Jamming Resilient Communication Using MIMO Interference Cancellation

Qiben Yan, *Member, IEEE*, Huacheng Zeng, Tingting Jiang, *Student Member, IEEE*, Ming Li, *Member, IEEE*, Wenjing Lou, *Fellow, IEEE*, and Y. Thomas Hou, *Fellow, IEEE*

***Abstract*— Jamming attack is a serious threat to the wireless communications. Reactive jamming maximizes the attack efficiency by jamming only when the targets are communicating, which can be readily implemented using software-defined radios. In this paper, we explore the use of the multi-input multi-output (MIMO) technology to achieve jamming resilient orthogonal frequency-division multiplexing (OFDM) communication. In particular, MIMO interference cancellation treats jamming signals as noise and strategically cancels them out, while transmit precoding adjusts the signal directions to optimize the decoding performance. We first investigate the reactive jamming strategies and their impacts on the MIMO-OFDM receivers. We then present a MIMO-based anti-jamming scheme that exploits MIMO interference cancellation and transmit precoding technologies to turn a jammed non-connectivity scenario into an operational network. We implement our jamming resilient communication scheme using software-defined radios. Our testbed evaluation shows the destructive power of reactive jamming attack, and also validates the efficacy and efficiency of our defense mechanisms in the presence of numerous types of reactive jammers with different jamming signal powers.**

***Index Terms*— Reactive jamming, MIMO, software defined radio, interference cancellation, transmit precoding.**

I. Introduction

JAMMING has been a serious threat in wireless networks [2], [3]. Jammers intentionally emit jamming signals to disturb network communications, resulting in throughput degradation, network partition, or even a complete zero connectivity scenario. Reactive jamming is one of the most effective jamming attacks. A reactive jammer continuously listens for the activities on the channel, 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 [4], [5]. The recent advance in the highly programmable software defined radio (SDR) has made such sophisticated but powerful jamming attacks very realistic – [6], [7] demonstrated that a reactive jammer is readily implementable and the jamming results devastating. Furthermore, the reactive jamming can be triggered rapidly on any field of the packet, making it a realistic threat for wireless communications.

Modern broadband wireless communications, such as WLAN, digital TV and cellular communication, all adopt orthogonal frequency-division multiplexing (OFDM) as one of the core technologies. OFDM strengthens the systems' robustness against multipath fading and severe noisy environment, but it is not ideal for the environments where adversaries try to intentionally jam the communications. Such increasingly hostile environments with advanced jamming threats prompt the development of jamming resilient OFDM communication systems. Recent studies investigate and attempt to alleviate the impacts of jamming attacks to the OFDM systems. Han et al. [8] proposed a jammed pilot detection and excision algorithm for OFDM systems to counteract a narrow-band jammer that jams the pilot tones. Clancy [9] 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 focused on the adversaries jamming pilot tones, who require the knowledge of 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 under the reactive jamming attack.

As a major advance, multi-input multi-output (MIMO) has emerged as a key technology for wireless networks, which has been adopted in LTE, 802.11n and 802.11ac. 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 channel capacity. More importantly, recent advance in MIMO interference cancellation (IC) technique [10]–[12] has greatly enhanced MIMO communication capability under multiple concurrent transmissions. MIMO IC has been utilized to enable 802.11 communication under high-power and relatively wideband interference from interferers such as microwave and baby monitor [11]. This inspires us to ponder: whether it is possible to exploit MIMO IC technique to mitigate jamming attacks

Manuscript received June 5, 2015; revised October 15, 2015 and January 7, 2016; accepted February 10, 2016. Date of publication February 29, 2016; date of current version April 12, 2016. This work was supported in part by the National Science Foundation (NSF) within the Division of Electrical, Communications and Cyber Systems under Grant ECCS-1102013, in part by NSF within the Division of Computer and Network Systems under Grant CNS-1064953, Grant CNS-1405747, Grant CNS-1443889, Grant CNS-1446478, and Grant CNS-1564477, and in part by the Office of Naval Research under Grant N00014-15-1-2926. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Lifeng Lai.

Q. Yan is with the Department of Computer Science and Engineering, University of Nebraska-Lincoln, Lincoln, NE 68588 USA (e-mail: yan@unl.edu).

H. Zeng and Y. T. Hou are with the Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: zeng@vt.edu; thou@vt.edu).

T. Jiang and W. Lou are with the Department of Computer Science, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: virjtt03@vt.edu; wjlou@vt.edu).

M. Li is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: lim@email.arizona.edu).

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

Digital Object Identifier 10.1109/TIFS.2016.2535906

targeting OFDM systems, in particular, SDR based reactive jamming attacks. In this paper, we try to answer this question by first examining the jammer's capability in disrupting MIMO-OFDM 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 capable of restoring admissible OFDM communications in the presence of reactive jammers.

Spread spectrum is a well-known physical layer technology for anti-jamming communications. Spread spectrum techniques, such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), deliberately spread the frequency of the original signal onto a much wider bandwidth in the frequency domain so that the resulting signal becomes more resilient to interference and jamming signals while being transmitted. MIMO IC based anti-jamming method is fundamentally different from traditional anti-jamming methods. MIMO IC exploits the spatial freedom provided by multiple antennas to cancel out the jamming signal, instead of relying on frequency domain or code domain modulation like in FHSS and DSSS. Rather than hopping away from the jammed spectrum, MIMO IC recovers the jammed signals within the jammed spectrum. Using MIMO IC, the signal jammed by the jamming signals can be recovered through projecting the received signals onto an orthogonal space of the jamming signals.

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 results or to evade anti-jamming techniques, 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 an 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 disrupt the receiver's cancellation scheme.

To address these challenges, we propose a novel defense mechanism to achieve jamming resilient OFDM communication using 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 *sender signal enhancement* (SSE) 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 mainly three-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 *sender signal enhancement* to effectively sustain acceptable throughput under reactive jamming attack. Iterative channel tracking updates two sets of channel estimations including sender-to-receiver and jammer-to-receiver channels alternately by inserting multiple pilots. Sender signal enhancement smartly adjusts transmitting signals' directions to diminish the jammers' destructive impact.

