TAMPERE UNIVERSITY OF TECHNOLOGY

On the prospects of full-duplex military radios

Citation
Riihonen, T., Korpi, D., Rantula, O., & Valkama, M. (2017). On the prospects of full-duplex military radios. In *2017 International Conference on Military Communications and Information Systems, ICMCIS 2017* IEEE. https://doi.org/10.1109/ICMCIS.2017.7956490

Year
2017

Version
Peer reviewed version (post-print)

Link to publication
TUTCRIS Portal (http://www.tut.fi/tutcris)

Published in
2017 International Conference on Military Communications and Information Systems, ICMCIS 2017

DOI
10.1109/ICMCIS.2017.7956490

Copyright
This publication is copyrighted. You may download, display and print it for Your own personal use. Commercial use is prohibited.

Take down policy
If you believe that this document breaches copyright, please contact cris.tau@tuni.fi, and we will remove access to the work immediately and investigate your claim.

Download date:21.10.2020

On the Prospects of Full-Duplex Military Radios

Taneli Riihonen*, Dani Korpi†, Olli Rantula*, and Mikko Valkama†

*Department of Signal Processing and Acoustics, Aalto University School of Electrical Engineering, Helsinki, Finland
†Laboratory of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
e-mail: {taneli.riihonen, olli.rantula}@aalto.fi, {dani.korpi, mikko.e.valkama}@tut.fi

***Abstract*—In-band full-duplex (FD) operation can be regarded as one of the greatest discoveries in civilian/commercial wireless communications so far in this century. The concept is significant because it can as much as double the spectral efficiency of wireless data transmission by exploiting the new-found capability for simultaneous transmission and reception (STAR) that is facilitated by advanced self-interference cancellation (SIC) techniques. As the first of its kind, this paper surveys the prospects of exploiting the emerging FD radio technology in military communication applications as well. In addition to spectrally efficient two-way data transmission, the STAR capability could give a major technical advantage for armed forces by allowing their radio transceivers to conduct electronic warfare at the same time when they are also receiving or transmitting information signals at the same frequency band. After providing a detailed introduction to FD transceiver architectures and SIC requirements in military communications, this paper outlines and analyzes some potential defensive and offensive applications of the STAR capability.**

I. Introduction

In-band full-duplex (FD) wireless communication [1] means that a radio device is receiving and transmitting information signals at the same time and at the same center frequency, as opposed to half-duplex (HD) operation. Especially, to avoid misconception, one should note that neither time-division duplexing nor frequency-division duplexing (TDD nor FDD) is considered real FD operation in the modern terms despite they allow simultaneous two-way conversation, because the perspective is shifted to spectrum usage at the physical layer. While the promising civilian/commercial applications of the FD radio technology have already been widely studied, this paper considers its novel military applications in particular.

In general, when extending beyond the pure communication context, prospective military FD radios will have the progressive capability for simultaneous transmission and reception (STAR) by which they can conduct electronic warfare at the same time when they are also using the same frequency band for communication or perform an electronic attack with simultaneous signals intelligence. It is quite obvious that, by utilizing the STAR capability, armed forces could gain a major technical advantage over an opponent that does not possess similar technology. However, viable FD operation relies on efficient self-interference cancellation (SIC) [2], because the strong electromagnetic field radiated by a transceiver leaks back to its own receiver circuitry interfering with the reception of signals-of-interest that are usually weak.

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."

Scientific discourse on the military applications of the full-duplex radio technology is in its absolute infancy in the open literature, if not still practically unborn. To the best of our knowledge, so far the only explicit and elaborate reference to full-duplex military radios is the following passage:

> "In military applications, jammers flood the airwaves with strong transmission to prevent other devices from communicating (e.g., cell phones to activate improvised explosive devices). But as it does so, it also prevents its own radios from transmitting, making communication impossible. With SIC [self-interference cancellation] technology, the military could continue to disrupt enemy communications and at the same time listen to its own troop communications, thus saving lives in the field." [2]

By this paper, we aim at bringing forward the prospects of full-duplex military radios in order to induce more interest in this emerging research topic in the scientific community.

Earlier literature has discussed only two specific concepts that implicitly relate to military systems, namely radars [1] and so-called physical-layer security, although studies on the latter almost never explicitly mention the potential military use. In particular, continuous-wave radars are inherently based on the STAR capability, and the general field of information theory has recently begun to analyze the capacity of communication links, where a FD receiver hinders eavesdropping by simultaneously broadcasting a jamming signal [3].

