MIMO-based Jamming Resilient Communication in Wireless Networks

Qiben Yan* Huacheng Zeng* Tingting Jiang* Ming Li† Wenjing Lou* Y. Thomas Hou*
* Virginia Polytechnic Institute and State University, Blacksburg, VA, USA
† Utah State University, Logan, UT, USA

***Abstract*—Reactive jamming is considered the most powerful jamming attack as the attack efficiency is maximized while the risk of being detected is minimized. Currently, there are no effective anti-jamming solutions to secure OFDM wireless communications under reactive jamming attack. On the other hand, MIMO has emerged as a technology of great research interest in recent years mostly due to its capacity gain. In this paper, we explore the use of MIMO technology for jamming resilient OFDM communication, especially its capability to communicate against the powerful reactive jammer. We first investigate the jamming strategies and their impacts on the OFDM-MIMO receivers. We then present a MIMO-based anti-jamming scheme that exploits interference cancellation and transmit precoding capabilities of MIMO technology to turn a jammed non-connectivity scenario into an operational network. Our testbed evaluation shows the destructive power of reactive jamming attack, and also validates the efficacy and efficiency of our defense mechanisms.**

I. Introduction

Orthogonal frequency-division multiplexing (OFDM) has developed into a popular scheme for broadband wireless communications. Modern wireless communication systems, such as WLAN, digital TV systems and cellular communication systems, all adopt OFDM as one of the primary technologies. While OFDM systems are robust against multipath fading and have the ability to cope with severe interference and noise, they are not ideal for environments where adversaries try to intentionally jam communications.

Jamming has been a major denial-of-service attack to wireless communications [1], [2]. By intentionally emitting jamming signals, adversaries can disturb network communications, resulting in throughput degradation, network partition, or a complete zero connectivity scenario. Reactive jamming is one of the most effective jamming attacks. A reactive jammer continuously listens for the channel activities, and emits jamming signals whenever it detects activities, otherwise it stays quiet when the sender is idle. Reactive jamming is regarded as one of the most effective, stealthy, and energy-efficient jamming strategies [3], [4]. The recent advance in the highly programmable software defined radio has made such sophisticated but powerful jamming attacks very realistic – [5], [6] demonstrated that a reactive jammer is readily implementable and the jamming results devastating.

The increasingly severe hostile environments with advanced jamming threats prompt the development of security extensions to the OFDM systems. Some recent works investigate and attempt to alleviate the impacts of jamming attacks to the OFDM systems. Han et al. [7] proposed a jammed pilot detection and excision algorithm for OFDM systems to counteract narrow-band jammer that jams the pilot tones. Clancy et al. [8] further introduced pilot nulling attack that minimizes the received pilot energy to be more destructive, and provided mitigation schemes by randomizing the location and value of pilot tones. However, they both specifically focus on the adversaries jamming pilot tones, who require knowing the pilot locations and also demand very tight synchronization. Moreover, their defense mechanisms will fail to recover signals when all the OFDM subcarriers including the pilots are jammed as in the case of reactive jamming attack.

On the other hand, multi-input multi-output (MIMO) has emerged as a key technology for wireless networks mostly due to its potential capacity gain. New wireless devices are equipped with a growing number of antennas. MIMO can be exploited to obtain diversity and spatial multiplexing gains, and lead to an increase in the network capacity. More importantly, recent advance in MIMO interference cancellation (IC) technique [9]–[11] has greatly enhanced MIMO communication capability under multiple concurrent transmissions. This inspires us to ponder: whether it is possible to exploit IC technique in MIMO to mitigate jamming attacks targeting OFDM systems, in particular, software radio based reactive jamming attacks. In this paper, we try to answer this question by first examining the jammer's capability in disrupting OFDM-MIMO communications, and then devising MIMO-based defense mechanisms by utilizing MIMO technology coupled with IC and transmit precoding techniques. We show that our design is able to restore admissible OFDM communication in the presence of reactive jammers.

The similarity between interference cancellation and jamming resistance is obvious– both the interferer and the jammer lead the desired signals to be non-decodable at the receiver side. They are also different– jamming signals are sent by malicious jammers deliberately, who can intentionally alter the jamming signals for best jamming effect or to evade anti-jamming technique, while the interferer introduces interference inadvertently. Hence, jamming signals that can be purposefully and rapidly altered are much harder to track and remove than conventional interference.

Consequently, designing the effective defense mechanism faces several key challenges. *First*, since different jammers emit different types of jamming signals, the receiver needs to cancel them regardless of their signal structures. *Second*, an effective defense mechanism should be able to track the jammers' purposeful adaptation. *Finally*, the defense mechanism should be robust against sophisticated jammers attempting to

This work was supported in part by NSF under grants CNS-1343222, CNS-1247830, CNS-1156318, and CNS-1156311, and by ONR under grant N000141310080.

978-1-4799-3360-0/14/$31.00 ©2014 IEEE

disrupt the receiver's cancellation scheme.

To address these challenges, we propose a novel defense mechanism for jamming resilient OFDM communication based on MIMO IC technique, which tracks the jamming signal's direction in real-time before canceling it out. We devise an *iterative channel tracking* mechanism using multiple pilots to estimate the sender and jammer's channels alternately and iteratively in a timely fashion. More importantly, we introduce an enhanced defense mechanism leveraging *signal enhancing rotation* and message feedback techniques, which strategically enhances the projected sender signal strength via signal rotation, resulting in an improved anti-jamming performance. A tactical IC scheme is designed not only to protect the forwarding frame transmission, but also to guard the feedback messages against jamming.

The goal of this paper is to sustain operational OFDM communications under reactive jamming attack. The contributions of this paper are two-fold: (1) we exploit the MIMO IC and transmit precoding techniques to counteract reactive jamming attacks for securing OFDM wireless communications. We propose two novel mechanisms: *iterative channel tracking* and *signal enhancing rotation* to effectively sustain acceptable throughput under reactive jamming attack; (2) we implement the jamming attack and defense mechanisms using USRP radios, and conduct extensive experiments to evaluate the performance in terms of packet delivery rate. The experimental results show that in the presence of a reactive jammer, the packet delivery rate improves significantly using our enhanced defense mechanism with signal rotation.

II. Problem Formulation

In this section, we present the system model, define the attack model and lay out preliminary knowledge of OFDM-MIMO networks.