(2) We implement the jamming attack and defense mechanisms using USRP-N200 radio platforms. Specifically, we implement MIMO IC technique, and SSE with message feedback schemes. We also design an emulated configurable reactive jammer with control of jammer's reaction time.

(3) We conduct jamming attack and defense experiments to evaluate the performance in terms of packet delivery rate and throughput. The experimental results show that in the presence of various types of reactive jammers with different power levels, the packet delivery rate and packet transmission throughput improve significantly using our defense mechanisms with IC and SSE.

The remainder of this paper is organized as follows. We present the related work in section II. Then, we formulate the jamming defense problem in section III. In section IV, we describe the destructive impact of reactive jamming attack towards MIMO-OFDM communications. The defense mechanisms are illustrated in section V, followed by section VI, which describes the defending system implementation. Section VII presents the performance evaluation results by carrying out numerous experiments to defend against SDR-based reactive jammers in a lab environment. Finally, section VIII concludes the paper.

II. Related Work

A. Jamming Attack and Defense Mechanisms

The mainstream jamming defense mechanisms rely on FHSS and DSSS, either requiring the communicating parties to pre-share secret keys [13], [14], or let them communicate without pre-shared keys using Uncoordinated FHSS [15]–[19] or Uncoordinated DSSS [20], [21]. Recently, powerful reactive jamming has aroused many researchers' interests. For instance, [6] demonstrates the feasibility of reactive jamming using software-defined radios. Reference [4] proposes detection mechanism to unveil reactive jammer in sensor networks. Reference [22] investigates the impacts of reactive smart jamming attacks to IEEE 802.11 rate adaptation algorithms. Recent studies consider to defend against more powerful wideband and high power jamming attacks [23], [24]. 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 [25], Vo-Huu et al. propose 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. Another line of research focuses on theoretically analyzing the interactions between a user and a smart jammer, by applying game theory [26], [27] or sequential learning mechanisms [28], the results of which can be used to guide the user's communication strategy.

In the context of jamming resistant OFDM/MIMO communications, Miller and Trappe [29] 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, [8], [9] study pilot tone jamming attack. However, it is extremely difficult for the adversary to synchronize his/her transmission with the legitimate sender during the short channel sounding period, while this paper focuses on a more practical reactive jamming attack. Recently, Shen et al. [30] propose MCR decoding to defend against wireless jamming attacks using MIMO techniques. However, they assume all devices are immobile, and do not consider jammer's fast adaptions to avoid being tracked. On the other hand, we consider mobile jammers, and our defense mechanisms based on iterative channel tracking are able to track jammer's channel even when the jammer intentionally adjusts his/her strategy.

B. Interference Cancellation Mechanisms

Research efforts in the interference management area have developed novel interference cancellation techniques to improve the network throughput [10], medium access protocol [12] and robustness [11] of MIMO networks. Reference [10] proposes a centralized solution to combine interference cancellation and alignment for decoding concurrent transmissions in MIMO networks, doubling the throughput of MIMO LANs. Lin et al. [12] extend the previous work by presenting a distributed random access protocol. Shen et al. [31] further develop a rate adaptation scheme via learning clients' signal directions. However, all the above works consider interferences caused by concurrent transmissions from legitimate senders in the same network. The most relevant work is [11], which enables MIMO communications under high-power cross-technology interferers. Yet, our work has 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.

III. Problem Formulation

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

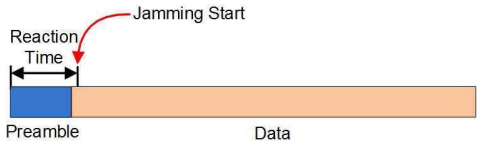


Fig. 1. Reactive jammer starts jamming after a certain reaction period.

A. System Model

We consider an adverse wireless environment with one or multiple jammers targeting at the communication link established by a sender and a receiver. We assume that the jammers are single-antenna devices, with the capability 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 consider reactive jammer in this paper. Reactive jammer is defined as a jammer who emits jamming signals only if the jammer senses packet transmission on the channel, and jams for a particular period of time during the course of one packet transmission [3], [4], [6].

At receiver R, 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 powerful jamming signals.

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 [4], which is the main focus of this paper.

The key feature of reactive jammer is sensing-before-jamming. The jamming reaction period 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 period* to perform channel sensing and jamming initialization before emitting jamming signals, during which the preamble of the frame could be transmitted without being jammed [6], [24], 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 [32], 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 [33].

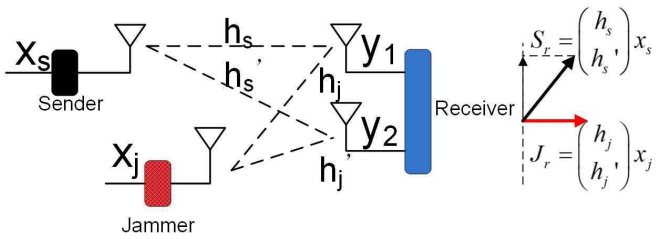


Fig. 2. 1×2 MIMO-OFDM link attacked by a Jammer.

Even the advanced software radio based reactive jammer, who is aware of the implementation details of the network, still incurs a considerable reaction delay including software and hardware delays 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 [6], [7], [34]. In addition, the jammer can transmit arbitrary signals with/without any signal structures.

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 [35]. 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:

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

which live in a two-dimensional vector space corresponding to two receiving 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 a 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 IC technique is known as: *Zero-Forcing* (ZF).

According to Eq. 2, the knowledge of channel coefficients seems indispensable in decoding x_s, the estimation of which is referred to as channel estimation, which can be done by evaluating a known symbol transmitted from the sender. However, as the jammer's signals may not have any recognizable signal structure, it becomes impossible to learn his/her corresponding channel coefficients. Fortunately, we claim that to learn the exact values of jammer's channel coefficients is unnecessary, since we are not interested in decoding jammer's signals. Instead, we show in Section V that it will be sufficient to know the direction of the received jamming signal. Note that, estimating jammer's signal direction[1] is the core of ZF decoder. Also, 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, and MIMO IC is carried out over each subcarrier.