In what follows, we first present an overview of general FD transceiver architectures developed originally for civilian/commercial wireless communications and extrapolate their requirements for military radios. While modern FD radios can achieve about 100 dB of SIC [4], their effective use in military systems likely needs much more and, moreover, usage in battlefield sets special requirements for extreme robustness to electronic warfare. Thus, practical operation environments are rather different from a laboratory where the FD technology is already demonstrated to be feasible for non-military use.

We then analyze the potential defensive and offensive applications of full-duplex military radios. The STAR capability is used for defense by protecting the radio operator from an opponent. In fact, the scenario postulated in [2] (cf. the excerpt above) is an example protective application. In the offensive applications, the radio operator uses the STAR capability for attacking an opponent. For example, it is reasonable to envision that an attacker could send jamming to force an opponent to increase its transmission power and, thus, facilitate its own simultaneous signals intelligence, e.g., locating used frequency band and transmitters or intercepting communication.

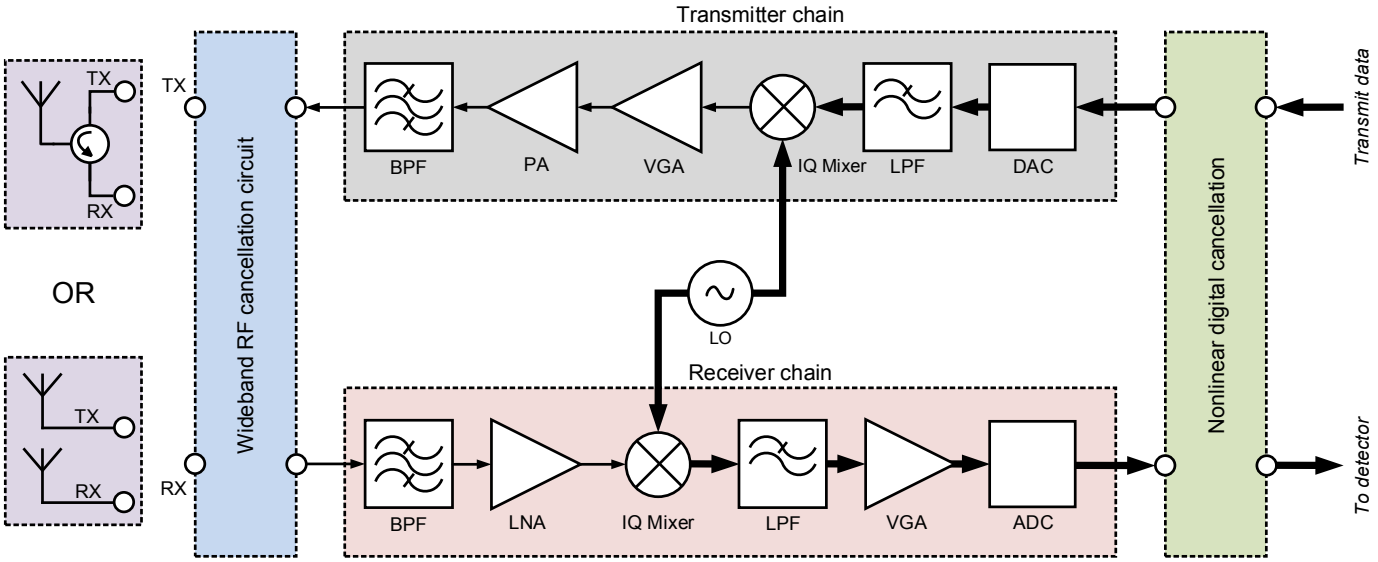

Fig. 1. A block diagram of a typical single-input single-output in-band full-duplex direct-conversion transceiver utilizing either a shared transmit/receive antenna or separate antennas. List of abbreviations: DAC, digital-to-analog conversion; LPF, low-pass filter; IQ, in-phase/quadrature-phase; LO, local oscillator; VGA, variable-gain amplifier; PA, power amplifier; BPF, band-pass filter; RF, radio-frequency; LNA, low-noise amplifier; ADC, analog-to-digital conversion.

II. Full-Duplex Military Radio Transceivers

A. General Full-Duplex Device Architecture

In general, the differences between legacy half-duplex transceivers and in-band full-duplex transceivers are related to the self-interference (SI), as already discussed. Especially, in typical civilian/commercial applications, the SI must be attenuated by *at least* 100 dB [1], [5], [6], which calls for extremely sophisticated processing techniques for SIC.