A. System Model

We consider an adverse wireless environment with a jammer targeting at the communication link established by a sender and a receiver. We consider the jammer as a common single-antenna device, who is capable of taking any attack strategy to be most destructive.

The frames in OFDM wireless communications have signal structures as shown in Fig. 1. A preamble is transmitted ahead of the data, which is used for signal acquisition, time synchronization and initial channel estimation. We assume the sender transmits when the jammer is not jamming, either by taking a random backoff between transmissions or by sensing jamming activity [12]. We assume every sender and the intended receiver share a secret key that is unknown to the jammer.

Let P_{SR} and P_{JR} be the received signal powers from S and J respectively. The signal-to-jamming ratio (SJR) at receiver R can be expressed as P_{SR}/P_{JR}, which determines the decoding performance. We do not consider the noise and interference, since they are negligible when compared to the jamming power.

B. Attack Model

There are three typical jamming attack models: 1) constant jammer continuously transmits jamming signals to corrupt packet transmission. He/She has the capability of covering the whole frame structure, whereas his/her energy consumption is extremely high, rendering himself/herself easily discoverable; 2) random jammer is more energy-efficient, as he/she emits jamming signals at random time for a random duration. However, his/her jamming capability is limited due to the randomized jamming behavior; 3) reactive jammer is more effective, energy-efficient and stealthier [3], which is the main focus of this paper.

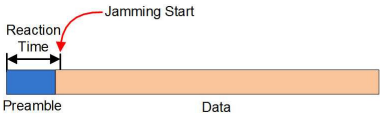


Fig. 1: Reactive jammer starts jamming after certain reaction time

The key feature of reactive jammer is sensing-before-jamming. The jamming reaction time denotes the time difference between the arrival of the original signal and the jamming signal at the receiver. It takes a reactive jammer a minimum *reaction time* to perform channel sensing and jamming initialization before sending out jamming signals, during which the preamble of the frame could be transmitted without being jammed [5], [12], as shown in Fig. 1.

In our experiment, a preamble takes only one OFDM symbol, which lasts $128\mu s$ with $1MHz$ bandwidth. On the other hand, the jammer, who is agnostic to the implementation details of the network (e.g., the transmission protocol and preamble symbols), can only carry out energy detection [13], which requires more than $1ms$ to detect the signal for a 0.6 detection probability and $-110dBm$ signal strength, when implemented in a fully parallel pipelined FPGA [14]. Even the advanced software radio based reactive jammer, who is aware of the implementation details of the network, still incurs a considerable reaction delay to process the incoming signal and to make a jamming decision, during which the preamble of a frame is successfully delivered to the receiver without being disturbed [5], [6].

In addition, the jammer can transmit arbitrary signals with/without any signal structures. The jammer is also capable of jamming the whole spectrum, invalidating the traditional spread spectrum anti-jamming methods [12], [15]. However, we assume the jammer cannot perform full-duplex communications, which essentially disallows the jammer to sense and jam simultaneously.

C. MIMO Interference Cancellation and OFDM Basics

In a MIMO network, the spatial multiplexing gain can be represented by a concept called *Degrees-of-Freedom* (DoF), which is defined as the dimension of *received signal space* over which concurrent communications can take place [16]. DoF indicates the number of concurrently transmitted streams that can be reliably distinguished at a MIMO receiver.

Consider a 1×2 MIMO communication between sender S and receiver R as shown in Fig. 2, the signals $\binom{x_s}{x_j}$ from the sender and jammer respectively are transmitted concurrently through the channel $\mathbf{H}$, and the received signals can be written as:

$$\binom{y_1}{y_2} = \binom{h_s}{h'_s} x_s + \binom{h_j}{h'_j} x_j, \quad (1)$$

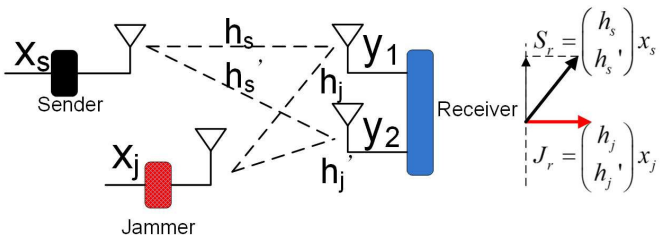


Fig. 2: 1×2 OFDM-MIMO link attacked by a Jammer

which live in a two-dimensional vector space corresponding to two receive antennas.

In order to decode x_s, the IC technique is utilized to remove the interference from x_j by projecting the received signals onto the subspace orthogonal to x_j (see Fig. 2), i.e., $[h'_j, -h_j]$, yielding the projected signal as:

$$y_{proj} = h'_j y_1 - h_j y_2 = (h'_j h_s - h_j h'_s) x_s. \quad (2)$$

After that, the projected signal can be decoded using any standard decoder. This IC technique is also called *Zero-Forcing* (ZF). Note that, estimating jammer's signal direction[1] is the core of ZF decoder. A loss of original signal amplitude after projection is observed from Fig. 2.

OFDM divides the spectrum into multiple narrow subbands called subcarriers. The receiver operates on each subcarrier, and applies FFT to the received signal for demodulation. This allows many narrowband signals to be multiplexed in the frequency domain, which greatly simplifies the channel estimation and equalization. In this paper, the sender and receiver establish OFDM communications with the signals of interest as OFDM-modulated signals.

Note that Eq. (1) assumes a narrowband channel, where h (such as h_s, h_j, etc) appears simply as a complex number. However, for wideband channels, the signals at different frequencies will experience different channels, bringing so called multi-path effects. As a result, h will become a complex vector indexed by different frequency responses. Yet, Eq. (1) still holds for each OFDM subcarrier in the OFDM communications, such that MIMO IC is carried out over each subcarrier.

III. Impact of Reactive Jamming Attack to OFDM-MIMO Communications

In this section, we characterize the impact of reactive jammer to the OFDM-MIMO communications. Without loss of generality, we explain the jamming strategy in the context of a two-antenna receiver decoding a single transmission from the sender in Fig. 2. The sender and receiver form a 1×2 MIMO link of two DoF with one DoF consumed by the jammer.

