Full-Duplex Radio Technology for Simultaneously Detecting and Preventing Improvised Explosive Device Activation

Taneli Riihonen, Dani Korpi, Matias Turunen, and Mikko Valkama

Laboratory of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
e-mail: {taneli.riihonen, dani.korpi, matias.turunen, mikko.e.valkama}@tut.fi

***Abstract*—Originating from civilian/commercial wireless networks, the progressive concept of same frequency simultaneous transmission and reception (SF-STAR), a.k.a. in-band full-duplex operation, has high potential also at the future battlefield. The prospects of a military full-duplex radio (MFDR) are not limited to enhancing the spectral efficiency of tactical communications, which would already be a significant advancement considering the universal congestion of electromagnetic spectrum. Perhaps even more importantly, armed forces could gain a major technical advantage by employing multifunction MFDRs that are capable of jointly conducting signals intelligence, electronic warfare, and tactical communications owing to their SF-STAR capability. This study focuses on one specific promising application, where a radio transceiver performs spectrum monitoring and signal surveillance for potential hostile transmissions when simultaneously performing an electronic attack against opposing forces' receivers at the same frequency band. In particular, we demonstrate by experiments in a laboratory environment that the MFDR technology can be successfully used for detecting an attempt to control remotely an improvised explosive device while also preventing its activation by transmitting a jamming signal.**

I. Introduction

In-band full-duplex (IBFD, or just FD) radios [1]–[3] are capable of tuning their receive and transmit chains on the same center frequency due to efficient self-interference cancellation. Hence, a future *military full-duplex radio* (MFDR) will be provided with an unprecedented capability for *same frequency simultaneous transmit and receive* (SF-STAR) operation, possibly offering even a major technical advantage over opposing forces, whose radios do not have the same capability. In particular, as envisioned in [4], the usage of FD radios not only facilitates spectrum-efficient two-way information transfer, but they also allow armed forces to merge electronic warfare [5] into tactical communications and, thus, establish novel combat tactics and techniques pertaining to information reception with simultaneous electronic attacks and signals intelligence during information transmission or an electronic attack.

While scientific discourse on the theory of MFDR systems at large is still in its infancy too (see [4], [6] for a full account), experimental research on applications thereof is practically unborn to the best of our knowledge. Thus, strictly speaking, one cannot yet know for sure whether the MFDR technology is practicable in the aforementioned multifunction operation in reality at all, because the envisioned concepts have not been tested even in a laboratory. Motivated by these premises, the objective of our study is to initiate the experimentation of the practical applications of multifunction MFDR transceivers.

This research work was funded by the Finnish Scientific Advisory Board for Defence (MATINE — Maanpuolustuksen tieteellinen neuvottelukunta) under the project "Full-Duplex Radio Technology in Military Applications."

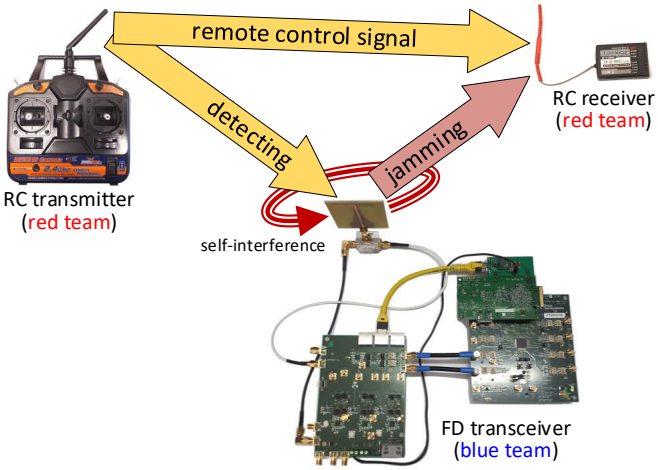


Fig. 1. A sketch of the considered battlefield scenario, where the blue team exploits an in-band full-duplex (FD) transceiver for simultaneously detecting and jamming the red team's remote radio control (RC) system.

We consider the battlefield scenario illustrated in Fig. 1. The red team attempts to use an improvised radio control (RC) system to activate an explosive device. The blue team's FD radio attempts to prevent that by broadcasting jamming [7] as usual, but now its SF-STAR capability enables simultaneous spectrum monitoring and signal surveillance for detecting the red team's RC transmitter. In contrast, a conventional radio would alternate between the transmit and receive functions [7].

