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, VA, USA
† Utah State University, Logan, Utah, 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. By intentionally transmitting 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. This jamming strategy is considered most effective, stealthy, and difficult to deal with. The recent advance in the highly programmable software defined radio has made such sophisticated but powerful jamming attacks very realistic – [1] 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. [2] proposed a jammed pilot detection and excision algorithm for OFDM systems to counteract narrow-band jammer that jams the pilot tones. Clancy et al. [3] 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 focus on pilot tone jamming attack, which requires to know the pilot location and also demands 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) technology 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 technique [4]–[6] has greatly enhanced MIMO communication capability. This inspires us to ponder the question: whether it is possible to exploit MIMO technology to devise anti-jamming techniques for OFDM systems, in particular against reactive jamming attack. In this paper, we try to answer this question by first examining the jammer's capability in disrupting OFDM-MIMO communication, and then devising MIMO-based defense mechanisms by utilizing MIMO technology coupled with interference cancellation and transmit precoding techniques. We show that our design is able to restore admissible OFDM communication in the presence of reactive jammers at the expense of consuming available degrees-of-freedom (DoF) of MIMO links.

Although the problems of interference cancellation and jamming resistance are related as both the interferer and the jammer will lead to undecodable signals at the receiver side, they have some significant differences: a) jamming signals are sent by malicious jammers deliberately, who can intentionally alter the jamming signals for their own benefits, while the interferers produce interference inadvertently; b) jammers can modify their signals much faster and more freely than interferers. Hence, jamming signals are much harder to track and remove than conventional interference.

Consequently, designing effective defense mechanisms faces several key challenges. *First*, different jammers transmit different types of jamming signals, and the receiver must cancel

these jamming signals regardless of their signal structures. *Second*, since jammers are able to adapt their jamming signals in real-time, the defense mechanisms should be able to track their adaptations to guide the receiver's cancellation strategy. *Finally*, the defense mechanisms must be robust against the jammers who attempt to disrupt receiver's cancellation scheme.

To meet these challenges, we propose a defense mechanism for resilient OFDM communication based on MIMO interference cancellation technique, which tracks jamming signal's direction in real-time before canceling it out. We devise an *iterative channel tracking* mechanism 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 enhance rotation* technique, which strategically rotates sender's signal to enhance the projected signal strength, resulting in an improved anti-jamming performance. Two main challenges in designing these mechanisms are: how to track the channels promptly, and how to feedback the rotation vectors reliably. In response, we deploy multiple pilots to facilitate channel tracking, while carrying out tactical interference cancellation to feedback messages.

The goal of this paper is to sustain operational OFDM systems in the face of reactive jamming attack. The contributions of this paper are two-fold: First, we exploit the MIMO interference cancellation and transmit precoding techniques to counter reactive jamming attacks for securing OFDM wireless communications. We propose two novel mechanisms: *iterative channel tracking* and *signal enhance rotation* to effectively sustain acceptable throughput under reactive jamming attack. Furthermore, our defense mechanisms can also defeat pilot tone jamming attack as long as the preamble remains undistorted. Second, we implement the jamming attack and defense mechanisms using USRP radios, and conduct extensive experiments to evaluate their performance. The experimental results show that in the presence of a reactive jammer, the packet delivery rate improves significantly using our enhanced defense mechanism.

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 communication 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 [7].

Fig. 1: Reactive jammer starts jamming after certain reaction time.(P: Preamble)

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. She has the capability of covering the whole frame structure, whereas her energy consumption is extremely high, rendering herself easily discoverable; 2) random jammer is more energy-efficient, as she emits jamming signals at random time for a random duration. However, her jamming capability is limited, because of the small collision probability induced by her random behavior; 3) reactive jammer is more effective, energy-efficient and stealthier [8], which is the main focus of this paper.

The key feature of reactive jammer is sensing-before-jamming. There exists a reaction period before jamming takes place, which includes channel sensing and jamming initialization time. We assume the preamble of transmitted frame remains undistorted by the jamming signal, as shown in Fig. 1, since the reactive jammer needs to detect the presence of the preamble before emitting the jamming signals.

In addition, the jammer can transmit arbitrary signals without any signal structures, and she is also free to adapt the signal amplitude or phase in real time. However, we assume the jammer cannot perform full duplex communications, which disables her ability of sensing and jamming simultaneously.

C. OFDM-MIMO Preliminary

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 our system, two cellular phones acting as the sender and receiver try to establish OFDM communication in the presence of a reactive jammer with the signals of interest as OFDM signals.

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 [9]. DoF indicates the number of transmitted streams that can be reliably distinguished at the receiver.