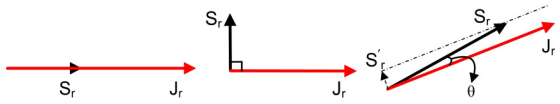
According to Eq. (1), the received frequency-domain signals for each OFDM subcarrier i are shown below:

$$y_{1i} = h_{ji} x_{ji} + h_{si} x_{si}, \quad (3)$$

$$y_{2i} = h'_{ji} x_{ji} + h'_{si} x_{si}, \quad (4)$$

where h_{ji}, h'_{ji}, h_{si} and h'_{si} are frequency version of channels at subcarrier i, and x_{ji} and x_{si} are frequency-domain signals

[1]Signal direction is determined by the received signal vector induced on the receive antenna array by the transmitted signal [16], which is defined in the antenna-spatial domain and not the I-Q domain.



(a) Overlap Signals (b) Orthogonal (c) Small angle

Fig. 3: Different two-dimensional received signal spaces

from the jammer and sender. Note that the jamming signals need not be OFDM-modulated narrowband signals, and x_{ji} simply represents the narrowband portion of jamming signals on i-th OFDM subband. As mentioned in Section II-C, the MIMO IC technique is carried out over each subcarrier to recover the legitimate signal, which is deemed as the key to the data recovery process. Naturally, the MIMO IC technique becomes the target of the jammer.

We reformulate Eqs. (3), (4) as follows (in the following, we omit the subscript notation i for i-th subcarrier):

$$\binom{y_1}{y_2} = \mathbf{H}\binom{1}{0} x_j + \mathbf{H}\binom{0}{1} x_s, \quad (5)$$

where $\mathbf{H} = \begin{bmatrix} h_j & h_s \\ h'_j & h'_s \end{bmatrix} = [\mathbf{h}_j, \mathbf{h}_s]$ is the 2×2 channel matrix. The received signals are the sum of two vectors $J_r = \mathbf{H}[1\ 0]^T x_j$ and $S_r = \mathbf{H}[0\ 1]^T x_s$, as shown in Fig. 2. We find that the angle[2] between J_r and S_r, determined by $\mathbf{h}_j$ and $\mathbf{h}_s$, can be exploited by the jammer to launch effective attack.

Attacking MIMO Interference Cancellation. In order to understand the attack strategy, we inspect three special scenarios in Fig. 3 with different received signal spaces. Undoubtedly, the most severe attack is depicted in Fig. 3(a), in which J_r overshadows S_r in the received signal space, preventing S_r from being recovered. On the contrary, the least powerful attack emits a jamming signal that is orthogonal to the legitimate signal as shown in Fig. 3(b), in which the projected signal is equivalent to the original signal, yielding the highest projected signal amplitude. Fig. 3(c) shows a case in between the above two extreme cases, where the angle between two received signals takes a small value. Therefore, by manipulating the jamming signal direction, the jammer has the potential of affecting the effectiveness of MIMO IC mechanism.

Correspondingly, the jammer's attack strategy is to shrink the angle between the jamming signal and the intended signal by moving towards the vicinity of the sender. As a matter of fact, the difference between $\mathbf{h}_s$ and $\mathbf{h}_j$ deviates according to the distance between S and J [17]. More specifically, if the spacing between two antennas is narrower than a half wavelength, the channels from these two antennas will become highly correlated [16], which renders two received signal directions similar.

In order to demonstrate the effectiveness of such attack strategy, we perform an experiment on a 1×2 MIMO link of Fig. 2 by varying the distance between the jammer and sender's antennas. Fig. 4 shows the *packet delivery rate* (PDR) performance, in which sender's PDR drops to zero when the antenna distance decreases below $6cm$.

[2]The angle between two received signal vectors is equal to the angle between two channel vectors, computed by $cos\theta = \frac{|\mathbf{h}_j^H \cdot \mathbf{h}_s|}{\|\mathbf{h}_j\| \|\mathbf{h}_s\|}$. The angle's range is $[0, \frac{\pi}{2}]$.

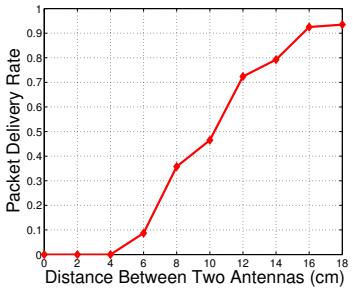


Fig. 4: Jamming attack performance by approaching the sender's location (in this experiment, the device works on 2.45GHz central frequency with a half wavelength $\frac{\lambda}{2} = \frac{c}{2f} \approx 6.12cm$)

IV. Defense Mechanisms Against Reactive Jamming Attack

In this section, we propose effective MIMO-based defense mechanisms to counteract reactive jamming attack based on IC technique. We first develop an *iterative channel tracking* mechanism to cancel arbitrary jamming signals by keeping track of the jamming signal direction. Then, we build an enhanced defense mechanism by incorporating *signal enhancing rotation* to enable a more robust OFDM communication.

As opposed to the attack strategy to shrink the angle between two arrival signals, the defense mechanism attempts to expand the angle. We address two major issues in this section: 1) how to decode the signals of interest in the presence of arbitrary jamming signals; 2) how to strengthen the robustness of OFDM communications against adaptive and reactive jammer.

A. Defense Mechanism Overview

We offer an overview of proposed defense mechanisms in this section. The defense mechanism mainly includes angle expansion, signal decoding (Section IV-B), channel tracking (Section IV-B) and jamming detection (Section IV-C) modules. Angle expansion module aims at expanding the angle of arrival signals to make intended signals decodable. As long as the jammer fails to approach the sender, the channels $\mathbf{h}_s$ and $\mathbf{h}_j$ will be uncorrelated, resulting in a random angle between S_r and J_r, and thus a high decoding rate. To prevent the jammer from getting close is straightforward, the sender can move randomly inside the receiver's reception range to avoid being approached. Alternatively, spatial retreat [18] technique can be utilized to strategically move away from the jammer. Then, signal decoding is implemented using MIMO IC technique after channel estimation. Meanwhile, jamming detection module intends to instantly identify the beginning and end of a jamming attack to trigger the defending process.

Enhanced defense mechanism (Section IV-D) involves signal enhancing rotation module, for rotating the transmitted signal to improve sender signal decodability. It also incorporates a feedback mechanism to reliably guide the sender's rotation process.

B. Decoding the Signal of Interest

According to Eqs. (2), (5), the estimation of the sender's and jammer's channels is the most crucial task in jamming-resistant solution based on MIMO IC technique. Initial estimation of sender's channel $\mathbf{h}_s$ can be derived via analyzing the undisturbed preamble. However, since initial channel estimation is only valid within the channel coherence time, updating the channel estimation over time becomes a necessity.

