Full-Duplex Constant-Envelope Jamceiver and Self-Interference Suppression by Highpass Filter: Experimental Validation for Wi-Fi Security

Jaakko Marin, *Graduate Student Member, IEEE*, Micael Bernhardt, and Taneli Riihonen, *Senior Member, IEEE*

***Abstract*— Unauthorized access to data has been a recognized risk of wireless systems for many decades. While security solutions in communications engineering have typically revolved around cryptography in the higher layers, a semi-recent development is the elevating interest into security in the physical layer, namely by utilizing jamming for protection. In this paper, we present an experimental study into a full-duplex jammer–receiver (i.e., "jamceiver") that is able to simultaneously interfere with the same radio resources it is actively receiving from. The radio architecture is loosely based on frequency-modulated continuous-wave radars that are constant-envelope radio transceivers, which benefit from simple-but-efficient self-interference suppression in the analog baseband domain by using a passive highpass filter. Its limitation to constant-envelope transmission is not an issue for efficient jamming waveforms unlike it would be with conventional direct-conversion transceivers in full-duplex communications. To show the performance limits of a practical jamceiver, we present comprehensive measurement results from a laboratory environment as well as a jamming case study from an open park area with actual Wi-Fi signals. Especially, the experiments validate the feasibility of preventing eavesdropping with continuous low-power jamming in a large area around a full-duplex jamceiver that acts as an access point for simultaneously offering decent Wi-Fi service to an off-the-shelf laptop.**

***Index Terms*— Physical-layer security, in-band full-duplex radio, self-interference, jamming, eavesdropping.**

I. Introduction

SECURITY of wireless data transfer has been an important and greatly researched topic for decades. Due to the broadcasting nature of wireless communications systems, it is difficult to prevent others from intercepting or counterfeiting messages. Instead, the focus in ensuring data secrecy and integrity has mostly been in the realm of encrypting the transmitted messages and verifying the message sender through software means. However, in recent years physical-layer security has gained increasing interest amongst researchers [1].

One major goal of physical-layer security is to prevent eavesdropping by utilizing directive antennas and/or jamming to deny others from receiving the transmitted signal-of-interest (SOI). In jamming, the accurate reception and even detection of a signal is prevented by transmitting a powerful interference signal over the time–frequency resources used by the system that is being jammed. Curious readers unfamiliar with jamming may refer to the profound survey in [2]. Utilizing jamming in physical-layer security is very well researched topic, and there are plenty of excellent publications with half-duplex systems into the topic of physical-layer security proving the concept through simulations [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17] and measurements [18], [19], [20], to name just a few. Unfortunately, despite security intentions, half-duplex jamming can also negatively impact friendly users utilizing the same resources.

To further the plausibility of jamming in physical-layer security, we can look into full-duplex (FD) transceivers (TRX), which are capable of simultaneously transmitting and receiving on the same frequency resources [21]. By using such a system as a jammer–receiver (i.e., "jamceiver") it is possible to achieve physical-layer security by utilizing jamming, without carefully calibrating different subsystems to prevent disruptive friendly interference. In practice, the receiving system can simultaneously transmit a jamming signal to prevent eavesdroppers from interpreting the SOI, while its own reception is not compromised. While there is a significant number of

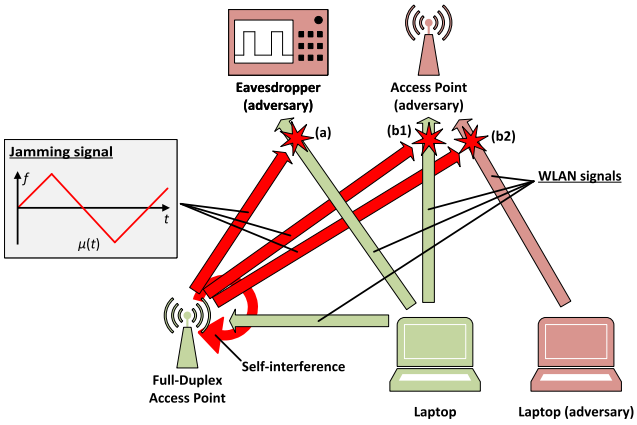


Fig. 1. Conceptual use-case scenarios covered by our experimental validation, where the full-duplex access point prevents an adversary from (a) eavesdropping, (b1) operating a fake access point or (b2) communicating on the same spectrum, while simultaneously receiving WLAN transmission-of-interest. For the clarity of the figure, arrows from the laptop (adversary) towards the eavesdropper and the FD access point have been omitted.

Manuscript received 25 October 2022; revised 20 April 2023; accepted 27 April 2023. Date of publication 21 June 2023; date of current version 21 August 2023. This work was supported by the Research Council of Finland under Grant 315858, Grant 341489, and Grant 346622. *(Corresponding author: Jaakko Marin.)*

The authors are with the Faculty of Information Technology and Communication Sciences, Tampere University, 33720 Tampere, Finland (e-mail: jaakko.marin@tuni.fi; micael.bernhardt@tuni.fi; taneli.riihonen@tuni.fi).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSAC.2023.3287615.

Digital Object Identifier 10.1109/JSAC.2023.3287615

splendid publications showing the plausibility and theoretical performance of such a system through numerical and simulated results [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], to the Authors' knowledge there appears to be only a few experimental works showing how well a FD prototype system would perform in a jamming context in the real world, such as [32] and [33]. Furthermore, these studies were conducted using direct conversion architectures.

To further motivate a possible improvement that a FD capable jamceiver could bring to physical-layer security, we can consider a use-case where a full-duplex capable jamceiver would act as an access point to a wireless local area network (WLAN); Fig. 1 shows such a conceptual scenario. The eavesdropper is prevented from receiving the WLAN transmission from the laptop by the jamming transmission sent by the jamceiver. Meanwhile, due to self-interference (SI) suppression, the jamceiver access point is able to receive the WLAN transmission without severe deterioration to signal-to-interference-plus-noise ratio (SINR). Such operation could be also used to prevent other adversaries, such as fake access points, from receiving the laptop's transmissions or to prevent them from using the whole bandwidth the access point is operating on for their own purposes. A useful scenario for the first operation could be for instance in relaying [4], [23], [27]. Meanwhile for the latter, such scenarios could be for instance in a school setting, where a teacher wants to prevent students from using their cellphones while she or he can still access internet resources. Other possible use scenarios could be preventing drone use in an area [20], or an extreme case where security forces try to prevent a remotely triggered bomb from detonating [32].

In this paper, we present an experimental full-duplex capable transceiver which transmits a frequency-sweeping continuous-waveform (FMCW) signal, commonly seen in low-cost radars, to prevent an eavesdropper from correctly interpreting a WLAN signal, while still being able to receive the same signal. This jamceiver uses the transmitted sweeping waveform in the downmixer, which causes the self-interference from the antenna coupling and nearby reflections to devolve into stationary low-frequency tones. They can then be attenuated with a sufficiently wide *passive* highpass filter (HPF). Thus, at the cost of limiting the transmitted waveform to have constant envelope, the SI suppression becomes significantly of lower complexity than with *active* and adaptive subtraction-based SI cancellation used conventionally in full-duplex prototypes that are based on the direct-conversion architecture.

In our considered threat model, the capabilities of the eavesdropper are assumed to be on the level of a packet-sniffing off-the-shelf laptop. We utilize jamming in the uplink to prevent the threat of eavesdropping, i.e., intercepting transmitted bits, during a sensitive period in data transfer. As such, the target of our transmission is to cause as much bit errors to the eavesdropper as possible. Additionally, we measure how widening the jamming to cover the entire 2.4 GHz industrial, scientific, and medical (ISM) band affects our own reception performance, in order to showcase the extreme situation, where there is a need to prevent all traffic in the shared spectrum.

TABLE I
REFERENCES EVALUATING JAMMING AS PHYSICAL-LAYER SECURITY

	Half-duplex systems	Full-duplex direct conv. arch.	Full-duplex FMCW arch.
Simulations	[3]–[17]	[22]–[31]	[34]–[36]
Measurements	[18]–[20], etc.	[32], [33]	**this paper**

The effectiveness of the proposed FMCW signal in jamming has been extensively studied in the past [18], [37], and thus we instead focus on the reception performance of our proposed jamceiver; since, while the limitation to constant envelope is not a problem for jamming, downmixing the WLAN signal with a sweeping local oscillator (LO) signal unfortunately causes the WLAN signal after downmixer to sweep through the frequency band, according to the transmitted signal. This way, the WLAN signal sweeps though our highpass filter, which causes a frequency-varying attenuation, i.e., a notch sweeping through it. This effect distorts the received signal and may cause some unavoidable symbol and bit errors. A further limitation is that we consider only the uplink to be physically secured, as fitting the proposed architecture to already space constrained user equipment might prove difficult.

We have previously presented initial theoretical and simulation results of a similar system in [34] and [35]. Within this paper, we give comprehensive experimental characterization of how different sweep and HPF parameters affect the reception performance of our FD system in a laboratory environment. As the ultimate validation, we especially show that the jamceiver is in practice capable of simultaneous data reception and eavesdropping prevention through an outside measurement. Through these results we show that our system is capable of improving physical-layer security through jamming while still being able to receive data with sufficient performance. These are the first experimental results presenting the real over-the-air WLAN reception and jamming performance of our proposed system as well as, to the best of our knowledge, one of the first publications overall showcasing the real-world performance of a FD jamceiver, as is emphasized by Table I.

The remainder of this article is organized as follows. In Section II, we present the theoretical basis and signal models of our experimental system. Next, in Section III, we describe the measurement setup and used measurement parameters. Section IV presents the numerical results gained from the experiments while, in Section V, these are analyzed and discussed. Finally, Section VI concludes the paper.

II. SIGNAL MODEL AND THEORETICAL BASIS

The radio-frequency (RF) jamming signal $s_{\text{TX}}(t)$ transmitted by the considered full-duplex jamceiver (cf. Fig. 1 and 2) can be expressed as

$$s_{\text{TX}}(t) = \text{Re}\left\{e^{j\varphi_{\text{c}}(t)}\right\}, \tag{1}$$

for which the instantaneous phase is given by

$$\varphi_{\text{c}}(t) = 2\pi f_{\text{c}} t + \varphi(t) \quad \text{and} \quad \varphi(t) = 2\pi \int_0^t \mu(\theta) d\theta. \tag{2}$$

Here, f_c is the carrier frequency and $\varphi(t)$ is a continuous-phase signal per the frequency-modulating waveform $\mu(t)$ that

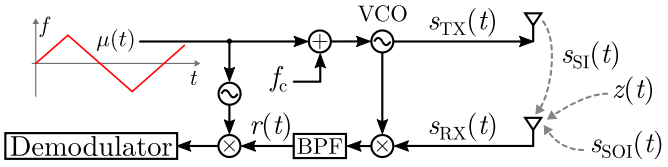


Fig. 2. Block diagram of the considered full-duplex constant-envelope transceiver with self-interference suppression by a passive highpass filter.

