Riihonen, Taneli; Korpi, Dani; Turunen, Matias; Peltola, Tatu; Säikanmaki, Joni; Valkama, Mikko; Wichman, Risto

Military Full-Duplex Radio Shield for Protection Against Adversary Receivers

Published in:
2019 International Conference on Military Communications and Information Systems, ICMCIS 2019

DOI:
10.1109/ICMCIS.2019.8842696

Published: 01/05/2019

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Military Full-Duplex Radio Shield for Protection Against Adversary Receivers

Taneli Riihonen[1], Dani Korpi[1], Matias Turunen[1], Tatu Peltola[2],
Joni Saikanmäki[1], Mikko Valkama[1], and Risto Wichman[2]

[1]Faculty of Information Technology and Communication Sciences, Tampere University, Finland
[2]Aalto University School of Electrical Engineering, Helsinki, Finland
e-mail: taneli.riihonen@tuni.fi

***Abstract*—This paper provides experimental results regarding an emerging physical-layer concept within the field of military communications, viz. *the full-duplex 'radio shield'*, by building on the recently discovered full-duplex technology that allows an individual radio device to simultaneously transmit and receive (STAR) on the same spectrum. Its basic idea is to protect the surroundings of a radio device by broadcasting powerful jamming while successfully receiving tactical transmissions on overlapping frequencies. The jamming creates a protective dome of interference around such a military full-duplex radio (MFDR). The experimental results reported herein prove that the radio shield yields a large SINR advantage against interception, even though a fully practical full-duplex radio prototype with residual self-interference is used. Moreover, we show that the prototype radio shield is capable of preventing the control of improvised explosives or rogue drones while simultaneously receiving tactical signals. Therefore, the full-duplex radio shield can give armed forces a significant technical lead over an enemy by preventing it from using the frequency band for offensive purposes.**

I. Introduction

In the fields of non-military wireless communications, the so-called inband full-duplex (IBFD) radio technology has been recently receiving a significant amount of attention [1]–[4]. Its basic premise is to allow each individual radio device to transmit and receive simultaneously on the same frequency band, which naturally results in a twofold improvement in spectral efficiency over time-division or frequency-division duplex (TDD or FDD) systems. The main challenge in implementing such IBFD, or just full-duplex (FD), devices is the own transmit (TX) signal, which is in this case a powerful self-interference (SI) source for the receiver (RX) chain. Nevertheless, many demonstrator implementations already exist that can suppress the SI by a sufficient amount [5], [6].

However, what still remains a largely unknown aspect of the IBFD technology are its potential applications in *defense and security* [7]. While the improvement in spectral efficiency is important in itself also in tactical networks [8], [9], military full-duplex radios (MFDRs) can give an advantage also by other means through electronic warfare, as we have envisioned at a concept level [10], [11] and recently demonstrated in a laboratory environment under limited transmit power [12].

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."

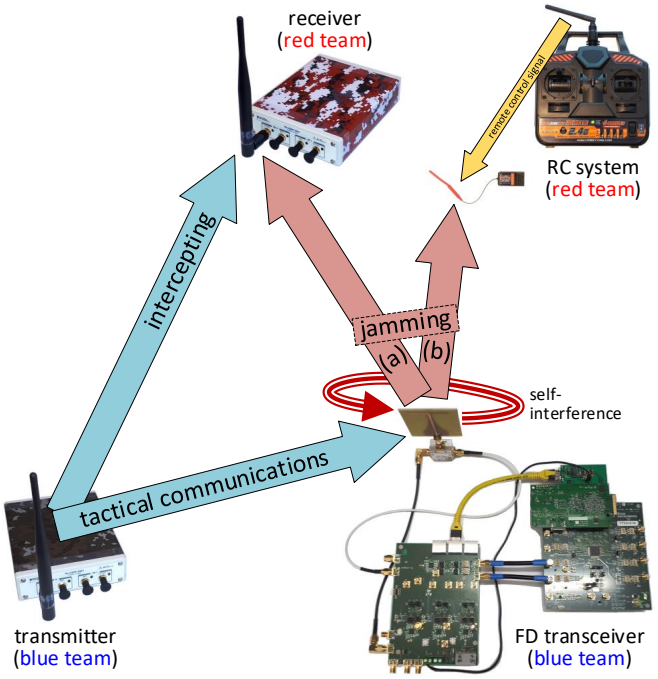


Fig. 1. A sketch of the considered battlefield scenario, where the blue team exploits an in-band full-duplex (FD) transceiver as a 'radio shield' by jamming the red team's radio receivers while receiving tactical communication signals.

