Enabling Jamming-Resistant Communications in Wireless MIMO Networks

Huacheng Zeng† Chen Cao† Hongxiang Li† Qiben Yan‡

† University of Louisville ‡ University of Nebraska-Lincoln

***Abstract*—In this paper, we propose a practical anti-jamming solution for wireless MIMO networks to enable their legitimate communications in the presence of *multiple high-power* and *broadband* radio jamming attacks, and evaluate the proposed solution using real-world implementations in a WiFi network. We first develop a blind jamming mitigation (BJM) algorithm, which can cancel jamming signals from *multiple unknown* radio jammers and, at the same time, equalize channel to recover the signals from the legitimate sender. Unlike the existing jamming mitigation algorithms, the BJM algorithm does not need any channel information for jamming mitigation and signal recovery. Based on the BJM algorithm, we develop a jamming-resistant receiver (termed JrRx) and a holistic anti-jamming scheme to salvage legitimate communications in the face of jamming attacks. We have built a prototype of JrRx and evaluated its performance in a WiFi network. Experimental results show that, as long as JrRx has more antennas than the jammers, it can successfully decode the signals from the sender, even if the jamming signals are 20 dB stronger than the signals of interest.**

I. Introduction

As an important topic of network security, radio jamming attacks in wireless networks have received a large amount of research efforts in the past decades and have produced many insightful results regarding the attack destructiveness and defense mechanisms (see, e.g., [1], [2]). Traditional anti-jamming approaches include frequency hopping spread spectrum (FHSS) (see, e.g., [1], [3], [4], [5], [6], [7]) and direct-sequence spread spectrum (DSSS) (see, e.g., [8], [9], [10]). However, these two approaches are not capable of tackling powerful broadband jamming attacks and also result in an inefficient spectrum utilization.

With the proliferation of wireless devices with multiple antennas, multiple-input and multiple-output (MIMO) has been adopted by the mainstream anti-jamming solutions to salvage legitimate communications in jamming environments through spatial jamming mitigation at the authorized users. For example, [11] developed interference cancellation solution to enable WiFi communications in the presence of jamming signals from home devices such as microwave oven and baby monitor. [12] developed a counter-jamming solution by combining mechanical antenna reconfiguration and digital signal processing. [13] proposed an anti-jamming mechanism to defend against reactive jammer attacks in WiFi communications. However, the existing MIMO-based anti-jamming solutions highly hinge upon the availability of accurate jamming channel information (e.g., channel ratio), which is hard to estimate in real-world wireless systems due to the lack of knowledge of jamming signals. Therefore, the existing MIMO-based anti-jamming solutions are not amenable to practical implementation in real-world wireless systems, especially in multi-jammer environments.

In this paper, we propose a practical anti-jamming solution to salvage legitimate communications in wireless networks with multiple high-power and broadband radio jammers by leveraging the recent advances in MIMO techniques at the PHY layer, and evaluate the proposed solution on a wireless testbed consisting of USRP2 and GNURadio. We first develop a blind jamming mitigation (BJM) algorithm, which can cancel the jamming signals from unknown jammers and recover the desired signals from the legitimate sender. Unlike the existing jamming mitigation algorithms that rely on the availability of accurate jamming channel ratio (see, e.g., [11], [12], [13]), the BJM algorithm does not need any channel information for jamming mitigation and signal recovery.

Based on the BJM algorithm, we develop a jamming-resistant receiver (termed JrRx) to decode data packets from a legitimate sender in the presence of interfering signals from multiple unknown jammers. JrRx has two key modules: jamming-resilient synchronization and BJM. The core of each module is a linear spatial filter. JrRx has a low complexity (linear operations without iterative decoding) and therefore is suited for practical use. Based on JrRx, we design a holistic anti-jamming scheme to enable legitimate communications in WiFi networks when attacked by multiple jammers.

We have built a prototype of JrRx using GNURadio-USRP2 and evaluated its performance in a WiFi network with multiple jammers. Unlike prior works that use packet delivery rate as the performance metric (e.g., [11], [12], [13]), we use the post signal-to-jamming-plus-noise ratio (pSJNR) of the decoded signal symbols to evaluate the performance of JrRx. Since pSJNR determines the raw bit error rate (raw BER, BER without channel code), it is more accurate to qualify the jamming mitigation capability of our solution. Experimental results show that (i) JrRx is robust to various jamming signals (e.g., full-spectrum jamming, half-spectrum jamming, single-frequency jamming, and rectangular-waveform jamming); and (ii) as long as JrRx has more antennas than the jammers, it can successfully decode the signals from the sender, even in the scenarios where the jamming signals are 20 dB stronger than the desired signals.

Our anti-jamming solution advances the state-of-the-art in the following aspects: (i) Unlike the prior solutions that require

978-1-5386-0683-4/17/$31.00 ©2017 IEEE
978-1-5386-0683-4/17/$31.00 ©2017 IEEE

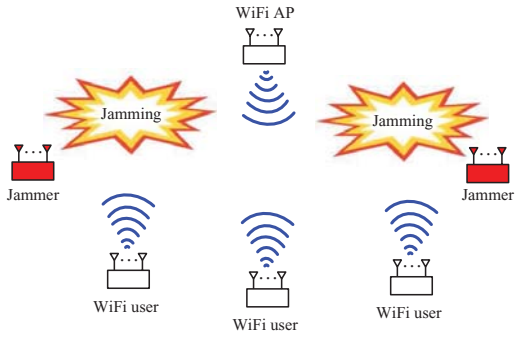


Fig. 1: Jamming attacks in WiFi networks.

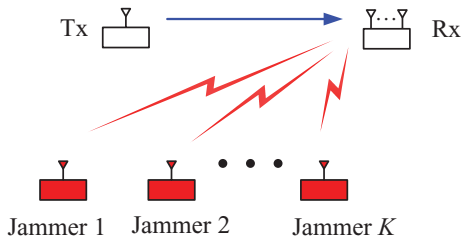


Fig. 2: A simplified jamming model.

jamming channel ratio, our solution does not require *any channel information*, making it suitable for practical use. (ii) Our solution can be used in both jamming and non-jamming scenarios, thereby eliminating the requirement of jamming detection. (iii) Our solution is a *holistic* solution, which includes not only jamming mitigation but also jamming-resilient synchronization and carrier sensing components. (iv) Our solution can tackle *multiple* high-power broadband jamming attacks in real-world systems. To the best of our knowledge, this is the first practical anti-jamming solution that can tackle multiple high-power broadband jamming attackers.

