Simultaneous Jamming and RC System Detection by Using Full-Duplex Radio Technology

Joni Saikanmäki, Matias Turunen, Miikka Mäenpää, Antti-Pekka Saarinen, and Taneli Riihonen
Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland
email: joni.saikanmaki@gmail.com, {matias.turunen, miikka.maenpaa, antti-pekka.saarinen, taneli.riihonen}@tuni.fi

***Abstract*—The prospects of the inband full-duplex (IBFD) technology are praised in non-military communications as it allows each radio to simultaneously transmit and receive (STAR) on the same frequencies enabling, e.g., enhanced spectral efficiency. Likewise, future defense forces may significantly benefit from the concept, because a military full-duplex radio (MFDR) would be capable of simultaneous integrated tactical communication and electronic warfare operations as opposed to the ordinary time- or frequency-division half-duplex radios currently used in all military applications. This study considers one particular application, where the MFDR performs jamming against an opponent's radio control (RC) system while simultaneously monitoring RC transmissions and/or receiving data over the air from an allied communication transmitter. The generic RC system can represent particularly, e.g., one pertaining to multicopter drones or roadside bombs. Specifically, this paper presents outcomes from recent experiments that are carried out outdoors while earlier indoor results are also revisited for reference. In conclusion, the results demonstrate that MFDRs can be viably utilized for RC signal detection purposes despite the residual self-interference due to jamming and imperfect cancellation.**

I. Introduction

The so-called inband full-duplex (IBFD, or just FD) technology has recently been receiving a significant amount of attention in non-military research as it can, in theory, double the spectral efficiency of wireless links and, e.g., solve the hidden-node problem, which is a common difficulty with half-duplex (HD) broadcasts [1]–[3]. Practically all of today's military radios are utilizing conventional time- or frequency-division HD transmissions for tactical networking, and therefore military communication systems can also benefit from the IBFD technology as it enables same-frequency simultaneous transmit and receive (SF-STAR) operations.

We believe that military full-duplex radios (MFDRs) can become a major factor in gaining spectrum dominance over opposing forces, which could render even a bigger paradigm shift than efficient two-way communication [4]–[6]. Especially, MFDRs also facilitate electronic warfare operations, which constitute a major part of today's modern warfare [7]. It is possible, e.g., simultaneously to intercept an opponent's tactical data transfer by using an IBFD transceiver's receiver (RX) chain while jamming the opponent's radio receivers by utilizing its transmitter (TX) chain. We also anticipate that, on top of those discussed in [5] and [6], many other new promising scenarios could be still discovered in both civilian and military environments.

This research work was funded by the Finnish Scientific Advisory Board for Defence (MATINE — Maanpuolustuksen tieteellinen neuvottelukunta) under the project 2500M-0092 "Full-Duplex Radio Technology in Military Applications" and the Academy of Finland under the grant 315858 "Radio Shield Against Malign Wireless Communication."

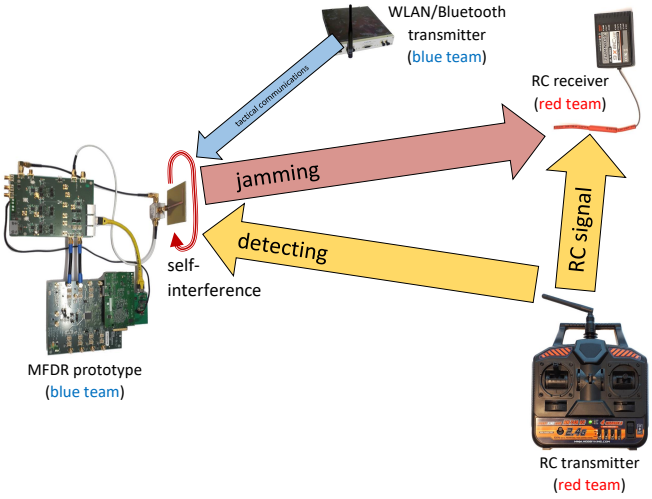


Figure 1: Setup of the experiments, where the red team utilizes an off-the-shelf radio control (RC) system and the blue team utilizes a military full-duplex radio (MFDR) capable of detecting and jamming the red team's operations while receiving data from their own WLAN/Bluetooth radio transmitter.