In this work, we perform a measurement-based evaluation of the specific scenario depicted in Fig. 1, where the IBFD capability is used for defensive purposes by generating a *'radio shield'*. In particular, the blue team's MFDR transmits jamming while receiving a tactical communication waveform from their own distant transmitter, thereby (a) preventing the interception of the transmission within its vicinity, ergo a protective radio shield. On the side, we also evaluate how effectively the jamming signal transmitted by the blue team's MFDR transceiver performs in (b) preventing the activation of an improvised explosive device [13], [14], consisting of a radio control (RC) transmitter–receiver pair. Furthermore, due to the off-the-shelf RC components in use, the results apply also to related anti-drone applications [15] to some extent.

II. Laboratory Setup

We implemented an experimental setup in an indoor laboratory room operating at the 2.4-GHz industrial, scientific, and medical (ISM) band. Hence, transmit power must be very limited in experiments, but the short link distances somewhat compensate for the gap w.r.t. authentic electronic warfare.

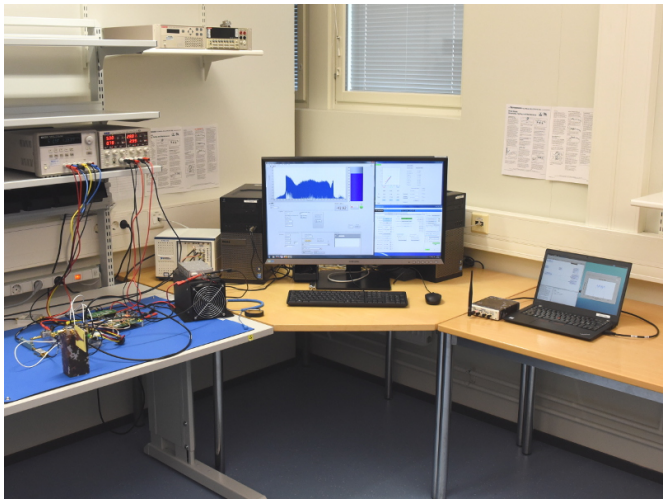
A. Blue Team's Equipment

The tactical communications link of the blue team consists of a radio transmitter and a FD transceiver prototype, both of them depicted in Fig. 2(a). The objective of the FD transceiver is to successfully receive the signal from the own transmitter, while preventing the red team's receivers from operating.

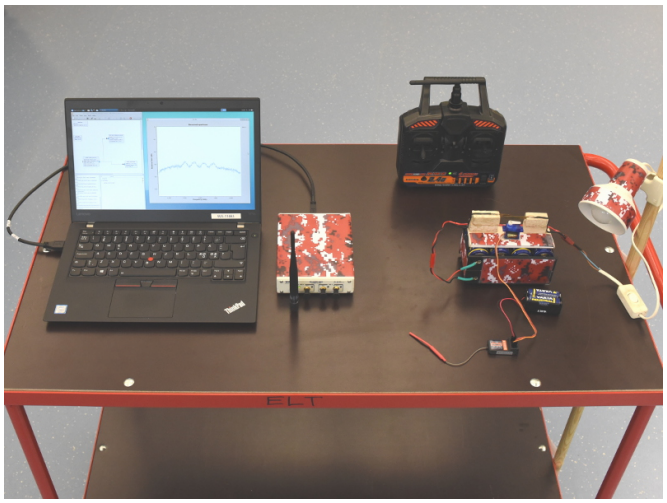
1) Tactical Radio Transmitter: The transmitter of the blue team is a National Instruments (NI) USRP-2901 transceiver, controlled with the GNU Radio software toolkit, and it is visible on the right edge of Fig. 2(a). The transmit signal follows the soldier radio waveform (SRW) from [16]–[18], essentially relying on Gaussian minimum-shift keying (GMSK) modulation. To implement a wideband tactical radio link, the transmit signal consists of four adjacent GMSK carriers, each being 1.2 MHz in bandwidth. As a result, the overall transmit signal bandwidth is 4.8 MHz. As for the parameters of the individual carriers, the symbol rate is 1.75 MHz with binary symbols (i.e., the total bit rate is 7 Mbit/s), the bandwidth–time product is 0.1, and the modulation index is $1/2$.

