Demo Abstract: An Anti-Jamming Wireless Communication System

Huacheng Zeng
University of Louisville

***Abstract*—This demonstration presents a real-time anti-jamming MIMO-OFDM wireless communication system that consists of a transmitter, a receiver, and a high-power wideband radio jammer. The key component of our system is a new PHY design for the receiver, which can mitigate jamming signal and recover the desired signal. We demonstrate using software-defined radio (SDR) USRP devices that OFDM-MIMO wireless communications can be enabled in the face of unknown high-power wideband jamming attacks. We show that our PHY design for the receiver can achieve up to 30 dB jamming cancellation.**

***Index Terms*—Anti-jamming, wireless communications, wireless security, jamming mitigation, channel equalization**

I. Introduction

The destructiveness of radio jamming attacks in wireless networks has been widely recognized and many anti-jamming approaches have been developed to protect legitimate wireless communications against jamming attacks. Traditional anti-jamming approaches include frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). However, these approaches are not capable of tackling high-power wideband jamming attacks.

With the recent advances in MIMO technology, multiple antennas on wireless devices have been exploited to defend against jamming attacks in wireless communications (see, e.g., [1], [2]). However, most of the existing MIMO-based anti-jamming solutions rely upon the availability of accurate jamming channel information (e.g., channel ratio), which is hard to obtain in real-world wireless systems due to the lack of knowledge of jamming signals. Therefore, these MIMO-based anti-jamming solutions are not amenable to practical implementation in real-world wireless systems.

In [3], we presented a jamming-resistant solution to secure legitimate Wi-Fi communication against constant wideband jamming attacks by leveraging multiple antennas on Wi-Fi devices. We first developed a jamming mitigation algorithm, which can cancel the interfering signals from the jammer and recover the desired signals from the legitimate transmitter. Unlike the existing jamming mitigation algorithms that rely on the availability of accurate jamming channel ratio, the proposed jamming cancellation algorithm does not require any channel information. Based on the jamming mitigation algorithm, we further developed a jamming-resistant receiver which can decode data packets from a legitimate transmitter in the presence of interfering signals from multiple unknown jammers.

In this demonstration, we present an enhanced PHY design for wireless receiver which can defend against not only constant but also reactive and proactive high-power wideband jamming attacks. Figure 1 shows our anti-jamming wireless communication system. Figure 2 shows the proposed signal frame format, where L-STF is legacy short training field, L-LTF is legacy long training field, L-SIG is legacy signal field, and RTF is the rear training filed. We will show that the receiver can successfully decode the OFDM signals from the transmitter in the face of unknown wideband jamming signal, and its jamming cancellation capability is up to 30 dB. A short demo video is provided in [4].

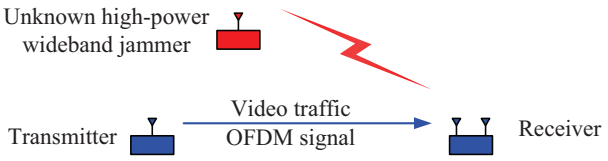


Fig. 1: An anti-jamming wireless communication system.

Fig. 2: Frame format of OFDM signals.

II. Anti-Jamming Receiver Design

In this section, we present an anti-jamming receiver that decodes its desired signals in the presence of jamming signals. Figure 3 shows its architecture, where the signal processing blocks in the shadowed area are the new modules. In what follows, we present the two new modules of the anti-jamming receiver.

Synchronization. The sync module has two functionalities: timing synchronization and frequency synchronization. Timing synchronization is to search for the bursty frames 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 transmitter and the receiver.

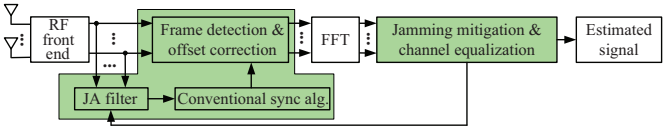


Fig. 3: A new PHY design for wireless receiver.