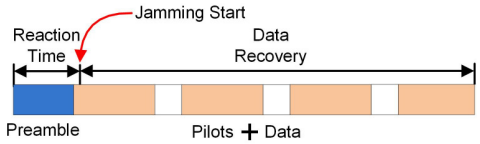


Fig. 5: Extended frame structure

Inspired by ZigZag decoding technique [19], we devise an iterative channel tracking mechanism by jointly keeping track of both the sender and jammer's channel conditions in a timely manner. In the following, we first exhibit jammer channel estimation method, and then present the iterative mechanism for updating both channels iteratively.

Jammer Channel Estimation. Without pre-known preambles in the jamming signals, it is difficult to carry out jammer channel estimation. Fortunately, the most recent advance [10] shows that the complete knowledge of $\mathbf{h}_j = [h_j, h'_j]^T$ is not necessary for decoding x_s. Due to the nice scale invariance property of signal direction, i.e., the direction of $[h_j, h'_j]^T$ is equivalent to that of $[\frac{h_j}{h'_j}, 1]^T$, the only information required about jamming signal for IC to work is the signal direction, i.e. jammer's channel ratio $\frac{h_j}{h'_j}$.

Note that the received signal is a mixed signal $J_r + S_r$. If we can extract jammer's signal $J_r = (\frac{h_j}{h'_j})x_j$, we can derive the jammer's channel ratio by computing the ratio of received jamming signals on two receiving antennas, as $\frac{h_j}{h'_j} = \frac{x_j \cdot h_j}{x_j \cdot h'_j}$. Based on this derivation, We propose the following method to enable the extraction of the jamming signal J_r so that the channel ratio can be computed.

As shown in Fig. 5, the basic idea of extracting the received jamming signal J_r is to insert known symbols (i.e. pilots) in the original data frame, and then subtract them from the received mixed signal. The location of the inserted pilots should remain secret between the sender and intended receiver, because if the jammer learns the locations of the pilots, he/she can intentionally stop jamming during these pilot periods to avoid being tracked. Moreover, the pilots should be inserted frequently to enable frequent updates of the channel estimation. Note that, the extension of the frame structure introduces limited overheads, which will be evaluated in Section VI-D.

The complete jammer channel estimation scheme proceeds as follows: 1) after detecting the beginning of jamming (refer to Section IV-C), the intended receiver finds the next jammed pilots; 2) the received pilots are reconstructed using the known pilot symbol transformed by the estimated sender's channel (sender channel estimation is presented below); 3) the constructed received pilots are subtracted from the jammed pilots to restore the jamming signal; 4) the extracted jamming signal is used to compute the jammer's channel ratio (jamming signal direction).

Iterative Channel Tracking Mechanism. For IC to work, we need the estimations of both the sender channel and the

jammer channel. When the channel is being jammed, deriving an accurate estimation of sender channel is a difficult task. In addition, wireless channels are time-varying due to inevitable multipath fading. Jammers are also motivated to vary the channel in order to evade the defense mechanism. To keep the channel estimation updated and accurate, we need to carry out the channel estimation frequently. However, the estimation of both channels under the jamming situation is hard - we have two channel responses to estimate and the received signal is a mixed signal with two unknown signal components.

We propose the following alternating and iterative method to keep track of the sender and jammer channels. The key idea of the proposed method is that, we will not be able to calculate the two channel estimations given two unknown signals. However, we will be able to estimate one channel if the other is known. We can make the initial sender channel estimation after receiving the preamble. Assume there was no jamming signal, the initial sender channel response can be estimated as:

$$H_s(0) = \binom{h_s(0)}{h'_s(0)} = \binom{y_1}{y_2}/x_s^{\diamond}, \tag{6}$$

where $x_s^{\diamond}$ denotes the known pilots. We will then do the sender and jammer channel estimations alternately for every pilot received. Assume the pilots are numbered as $i = 1, ..., n$. After receiving the first pilot (or odd numbered pilot), the receiver updates the jammer channel ratio as:

$$h_j(i)/h'_j(i) = \frac{y_1 - x_s^{\diamond} \cdot h_s(i-1)}{y_2 - x_s^{\diamond} \cdot h'_s(i-1)}, \ i = 1, 3, ..., \tag{7}$$

where we assume the sender channel did not change in the past time slot. Similarly, after receiving the second pilot (or an even numbered pilot), the receiver updates the sender channel estimation $H_s(i) = \binom{h_s(i)}{h'_s(i)}$ according to:

$$h_s(i) - \frac{h_j(i-1)}{h'_j(i-1)} h'_s(i) = (y_1 - \frac{h_j(i-1)}{h'_j(i-1)} y_2)/x_s^{\diamond}, \ i = 2, 4, ..., \tag{8}$$

where we assume the jammer channel did not change in the past time slot. Two unknown sender channel components $h_s(i)$ and $h'_s(i)$ in Eq. (8) are updated alternately after receiving an even numbered pilot. Specifically, $h_s(i)$ gets updated when $i = 4, 8, ...$, while $h'_s(i)$ gets updated when $i = 2, 6, ...$, by assuming the other channel component did not change over the past two time slots. This updating process continues in such a way that the sender and jammer channels are updated alternately. Note that this mechanism requires very frequent channel updates, within the channel coherence time, which can be as short as tens of OFDM symbol time [20] in some application scenarios. On the other hand, this frequent channel updates help us to keep close track of the jammer's potential fast adaptation.

Sender Signal Decoding. Based on Eq. (2), the signal of interest x_s^* can be written as:

$$x_s^* = \frac{y_1 - \frac{h_j}{h'_j} y_2}{h_s - \frac{h_j}{h'_j} h'_s}, \tag{9}$$

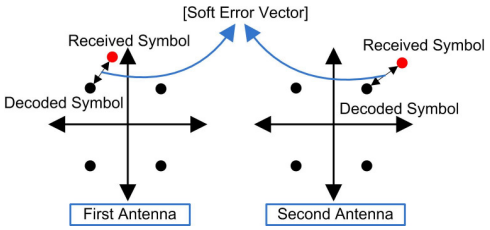


Fig. 6: Soft error vector in QPSK constellation

in which $\frac{h_j}{h'_j}$ is updated every odd numbered pilot in Eq. (7), and $(h_s - \frac{h_j}{h'_j} h'_s)$ is updated every even numbered pilot in Eq. (8). With precise and frequent updates of channel estimation, the signal of interest can be correctly recovered using any standard decoder.