In what follows, Section II describes our laboratory setup with a prototype FD radio transceiver and an improvised RC system, while measurement results from our experiments are presented in Section III. Finally, Section IV discusses the outcomes of our laboratory tests leading to the ultimate conclusion: We have demonstrated beyond doubt that the MFDR technology can indeed be successfully used for detecting an attempt to activate remotely an improvised explosive device while simultaneously also preempting the activation attempt.

978–1–5386–4559–8/18/$31.00

II. Laboratory Setup

The laboratory setup constructed for our experiments operates at the unlicensed 2.4-GHz industrial, scientific and medical (ISM) radio band. The prototype FD transceiver shown in Fig. 2(a) is repurposed from our earlier research on non-military wireless communications and its development is reported in [8]–[10]. On the other hand, the RC trigger system was designed and implemented specifically for this study by an external consultant, which guarantees scientific objectivity by presenting us an independent simulated adversary.

A. Blue Team: Experimental Full-Duplex (FD) Transceiver

The prototype MFDR is built on top of a high-quality vector signal transceiver (National Instruments PXIe-5645R). The device transmits white jamming noise with 80-MHz bandwidth that acts as self-interference (SI) for spectrum monitoring and signal surveillance at its receive chain. The necessary SI suppression is implemented in three stages. Firstly, a *circulator* allows the transmit and receive chains to share a single antenna, while also providing 29-dB passive isolation. Secondly, SI is suppressed by custom-made active *analog cancellation* electronics to ensure that SI power entering analog-to-digital conversion does not saturate it. Finally, the remaining SI is suppressed by non-linear *digital cancellation* in software.

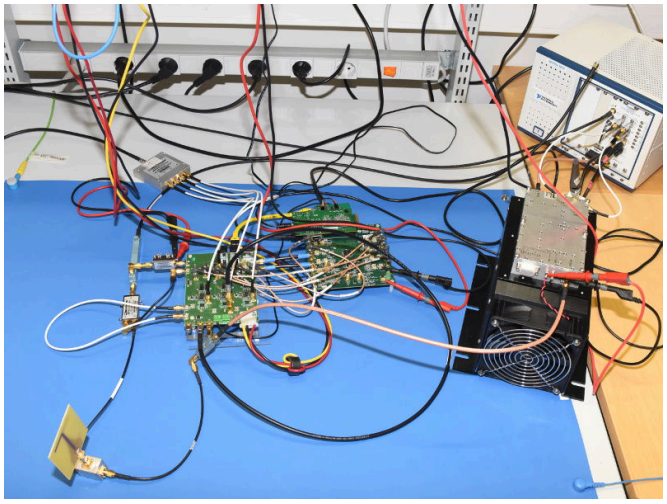
B. Red Team: Improvised Radio Control (RC) System

As for the opposing force, the laboratory setup simulates a scenario, where the red team has improvised an RC system for explosive devices using off-the-shelf consumer electronics as shown in Fig. 2(b). Equivalent electrical components could be scavenged from RC toys, drones/multicopters, or model airplanes/helicopters/cars, while new ones cost in total at most 20–30 euros in an online store. The setup represents well any general improvised RC system, for which parts could be taken from a cellular phone, a personal mobile radio, a baby monitor, a wireless doorbell, a pager, a garage door opener, etc.

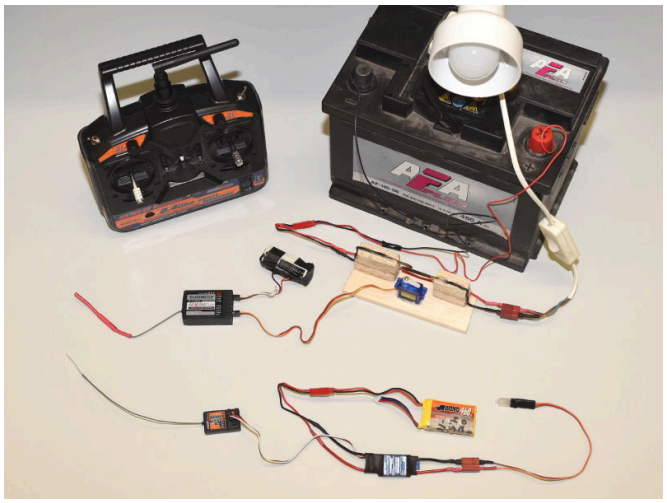
The 2.4-GHz signaling implemented by the RC components at hand follows a proprietary automatic frequency hopping digital system (AFHDS) protocol, also known as the FlySky or Turnigy 9X protocol, for which compatible transmitters and receivers are based on AMICCOM A7105 wireless transceiver chips. In the AFHDS protocol, the ISM band is divided into 160 subbands with center frequencies spanning uniformly from 2400.5 MHz to 2479.5 MHz. Each radio hops frame-by-frame between 16 subbands following one of 160 different patterns for multiple access among AFHDS transmitters and robustness against other ISM-band usage, e.g., RF interference (RFI) from wireless local area networks (WLANs). The remote control information is transferred by uncoded binary Gaussian frequency shift keying (GFSK) with about 200-kHz deviation.