II. Jamming Attack Model

We consider a WiFi network as shown in Fig. 1, which has a WiFi access point (AP) and a group of WiFi users. The data transmission uses OFDM modulation at the PHY layer, which is the case in most of WiFi networks (e.g., 802.11 a/g/n/ac/ad/ax/ay). Each WiFi device is equipped with multiple antennas. Carrier sense multiple access (CSMA) or its variation is used as the MAC protocol to control the media access among the users.

In the network, there exists one or more radio jamming devices. The jammers intentionally emit radio jamming signals into the air with the aim of disrupting the legitimate communications in the WiFi network. In our study, we make the following assumptions on the jamming attacks.

- The WiFi devices have no knowledge of the jamming devices and jamming signals, including the number of jamming devices, the bandwidth and power of jamming signals, and the waveform of jamming signals.
- The bandwidth of jamming signals can be larger than, equal to, or less than the bandwidth of legitimate signals. The spectrum of jamming signals can either fully or partially overlap with the spectrum of legitimate signals.
- The jamming signals can be any waveform (e.g., OFDM signals, single-frequency signals, rectangular-waveform signals, and noise-like signals). The waveform of jamming signals may vary over time.
- The power of jamming signal can be much larger than the power of legitimate signal (e.g., 20 dB stronger).
- Each jamming emitter can be a constant jammer (constantly emitting jamming signals), random jammer (randomly emitting jamming signals), or reactive jammer (intermittently emitting jamming signals).

In addition to the above assumptions for the jamming attacks, we also make the following assumptions for the WiFi devices. We assume that the number of antennas at each WiFi device is greater than the total number of antennas at all jamming devices. Note that, nowadays, multiple antennas are widely available at WiFi devices on the market. For example, Linksys AC5400 WiFi router has eight antennas. Commercial off-the-shelf network interface card (NIC) such as Intel WiFi chip 6300 and Qualcomm WiFi chip AR9590 have three antennas. Considering the advances of MIMO technique in semiconductor industry and the emergence of "massive MIMO", we believe this is a mild assumption in wireless networks.

Roadmap of Our Solution Development. We first present a BJM algorithm and then develop a jamming-resistant receiver (JrRx). After that, we show that JrRx can enable legitimate communications in the presence of multiple jammers as shown in Fig. 1. Finally, we prototype the JrRx using GNURadio-USRP2 and evaluate its performance using experimental results.

III. A Blind Jamming Mitigation Algorithm

Consider a simplified jamming model as shown in Fig. 2. It consists of 1 single-antenna sender, one M-antenna receiver, and K single-antenna jammers. We denote this network as $\mathcal{N}(1, K, M)$. In this network, we assume the number of antennas on the receiver is greater than the total number of antennas on the jammers, i.e., $M > K$. In what follows, we first develop a BJM algorithm in a narrow-band network and then apply it to an OFDM-based broadband network.

A. BJM in Narrow-Band Network

Denote H_j as the channel coefficient between the sender's antenna and the receiver's jth antenna. Denote G_{jk} as the channel coefficient between the kth jammer's antenna and the receiver's jth antenna. Denote X as the original signal at the sender. Denote Z_k as the jamming signal at the kth jammer. At the receiver, denote $\mathbf{Y} = [Y_1, Y_2, \cdots, Y_M]^T$ as the received signal vector, with Y_j being the signal from its jth antenna; denote $\mathbf{W} = [W_1, W_2, \cdots, W_M]^T$ as the noise vector, with

W_j being the noise from its jth antenna. Then, we have

$$Y_j = H_j X + \sum_{k=1}^{K} G_{jk} Z_k + W_j, \qquad 1 \le j \le M. \tag{1}$$

At the receiver, we employ a linear spatial filter to decode the signal from its sender in the face of jamming signals. Here, the linear spatial filter refers to a set of complex weights that are used to combine the signal streams from different antennas at the receiver. Denote $\mathbf{P}$ as the linear spatial filter (a $M \times 1$ complex vector) and $\hat{X}$ as the decoded (estimated) signal. Then we have

$$\hat{X} = \mathbf{P}^H \mathbf{Y}, \tag{2}$$

where $(\cdot)^H$ operator represents the conjugate transpose.

Based on the above definition, the mean squared error (MSE) can be written as:

$$\begin{aligned} \text{MSE} = \mathbb{E}\big[|\hat{X} - X|^2\big] = \mathbb{E}\big[|\mathbf{P}^H \mathbf{Y} - X|^2\big] = \mathbf{P}^H \mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]\mathbf{P} \\ + \mathbb{E}\big[X X^H\big] - \mathbb{E}\big[\mathbf{P}^H \mathbf{Y} X^H\big] - \mathbb{E}\big[X \mathbf{Y}^H \mathbf{P}\big], \end{aligned} \tag{3}$$

where $\mathbb{E}(\cdot)$ represents the statistical expectation operator.

This equation is actually a quadratic function of $\mathbf{P}$. To minimize MSE, we can take the gradient with respect to $\mathbf{P}$. The optimal filter $\mathbf{P}$ can be obtained by setting the gradient to zero, which we show as follows:

$$\frac{\partial \text{MSE}}{\partial \mathbf{P}} = 2\mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]\mathbf{P} - 2\mathbb{E}\big[\mathbf{Y} X^H\big]. \tag{4}$$

By setting $\frac{\partial \text{MSE}}{\partial \mathbf{P}}$ to zero, we can obtain the optimal filter by

$$\mathbf{P} = \mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]^{\dagger} \mathbb{E}\big[\mathbf{Y} X^H\big], \tag{5}$$

where $(\cdot)^{\dagger}$ operator represents pseudo-inverse.

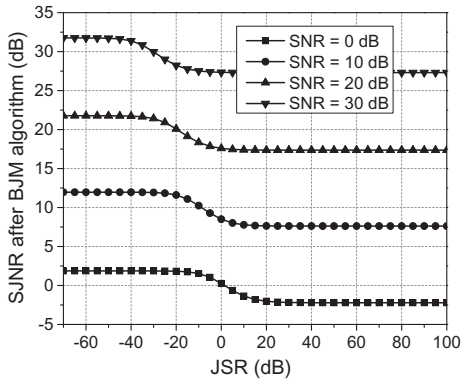
Eq. (5) is the optimal design of $\mathbf{P}$. To estimate $\mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]$ and $\mathbb{E}\big[\mathbf{Y} X^H\big]$ in (5), we exploit the pilot signals (preamble or reference symbols) that are widely available in wireless communication systems. Denote L as the number of pilot signals in the system. Denote $[\tilde{X}(1), \tilde{X}(2), \cdots, \tilde{X}(L)]$ as the pilot signals at the sender. Denote $[\tilde{\mathbf{Y}}(1), \tilde{\mathbf{Y}}(2), \cdots, \tilde{\mathbf{Y}}(L)]$ as the received pilot signals at the receiver, which also includes jamming signals. Then, we can approach the statistic expectation using the average operation over a set of pilot signals. Specifically, we estimate $\mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]$ and $\mathbb{E}\big[\mathbf{Y} X^H\big]$ as follows:

$$\mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big] := \frac{1}{L} \sum_{l=1}^{L} \tilde{\mathbf{Y}}(l) \tilde{\mathbf{Y}}(l)^H, \tag{6}$$