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

In this section, we investigate the impact of reactive jammer to the MIMO-OFDM 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:

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

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

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 the jammer and sender. Note that the jamming signals need not be OFDM signals, and x_{ji} simply represents the narrowband portion of jamming signals on i-th OFDM subband. As mentioned in Section III-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):

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

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.

[1]Signal direction is determined by the received signal vector induced on the receive antenna array by the transmitted signal [35], 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 $[0, \frac{\pi}{2}]$.

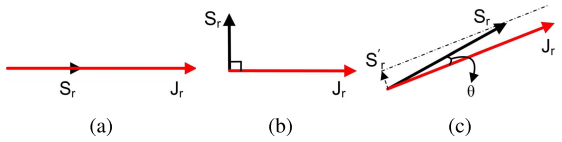


Fig. 3. Different two-dimensional received signal spaces. (a) Overlapped signals. (b) Orthogonal signals. (c) Small angle signals.

A. 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 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 [36]. More specifically, if the spacing between two antennas is narrower than a half wavelength, the channels from these two antennas will become highly correlated [35], which renders two received signal directions similar.

V. Defense Mechanisms Against Reactive Jamming Attack

In this section, we propose effective MIMO-based defense mechanisms to counteract reactive jamming attack based on the 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 *sender signal enhancement* (SSE) 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. 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.

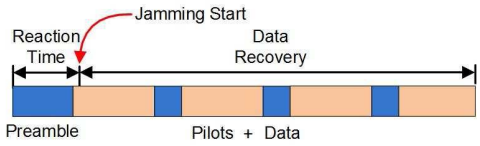


Fig. 4. Extended frame structure.

Inspired by ZigZag decoding technique [37], 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.

1) 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 [11] 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. 4, the basic idea of extracting the received jamming signal J_r is to insert known symbols (i.e. pilots) into the original data frame, and then subtract them from the received mixed signal. The complete jammer channel estimation scheme proceeds as follows: 1) after detecting the beginning of jamming (refer to Section V-B), 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).

2) 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 multipath fading effects. 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 be able to estimate one channel if the other is known. We can make the initial sender channel estimation after receiving the unjammed preamble, and 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 $i = 1, \ldots, n$. After receiving the first pilot (or odd numbered pilot), the receiver updates the jammer channel ratio as:

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

when 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:

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

when 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 $i = 4, 8, \ldots$, while $h'_s(i)$ gets updated when $i = 2, 6, \ldots$. We design the length of two time slots to be within channel coherence time, so that Eqs. (7, 8) hold. 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 [38] 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.

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

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

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.

4) Pilot Insertion and Identification: In order to obtain accurate channel state information at the receiver, the pilots should be inserted frequently when the sender transmits its signals. The density of pilots will be determined by channel coherence time. Denote d as the maximum number of OFDM symbols residing between any two consecutive pilots.

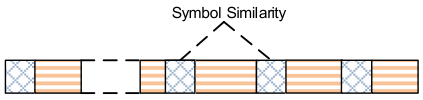


Fig. 5. Symbol similarity between consecutive jammed pilots.

Since the proposed mechanism requires the channel to remain the same during two time slots, channel coherence time should be longer than the time duration of $2d$ OFDM symbols. Note that, the additional pilots introduce limited overheads, which is evaluated in [1].

However, if the location of the pilots is known to the jammer, the jammer may intentionally suspend jamming during these pilot periods to avoid being tracked. Therefore, besides satisfying the insertion frequency requirement, the pilots should be inserted randomly into the packet frame. The jammer has no way of figuring out the exact pilot locations, while the receiver can identify the pilots by the observation that two consecutive jammed pilots will be similar to each other as shown in Fig. 5, which are represented as $(x_s^{\diamond} h_s + x_j h_j)$. When the jamming signals remain unchanged during the transmission of two subsequent pilots, we compute the Euclidean distance between the received symbol y_r and the previously received pilot $y_r^{\diamond}$. The received symbol is identified as a jammed pilot if $\|y_r - y_r^{\diamond}\|^2 < \tau$, where τ can be set as a small threshold such as: 0.1. After identifying the jammed pilots, we can compute the jamming channel ratio accordingly. Even if jamming signals change across two pilots, we can calculate more robust *correlation coefficients* between two received symbols as $E[y_r \cdot (y_r^{\diamond})^*]$. Regardless of jamming signal's variations, the correlation of two jammed pilots is still significantly higher than that of two different symbols. Consequently, the correlation technique is used to reliably identify the jammed pilots.

The aforementioned method will require two pilots to be jammed consecutively. Note that reactive jammers start jamming when they detect the activities on the channel. The jamming activities last for a particular period of time. As long as two consecutive pilots are jammed, the defense mechanism will be able to identify the pilots and conduct interference cancellation. In case when the jammer only jams one single pilot, the number of jammed symbols will be very limited and the rest of unjammed symbols can still be correctly decoded.

Next, we consider two types of advanced reactive jamming attack. The first type of reactive jammer can send jamming signals in a relatively long interval during the course of one packet transmission. As described in Section V-B, the receiver is able to detect the start and termination of jamming signals. The unjammed symbols between two jamming signals can still be decoded correctly. If the jammer sends two jamming signals in a relatively long interval, the jamming channels passed through by these two jamming signals may not be correlated with each other. In that case, the defense mechanism may not be able to identify pilot locations.

Although it is possible for the jammers to launch jamming attack in a relatively long interval while covering one pilot at a time, this possibility is very small. On one hand, as we randomly inserting pilots, it is extremely difficult for the

jammer to shorten their jamming duration to avoid jamming two consecutive pilots while sustaining the jamming effectiveness. On the other hand, the damage caused by such jammers is limited, since all the unjammed symbols can still be recovered. In addition, we can apply error-correcting coding to add resilience to decoding errors.

Moreover, the second type of advanced reactive jammer can launch short burst attack during the jamming period, which increases their chance to cover single pilot at a time, or not cover any pilot at all. Such advanced reactive jammer may be able to defeat our detection mechanisms. Fortunately, the burst symbol error caused by short burst attack presents the pattern that is similar to that caused by channel fading and multipath effect. Therefore, advanced error-correcting codes such as Reed-Solomon codes, Turbo code and LDPC [39] can be applied to resist/recover the errors induced by such advanced jammers.