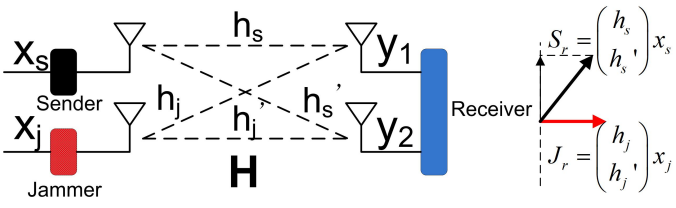


Fig. 2: 1×2 OFDM-MIMO link attacked by a Jammer

Consider the MIMO link with DoF of two in Fig. 2, the signals $\binom{x_s}{x_j}$ are transmitted concurrently through the channel $\mathbf{H}$, and the received signals can be written as:

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

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

In order to decode x_s, interference cancellation 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:

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

After that, the projected signal can be decoded using any standard decoder. This interference cancellation technique is also called *Zero-Forcing* (ZF) technique. Note that, estimating jammer's signal direction[1] is the core of ZF decoder. From Fig. 2, we notice the projected signal is a scaled version of the original signal, indicating a loss of signal amplitude.

Note that Eq. (1) assumes a narrowband channel, where h (such as h_s, h_j, etc) appears as a complex number. For wideband channels, 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. However, in a OFDM-MIMO system, Eq. (1) satisfies for each OFDM subcarrier, such that ZF decoding is carried out over each subcarrier.

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

We exploit MIMO technology to defend against reactive jamming attack in OFDM systems. In this section, we characterize the impact of reactive jammer to the OFDM-MIMO communications. For clarity, we will explain the jamming strategy in the context of a two-antenna receiver decoding a single transmission in Fig. 2. The sender and receiver form a 1×2 MIMO link with DoF of two, one of which will be consumed by the jammer. We conjecture that the receiver can process a concurrent data stream x_s from the sender.

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

$$y_{1i} = h_{ji} x_{ji} + h_{si} x_{si}, \tag{3}$$

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

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 from jammer and sender. Note that the jamming signals need not be OFDM modulated, and can be wideband, which would be partitioned into multiple narrowband jamming signals contained in the OFDM subbands of the sender's signals. The recovery of the legitimate signal, implemented by ZF mechanism, will be carried out for each subcarrier. Thus, the ZF mechanism is the key to the data recovery process, which would definitely become the target of the jammer. In order to see this point clearly, we reformulate Eqs. (3), (4) as follows (in the following, we omit the subscript notation i for i-th subcarrier):

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

where $\mathbf{H} = \left[\begin{smallmatrix} h_j & h_s \\ h'_j & h'_s \end{smallmatrix}\right] = [\mathbf{h}_j, \mathbf{h}_s]$ 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. The angle[2] between J_r and S_r is determined by $\mathbf{h}_j$ and $\mathbf{h}_s$, which will be exploited by the jammer to launch effective attack.

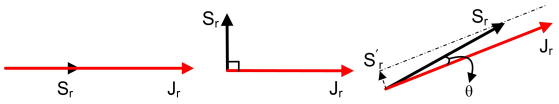
Attacking Zero Forcing Mechanism. In order to understand the attack strategy, we inspect three special cases in Fig. 3 with different received signal spaces. Undoubtedly, the most severe attack is depicted in Fig. 3(a), in which J_r overlaps with S_r in the received signal space, preventing S_r from 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 this case, the projected signal is equivalent to the original signal, yielding the highest projected signal amplitude. Fig. 3(c) shows the case between the above two extreme cases, when the angle of two received signals is a small value. The corresponding projected signal will have a signal amplitude that is too low to make itself recoverable. Therefore, the key idea of attack strategy is to control the jamming signal direction in order to nullify ZF mechanism.

Clearly, the jammer's attack strategy is to shrink the angle between the jamming signal and the intended signal by exploiting the jammer's spatial location. In fact, the difference between $\mathbf{h}_s$ and $\mathbf{h}_j$ deviates according to the distance between S and J [10]. More specifically, if the spacing between two antennas is narrower than a half wavelength, the channels from these two antennas will become highly correlated [9], which makes two received signal directions similar. Consequently, a smart jammer will simply attempt to approach the sender.

In order to demonstrate the effectiveness of such attack strategy, we perform an experiment with varying distances between the jammer and sender's antennas. The *packet delivery rate* (PDR) performance is shown in Fig. 4, from which we can see that when the antenna distance is below $6cm$, no packet can be successfully delivered.

[1]Signal direction is determined by the received signal vector induced on the receive antenna array by the transmitted signal [9], which is defined in the antenna-spatial domain and not the I-Q domain.

[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 $[0, \frac{\pi}{2}]$.



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

Fig. 3: Different two-dimensional received signal spaces

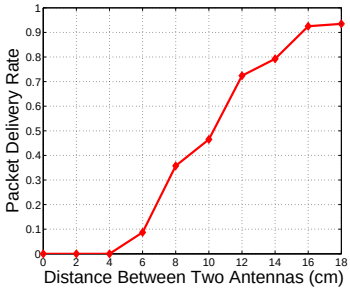


Fig. 4: Jamming performance by exploiting spatial location (in this experiment, the device works on 2.45GHz central frequency with a half wavelength $\frac{\lambda}{2} = \frac{c}{2f} \approx 6.12cm$)

Antenna-Spatial Domain vs. I-Q Domain. The jammer has the option of varying the phase of the jamming signal, resulting in a same situation as having frequency offset. The frequency offset causes the signal vectors to rotate in the I-Q plane. It may seem that the jamming signal will not have a constant phase offset to the signal of interest as shown in Fig. 3. This reasoning however is incorrect, since the received signal space of Fig. 3 is in the antenna-spatial domain and not the I-Q domain. The frequency offset only determines how signal rotates in the I-Q domain, but only scales the direction of the signal vectors in the antenna-spatial domain by a complex number [4]. In other words, the jamming signal direction in the received signal space is unaffected by rotation in the I-Q domain, but instead is determined by the channels between the jammer and the receiver.