Our recently published research [8]–[10] has already shown in a clinical indoor laboratory environment that the IBFD technology can be successfully used for tactical communication while simultaneously executing electronic warfare operations. In the present work, we take a small step toward real battlefields by continuing the experiments outdoors at our campus yard in the scenario illustrated in Fig. 1. Thus, the experiments are similar to those reported in [8] based on indoor measurements and revisited herein for reference.

By these two works (namely, [8] and the present one), we have demonstrated that the MFDR is capable of detecting an opponent's RC transmitter both indoors and outdoors, while preventing its RC receiver's operation for controlling, e.g., improvised explosive devices [8] and unmanned aerial vehicles [11]. The capability for successful RC detection is concretely evaluated by measuring signal-to-interference-plus-noise ratio (SINR) for the RC signal under residual self-interference (SI) from SF-STAR operation and simultaneous tactical transmissions from allied radios to the MFDR. We can deem detection successful in almost all of the tested cases, because large SINR values are achieved consistently.

II. Equipment for Experiments

The work presented herein examines the capabilities of a blue team's MFDR prototype to detect and simultaneously prevent (with jamming) hostile RC transmissions by an opposing red team as sketched in Fig. 1. Furthermore, major spectrum dominance can be achieved when the blue team's MFDR is also capable of simultaneously receiving communication waveforms from its allied tactical radios. The equipment for the outdoor experiments is photographed in Fig. 2.

A. Red Team: Improvised Radio Control (RC) System

In our earlier indoor [8], [10] and present outdoor experiments, the red team employs an off-the-shelf RC system from HobbyKing. Equivalent consumer electronics could also be found in, e.g., alarm systems or multicopters, if building an improvised system. The RC transmitter illustrated in Fig. 2(a) is continuously powered up in its normal broadcasting mode.

The proprietary RC protocol at hand is called an automatic frequency hopping digital system (AFHDS) and it employs AMICCOM A7105 wireless transceiver chips for operation in the radio-frequency (RF) range of 2.4055–2.4750 GHz within the industrial, scientific, and medical (ISM) radio band. With AFHDS signalling, the specific RC unit we have sends uncoded binary Gaussian frequency-shift keying (GFSK) frames hopping between 500-kHz subbands centered at

$$\begin{aligned}\{&2407.0, 2412.0, 2417.0, 2419.5, 2422.0, 2427.0, 2429.5, 2432.0,\\ &2437.0, 2442.0, 2447.0, 2452.0, 2457.0, 2462.0, 2467.0, 2472.0\}\end{aligned} \quad (1)$$

[MHz]. On the side, we also tested jamming effectiveness against a compatible off-the-shelf receiver from HobbyKing.

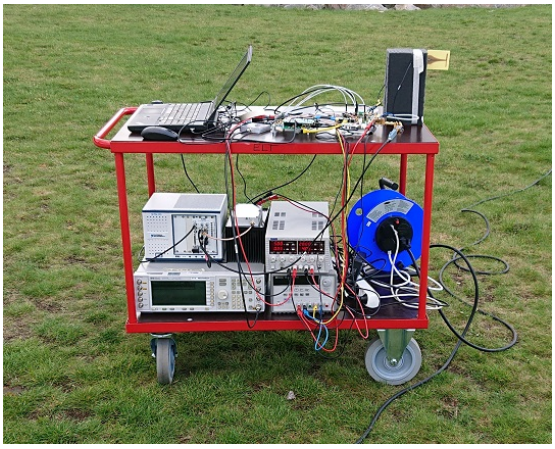
B. Blue Team: Military Full-Duplex Radio (MFDR) Prototype

The MFDR prototype depicted in Fig. 2(b) has originally been developed for non-military communication applications. High-end National Instruments (NI) PXIe-5645R vector signal transceiver (VST) acts as the baseline radio component that operates at the ISM radio band by transmitting a jamming signal against the RC system, which simultaneously couples to its receiver when monitoring the spectrum for RC transmissions and receiving tactical communications from an allied transmitter. This is called self-interference (SI) and the MFDR prototype aims to suppress it as much as possible in order to receive the communication signals and be able to detect the RC signal correctly.