B. Detecting the Jamming Signal

As mentioned in the previous section, the receiver needs to detect the beginning and the end of jamming to facilitate IC mechanism. The jamming detection problem has been studied in [24], 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. The soft error is further normalized by minimum distance of the constellation. We depict the normalized soft error vector as $\|\mathbf{V}_k\|$ 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 the *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 $\gamma = 2$.

C. Enhanced Defense Mechanism

The basic 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 [11], [31]. 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 [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*.[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.

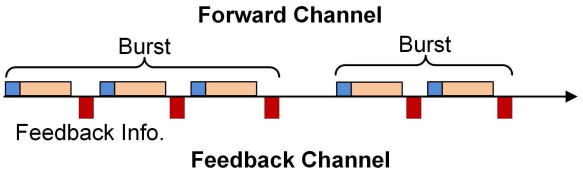


Fig. 6. Burst of packets.

1) 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.

2) Sender Signal Enhancement 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, SSE 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.

We define a "*burst of packets*" as a consecutive sequence of packets during the communications as shown in Fig. 6. 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) 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

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

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.

D. Defending Against Multiple Jammers

Jamming signals from multiple jammers are much harder to eliminate using IC. Without loss of generality, we consider there exist two jammers J_1 and J_2, as shown in Fig. 7. We consider the case when the two jammers do not synchronize with each other, and they do not change their jamming power during the course of one packet transmission. For the receiver, in order to have enough DoF to recover the intended message, it needs to have at least 3 antennas. During the course of multiple jamming attacks, the receiver obtains:

$$\begin{aligned} y_1 &= h_s x_s + h_{j1}x_{j1} + h_{j2}x_{j2}, \\ y_2 &= h'_s x_s + h'_{j1}x_{j1} + h'_{j2}x_{j2}, \\ y_3 &= h''_s x_s + h''_{j1}x_{j1} + h''_{j2}x_{j2}. \end{aligned}$$

When multiple jammers start jamming the communication, we first need a method to detect multiple jamming signals. We exploit the received SNR or network topology changes under multiple jamming attacks to identify the start and termination of multiple jamming attacks [40]. For instance, the received

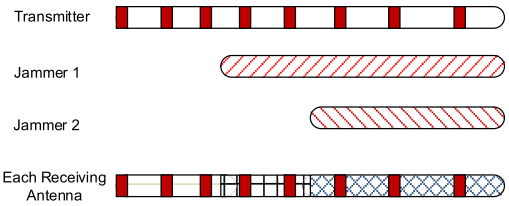


Fig. 7. The attack scenario with two jammers.

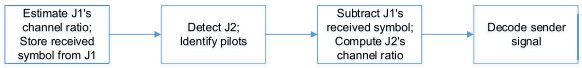


Fig. 8. Message decoding mechanism in the presence of two jammers.

SNR without jamming attacks would be $SNR = \frac{P_{SR}}{P_N}$, and SNR in the presence of J_1 would be $SNR = \frac{P_{SR}}{P_N + P_{J_1R}}$, which turns into $SNR = \frac{P_{SR}}{P_N + P_{J_1R} + P_{J_2R}}$ in the presence of J_1 and J_2. So the receiver can continuously measure received SNR to identify the start and termination of multiple jamming signals.

Without time synchronization, different jammers start jamming at different points of time sequentially, as shown in Fig. 7. The proposed defense mechanism is illustrated in Fig. 8, where we use the first few pilots to capture J_1's jamming channel ratio. Then we use the jamming channel ratio to cancel out the jamming signals. Meanwhile, the receiver will keep record of the received jamming signals, i.e. $h_{j1}x_{j1}$, $h'_{j1}x_{j1}$ and $h''_{j1}x_{j1}$. Once the second jammer starts jamming, we first attempt to find jammed pilots. We use the pilot identification method proposed in Section V-A: since jammed pilots under multiple jamming attacks would still be similar to each other, the receiver stores every received symbols and intends to find two symbols that are highly correlated to each other using the correlation technique. The highly correlated jammed symbols will be identified as pilots. After identifying pilots, we will subtract J_1's jamming signals from received signals as follows:

$$\begin{aligned} y_1 - h_{j1}x_{j1} &= h_s x_s^{\diamond} + h_{j2}x_{j2}, \\ y_2 - h'_{j1}x_{j1} &= h'_s x_s^{\diamond} + h'_{j2}x_{j2}, \\ y_3 - h''_{j1}x_{j1} &= h''_s x_s^{\diamond} + h''_{j2}x_{j2}, \end{aligned}$$

where $x_s^{\diamond}$ is the pilot symbol. Based on the known pilot symbol, we will compute three channel ratios $\frac{h_{j2}}{h'_{j2}}$, $\frac{h_{j2}}{h''_{j2}}$ and $\frac{h'_{j2}}{h''_{j2}}$. Then we use three channel ratios to cancel out jamming signal from J_2 to decode the intended messages as follows:

$$\begin{aligned} x_s^* &\leftarrow \frac{(y_1 - h_{j1}x_{j1}) - \frac{h_{j2}}{h'_{j2}}(y_2 - h'_{j1}x_{j1})}{h_s - \frac{h_{j2}}{h'_{j2}}h'_s}, \\ x_s^* &\leftarrow \frac{(y_1 - h_{j1}x_{j1}) - \frac{h_{j2}}{h''_{j2}}(y_3 - h''_{j1}x_{j1})}{h_s - \frac{h_{j2}}{h''_{j2}}h''_s}, \\ x_s^* &\leftarrow \frac{(y_2 - h'_{j1}x_{j1}) - \frac{h'_{j2}}{h''_{j2}}(y_3 - h''_{j1}x_{j1})}{h'_s - \frac{h'_{j2}}{h''_{j2}}h''_s}. \end{aligned} \quad (11)$$

In fact, based on Eq. 11, we are able to get the decoded result x_s^* using any of the three different channel ratios. But a majority vote can be used to improve the decoding accuracy at the expense of additional computational costs. Although numerous intended messages can be decoded using Eq. 11 under multiple jamming attacks, we still need to update sender channel h_s and J_1's channel ratio h_{j1}/h'_{j1}. We can achieve this by following the iterative channel tracking in Section V-A to update sender channel, J_1's channel ratio and J_2's channel ratio alternately.