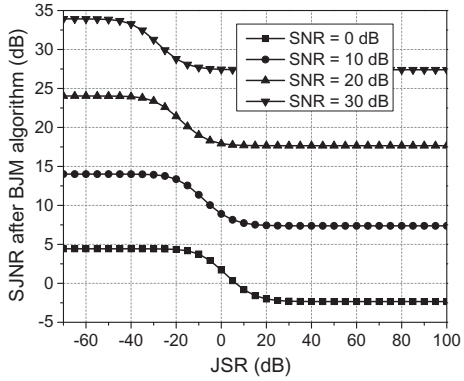
$$\mathbb{E}\big[\mathbf{Y} X^H\big] := \frac{1}{L} \sum_{l=1}^{L} \tilde{\mathbf{Y}}(l) \tilde{X}(l)^H, \tag{7}$$

where $:=$ operator represents value estimation. It should be noted that $\tilde{\mathbf{Y}}(l)$ includes both the pilot signals from the sender and the jamming signals from the jammers. Based on (6) and (7), the filter $\mathbf{P}$ can be written as

$$\mathbf{P} := \Big[\sum_{l=1}^{L} \tilde{\mathbf{Y}}(l) \tilde{\mathbf{Y}}(l)^H\Big]^{\dagger} \Big[\sum_{l=1}^{L} \tilde{\mathbf{Y}}(l) \tilde{X}(l)^H\Big]. \tag{8}$$



(a) Performance of BJM algorithm in $\mathcal{N}(1, 1, 2)$.



(b) Performance of BJM algorithm in $\mathcal{N}(1, 2, 3)$.

Fig. 3: Performance of BJM algorithm in two networks. JSR represents the *jamming-to-signal ratio* before BJM and SJNR represents the *signal-to-jamming-plus-noise ratio after BJM*.

We now summarize the BJM algorithm as follows:

Algorithm 1 (BJM): The BJM algorithm consists of two steps: (i) the receiver computes complex vector $\mathbf{P}$ *using (8); and (ii) the receiver employs the resulting complex vector* $\mathbf{P}$ *to decode the desired signals using (2).*

It is worth pointing out that the spatial filter $\mathbf{P}$ has two functionalities: *jamming mitigation* and *channel equalization*. That is, the filter $\mathbf{P}$ not only mitigates the jamming signals, but it also equalizes the channel to recover the desired signal from the sender.

Performance of BJM Algorithm. Filter $\mathbf{P}$ in (8) is the core of the BJM algorithm. As we can see from (8), the BJM algorithm requires no knowledge of the jamming signals and devices. Specifically, it does not need to know the jamming channel information G_{jk}; it does not need to know the jamming signals Z_k; and it does not need to know the signal channel information H_j. It only needs to know the pilot signals at the sender $[\tilde{X}(1), \tilde{X}(2), \cdots, \tilde{X}(L)]$. Due to these special properties, the BJM algorithm is particularly suited for jamming mitigation in a blind manner.

From the derivation of $\mathbf{P}$, we can see that the BJM algorithm guarantees to yield the minimum MSE between the estimated and original signals. Suppose that the sender has sufficient pilot signals. Then we have the following lemmas regarding

the performance of the BJM algorithm.

Lemma 1: In noise-negligible scenarios, the BJM algorithm can: (i) completely cancel jamming signals; and (ii) perfectly recover the desired signal.

Proof. Consider the network in Fig. 2. Denote $\mathbf{H}$ as the compound channel matrix between the transmitters and the receiver, which is a $M \times (1+K)$ complex matrix. The first column of $\mathbf{H}$ is the channel vector between the sender and the receiver and the $(k+1)$th column of $\mathbf{H}$ is the channel vector between the kth jammer and the receiver (for $1 \le k \le K$). Denote $\mathbf{X}$ as the compound transmit signals at all transmitters (sender and jammers), i.e., $\mathbf{X} = [X,\ Z_1,\ Z_2, \cdots, Z_K]^T$. Then, the received signal vector at the receiver can be written as $\mathbf{Y} = \mathbf{HX} + \mathbf{W} \overset{(a)}{=} \mathbf{HX}$, where (a) follows from our assumption that the noise is negligible.

When the sender has enough pilot signals, (8) is equivalent to (5). Based on (5), we have

$$\mathbf{P} = \mathbb{E}\big[\mathbf{Y}\mathbf{Y}^H\big]^\dagger \mathbb{E}\big[\mathbf{Y}X^H\big] = \big[\mathbf{H}\mathbf{R}_\mathrm{X}\mathbf{H}^H\big]^\dagger \big[\mathbf{H}\mathbf{D}_X\big], \quad (9)$$

where $\mathbf{R}_\mathrm{X}$ is $\mathbf{X}$'s autocorrelation matrix and $\mathbf{D}_X = [\sigma_X^2,\ 0,\ 0 \cdots, 0]$ with σ_X^2 being X's variance.

Based on (2) and (9), we have

$$\hat{X} = \mathbf{P}^H\mathbf{Y} = \mathbf{P}^H\mathbf{HX} = \Big(\big[\mathbf{H}\mathbf{R}_\mathrm{X}\mathbf{H}^H\big]^\dagger \big[\mathbf{H}\mathbf{D}_X\big]\Big)^H \mathbf{HX}$$
$$= \Big(\mathbf{H}^H\big[\mathbf{H}\mathbf{R}_\mathrm{X}\mathbf{H}^H\big]^\dagger \big[\mathbf{H}\mathbf{D}_X\big]\Big)^H \mathbf{X} = [1\ 0 \cdots 0]\mathbf{X} = X.$$

Recall that $\hat{X}$ are the estimated signal at the receiver and X is the original signal at the sender. The above equation indicates that the jamming signals can be completely cancelled and the desired signal can be perfectly recovered. □

Lemma 1 shows the superior performance of the BJM algorithm in noise-negligible scenarios. In the scenarios where the noise is not negligible, it is hard to analytically qualify the performance of the BJM algorithm. Hence, we resort to simulation. Fig. 3 shows the performance of the BJM algorithm in two networks: $\mathcal{N}(1,1,2)$ and $\mathcal{N}(1,2,3)$. In the figures, the x-axis is the jamming-to-signal ratio (JSR) before BJM and the y-axis is the signal-to-jamming-plus-noise ratio (SJNR) after BJM. We can see that, in all noise scenarios (SNR 0 dB, 10 dB, 20 dB, or 30 dB), when the JSR increases from -60 dB to 100 dB, the SJNR degradation is less than 5 dB in $\mathcal{N}(1,1,2)$ and less than 7 dB in $\mathcal{N}(1,2,3)$. This indicates that the BJM algorithm is very effective in jamming mitigation in low-, mid-, and high-SNR scenarios.