IV. Defense Mechanisms Against Reactive Jamming Attack

In this section, we propose effective MIMO-based defense mechanisms to counteract reactive jamming attack. We first present a defense mechanism based on interference cancellation technique. We propose to cancel arbitrary jamming signals by keeping track of the jamming signal direction, for which we develop an *iterative channel tracking* mechanism. Then, an enhanced defense mechanism is built by incorporating *signal enhance rotation* to make the OFDM-MIMO system more robust against smart jammers.

As opposed to the attack strategy that is to force shrinking 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 signals of interest in the presence of arbitrary jamming signals; 2) how to improve the robustness of OFDM communication against reactive jammer.

A. Defense Mechanism Overview

We offer an overview of proposed defense mechanisms in this section. A high-level flow chart is illustrated in Fig. 5, which shows both the defense mechanism and its enhanced version. The defense mechanism is carried out wholly at the receiver side, which 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. A random angle represents for a high decoding rate as shown below.

In the physical SJR model, the transmission from a sender S is successfully received by receiver R under a simultaneous interfering transmission from a jammer J if:

$$\frac{P_{SR}}{P_{JR}} \geq \gamma_R, \tag{6}$$

We assume the angle between legitimate signal and jamming signal is θ, so that $SJR = \frac{P_s\|\mathbf{h}_s\|^2 sin(\theta)}{P_{JR_{proj}}}$, where P_s is the sender's transmission power. Substituting this expression into Eq. (6), we derive threshold θ_{th} defined as the minimal angle required for successful reception:

$$\theta_{th} = arcsin\frac{P_{JR_{proj}}\gamma_R}{P_s\|\mathbf{h}_s\|^2}.$$

As long as the jammer fails to approach the sender, the angle will become a random number in $[0, \frac{\pi}{2}]$ due to channels' spatial and temporal variability. Hence, a *successful attack rate* of the jammer is given by $\frac{\theta_{th}}{\pi/2}$. Typically, $P_s\|\mathbf{h}_s\|^2 \gg P_{JR_{proj}}$, which renders a small θ_{th}, and thus a low successful attack rate or a high decoding rate.

In our defense mechanism, we take advantage of spatial retreat [11] technique to get away from the jammer. Alternatively, the sender can also move randomly inside the receiver's reception range to avoid being approached by the jammer.

After clearing way for the decoding process, signal decoding is then implemented using ZF technique, based upon the channel tracking results. Meanwhile, jamming detection module intends to detect jamming attack promptly for triggering other modules' operations.

Enhanced defense mechanism (Section IV-D) involves more modules at both the sender and receiver sides, whose centerpiece is signal enhance rotation module, for rotating the transmitted signal to improve the decoding rate. It also incorporates a feedback mechanism for instructing the sender's rotation process.

B. Decoding the Signal of Interest

According to Eqs. (2), (5), ZF mechanism can be directly applied for decoding x_s at each OFDM subcarrier, once the channel estimation of $\mathbf{H} = [\mathbf{h}_j, \mathbf{h}_s]$ is obtained. Initial estimation of $\mathbf{h}_s$ can be derived via analyzing the undisturbed preamble. However, since initial estimation can only be used

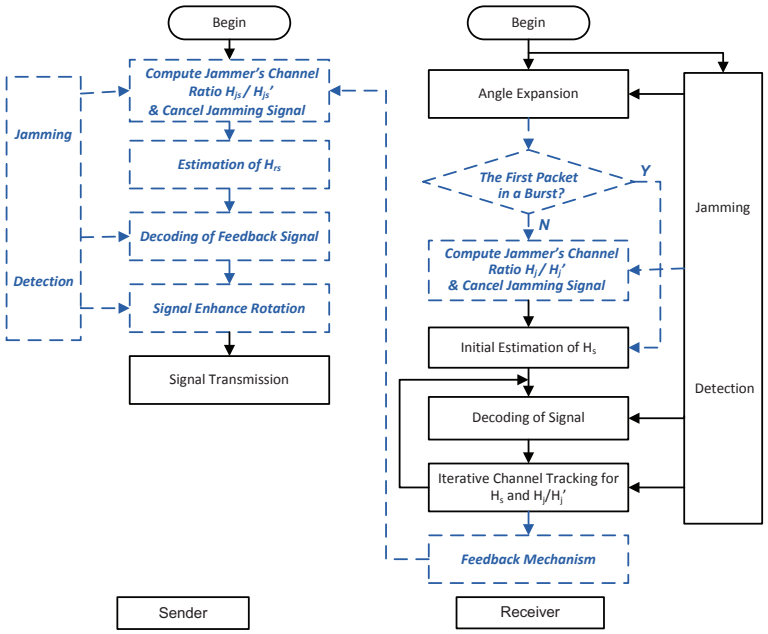


Fig. 5: A flow chart of proposed defense mechanisms (solid box: modules of basic defense mechanism, dashed box: modules of enhanced defense mechanism)

within the channel coherence time, tracking the channel estimation becomes a necessity.