Inter-Symbol Interference Issue. Another practical issue with the wideband jamming signal is that it suffers from multipath effects, which leads to inter-symbol interference (ISI). ISI of jamming signals will impose additional noise to Eq. (5). To counteract ISI, we average our channel tracking results derived from multiple pilots within channel coherence time to mitigate the negative effects of ISI on channel estimation. While it is not a problem for accurate channel estimation, this additional noise would reduce the SNR of the intended signal, hence, affects the throughput. To address ISI issue, we must directly investigate the time-domain signal, since ISI is inherently a time-domain phenomenon. We apply the method in [10] to deal with ISI issue, i.e., we convolute the received time-domain signals with a filter constructed by taking the IFFT of jammer's channel ratio to cancel out the ISI and jamming signal simultaneously. The signal of interest can then be decoded using a standard decoder.

C. Detecting the Jamming Signal

As mentioned in previous section, the receiver needs to detect the beginning and end of jamming to facilitate IC mechanism. The jamming detection problem has been studied in [12], in which the constellation diagrams are employed to identify jammed symbols. We follow the same principle. *Soft error vector* is utilized to build the detection metric, defined as the distance vector between the received symbol vector and the nearest constellation points in the I/Q diagram, as shown in Fig. 6. The soft error is further normalized by minimum distance of the constellation. We assume the normalized soft error vector is $\|\mathbf{V}_k\|$ for k-th received symbol, then the jamming detection metric is defined as $\|\mathbf{V}_k\|/\|\mathbf{V}_{k-1}\|$ at k-th symbol time, which is named as *jumped value*. Jamming attack is supposed to start when $\|\mathbf{V}_k\|/\|\mathbf{V}_{k-1}\| > \gamma$, where γ is a pre-defined threshold for jamming detection. Jamming attack stops if the jumped value returns to normal. In our system design, we discover a potential jammer by identifying a jump that is higher than doubling the errors with the jamming attack, so that $\gamma = 2$.

D. Enhanced Defense Mechanism

The fundamental idea of IC is to project the received sender signal to the direction that is orthogonal to the received jammer signal. As shown in Fig. 3, the signal after projection will have a reduced signal amplitude, depending on the angle between the two signals. The IC method is most effective

when the sender signal and the jammer signal are orthogonal [10], [21]. Therefore, another approach we can explore here is to maximize the amplitude of projected sender signal, i.e. to improve the sender signal decodability.

The key idea is to rotate the sender's signal so that the received sender signal is orthogonal to the jamming signal. This mechanism works for a multi-antenna sender. Using a 2×2 MIMO link as an example,

$$\binom{y_1}{y_2} = \mathbf{h}_j x_j + \mathbf{H}_s \binom{1}{0} x_s, \tag{10}$$

where $\mathbf{h}_j$ denotes a two-dimensional channel vector from J to R, and $\mathbf{H}_s$ is the 2×2 channel matrix from S to R. We exploit the nice property of MIMO communications to control the received signal vector along which the signal is received [9]. Instead of multiplying vector $[1\ 0]^T$, MIMO allows the sender to multiply with a different two-dimensional vector $\vec{\mathbf{r}}$, which we call *rotation vector*[3] . After that, the sender will transmit two elements of $\vec{\mathbf{r}} \cdot x_s$, one over each antenna respectively, and the receiver will receive $\mathbf{H}_s \cdot \vec{\mathbf{r}} \cdot x_s$. In this way, the sender is able to control the received signal vector, thus the received signal direction.

Constraints on Rotation Vector. After signal rotation, the received signal can be represented as:

$$\binom{y_1}{y_2} = \mathbf{h}_j x_j + \mathbf{H}_s \vec{\mathbf{r}} x_s,$$

with a 2×2 channel matrix between S, J and R as $\mathbf{H} = \{\mathbf{h}_j, \mathbf{H}_s \vec{\mathbf{r}}\}$. In order to make x_s decodable, $\mathbf{H}$ should remain as a full rank matrix. Thus, one constraint on $\vec{\mathbf{r}}$ is that it cannot reduce the rank of channel matrix.

In addition, the received signal powers from the sender and jammer are $P_{SR} \propto P_s \|\mathbf{H}_s \vec{\mathbf{r}}\|^2$ and $P_{JR} \propto P_j \|\mathbf{h}_j\|^2$, where P_s and P_j are the sender and jammer's transmission powers. From the above formulas, different $\vec{\mathbf{r}}$ may induce different P_{SR} and SJR, which will in turn affect the decoding performance. Therefore, we set $\vec{\mathbf{r}}$ as a *unit vector*, i.e., $\|\vec{\mathbf{r}}\| = 1$, such that P_{SR} can be confined in a reasonable range.

Signal Enhancing Rotation Mechanism. In a 2×2 MIMO link of Eq. (10), signal rotation can be achieved by simply multiplying normalized $\vec{\mathbf{r}} = (\mathbf{H}_s^{-1} \cdot \mathbf{h}_j^{\perp}) / \|\mathbf{H}_s^{-1} \cdot \mathbf{h}_j^{\perp}\| = \mathbf{H}_s^{-1} \cdot [1, -\frac{h_j}{h'_j}]^T / \|\mathbf{H}_s^{-1} \cdot \mathbf{h}_j^{\perp}\|$ to the sender signal, so that the received legitimate signal will be orthogonal to the jamming signal, where $\mathbf{h}_j^{\perp}$ stands for the orthogonal vector of $\mathbf{h}_j$. However, signal enhancing rotation is carried out over sender signal, while the channel estimation is conducted at the receiver side. A feedback mechanism is necessary for sending the rotation vector $\vec{\mathbf{r}}$ calculated at the receiver back to the sender.

A "*burst of packets*" is regarded as a consecutive sequence of packets during the communications as shown in Fig. 7. During each burst, after identifying jamming threats, the sender continuously rotates the transmit signals of the subsequent frame using the computed rotation vector of the previous frame carried by the feedback frame. To reliably feedback rotation vectors in the presence of reactive jammer, we develop a feedback mechanism as follows.

[3]Note that the signal rotation is carried out in the antenna-spatial domain rather than in the I-Q domain.