E. Defending Against Reactive Jamming in a Multi-Hop Network

In a multi-hop network with legitimate nodes and reactive jammers, every receiver in the network performs IC-based defense mechanism when detecting jamming signals during the packet reception period. With a reliable communication protocol such as TCP, the receiver turns into a sender by sending back a feedback message to inform the original sender about the reception status, after recovering the signals of interest. Because of the "quiet/stealthy" nature of reactive jammer, the traditional media access control (MAC) protocol for wireless networking can still be applied to avoid concurrent transmissions from multiple legitimate senders.

Our defense mechanisms bring conspicuous opportunities to the multi-hop networking. In a traditional multi-hop network with jammers, the link being jammed will be unable to transfer information. However, by employing the proposed IC-based jamming resilient communication scheme, the jammed link is still capable of transmitting information, which introduces new optimization problems associated with rate allocation, resource scheduling, and relay selection in the presence of jammers, while under the protection of IC-based mechanisms. As we can see in Section VII-A, with the presence of reactive jammers, our IC-based mechanism achieves nearly 50% of normal condition throughput on average. Therefore, for a simplified problem formulation, we can use the same optimization algorithm in [41] by considering halving the achievable throughput for each link. We will investigate the cross-layer optimization of networking under jamming attacks in our future work.

F. Dealing With Other Types of Jammers

Our defense mechanisms are designed for reactive jammer. In this section, we briefly discuss about the impacts of constant jammer and random jammer to our defense mechanisms. Constant jammer can jam all the packets including their preambles, which will defeat our defense mechanisms by disrupting the initial channel estimation. On the other hand, constant jamming consumes enormous power, and can be easily detected with a high detection probability [3]. Random jammer randomly alternates between jamming and sleeping. In order to quantify the random jammer's probability of jamming preambles, we give an example of a simplified random jamming attack, and present the necessary 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: $\frac{10/0.1}{(500-10)/0.1} \cdot \frac{1}{2} \approx 1\%$. One can further reduce the probability by introducing a longer burst or burst interval, which makes the preamble distortion a small probability event. Second, as the jamming detector can identify the beginning and the end of jamming attacks promptly, we can modify our defense mechanisms to perform normal processing when the jammer is sleeping and conduct IC within his/her jamming periods. As long as the packet preamble remains intact, MIMO IC can cancel out jamming signals to recover the transmitting packets.

G. Discussion

In the above sections, we show that our defense mechanisms can be applied to the scenario where the receiver has two/three antennas. However, our mechanisms can be generalized to a system with M concurrent transmissions and N receiving antennas using the method in [11].

Our defense mechanisms enable a reliable OFDM communication in the presence of powerful single-antenna reactive jammer. Extending to a network with multi-antenna jammers, the defense mechanism should succeed in canceling jamming signals as long as the jammers' antenna 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 or multiple synchronized single-antenna jammers sending multiple jamming streams simultaneously are more destructive to the MIMO-OFDM communications, since they can deplete the DoF of MIMO links, and also their channels are much harder to estimate. When two single-antenna jammers start jamming simultaneously, the received signals are shown in Eq. 11, where we have eight unknowns including h_{j1}, h'_{j1}, h''_{j1}, h_{j2}, h'_{j2}, h''_{j2}, x_{j1}, x_{j2}. Therefore, it is impossible to solve the equations with only these known variables. It should be noted that the same conclusion can be drawn for the multi-antenna jammer case. Currently, there is no available solution in the literature to provide jamming resilient communication under multi-antenna jammers sending multiple concurrent jamming streams. How to deal with such jammers will be considered in our future work.

VI. Implementation

We build a prototype using five USRP-N200 radio platforms [42] 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 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 enhanced defense mechanism by incorporating SSE.

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 SSE. 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. Otherwise, the sender will directly send the newly generated symbols without applying the rotation vectors. We set the transmission power of both the sender and jammer as $100mW$ by default.

Implementing a SDR-based reactive jammer is itself a non-trivial task [6], [34]. 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 $(t_{\Delta 2} - t_{\Delta 1})$. This mechanism allows us to easily adjust the reaction time of the reactive jammer to emulate different attacking capabilities. Also, the real-world reactive jammers have exactly the same impacts to the targeted communication as our implemented jammers.

VII. Evaluation

In this section, we demonstratively show the ability of jammer to disable MIMO IC mechanism, and we also evaluate the performance of our defense mechanisms in an indoor lab environment. In our experiments, we show the performance of jamming attack and defense mechanisms using a testbed under different bandwidth settings, different jamming powers and different types of jamming signals. The default system parameters are listed in Table I. The relationship between the received signal direction and PDR performance, the measurement of channel coherence time, and the overhead analysis are illustrated in [1].

A. 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. 9. In each run, we place the sender and jammer at the selected locations in Fig. 9. We run the experiments in seven different cases, as shown in Table II. We repeat each case for more than 10 times, with each run transmitting 5000 packets. The jamming signals are randomly generated OFDM-modulated signals with similar configurations as in Table I, but with 512 OFDM FFT length, 200 occupied tones and 128 CP length.

TABLE I
DEFAULT SYSTEM SETUP

Carrier Frequency	2.4512GHz
Modulation Type	BPSK
Transmit Amplitude	1
Transmit Gain	30dB
Receive Gain	30dB
OFDM FFT Length	64
OFDM Occupied Tones	48
OFDM CP Length	64

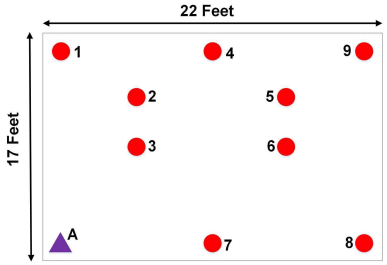


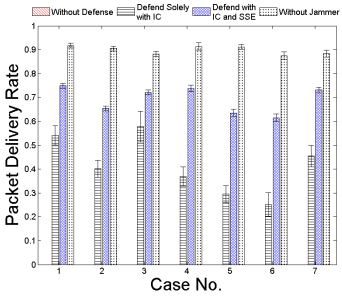
Fig. 9. **Testbed**. The receiver is placed at A, while the sender and jammer are placed at the selected locations 1 to 9.