Moreover, because of the adaptive jammer's rapid reaction, one requirement of our scheme is to response fast to the jammer's adaptation. Inspired by ZigZag decoding technique [12], 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's channel estimation method, and then present the iterative mechanism for updating both channels iteratively.

Jammer's Channel Estimation. $\mathbf{h}_j$ seems unreachable due to the randomness of the jamming signal structure (no known symbols). However, since jamming signal x_j is not an interest for the receiver, we claim that the knowledge of $\mathbf{h}_j$ is not necessary for decoding x_s. In fact, as stated in Section II-C, the only information required about jamming signal for ZF decoder is its signal direction, determined by channel vector $\mathbf{h}_j = [h_j, h_j']^T$. We observe the nice scale invariance property of signal direction, i.e., the direction of $[h_j, h_j']^T$ is equivalent to that of $[\frac{h_j}{h_j'}, 1]^T$. Therefore, we only need to acquire jammer's channel ratio $\frac{h_j}{h_j'}$.

The received signal is a mixed signal consisting of the sender and jammer's signals. If we can extract jammer's signals $J_r = (\frac{h_j}{h_j'})x_j$, we can derive the jammer's channel ratio by computing the ratio of received jamming signals on two receive antennas, since $\frac{h_j}{h_j'} = \frac{x_j \cdot h_j}{x_j \cdot h_j'}$.

However, reactive jammer guarantees the jamming attack happens immediately after the legitimate transmission, such that the jamming signal always intertwines with the legitimate signal, making it hard to separate them. Our solution is based on an intuition that if we purposefully let the jamming signal intertwine with pre-known signals, we are able to extract the jamming signal. In order to achieve this, we insert multiple pre-known symbols or pilots into the original data packets, and extend the frame structure as shown in Fig. 6. The pilots are inserted in the specified locations periodically in the packet. However, if the jammer learns the locations of the pilots, she can intentionally stop jamming during these pilot periods to avoid being tracked. Therefore, we assume both the sender and receiver agree upon a series of secret locations of pilots. Note that, the extension of the frame structure causes limited overheads, which will be evaluated in Section VI-D.

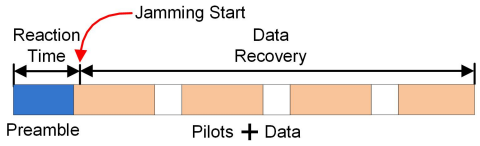


Fig. 6: Extended frame structure

The basic idea for extracting jamming signal is to subtract the received pilot from the received mixed signal. The subtracting step is widely studied and has been shown to work in practical implementations [12], [13]. It proceeds as follows: 1) after detecting the start of jamming (see Section IV-C), the receiver finds the locations of pilots; 2) received pilots are reconstructed using the known pilot symbol distorted by the estimated channel; 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 jamming signal direction (jammer's channel ratio).

Iterative Channel Tracking Mechanism. Now, we delve

into the details of channel tracking mechanism. In order to update the channel estimation in a timely manner for tracking jammer's adaptation, we will make use of multiple pilots from the extended frame structure in Fig. 6.

Our mechanism is bootstrapped by initial channel estimation from the preamble. During the first pilot, we learn jammer's channel ratio by reconstructing the received pilot using the initial channel estimation and subtracting it from the received mixed signal, as mentioned above. During the following pilots, if we continuously utilize initial channel estimation to update jammer's channel ratio and recover the data, eventually, this process will fail because of the expiration of initial channel estimation. Therefore, we propose to update the sender's channel estimation and jammer's channel ratio alternately and iteratively using multiple pilots.

The key observation is that the received signal is a mixed signal with two signal components. Without fixing one of them, we are not able to extract the other one. Therefore, we preserve the freshly estimated jammer's channel ratio for updating sender's channel, while retaining the sender's recent channel estimation for tracking jammer's channel ratio. We propose to update sender's channel estimation during even number of pilots, and update jammer's channel ratio during odd number of pilots. For example, during the second pilot, we keep the estimated jammer's channel ratio $\frac{h_j}{h'_j}$ fixed, and rewrite Eq. (5) as follows:

$$\binom{y_1}{y_2} = \binom{h_j}{h'_j} x_j + \binom{h_s}{h'_s} x_s^{\diamond}, \tag{7}$$

where $x_s^{\diamond}$ represents the known pilot signal. Then, we project the received signal onto the subspace $[1, -\frac{h_j}{h'_j}]$. The projected signal is represented as:

$$y_{proj} = y_1 - \frac{h_j}{h'_j} y_2 = (h_s - \frac{h_j}{h'_j} h'_s) x_s^{\diamond}, \tag{8}$$

from which we can update $(h_s - \frac{h_j}{h'_j} h'_s)$, consisting of two unknowns h_s and h'_s. Then we use the previously estimated h_s to update h'_s. Similarly, during the fourth pilot, we use this fresh h'_s to update h_s, which implies that the sender's channel will be updated every other pilot.