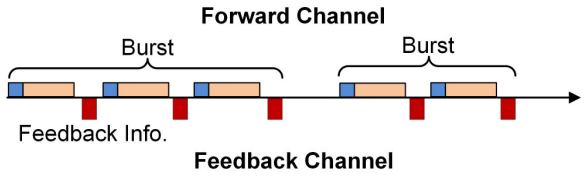


Fig. 7: Burst of packets

Feedback Mechanism. The feedback frame can be formulated using the same frame structure in Fig. 1 because it is short. The same IC technique can be employed to decode the feedback information at the sender, reversing the roles of the sender and receiver in the forward channel. However, during the transmission of packet bursts, it is highly likely that both the feedback packets and the subsequent forwarding packets will be completely jammed by the reactive jammer. In such a scenario, we try to find an opportunity to compute the jammer's channel ratio when the jammer is alone on the medium.

There are various situations that a jammer's isolated transmission could be captured. In the case that the feedback packets are covered by the jamming signals, the jamming signal transmits ahead of the feedback signal, leaving the opportunity of capturing the jammer's isolated transmission, from which the sender can compute the jammer's channel ratio $\frac{h_{js}}{h'_{js}}$ by taking the ratio of two jamming signals received on his/her two antennas $y_{s1} = h_{js} x_{js}$ and $y_{s2} = h'_{js} x_{js}$. The receiver could also delay the transmission of the feedback packet for a random time period so that the sender could capture jammer's isolated transmission right after his/her own transmission finishes. In either case, the sender uses the jammer's channel ratio to eliminate the jamming signal from the received mixed signal $J_r + S_r$, and find the preamble to estimate the feedback channel using Eq. (6), which can be used for signal decoding as usual.

Similarly, the receiver can also use the same mechanism to recover the completely jammed forwarding packets in a packet burst. Two points are worth noting: first, the sender needs to detect the jamming signals to decide whether he/she will apply the rotation vectors to the subsequent packet. In particular, if the sender detects jamming signals when decoding the feedback packet, he/she will apply rotation vectors, assuming the jammer will be active for the subsequent transmission. Second, the feedback information should be received in a timely fashion, because if the channel estimation expires, the rotation vector will no longer be effective. Thus, the sender will count the feedback time to determine whether to apply rotation vectors or not.

V. Implementation

We build a prototype using five USRP-N200 radio platforms [22] and GNURadio software package. Each USRP board is equipped with one XCVR2450 daughterboard operating on 802.11 spectrums. The MIMO cable allows two USRP devices to share reference clock and achieve time synchronization by letting the slave device acquire clock and time reference from the master device. By connecting two USRP boards using MIMO cable to act as one MIMO node, we build a 2×2 MIMO system using four USRP boards. Each MIMO node

runs 802.11-like PHY layer protocol using OFDM technology with 64 OFDM subcarriers. The MIMO system works with various modulation types, while we use BPSK for legitimate communications in our experiments. We configure each USRP to span $1MHz$ bandwidth by setting both the interpolation rate and decimation rate to 100. MIMO IC technique is implemented at the receiver to recover the signals of interest. We also implement the decoding mechanism incorporating signal enhancing rotation at both the sender and receiver sides.

The reactive jammer is another USRP device connected with XCVR 2450 daughterboard. To defend against jamming attack, the receiver first estimates sender's channel and jammer's channel ratio, then uses IC technique to eliminate the signals from the jammer. Meanwhile, the receiver will compute the rotation vector and transmit it back to the sender for signal enhancing rotation. After receiving the rotation vector, the sender checks whether it is still within the predefined channel coherence time since its previous transmission. If it is, the sender will apply the rotation vector to the newly generated symbols and send the rotated elements through two antennas. We set the transmission power of both the sender and jammer as $100mW$.

Implementing a software radio-based reactive jammer is itself a non-trivial task [5], [23]. Here, we emulate the reactive jamming attack and the jammer's carrier sensing process by letting the receiver broadcast a trigger signal. Both the jammer and sender record the timestamp of detecting the trigger t_{trig}, then sender sets its beginning time of transmission as $t_{send} = t_{trig} + t_{\Delta 1}$, and jammer sets its jamming start time as $t_{jam} = t_{trig} + t_{\Delta 2}$. Then, the reactive jammer's reaction time is equivalent to $(t_{\Delta 2} - t_{\Delta 1})$.

VI. Evaluation

In this section, we demonstratively show the ability of jammer to disable MIMO IC mechanism by managing the received signal directions, and we also evaluate the performance of our defense mechanisms in an indoor lab environment. In our experiments, we first show how the received signal direction affects the packet delivery performance. Then, we present our measured channel coherence time in the indoor environment and discuss how it will affect the performance of our defense mechanism. Finally, we exhibit the performance of jamming attack and defense mechanisms under different bandwidth settings.

A. Impact of Received Signal Direction

We argued in Section III that the angle between two received signal directions will affect the decoding performance using IC. In this section, we will show the packet delivery performance with respect to different angles. We set up two clients synchronized by a MIMO cable, together with a two-antenna receiver. Then, two clients transmit different streams to the receiver. The receiver applies IC technique to decode one of the streams by regarding the other stream as interference from the jammer. We mentioned that the signal direction is determined by the channels between the transmitter and the receiver in Section II-C. Although the channel evolves over time, we observe that the angle remains relatively stable for the time being, given the fixed locations of clients and receiver. Then, we change the locations of the clients and receiver to measure the packet delivery performance with different angles between two received signals. We fix the distance between the clients and receiver, so that the performance variation among different cases is mainly induced by different angles, rather than different path losses.

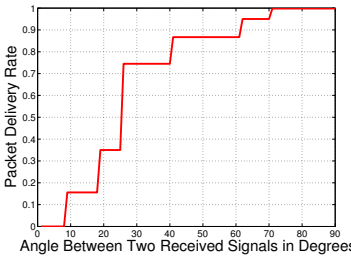


Fig. 8: Packet delivery rate performance with different angles between two received signals

We show the performance measurement in Fig. 8, from which we can see the angle between two received signals indeed affects the packet delivery performance significantly. The major observation is that PDR declines below 20% once the angle becomes smaller than $20°$, while PDR rises above 90% once the angle expands greater than $60°$. This result confirms our analysis.

B. Impact of Channel Coherence Time

The channel coherence time determines how often the channel estimation should be updated and the validity period of the rotation vector. In this section, we measure the channel coherence time in an indoor environment.

