Full-Duplex Operation for Electronic Protection by Detecting Communication Jamming at Transmitter

Taneli Riihonen[1], Matias Turunen[1], Karel Pärlin[2], Mikko Heino[1], Jaakko Marin[1], and Dani Korpi[1]

[1]Tampere University, Finland
[2]Rantelon, Tallinn, Estonia
e-mail: taneli.riihonen@tuni.fi

***Abstract*—Inband full-duplex (IBFD) technology enables radios to simultaneously transmit and receive (STAR) on the same frequencies with the benefit of, e.g., enhanced spectral efficiency in non-military communications. In addition, there is significant potential in the IBFD concept in military applications as currently conventional time- or frequency-division half-duplex radios are used in all military applications. A military full-duplex radio (MFDR) would be capable of simultaneous integrated tactical communication and electronic warfare operations. This paper presents an application where an MFDR enables the user to successfully detect an electronic attack, i.e., jamming from an adversary, while simultaneously transmitting tactical transmissions to an ally on the same frequency channel. Successful detection enables the MFDR to gather intelligence and take countermeasures against the jamming, e.g., switching to a different carrier frequency. The experimental results reported herein prove that the radio is able to reliably detect the presence of jamming for received jamming signal powers down to -95 dBm while simultaneously transmitting to an ally at 10-dBm power level. Therefore, the full-duplex radio can give armed forces a significant technical lead over an enemy by detecting enemy jamming even when the adversary only transmits jamming during friendly transmissions.**

I. Introduction

Inband full-duplex (IBFD) radio technology has been recently a popular topic with significant interest in the research fields of non-military wireless communications [1]–[4]. Especially, IBFD enables radio devices to transmit (TX) and receive (RX) at the same frequency band simultaneously. This leads to the doubling of spectral efficiency compared to conventional time-division duplex or frequency-division duplex (TDD or FDD) systems. However, the main challenge related to IBFD, or a.k.a. just full-duplex (FD), is the strong received self-interference due to the devices' own transmit signal.

The benefits of IBFD technology in *defence and security* [5] applications are still largely unexplored as currently practically all military radios utilize conventional time- or frequency-division half-duplex (HD) transmissions for tactical communications. The improvement in spectral efficiency is important also in military networks [6], [7]. However, military full-duplex radios (MFDRs) have other promising applications in electronic warfare as we have envisioned at a concept level [8], [9] and recently demonstrated in a laboratory environment under limited transmit power and in outdoor scenarios with realistic transmission distances [10]–[12].

This research work was supported in part by the Academy of Finland and the Finnish Scientific Advisory Board for Defence (MATINE).