Figure 1 shows a general illustration of a typical in-band full-duplex transceiver [6], where the necessary SI suppression is implemented in three separate stages:

- The so-called *circulator* allows the transmitter and receiver to share the same antenna, while also providing some passive isolation between them. Typically, the SI is attenuated here by roughly 20 dB [6]. Alternatively, the transceiver may employ separate transmit and receive antennas that offer *physical isolation* between them.
- After the circulator, the SI is suppressed by an active *analog canceller*, which ensures that the SI power entering the actual receiver chain is not too high. The RF canceller can be expected to provide 40–50 dB of SI suppression, depending on the bandwidth [6], [7].
- Finally, the SI remaining after the first two stages is then suppressed in the digital domain by a *digital canceller*. By utilizing advanced nonlinear signal models, the digital canceller can attenuate the SI by as much as 40 dB [4], thereby cancelling it almost perfectly.

These different stages together can provide the required amount of SIC, and thereby facilitate STAR operation, even when using only a single antenna. However, it is reasonable to expect conservatively that effective military applications require even much more attenuation in each of these stages.

B. Requirements for Military Radios

When considering military radios, the requirements for the hardware and system level aspects are somewhat different from civilian/commercial applications. Namely, the need for high security and high reliability must be taken into account already when designing the actual transceivers [8], [9]. Perhaps the most distinguishing feature of the wireless networks designed for military use is their distributed and dynamic nature. In particular, the network topology is heavily time-variant and the different radios must be capable of constantly updating their knowledge regarding their close-by peers [10], or opponents. This means that each radio should always have up-to-date information about the other radios within its vicinity or otherwise it does not have sufficient knowledge about the current network topology. Such stringent requirement on the topology awareness calls for some sort of sensing solutions, meaning that each radio should be capable of listening the relevant information transmitted by others, while also informing other friendly radios about its presence [11].

Another relevant constraint for military radios is the scarcity of available bandwidth [12], [13]. This is caused by the increased bandwidth requirements of the commercial networks, resulting in less spectral resources for the military systems [14]. Hence, the spectral efficiency of the military transceivers must be as high possible for the network to be capable of fulfilling all the communication needs. In the legacy systems, this has been achieved by high spectral reuse, efficient waveforms, and prioritizing the information that is disseminated within the network [13]. In the future systems, the spectral efficiency can be further improved, for instance, by improving the cooperation between the radar and the communication systems [12], or by utilizing some of the recent advances in transceiver design, such as in-band full-duplex communications [6].

Military radios must also be able to tolerate jamming attacks, where a strong interfering signal is maliciously transmitted to disturb the data communication [2], [15], [16]. Hence, the situational awareness is an essential requirement in modern military context, and robust communication technologies are crucial to provide information between all platforms in the battlefield. Therefore, each transceiver must be capable of delivering and/or receiving at least some data even when there is a strong interfering signal present. Another perspective on this is that it would greatly benefit the transceiver if it was capable of some form of communication while it is itself jamming on the same frequency. This is of course very hard, if not impossible, with conventional radio technologies, while it could be facilitated by the STAR capability like envisioned in this paper and in [2].

In addition, high security within the network is needed in military applications, meaning that the transmitted data must be encrypted and secured for jamming by some means [17]. There are variety of approaches of achieving this such as chirp spread spectrum (CSS), direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS) and time-hopping (TH). The tactical data link (TDL) network standard Link 16 has become the major information channel within the military communication systems of the United States Joint Services, and forces of the North Atlantic Treaty Organization (NATO). Link 16 utilizes FHSS for improving immunity to jamming and introducing redundancy [18]. However, the communication is based on legacy half-duplex transceivers.

C. Using Full-Duplex Radios in Military Networks

When envisioning the usage of in-band full-duplex transceivers in military communication networks, the above different requirements must be carefully considered. In terms of the distributed nature of the network, the full-duplex capability allows for more efficient searching of the close-by radios, since it facilitates simultaneous transmission and sensing [19]. This has already been investigated in the context of cognitive radio systems, and shown to be feasible [20].

In-band full-duplex communication also helps in coping with the scarcity of the available bandwidth, since it can potentially provide a two-fold increase in the spectral efficiency [1], [6]. This is obviously a crucial advantage in helping to ensure the situation awareness and the tactical communication capabilities under all circumstances.