Complexity of BJM Algorithm. From Alg. 1 we can see that the BJM algorithm involves matrix multiplication and pseudo-inverse manipulations. All these manipulations are linear operations. The dimension of the matrix is the number of antennas at the receiver, which is typically small (less than or equal to eight in 802.11ac). Hence, the complexity of this algorithm is very low and acceptable in real-world wireless systems.

B. BJM in OFDM-MIMO broadband Network

Multiple Antennas at Transmitters. The BJM algorithm was developed based on the simplified jamming model in Fig. 2, where each sender/jammer has a single antenna. Now the question is if the BJM algorithm can be used in a MIMO network where the sender and jammer have multiple antennas as shown in Fig. 4. The answer is yes and we elaborate it as follows. Consider the case where the sender has multiple antennas. It can use its multiple antennas for spatial diversity and send one data stream to the receiver. This diversity mode is supported by all WiFi standards. In this mode, a sender with multiple antennas can be viewed as a sender with one combined antenna according to the MIMO theory [14, Ch. 7]. Therefore, the BJM algorithm can be used in the network where the sender has multiple antennas.[1] We now consider the case where the jammer has multiple antennas. In the context of blind jamming mitigation, a jammer with N antennas can be treated as N independent single-antenna jammers. Therefore, the BJM algorithm can be used in the network where each jammer has multiple antennas.

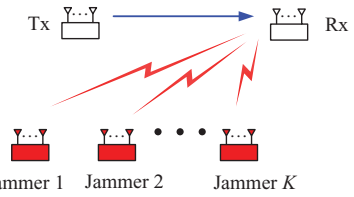


Fig. 4: A jamming model in a MIMO network.

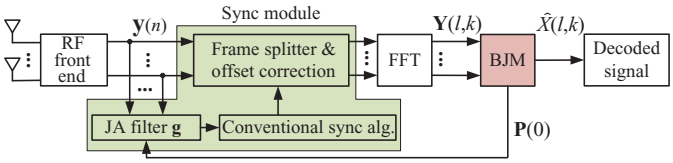


Fig. 5: Architecture of JrRx.

To sum up, as long as the number of antennas at the WiFi device is greater than the total number of antennas at the jammers, the receiver can successfully decode the signals from the multi-antenna sender. We will show this point using experiment results in Section VII.

Broadband Communications. In a broadband MIMO-OFDM network as shown in Fig. 4, in order to support high-rate data transmission, the broadband channel is divided into many narrow-band channels using OFDM modulation. Each OFDM subcarrier corresponds to a narrow-band channel. To handle the jamming attacks in a broadband network, we apply the BJM algorithm in Alg. 1 to each of the OFDM subcarriers. Specifically, for the signals on each individual subcarrier, we use (8) to compute its BJM filter and then use (2) to decode its desired signal at the receiver.

IV. JrRx: A Jamming-Resistant Receiver

In this section, we design a jamming-resistant receiver (JrRx) that decodes its desired signals in the presence of

[1]Note that, even if the sender uses its multiple antennas for spatial multiplexing and sends multiple data streams to the receiver, the BJM algorithm can still work as long as the receiver has enough antennas.

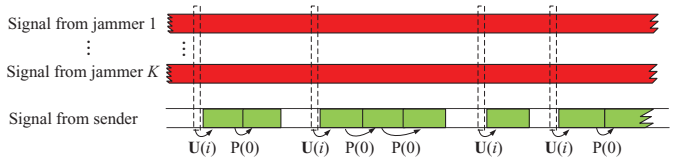


Fig. 6: Jamming signals and WiFi signal patterns.

jamming signals. Fig. 5 shows JrRx's architecture, which includes a RF front-end module, a sync module, a FFT module, and a BJM module. Compared to a conventional multi-antenna receiver, JrRx does not need any hardware change; it only needs baseband signal processing algorithm upgrade. As shown in Fig. 5, JrRx has two new components: the sync module and the BJM module. In what follows, we first present the design of JrRx, with emphasis on these two modules, and then discuss the applications of JrRx.

A. Synchronization

The sync module in a receiver has two functionalities: timing synchronization and frequency synchronization. Timing synchronization is to search for the start of each frame by exploiting auto or cross correlation of the signal stream in the time domain. Frequency synchronization is to estimate and correct the frequency offset between the sender and the receiver.

Synchronization is a main challenge in JrRx, as it must be done in the presence of jamming signals. As shown in Fig. 5, our synchronization approach consists of three steps: (i) design a spatial jamming-alleviation (JA) filter, denoted as $\mathbf{g}$, to alleviate the jamming signals for the time-domain signal streams; (ii) employ conventional methods (e.g., [15], [16]) to estimate the time and frequency offset over the jamming-alleviated signal stream; and (iii) split the signal streams into individual frames and compensate for their frequency offset. In this approach, JA filter $\mathbf{g}$, which is a $M \times 1$ complex vector, is the key component. This filter combines the signal streams from different JrRx's antennas with the aim of alleviating jamming signals by exploiting the spatial degrees of freedom provided by the multiple antennas. In what follows, we present our design of the JA filter in two cases.

Case I: Use BJM Filter as JA Filter. Referring to Fig. 6, if a frame was previously found in a given amount of time,[2] we use the BJM filter as the JA filter to alleviate the jamming signals. Specifically, we design the JA filter by letting $\mathbf{g} = \mathbf{P}(0)$, where $\mathbf{P}(0)$ is subcarrier 0's BJM filter in the previous frame. Note that subcarrier 0 is the central subcarrier in their OFDM spectrum. Regarding the performance of this filter, we have the following lemma:

Lemma 2: If the channels between sender/jammer and receiver are frequency-flat and the noise is negligible, then JA filter $\mathbf{g} = \mathbf{P}(0)$ *can completely cancel jamming signals.*

The argument of this lemma is straightforward based on Lemma 1 and therefore we omit it. Lemma 2 shows the efficacy of our JA filter design in an ideal scenario. In practice, although the channels are not frequency-flat, the frequency responses of neighboring OFDM subcarriers are highly correlated. Therefore, filter $\mathbf{P}(0)$ can significantly alleviate the jamming signals in the time domain at the receiver.