The SI cancellation is separated into three different stages that are capable of suppressing the SI by 90–100 dB in total:

1) The TX output and RX input of the MFDR prototype are connected to a shared antenna with a circulator supporting *passive isolation* between the TX and RX chains. In the experiments reported in [12], the circulator provides roughly 30 dB of isolation, which is necessary because substantial SI power would otherwise saturate the low-noise amplifier in the receiver. Furthermore, a custom-made dipole patch antenna is used in order to minimize SI reflection with precise impedance matching.

(a) the red team's RC transmitter



(b) the blue team's military full-duplex radio prototype

(c) the blue team's wireless radio transmitter

Figure 2: The equipment used in the outdoor experiments.

Table I: Essential Outdoor Measurement Parameters

Parameter		Value
Center frequency		2.44 GHz
Blue team	Communication waveform	WLAN or Bluetooth
	Communication bandwidth	20 MHz (WLAN) or 80 MHz (Bluetooth)
	Communication TX power	20 dBm (WLAN) or 4 dBm (Bluetooth)
	TX/RX sampling rate	120 MHz
	Jamming waveform	wideband or RC-specific
	Jamming bandwidth	80 MHz
	Jamming power	$\{0, 5, 10, 15, 20\}$ dBm
Red team	RC waveform	GFSK with frequency hopping
	Protocol	AFHDS

2) Before the VST, a three-tap *wideband RF canceller* [13], [14] is utilized to further suppress the SI. Each tap, with a predefined delay, tunes the amplitude and phase of the TX signal and they are then combined and subtracted from the RX signal. The RF canceller is capable of suppressing the SI by roughly 40–50 dB.
3) *Digital cancellation* [13] is performed offline in Matlab, where the residual SI cancellation signal is generated based on the received and original transmitted signals by utilizing a nonlinear channel model. Then, the cancellation signal is subtracted from the received signal, by which the SI can be suppressed by roughly 25 dB [12].

The MFDR prototype is reported in more detail by [12]–[14].

We tested two jamming signals in the experiments. In the case of a *wideband jamming* signal, white Gaussian-like noise is transmitted with a bandwidth of 80 MHz, while an *RC-specific jamming* signal is tailored according to the subbands listed in (1). In RC-specific jamming, only the RC transmitter's subbands are continuously jammed due to which higher power spectral density with the same transmission power can be achieved in comparison to wideband jamming, but the blue team needs to know them to begin with.

C. Blue Team: Communication Radio Transmitter

The communication transmitter is implemented with NI USRP-2953R software-defined radio that is controlled via LabVIEW. A photograph of the equipment when located in the farther measurement position is shown in Fig. 2(c). The transmitter broadcasts the standard WLAN and Bluetooth signal waveforms described in [15] and [16], respectively. The WLAN signal with a bandwidth of 16.6 MHz is of orthogonal frequency-division multiplexing (OFDM) -type consisting of 52 quadrature phase-shift keying (QPSK) subcarriers and modulated to the center frequency of 2.462 GHz. The Bluetooth signal, on the other hand, is of Gaussian frequency shift keying (GFSK) -type with frequency hopping, where data packets are sent through 79 evenly distributed 1-MHz subchannels around the center frequency of 2.440 GHz. The Bluetooth and WLAN signals are transmitted at their nominal maximum powers of 4 dBm and 20 dBm, respectively.