Similarly, we can update jammer's channel ratio using the sender's recent channel estimate, since $\frac{h_j}{h'_j} = \frac{y_1 - x_s^{\diamond} \cdot h_s}{y_2 - x_s^{\diamond} \cdot h'_s}$ (derived from Eq. (7)). During the odd number of pilots, jammer's channel ratio will be kept updated using jammer's channel estimation method to ensure correct decoding of the signal of interest.

In fact, we can express the signal of interest by replacing the known pilot signal in Eq. (8) as:

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

which shows that as long as $(h_s - \frac{h_j}{h'_j} h'_s)$ and $\frac{h_j}{h'_j}$ are precisely updated, the signal of interest can be correctly recovered. Note that this mechanism becomes reasonable only if we keep two consecutive pilots staying within the channel coherence time, which means the jammer's channel gets updated in a very short period, facilitating the defense mechanism to track the jammer's agile adaptation.

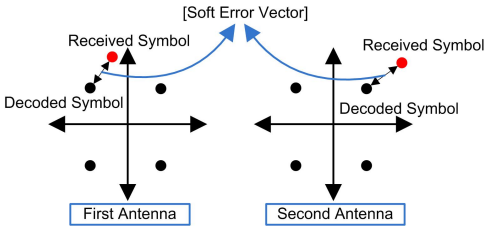


Fig. 7: Soft error vector in QPSK constellation

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 signal will impose additional noise to Eq. (5). In response to ISI, we average our channel tracking results derived from multiple pilots to mitigate the negative effects of ISI. Although channel estimation becomes more accurate, ISI still reduces the SNR of the intended signal. 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 [5] to deal with ISI issue, i.e., we convolute the received time-domain signal with a filter obtained 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 above, the receiver needs to detect the start and termination of jamming. The jamming detection problem has been studied in [7], in which the constellation diagrams are employed to identify jammed bits. We follow the same principle. *Soft error vector* is used as 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. 7. 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 called *jumped value*. Jamming attack is supposed to start when $\|\mathbf{V}_k\|/\|\mathbf{V}_{k-1}\| > \gamma_v$, where γ_v is pre-defined threshold for jamming detection. Jamming attack stops if jumped value returns to normal. In our design, we consider a jump that is higher than doubling the errors as a potential jammer, so that $\gamma_v = 2$.

D. Enhanced Defense Mechanism

Although the signal of interest can be decoded using the above defense mechanism, the signal after projection will have a reduced signal amplitude, which will affect the throughput performance, as pointed out in [5], [14] and also shown in Fig. 2. This motivates us to build an enhanced defense mechanism to raise the amplitude of projected signal, so as to

achieve a more robust OFDM communication against smart and adaptive jammers. The key idea is to rotate the sender's signal to make it orthogonal to the jamming signal. This mechanism works for a multi-antenna sender, but we focus on 2×2 link for ease of explanation. For a 2×2 MIMO link, the received two-dimensional signal can be represented as:

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

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. Since the jammer consumes one DoF, the two-antenna sender is allowed to transmit one OFDM data stream as seen from Eq. (10).

We exploit the nice property of MIMO communication to control the received signal vector along which the signal is received [4]. In Eq. (10), 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*. 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.

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 $\mathbf{H} = \{\mathbf{h}_j, \mathbf{H}_s \vec{\mathbf{r}}\}$. Since $\mathbf{H}$ should remain as a full rank matrix in order to let x_s decodable, one constraint on $\vec{\mathbf{r}}$ is that it cannot reduce the rank of channel matrix.

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

Specifically, $\vec{\mathbf{r}}$ can be set to rotate the received legitimate signal so as to make it overlapped with the jamming signal, if $\mathbf{H}_s \vec{\mathbf{r}} = \mathbf{h}_j$. On the other hand, $\vec{\mathbf{r}}$ can also turn the received legitimate signal to be orthogonal to the jamming signal, if $\mathbf{H}_s \vec{\mathbf{r}} = \mathbf{h}_j^{\perp}$, i.e., $\vec{\mathbf{r}} = \mathbf{H}_s^{-1} \cdot \mathbf{h}_j^{\perp}$, where $\mathbf{h}_j^{\perp}$ stands for the orthogonal vector of $\mathbf{h}_j$. This indeed is the key idea of our signal enhance rotation technique.