We let a sender transmit consecutive known OFDM symbols following a preamble to track the channel variations. The receiver uses these known OFDM symbols to estimate the channel coefficients, and examines how long the channel from the sender to the receiver remains correlated. Each channel coefficient is a complex number with *amplitude* and *phase* values. We investigate multiple subcarriers over several rounds. Fig. 9 shows the autocorrelation of channel phase over multiple subcarriers. The channel phase correlates over multiple OFDM symbols before it becomes uncorrelated (i.e. autocorrelation value becomes zero [20]). The number of correlated OFDM symbols varies with subcarriers, with the average number of 33. On the other hand, the channel amplitude stays more stable over multiple OFDM symbols, whose autocorrelation value shows correlation over 500 OFDM symbols. Therefore, the channel coherence time in our experimental environment is nearly 33 OFDM symbols or $8.5ms$, which indicates that the channel estimation should be updated at least every 30 OFDM symbols, nearly 200 bytes under $500KHz$ bandwidth, or nearly 400 bytes under $1MHz$ bandwidth. Therefore, the pilots should be inserted at least once every 100 (200) bytes of data under $500KHz$ $(1MHz)$ bandwidth, because the estimation of the sender's and jammer's channels is updated alternately every other pilot as shown in Section IV-B. This result also tells us the rotation vector is effective within the 33 OFDM symbol time, after which the rotation vector becomes expired.

Note that during jammer's channel estimation in Section IV-B, we assume jammer's channel keeps static during the channel coherence time. However, mobile jammer has the ability of changing his/her channel conditions in real-

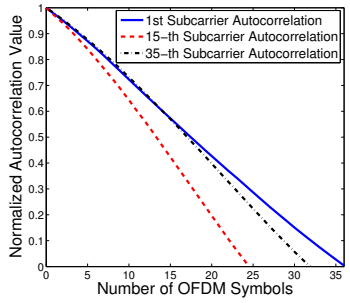


Fig. 9: Autocorrelation of the channel phase in an indoor environment (tested using 500KHz bandwidth communications)

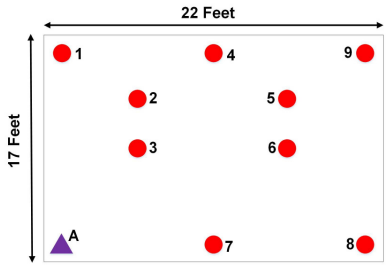


Fig. 10: **Testbed**. The receiver is placed at A, while the sender and jammer are placed at the selected locations 1 to 9.

time. Referring back to Fig. 4, we notice $10cm$ distance change will bring a dissimilar channel, i.e., if the jammer moves $10cm$ within the channel coherence time, not only the jammer's channel estimation will be inaccurate, but the jammer can also vary his/her signal directions to nullify the channel tracking. However in this case, the jammer should move at a speed of at least $\frac{10cm}{8ms} = 12.5m/s$, or equivalently $45km/h$, making it extremely difficult to target at a specific MIMO link. Apparently, reducing the pilot interval is a remedy to defeat a high-speed jammer. We will design experiments to evaluate the IC performance under mobile jammers in our future work.

C. Jamming Attack and Defense Performance

In this section, we evaluate the performance of the jamming attack and defense mechanisms in terms of packet delivery rate. We place the receiver at location A in Fig. 10. In each run, we place the sender and jammer at the selected locations in Fig. 10. We run the experiments in seven different cases, i.e., case 1: (1,2); case 2: (3,7); case 3: (4,5); case 4: (6,8); case 5: (8,9); case 6: (5,9); case 7: (4,8), where (x, y) denotes the locations of the sender and jammer respectively. We repeat each case for more than 10 times, with each run transmitting 5000 packets.

First, we present the jamming attack performance by jamming the 1×2 MIMO link in Fig. 11, from which we can see that the PDR drops to $zero$ in almost all seven cases in the presence of the reactive jammer. This result shows the reactive jammer succeeds in throttling OFDM-MIMO communications completely.

Then, we run another set of experiments to jam a 2×2 MIMO link. Fig. 12 plots the sender's PDR performance under different bandwidth settings. This figure also shows the reactive jammer is very effective in degrading packet delivery performance of the MIMO links, as none of the packets is successfully delivered to the receiver using the traditional MIMO decoding scheme. In contrast, using our defense mechanism without signal enhancing rotation, the jamming signals can be eliminated to some extent by estimating jammer channel ratio. Therefore, the PDR under $500KHz$ bandwidth can stay higher than 30%, while exact PDR value depends on the channel estimation accuracy and the relative angles between the received signals from the jammer and sender. We notice that the achieved performance shows great variations across difference cases.

Finally, the PDR performance can be further improved using signal enhancing rotation. Both Fig. 12(a) and Fig. 12(b) reveal that the packet delivery performance using enhanced defense mechanism after applying signal enhancing rotation has been significantly improved and becomes more stable. In particular, the jamming resilient communications achieve more than 60% PDR under $500KHz$ bandwidth and more than 40% PDR under $1M$ bandwidth. Thus, we conclude that signal enhancing rotation can help sustain more robust OFDM communications. From Fig. 12(a) to Fig. 12(b), we note a trend that the packet delivery performance becomes worse as the transmission bandwidth expands. That is because higher data rate transmission is more sensitive to burst of interference and noise in the environment [24].

D. Overhead Analysis

We analyze the overhead for both the pilots and feedback information. As mentioned in Section VI-B, one pilot symbol is inserted every 15 OFDM data symbols. Therefore, the pilot takes nearly 6% of the whole packet. On the other hand, the feedback message includes 48 rotation vectors with one for each subcarrier in our setting. In order to reduce the feedback size, instead of returning all the 48 vectors, it is sufficient to respond 12 vectors, since the channels for consecutive subcarriers are rather similar. In addition, as the direction of vector $[v_1, v_2]$ is equivalent to $[1, \frac{v_2}{v_1}]$, we can reduce the number of elements in a vector into one complex number. The overall feedback overhead adds up to 24 bytes, or 4 OFDM symbols. Therefore, the feedback information is also very short with only a few OFDM symbols.