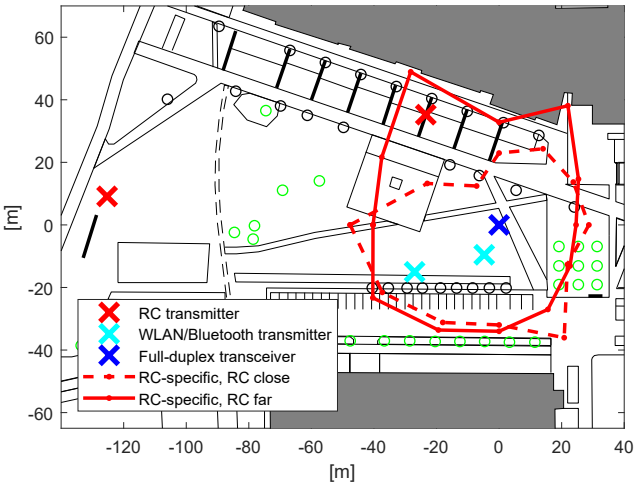


Figure 3: The relative locations of the different devices during the outdoor experiments, where also the coverage areas of RC-specific jamming are included with 20-dBm jamming power. The communication transmitters are positioned 'close' (10 m) or 'far' (30 m) and the RC transmitter is positioned 'close' (40 m) or 'far' (125 m) with respect to the MFDR prototype.