The red team uses a six-channel HobbyKing transmitter (HK-T6A-M2*) to control remotely devices that are equipped with compatible receivers. The 'channels' refer herein to the parallel control signals, each of which could be used to trigger one or two separate explosives. We performed jamming tests against an eight-channel Turnigy receiver (RX-9X8Cv2*) and a three-channel HobbyKing receiver (HK-GT2_RX*) without noticing any performance difference in our indoor experiments despite the former branded, and more expensive, one is labeled as a "full-range receiver" unlike the latter unbranded one.

Instead of containing electric blasting caps, the laboratory setup employs common 12-V light bulbs for safely simulating detonation. The improvised RC system came with two alternatives for turning on the light bulbs, i.e., setting off blasting caps. In the upper one of Fig. 2(b), a HexTronik micro servo (HXT900*) bends a conductive metal strip so that it touches another one and current flows from a car battery to a 3.5-W LED lamp. Thus, a separate battery pack (4.5–6.5 V) is needed for the receiver unlike in the lower one of Fig. 2(b), where a Turnigy speed controller for brushed motors (TGY-30A*) converts its input voltage (6–12.6 V), e.g., from two/three LiPo cells, for both the receiver and a 20-W halogen light bulb.



(a) experimental FD transceiver



(b) improvised RC system

Fig. 2. The main components of the laboratory setup used for demonstrating that the MFDR technology is practicable for detecting the radio control of an improvised explosive device simultaneously when preventing it with jamming.

*The stock keeping unit (SKU) at `http://hobbyking.com`.

III. Experimental Results

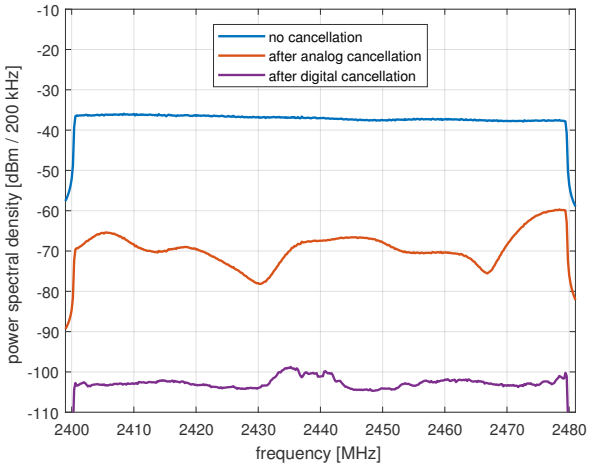
The experiments reported in this paper cover two measurement scenarios: (i) for reference, the RC transmitter was placed in the same laboratory room with the FD transceiver and the RC receivers; and (ii) for the actual proof-of-concept, the RC transmitter was placed farther away in a corridor that is adjacent to the laboratory. The respective distances from the RC transmitter to the FD transceiver were (i) 6 m with a line-of-sight and (ii) about 30 m through walls and a glass door. Consequently, received RC signal power at the FD transceiver was roughly (i) -40 dBm and (ii) -80 dBm in these scenarios, the latter being somewhat at the same level with background RFI from nearby WLAN access points and devices.

The jamming power was firstly fixed to 18 dBm that represents roughly the minimum level at which the RC receivers lose their connection everywhere in the laboratory room, where the FD transceiver is, when the RC transmitter is placed in the adjacent corridor (while, if the RC transmitter is brought to the laboratory room, jamming is effective only within a few centimeters from the FD transceiver). Secondly, the measurements were repeated by increasing the jamming power step-by-step from 0 dBm to 25 dBm with 5-dB intervals below 15 dBm and 1-dB intervals above 20 dBm, where the latter range represents an extreme case w.r.t. the SI suppression capability of the prototype MFDR. The number of recorded 50-ms signal vectors at 120-MHz sampling rate were 30 for 18-dBm jamming power and 5 for the other cases, out of which 10 and 1 representatives were respectively selected to discard vectors that had been badly cluttered by WLAN signals.