[2]The amount of time varies depending upon channel coherent time and it can be empirically set.

Algorithmus 2 Design of JA filter $\mathbf{g}$ for synchronization.

1: **if** A frame was found in a given amount of time **then**
2: Denote $\mathbf{P}(k)$ as subcarrier k's BJM filter in that frame;
3: $\mathbf{g} = \mathbf{P}(0)$;
4: **else**
5: Compute the left unitary matrix $\mathbf{U}$ using (10);
6: **for** i from 1 to M **do**
7: Compute the maximum correlation value of signal stream $\mathbf{U}(i)^H\mathbf{y}(n)$, which we denote as c_i;
8: **end for**
9: $i_m = \arg\max_{1\le i\le M}\{c_i\}$;
10: $\mathbf{g} = \mathbf{U}(i_m)$;
11: **end if**

Case II: Using Left-Singular Vector as JA Filter. Again, referring to Fig. 6, if a frame was not found in a given amount of time, then we use a left-singular vector of the signals as the JA filter to alleviate the jamming signals. Specifically, we conduct the singular value decomposition (SVD) as follows:

$$[\mathbf{U} \quad \mathbf{\Sigma} \quad \mathbf{V}] = \text{svd}\Big(\sum_{n=1}^{N_\text{s}} \mathbf{y}(n)\mathbf{y}(n)^H\Big), \tag{10}$$

where $\mathbf{y}(n)$ is the time-domain signal vector at the receiver (see Fig. 5), N_s is the number of signal samples, $\mathbf{U}$ is the left complex unitary matrix ($M \times M$). Denote $\mathbf{U}(i)$ as the ith column of matrix $\mathbf{U}$, which is also know as the ith left-singular vector. For each of the M left-singular vectors in $\mathbf{U}$, we measure the auto/cross correlation of the resulting signal $\mathbf{U}(i)^H\mathbf{y}(t)$ for $1 \le i \le M$, and choose the one that results in the largest correlation value as the JA filter $\mathbf{g}$.

For this JA filter, we have the following lemma:

Lemma 3: If the channels between sender/jammer and receiver are frequency-flat and the noise is negligible, then there is at least one column of $\mathbf{U}$ *that can completely cancel jamming signals.*

The argument and interpretation of Lemma 3 are similar to those of Lemma 2. We therefore omit it.

Summary of JA Filter Design. Alg. 2 summarizes our algorithm of the JA filter design, where lines 2–3 correspond to Case I and lines 5–10 correspond to Case II. The worst-case computational complexity of this synchronization algorithm is M times that of conventional synchronization algorithm. In real-world systems, Case I is dominant and, therefore, the complexity of sync module is similar to that of the conventional sync algorithm.

B. Jamming Mitigation and Channel Equalization

As shown in Fig. 5, once a radio frame has been found and the frequency offset has been corrected, the signal streams are fed into the FFT module, which converts each signal

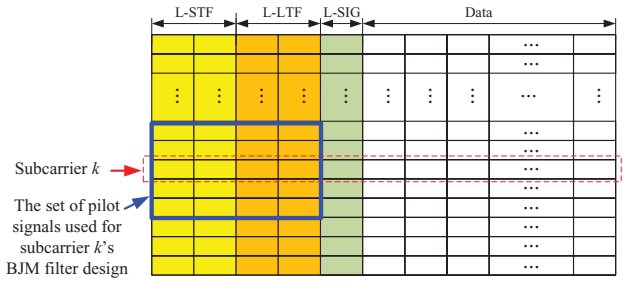


Fig. 7: A WiFi frame structure. The legacy short training field (L-STF) has two OFDM symbols and the legacy long training field (L-LTF) has two identical OFDM symbols, which are used for synchronization and channel estimation.

stream from the time domain to the frequency domain. For each subcarrier of the resulting frequency-domain signals, we employ the BJM algorithm to mitigate jamming signals and equalize the channel distortion. Specifically, for subcarrier k, we use (8) to compute its BJM filter $\mathbf{P}(k)$ and use (2) to decode its desired signal $\hat{X}(k)$.

As shown in (8), the design of the BJM filter needs pilot signals. The more pilot signals are available, the better the BJM filter performs. Now the question is: for each subcarrier, which pilot signals in the preamble field can be used for its BJM filter design? For this question, as illustrated in Fig. 7, for the design of subcarrier k's BJM filter, we use the pilot signals not only on that subcarrier but also on its neighboring subcarriers. This is because the channels on the neighboring subcarriers are highly correlated in real-world networks.

Denote $\mathcal{P}_k$ as the set of pilot signals that are used for subcarrier k's BJM filter design. Based on WiFi's frame structure in Fig. 7, we have $\mathcal{P}_k = \{(l,k') : 1 \le l \le 4; k-2 \le k' \le k+2\}$, where $1 \le l \le 4$ means the pilot OFDM symbols in L-STF and L-LTF fields, and $k-2 \le k' \le k+2$ means the neighboring two subcarriers.[3] Then, based on (8), subcarrier k's BJM filter $\mathbf{P}(k)$ can be written as:

$$\mathbf{P}(k) = \Big[\sum_{(l,k')\in\mathcal{P}_k} \mathbf{Y}(l,k')\mathbf{Y}(l,k')^H\Big]^{\dagger}\Big[\sum_{(l,k')\in\mathcal{P}_k} \mathbf{Y}(l,k')X(l,k')^H\Big],$$

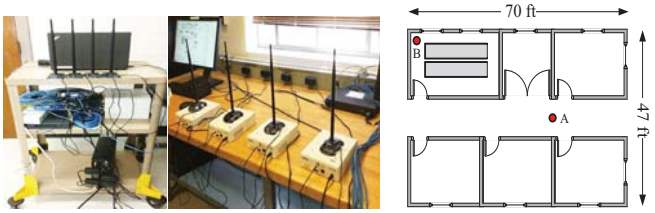
where $X(l,k')$, $(l,k') \in \mathcal{P}_k$, represents the pilot signals at the sender and $\mathbf{Y}(l,k')$, $(l,k') \in \mathcal{P}_k$, represents the received signal vector at the receiver, which includes both pilot signals and jamming signals.