Malicious jamming is of course a serious challenge also for full-duplex transceivers, although there is already some literature available where the full-duplex capability is successfully used (in theory) to counter-act jamming. Furthermore, the capability to cancel the own transmission allows for generating a jamming signal while also receiving useful data [2]. Hence, in the context of jamming, the full-duplex capability creates variety of new possibilities in the radio level.

As for the transmitter–receiver isolation requirements in military networks, in typical data transfer applications the SI should obviously be cancelled as much as possible. This is especially crucial due to the limited bandwidth of the military

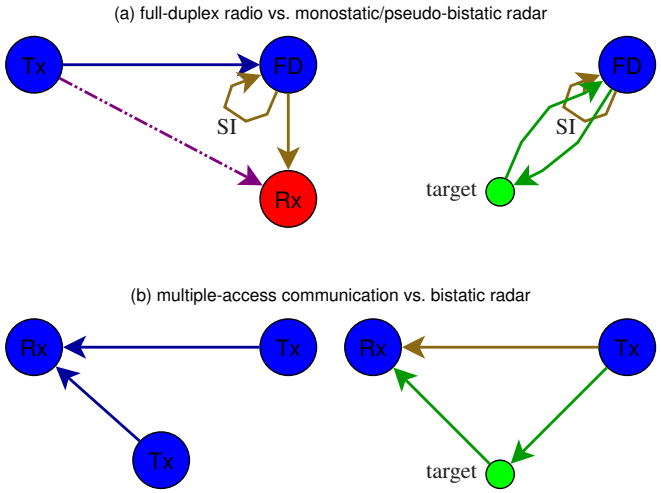

Fig. 2. The relationship between wireless communication and radar systems.

systems, since any residual SI will result in a decreased spectral efficiency. In this regard, many prototype implementations are already capable of obtaining the required SI isolation [4], [6]. Especially, in [6] an overall SIC of 90 dB is achieved with a shared transmit/receive antenna over a bandwidth of 80 MHz, while [4] reports 100 dB of suppression for a relay-type FD device over the same bandwidth.

D. Continuous-Wave Radar

A very specific field within military radios are the radars, which can be used to detect targets by transmitting and receiving electromagnetic signals. In this case, the direct leakage between the own transmitter and the own receiver must be efficiently suppressed, while the echoes from the targets must be successfully received, meaning that some form of SI cancellation is needed [1]. In the earlier applications, an isolation of 60 dB for the direct leakage was obtained [1], [21], while the more recent compact single-antenna radars have reportedly obtained suppression performances of 30–40 dB [22]–[24]. Although the compact radars typically operate in the mm-wave frequencies, these attenuation figures can be used as some sort of a ballpark figure for the SIC performance.

In fact, in-band full-duplex operation has already been used in the context of continuous-wave radars (as opposed to pulsed radars), such that the concept dates back to at least the 1940s [1]. Figure 2 illustrates the similarity between full-duplex radios and radars. In particular, a continuous-wave radar using one or two co-located antennas (monostatic or pseudo-bistatic) is technically similar to a one or two antenna full-duplex radio. However, the fundamental conceptual difference between radars and full-duplex radios is that, except for near-end local leakage, the echo signal looping back to a radar receiver is a useful signal revealing information about a target while the corresponding signal is completely self-interference for a full-duplex radio. Moreover, the isolation provided by circulators developed for monostatic radars is usually insufficient for communication purposes. On the other hand, bistatic radars