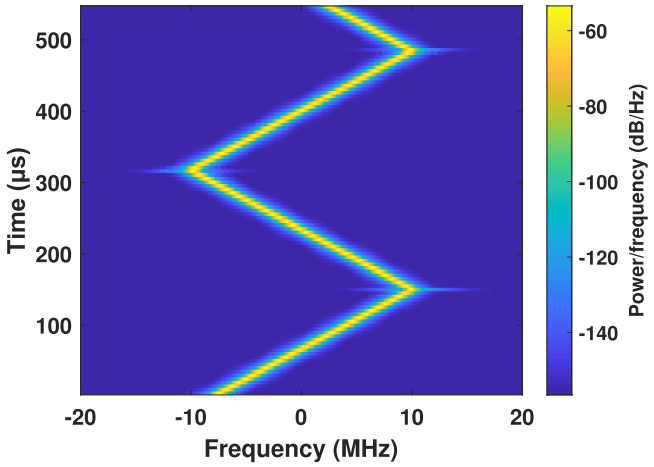


Fig. 3. Spectrogram of the transmit signal at baseband, illustrating a frequency sweeping waveform with 20 MHz bandwidth and 3 kHz sweep frequency.

represents the instantaneous frequency and could be quite freely chosen in theory.

In the experiments, we consider that $\mu(t)$ is a triangular waveform sweeping linearly and periodically between the values $\pm\frac{B_s}{2}$ with a frequency equal to f_s, although the system would be applicable in theory with any other signal too. The sweep period is $t_s = \frac{1}{f_s}$, including an upsweep and a downsweep, while the sweep rate is $\rho = 2B_s f_s$. Sweep rate ρ essentially determines the speed at which the waveform changes its instantaneous frequency. The instantaneous frequency of a triangular sweep can be expressed with

$$\mu(t) = \begin{cases} \left(f_c - \frac{B_s}{2}\right) + \rho(t-(m-1)t_s), \\ \qquad\qquad \text{if } t < t_s\left(\frac{1}{2}+(m-1)\right) \\ \left(f_c + \frac{B_s}{2}\right) - \rho(t-(2m-1)\frac{t_s}{2}), \\ \qquad\qquad \text{if } t \geq t_s\left(\frac{1}{2}+(m-1)\right) \end{cases} \tag{3}$$

where $m = 1, 2, \ldots$ is the sweep index. Fig. 3 illustrates with an example spectrogram[1] a baseband transmit waveform when $f_s = 3$ kHz and $B_s = 20$ MHz.

The signal captured by the jamceiver's receive antenna is the sum of the signal-of-interest $s_{SOI}(t)$, the self-interference $s_{SI}(t)$, and additive white Gaussian noise $z(t)$, i.e.,

$$s_{RX}(t) = s_{SOI}(t) + s_{SI}(t) + z(t). \tag{4}$$

This signal corresponds to the illustrative spectrogram seen in Fig. 4(a). The SOI component, which is a WLAN transmission in our case, can be expressed as

$$\begin{aligned} s_{SOI}(t) &= h_{SOI}(t) * s_{WLAN}(t) \\ &= \mathrm{Re}\left\{e^{j2\pi f_c t} s_{SOI}^{(bb)}(t)\right\}. \end{aligned} \tag{5}$$

In this equation, $h_{SOI}(t)$ is a linear channel and $s_{WLAN}(t)$ is the WLAN transmission which shares the same carrier f_c as the jamceiver. Hence, the received SOI can also be defined in terms of its complex baseband version $s_{SOI}^{(bb)}(t)$ and the carrier frequency, as shown in (5).

If we neglect practical transceiver non-idealities, the self-interference component in (4) can be also expressed using convolution as follows:

$$s_{SI}(t) = h_{SI}(t) * s_{TX}(t) = \left(\sum_{l=1}^{L} \beta_l \delta(t-\tau_l)\right) * s_{TX}(t), \tag{6}$$

where transmit signal $s_{TX}(t)$ was defined in (1), and $h_{SI}(t)$ is a linear channel that accounts for electromagnetic coupling between transmit and receive signal branches of the jamceiver. This coupling might occur within the device's internal circuits and/or between transmit and receive antennas due to nearby reflectors. Therefore, path delays τ_l are expected to be small. On the other hand, SI channel gains β_l might be quite large due to the proximity of transmit and receive signal branches, and a considerable amount of power is leaked from the former to the latter one.

The received RF signal is downconverted using the conjugate of the complex exponential waveform appearing in (1). Since the SI path delays τ_l are relatively small, the downmixing carrier has a frequency which is almost identical to the self-interference captured by the receive antenna, and the spectrum of $s_{SI}(t)$ will be concentrated around DC. Hence, it can be greatly reduced — if not totally suppressed — by a suitable highpass filter. Furthermore, unwanted high-frequency components inherent to downconversion have to be suppressed with a lowpass filter (LPF). In our analysis, we combine these two filters into an equivalent bandpass filter (BPF) as $\mathcal{F}_{BPF}\{\cdot\} = \mathcal{F}_{LPF}\{\mathcal{F}_{HPF}\{\cdot\}\}$. With this information, we can express the result of downconversion and filtering as

$$r(t) = \mathcal{F}_{BPF}\left\{e^{-j\varphi_c(t)} s_{RX}(t)\right\} \tag{7}$$

$$= \mathcal{F}_{BPF}\left\{e^{-j2\pi f_c t - j\varphi(t)} \mathrm{Re}\left[e^{j2\pi f_c t} s_{SOI}^{(bb)}(t)\right]\right\} \tag{8}$$

$$+\mathcal{F}_{BPF}\left\{\sum_{l=1}^{L} \beta_l e^{-j\varphi_c(t)} e^{j\varphi_c(t-\tau_l)}\right\} \tag{9}$$

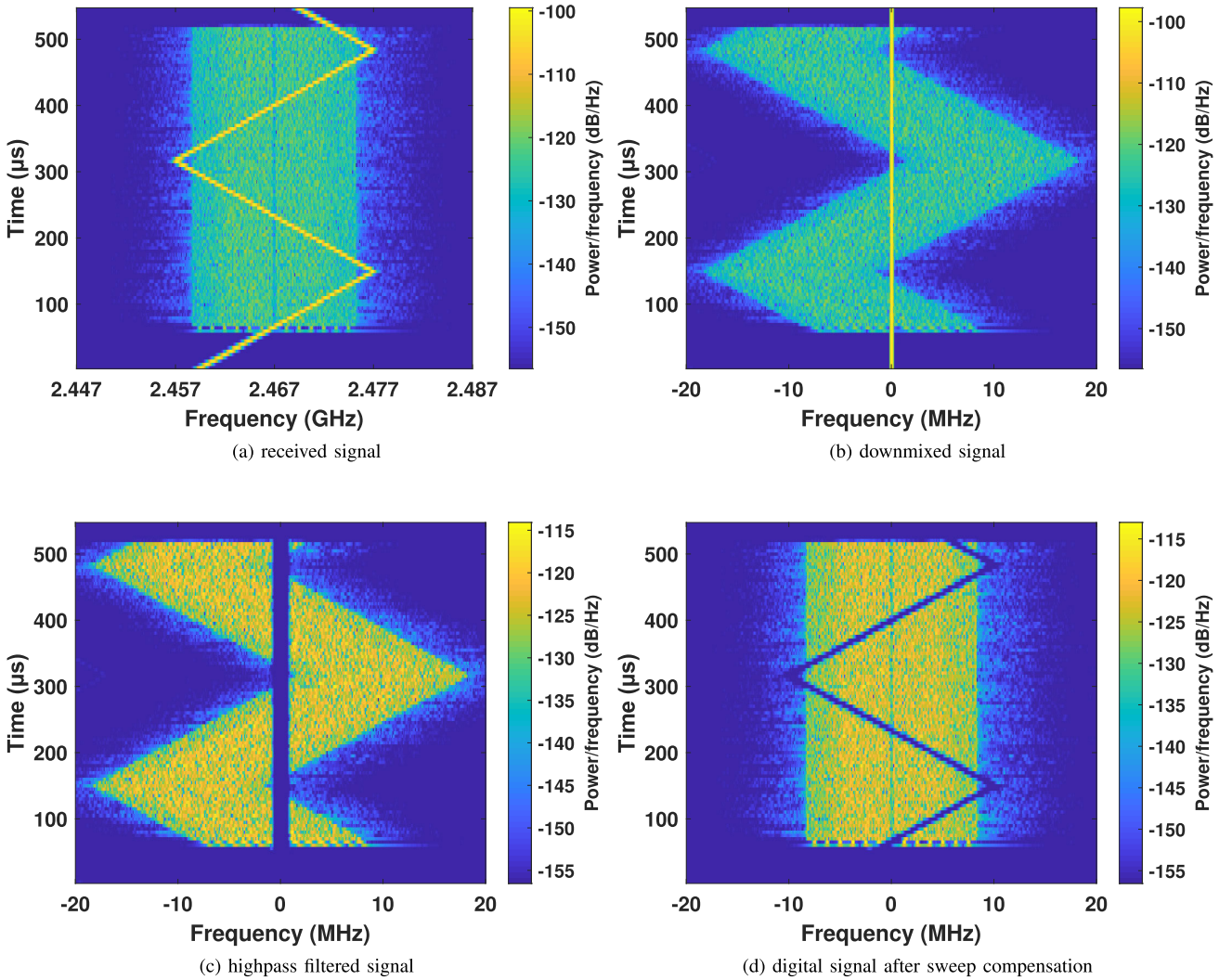
$$+\mathcal{F}_{BPF}\left\{z(t)\right\}, \tag{10}$$

where we expanded $s_{RX}(t)$ according to (4)–(6), and in (8) we also used the first part of (2). The situation after downmixing, but before filtering, can be seen in Fig. 4(b). The result after filtering out undesired frequency components is expressed as

$$r(t) = \tilde{s}_{SOI}^{(bb)}(t) e^{-j\varphi(t)} + \tilde{s}_{SI}(t) + \tilde{z}(t), \tag{11}$$

where $\tilde{s}_{SOI}^{(bb)}(t)$ indicates the filtered baseband version of the SOI, $\tilde{s}_{SI}(t)$ is the weak residual SI after filtering, and $\tilde{z}(t)$ is the filtered noise.