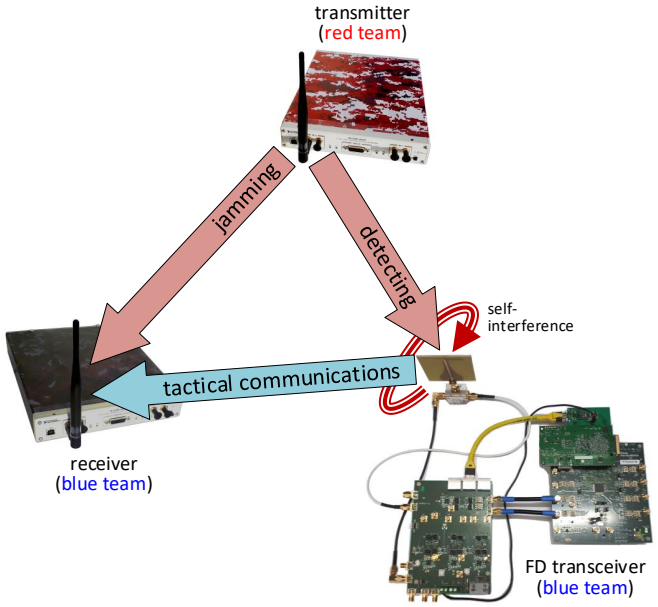
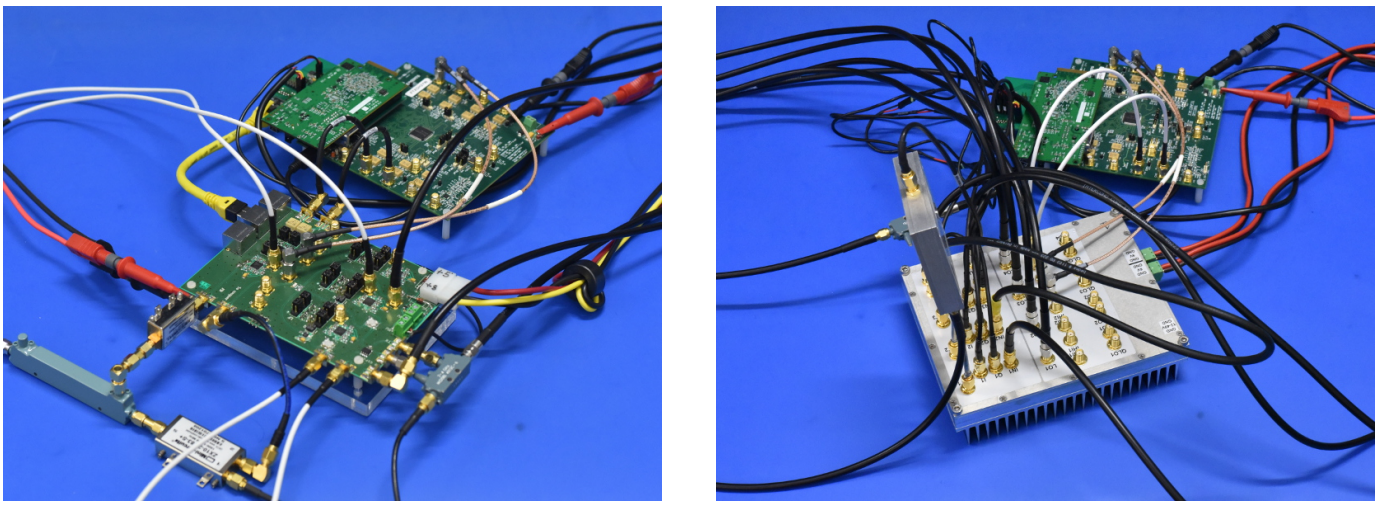


Fig. 1. A sketch of the considered battlefield scenario, where the blue team exploits an in-band full-duplex (FD) radio transceiver to detect the red team's electronic attack while transmitting tactical communication signals.

In this work, we perform a measurement-based evaluation of the novel scenario depicted in Fig. 1, where the IBFD capability is used for defensive purposes by detecting the enemy's electronic attack during the MFDR's own transmission. To the authors' knowledge, such application has not been evaluated before. In particular, the blue team's MFDR transmits tactical communications while at same time detecting if an adversary is attempting to electronically jam the signal, thereby: (a) detecting the presence of the enemy; (b) enabling to take countermeasures against the jamming; and (c) informing the team members about the attack. The experiments evaluate the detection threshold at how low levels of received jamming the MFDR is able to detect the presence of the electronic attack. The proposed method has the benefit that it is able to detect the jamming even if a smart stealth adversary stops the jamming signal whenever the MFDR itself stops transmitting.



(a) original version by TUT/TAU

(b) new revision by Rantelon

Fig. 2. The experiments were repeated with the illustrated two canceller prototypes while otherwise keeping the setup and data processing the same.

II. Laboratory Setup

We implemented an experimental over-the-air setup in a small indoor laboratory room operating at the 2.4-GHz industrial, scientific, and medical (ISM) band. Due to this reason, TX power levels were very limited in experiments, but the short link distances compensate for the difference in received power levels compared to authentic electronic warfare. Moreover, the external co-channel transmissions can cause false alarms in energy detection. The setup is very similar as in Fig. 2 of [10] and Fig. 2(a) of [11].

A. Blue Team's Equipment

The tactical communications link of the blue team consists of a FD transceiver prototype and a radio receiver, both of them depicted in Fig. 1. The objective of the FD transceiver is to successfully transmit a tactical communications signal to the receiver of the blue team while at the same time detecting possible jamming from the red team. In this paper, we focus on the capability of the FD transceiver to detect the jamming of the red team's transmitter, therefore the real receiver of the blue team was not relevant for the measurements.