VII. Related Work

Jamming Attack and Defense Mechanisms. Powerful reactive jamming has aroused many researchers' interests. For instance, [5] demonstrates the feasibility of reactive jamming using software-defined radios. [3] proposes detection mechanism to unveil reactive jammer in sensor networks. [25] investigates the impacts of reactive smart jamming attacks to IEEE 802.11 rate adaptation algorithms. Recent studies consider more powerful wideband and high power jamming attacks [12], [15]. However, both of them only support low data rate communications. Besides that, both of these two defense mechanisms only work for conventional wireless communications that are not OFDM-based. In [26], Vo-Huu et al. proposes a mechanical beamforming scheme and a digital interference cancellation algorithm to cancel jamming signals. However, they can only deal with static adversaries and require additional hardware costs, while our mechanism is purely digital which is capable of dealing with mobile attackers as long as the channel estimation is accurate. Further, they only focus on non-OFDM systems.

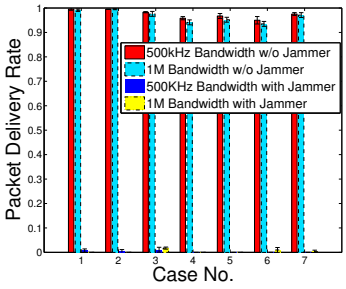
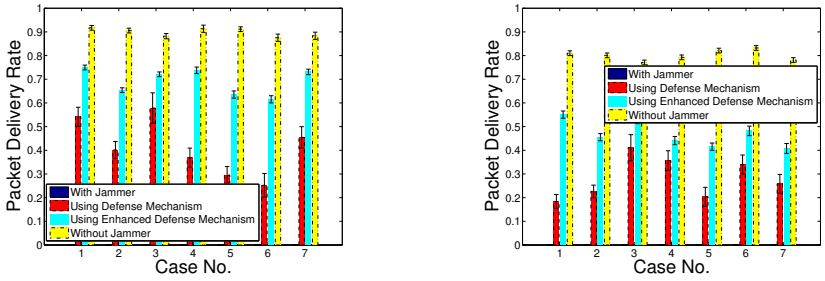


Fig. 11: Packet delivery rate with and without jammer in 1×2 link



(a) 500KHz Bandwidth (b) 1M Bandwidth

Fig. 12: Jamming attack and defense performance

Interference Cancellation Mechanisms. Research efforts in the interference management area have developed novel interference cancellation techniques to improve the network throughput [9], medium access protocol [11] and robustness [10] of MIMO networks. The most relevant work is [10], which enables MIMO communications under high-power cross-technology interferers. Yet, our work exposes several significant differences: 1) we consider smart jammers, who can adapt their attack strategy to be more destructive, while interferers are unintentional; 2) their channel estimation methods require to average over multiple OFDM symbols, which is not applicable for tracking jammer's channel due to jammer's fast adaptation, while our mechanism inserts pilots into known locations to jointly track the sender and jammer's channels instantaneously.

VIII. Conclusion

OFDM is one of the most widely adopted wireless communication schemes. Despite of its popularity in the wireless field, it is vulnerable to advanced jamming attacks, especially the powerful reactive jamming attack enabled by software defined radio technology. While no effective anti-jamming solutions exist to secure OFDM communications, for the first time, we exploited MIMO technologies to defend against such jamming attacks. We showed that such attacks can severely disrupt OFDM-MIMO communications through controlling the jamming signal vectors in the antenna-spatial domain. Accordingly, we proposed defense mechanisms based on interference cancellation and transmit precoding techniques to maintain OFDM communications under reactive jamming.

References

[1] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '05, 2005, pp. 46–57.

[3] M. Strasser, B. Danev, and S. Capkun, "Detection of reactive jamming in sensor networks," *ACM Transactions on Sensor Networks(TOSN)*, vol. 7, no. 16, pp. 1–29, 2010.

[4] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[5] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactive jamming in wireless networks - how realistic is the threat?" in *Proc. of WiSec*, June 2011.

[6] A. Cassola, W. Robertson, E. Kirda, and G. Noubir, "A practical, targeted, and stealthy attack against wpa enterprise authentication," in *Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS '13)*, February 2013.

[7] M. Han, T. Yu, J. Kim, K. Kwak, S. Lee, S. Han, and D. Hong, "OFDM channel estimation with jammed pilot detector under narrowband jamming," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1934–1939, 2008.

[8] T. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *Proc. of ICC*, 2011.

[9] S. Gollakota, S. D. Perli, and D. Katabi, "Interference alignment and cancellation," in *Proc. of SIGCOMM*, August 2009.

[10] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the RF smog: Making 802.11 robust to cross-technology interference," in *Proc. of SIGCOMM*, August 2011.

[11] K. C.-J. Lin, S. Gollakota, and D. Katabi, "Random access heterogeneous MIMO networks," in *Proc. of SIGCOMM*, August 2011.

[12] Y. Liu and P. Ning, "Bittrickle: Defending against broadband and high-power reactive jamming attacks," in *Proc. of IEEE INFOCOM*, 2012.

[13] H. Kim and K. G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?" in *Proc. of MobiCom*, September 2008, pp. 14–25.

[14] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in *Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum*, ser. TAPAS '06, 2006.

[15] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proc. of WiSec*, 2008.

[16] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[17] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. of IEEE S&P*, May 2010.

[18] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. of WiSe*, 2004.

[19] S. Gollakota and D. Katabi, "ZigZag decoding: Combating hidden terminals in wireless networks," in *Proc. of SIGCOMM*, August 2008, pp. 159–170.

[20] K. Miller, A. Sanne, K. Srinivasan, and S. Vishwanath, "Enabling real-time interference alignment: promises and challenges," in *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*, 2012, pp. 55–64.

[21] W.-L. Shen, Y.-C. Tung, K.-C. Lee, K. C.-J. Lin, S. Gollakota, D. Katabi, and M.-S. Chen, "Rate adaptation for 802.11 multiuser MIMO networks," in *Proc. of MobiCom*, August 2012.

[22] "Ettus research llc," *http://www.ettus.com/*.

[23] D. Giustiniano, V. Lenders, J. B. Schmitt, M. Spuhler, and M. Wilhelm, "Detection of reactive jamming in dsss-based wireless networks," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '13, 2013, pp. 43–48.

[24] W. Stallings, *Data and Computer Communications (9th Edition)*. Prentice Hall, 2010.

[25] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of ieee802.11 rate adaptation algorithms against smart jamming," in *Proc. of WiSec*, June 2011.

[26] T. D. Vo-Huu, E.-O. Blass, and G. Noubir, "Counter-jamming using mixed mechanical and software interference cancellation," in *Proc. of WiSec*, April 2013.