[1] https://www.mathworks.com/help/signal/ref/spectrogram.html



(a) received signal

(b) downmixed signal

(c) highpass filtered signal

(d) digital signal after sweep compensation

Fig. 4. Spectrograms illustrating the operating principle of the jamceiver, up to sweep compensation in digital signal processing. In the figures there is a single WLAN packet and a triangular sweeping waveform that has a 20 MHz sweep bandwidth and a sweep frequency of 3 kHz. The used highpass filter stopband width is 1 MHz.

The first term of (11) contains the desired signal, multiplied by a complex exponential which causes a time-varying spectral sweep according to $\varphi(t)$. In other words, the central frequency of the SOI's bandwidth will coincide with the instantaneous frequency dictated by the modulating function $\mu(t)$. Fig. 4(c) illustrates the spectrogram of (11) when the signal-of-interest is a standard WLAN signal with 20 MHz bandwidth, down-converted using a triangular FMCW signal with $f_\mathrm{s} = 3$ kHz and $B_\mathrm{s} = 20$ MHz. Note that the filter eliminates not only the SI, but also some energy from the signal-of-interest. Therefore, the stopband of the highpass filter has to be established from a trade-off between SI suppression and SOI degradation.[2]

We can determine the necessary electrical HPF stopband width to remove all the SI from channel echoes by using

$$B_\mathrm{HPF} \geq \frac{2d_\mathrm{L}\rho}{c} = \tau_\mathrm{L}\rho, \tag{12}$$

where d_L is the distance to the furthest significant SI reflector in the channel, c is the speed of light and τ_L is the delay of the signal from the furthest reflector. Please note that, in the following measurements, we use a digital HPF to study how the stopband width affects our own reception performance. However, in a real system, one would have an electronic filter with its stopband width predetermined to filter out all echoes with a meaningful power level from the deployment channel.

To compensate for the sweeping-spectrum effect and obtain estimate $\check{s}^{(\mathrm{bb})}_\mathrm{SOI}(t)$ of the baseband SOI, we multiply (11) with a complex exponential as follows:

$$\begin{aligned}\check{s}^{(\mathrm{bb})}_\mathrm{SOI}(t) &= e^{j\varphi(t)} r(t) \\ &= \tilde{s}^{(\mathrm{bb})}_\mathrm{SOI}(t) + e^{j\varphi(t)}\tilde{s}_\mathrm{SI}(t) + e^{j\varphi(t)}\tilde{z}(t).\end{aligned} \tag{13}$$

The first term of the right-hand side in (13) contains the compensated baseband SOI, with distortions caused by the SI suppression HPF. The second term represents the residual self-interference, which is now sweeping in spectrum according to $\varphi(t)$. The last term contains the effective noise. The result of compensating the received signals can be seen in Fig. 4(d). Note that the WLAN signal is now correctly centered around the zero frequency, and the attenuating effect of the high-pass filter is sweeping through the spectrum. The sweeping

[2]In Fig. 4, the bandwidth of this filter (1 MHz) is intentionally exaggerated to visualize its negative effects on the SOI although feasible values are demonstrated to be below 125 kHz in the following experimental results.

TABLE II
LIST OF HARDWARE

Notation/name	Brand	Model
VST	National Instruments	PXIe-5840
I/Q downmixer	Analog Devices	ADL5382
PA	Mini-Circuits	ZHL-4240
VA	Mini-Circuits	RCDAT-6000-30/60
TX/RX antenna	Laird Connectivity	WTS2333C-FRSMM
Oscilloscope	Rohde & Schwarz	RTO2064
Laptop	Lenovo	Thinkpad T470s
SDR	National Instruments	USRP-2945R
Eavesdropper	National Instruments	PXIe-5645R
Eave. RX antenna	Siretta	DELTA 6C

attenuating effect will cause unavoidable degradation of the SOI. However, the reduction in performance can be tolerable with proper parameter selection.

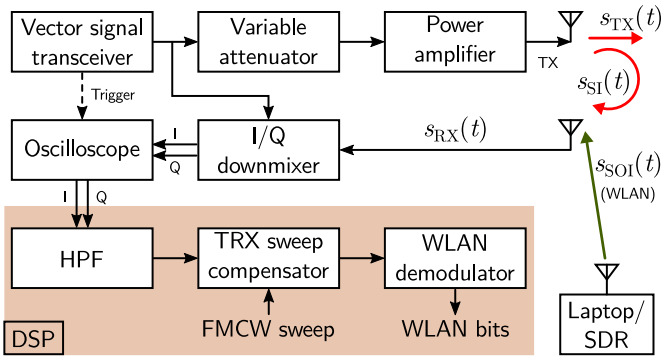
Although in this paper the transmit signal is considered to be a triangular pattern FMCW-signal, other possible waveforms could be a single stationary tone or a sawtooth pattern FMCW-signal. With a tone signal, the SI cancelation would be trivial and the HPF could be extremely narrow, however it would only interfere with a single subcarrier from the considered WLAN SOI. With a sawtooth pattern FMCW-signal, the jamming performance would be quite same as with a triangular pattern, however the rapid frequency shifts at the end of each sweep would cause large frequency shifts away from the DC, which could reduce the SI attenuation. With more complicated transmit waveforms and non-constant envelope, such as an OFDM-signal, the downmixing could produce extreme distortions and the SI suppression technique would be mostly useless.

III. EXPERIMENTAL SETUP

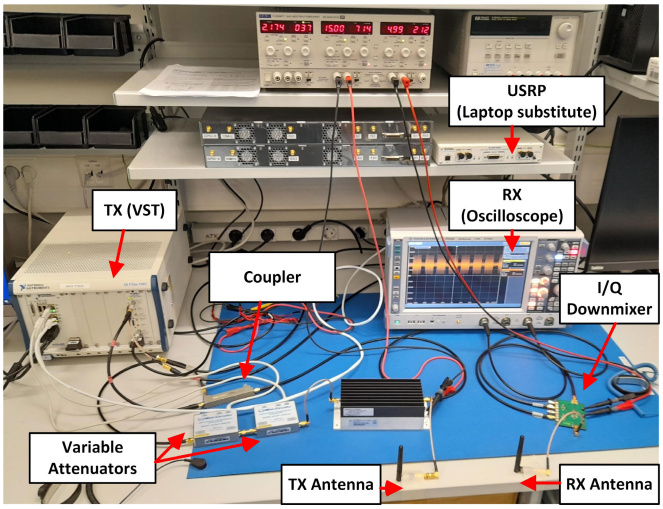
We used commercial and off-the-shelf devices to implement the proposed transceiver and test it under diverse system parameter combinations in a laboratory and an outdoors scenario. In this section, we describe the hardware implementation, the structure of waveforms used for our experiments, the signal processing carried out on the received signals, and the parameters we varied in the experiments.

A. Hardware Implementation

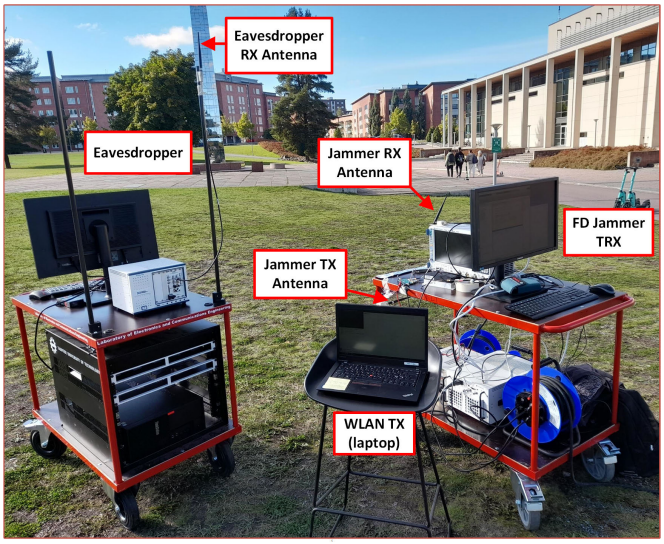
The block diagram of the measurement setup can be seen in Fig. 5(a), while Fig. 5(b) shows a photograph of the indoor implementation. The list of hardware used is presented in Table II. A vector signal transceiver (VST) provides the continuous-envelope FMCW signal used for jamming and downconversion. This signal is fed to the I/Q downmixer's local oscillator port, as well as to one of two computer-controlled variable attenuators (VA) in the transmit chain. The attenuated FMCW signal is fed into a power amplifier (PA). By acclimating either of the two attenuators and PA, the effective transmitted power is adjusted to the desired values. The system uses two separate antennas for transmission and reception, each with 2.3 dB gain at the 2.4 GHz ISM band. The isolation measured between the two antennas is only 43 dB. The RX signal, containing the SI and the WLAN signal, is downmixed using the transmitted FMCW waveform, and is separated into its in-phase (I) and quadrature (Q) branches. Next, an oscilloscope samples the received signal, which is recorded to perform offline digital signal processing (DSP). The oscilloscope starts recording when it receives a trigger signal sent by the VST. This way, we observe roughly the same delay between all signals; however, there is



(a) block diagram of the setup

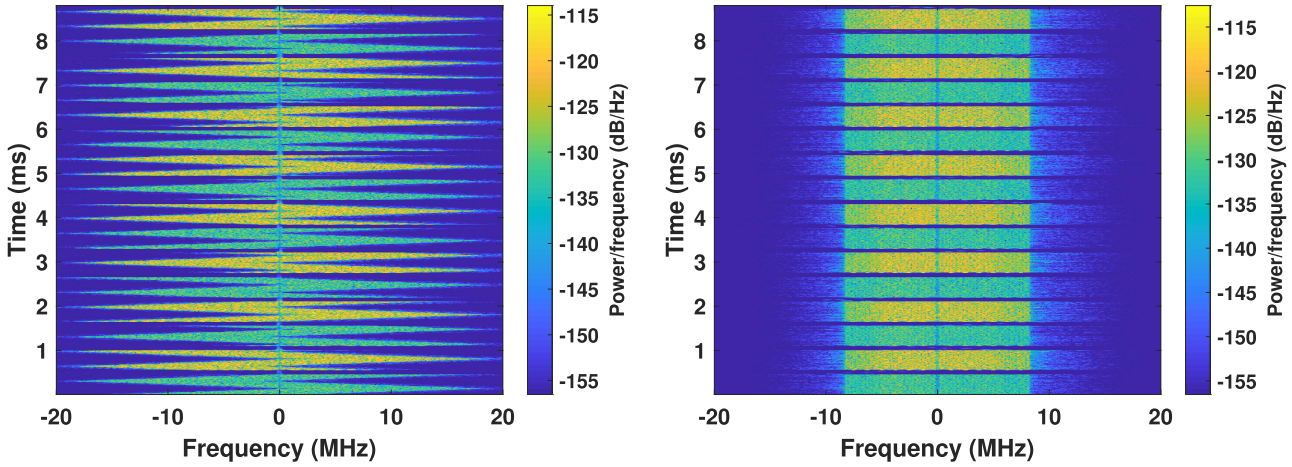


(b) photo of the indoor setup



(c) photo of the outdoor setup

Fig. 5. Implemented experimental setup for simultaneous jamming transmission and WLAN reception using the full-duplex constant-envelope transceiver and self-interference cancelation by highpass filtering. The laptop acting as the SOI transmitter is shown only in subfigure (c).