The blue team's full-duplex transceiver is visible on the left edge of Fig. 2(a) in [11]. A NI PXIe-5645R vector signal transceiver (VST) is used for the basic transceiver operations. In addition, the cancellation of the SI required to detect the jamming is performed at three different stages. First, to enable full-duplex operation using a single shared antenna, a passive circulator is used to obtain around 25 dB of TX-RX isolation.

Two options for a three-tap RF canceller are tested for further SI suppression as shown in Fig. 2. The first one is the RF canceller developed in Tampere University [of Technology] (TUT/TAU) as reported in [13]. The second is a new version of the canceller, further developed by Rantelon. The Rantelon version includes a low-noise amplifier (LNA) to amplify the canceller output and feedback signal to increase the cancellation capability. The same adaptive controller from TUT/TAU was used for both models. The RF canceller is connected with a coupler to the transmitter output enabling the regeneration of the SI observed at RX input. The canceller then substracts the generated SI signal from the RX signal. Both models of cancellers are usually capable of suppressing the SI by 40–50 dB with more details presented in [13] and [14].

After the RF canceller, the remaining RX signal is recorded with the VST and adaptive nonlinear digital cancellation is performed to cancel the remaining self-interference, described in detail in [2]. Altogether, the prototype FD device can suppress the SI by 90–110 dB.

After SI cancellation, the received noise power of the FD transceiver for the full measurement bandwidth is then measured for the defined integration time. The received noise power is then compared to the expected power level without any jamming to detect the presence of an electronic attack with varying detection threshold.

B. Red Team's Equipment

In this work, the red team engages in the adversary activity of broadcasting a jamming signal that is also propagated to the FD transceiver of the blue team. The transmitted power level of the jammer is varied and the received jamming power level in the blue team's FD transceiver is evaluated.

The transmitter used for the jamming is an NI USRP-2954R software-defined radio, controlled with LabVIEW. In this study, it is assumed that the red team knows the center frequency and bandwidth at which the blue team is operating, which is feasible by monitoring the tactical transmissions. The TX power of the jammer is controlled with a variable attenuator so that the starting received jamming signal power measured from the antenna of the FD transceiver is -68 dBm. The power is then decreased down to -99 dBm with 1 dB steps to see the threshold of the detection of the electronic attack. The jamming signal is band-limited Gaussian noise with a bandwidth of 1.4 MHz or 5 MHz depending on the bandwidth used by the blue team.

TABLE I
ESSENTIAL MEASUREMENT PARAMETERS

Parameter		Value
Center frequency		2.44 GHz
Blue team	Tactical waveform	one-carrier or four-carrier GMSK
	Tactical bandwidth	1.2 MHz or 4.8 MHz
	Tactical TX power	10 dBm
	RX sampling rate	40 MHz (8 MHz after processing)
Red team	Jamming waveform	band-limited noise
	Jamming bandwidth	1.4 MHz or 5 MHz
	Jamming RX power	$\{-99, -98, \ldots, -68\}$ dBm
	TX sampling rate	40 MHz

III. EXPERIMENTAL RESULTS

The transmit signal of the FD transceiver follows the soldier radio waveform (SRW) from [15]–[17], essentially utilizing the Gaussian minimum-shift keying (GMSK) modulation. The same waveform was also used in [10] and [11]. To estimate a wideband tactical radio link, the transmit signal has four adjacent GMSK carriers with each having a bandwidth of 1.2 MHz, resulting in overall transmit signal bandwidth of 4.8 MHz. Also, a narrowband signal with only one subcarrier is considered resulting in 1.2 MHz of bandwidth. For the individual carriers, a symbol rate of 1.75 MHz is used with binary symbols (i.e., the total bit rate is 7 Mbit/s). The bandwidth–time product is 0.1, while the modulation index is 1/2. The transmit power is kept constant at 10 dBm for all measurement cases.

In the experiments, the following scenarios are considered:

- The blue team transmits an SRW signal with a bandwidth of 1.2 MHz and the red team transmits a 1.4-MHz jamming signal at the same carrier frequency.
- The blue team transmits an SRW signal with a bandwidth of 4.8 MHz and the red team transmits a 5-MHz jamming signal at the same carrier frequency.
- The blue team's FD transmitter is idle and the red team transmits a 1.4-MHz jamming signal.
- The blue team's FD transmitter is idle and the red team transmits a 5-MHz jamming signal.