After computing the BJM filter $\mathbf{P}(k)$, we use (2) to decode the desired signals on each subcarrier of all the OFDM symbols in the frame.

V. An Anti-Jamming Scheme

In this section, we show how JrRx enables legitimate communications in a WiFi MIMO network with one or multiple jamming emitters as shown in Fig. 1. In what follows, we first present the operations at the WiFi receivers and then present the operations at the WiFi transmitters. Collectively, these operations constitute an anti-jamming scheme that enables jamming-resistant communications in a network environment.

[3]The number of neighboring subcarriers should be determined upon the channel correlation in the network, which can be empirically set.



(a) JrRx. (b) Sender and jammers. (c) Test scenario.

Fig. 8: Experimental setup and test scenario.

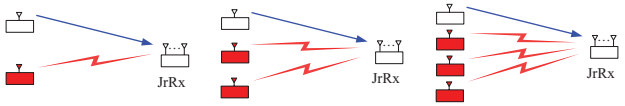
Jamming Mitigation at WiFi Receiver. Although the WiFi network has many devices (AP and users), only one of them is actively transmitting signals at one moment due to the media access control. Hence, the communication in the WiFi network under jamming attacks can be modeled as the jamming problem in Fig. 4. Recall that we assumed that each WiFi device has more antennas than the jammers. Based on the results in Section IV, we know that JrRx can successfully decode the signals from the sender in the presence of jamming signals.

Carrier Sensing at WiFi Transmitter. In a WiFi network, CSMA mechanism is used for media access control. Specifically, if a device wants to transmit, it first conducts carrier sense to assess whether the channel is idle. If the channel is idle, the device will defer and wait for a random amount of time; otherwise, the device will use the channel for data transmission.

Now the question is how a WiFi device conducts carrier sense in the presence of jamming signals. Considering the robustness of auto/cross correlation of WiFi preamble in the presence of jamming [15], we employ the preamble detection method for carrier sense at each WiFi device. Specifically, each WiFi device acts as a receiver before transmitting, and uses the information from the synchronization algorithm in Section IV-A to assess whether there is a WiFi signal in the channel. If a WiFi frame was found by the time synchronization algorithm in a given amount of time, then the channel is considered busy and the WiFi device defers and waits for a random amount of time before its next attempt. Otherwise, the channel is considered idle and the WiFi device uses it for data transmission.

VI. Implementation

We have built a prototype of JrRx using USRP N210 devices [17], OctoClock-G CDA-2990 [17], Gigabit-Switch, and GNURadio software package [18], as shown in Fig. 8a. We have also built a prototype of one sender using one USRP N210 device and GNURadio. The sender and JrRx run a simplified PHY layer of 802.11n in legacy mode, using the frame structure in Fig. 7. Each OFDM symbol has 64 subcarriers, with 52 of them being used for payloads. QPSK modulation is used for data transmission. Due to the hardware limitations, each USRP N210 at the sender and JrRx is



(a) 1-jammer case. (b) 2-jammer case. (c) 3-jammer case.

Fig. 9: Three experimental cases.

configured to span a 5 MHz channel by setting the decimation rate to 20. The carrier frequency is configured to 2.4 GHz.

We have built a prototype of three jammers using three USRP N210 devices and GNURadio. The waveform, spectrum, and power of each jammer's radio signal can be configured as needed. The sender and the three jammers are shown in Fig. 8b.

VII. Performance Evaluation

A. Experimental Setup

We evaluate the performance of JrRx in three cases as shown in Fig. 9. In each case, the sender and jammers are placed at location A and the receiver (JrRx) is placed at location B in Fig. 8c. Fig. 8b shows the physical placement of the sender and the jammers at location B. We place the jammers closely to the sender because this setting leads to one of the most destructive jamming attacks.

The sender's transmit power is fixed to 0 dBm and each jammer's power can be adjusted from 0 dBm to 20 dBm. The spectrum of jamming signals fully covers that of the legitimate signals, unless stated otherwise.

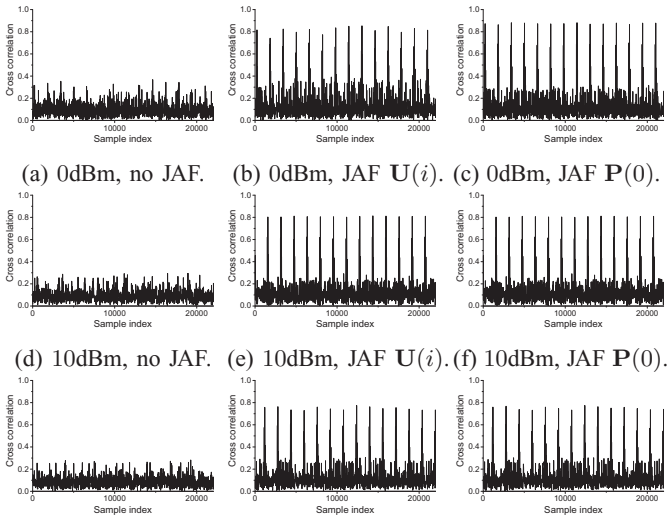
B. Performance Metric

We use the post signal-to-jamming-plus-noise ratio (pSJNR) as the performance metric to assess the performance of JrRx. Mathematically, $\text{pSJNR} = 10\log_{10}(\mathbb{E}(|X|^2)/\mathbb{E}(|X-\hat{X}|^2))$, where X is the original signal at the sender and $\hat{X}$ is the estimated signal at JrRx. Once we have measured the pSJNR at JrRx, the Raw-BER (BER without channel code) of QPSK data transmission can be inferred by Raw-BER $= 2Q(\sqrt{\gamma}) - Q^2(\sqrt{\gamma})$, where $Q(\cdot)$ is Q-function and γ is the linear value of pSJNR (i.e., $\gamma = 10^{\text{pSJNR}/10}$) [19, Ch. 4]. In real-world wireless systems (e.g., WiFi and LTE), Raw-BER 10^{-2}, which corresponds to pSJNR 8.2 dB according to the above formula, is sufficient for the receiver to successfully decode the signal. Therefore, pSJNR 8.2 dB will be used as the pSJNR threshold of successful data reception at JrRx.

C. A Case Study

As a case study, we explore the performance of JrRx in the network as shown in Fig. 9a, where the sender and jammer have one antenna and JrRx has two antennas. The sender's transmit power is fixed to 0 dBm and the jammer's transmit power is set to $\{0,\ 10,\ 20\}$ dBm, respectively.