(a) before sweep compensation (b) after sweep compensation

Fig. 6. Spectrograms of a WLAN burst before and after sweep compensation. The alternating packet power level caused by the spatial redundancy is clearly visible. Sweeping bandwidth and frequency are 20 MHz and 3 kHz, respectively. Highpass filter stopband width is 200 kHz. Weak residual self-interference is visible.

still some fluctuation to the exact delay between recordings and this needs to be estimated and compensated for.

The measurements were conducted in an indoors laboratory environment, where the SOI was transmitted by a laptop with a Linux operating system and a software which allows modulating arbitrary data on the WLAN signals. We describe the characteristics of the SOI more in detail in the next subsection. However, due to some limitations of this approach, which will be discussed more in depth in section III-B, for some measurements the SOI was transmitted from a software-defined radio (SDR) equipment instead. To achieve this, we recorded all the desired variations of the laptop's transmitted SOI waveforms in our university's electromagnetically shielded chamber. These recorded waveforms were then re-sent by the SDR with a transmit power such that the received SOI power was matched with the laptop TX power level.

In addition to the aforementioned laboratory measurements, we also used our setup to conduct outdoors measurement which allowed us to evaluate the jamming performance of this realistic proof-of-concept. In the case study, we did not consider encryption or other data protection schemes, but we simply observed how many bit errors were caused by the jammer to an eavesdropper attempting to demodulate the WLAN data packets sent by the laptop. Fig. 4(a) also shows the situation at the eavesdropper. Without interference suppression, the eavesdropper has to deal with the strong sweeping signal, which causes problems in packet detection, channel equalisation and symbol demodulation. The measurement was conducted in the front yard of Tampere University's Hervanta campus, and the devices used in the measurements can be seen in Fig. 5(c), while an aerial photo is available in Fig. 11 along with experimental results that are discussed in section V. The FD jammer–receiver used the same setup and components as the one used in the laboratory measurements, and the laptop shown is the same as in the measurements described previously. The eavesdropper was constituted by a VST configured for receiving signals from the ISM band through a suitable antenna.

B. WLAN Signal-of-Interest

The laptop (Lenovo Thinkpad T470s) we used in the measurements came equipped with a WiFi chip (Intel 8265NGW), which is compliant with the IEEE 802.11ac standard.[3] We used a packet manipulation program called Scapy[4] to force the laptop to transmit nothing but a fixed bit sequence on an endless loop. In the program, it was possible to set the data payload of the transmission, as well as the modulation and coding scheme (MCS) and the wait period between transmit bursts. A single data transmission, or burst, contained 16 repetitions of the same packet, with their power levels alternating between two values between concurrent packets. A full burst before and after sweep compensation can be seen in Fig. 6(a) and 6(b), respectively, which also illustrate how weak residual SI looks before and after said compensation. The changes in power level between the concurrent packets were caused by spatial redundancy built into the laptop transmitter, where half of the repetitions were transmitted towards the screen of the laptop and the other half was transmitted from behind it. This was verified by changing the azimuth rotation of the laptop, which caused the relative power levels of the concurrent packets to change.

According to the laptop's operating system, the packets were transmitted at a fixed power level of 0 dBm from the device, but there was no way to verify this. The WLAN chip built into the computer did not allow us to change the power level. Given this circumstance, the laptop was placed in such a way that the strongest signal power at the receiver antenna was around 30 dB higher than the RX noise floor, with a fluctuation of a few decibels between packets. Certainly, the power level of half of the packets was significantly lower than that due to spatial redundancy, and thus those packets were discarded. Every measurement encompassed roughly 50–60 non-discarded packets, each containing 2200 payload bits.

The spacing between concurrent bursts was set to 0.1 ms, measured from the start of a single 16-packet burst to the

[3]https://standards.ieee.org/ieee/802.11ac/4473/
[4]https://scapy.net/

beginning of the subsequent one. With higher modulation orders, the downtime between bursts increased, but the number of bursts between different modulation orders was kept very uniform. Likewise, the number of symbols within a packet changed according to the modulation order, although the actual demodulated bit sequence remained the same. During modulation, the WLAN chip performed redundancy addition, interleaving and scrambling to the bit sequence according to the WLAN standard.

Unfortunately, the chip also added a presumably random bit sequence to the end of the data payload, which caused the unmodulated symbols to change between packets, even within a single burst. This makes SER measurements from laptop transmissions quite impossible, since the attenuation caused by the SI suppression filter makes signal reconstruction after bit demodulation unreliable. Even if there is some logic to the sequence of the added padding bits, during our measurements we did not spot even just two packets with exactly the same symbols. This situation was exacerbated by the fact that the TRX structure caused some inevitable symbol errors. The attenuating effect can be seen in Fig. 7, where some of the symbols have been attenuated close to zero amplitude. The figure also demonstrates how the attenuation affects the channel estimation, causing noise-like spreading of some of the symbols as well as light phase rotation around the origin. An additional problem caused by the chip was that it stopped transmission when it detected that the designated frequency band was occupied, which is not surprising considering the multiple access scheme intrinsic to WLAN. This meant that we also had to use the SDR for all measurements where the jamming bandwidth was coincident with that of the WLAN signal, as the laptop refused to transmit anything when any reasonable jamming TX power was used over the operating channel.

To facilitate SER measurements, we recorded single SOI signal realizations from the laptop in our university's electromagnetically shielded chamber, for all the used modulation orders. This allowed us to transmit these fixed WLAN packet sequences with an SDR, which made it possible for us to compare the unmodulated symbols afterwards. The SDR transmit power was fixed such that the received SOI power was matched with the laptop's power level.

C. Digital Signal Processing

Due to the operating principle of our TRX structure, the downmixed WLAN signal sweeps through a relatively wide band. Thus, it was necessary to have a very high sampling frequency in order to adequately capture the SOI. Conversely, this meant that the recording lengths had to be kept relatively short, with a length of 100 ms. We recorded two repetitions of the experiments for every system parameter combination. However, the total amount of received bits remained rather low, only around 150e3, which is discernible in the results presented in the next section. Despite this, the amount of data recorded thus far is already quite massive — 1.9 TB — which also translates to excessively long processing times.

The digital signal processing flow can be seen in Fig. 8. To begin, the SI is removed from the recorded waveforms using a digital HPF. This way, the stopband width of the filter can be chosen arbitrarily, which allows us to see how widening the HPF response affects SI suppression, as well as deteriorates the WLAN signal. In a real jamceiver setup utilizing our structure, the HPF would be a discrete electrical component limiting the power of the SI fed into the analog-to-digital converter, and tailored to the implemented setup

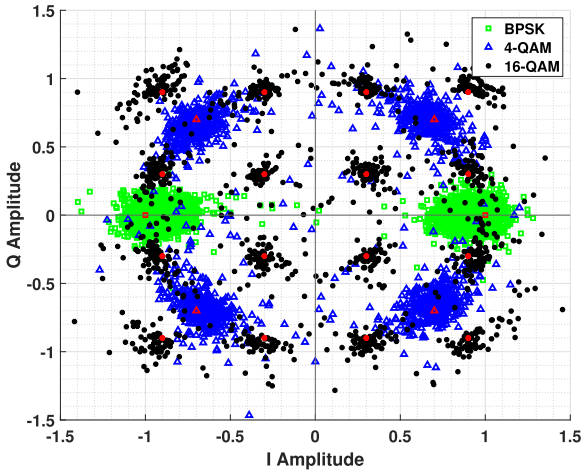


Fig. 7. The effect that the TRX structure has on symbols from a single packet after channel equalization. The HPF stopband width is 80 kHz while the sweep bandwidth and frequency are 80 MHz and 3 kHz, respectively. The scatter plot includes BPSK (green squares), 4-QAM (blue triangles) and 16-QAM (black dots) modulations. The transmitted symbol locations are marked with red color. The HPF causes attenuation to the affected symbols, as well as distorts channel and phase correction.

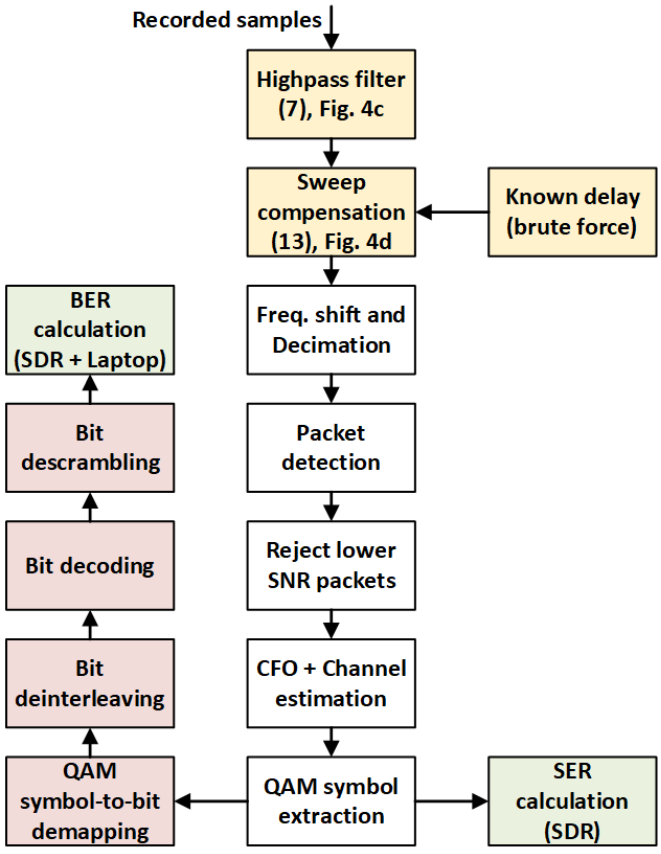


Fig. 8. Digital signal processing flowchart. The yellow boxes show how the processing differs from standard WLAN demodulation. The red boxes denote the operations where Matlab functions provided in Table V were utilized. The green boxes signify the positions where result data is extracted.

according to (12). The realized reception powers were chosen in such a way to not saturate the high-resolution ADC in the oscilloscope, and to use its full dynamic range. The digital highpass filters were of the IIR type, due to the fact that the relative stopband width to total measurement bandwidth ratio was very small, although they introduced a frequency-varying group delay. This effect is non-desirable when there is a SOI sweeping through the spectrum, however the WLAN processing done afterwards was seemingly able to cope with it and did not produce appreciable errors. The processing time when testing FIR filters resulted beyond excessive.