The two cases where the blue team's FD transmitter is idle (half-duplex operation) are measured as a reference for comparison to see how much the residual SI in the first two cases affects the attack detection probability.

All of the above cases are measured with various jamming powers for the red team transmitter, and the essential measurement parameters are listed in Table I. Figure 3 illustrates the power spectral densities (PSDs) of the relevant transmitted and received signals at the blue team's FD transceiver.

The quality of the blue team's jamming detection is characterized by calculating the detection probability as a function of the false alarm probability with various levels of received jamming powers. Conventional energy detection is used for detection of jamming by comparing the received energy with a

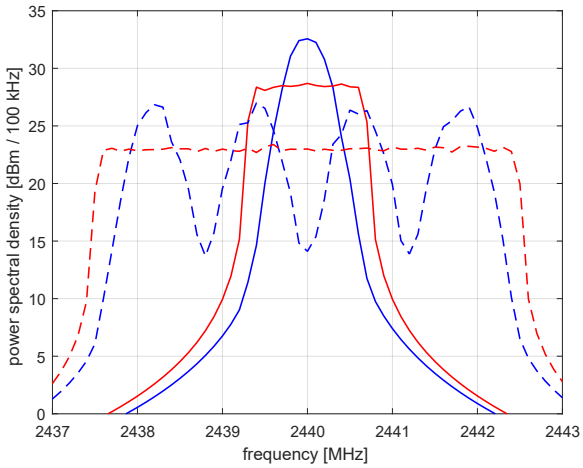


Fig. 3. Spectra of the transmitted signals in the laboratory experiments when all transmit powers are normalized to 10 dBm. In the actual measurements, the received jamming power was calibrated at chosen levels at the receiver antenna after a variable attenuator and 56-dB path loss over 1 m distance.

preset threshold. The detection problem is a binary hypothesis test with the two options:

$$H_1 : y[n] = s[n] + w[n], \tag{1}$$
$$H_0 : y[n] = w[n], \tag{2}$$

where $s[n]$ is the jamming signal and $w[n]$ the received noise and residual SI signal. The used test statistic is defined as

$$\Lambda = \sum_{n=1}^{N} |y[n]|^2 \tag{3}$$

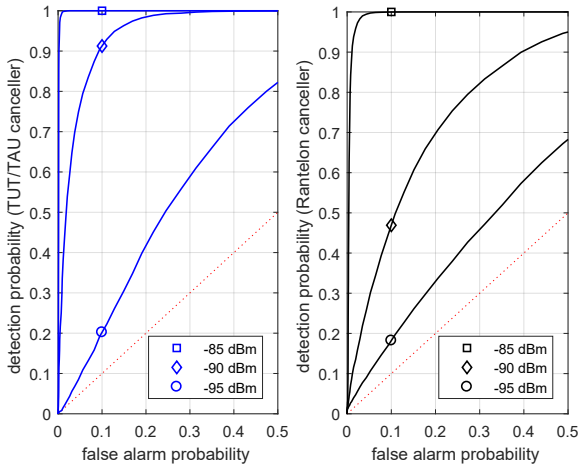
where $N = f_s T$ is the number of samples depending on the integration time T and sampling rate f_s. Thus, the probabilities for detection P_D and false alarm P_{FA} are obtained as

$$P_D = \text{Prob}[\Lambda > \lambda \,|H_1], \tag{4}$$
$$P_{FA} = \text{Prob}[\Lambda > \lambda \,|H_0], \tag{5}$$

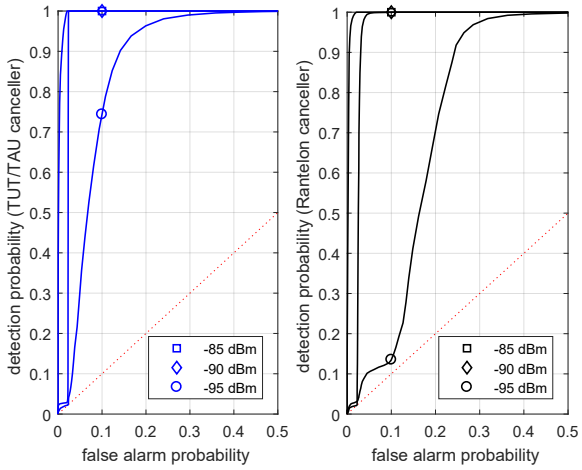
which are determined empirically from the recorded measurement data after digital cancellation.