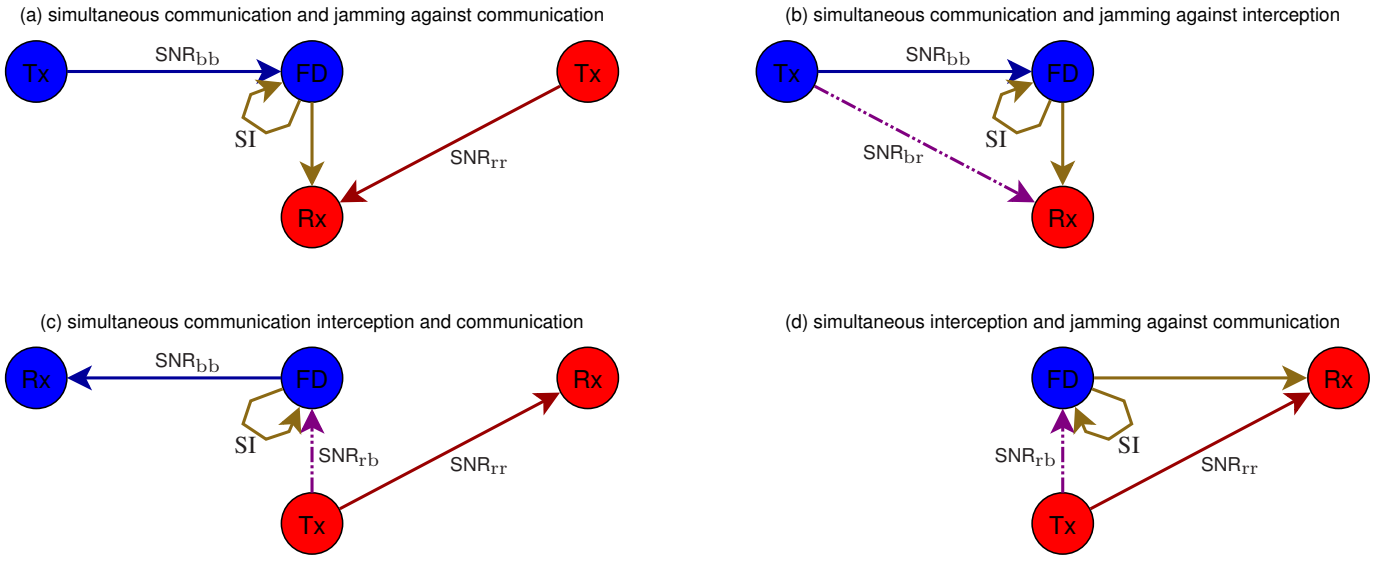

Fig. 3. Four military applications for the simultaneous transmission (Tx) and reception (Rx) capability of full-duplex (FD) radios under self-interference (SI).

are similar to a multiple-access communication scenario since they need to separate the direct leakage from the transmitter and echoes from a target (cf. signals from another transmitter).

The SI cancellation figures reported so far also indicate that the current full-duplex radios could be readily used for low-power military radar applications. Even though these radars typically use much higher frequencies than the reported full-duplex prototypes, many of the SI cancellation solutions could potentially be applied also to mm-wave systems. Moreover, for radar systems, it is not necessary to obtain as much isolation as for the data transfer applications [22]–[24]. Hence, even if the obtained amount of isolation in the higher frequencies was significantly less than the 90–100 dB obtained in the 2–3 GHz band, the current solutions could still most likely fulfill the isolation needs of the radar applications.

III. Analysis of Military Communication Applications for Full-Duplex Radios

Let us consider a military scenario, where two opposing teams (blue and red) use the same frequency band for communications and/or electronic warfare. The former use refers to the transfer of any information (e.g., voice, data or an activation signal) over a link between two radios in either team while the latter use can be interception or jamming that targets a radio in the other team. Let us further assume for simplicity that only one blue radio can operate in the FD mode and the red team does not possess such technology. Consequently, we can identify the four different system variations illustrated in Fig. 3 when both teams have at maximum two radios and they can be used for receiving either communication or interception signal and transmitting either communication or jamming signal. Plain two-way FD information transfer without electronic warfare is not considered herein because it is already widely studied in the civilian/commercial context.

A. Jamming against Communication

In the application of Fig. 3(a), both teams use the same frequency band for their communications. In a conventional case without any FD radios, the blue and red teams' communication links would achieve signal-to-noise ratios (SNRs) of $\mathsf{SNR}_{\rm bb}$ and $\mathsf{SNR}_{\rm rr}$, respectively. The STAR capability allows the blue receiver to transmit a jamming signal causing extra interference to the red receiver at the cost of suffering from self-interference. Thus, the blue and red teams' communication links achieve signal-to-interference-and-noise ratios (SINRs) of $\mathsf{SINR}_{\rm bb}$ and $\mathsf{SINR}_{\rm rr}$, respectively, that are given by

$$\mathsf{SINR}_{\rm bb} = \frac{\mathsf{SNR}_{\rm bb}}{P_{\rm SI}/P_{\rm N}+1} \quad \text{and} \quad \mathsf{SINR}_{\rm rr} = \frac{\mathsf{SNR}_{\rm rr}}{P_{\rm J}/P_{\rm N}+1}, \tag{1}$$

where $P_{\rm SI}$, $P_{\rm J}$ and $P_{\rm N}$ denote residual self-interference power in the blue receiver after SIC, jamming signal power disrupting the red receiver and background noise power, respectively.