2) Full-Duplex Transceiver: The recipient party of the blue team's tactical link is the prototype FD transceiver visible on the left edge of Fig. 2(a). The basic transceiver operations are handled by the NI PXIe-5645R vector signal transceiver (VST), while the SI cancellation required for successful FD operation is executed in three separate stages. Firstly, to facilitate simultaneous transmission and reception on a single shared antenna, the TX and RX ports are connected to the antenna via a circulator. It is a passive device that provides roughly 30 dB of isolation between the transmitter and the receiver [5]. After this, a three-tap RF canceller is used for further SI suppression [19]. The RF canceller utilizes the transmitter output signal to regenerate the SI observed at RX input and is usually capable of suppressing the SI by 40–50 dB [5], [19]. After this, the remaining signal is fed to the RX port of the VST and recorded for further digital cancellation. This final cancellation stage is performed with an adaptive nonlinear canceller, reported in detail in [2]. Altogether, the prototype FD device can suppress the SI by 90–100 dB.

After SI cancellation, the signal is matched to the blue team's known tactical signal for signal-to-interference-plus-noise ratio (SINR) estimation. For this, the RX signal is equalized that involves time and frequency synchronization with channel estimation, after which the noise-plus-interference component is calculated by subtracting the estimated useful signal from the overall RX signal. Due to the FD operation, the SINR is reduced by the residual SI, in addition to the receiver noise. Consequently, the obtained results correspond to a fully practical scenario, as they inherently include also the prevalent downside of FD operation, i.e., the residual SI.



(a) the blue team's equipment



(b) the red team's equipment

Fig. 2. The main components of the laboratory setup used for demonstrating that full-duplex technology is practicable for simultaneously receiving tactical communications and transmitting jamming against adversary receivers.

B. Red Team's Equipment

In this work, the red team engages in two adversary activities: intercepting the tactical transmissions of the blue team, and remotely operating a radio-controlled (RC) improvised explosive device. The effectiveness of the blue team's radio shield is evaluated against both of these activities.

1) Receiver for Signals Intelligence: The intercepting receiver of the red team is an NI USRP-2901 software-defined radio, controlled also with the GNU Radio software toolkit. For the purposes of this study, it is assumed that the red team knows the center frequency at which the blue team is operating, even though in some of the measurement examples the blue team's tactical waveform is actually not detectable due to the jamming. The effectiveness of the interception is determined by recording the received waveform and estimating the SINR of the blue team's transmission following a similar procedure as for the blue team's FD transceiver.

2) Improvised Radio Control System: An external consultant has designed and implemented the red team's RC system in order to guarantee scientific objectivity by presenting us an independent simulated adversary. The system represents a scenario, where the red team has improvised a remote trigger system for explosive devices using off-the-shelf consumer electronics as shown on the right in Fig. 2(b). The components cost in total at most 20–30 euros in an online store (with shipping). Similar electrical components could be scavenged from any common radio device such as an RC toy, a multicopter, a cellular phone, a personal mobile radio, a baby monitor, a wireless doorbell, a pager, a garage door opener, etc.

In particular, the red team uses an inexpensive AFHDS ("automatic frequency hopping digital system") RC transmitter (viz. HK-T4A-M2*) to control remotely an improvised explosive device that is equipped with a compatible RC receiver (viz. HK-T6A-V2*). Both of them are based on AMICCOM A7105 wireless transceiver chips. In the AFHDS protocol, the 2.4-GHz ISM band is divided into 500-kHz subbands and each transmitter cycles frame-by-frame through a frequency hopping pattern of 16 subbands. For the specific radios at hand, the cycle is the following:

$$2407.0 \to 2447.0 \to 2412.0 \to 2452.0 \to 2427.0 \to 2467.0 \to 2422.0 \to 2462.0 \to 2432.0 \to 2472.0 \to 2417.0 \to 2457.0 \to 2429.5 \to 2442.0 \to 2437.0 \to 2419.5 \to 2407.0 \text{ [MHz]}.$$

Each frame is modulated by uncoded binary Gaussian frequency-shift keying (GFSK) with about 200-kHz deviation.

The laboratory setup employs a 12-V LED light for safely indicating detonation instead of an electric blasting cap. The improvised RC system turns on the light bulb, i.e., sets off a blasting cap, using a HexTronik micro servo (HXT900*) that bends a conductive metal strip so that it touches another one and current flows from a 12-V battery pack to the LED light. A separate 6-V battery pack supplies power to the receiver.