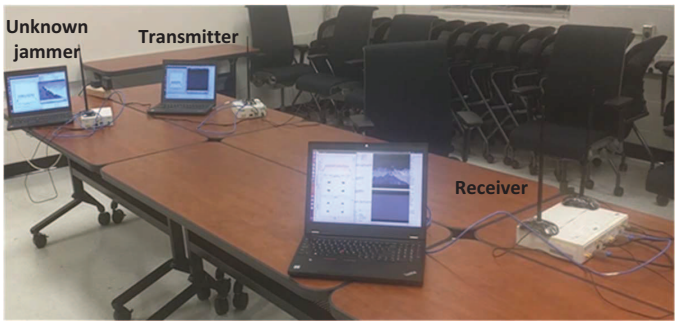


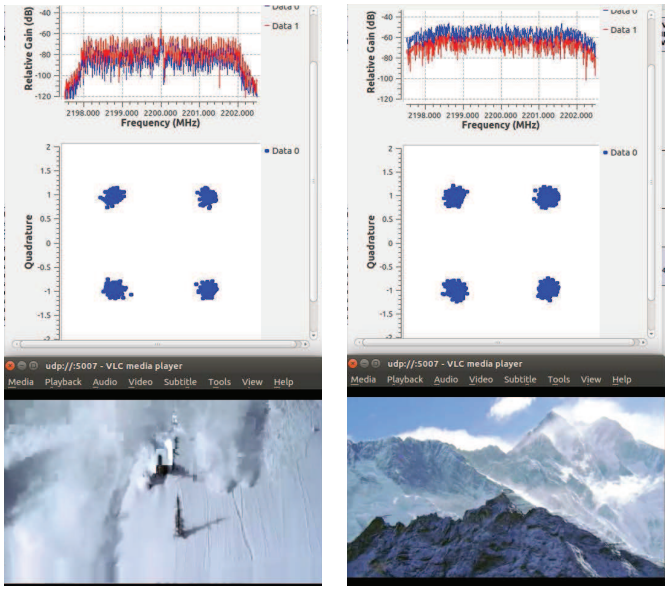
Fig. 4: Demonstration setup (a transmitter, a receiver, and an unknown jammer).

Synchronization in anti-jamming receiver is a challenging task as it must be done in the presence of jamming signals. Our synchronization approach consists of three components: (i) a spatial jamming-alleviation (JA) filter, which is used to alleviate the jamming signals for the time-domain signal streams; (ii) a conventional sync algorithm, which is used to estimate the timing and frequency offsets; and (iii) frame detection and carrier frequency offset correction. The JA filter is the key component in the synchronization module. We constructed the JA filter through a sophisticated manipulations of the jamming-mitigation filters and the left-singular vectors of the incoming signals.

Jamming Mitigation and Channel Equalization (JMCE). As shown in Figure 3, 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 stream from the time domain to the frequency domain. For each subcarrier of the resulting frequency-domain signals, we employ a jamming mitigation algorithm to cancel jamming signals and equalize channel distortion. Specifically, for each subcarrier, we compute a JMCE filter and use this filter to estimate the original signal. To compute the JMCE filters, we leverage the reference signals in the L-STF, L-LTF and RTF. We developed an adaptive jamming mitigation algorithm to construct the JMCE filter, which can achieve up to 30 dB jamming mitigation.

III. Demonstration

In this demonstration, we will show the jamming resistance of our designed wireless receiver. Figure 4 shows the setup of our demonstration. We have built the transmitter using a USRP N210 device and a laptop. We also have built the anti-jamming receiver using two USRP N210 devices and a laptop. The two USRP N210 devices are connected via a MIMO cable. The proposed PHY for the receiver has been implemented on the laptop using the GNURadio software package [5]. The carrier frequency is set to 2.48 GHz and the bandwidth is set to 5 MHz. The transmitter runs a revised PHY layer of 802.11n using the frame format in Figure 2. Each OFDM symbol has 64 subcarriers, with 52 of them being used for payloads. QPSK modulation is used for data transmission. We have built a radio jammer using a USRP N210 device and a laptop. The waveform, bandwidth, carrier frequency, and



(a) Performance of receiver without jamming.

(b) Performance of receiver with 15 dB stronger jamming.

Fig. 5: Performance of anit-jamming receiver.

power of the jamming signal can be controlled through the user interface of GNURadio software on the laptop.

We demonstrate that the receiver can successfully decode the signal from the transmitter in the face of unknown jamming attack. The receiver displays the constellation diagram of the decoded video signal from the transmitter and plays the video smoothly, as shown in Figure 5. The demo participants can control the parameters (e.g., bandwidth, power, waveform, carrier frequency) of jamming signal using the interface control panel. The demo participants can observe the impact of the jamming attacks on the performance of the receiver through the constellation diagram and the played video. The demo participants will see that the receiver can successfully decode the video signals from the transmitter and play the video even if the jamming signal is 20 dB stronger than the useful signal.

IV. Acknowledgments

This work was supported in part by NSF grant CNS-1717840, KSEF-148-502-17-400, and NASA Kentucky EPSCoR under NASA award No. NNX15AK28A.

References

[1] 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.

[2] 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.

[3] H. Zeng, C. Cao, H. Li, and Q. Yan, "Enabling jamming-resistant communications in wireless mimo networks," in *IEEE Conference on Communications and Network Security (CNS)*, 2017.

[4] H. Zeng, "Demo: An anti-jamming wireless communication system," *http://www.ece.louisville.edu/hzeng/aj.html [Online; accessed 27-December-2017]*.

[5] E. Blossom, "GNU Radio: Tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, pp. 1–4, 2004.