Signal Enhance Rotation Mechanism. In a 2×2 MIMO link, signal rotation can be achieved by simply multiplying $\vec{\mathbf{r}} = \mathbf{H}_s^{-1} \cdot \mathbf{h}_j^{\perp} = \mathbf{H}_s^{-1} \cdot [1, -\frac{h_j}{h_j'}]^T$ to the transmit signal. Note that both $\mathbf{H}_s$ and $\mathbf{h}_j^{\perp}$ can be derived using the channel tracking mechanism in Section IV-B. After signal rotation, the received legitimate signal will be induced orthogonal to the jamming signal, yielding the largest projected signal amplitude. As a result, we name this mechanism as a *signal enhance rotation* mechanism.

However, signal enhance rotation happens at the sender side, while channel estimation is performed at the receiver side. Therefore, we need to feedback the rotation vectors from the receiver, which is achieved by piggybacking ACK information with the rotation vectors for each packet. To facilitate signal enhance rotation, we define a "$burst$" as a consecutive sequence of packets, shown in Fig. 8. During each burst, the sender will continuously carry out signal enhance rotation using the feedback information, if the jammer is found active. To reliably feedback rotation vectors in the presence of reactive jammer, we develop a feedback mechanism as follows.

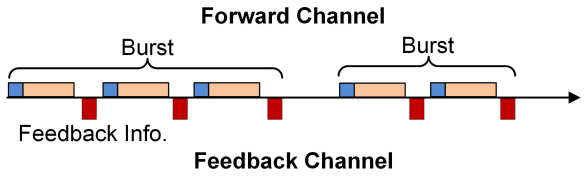


Fig. 8: Burst of packets

Feedback Mechanism. Now we present a feedback mechanism resembling the forward transmission. The feedback frame is formulated using the frame structure in Fig. 1. Since feedback information is rather short, we preclude the need of tracking the channel using extended frame structure. The same interference cancellation technique can be employed to decode the feedback information at the sender, although the role of the sender and receiver is reversed.

However, besides the reversed role of S and R, another key difference exists between the feedback and forward transmissions. Remember in the forward transmission, preambles are used for bootstrapping process, which are not supposed to be destroyed. But during the feedback transmission, if the jammer is continuously jamming during a burst, both the forwarding packets (except the first one) in the burst and the feedback packets will be completely covered, leading to a breakdown of the bootstrapping process. To address this issue, we try to identify the jammer's isolated transmission.

Let us first focus on the feedback packets covered by the jamming signal. In this case, 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 her two antennas $y_{s1} = h_{js} x_{js}$ and $y_{s2} = h'_{js} x_{js}$. Then, the sender uses the jammer's channel ratio to cancel out the jamming signal, and find the preamble to estimate the feedback channel, which can be used for signal decoding.

Similarly, the receiver can also use the same mechanism illustrated above to recover the forwarding packets including: computing jammer's channel ratio, finding the preamble, estimating forward channel h_s and decoding the signal. Therefore, as long as the preamble of the first packet in a burst is not jammed, the defense mechanism should succeed.

Two points are worth noting. First, the reactive jammer may stop jamming anytime during a burst. Therefore, during the feedback period, the sender will carry out two methods simultaneously to decode the feedback information. The first method performs interference cancellation by assuming jamming is *on*, while the second method processes normal

decoding by assuming jamming is *off*. Based on the decoding results, the sender will learn the jammer's status (*on/off*), and decide whether she will perform signal enhance rotation for the next packet.

Second, the feedback information should be received in a timely fashion, i.e., once the channel estimation expires, the rotation vector will no longer be effective. In our design, the sender will count the feedback time to determine whether to apply signal enhance rotation.

E. Other Types of Jammers

In this section, we briefly discuss about the impacts of constant jammer and random jammer to our defense mechanisms. Constant jammer can cover all the packets including their preambles, which will certainly disable our defense mechanisms. However, constant jamming is impractical due to its enormous energy consumption. Random jammer randomly alternates between jamming and sleeping. We investigate the jammer's probability of covering preambles, and present the modifications to the defense mechanisms. First, let us assume both the jamming and sleeping periods are uniformly distributed within $[0, 20]$ms with an average of $10ms$, thus the random jammer starts jamming with a probability of $1/2$. We further assume the preamble length is $0.1ms$, and one burst lasts for $100ms$ with $400ms$ inter-burst idle interval. Then, the probability of covering the preamble of the first packet in the burst can be easily written by: $\frac{10/0.1}{(500-10)/0.1} \cdot \frac{1}{2} \approx 0.01$. One can further reduce the probability by introducing a longer burst or burst interval, which makes the preamble distortion a small probability event. As long as the first preamble avoids of getting jammed, our defense mechanism becomes functional. Second, the jamming detector can identify the start and end of jamming attacks promptly. Then, we modify our defense mechanism to perform normal processing when the jammer is sleeping and conduct interference cancellation within her jamming duration.