After filtering, the spectrum of the received signal is still sweeping through the frequencies according to the FMCW signal used for downmixing. To allow for WLAN demodulation, this sweeping effect needs to be compensated for. If the signal delay in the RX line is known, the sweeping effect can be easily compensated with a multiplication by a conveniently delayed version of the transmitted waveform as shown in (13). In our experiments, this synchronization was done by a brute force method. Before processing all the recorded signals with different HPF bandwidths, we tested various delays with sub-sample level accuracy to obtain an optimal delay for every measurement determined by the bit error rate (BER). In our previous paper [34], we showed that it is possible to reliably find an accurate estimate of the delay by using an analytical solution. Unfortunately, with the higher sweep frequencies measured for this journal, the ambiguity bounds of the function prevents us from using that method, and thus a brute force method was used for all of the measurements.

During testing it was found that the SI and the attenuation caused by the HPF makes it unreliable to accurately synchronize the known WLAN signal transmitted by the SDR to the received signal captured by the oscilloscope. In-order to contrast the received symbols with the known ones, the symbol sequence of the received packets was compared to the known sequences to find the most probable match, after which symbol errors were calculated. In a high SI situation, this matching could fail and cause additional symbol errors.

To demodulate the WLAN packets, we first identified the packet start positions by correlating with the known WLAN preamble. We dropped half of the packets which had a significantly lower power level due to spatial redundancy. After that, we used the short training field (STF) and long training field (LTF) portions of the packet to compensate for coarse and fine carrier frequency offset respectively. The initial channel estimate was likewise done from the LTF. We also found that when the SI suppression filter attenuated the LTF portion of a recorded waveform, the initial channel estimate was incorrect, which in turn caused severe distortion to all of the symbols in the packet. A zero-forcing equalizer was used to compensate for the channel effects in the symbols.

Next, the signaling field of the packet was decoded to find out the packet length, modulation, and coding rate information, which are necessary for decoding the data bits. The deinterleaving was done manually according to the WLAN standard, while the decoding was done by using the `wlanBCCDecode` function from the WLAN toolbox by Matlab. Afterwards, the rest of the OFDM symbols were extracted, and the pilot subcarriers within them were used to compensate for phase rotations within their respective OFDM symbols.

After all of the channel-equalized and phase-corrected IQ-amplitudes from each subcarrier within their own respective OFDM symbols have been extracted, we used the Matlab functions provided in Table V, in the order shown in Fig. 8, to demodulate these IQ-amplitudes to their most likely demodulated data bit sequence after error-control coding. This bit sequence was then compared to the known bits fed to the WLAN chip in the laptop, to determine bit errors. The WLAN chip of the laptop added some random junk bits to the end of the WLAN packets, which meant that the data symbols of every packet were different, as was mentioned previously.

The bit error rates (BER) and symbol error rates (SER) were calculated by counting all of the bit errors and symbol errors, and comparing them to the total number of bits and symbols, respectively. This was done from all of the non-dropped packets from the entire measurement set. Naturally, due to the difficulties with symbol error detection mentioned previously, SER was only calculated from the measurements where the SDR was used as the WLAN transmitter. In all of the measurements, the ambient SINR at the laboratory was high enough that the SER and BER was 0% when the TX was turned off and no digital filtering was performed.

Regarding the processing load increase introduced by the proposed system, it should be noted that the only additional processing compared to traditional WLAN processing comes from the sweep compensation. Sweep compensation is effectively a multiplication operation between two signals, so this introduces one complex multiplication per measured sample, which is very easy for firmware/hardware. For reference, with the first author's generic off-the-shelf laptop, this operation took 85 ms for 20e6 samples. At 200 MHz sampling frequency used in the measurements, this meant a recording length of 100 ms, which included a total of 64 packets. A real-life system with a sampling frequency just high enough for the selected jamming bandwidth, using dedicated complex multiplication hardware and a shorter WLAN packet or burst length recording, should achieve a negligible increase in processing time. We are confident this should allow for online processing.

However, in the measurement campaign, we used a digital HPF for SI suppression to emulate and test a wide selection of stopband widths. Additionally, because the delay between downmixer path and the sampling oscilloscope was not constant, we had to find the delay by brute force. In a real custom-made end product, we would know the delay exactly and have an electronic HPF, which would remove these problems. Due to these issues, we were effectively forced to process the results offline.

D. Measurement Parameters

Next, let us look at the parameters of the transmitted sweeping signal as well as the received WLAN packets that were used in the measurement. From Table III, we can see that the tested sweep frequencies were in the range of 3–250 kHz, with an increased resolution at the lower frequencies. These values were chosen due to the knowledge that higher sweep frequencies make the interference removal

TABLE III
JAMMING PARAMETERS USED IN THE MEASUREMENTS

Sweep frequencies	Sweep bandwidths	TX powers at antenna port
3, 4, 5, 10, 20, 30, 40, 60, 80, 100, 125, 250 kHz	20 and 80 MHz	-23, -20, -17, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19 dBm

TABLE IV
WLAN PARAMETERS USED IN THE MEASUREMENTS

Modulation	Bandwidth	Center frequency	Payload bits
BPSK (MCS: 0), 4-QAM (MCS: 2), 16-QAM (MCS: 3)	20 MHz	2.467 GHz (channel 12)	2200

TABLE V
MATLAB TOOLBOX FUNCTIONS USED

Function used	Purpose
`wlanConstellationDemap`	Demap the received QAM symbols
`wlanBCCDeinterleave`	Deinterleave the raw bit sequence
`wlanBCCDecode`	Remove redundancy coding
`wlanScramble`	Descramble the bit sequence

operation more detrimental to reception, and therefore lower sweep frequencies generally provide better performance. For the sweep bandwidths we considered two cases: 20 MHz, where only the WLAN signal band is jammed; and 80 MHz, where the entire ISM band is jammed. The 20 MHz bandwidth is more relevant for the main considered use case of this work, where the jammer wants to prevent eavesdroppers from receiving the WLAN signal meant for itself, while the 80 MHz case would be relevant for denying 2.4 GHz ISM band usage in a certain area. The transmit powers, which were measured at the transmit antenna, were chosen so that at the high end we would be close to the regulatory maximum TX power of 23 dBm of ISM band devices, and the lower end caused barely any received SI. The rest of the powers were chosen with a 3 dB resolution between these border values.

WLAN parameters had less variations between measurements, as can be seen from Table IV. The only change between the measurements was the used modulation order, with the three options being BPSK, 4-QAM and 16-QAM. The coding rates of these were 1/2, 3/4 and 1/2, respectively. The modulation coding scheme (MCS) index of these options were 0, 2 and 3, respectively. The 3/4 coding rate for 4-QAM was selected in order to see how the coding rate affects the error-corrected SER to BER conversion. Each of these options had a bandwidth of 20 MHz, and they were transmitted at WLAN channel 12, which was at the center frequency of 2.467 GHz.

As mentioned previously, in the laboratory measurements the relative distances between the TRX antennas and the WLAN transmitting laptop was fixed. All of the different parameter combinations were recorded with this configuration.

For the open-air jamming measurements, the transmitted jamming waveform had a sweeping frequency of 10 kHz and a sweeping bandwidth of 20 MHz, centered on top of the WLAN packets which were approximately 16–18 MHz wide as standardized. The effective isometric radiated power from the jamming TRX was 10 dBm, to comply with local laws for transmit power levels. The laptop had a transmit power of 0 dBm which could not be changed, as explained before. The measurement setup can be seen in Fig. 5(c). The isolation between the FD jammer TX and RX antennas was measured to be at 53 dB. At 10 dBm transmit power, the received self-interference power was -43 dBm.

The WLAN packets transmitted by the laptop were modulated with 16-QAM. The ambient SINR situation at the measurement site was such that when the jamming was turned off, the eavesdropper had 0% BER at all measurement points. During testing, we noticed that with lower modulation alphabets, i.e., BPSK and 4-QAM/4-QPSK, the sweeping waveform was less effective at causing erroneous symbol detections. However, with a higher modulation order the jamming efficiency improved considerably, causing more consistently detection errors. Unfortunately, this requirement of using a higher modulation order limited the effective range of the desired communication between the UE and the jamming FD TRX. However, that is a limitation to the setup caused by the robustness of the WLAN protocol.