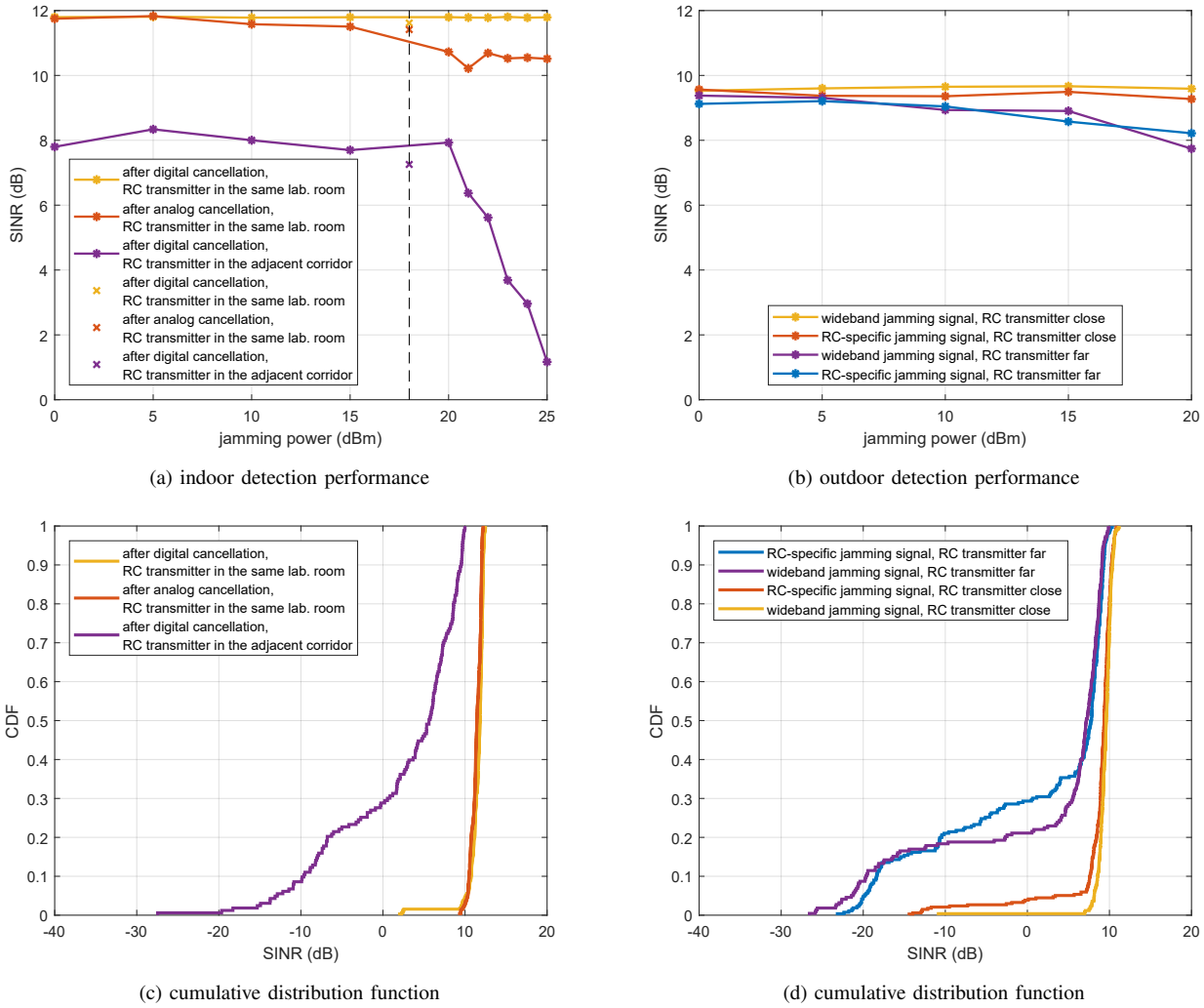
III. Measurements and Data Processing

A. Previous Indoor Experiments

The reference indoor setup is described in [8] and so all specific details can be omitted herein. In the experiments, the RC transmitter was first placed in the same room with the MFDR prototype and an RC receiver. Then, the RC transmitter was carried farther away to an adjacent corridor. Jamming power was increased step-by-step from 0 dBm to 25 dBm in both experiments with 1-dB intervals above 20 dBm and with 5-dB intervals below it. More measurements were performed also at the 18-dBm sweet spot, above which higher powers represent an extreme case for the prototype's SI suppression. Ten data vectors were measured with 18-dBm jamming power and four to five data vectors were stored for other jamming powers. The data vectors here are measurements of 50 ms recorded by the VST after RF cancellation.

B. New Outdoor Experiments

The outdoor experiments took place at the front yard of the Hervanta campus of Tampere University. The blue team's tactical transmitter was placed at two different distances from the MFDR prototype as seen in Fig. 3. The closer position was 10 meters, and the further 30 meters, away from the blue team's MFDR prototype. Similarly, the red team's RC transmitter was placed in two different locations, 40 meters and 125 meters away from the jammer. The areas where jamming was effective were measured with 20-dBm jamming power for both RC transmitter positions as shown in Fig. 3. Since the earlier indoor experiments had indicated that the detection capability of the MFDR prototype deteriorates at high jamming power levels, jamming power was increased now in the measurements from 0 dBm only up to 20 dBm with 5-dB intervals. Ten data vectors were measured outdoors providing more accurate results than the indoor laboratory experiments. All essential parameters are shown in Table I.



(a) indoor detection performance

(b) outdoor detection performance

(c) cumulative distribution function

(d) cumulative distribution function

Figure 4: The average signal-to-interference-plus-noise ratios of RC signals to be detected (a) indoors and (b) outdoors at the blue team's MFDR prototype's input as well as their cumulative distribution functions (c) indoors and (d) outdoors. The SINR distributions are plotted with (c) 18-dBm and (d) 20-dBm jamming powers. Likewise, all different jamming scenarios and RC transmitter positions are covered without tactical transmission.