TABLE II
TESTBED SETUP

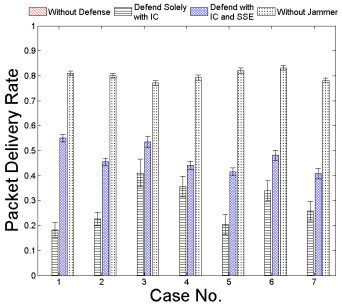
Case Number	Location Set (Sender, Jammer)
1	(1,2)
2	(3,7)
3 (default)	(4,5)
4	(6,8)
5	(8,9)
6	(5,9)
7	(4,8)

First, we show the jamming attack performance by jamming the 1×2 MIMO link, 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 MIMO-OFDM communications completely [1].

Then, we run another set of experiments to jam a 2×2 MIMO link. Fig. 10 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 with IC technique, 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.

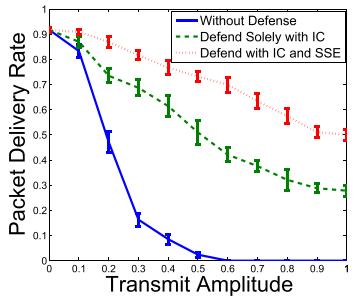


(a) 500KHz Bandwidth

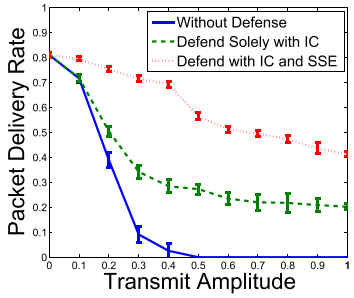


(b) 1M Bandwidth

Fig. 10. Jamming attack and defense performance. (a) 500KHz bandwidth. (b) 1M bandwidth.



(a)



(b)

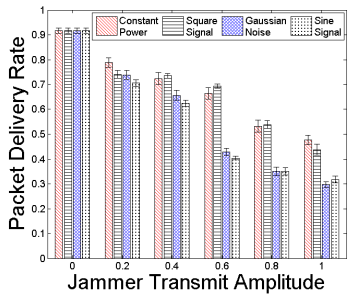
Fig. 11. PDR performance with different jamming powers. (a) Varying jammer's transmit amplitude under 500KHz bandwidth. (b) Varying jammer's transmit amplitude under 1M bandwidth.

Finally, the PDR performance can be further improved using SSE. Both Fig. 10(a) and Fig. 10(b) reveal that the packet delivery performance using enhanced defense mechanism after applying SSE 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 SSE can help sustain more robust OFDM communications. From Fig. 10(a) to Fig. 10(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 the burst of interference and noise in the environment [43].

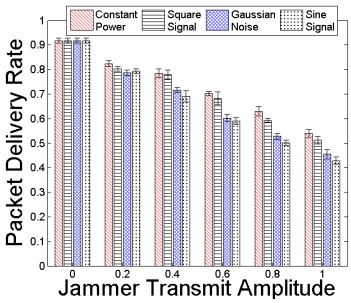
1) Different Jamming Signal Powers: Different jamming signal powers affect the jamming attack and defense performance significantly. High power jamming signals will decrease SJR, making it more difficult to cancel them out. We evaluate the PDR performance of 2×2 MIMO link under reactive jamming attacks with different jamming powers. We change the jamming power by adjusting the jammer's transmit amplitude from 0 to 1, corresponding to the range of jamming power from 0 to 100mW. The sender's transmit amplitude is set as 0.5, and we place the sender and jammer according to case 3. Both Fig. 11(a) and Fig. 11(b) show the PDR drops drastically with the increase of jamming power. Although high power jamming signals drag down the PDR performance using IC and SSE techniques, it is noticeable that the communication system using our defense mechanisms becomes more robust against high power jamming attacks. Even with the jamming power that is nearly two times of sender's power (i.e., with transmit amplitude of 1), the enhanced defense mechanism with IC and SSE still achieves more than 50% PDR under 500KHz bandwidth (40% PDR under 1MHz bandwidth). In the experiment, we find that our proposed defense mechanisms are robust against different power levels of the jammers.

2) Different Types of Jamming Signals: We also evaluate the PDR performance using four types of jamming signals: constant power signal, Gaussian noise, square signal, 100KHz sine signal. These signals are configured to have 0.5 transmit amplitude, 30dB transmit gain, 2.4512GHz RF frequency. Fig. 12(a) shows the PDR performance using IC technique to defend against different types of jamming signals. We vary the jammer's transmit power, and the results illustrate the effectiveness of our defense mechanism under various types of jamming signals. Comparing between different types of jamming signals, we find that Gaussian noise and sine signal lower down the PDR performance of our defense mechanism. This is because the constant power signals and square signals are much easier to cancel out compared with Gaussian noise and sine signals. Fig. 12(b) plots the PDR performance using our enhanced defense mechanism with IC and SSE, which demonstrates the benefits brought by SSE technique. Our enhanced mechanism achieves a improved PDR performance compared with Fig. 12(a) with IC technique under all four types of jamming signals. This result proves the robustness and wide applicability of our defense mechanisms to defend against various types of jamming signals.