IV. EXPERIMENTAL RESULTS

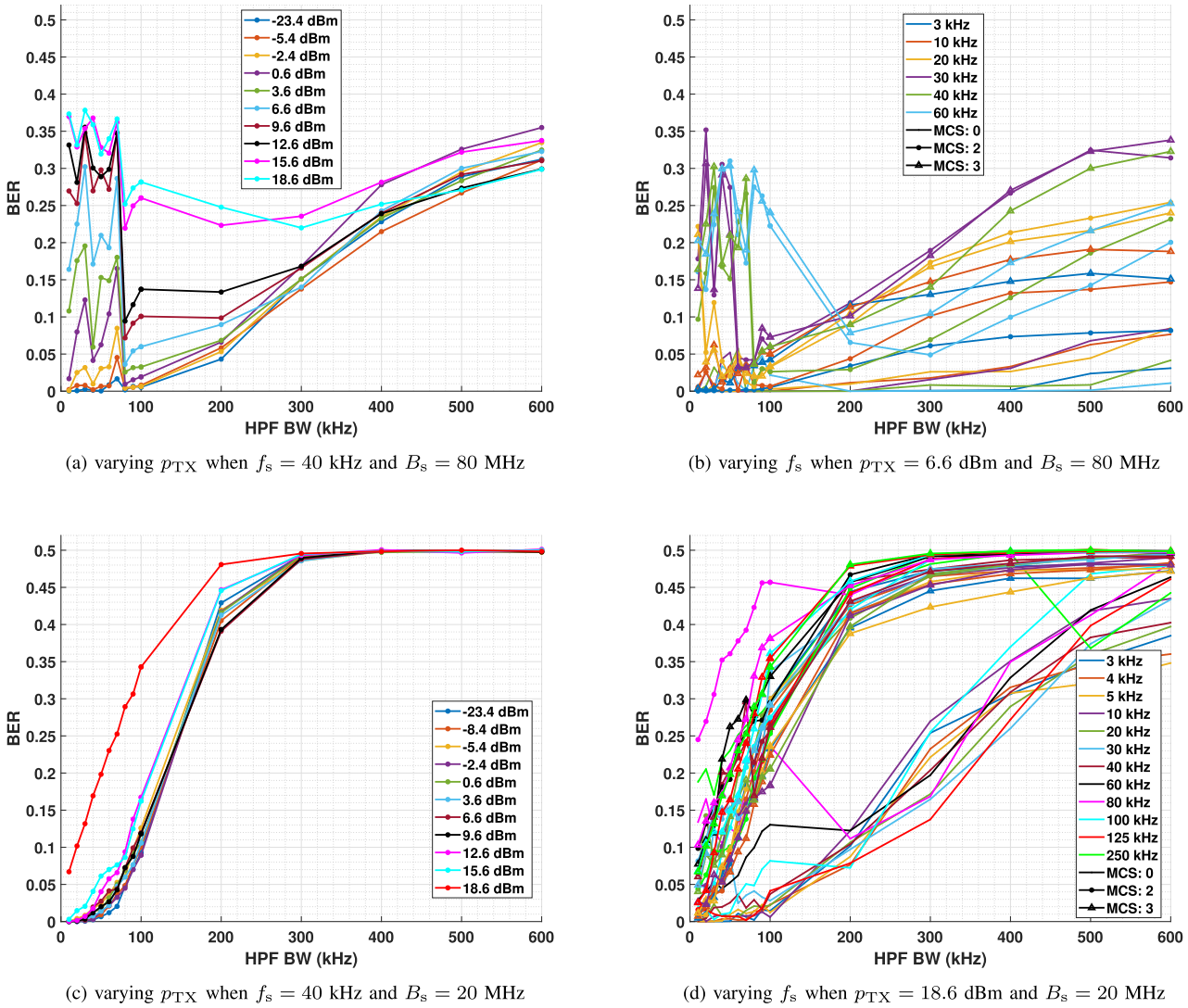
We tested performance of the full-duplex jamceiver by evaluating the bit- and symbol error rates in our setup with parameters described previously. Fig. 9 and 10 show the BER results and the accompanying SER results.

Both Fig. 9(a) and 9(b) were obtained with the laptop transmitting the WLAN SOI with 16-QAM modulation. The FMCW sweep bandwidth in both cases was set equal to 80 MHz. In Fig. 9(a), the sweep frequency was set to $f_\mathrm{s} = 40$ kHz, whereas transmit power was increased from -23.4 to 18.6 dBm. Conversely, Fig. 9(b) shows results for a fixed transmit power $p_\mathrm{TX} = 6.6$ dBm, while the sweep frequency was varied between 3 and 60 kHz, and modulation orders set to MCS $= \{0, 2, 3\}$. Fig. 9(c) and 9(d) are analogous to the two previous ones, except that the FMCW sweep bandwidth was set to $B_\mathrm{s} = 20$ MHz in these experiments, and the SOI was transmitted by the SDR. Because of this smaller bandwidth, in Fig. 9(d) we can show results for sweep frequencies larger than in Fig. 9(b), reaching up to $f_\mathrm{s} = 250$ kHz.

In Fig. 9(a) we can see how the increase in p_TX necessitates the use of a HPF in order to limit severe deterioration to BER. The sweep frequency has a direct correlation with the required width of the HPF, with higher sweep frequencies making it impossible to achieve low BER with higher p_TX.

Fig. 9(b) shows how different sweep frequencies behave at $p_\mathrm{TX} = 6.6$ dBm. Here we can clearly see that with lower sweep frequencies we can achieve relatively good BER with rather narrow HPFs, while higher sweep frequencies require wider HPFs to achieve rather poor minimum BER values.

Similar figures were drawn for a case where the sweeping bandwidth is lowered to 20 MHz and centered over the spectrum occupied by the WLAN signal. These results are obtained with the SDR acting as the transmitter. Comparing Fig. 9(a) and 9(c), we can see that lowering the sweep bandwidth to 20 MHz improves the situation significantly over the 80 MHz case, with even the highest TX power achieving



(a) varying p_{TX} when $f_{\mathrm{s}} = 40$ kHz and $B_{\mathrm{s}} = 80$ MHz

(b) varying f_{s} when $p_{\mathrm{TX}} = 6.6$ dBm and $B_{\mathrm{s}} = 80$ MHz

(c) varying p_{TX} when $f_{\mathrm{s}} = 40$ kHz and $B_{\mathrm{s}} = 20$ MHz

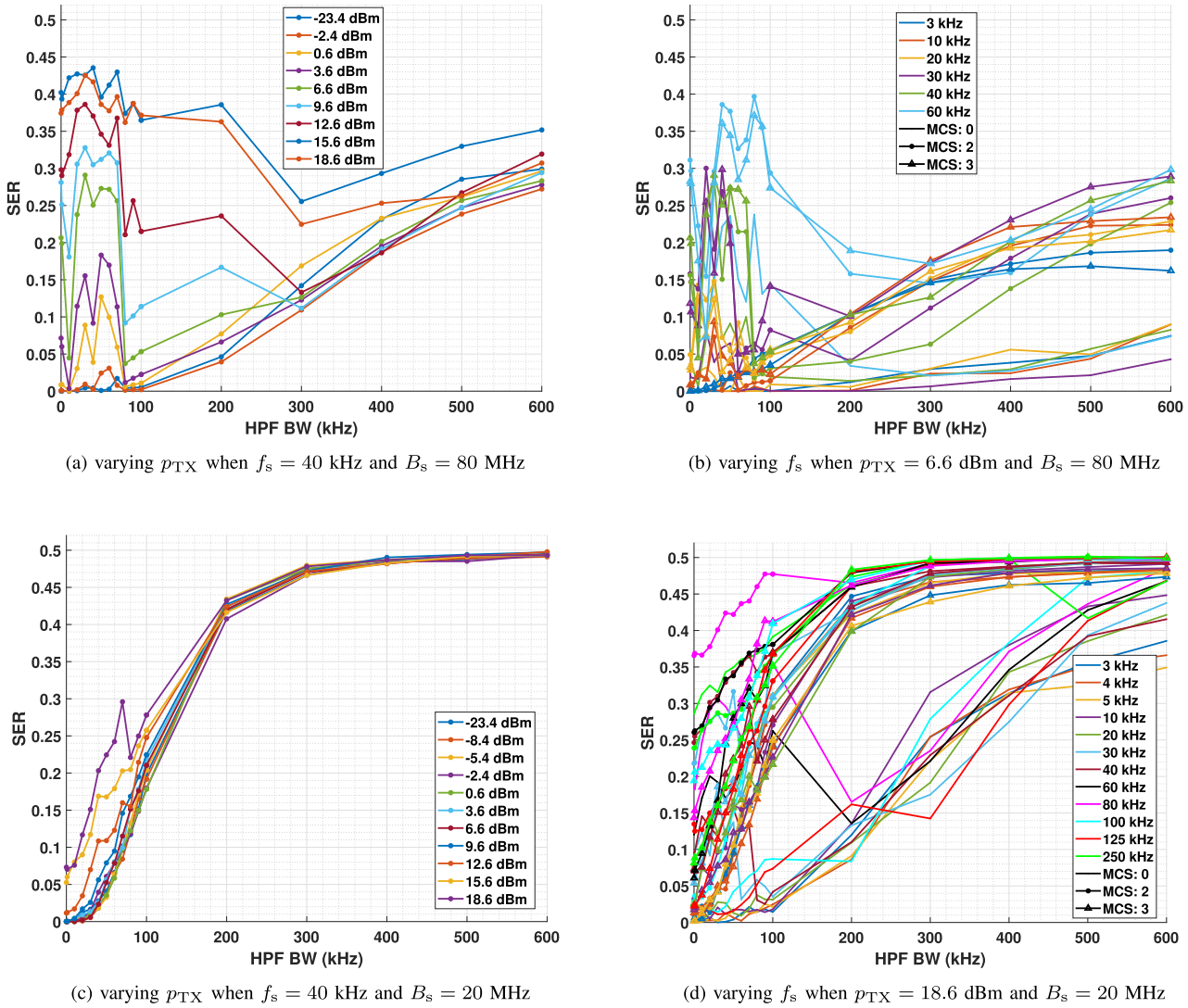
(d) varying f_{s} when $p_{\mathrm{TX}} = 18.6$ dBm and $B_{\mathrm{s}} = 20$ MHz

Fig. 9. Effect of the HPF bandwidth on the jamceiver's bit-error rate for different system configurations, measured in the laboratory. The results in subfigures (a) and (b) are obtained with laptop measurements, while subfigures (c) and (d) show results from SDR measurements. Subfigures (a) and (c) are obtained with MCS: 3. These results include error control coding inherent to WLAN standard.

a BER below 10%, and lower powers achieving very good BER at low HPF stopband widths.

The SER results for the 80 and 20 MHz sweep frequency measurements can be seen in Fig. 10, with the parameters and orders replicating those of Fig. 9. Please note that all of these results were obtained with the SDR as the transmitter instead of the laptop. The SER information was obtained this way because of the unpredictable nature of the symbols from the laptop as was detailed previously in section III-B. Regardless, the SER values obtained from the measurements seem to follow closely the laptop results shown earlier, with the intuitive increase in errors compared to BER results without error control mechanisms inherent in the WLAN standard.