C. Post-processing of Measurement Data

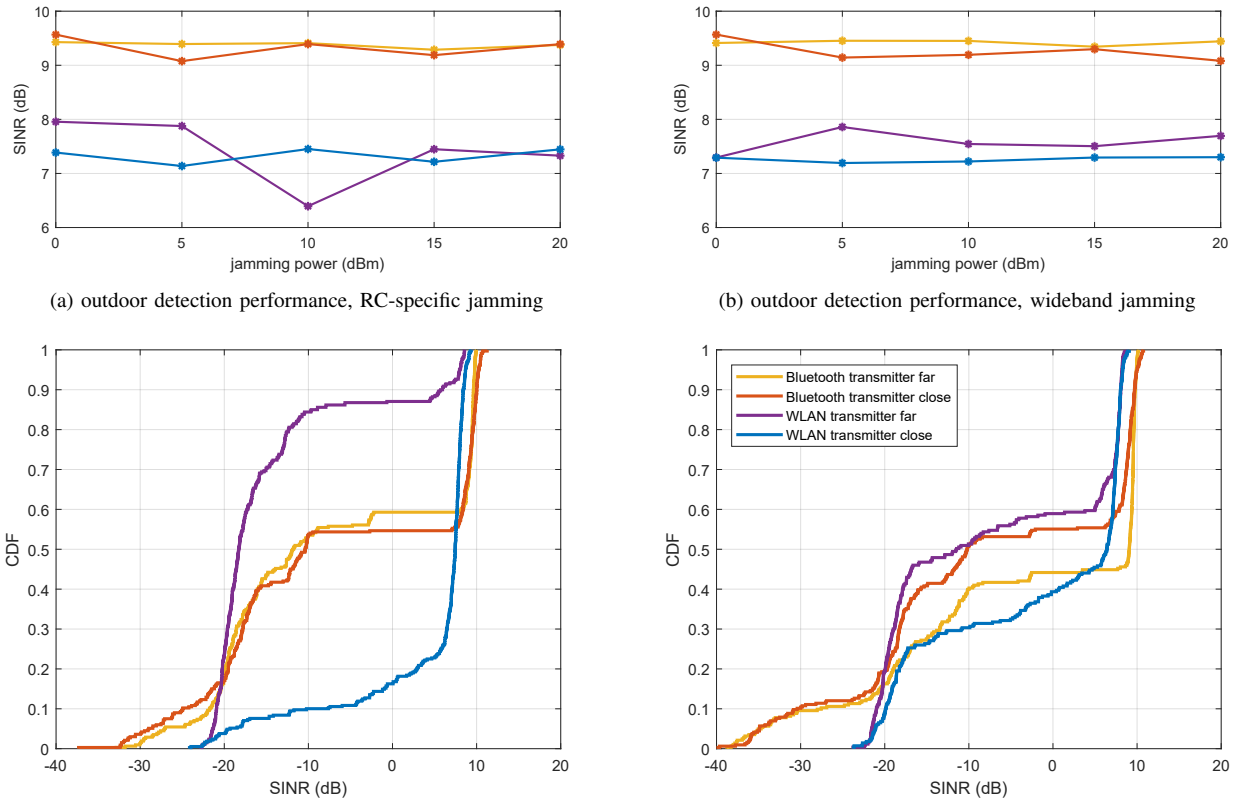
Digital SI cancellation was first executed on all measured data vectors by utilizing a nonlinear cancellation algorithm. Each 50-ms data vector contained around 30–40 frames of RC transmissions. Each of these 250-bit frames were decoded by using the Viterbi algorithm after which corresponding GFSK-modulated pilot signals were regenerated. Each received frame was then matched with the corresponding GFSK-modulated pilot signal for signal-to-interference-plus-noise ratio (SINR) estimation. The equalization process involved time and frequency synchronization using the channel estimate. Then, a noise-plus-interference component was calculated by subtracting the estimated useful signal from the overall RX signal. For calculating average SINRs, only the detected frames that had SINR above 0 dB at each jamming power were taken into account due to high probability that other transmissions, SI cancellation, and environment changes cause problems in small SINR values, degrading the estimates' accuracy.

IV. Experimental Results and Discussion

In what follows, the effectiveness of the MFDR prototype's RC signal detection is evaluated in terms of the SINRs that are estimated from the data measured in the experiments. While each specific detection algorithm offers its own specific sensitivity and reliability, SINR is a metric that allows us to analyze the detection performance in general. Generally speaking, we shall shortly see that SINR for detection is significantly above 0 dB in most cases despite residual SI, which demonstrates that even any primitive algorithm would likely be able to detect successfully the RC transmissions.

A. Previous Indoor Experiments

Figure 4(a) illustrates estimated SINRs at the detecting MFDR prototype's receiver in indoor experiments, where the jamming signal was white noise with 80-MHz bandwidth. More accurate SINR values for 18-dBm jamming power are indicated separately with a dashed line in the same figure. The



(a) outdoor detection performance, RC-specific jamming

(b) outdoor detection performance, wideband jamming

(c) cumulative distribution function

(d) cumulative distribution function

Figure 5: The average SINR at the detecting blue team's MFDR prototype RX input when using (a) RC-specific and (b) wideband jamming signals. The respective cumulative distribution functions (CDFs) with 20 dBm jamming power are plotted in (c) and (d). For both outdoor experiment scenarios, the RC transmitter was positioned close and the communication radio transmitter was turned on. Likewise, different WLAN and Bluetooth transmitter positions were utilized and here only one legend is used as the colours remain the same in all four subfigures.

data from 18-dBm jamming power is utilized for plotting an empirical cumulative distribution function (CDF) in Fig. 4(c).