The blue communication link achieves the information rate

$$R_{\rm bb} = \begin{cases} \log_2(1+\mathsf{SNR}_{\rm bb}), & \text{without jamming,} \\ \log_2(1+\mathsf{SINR}_{\rm bb}), & \text{with jamming,} \end{cases} \tag{2}$$

and the red communication link achieves the information rate

$$R_{\rm rr} = \begin{cases} \log_2(1+\mathsf{SNR}_{\rm rr}), & \text{without jamming,} \\ \log_2(1+\mathsf{SINR}_{\rm rr}), & \text{with jamming.} \end{cases} \tag{3}$$

Obviously, $\mathsf{SINR}_{\rm bb} < \mathsf{SNR}_{\rm bb}$ and $\mathsf{SINR}_{\rm rr} < \mathsf{SNR}_{\rm rr}$ so that both $R_{\rm bb}$ and $R_{\rm rr}$ decrease due to jamming. However, in principle, the SI signal can be suppressed more efficiently than the jamming signal ($P_{\rm SI} \ll P_{\rm J}$) so that $\mathsf{SINR}_{\rm bb}/\mathsf{SNR}_{\rm bb} \gg \mathsf{SINR}_{\rm rr}/\mathsf{SNR}_{\rm rr}$. For example, Fig. 4 illustrates the information rates in a symmetric scenario where the SNRs of links between all radios are equal. We see that jamming decreases $R_{\rm bb}$ much less than $R_{\rm rr}$ because $P_{\rm J}/P_{\rm SI} = 10$ dB. It actually may be worthwhile for the blue team to tolerate some rate loss in order to make much bigger impact on the red team's rate.

B. Jamming against Interception

The application of Fig. 3(b) is similar to the above one except that the jamming signal is now used as a countermeasure for interception. With jamming, the SINR for intercepting the blue communication link in the red receiver is given by

$$\mathsf{SINR}_{\mathrm{br}} = \frac{\mathsf{SNR}_{\mathrm{br}}}{P_{\mathrm{J}}/P_{\mathrm{N}} + 1}, \tag{4}$$

when the corresponding SNR without jamming is $\mathsf{SNR}_{\mathrm{br}}$. The information rate of the blue communication link is still given by (2) while the rate of the information leaking from the blue transmitter to the red receiver is given by

$$R_{\mathrm{br}} = \begin{cases} \log_2(1 + \mathsf{SNR}_{\mathrm{br}}), & \text{without jamming,} \\ \log_2(1 + \mathsf{SINR}_{\mathrm{br}}), & \text{with jamming.} \end{cases} \tag{5}$$

Obviously, if $\mathsf{SNR}_{\mathrm{br}} > \mathsf{SNR}_{\mathrm{bb}}$, e.g., the red receiver is closer to the blue transmitter than the blue receiver, then secure transmission is impossible with conventional technology. In contrast, it is possible to achieve $\mathsf{SINR}_{\mathrm{br}} < \mathsf{SINR}_{\mathrm{bb}}$ with FD operation such that $R_{\mathrm{br}} < R_{\mathrm{bb}}$ even if $\mathsf{SNR}_{\mathrm{br}} > \mathsf{SNR}_{\mathrm{bb}}$.

Based on the theory of physical-layer security [25], [26], the secure information rate of the blue communication link can be expressed as

$$R_{\mathrm{bb}}^{\mathrm{S}} = \left[R_{\mathrm{bb}} - R_{\mathrm{br}}\right]^{+}, \tag{6}$$

where $[x]^{+} = \max\{0, x\}$. Firstly, we can see that jamming decreases both R_{bb} and R_{br}. However, the effect on the latter is typically much more severe such that the secure rate $R_{\mathrm{bb}}^{\mathrm{S}}$ increases despite the total rate R_{bb} decreases. For example, in the example of Fig. 4, $R_{\mathrm{bb}}^{\mathrm{S}} = 0$ bit/s/Hz without jamming but the FD technology allows to achieve positive secure rate.

C. Simultaneous Interception and Communication

In the application illustrated in Fig. 3(c), the blue communication link uses the STAR capability for simultaneous interception. The SNR for interception would be $\mathsf{SNR}_{\mathrm{rb}}$ without simultaneous information transmission while it decreases to

$$\mathsf{SINR}_{\mathrm{rb}} = \frac{\mathsf{SNR}_{\mathrm{rb}}}{P_{\mathrm{SI}}/P_{\mathrm{N}} + 1} \tag{7}$$

in FD operation due to residual self-interference.