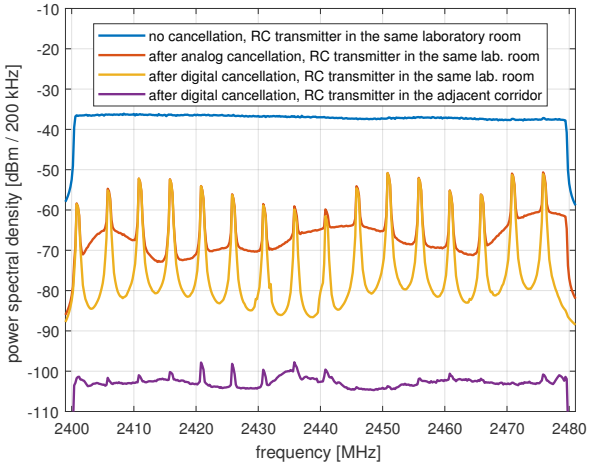
Figure 3 shows the average power spectral densities of signals measured after different cancellation stages in the receive chain of the prototype MFDR. The principal case for demonstrating the practicability of simultaneous RC transmitter detection and RC receiver jamming is shown by Fig. 3(b), whereas the reference cases turn off RC transmission in Fig. 3(a) and jamming in Fig. 3(c). The spectrum peaks with 5-MHz intervals from 2401 MHz to 2476 MHz are the RC transmitter's signal while residual SI manifests itself with rather uniform density over the whole band and RFI from WLAN access points is visible as bumps around 2437 MHz.

Figure 4 shows measured spectrograms for the duration of one full frequency hopping pattern in the AFHDS protocol (a) without digital cancellation when the RC transmitter is in the laboratory room and (b) with digital cancellation when the RC transmitter is in the adjacent corridor. The scattered narrowband signals in the spectrograms are the RC transmitter's GFSK frames and the intermittent wideband signals come from nearby WLAN access points and devices.

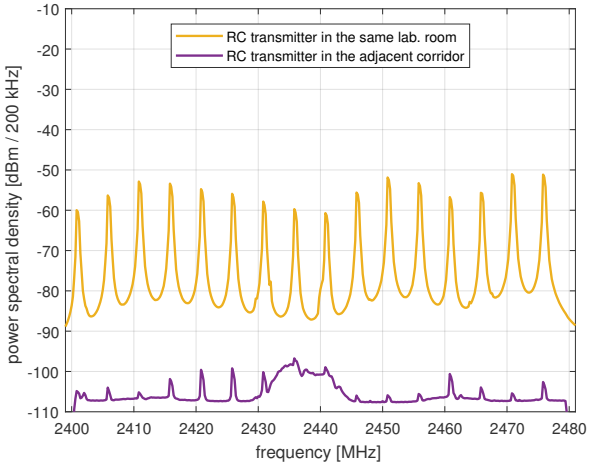
Finally, Fig. 5 shows the measured signal-to-interference-and-noise ratios for detecting the RC transmitter when jamming power is increased step-by-step from 0 dBm to 25 dBm. Each data point in this numerical result is estimated from just a single representative signal vector due to which there is significant random variance between successive points, especially with above 20-dBm jamming power levels.