Next we will show the results from the outdoors jamming measurement. The measurement environment and a rough outline of the results can be seen in Fig. 11. The laptop and the jammer TRX were spaced 26 m apart, which allowed a BER of less than 5% for the FD jamceiver's reception. Since the 2.4 GHz ISM band was extremely noisy during the measurement day, the values for FD jamceiver's and eavesdropper's BER was taken from the best packet of the complete measurement duration of 100 ms. The average BER of a single measurement fluctuated widely, and was usually in the range of 35% to 50%. The eavesdropper performance was recorded at various distances and directions from the jammer, with the goal of finding the cutoff points where the eavesdropper was unable to obtain packets and where the reception started to work. The eavesdropper's reception performance did not change linearly when moving away from the jammer and towards the WLAN transmitter. Instead, the eavesdropper experienced very high BER—larger than 20%—until a certain cutoff distance, after which it improved almost immediately to a very low BER range, around 0%–5%. These cutoff points have been roughly marked on the previous figure, and a connecting line has been drawn based on them, as well as an extrapolated dotted line where the authors presume the cutoff point would be around the measurement environment. These show rough areas where the jamming prevents efficient eavesdropping, and where it might not be strong enough to ensure secure WLAN data transfer. These estimated areas are



(a) varying p_{TX} when $f_{\mathrm{s}} = 40$ kHz and $B_{\mathrm{s}} = 80$ MHz

(b) varying f_{s} when $p_{\mathrm{TX}} = 6.6$ dBm and $B_{\mathrm{s}} = 80$ MHz

(c) varying p_{TX} when $f_{\mathrm{s}} = 40$ kHz and $B_{\mathrm{s}} = 20$ MHz

(d) varying f_{s} when $p_{\mathrm{TX}} = 18.6$ dBm and $B_{\mathrm{s}} = 20$ MHz

Fig. 10. Effect of the HPF bandwidth on the jamceiver's symbol-error rate for different system configurations, measured in the laboratory. The results in all the subfigures are obtained with SDR measurements. Subfigures (a) and (c) are obtained with MCS: 3.

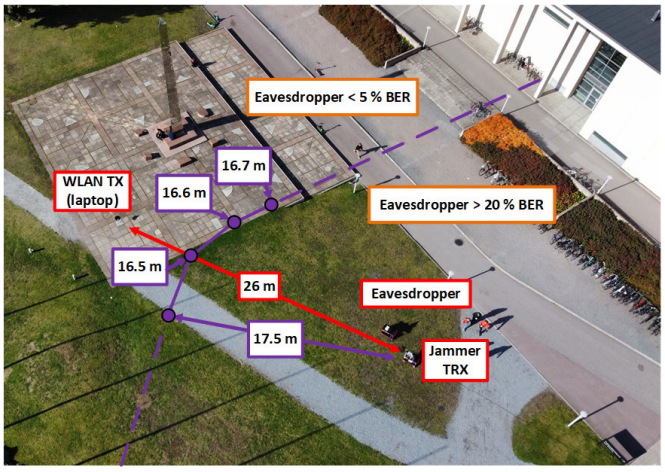


Fig. 11. Aerial photograph of the outdoor measurement setup, showing locations of the jammer, eavesdropper, and SOI transmitter (laptop). Regions with different BER performances of the eavesdropper are also shown.

conservative in the sense that, in reality, the effective jamming distance would most probably increase as the eavesdropper moves further away from the laptop. Additionally, when the eavesdropper was only a few meters from the jammer, its packet detection failed and it was not able to decode any information from the recorded packets. This area is not shown in the photo, as it was so close to the jammer that this complete denial of reception would not be relevant in real-life applications.

V. Analysis and Discussion

Overall, the results shown in section IV seem quite intuitive. The higher sweep bandwidth measurements have a harder time removing the SI stemming from all of the channel echoes without a loss to the reception performance, which is due to the attenuation of an ever widening HPF stopband width. In the situation where the whole 80 MHz of the ISM band needs to be jammed, the system designers need to be very careful in choosing the sweep frequency and the corresponding HPF stopband width in such a manner that the reception performance of the SOI is within acceptable range, while also maintaining the desired jamming performance. Alternatively,

if possible, the SOI could be designed to be such that the interference caused by this TRX structure is minimized. Our setup might be especially interesting in a spectral monitoring use-scenario, since the partial loss of signals we might not even try to decode might be a preferable trade-off compared to complex analog components and digital processing necessary in other FD-capable jammers. Additionally, the operating principle is basically the same as for an FMCW radar, and we have shown previously that it is possible to modulate data to the waveform [36], essentially allowing for joint communication and sensing.

With a 20 MHz sweep bandwidth, the design requirements are significantly relaxed. Even with a very high sweep frequency and a high transmit power, the results show that it is still possible to have acceptable BER, while with a lower—and perhaps more reasonable—sweep frequency the performance achieves very good values, i.e. below 1%. In this manner, the presented TRX structure could indeed be considered as a cost-effective alternative for the physical-layer security use scenario, preventing eavesdroppers from listening in on the WLAN signal without excessive loss to the reception performance. Moreover, this way the interference to the other users of the channel is minimized, since they cannot use the band occupied by the WLAN transmitter anyway. As a side note, sending intentional interference in a civilian context for any reason is currently illegal in many countries.

As can be deduced from the results in the preceding section, each sweep frequency has an optimal B_{HPF} that achieves the highest BER. A further processed version of the result data that shows more concisely how the sweep parameters, transmit power, WLAN MCS index and the HPF bandwidth interact with each other, can be seen in Fig. 12. These show the HPF stopband widths that achieve the minimum BER and SER at different TX powers and sweep frequencies for the 80 and 20 MHz wide jamming signals, as well as what is the BER and SER at those stopband widths. The results quite clearly show that as the sweep frequency and transmit power are increased, the required HPF stopband width increases as well as the residual increase in BER and SER. However, the situation is much better with the 20 MHz bandwidth, wherein we see lower sweep frequencies achieving reasonable BER and SER values—below 1%—even at the highest transmit power levels.

With current technology, it might be unfeasible to attempt to fit the proposed architecture to user equipment. As such, we only consider the uplink to have a physically secured data stream, while the downlink needs to rely on cryptography or other securing mechanisms. Let us clearly state that any additional increase of BER from usual operation inherently decreases the data throughput of the system, which in our case means the uplink to an access point. However, the setup does not inherently cause additional errors in the downlink direction, when jamming is turned off.

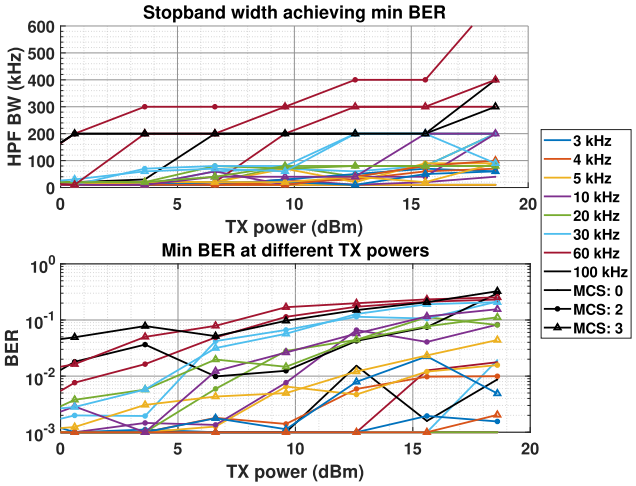
The SER results give us an idea of how our system might perform before error control coding when receiving generic OFDM-signals. Furthermore, when comparing Fig. 9, 10 and 12 we can see that there is a slight improvement between BER and SER values, with 20 MHz sweep bandwidth achieving better results. This seems to imply that the error control coding inherent to WLAN does help somehow in mitigating the attenuating effect of the system, however there might be room to select or develop a more effective algorithm to further enhance the performance. Additionally, we can see that 4-QAM with 3/4 coding rate does not perform significantly worse than 1/2 coding rates, which implies that the errors caused by the operating principle are not consistent enough to disrupt more effectively the error correction even with reduced redundancy.

Regarding jamming performance, it is intuitive that, as the transmit power of the jamming signal is increased, the effective jammed geographical area likewise increases. Therefore to have maximum protected area, we want to maximize our transmit power. The second parameter affecting jamming performance is sweep frequency. By increasing it, we increase the chance that the jamming waveform overlaps the pilot symbols required for accurate channel and phase correction, which causes additional symbol errors to just having interference over some data symbols. With extreme sweep frequencies, the jamming waveform starts having similarities with wideband barrage jamming, which is undesirable as the jamming power is spread evenly among all symbols instead of focused over a single or just a few of them. Therefore the requirements of good reception and jamming performance include a trade-off. One wants to maximize transmit power and have medium-to-high sweep frequency for jamming, however these requirements cause increasing bit errors for their own reception.

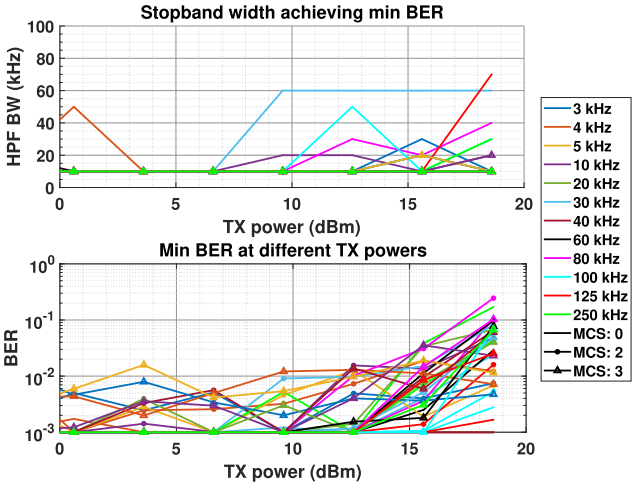
Although the jamming performance with different transmit parameters is not conclusively studied herein, we still see from the outdoors measurements that the sweeping waveform is effective at preventing eavesdropping of a WLAN signal at a reasonable range from the jamceiver, even with the relatively low transmit powers used. This result, combined with the knowledge of how the sweeping properties of the jamming waveform affect the reception performance, provides us with information about how this setup could be used in different scenarios. An interesting follow-up study could be targeted to finding out what are the optimal sweeping parameters to jam a WLAN signal or other popular protocols used in the ISM band, such as Bluetooth or Zigbee, as well as how the highpass filtering affects the reception of these other protocols.

Another interesting future research direction would be studying how multiple access points securing their WLAN receptions would work in a shared-spectrum use case. For instance, if multiple user equipment–access point pairs were operating on the same channel, jamming would need to be synced to only occur during the time–channel slot used by their own packets. Accurate timing would be required in order to avoid jamming the operation of other data-streaming pairs.