3) Throughput Performance: Finally, We further evaluate the throughput performance of the proposed jamming resilient communication mechanism under reactive jammers. Fig. 13(a) and Fig. 13(b) show that our enhanced defense mechanism achieves 140 Kbps (maximum) and 125 kbps (average) under 500KHz bandwidth and 220 Kbps (maximum) and 180 kbps (average) under 1MHz bandwidth. Without jammers,

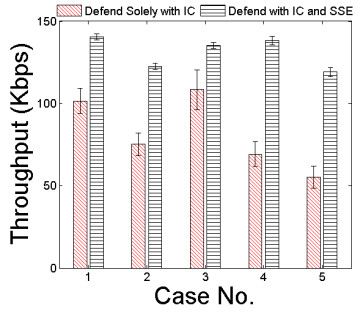


(a)

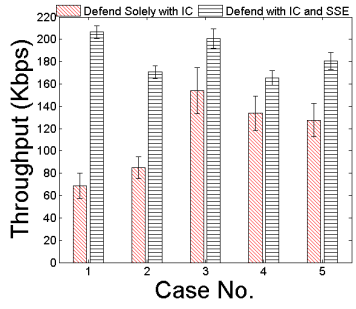


(b)

Fig. 12. PDR performance with different types of jamming signals. (a) Using IC. (b) Using IC and SSE.



(a)



(b)

Fig. 13. Throughput performance using MIMO IC defense mechanisms. (a) 500K bandwidth. (b) 1M bandwidth.

the maximal achievable throughput under 500KHz is 187.5 Kbps, while the achievable throughput under 1MHz is 375 Kbps. Therefore, our enhanced defense mechanism achieves 66.6% of throughput in normal condition under 500kHz, and 48% throughput in normal condition under 1MHz. It is worth mentioning that the reative jammer causes a non-connectivity scenario without defense mechanisms as shown in Fig. 10(a) and Fig. 10(b). Therefore, considering the powerfulness and effectiveness of reactive jammers, the throughput achieved using our defense mechanisms is very promising. In summary, our defense mechanisms indeed retain acceptable data rate communications under powerful reactive jamming attacks.

TABLE III
THROUGHPUT PERFORMANCE COMPARISON

Method	Average Throughput Performance (kbps)
801.11 DSSS	0
BitTrickle	0.55
IC Defense	120
IC+SSE Defense	180

4) Performance Comparison With Existing Methods: We compare the throughput performance with *BitTrickle* [24] and *802.11 DSSS*. BitTrickle defends against high power and wideband jammers, which exploits unjammed bits to establish communication. The USRP+GNURadio prototype implementation uses Reed-Solomon (RS) error correction codes with differential 8PSK modulator/demodulator, and the backoff time is $0ms$. IEEE 802.11 DSSS protocol is used in 802.11 wireless devices, which uses 11-bits barker code for spreading, CSMA/CA and forward error correction to improve the communication resilience. The jammer has a frequency range of 2.3-2.9GHz, with 50mw transmit power and 0.6ms channel sensing time. The transmission bit rate of sender is 1Mbps. The sender transmits 100 data packets each with 1500 byte length, and the experiment is repeated 40 rounds as illustrated in [24]. The average throughput of different methods is shown in Table III, where we can notice a significant throughput improvement using our defense mechanisms to establish jamming resilient communications.

VIII. CONCLUSION

Current wireless communication systems are extremely 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, we exploited MIMO technologies to defend against such jamming attacks. We showed that such attacks can severely disrupt MIMO-OFDM 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. Our prototype experimental results demonstrated that, while the MIMO-OFDM communication can be completely throttled by jamming attacks, our defense mechanisms can effectively turn it into an operational scenario with considerable throughput under different types of jamming attacks.

ACKNOWLEDGEMENT

We appreciate anonymous reviewers for their helpful comments.

REFERENCES

[1] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Mimo-based jamming resilient communication in wireless networks," in *Proc. IEEE INFOCOM*, Apr./May 2014, pp. 2697–2706.

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

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, 2005, pp. 46–57.

[4] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sensor Netw.*, vol. 7, no. 16, 2010, Art. no. 16.

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

[6] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "reactive jamming in wireless networks: How realistic is the threat?" in *Proc. WiSec*, Jun. 2011, pp. 47–52.

[7] A. Cassola, W. Robertson, E. Kirda, and G. Noubir, "A practical, targeted, and stealthy attack against WPA enterprise authentication," in *Proc. 20th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2013, pp. 1–15.

[8] M. Han *et al.*, "OFDM channel estimation with jammed pilot detector under narrow-band jamming," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1934–1939, May 2008.

[9] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *Proc. IEEE ICC*, Jun. 2011, pp. 1–5.

[10] S. Gollakota, S. D. Perli, and D. Katabi, "Interference alignment and cancellation," in *Proc. SIGCOMM*, Aug. 2009, pp. 159–170.

[11] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the RF smog: Making 802.11n robust to cross-technology interference," in *Proc. SIGCOMM*, Aug. 2011, pp. 170–181.

[12] K. C.-J. Lin, S. Gollakota, and D. Katabi, "Random access heterogeneous MIMO networks," in *Proc. SIGCOMM*, Aug. 2011, pp. 146–157.

[13] S. Liu, L. Lazos, and M. Krunz, "Thwarting inside jamming attacks on wireless broadcast communications," in *Proc. WiSec*, Jun. 2011, pp. 29–40.

[14] R. Zhang, Y. Zhang, and X. Huang, "JR-SND: Jamming-resilient secure neighbor discovery in mobile ad hoc networks," in *Proc. ICDCS*, Jun. 2011, pp. 529–538.

[15] M. Strasser, C. Popper, S. Capkun, and C. Mario, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE SP*, May 2008, pp. 64–78.

[16] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, 2009, pp. 207–218.

[17] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Delay-bounded adaptive UFH-based anti-jamming wireless communication," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1413–1421.

[18] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 297–309, Feb. 2012.

[19] S. Liu, L. Lazos, and M. Krunz, "Thwarting control-channel jamming attacks from inside jammers," *IEEE Trans. Mobile Comput.*, vol. 11, no. 9, pp. 1545–1558, Sep. 2012.

[20] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[21] C. Pöpper, M. Strasser, and S. Čapkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. 18th Conf. USENIX Secur. Symp. (SSYM)*, 2009, pp. 231–248.

[22] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming," in *Proc. WiSec*, Jun. 2011, pp. 97–108.

[23] W. Xu, W. Trqappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proc. WiSec*, 2008, pp. 203–213.