III. Experimental Results

In the experiments, the following scenarios are considered.

- The blue team protects its tactical link by creating a radio shield with a 5-MHz jamming signal at the same subband.
- The blue team protects and hides its tactical link by creating a radio shield with a 80-MHz jamming signal.
- The blue team prevents the activation of an improvised explosive device (or the control of a rogue drone) while maintaining its own tactical communications capability.

In the case of 5-MHz jamming, the power spectral density over the blue team's actual transmit signal is much higher and the jamming is consequently more effective, but the opposing team will inherently be aware that the blue team is using the specific tactical subband for some purpose. Therefore, we also consider a scenario, where a very wideband jamming signal is used, as it can hide the existence of the blue team's tactical link altogether. However, the unavoidable drawback of 80-MHz jamming is the fact that the overall transmit power must be increased to hide the much narrower information signal.

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

TABLE I
Essential Measurement Parameters

Parameter		Value
Center frequency		2.44 GHz
Blue team	(a) Tactical waveform	four-carrier GMSK
	Tactical bandwidth	4.8 MHz
	Tactical TX power	$\{-5, 0, 5, 10, 15\}$ dBm
	RX sampling rate	120 MHz
	(b) Jamming waveform	band-limited noise or RC-specific
	Jamming bandwidth	5 MHz or 80 MHz
	Jamming power	$\{-10, -5, 0, 5, 10, 15, 20\}$ dBm
	TX sampling rate	(a) 14 MHz and (b) 120 MHz
Red team	RC waveform	GFSK with frequency hopping
	RX sampling rate	14 MHz

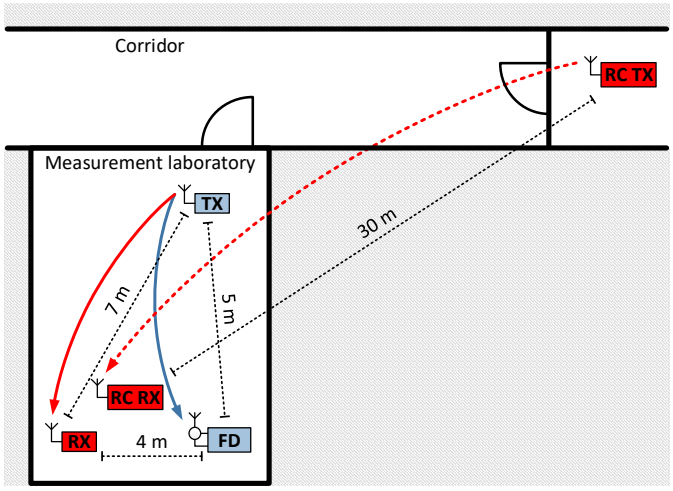
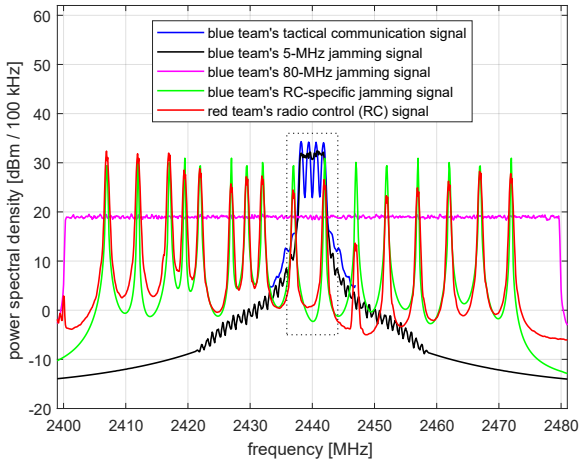


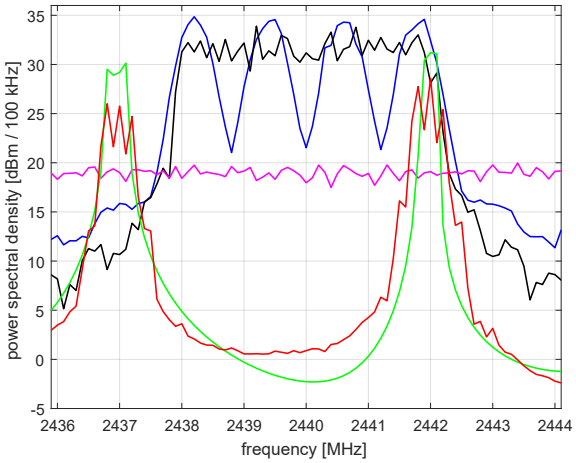
Fig. 3. Diagram of the relative locations of the devices in the measurements. The RC receiver's operation was tested by moving it all around the room.