F. Discussion

Our defense mechanisms can enable a reliable OFDM communication in the presence of powerful single-antenna reactive jammer. Extending to a network with multiple jammers, the defense mechanism should succeed in canceling jamming signals as long as different jammers operate on different spectrum bands or transmit at different time slots, since the cancellation is carried out for each OFDM subband at one time. In addition, our defense mechanism defeats the multi-antenna jammers transmitting the same jamming signals over all the antennas, because they can be regarded as single-antenna jammers with aggregated channel state information. However, multi-antenna jammers sending multiple jamming streams are more destructive to the OFDM-MIMO networks, since they can deplete the DoF of MIMO links. Our anti-jamming solutions are not effective in cancelling out multiple jamming streams without any frame structure. However, there is no available solution in the literature to provide jamming-resistant communication under multi-antenna jammers with multiple jamming streams. We would like to leave it for our future research.

V. Implementation

We build a prototype using five USRP-N200 radio platforms [15] and GNURadio software package. Each USRP board is equipped with one XCVR2450 daughterboard operating on 802.11 spectrum. 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 communication in our experiments. We configure each USRP to span $1MHz$ bandwidth by setting both the interpolation rate and decimation rate to 100. ZF technique is implemented at the receiver to recover the signals of interest. We also implement the decoding mechanism incorporating signal enhance rotation at both the sender and receiver sides.

The jammer is implemented using another USRP device. To defend against jamming attack, the receiver first estimates sender's channel and jamming signal direction, then uses ZF mechanism to eliminate the signals from the jammer. Meanwhile, the receiver will compute the rotation vector and transmit it back to sender for signal enhance rotation. The sender checks whether it still stays in the channel coherence time since its last transmission, if it does, the sender will apply the rotation vector to its newly generated symbols and send the rotated elements through two antennas. We set the transmission power of both the sender and jammer as $100mW$.

In our implementation, we emulate the reactive jamming and the jammer's 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 ZF 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.

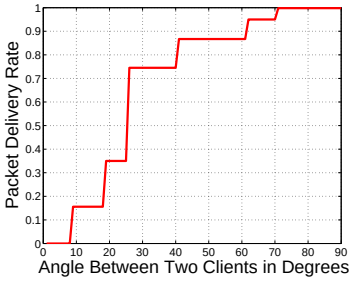


Fig. 9: Packet delivery rate performance with different angles between two clients

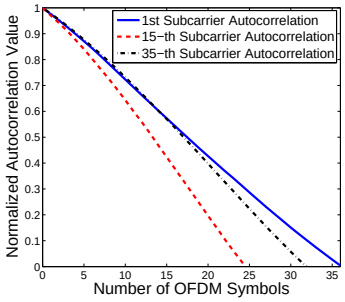


Fig. 10: Autocorrelation of channel phase in an indoor environment (with 500KHz Bandwidth)

A. Impact of Received Signal Direction

We argued in Section III that the angle between two received signal directions will affect the ZF decoding performance. 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 conducts ZF mechanism to decode the streams. We have mentioned that the signal direction is determined by the channels between the transmitter and the receiver. Although the channel evolves over time, we observe that the angle remains relatively stable for the time being, once the locations of clients and receiver are fixed. Then, we change the locations of clients and receiver to measure the packet delivery performance when two received signals have different angles. We keep the distance from clients to receiver fixed, so that the performance variation among different cases is mainly induced by different angles, rather than different path losses.

We show the performance measurement in Fig. 9, from which we can see the angle between two received signals indeed affects the packet delivery performance significantly. The major observation is that PDR deteriorates to be 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 the indoor environment.

We let a sender transmit consecutive known OFDM symbols following a preamble to track the channel variation. 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. We investigate multiple subcarriers over several rounds. Fig. 10 shows the autocorrelation of channel phase over multiple subcarriers. The channel phase correlates over multiple OFDM symbols before it becomes uncorrelated (i.e. the normalized autocorrelation value is below zero). 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 is nearly 33 OFDM symbols or $8.5ms$, i.e., we need to update channel estimation at least every 30 OFDM symbols, nearly 200 bytes under $500KHz$ bandwidth, or nearly 400 bytes under $1MHz$ bandwidth. Consider $500KHz$ bandwidth case, as we update the channel estimation every other pilot in Section IV-B, we need to insert pilots at least once every 100 bytes of data. This result also tells us the rotation vector takes effect during the 33 OFDM symbols. After channel coherence time, 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 her channel condition. 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 her signal directions in real-time to nullify the channel tracking. However in this case, the jammer should move at a speed of at least $\frac{0.1}{0.008} = 12.5m/s$, 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.

C. Jamming Attack and Defense Performance

In this section, we evaluate the performance of jamming attack and our defense mechanisms. In the experiment, we place the sender, jammer and receiver at different locations, and repeat the experiments for 10 times under seven different cases respectively (approximately 4-8 meters between sender and receiver, 3-8 meters between jammer and receiver), with the average PDR as the performance criterion. We first present the jamming performance to 1×2 link in Fig. 11, from which we can see the PDR drops to $zero$ in almost all seven cases. This result shows us the reactive jammer can throttle communication completely.