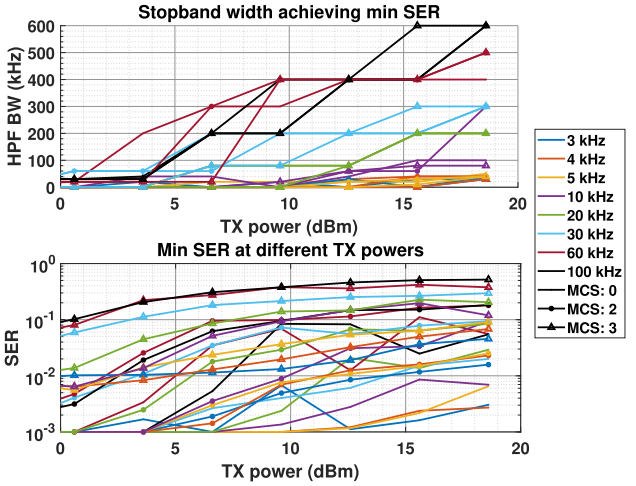
As a final note, it needs to be emphasized that the presented operation scheme is not possible with current off-the-shelf access point architectures since the transmitted signal is used in the downmixer, nor legal everywhere. Furthermore, the shared medium access protocols belonging to the IEEE 802.11 category would need to be adjusted in order to allow for this particular kind of physical-layer security with off-the-shelf



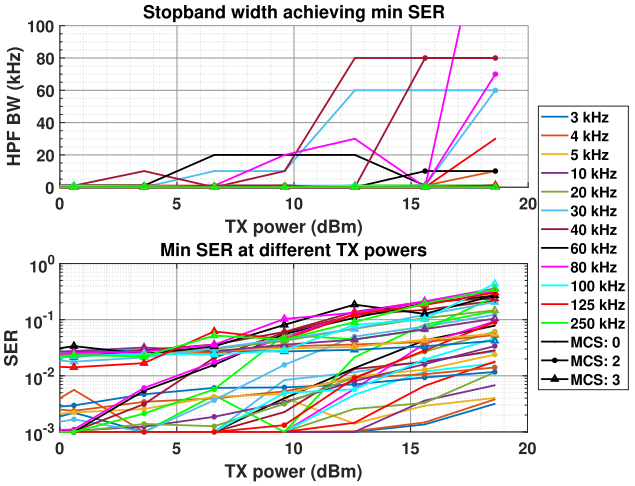
(a) in terms of bit-error rate for 80 MHz sweep bandwidth



(b) in terms of bit-error rate for 20 MHz sweep bandwidth



(c) in terms of symbol-error rate for 80 MHz sweep bandwidth



(d) in terms of symbol-error rate for 20 MHz sweep bandwidth

Fig. 12. Jamceiver's minimum bit or symbol error rates for different f_{s} and increasing p_{TX} as well as the corresponding B_{HPF}, where the minimum is achieved. The results in subfigure (a) are obtained with laptop measurements while the other subfigures show results from SDR measurements. These results were measured in the laboratory.

user equipment, as with the current implementations devices could stop transmitting when detecting strong jamming signals occupying their chosen channel. Yet the results are valuable in demonstrating what could be achieved if the jamceiver concept is adopted into standards and regulations in the future.

VI. Conclusion

In this work we demonstrated the jamming and reception performance of an experimental full-duplex capable jamceiver (which is our original neologism from "jammer–receiver") in simultaneous eavesdropping prevention and WLAN signal reception. In the considered setup, the transmitted sweeping tone signal is used in the downmixer, which allows the down-converted self-interference to be suppressed with a highpass filter. The operation, however, requires more involved digital processing and some portions of the received signal are unfortunately attenuated as well. Through the measurements we have shown that the proposed setup is capable of sufficiently attenuating the self-interference caused by sending a jamming signal at maximum transmit power levels allowed for the ISM band without an excessive loss to reception performance. The presented results likewise show the limitations of the setup, and the trade-off that having a wider and faster sweeping signal in the transmit side causes to the reception performance. These findings provide practical insights to designers wishing to utilize the presented jamceiver in different usage scenarios of physical-layer security.

References

[1] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.

[2] M. Lichtman et al., "A communications jamming taxonomy," *IEEE Secur. Privacy*, vol. 14, no. 1, pp. 47–54, Jan. 2016.

[3] W. Wang and J. Cai, "A technique for jamming Bi- and multistatic SAR systems," *IEEE Geosci. Remote Sens. Lett.*, vol. 4, no. 1, pp. 80–82, Jan. 2007.

[4] H. Wang, M. Luo, Q. Yin, and X. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[5] L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1790–1793, Oct. 2015.

[6] J. Yang, S. Salari, I. Kim, D. I. Kim, S. Kim, and K. Lim, "Asymptotically optimal cooperative jamming for physical layer security," *J. Commun. Netw.*, vol. 18, no. 1, pp. 84–94, Feb. 2016.

[7] J. Choi, "Physical layer security for channel-aware random access with opportunistic jamming," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2699–2711, Nov. 2017.

[8] K. Cumanan et al., "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2017.

[9] L. Hu et al., "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[10] B. Ma, Z. Liu, Y. Zeng, and J. Ma, "Cooperative jamming for secrecy of wireless communications," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2018, pp. 14–21.

[11] R. Li, Q. Duan, J. Xue, S. Zhang, and C. He, "A directional reactive jamming scheme based on machine learning," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2019, pp. 1–5.

[12] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for beyond 5G: Ultra secure low latency communications," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2232–2242, 2021.

[13] X. Jiang, P. Li, B. Li, Y. Zou, and R. Wang, "Intelligent jamming strategies for secure spectrum sharing systems," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1153–1167, Feb. 2022.

[14] M. S. J. Solaija, H. Salman, and H. Arslan, "Towards a unified framework for physical layer security in 5G and beyond networks," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 321–343, 2022.

[15] Z. Wang, J. Guo, Z. Chen, L. Yu, Y. Wang, and H. Rao, "Robust secure UAV relay-assisted cognitive communications with resource allocation and cooperative jamming," *J. Commun. Netw.*, vol. 24, no. 2, pp. 139–153, Apr. 2022.

[16] Y. Wu, G. Ji, T. Wang, L. Qian, B. Lin, and X. Shen, "Non-orthogonal multiple access assisted secure computation offloading via cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7751–7768, Jul. 2022.

[17] D. Xu and H. Zhu, "Jamming-assisted legitimate eavesdropping and secure communication in multicarrier interference networks," *IEEE Syst. J.*, vol. 16, no. 1, pp. 954–965, Mar. 2022.

[18] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in *Proc. MILCOM Mil. Commun. Conf.*, Nov. 2011, pp. 2129–2135.

[19] 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 *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 174–188.

[20] K. Pärlin, M. M. Alam, and Y. L. Moullec, "Jamming of UAV remote control systems using software defined radio," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2018, pp. 1–6.

[21] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[22] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[23] J. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[24] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.

[25] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Towards secure communication via a wireless-powered full-duplex jammer," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Oct. 2016, pp. 1–4.

[26] J. Choi, "Full-duplexing jamming attack for active eavesdropping," in *Proc. 6th Int. Conf. IT Converg. Secur. (ICITCS)*, Sep. 2016, pp. 1–5.

[27] R. Nirala, S. S. Chauhan, and G. Verma, "Improving physical layer security in full-duplex relaying system," in *Proc. 2nd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2017, pp. 997–1001.

[28] O. Taghizadeh, P. Neuhaus, and R. Mathar, "Can full-duplex jamming reduce the energy-cost of a secure bit?" in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[29] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 120–135, Jan. 2019.

[30] R. Ma, S. Yang, M. Du, H. Wu, and J. Ou, "Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks," *IET Commun.*, vol. 13, no. 10, pp. 1530–1536, Jun. 2019.

[31] H. Wang, B. Zhao, and T. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[32] J. Saikanmäki, M. Turunen, M. Mäenpää, A. Saarinen, and T. Riihonen, "Simultaneous jamming and RC system detection by using full-duplex radio technology," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2019, pp. 1–6.

[33] N. Ebrahimi, H.-S. Kim, and D. Blaauw, "Physical layer secret key generation using joint interference and phase shift keying modulation," *IEEE Trans. Microw. Theory Techn.*, vol. 69, no. 5, pp. 2673–2685, May 2021.

[34] M. Bernhardt, J. Marin, and T. Riihonen, "Estimation of receiver frequency deviations in multifunction frequency-modulating transceivers," in *Proc. IEEE 95th Veh. Technol. Conf., (VTC-Spring)*, Jun. 2022, pp. 1–5.

[35] M. Bernhardt, J. Marin, and T. Riihonen, "Characterization of full-duplex constant-envelope transceiver for emerging multifunction systems," in *Proc. 30th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2022, pp. 1012–1016.

[36] J. Marin, M. Bernhardt, M. Heino, and T. Riihonen, "Monostatic FMCW radar architecture for multifunction full-duplex radios," in *Proc. 55th Asilomar Conf. Signals, Syst., Comput.*, Oct. 2021, pp. 640–644.

[37] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.

Jaakko Marin received the B.Sc. and M.Sc. degrees in information technology from Tampere University, Finland, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree. His current research interests include utilizing full-duplex technology in achieving multifunctionality, namely by integrating wireless communications, sensing, and jamming to a single device. He was a recipient of the Finnish Technical Sector's Award for the Best Master's Thesis of the Year.

Micael Bernhardt received the B.Sc. degree in electronic engineering from Universidad Nacional de Misiones, Argentina, and the Ph.D. degree from the National University of the South, Argentina. From 2019 to 2021, he was a Post-Doctoral Research Fellow with Tampere University, Finland, where he is currently working as a Visiting Researcher. His research interests include signal processing algorithms applied to wireless communications, with particular emphasis on full-duplex systems, integrated sensing and communications, and resource-efficient wireless communications and networks.

Taneli Riihonen (Senior Member, IEEE) received the D.Sc. degree in electrical engineering from Aalto University, Finland, in 2014. He is currently a tenure-track Associate Professor with the Faculty of Information Technology and Communication Sciences, Tampere University, Finland. His research interests include physical-layer OFDM(A), multiantenna, multihop, and full-duplex wireless techniques with current focus on the evolution of 6G communication and sensing systems and the stochastic geometry of massive low Earth orbit satellite networks. He was a recipient of the Finnish Technical Sector's Award for the Best Doctoral Dissertation of the Year and the EURASIP Best Ph.D. Thesis Award in 2017.