and power control," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 7897–7912, 2017.

[12] C. Shepard, H. Yu, N. Anand, E. Li, T. Marzetta, R. Yang, and L. Zhong, "Argos: Practical many-antenna base stations," in *Proceedings of ACM MobiCom*, pp. 53–64, 2012.

[13] E. Blossom, "GNU radio: Tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.

[14] Ettus Research, "USRP N210," *www.ettus.com/product/details/UN210-KIT [Online; accessed 8-March-2018]*.

[15] IEEE 802.11ac, "IEEE standard for information technology local and metropolitan area networks part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Enhancements for higher throughput," *IEEE Standards 802.11ac*, 2014.