The threshold λ is then varied from very small values to very high values to obtain the relation between the probability of detection and the probability of false alarm, i.e., the receiver operating characteristic curve (ROC). The ROC curves for the scenarios with 1.2-MHz tactical transmission bandwidth are shown in Fig. 4 and with 4.8-MHz tactical bandwidth in Fig. 5 with various power levels. The integration time for the curves is 100 µs. The dashed diagonal line in the figures represents purely random guess.

The area under the ROC curve (AOC) is a widely used measure for detector performance. In particular, it measures the probability that jamming detection will rank a randomly chosen positive event higher than a randomly chosen negative one. Thus, Fig. 6 shows the AOC as a function of the received jamming power and Fig. 7 shows the AOC as a function of the integration time for each measurement scenario.

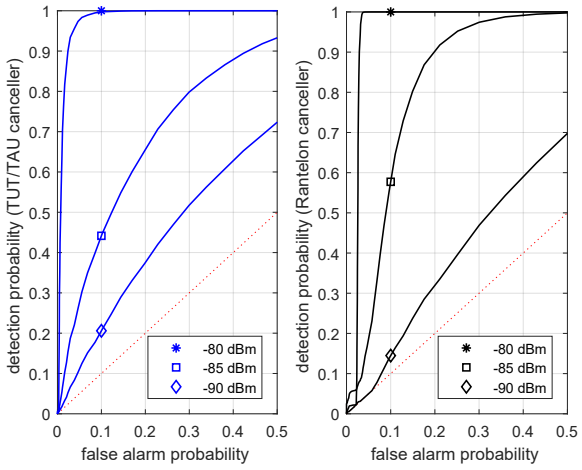


(a) with tactical transmission (full-duplex mode)

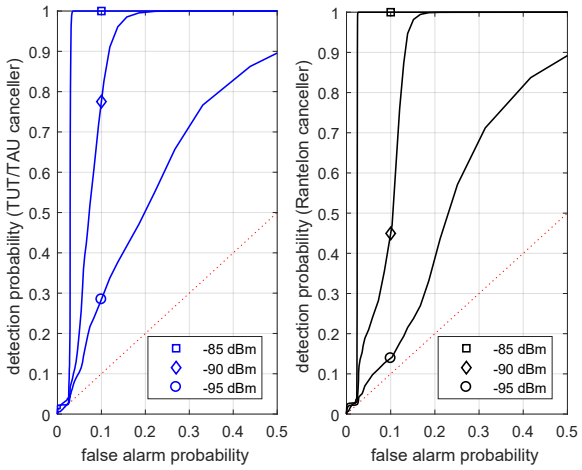


(b) no tactical transmission (half-duplex mode)

Fig. 4. Receiver operating characteristics with a single GSMK carrier (1.2-MHz tactical TX under 1.4-MHz jamming) and 100-µs integration time.



(a) with tactical transmission (full-duplex mode)



(b) no tactical transmission (half-duplex mode)

Fig. 5. Receiver operating characteristics with four GMSK carriers (4.8-MHz tactical TX under 5.0-MHz jamming) and 100-µs integration time.

IV. Discussion on Results

Considering the case without the FD transmitter's own tactical transmission (i.e., half-duplex operation) in Fig. 4(b), it is evident that the detection is possible with high detection probability even for the low received jamming power level of -95 dBm with the TUT/TAU canceller. However, the ability of the Rantelon canceller to detect the -95-dBm jamming power level is not as good as with the TUT/TAU canceller. Without the residual SI, the LNA in the Rantelon canceller is unnecessary and adds noise for the signal passing through making detection of low power signals more difficult. For the wider bandwidth of 4.8 MHz in Fig. 5(b), the ROC curves are lower for both cancellers. This is due to higher integrated noise power for the wider bandwidth. In the overall AOC curves in Fig. 6, the same conclusion is valid: the TUT/TAU canceller performs better in the conventional HD mode.