Lastly, the operation of the improvised explosive device's RC receiver is prevented using a waveform that is tailored to the characteristics of the RC transmission. Namely, since the RC system utilizes a frequency-hopping control signal, the receiver is most effectively blocked by only transmitting on the specific ISM subbands used by the RC transmitter. Further gain could be achieved by not jamming continuously on the subbands but following synchronously the hopping pattern in the time–frequency plane. Moreover, the blue team should at the same time be capable of maintaining its tactical communications link, which is also evaluated in the forthcoming results.

All of the above cases are measured with various tactical transmit powers and jamming powers, and the essential measurement parameters are listed in Table I. Furthermore, the relative positions of the various nodes are illustrated in Fig. 3. The qualities of the different communications links are determined based on the SINRs, which are estimated from the recorded RX signals at the blue team's FD transceiver and at the red team's intercepting receiver using the blue team's tactical transmission as a known pilot signal.



(a) overview of the whole ISM band



(b) zoom-in to the tactical signal band

Fig. 4. Spectra of the transmitted signals in the laboratory experiments when all transmit powers are normalized to 18 dBm. The RC signal has been recorded over-the-air in the small room since the RC transmitter has a fixed built-in antenna, which results in the significant frequency selectivity shown in the spectrum.

The measurement results are displayed in Figs. 4–7, where Fig. 4 illustrates the spectra of the various transmitted signals for reference, while the other figures are drawn based on the estimated receiver SINRs in the different scenarios.

In particular, Fig. 4 shows the power spectral densities (PSDs) of the relevant signals when the corresponding transmit powers are normalized to 18 dBm. The purpose of this figure is to provide an intuitive depiction of the spectral characteristics of the different jamming scenarios.

Then, Fig. 5(a) shows the SINRs of both the blue team's FD transceiver and the red team's intercepting receiver with respect to the jamming power when using an 80-MHz jamming signal for generating the radio shield. Furthermore, the SINRs are shown separately for each considered tactical TX power. Figure 5(b) shows the respective results when the blue team's FD transceiver uses the narrower 5-MHz radio shield.

Using the results of Fig. 5(a), Fig. 6(a) shows the advantage in SINR that the blue team's FD transceiver obtains over the red team's intercepting transceiver by utilizing the 80-MHz radio shield, again with respect to the jamming power. That is, the higher the blue team's SINR advantage is, the better the radio shield performs. The respective results for the 5-MHz radio shield are shown in Fig. 6(b).

Finally, Fig. 7 shows the SINR of the FD transceiver when jamming against the improvised RC system. For reference, the corresponding SINRs are also shown for the regular 5-MHz and 80-MHz jamming signals. Also note that now the SINRs are plotted against the tactical transmit power, while the different jamming powers are merely represented by curves showing the minimum, average, and maximum SINRs observed with different jamming powers.

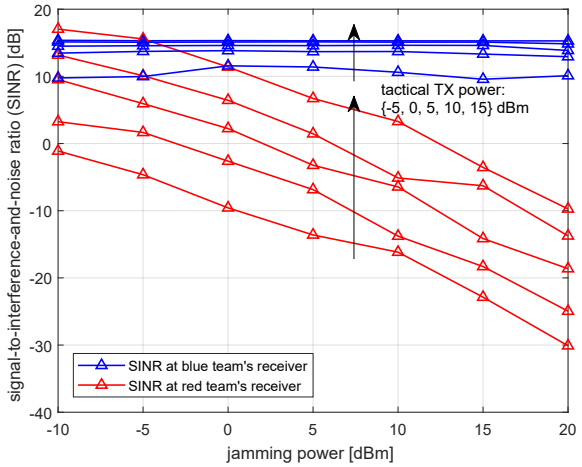
IV. Discussion on Results

Considering first the 80-MHz radio shield, it is evident from Fig. 5(a) that increasing jamming power does not affect the SINR at the blue team's FD transceiver, while it heavily reduces the SINR of the intercepting receiver. This is a very favorable result, as it confirms that the proposed radio shield is capable of protecting the tactical communications link against malicious interception, or even detection in the first place.