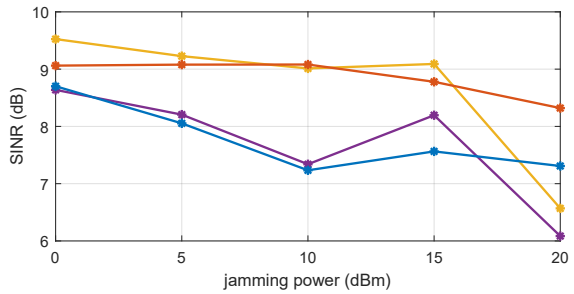
The MFDR prototype would be able to detect the RC transmissions regardless of the residual SI and co-channel interference that degrade the actual signal-of-interest [8], because SINR is round 8 dB when jamming power is below 18 dBm. However, when the jamming power is increased above 20 dBm, the MFDR may not anymore be able to detect the RC signal as the average SINR decreases dramatically.

B. New Outdoor Experiments

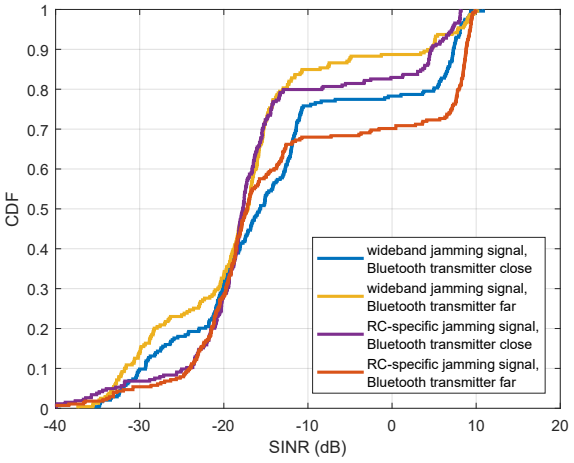
The outdoor experiments are herein obtained under the campus yard scenario mapped in Fig. 3 that shows the relative positions of the devices in two measurement cases. In the first case, the MFDR tries only to detect signals sent by the opponent's RC transmitter while jamming the ISM radio band. In the second case, the MFDR prototype receives a communication waveform from a radio transmitter while simultaneously jamming and detecting the opponent's RC transmissions.

Firstly, Figs. 4(b) and 4(d) represent cases, where the communication signal was not active. Figure 4(b) shows SINRs at the detecting MFDR prototype's receiver when the RC transmitter was positioned close and far, and it uses the wideband and RC-specific jamming signals. The same data is used in Fig. 4(d) for plotting the CDF at the maximum 20-dBm jamming power. Regardless of the position of the RC transmitter or the jamming signals, over 70% of frames can be decoded correctly resulting in very accurate SINRs above 9 dB that would definitely allow successful detection.

Secondly, Fig. 5(a) shows the SINRs at the MFDR prototype's receiver when the RC transmitter was placed close, and the RC-specific jamming signal was used. Figure 5(b), on the other hand, illustrates the SINRs at the receiver of the detecting MFDR prototype when the wideband jamming signal was employed, and the RC transmitter's position remained unchanged. The communication signal was transmitted in two different locations as seen in Fig. 3. Using the same data, CDFs are drawn in Figs. 5(c) and 5(d) at the maximum jamming power of 20 dBm. The SINRs remain at the same level regardless of the jamming power. However, the MFDR prototype detects better RC transmission if Bluetooth signal is used for communicating. Nevertheless, the presence of a communication signal lowers the probability of the MFDR to decode received frames correctly, therefore affecting also SINRs. As Fig. 5(c) indicates, by positioning RC transmitter close, WLAN transmitter far, and using RC-specific jamming signal, only 10 % of the total frames can be decoded correctly, but round 7-dB SINR is sufficient for successful detection.



(a) outdoor detection performance



(b) cumulative distribution function

Figure 6: The SINR after SI cancellation at the detecting MFDR prototype's input when using both jamming signals, Bluetooth transmitter is chosen, and RC transmitter is at its farthest location. The cumulative distribution function with maximum jamming power of 20 dBm is drawn and only one legend is exploited as the colours remain the same in both figures.