With the tactical transmission on (i.e., FD operation), the detection probability is worse due to the residual SI increasing the noise floor of the receiver as seen in Figs. 4(a) and 5(a) for both bandwidths. However, both cancellers are able to detect at minimum 1.4-MHz jamming with power of -95 dBm and 4.8-MHz jamming with power of -90 dBm. When comparing the two cancellers, it is seen that the Rantelon canceller works slighty worse compared to the TUT/TAU canceller for lower bandwidth in Fig. 4(a) and slightly better in Fig. 5(a). This is due to the Rantelon canceller being optimized to operate for the whole ISM band of 80 MHz for drone monitoring and jamming. It is evident also from the AOCs in Fig. 6 that the Rantelon canceller performs better for the wider bandwidth.

Figure 7 indicates that, without the tactical transmission, the required integration time for the AOC to saturate is very low, under 25 µs. With the tactical transmission, the required integration time increases especially for the 4.8-MHz case. This is due to the increased total SI and noise power for the wider bandwidth making the detection of the jamming power with constant power density more difficult.

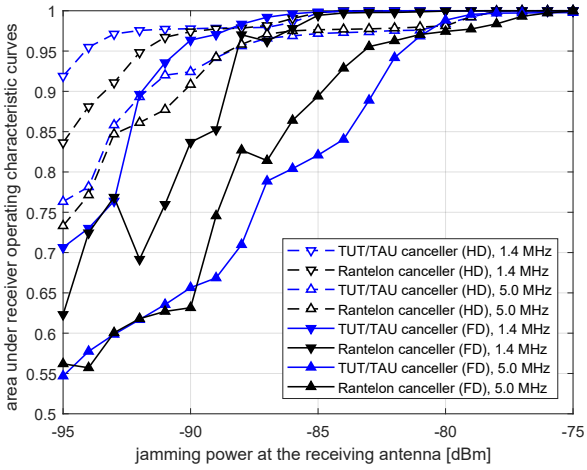


Fig. 6. The effect of jamming power on the performance of jamming detection when integration time is 100 µs.

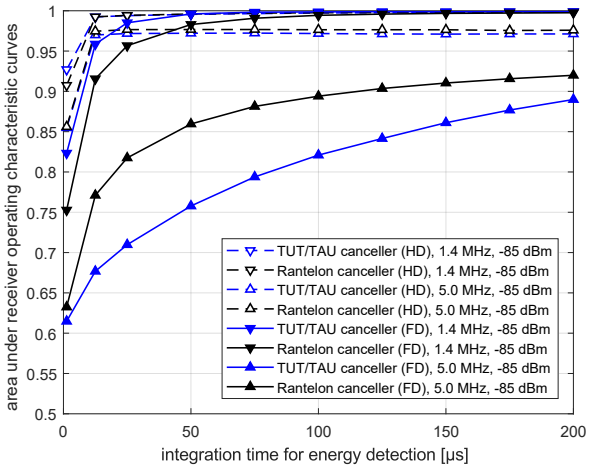


Fig. 7. The effect of integration time on the performance of jamming detection.

V. Conclusion

This paper evaluated a novel concept where a military full-duplex radio is able to detect the presence of jamming while simultaneously transmitting to an ally on overlapping frequencies. This enables the transceiver to gather intelligence about the enemy and possibly take countermeasures against the jamming giving the user a tactical advantage. The experimental findings confirmed that with two versions of the RF canceller, the system was able to detect the presence of jamming down to low received jamming power of -95 dBm while simultaneously transmitting tactical communications at 10-dBm power level. The system was verified both with 1.2-MHz and 4.8-MHz tactical communication signals.

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, Sept. 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] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] ——, "Military full-duplex radio shield for protection against adversary receivers," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[12] J. Saikanmäki, M. Turunen, M. Mäenpää, A.-P. Saarinen, and T. Riihonen, "Simultaneous jamming and RC system detection by using full-duplex radio technology," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[13] 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.

[14] 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, Sept. 2016.

[15] 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.

[16] 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.

[17] 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.