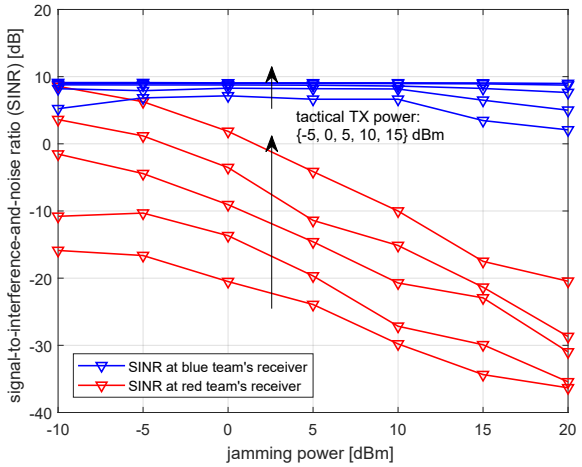
To quantify the efficacy of the jamming, let us then investigate Fig. 6(a), which shows the SINR advantage the 80-MHz radio shield provides. There, high values indicate that the radio shield is beneficial for the blue team as it ensures that the SINR of the tactical communications link is significantly higher than the SINR of the interceptor. It can be easily observed from Fig. 6(a) that increasing the jamming power improves the protective capabilities of the radio shield. Recalling that the jamming power does not affect the SINR of the blue team's FD transceiver, the jamming power can therefore be freely chosen to provide the desired SINR advantage. For instance, with the lowest considered tactical TX power and the highest jamming power, Fig. 6(a) shows the SINR advantage of the blue team to be in the order of 40 dB, which could be enough to completely secure the tactical communications link.

The above conclusions can largely be applied also to the 5-MHz radio shield, as demonstrated by Figs. 5(b) and 6(b). In other words, while the jamming power does not affect the SINR of the tactical link, it significantly reduces the red team's SINR. Therefore, as is evident from Fig. 6(b), the jamming power can be chosen such that sufficient SINR advantage over the red team's interceptor is obtained. Similar to the 80-MHz radio shield, with a high jamming power and a suitable tactical TX power, the SINR advantage can be as much as 40 dB.

Let us then finally analyze the case, where the blue team's FD transceiver jams the RC system, while maintaining the tactical communications link; the resulting SINR is shown in Fig. 7. It can firstly be observed that tailored RC-specific jamming results in a decreased tactical SINR for the blue team when compared to regular 80-MHz jamming. The spectrum of the RC-specific jamming signal shown in Fig. 4(b) provides

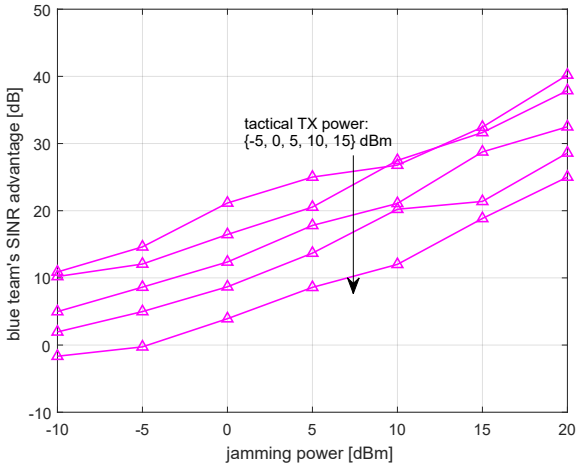


(a) 80-MHz jamming signal

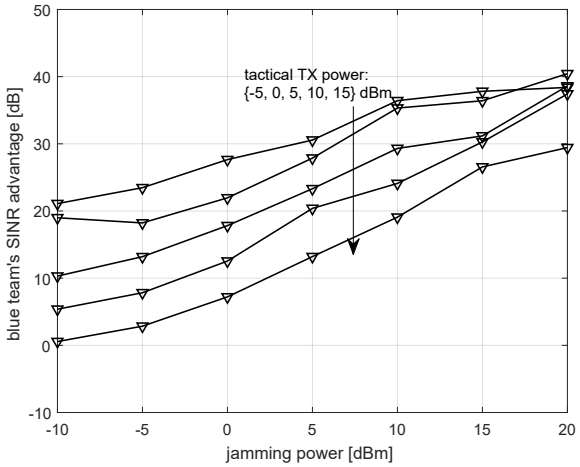


(b) 5-MHz jamming signal

Fig. 5. SINR of the tactical signal at the blue team's MFDR and at the red team's intercepting receiver with (a) 80-MHz and (b) 5-MHz radio shields.