(a) only SI signal

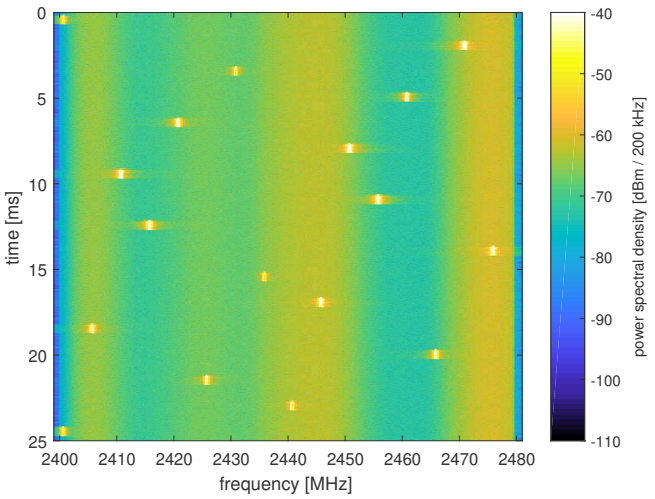


(b) both signals

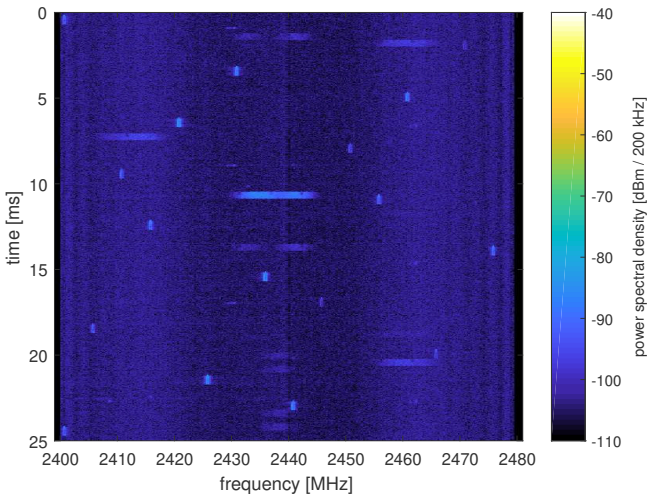


(c) only RC signal

Fig. 3. The measured power spectral densities of different signal components at the receive chain of the prototype MFDR when the transmitted jamming power is set to 18 dBm. In this experiment, when the RC transmitter was in the adjacent corridor, jamming was effective everywhere in the laboratory room while the RC transmission could be also detected after SI cancellation.



(a) after analog cancellation, RC transmitter in the same lab. room



(b) after digital cancellation, RC transmitter in the adjacent corridor

Fig. 4. The measured spectrograms at the input of the prototype MFDR when the output jamming power is set to 18 dBm. The frequency-hopping RC signal is clearly visible in both plots (even without digital cancellation if the RC transmitter is in the same room with the FD transceiver).

IV. Discussion and Conclusion

Figures 3(b) and 4(b) prove that an MFDR can successfully detect attempts to trigger improvised explosive devices while simultaneously also preempting them, because the RC transmission is visible in the measured data at the same time that the RC receivers are jammed to become inoperable. Consequently, Fig. 5 explains that, below 15-dBm jamming power, the detection performance was mainly limited by the background RF interference of the ISM band while the residual SI becomes the primary factor above 20-dBm jamming power in our laboratory setup. One should also note that the signal detection and jamming schemes used in this study are very basic ones. Thus, major performance gain can be obtained with properly optimized schemes. As for detection, our results measure only signal powers while exploiting knowledge about the correlation properties and structure of the RC signal would allow detection at much lower power levels. Likewise, the jamming signal could be tailored in advance or adapted responsively to be much more effective against the RC receivers.

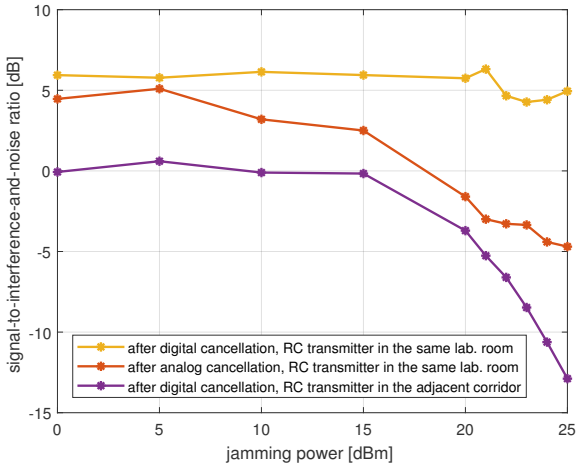


Fig. 5. The measured signal-to-interference-and-noise ratios at the input of the experimental FD transceiver when attempting to detect the RC transmission from residual self-interference and background WLAN interference.

References

[1] 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.

[2] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Communication Surveys and Tutorials*, vol. 17, no. 4, pp. 2017–2046, Q4 2015.

[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, 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.

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

[6] 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.

[7] J. Mietzner, P. Nickel, A. Meusling, P. Loos, and G. Bauch, "Responsive communications jamming against radio-controlled improvised explosive devices," *IEEE Communications Magazine*, vol. 50, no. 10, pp. 38–46, Oct. 2012.

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

[9] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y.-S. 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.

[10] D. Korpi, M. Heino, C. Icheln, K. Haneda, and M. Valkama, "Compact inband full-duplex relays with beyond 100 dB self-interference suppression: Enabling techniques and field measurements," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 2, pp. 960–965, Feb. 2017.