Performance of Sync Algorithm. We first evaluate the performance of our proposed sync algorithm in JrRx. Recall that the core of our sync algorithm is two jamming-alleviation filters (JAF): BJM filter $\mathbf{P}(0)$ and left-singular vector $\mathbf{U}(i)$. We

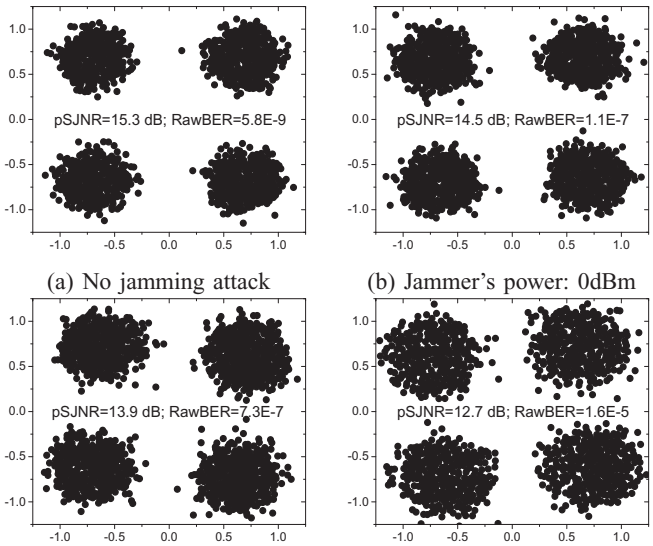


(a) 0dBm, no JAF. (b) 0dBm, JAF $\mathbf{U}(i)$. (c) 0dBm, JAF $\mathbf{P}(0)$.

(d) 10dBm, no JAF. (e) 10dBm, JAF $\mathbf{U}(i)$. (f) 10dBm, JAF $\mathbf{P}(0)$.

(g) 20dBm, no JAF. (h) 20dBm, JAF $\mathbf{U}(i)$. (i) 20dBm, JAF $\mathbf{P}(0)$.

Fig. 10: Performance of the two jamming-alleviation filters (JAF) in the sync algorithm when the jammer's transmit power is 0 dBm, 10 dBm, and 20 dBm.



(a) No jamming attack (b) Jammer's power: 0dBm

(c) Jammer's power: 10dBm (d) Jammer's power: 20dBm

Fig. 11: Constellation diagram of the decoded symbols at JrRx when the jammer uses different transmit powers.

evaluate their impacts on the cross-correlation of the received signals, respectively. In our experiments, the cross-correlation results are obtained by correlating WiFi's L-LTF signal with a local L-LTF signal.

Fig. 10 presents the impacts of the two JAFs on the cross-correlation results of the received signals at JrRx, where (a–c) presents the cross-correlation results when the jammer's transmit power is 0 dBm, (d–f) presents the cross-correlation results when the jammer's transmit power is 10 dBm, and (g–i) presents the cross-correlation results when the jammer's transmit power is 20 dBm. Let's first look at the first row of

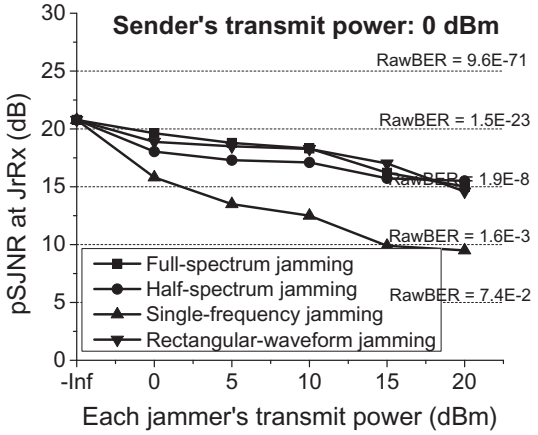


Fig. 12: Impact of jamming signal waveforms on the performance of JrRx.

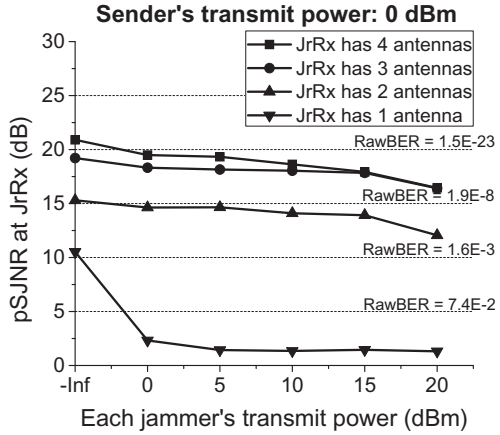


Fig. 13: Impact of Jamming power on the performance of JrRx when the network has one jammer.

Fig. 10 (i.e., when the jammer's transmit power is 0 dBm). Comparing (a) and (b) we can see that using left-singular vector $\mathbf{U}(i)$ as JAF can significantly improve the performance of the sync algorithm. Comparing (a) and (c) we can see that using BJM filter $\mathbf{P}(0)$ as JAF can significantly improve the performance of the sync algorithm as well. The same phenomenon can be observed in the second and third rows of Fig. 10 (i.e., when the jammer's transmit power is 10 and 20 dBm). Based on the above observations, we conclude that the proposed sync algorithm is competent to achieving synchronization in the presence of jamming attacks.

Performance of BJM Algorithm. We now evaluate the performance of the BJM algorithm in JrRx. Fig. 11 presents the constellation diagram of the decoded symbols at JrRx. Fig. 11a presents the constellation diagram when there is no jamming attack. In this case, the pSJNR is 15.3 dB, which corresponds to Raw-BER 5.8E-9. Fig. 11b presents the constellation diagram when jammer's transmit power is 0 dBm. In this case, the pSJNR is 14.5 dB, which corresponds to Raw-BER 1.1E-7. Fig. 11c presents the constellation diagram when jammer's transmit power is 10 dBm. In this case, the pSJNR is 13.9 dB, which corresponds to Raw-BER 7.3E-7. Fig. 11d presents the constellation diagram when jammer's transmit power is 20 dBm. In this case, the pSJNR is 12.7 dB, which corresponds to Raw-BER 1.6E-5. Comparing Fig. 11d to Fig. 11a we can see that the pSJNR degradation is less than 3 dB when the jamming signal is 20 dB stronger than the desired signal. This indicates the robustness of the proposed BJM algorithm.

D. Impact of Jamming Waveforms

We study the destructiveness of different jamming waveforms in the network as shown in Fig. 9a. In this experiment, we consider four jamming attacks: (i) full-spectrum jamming, (ii) half-spectrum jamming, (iii) single-frequency jamming (i.e., cosine jamming signal), (iv) rectangular-waveform jamming (i.e., sinc-shaped jamming spectrum). Fig. 12 presents the performance of JrRx under these four jamming attacks. We can see that the pSJNR at JrRx is greater than 8.2 dB and thus JrRx can successfully decode the desired signal under the four jamming attacks.