(a) 80-MHz jamming signal



(b) 5-MHz jamming signal

Fig. 6. SINR advantage that the blue team's MFDR obtains over the red team's intercepting receiver with (a) 80-MHz and (b) 5-MHz radio shields.

some further insight into this phenomenon, as it can be observed that in this case the SI is only affecting a part of the tactical signal. This, on the other hand, was observed to be a problematic scenario for the digital SI cancellation architecture that was originally developed for the case of wideband SI signals and not modified for the present application.

However, the benefit of the tailored jamming signal is that it can successfully prevent the RC receiver's operation* using a transmit power of only 6 dBm, as opposed to the 18-dBm jamming power required when using the very wideband jamming signal [14]. The reason for this is the higher power density achieved in the frequency domain when only the subbands used by the RC transmitter are jammed. Indeed, the RC-specific jamming signal has an overall effective bandwidth of roughly 5 MHz, and therefore each frequency bin has 12 dB more power in comparison to the wideband 80-MHz signal under the same jamming power. In other words, while some 2–3 dB is lost in the SINR of the tactical link when using the tailored signal, jamming power can be reduced by 12 dB.

*Everywhere inside the measurement laboratory room shown in Fig. 3.

V. Conclusion

This paper evaluated an emerging concept in military communications systems, which utilizes full-duplex radio devices to protect the own team's transmissions against an enemy's interception attempt. Such a full-duplex device can transmit a jamming signal while receiving tactical signals on the same frequency band, thereby creating a so-called *radio shield* and preventing any nearby nodes from intercepting the transmissions. The experimental findings confirmed this, as the radio shield was shown to reduce the SINR of the intercepting node significantly below the SINR of the intended recipient. As a result, the proposed radio shield concept can give a considerable tactical advantage by ensuring secure, hidden communications between the members of one's own team.

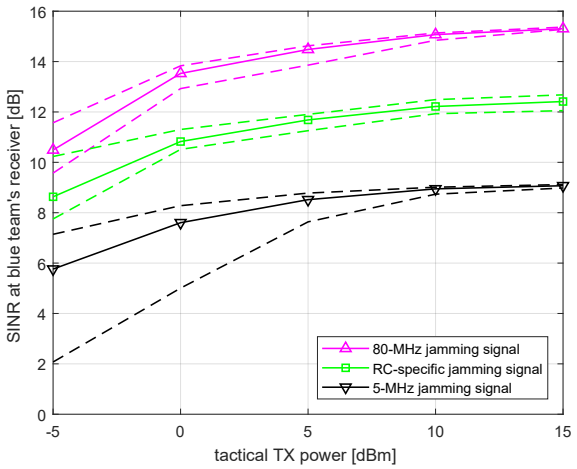


Fig. 7. SINR at the blue team's MFDR when jamming against an improvised RC system, together with the corresponding SINRs when utilizing regular 80-MHz and 5-MHz jamming signals; the latter is actually ineffective against the frequency-hopping RC signal and, thus, shown only for reference.

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

[3] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[4] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[5] 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.

[6] M. Chung, M. S. Sim, J. Kim, D. K. Kim, and C. B. Chae, "Prototyping real-time full duplex radios," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 56–63, Sep. 2015.

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

[8] B. Paul, A. Chiriyath, and D. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. 5, pp. 252–270, Dec. 2016.

[9] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, and L. Sadler, "Exploring value-of-information-based approaches to support effective communications in tactical networks," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 39–45, Oct. 2015.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] T. R. Halford, M. Johnson, S. Kim, and C. Kose, "On the design of a modern broadband communications waveform for tactical air-to-ground links," in *Proc. IEEE Military Communications Conference*, Oct. 2009.

[17] S. Kim, M. Johnson, O. W. Yeung, and D. Yin, "On the design of a modern broadband physical layer for teleoperations links," in *Proc. IEEE Military Communications Conference*, Nov. 2011.

[18] A. Blyskun, M. Johnson, S. Kim, J. Speros, G. Thatte, and D. R. Williamson, "Improving the SRW waveform via a physical layer retrofit," in *Proc. IEEE Military Communications Conference*, Nov. 2013.

[19] 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.