The information rate of the red communication link is given by (3) while the rate of the information leaking from the red transmitter to the blue receiver is given by

$$R_{\mathrm{rb}} = \log_2(1 + \mathsf{SINR}_{\mathrm{rb}}). \tag{8}$$

The corresponding secure information rate of the red communication link under interception is given by

$$R_{\mathrm{rr}}^{\mathrm{S}} = \left[R_{\mathrm{rr}} - R_{\mathrm{rb}}\right]^{+}. \tag{9}$$

It should be especially noted that performing simultaneous interception with information transmission does not affect the blue team's own rate so it comes at no cost during operation, if the transceiver has the STAR capability. Thus, it is always worthwhile to do as long as $\mathsf{SINR}_{\mathrm{rb}}$ is reasonably large such that R_{rb} is non-negligible like in the example of Fig. 4.

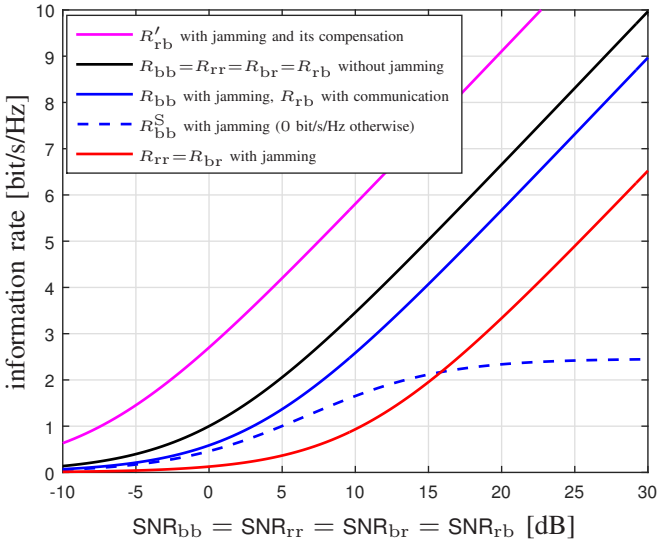

Fig. 4. Achievable information rates between transceivers in a symmetric battlefield scenario when $P_{\mathrm{SI}}/P_{\mathrm{N}} = 0$ dB and $P_{\mathrm{J}}/P_{\mathrm{N}} = 10$ dB.

D. Simultaneous Interception and Jamming

In the application illustrated in Fig. 3(d), the blue team transmits jamming to the red team's receiver in order to decrease its link quality from $\mathsf{SNR}_{\mathrm{rr}}$ to $\mathsf{SINR}_{\mathrm{rr}}$ which also decreases the link quality for interception from $\mathsf{SNR}_{\mathrm{rb}}$ to $\mathsf{SINR}_{\mathrm{rb}}$. However, the red team may try to compensate the jamming by increasing transmission power to achieve link quality $\mathsf{SINR}'_{\mathrm{rr}}$ ($\mathsf{SINR}'_{\mathrm{rr}} > \mathsf{SINR}_{\mathrm{rr}}$) by which the link quality for interception increases to $\mathsf{SINR}'_{\mathrm{rb}}$. It is possible that $\mathsf{SINR}'_{\mathrm{rb}} > \mathsf{SNR}_{\mathrm{rb}}$, i.e., it may be worthwhile to tolerate some self-interference in order to gain back much more from the opponent's countermove.

In the example of Fig. 4, the red transmitter increases its transmission power such that the link achieves information rate R'_{rr} that equals R_{rr} in the original case without jamming. Consequently, the maximum rate of information leaking to the blue transceiver increases significantly from R_{rb} to R'_{rb}. The secure information rate of the red team, $R_{\mathrm{rr}}^{\mathrm{S}}$, remains always zero in the example of Fig. 4, because they do not possess the FD technology. Otherwise, the smart countermove for jamming would be to launch jamming against potential interception if increasing transmit power is necessary.

IV. Conclusion

Inspired by the rapid advances in civilian/commercial full-duplex radios that we have recently observed, we believe that this progressive technology and the underlying unprejudiced idea of simultaneous transmission and reception on the same frequencies find their way in some form also to the field of military communications sooner or later. Thus, for the first time ever, this paper surveyed the prospects of the technology in electronic warfare in order to initiate scientific research on this emerging topic and to disseminate the idea to the military communications community. It is not out of the question that armed forces could gain a major technical advantage over an opponent that does not possess equivalent technology.

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, September 2014.

[2] 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, February 2014.

[3] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[4] 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*, 2016, in press.