From the figure we have another observation. That is, the single-frequency jamming attack is the most destructive one among the four jamming attacks. We analyzed the raw experimental data and found that the destructiveness of single-frequency jamming attack is attributed to its adverse effect on the frequency synchronization (i.e., estimating the frequency offset at JrRx). When the jamming signal is a strong cosine waveform, JrRx has difficulty to accurately estimate the frequency offset and, as a result, the pSJNR degrades accordingly.

E. Impact of Jamming Power

We now study the performance of JrRx under different jamming powers in the three cases as shown in Fig. 9.

One-Jammer Case. Fig. 13 presents the experimental results that were measured in the network with one jammer (see Fig. 9a). In this figure, "-Inf" on x-axis means that the network has no jamming signal. From the experimental results we can see that, when JrRx has two or more antennas, it successfully decodes the desired signal from the sender (i.e., pSJNR ≥ 8.2 dB). When we increase the jamming power from -Inf to 20 dBm, the pSJNR degradation at JrRx is less than 5 dB. This indicates the robustness of the BJM algorithm in JrRx.

Two-Jammer Case. Fig. 14 presents the experimental results that were measured in the network with two jammers (see Fig. 9b). Since there are two jammers in the network, the total jamming power is the sum of the signal power from the two jammers. We can see that, when JrRx has three or more antennas, it successfully decodes the desired signal from the sender (i.e., pSJNR ≥ 8.2 dB), even if the jamming signal is 20 dB stronger than the desired signal.

Three-Jammer Case. Fig. 15 presents the experimental results that were measured in the network with three jammers (see Fig. 9c). We can see that, when JrRx has four antennas, it successfully decodes the desired signal from the sender (i.e., pSJNR $\geq$ 8.2 dB), even if the jamming signal from each

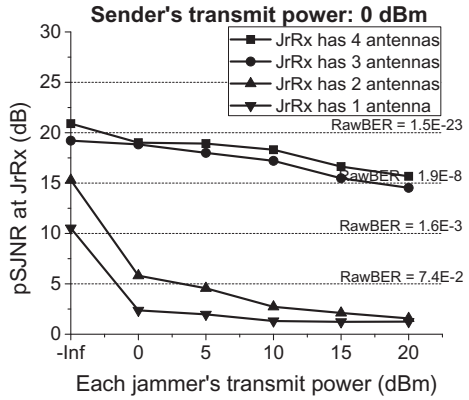


Fig. 14: Impact of Jamming power on the performance of JrRx when the network has two jammers.

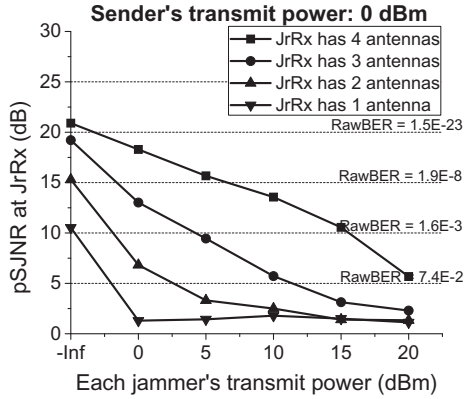


Fig. 15: Impact of Jamming power on the performance of JrRx when the network has three jammers.

jammer is 17 dB stronger than the desired signal. Note that there are three jammers in the network so there is additional 4.8 dB for the total jamming power.

Summary of Observations. We summarize our observations based on the experimental results. For the conventional receiver, it cannot successfully decode the desired signal when the jamming signal has similar or larger power than the desired signal. In contrast, for the proposed JrRx, *as long as it has more antennas than the jammers, it can successfully decode the desired signal, even if the jamming signals are* 20 *dB stronger than the desired signals.*

VIII. Conclusions

This paper presents the first practical anti-jamming solution that can tackle multiple high-power and broadband jamming attackers in wireless MIMO networks. The core of our solution is JrRx, which has two key components: a jamming-resilient sync algorithm and a BJM algorithm. The BJM algorithm can mitigate jamming signals without the need of any channel information, and the sync algorithm can accomplish timing and frequency synchronization in the presence of strong jamming. Experimental results show that (i) JrRx is robust to various jamming signals (full-spectrum jamming, half-spectrum jamming, single-frequency jamming, and rectangular-waveform jamming); and (ii) as long as JrRx has more antennas than the jammers, it can successfully decode the signals from the sender, even in the scenarios where the jamming signals are 20 dB stronger than the desired signals.

Acknowledgment

This work was supported in part by KSEF-148-502-17-400, NASA Kentucky EPSCoR under NASA award No. NNX15AK28A, and an EVPRI Internal Research Grant from the Office of the Executive Vice President for Research and Innovation at the University of Louisville.

References

[1] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, pp. 46–57, 2005.

[2] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *IEEE Symposium on Security and Privacy*, pp. 174–188, 2013.

[3] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems," *IEEE Transactions on Mobile Computing*, vol. 15, no. 9, pp. 2247–2259, 2016.

[4] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *ACM Workshop on Wireless security*, pp. 80–89, 2004.

[5] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE INFOCOM*, pp. 2526–2530, 2007.

[6] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Symposium on Security and Privacy*, pp. 64–78, 2008.

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

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

[9] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure," in *ACM ACSAC*, pp. 367–376, 2010.

[10] T. Jin, G. Noubir, and B. Thapa, "Zero pre-shared secret key establishment in the presence of jammers," in *ACM MobiHoc*, pp. 219–228, 2009.

[11] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the RF smog: Making 802.11n robust to cross-technology interference," in *ACM SIGCOMM*, vol. 41, pp. 170–181, 2011.

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

[13] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, 2016.

[14] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[15] A. B. Awoseyila, C. Kasparis, and B. G. Evans, "Robust time-domain timing and frequency synchronization for OFDM systems," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, 2009.

[16] Y.-C. Wu, K.-W. Yip, T.-S. Ng, and E. Serpedin, "Maximum-likelihood symbol synchronization for ieee 802.11a wlans in unknown frequency-selective fading channels," *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 2751–2763, 2005.

[17] E. Research, "USRP N210," *www.ettus.com/product/details/UN210-KIT [Online; accessed 8-March-2017]*.

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

[19] J. G. Proakis, "Digital communications," *McGraw-Hill, New York*, 1995.