Then, we perform experiments in 2×2 OFDM-MIMO networks, with one jamming antenna. Fig. 12 plots the PDR

performance of one transmit antenna under different bandwidth settings. This figure shows the jammer is very effective in degrading packet delivery performance in OFDM-MIMO networks, as none of the packets gets through using the traditional MIMO decoding method. In contrast, using our defense mechanism without signal enhance rotation, the signals from jammer can be canceled out by estimating her signal directions. Therefore, the PDR under $500KHz$ bandwidth can stay higher than 30%, whose exact value depends on the estimation accuracy and the angles between signals from jammer and sender. We notice that the performance varies a lot across difference cases using the defense mechanism. We further improve the performance using signal enhance rotation. From both figures, we notice that the packet delivery performance becomes more stable and significantly higher than the case without signal enhance rotation, with more than 60% PDR under $500MHz$ bandwidth and more than 40% PDR under $1M$ bandwidth. Thus, we conclude that signal enhance rotation helps sustain more robust OFDM communication. From Fig. 12(a) to Fig. 12(b), we observe the packet delivery performance becomes worse when the transmission bandwidth expands. That is because higher data rate transmission is more sensitive to interference and noise in the environment.

D. Overhead Analysis

We analyze the overhead for both the pilots and feedback information. As mentioned in Section VI-B, we insert one pilot symbol 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 response with 12 vectors, since the channels for consecutive subcarriers are very similar. Again, the direction of vector $[v_1, v_2]$ is equivalent to $[1, \frac{v_2}{v_1}]$, thus 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, [1] demonstrates the feasibility of reactive jamming using software-defined radios. [8] proposes detection mechanism to unveil reactive jammer in sensor networks. [16] 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 [7], [17]. However, both of them only support low data rate communication. Besides that, both of these two defense mechanisms only work for conventional wireless communications that are not OFDM-based. In [18], Vo-Huu et al. proposes a mechanical beamforming scheme and a digital interference cancellation algorithm to cancel high-power jamming signals. However, they can only deal with static attackers 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.

In the context of jamming-resilient OFDM/MIMO networks, Rob Miller et al. [19] study various jamming attacks to disrupt the MIMO communication by targeting its channel estimation procedure. Specifically, the adversary interferes with the preambles or pilots to let sender and receiver perform false estimation. In similar essence, [2], [3] study pilot tone jamming attack. However, it is extremely difficult for the adversary to synchronize her transmission with the legitimate sender during the short channel sounding period, while this paper focuses on a more practical reactive jamming attack.

Interference Cancellation Mechanisms. Research efforts in the interference management area have developed novel interference cancellation techniques to improve the network throughput [4], medium access protocol [6] and robustness [5] of MIMO networks. The most relevant work is [5], which enables MIMO communication under high-power cross-technology interferers. Yet, our work exposes 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 we insert pilots into known locations to jointly track sender and jammer's channels in a prompt manner.

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 exists 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 communication 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 communication under reactive jamming. To thwart smart attacks that change their signal vectors on-the-fly, we proposed iterative channel tracking and signal enhance rotation mechanisms to track the jammer's channel and adapt the transmitted legitimate signals. Our prototype experimental results demonstrated that, while the OFDM-MIMO communication can be completely throttled by jamming attacks, our defense mechanisms can effectively turn it into an operational scenario with more than 40% of normal throughput.

References

[1] 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.

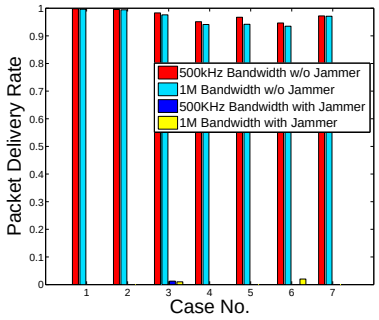
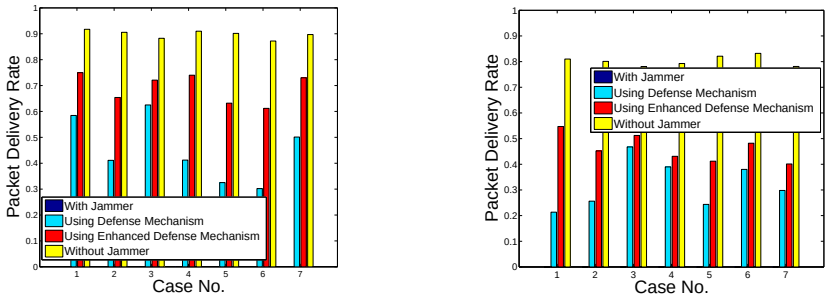


Fig. 11: Packet delivery rate with and without jammer in 1×2 link



(a) 500KHz Bandwidth

(b) 1M Bandwidth

Fig. 12: Jamming attack and defense performance

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

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

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

[5] 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.

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

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

[8] 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.

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

[10] 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.

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

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

[13] D. Halperin, T. Anderson, and D. Wetherall, "Taking the sting out of carrier sense: interference cancellation for wireless lans," in *Proc. of MobiCom*, Sep. 2008.

[14] 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.

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

[16] 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.

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

[18] 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.

[19] R. Miller and W. Trappe, "Subverting MIMO wireless systems by jamming the channel estimation procedure," in *Proc. of WiSec*, March 2010.