[24] Y. Liu and P. Ning, "BitTrickle: Defending against broadband and high-power reactive jamming attacks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 909–917.

[25] T. D. Vo-Huu, E.-O. Blass, and G. Noubir, "Counter-jamming using mixed mechanical and software interference cancellation," in *Proc. WiSec*, Apr. 2013, pp. 31–42.

[26] L. Xiao, J. Liu, Q. Li, N. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2578–2590, Dec. 2015.

[27] A. Garnaev, Y. Liu, and W. Trappe, "Anti-jamming strategy versus a low-power jamming attack when intelligence of adversary's attack type is unknown," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 2, no. 1, pp. 49–56, Mar. 2016.

[28] Q. Wang, K. Ren, P. Ning, and S. Hu, "Jamming-resistant multi-radio multi-channel opportunistic spectrum access in cognitive radio networks," *IEEE Trans. Veh. Technol.*, to be published.

[29] R. Miller and W. Trappe, "Subverting MIMO wireless systems by jamming the channel estimation procedure," in *Proc. WiSec*, Mar. 2010, pp. 19–24.

[30] W. Shen, P. Ning, X. He, H. Dai, and Y. Liu, "MCR decoding: A MIMO approach for defending against wireless jamming attacks," in *Proc. IEEE CNS*, Oct. 2014, pp. 133–138.

[31] W.-L. Shen *et al.*, "Rate adaptation for 802.11 multiuser MIMO networks," in *Proc. MobiCom*, Aug. 2012, pp. 29–40.

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

[33] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in *Proc. 1st Int. Workshop Technol. Policy Accessing Spectr. (TAPAS)*, 2006, Art. no. 12.

[34] D. Giustiniano, V. Lenders, J. B. Schmitt, M. Spuhler, and M. Wilhelm, "Detection of reactive jamming in dsss-based wireless networks," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2013, pp. 43–48.

[35] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[36] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE SP*, May 2010, pp. 286–301.

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

[38] K. Miller, A. Sanne, K. Srinivasan, and S. Vishwanath, "Enabling real-time interference alignment: Promises and challenges," in *Proc. 13th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2012, pp. 55–64.

[39] G. C. Clark, Jr., and J. B. Cain, *Error-Correction Coding for Digital Communications*. New York, NY, USA: Perseus Publishing, 1981.

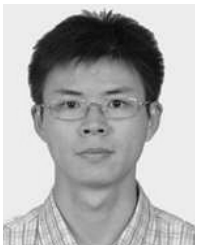
[40] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Localizing multiple jamming attackers in wireless networks," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2011, pp. 517–528.

[41] Y. Shi and Y. T. Hou, "A distributed optimization algorithm for multi-hop cognitive radio networks," in *Proc. IEEE INFOCOM, 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1966–1974.

[42] *Ettus Research LLC*. [Online]. Available: http://www.ettus.com/, accessed Jan. 15, 2016.

[43] W. Stallings, *Data and Computer Communications*, 9th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2010.

Qiben Yan (S'11–M'15) received the Ph.D. degree from the Computer Science Department, Virginia Tech, in 2014. He is currently an Assistant Professor with the Department of Computer Science and Engineering, University of Nebraska–Lincoln. His current research interests include wireless network security and privacy, mobile device privacy protection, botnet, and malware detection.



Huacheng Zeng received the B.E. and M.S. degrees in electrical engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2010, respectively, and the Ph.D. degree in computer engineering from Virginia Tech, Blacksburg, VA, in 2015. He is currently a Senior System Engineer with Marvell Semiconductor, Santa Clara, CA. His research interests lie in wireless network optimization and wireless network security. He was a recipient of 2014 ACM WUWNET Best Student Paper Award.

Tingting Jiang (S'11) received the B.S. (*summa cum laude*) degree in computer science from Virginia Tech, Blacksburg, VA, in 2007, where she is currently pursuing the Ph.D. degree in computer science. From 2007 to 2009, she was a Software Engineer with Intrexon Corporation, Blacksburg, VA. Her research area is in wireless networking and security. She is a recipient of an NSF Graduate Research Fellowship (2011–2014) and a Microsoft Research Graduate Women's Scholarship (2011).

Ming Li (S'08–M'11) received the Ph.D. degree from the Worcester Polytechnic Institute, in 2011. He was an Assistant Professor with the Computer Science Department, Utah State University, from 2011 to 2015. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Arizona. His main research interests are wireless networks and cyber security, with current emphasis on wireless and spectrum security, privacy-preserving big data analytics, and cyber-physical system security. He is a member of the Association for Computing Machinery. He received the NSF Early Faculty Development (CAREER) Award in 2014. He has won a Distinguished Paper Award from ACM ASIACCS 2013, and CCC Blue Sky Ideas Award for best vision papers at ACM SIGSPATIAL 2015.

Wenjing Lou (F'14) received the Ph.D. degree in electrical and computer engineering from the University of Florida, in 2003. From 2003 to 2011, she was a Faculty Member with the Worcester Polytechnic Institute. She has been a Professor with Virginia Tech since 2011. Since 2014, she has been serving as a Program Director at the U.S. National Science Foundation (NSF), where she is involved in the Networking Technology and Systems program and the Secure and Trustworthy Cyberspace program. Her current research interests focus on privacy protection techniques in networked information systems and cross-layer security enhancement in wireless networks, by exploiting intrinsic wireless networking and communication properties.

Y. Thomas Hou (F'14) received the Ph.D. degree from the New York University Tandon School of Engineering. He is currently the Bradley Distinguished Professor of Electrical and Computer Engineering with Virginia Tech, Blacksburg, VA. His current research focuses on developing innovative solutions to complex cross-layer problems in wireless and mobile networks. He has authored two graduate textbooks, *Applied Optimization Methods for Wireless Networks* (Cambridge University Press, 2014) and *Cognitive Radio Communications and Networks: Principles and Practices* (Academic Press/Elsevier, 2009). He is a member of the IEEE Communications Society Board of Governors and the Steering Committee Chair of the IEEE INFOCOM Conference.