[5] D. Korpi, T. Riihonen, V. Syrjälä, L. Anttila, M. Valkama, and R. Wichman, "Full-duplex transceiver system calculations: analysis of ADC and linearity challenges," *IEEE Transactions on Wireless Communications*, vol. 13, no. 7, pp. 3821–3836, Jul. 2014.

[6] 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.

[7] 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 (EUSIPCO)*, Aug. 2016, pp. 783–787.

[8] J. Nobre, D. Rosário, C. Both, E. Cerqueira, and M. Gerla, "Toward software-defined battlefield networking," *IEEE Communications Magazine*, vol. 54, no. 10, pp. 152–157, Oct. 2016.

[9] W. Medina-Pazmiño, A. Jara-Olmedo, and D. Valencia-Redrovín, "Analysis and determination of minimum requirements for a data link communication system for unmanned aerial vehicles- UAV's," in *Proc. IEEE Ecuador Technical Chapters Meeting (ETCM)*, Oct. 2016, pp. 1–6.

[10] N. Suri, G. Benincasa, M. Tortonesi, C. Stefanelli, J. Kovach, R. Winkler, U. S. R. Kohler, J. Hanna, L. Pochet, and S. Watson, "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *IEEE Communications Magazine*, vol. 48, no. 10, pp. 60–69, Oct. 2010.

[11] W. Abdellatief, H. Abdelkader, and M. Hadhoud, "An energy-efficient coverage hole detection technique for randomly deployed wireless senor networks," in *Proc. 11th International Conference on Computer Engineering Systems (ICCES)*, Dec. 2016, pp. 340–347.

[12] B. Paul, A. Chiriyath, and D. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. PP, no. 99, pp. 1–1, Dec. 2016.

[13] 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.

[14] J. Leland and I. Porche III, "Future army bandwidth needs and capabilities," RAND Corporation, Tech. Rep., 2004.

[15] Y. He, Y. Cheng, G. Wu, B. Dong, and S. Li, "Partial band noise jamming rejection with S-CFFH/16-QAM optimum and suboptimum maximum-likelihood receivers over Rayleigh fading channels with imperfect CSI," in *Proc. IEEE Military Communications Conference (MILCOM)*, Oct. 2015, pp. 842–847.

[16] A. Hansson, J. N. Senior, and K. Wiklundh, "Performance analysis of frequency-hopping ad hoc networks with random dwell-time under follower jamming," in *Proc. IEEE Military Communications Conference (MILCOM)*, Oct. 2015, pp. 848–853.

[17] L. O. Mailloux, M. R. Grimaila, J. M. Colombi, D. D. Hodson, R. D. Engle, C. V. McLaughlin, and G. Baumgartner, "Quantum key distribution: Examination of the decoy state protocol," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 24–31, Oct. 2015.

[18] W. J. Wilson, "Applying layering principles to legacy systems: Link 16 as a case study," in *Proc. IEEE Military Communications Conference (MILCOM)*, Oct. 2001, pp. 526–531.

[19] W. Cheng, X. Zhang, and H. Zhang, "Full duplex spectrum sensing in non-time-slotted cognitive radio networks," in *Proc. Military Communications Conference (MILCOM)*, Nov. 2011, pp. 1029–1034.

[20] V. Syrjälä, M. Valkama, M. Allén, and K. Yamamoto, "Simultaneous transmission and spectrum sensing in OFDM systems using full-duplex radios," in *Proc. IEEE 82nd Vehicular Technology Conference (VTC Fall)*, Sep. 2015.

[21] F. O'Hara and G. Moore, "A high performance CW receiver using feedthru nulling," *Microwave Journal*, vol. 6, p. 6371, Sep. 1963.

[22] J.-G. Kim, S. Ko, S. Jeon, J.-W. Park, and S. Hong, "Balanced topology to cancel Tx leakage in CW radar," *IEEE Microwave and Wireless Components Letters*, vol. 14, no. 9, pp. 443–445, Sep. 2004.

[23] K. Lin, Y. E. Wang, C. K. Pao, and Y. C. Shih, "A Ka-band FMCW radar front-end with adaptive leakage cancellation," *IEEE Transactions on Microwave Theory and Techniques*, vol. 54, no. 12, pp. 4041–4048, Dec. 2006.

[24] C. Y. Kim, J. G. Kim, and S. Hong, "A quadrature radar topology with Tx leakage canceller for 24-GHz radar applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 55, no. 7, pp. 1438–1444, Jul. 2007.

[25] Y. Liang, H. V. Poor, and S. Shamai (S.), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.