Finally, Fig. 6(a) illustrates a situation where the RC transmitter was installed farther away from the MFDR prototype at the front yard. Both jamming signals were utilized and the Bluetooth transmitter was placed to two locations at the yard. The CDFs according to measured data vectors at 20-dBm jamming power can be observed in Fig. 6(b). Regardless of the jamming strategy, the MFDR is capable of detecting RC signals better when the Bluetooth transmitter is at its farthest position, i.e., SI cancellation works worse when the communication radio transmitters are near as expected. Only the Bluetooth signal was utilized here; however, the same conclusion can be drawn for the WLAN signal.

V. Conclusion

The present study was able to demonstrate that, regardless of the jamming and communication waveforms in use and the positions of an own team's communication radio transmitters or an opponent's RC transmitter, the MFDR prototype used in the experiments is capable of detecting the opponent's RC system whenever the detection would be possible without simultaneous jamming in the first place. This is justified by the fact that SINRs of 8–10 dB were observed for 10–70% of frames consistently in all the experiments. The result is general since the considered RC system can be applied for many purposes, e.g., to control improvised explosive devises or unmanned aerial vehicles such as multicopters. The jamming interference created by the MFDR can be also seen as a radio shield within which malign wireless communication cannot be performed. Thus, not only military but also ordinary communication systems may benefit from MFDRs as the information signals used in the experiments were actually those utilized currently in the civilian world.

References

[1] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[2] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[3] Z. Zhang, K. Long, A. V. Vasilakos, and L. Hanzo, "Full-duplex wireless communications: Challenges, solutions, and future research directions," *Proceedings of the IEEE*, vol. 104, no. 7, pp. 1369–1409, Jul. 2016.

[4] T. Riihonen, D. Korpi, O. Rantula, and M. Valkama, "On the prospects of full-duplex military radios," in *Proc. International Conference on Military Communications and Information Systems*, May 2017.

[5] T. Riihonen, D. Korpi, O. Rantula, H. Rantanen, T. Saarelainen, and M. Valkama, "Inband full-duplex radio transceivers: A paradigm shift in tactical communications and electronic warfare?" *IEEE Communications Magazine*, vol. 55, no. 10, pp. 30–36, Oct. 2017.

[6] K. Pärlin, T. Riihonen, R. Wichman, and D. Korpi, "Transferring the full-duplex radio technology from wireless networking to defense and security," *Proc. 52nd Annual Asilomar Conference on Signals, Systems, and Computers*, Oct. 2018.

[7] A. E. Spezio, "Electronic warfare systems," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 633–644, Mar. 2002.

[8] T. Riihonen, D. Korpi, M. Turunen, and M. Valkama, "Full-duplex radio technology for simultaneously detecting and preventing improvised explosive device activation," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[9] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, and R. Wichman, "Tactical communication link under joint jamming and interception by same-frequency simultaneous transmit and receive radio," in *Proc. IEEE Military Communications Conference*, Oct. 2018.

[10] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, and R. Wichman, "Military full-duplex radio shield for protection against adversary receivers," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[11] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[12] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y. Choi, L. Anttila, S. Talwar, and M. Valkama, "Full-duplex mobile device: Pushing the limits," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 80–87, Sep. 2016.

[13] J. Tamminen, M. Turunen, D. Korpi, T. Huusari, Y. Choi, S. Talwar, and M. Valkama, "Digitally-controlled RF self-interference canceller for full-duplex radios," in *Proc. 24th European Signal Processing Conference*, Aug. 2016, pp. 783–787.

[14] D. Korpi, "Full-duplex wireless: Self-interference modeling, digital cancellation, and system studies," Ph.D. dissertation, Tampere University of Technology, Dec. 2017.

[15] D. Vassis, G. Kormentzas, A. Rouskas, and I. Maglogiannis, "The IEEE 802.11g standard for high data rate WLANs," *IEEE Network*, vol. 19, no. 3, pp. 21–26, May 2005.

[16] *IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*, IEEE Std. 802.15.1, 2002.